УДК 004.056.55

РЕШЕНИЕ КВАДРАТНЫХ УРАВНЕНИЙ В ПОЛЯХ ГАЛУА ХАРАКТЕРИСТИКИ 2

В.А. БОГРЕЦОВ, В.А. ЛИПНИЦКИЙ

Белорусский Государственный Университет
пр-т. Независимости, 4, Минск, 220030, Беларусь

Военная академия Республики Беларусь
Минск-57, 220057, Беларусь

Поступила в редакцию 24 октября 2012

Рассматриваются 4 метода решения квадратных уравнений в полях Галуа характеристики 2. В частности, предлагается авторская версия метода неопределенных коэффициентов. Проводится сравнительный анализ эффективности рассматриваемых методов, на основе которого даются рекомендации по применению данных на практике.

Ключевые слова: поле Галуа, характеристика поля, нормальный базис поля, формула Ченя, БЧХ-код, синдром ошибки, норма синдрома.

Введение

Решение многих задач науки и техники так или иначе связано с решением алгебраических уравнений. Во второй половине XX века бурное развитие теории и практики защиты информации актуализировало необходимость решения уравнений над конечными полями, называемых также полями Галуа. К примеру, в помехоустойчивом кодировании поиск *k*-кратных ошибок сводится к решению алгебраического уравнения степени k над полями Галуа. Такие же задачи актуальны и в защите информации от несанкционированного доступа. В криптографических протоколах на основе эллиптических кривых постоянно решается задача нахождения корней квадратных уравнений над полями Галуа. Следует отметить, что существующие методы практического решения алгебраических уравнений вызывают нарекания у пользователей ввиду вязкости и громоздкости выполняемых при этом вычислений. Особенно отмеченная ситуация усугубляется над полями характеристики 2, где становятся бесполезными самые стандартные формулы и методы.

В работе подводится итог исследований, проводимых с последней четверти XX века, по разработке и анализу методов решения квадратных уравнений над полями Галуа.

Необходимые сведения о полях Галуа

Всякое поле Галуа характеристики 2 содержит в качестве минимального подполя поле $GF(2) \cong Z/2Z$, является конечномерным векторным пространством над $Z/2Z$ и, следовательно, состоит из 2^m элементов, где m – размерность данного векторного пространства. Как фактор-кольцо, $GF(2^m)$ состоит из полиномов вида $a_{m-1}\alpha^{m-1}+\ldots+a_1\alpha+a_0$, где $a_i \in Z/2Z$ и $\alpha = \bar{x}$ – элемент фактор-кольца, порожденный полиномом $x \in Z/2Z[x]$. $GF\left(2^m\right)$ – является расширением Галуа поля $GF(2)$, поскольку его группа $GF(2)$ автоморфизмов является циклической порядка m и порождена степенями автоморфизма Фробениуса $\varphi: x \to x^2$.

Важным для дальнейшего является понятие следа элемента конечного поля. Для произвольного $\gamma \in GF(2^m)$ его след $tr(\gamma) = \gamma + \varphi(\gamma) + \varphi^2(\gamma) + \ldots + \varphi^{2^{m-1}}(\gamma) = \gamma + \gamma^2 + \gamma^{2^2} + \ldots + \gamma^{2^{m-1}}$.

Ясно, что $tr(\gamma) \in GF(2)$. Как известно [1], что ровно половина элементов в $GF(2^m)$ имеет след 0 и половина имеет след 1. Операция следа является линейным оператором $GF(2^m) \to GF(2)$. Наиболее просто след вычисляется, если элемент γ задан в нормальном базисе [1]. Базис $GF(2)$ – пространства $GF(2^m)$ вида

$$\beta, \varphi(\beta), \varphi^2(\beta), \ldots, \varphi^{2^{m-1}}(\beta) \qquad (1)$$

называется нормальным. При этом $tr(\beta) = 1$. Существование таких базисов было доказано Дэвенпортом в 1968 году [2]. Если $\gamma = \gamma_0\beta + \gamma_1\varphi(\beta) + \gamma_2\varphi^2(\beta) + \ldots + \gamma_{m-1}\varphi^{2^{m-1}}(\beta)$, то $tr(\gamma) = \gamma_0 + \gamma_1 + \ldots + \gamma_{m-1}$.

Предварительные сведения о квадратных уравнениях

Наиболее общий вид квадратного уравнения: $Ax^2 + Bx + C = 0$, $A \neq 0$. Поделив уравнение на A, приходим к уравнению

$$x^2 + ax + b = 0. \qquad (2)$$

***Предложение* 1.** Уравнение (2) имеет в поле $GF(2^m)$ двукратный корень тогда и только тогда, когда $a = 0$. В этом случае $x_1 = x_2 = b^{1/2} = b^v$, где $v = 2^{m-1}$.

Отметим, что в [3] предложена оригинальная процедура вычисления $b^{1/2}$ в конкретных конечных полях характеристики 2. Случай уравнения (2), когда $b = 0$, легко решается: $x_1 = 0$, $x_2 = a$.

Далее будем считать, что в уравнении (2) коэффициенты a и b не равны нулю и принадлежат полю $GF(2^m)$. Такое уравнение имеет два различных корня либо в $GF(2^m)$, либо в его конечном расширении. В силу предложения 1, уравнение (2) нельзя привести к двучлену вида $x^2 + b = 0$. В полях характеристики 2 канонической формой уравнения (2) принято считать уравнение вида

$$t^2 + t + \gamma = 0 \qquad (3)$$

для некоторого $\gamma \in GF(2^m)$. Уравнение (2) приводится к виду (3) заменой $x = at$ [4]. При этом $\gamma = b / a^2$. Каноническая форма удобна тем, что если найден один корень t_1 уравнения (3), то второй корень получается автоматически: $t_2 = t_1 + 1$. Именно для канонического уравнения (3) имеет место критерий его разрешимости.

***Предложение* 2.** (Берлекэмп, Рамсей, Соломон) [5, 6]. Уравнение (2) над полем $GF(2^m)$ имеет корни в этом поле тогда и только тогда, когда $tr(\gamma) = 0$.

Формула и метод Ченя

***Предложение* 3.** (Чень) [7]. Пусть в уравнении (3) $tr(\gamma) = 0$, $\beta, \beta^2, \ldots, \beta^{2^{m-1}}$ – нормальный базис поля $GF(2^m)$ над $GF(2)$ и $\gamma = \gamma_0\beta + \gamma_1\varphi(\beta) + \gamma_2\varphi^2(\beta) + \ldots + \gamma_{m-1}\varphi^{2^{m-1}}(\beta)$. Тогда корень уравнения (3) $x_0 = \gamma_0\beta + (\gamma_0 + \gamma_1)\varphi(\beta) + (\gamma_0 + \gamma_1 + \gamma_2)\varphi^2(\beta) + \ldots + (\gamma_0 + \gamma_1 + \ldots + \gamma_{m-1})\varphi^{2^{m-1}}(\beta)$.

К сожалению, формула Ченя уже с виду выглядит достаточно громоздкой. Реальное ее применение сразу же наталкивается на проблему построения нормального базиса в поле $GF(2^m)$. На сегодняшний день, в общем случае, процедура поиска нормального базиса не имеет эффективного алгоритма и фактически является переборной: по очереди перебирают элементы поля $GF(2^m)$, для каждого из них составляют систему (1) и исследуют ее на линейную

зависимость. В [8] дана оценка количества нормальных базисов для поля $GF(p^m)$, согласно которой, с ростом m, вероятность нахождения нормального базиса за разумное время стремится к нулю. На практике наиболее часто используется стандартный базис $1,\alpha,\alpha^2,\ldots,\alpha^{m-1}$. Поэтому возникает необходимость перехода от полиномиального базиса к нормальному и обратно. Как отмечено в [9], сам Чень отчаялся найти упрощения в этом конгломерате вычислений, предложил отказаться от его формул и использовать для решения уравнения (3) метод последовательной подстановки элементов поля в это уравнение. Из уважения к его трудам, эта очевидная процедура носит название «метод Ченя».

***Замечание* 1.** Для применения на практике формулу Ченя можно несколько улучшить следующим образом. Пусть B – матрица перехода к нормальному базису, T – матрица, соответствующая преобразованию из формулы Ченя (очевидно, что оно линейно). Тогда формулу Ченя можно записать следующим образом $t = TB\gamma$. При этом, непосредственно из формулы Ченя и формулы следа элемента, заданного в нормальном базисе, следует, что t_{m-1} (коэффициент вектора t при $\varphi^{2^{m-1}}(\beta)$) будет являться следом γ. К примеру, над полем $GF(2^6)$ минимальное количество битовых операций, для перехода к нормальному базису и обратно равно 14, при этом еще необходимо выполнить 6 битовых операций в формуле Ченя, что в сумме дает 20 битовых операций. Минимальное же количество битовых операций, требуемых для решения уравнения (3), с использованием матрицы TB равно 16.

***Замечание* 2.** Не трудно заметить, что в поле $GF(2^m)$ в худшем случае для решения уравнения (3) по формуле Ченя с известной матрицей перехода к нормальному базису и известной матрицей для обратного перехода к полиномиальному базису требуется $2m^2 + m$ битовых операций: m^2 для перехода к нормальному базису, m непосредственно для самой формулы и m^2 для обратного перехода к полиномиальному базису. Если использовать оптимизацию из замечания 1, то требуется только $2m^2$ операций: m^2 для перехода к нормальному базису и m^2 для обратного перехода к полиномиальному базису. Таким образом, сложность решения уравнения (3) по формуле Ченя оценивается величиной $O(m^2)$ битовых операций.

Метод неопределенных коэффициентов

Альтернативой формулам Ченя является метод неопределенных коэффициентов, который опирается только на стандартный базис $1,\alpha,\alpha^2,\ldots,\alpha^{m-1}$.

Согласно *предложению* 2, если в уравнении (3) $tr(\gamma) = 0$, то его корни принадлежат полю $GF(2^m)$, над которым данное уравнение и рассматривается. Пусть t – один из корней уравнения (3). Как элемент поля $GF(2^m)$, его можно представить в виде $t = t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}$, $t_i \in GF(2)$. Подставим данное выражение t в уравнение (3). Получим соотношение: $\left(t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}\right)^2 + \left(t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}\right) + \gamma = 0.$ Так как в поле характеристики 2 выполняется равенство $(a+b)^2 = a^2 + b^2$ [1], то последнее соотношение преобразуется к виду:

$$\left(t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}\right)^2 + \left(t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}\right) + \gamma =$$
$$= t^2{}_0 + t^2{}_1\alpha^2 + \ldots + t^2{}_{m-1}\alpha^{2(m-1)} + t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1} + \gamma.$$

где $t_i \in GF(2)$, поэтому $t_i^2 = t_i$, и последнее равенство будет эквивалентно следующему:

$$\gamma + t_0 + t_1\alpha^2 + \ldots + t_{m-1}\alpha^{2(m-1)} + t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1} = 0. \qquad (4)$$

Согласно [1], $GF(2^m) \cong (Z/2Z)[x]/ < p(x) >$, где $p(x)$ – некоторый неприводимый над $Z/2Z[x]$ полином. После приведения равенства (4) по модулю $p(\alpha)$, получим уравнение относительно неизвестных $t_0, t_1, \ldots, t_{m-1}$:

$$\left(a_{m-1,m-1}t_{m-1}+\ldots+a_{m-1,1}t_1+a_{m-1,0}t_0\right)\alpha^{m-1}+\ldots+$$

$$+\left(a_{1,m-1}t_{m-1}+\ldots+a_{1,1}t_1+a_{1,0}t_0\right)\alpha+\left(a_{0,m-1}t_{m-1}+\ldots+a_{0,1}t_1+a_{0,0}t_0\right)+\gamma=0.$$

Так как система $1,\alpha,\ldots,\alpha^{m-1}$ линейно независима, то данное равенство равносильно системе уравнений

$$\begin{cases} a_{0\ 0}t_0+\ldots+a_{0\ m-1}t_{m-1}=\gamma_0 \\ a_{1\ 0}t_0+\ldots+a_{1\ m-1}t_{m-1}=\gamma_1 \\ \qquad\qquad \ldots \\ a_{m-1\ 0}t_0+\ldots+a_{m-1\ m-1}t_{m-1}=\gamma_{m-1} \end{cases}, \tag{5}$$

где $\gamma=\gamma_0+\gamma_1\alpha+\ldots+\gamma_{m-1}\alpha^{m-1}$. Далее для краткости будем называть систему (5) соответствующей уравнению (3).

***Предложение* 4.** Пусть над полем $GF(2^m)$ задано уравнение (3) и $At=\gamma$ – соответствующая ему система (5), записанная в матричном виде. Тогда матрица A может быть приведена элементарными преобразованиями строк к виду:

$$A'=\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Доказательство. Так как γ не влияет на матрицу A, то можно ограничиться рассмотрением уравнения

$$t^2+t=0 \tag{6}$$

Очевидно, 0 является решением этого уравнения. Так как характеристика поля равна 2, то 1 также является решением. Согласно теореме Безу, квадратное уравнение может иметь не больше двух корней и, следовательно, других решений уравнение (6) иметь не может. Система (5) для уравнения (6) будет однородной. Ее решениями будут вектора $(0,0\ldots,0)$, $(1,0\ldots,0)\in(Z/2Z)^m$. Следовательно, фундаментальная система решений будет иметь вид $(\tau,0,\ldots,0)$, $\tau\in Z/2Z$. Но это означает, что базисный минор матрицы A системы (5) для уравнения (6) расположен в столбцах с номерами $2,\ldots,m$, поэтому матрицу A можно элементарными преобразованиями строк привести к требуемому виду.

***Следствие* 1.** Пусть задано уравнение (3) над полем $GF(2^m)$ и $At=\gamma$ – соответствующая ему система (5). Пусть далее $S_1,\ldots,S_n\in M_m(Z/2Z)$ – элементарные матрицы, соответствующие элементарным преобразованиям строк, приводящим матрицу A к A', $S=S_1S_2\ldots S_n$, $\gamma'=S\gamma$. При этом $\gamma',\gamma'+1$ – корни уравнения (3) тогда и только тогда, когда $\gamma'_0=0$, где

$$\gamma'=\gamma'_0+\gamma'_1\alpha+\ldots+\gamma'_{m-1}\alpha^{m-1}.$$

Тогда, если $\gamma'_0=1$, то уравнение не имеет решений.

Доказательство. Достаточно записать систему $SAt=A't=S\gamma=\gamma'$ в явном виде

$$\begin{cases} 0 = \gamma'_0 \\ t_1 = \gamma'_1 \\ \cdots \\ t_{m-1} = \gamma'_{m-1} \end{cases}.$$

Из предложения 2 вытекает

***Следствие* 2.** Из предложения 2 и следствия 1 вытекает следующее утверждение:

$\forall \gamma \in GF(2^m) \quad tr(\gamma) = \gamma'_0$.

Замечание 3. Очевидно, для решения квадратных уравнений над заданным полем не обязательно вычислять матрицу S каждый раз. Она может быть вычислена однажды для конкретного $p(x)$ и затем использоваться для решения уравнения (3) с произвольным γ.

***Замечание* 4.** Не трудно заметить, что решение уравнения (3) в поле $GF(2^m)$ методом неопределенных коэффициентов с известной матрицей S в худшем случае требует m^2 битовых операций. Таким образом, метод неопределенных коэффициентов для решения уравнения (3) имеет сложность в худшем случае $O(m^2)$.

Пример 1. Рассмотрим поле $F = GF\left(2^5\right) = (Z/2Z)[x]/ < 1 + x^2 + x^5 >$. Система (5) для уравнения (6) в этом поле имеет матрицу

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Непосредственные вычисления показывают, что в данном случае

$$S = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Рассмотрим над полем F квадратное уравнение $t^2 + t + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$. Для этого уравнения $\gamma = (1,1,1,1,1)$ и

$$S\gamma = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \gamma'.$$

Здесь $tr(\gamma) = \gamma'_0 = 0$, следовательно, $t_1 = \alpha^3 + \alpha^4$, $t_2 = 1 + \alpha^3 + \alpha^4$ – решения уравнения

$t^2 + t + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$.

Пример 2. Рассмотрим над полем из примера 1 уравнение $t^2 + t + 1 + \alpha + \alpha^2 + \alpha^4 = 0$. Для этого уравнения матрица S будет та же, что и в примере 1, $\gamma = (1,1,1,0,1)$:

$$S\gamma = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \gamma'$$

$tr(\gamma) = \gamma'_0 = 1$, следовательно, данное уравнение в поле F решений не имеет.

***Замечание* 5.** В некоторых случаях может быть более эффективным не вычисление произведения $S\gamma$, а применение к γ преобразований, соответствующих матрице S. В этом можно убедиться, рассмотрев поле $(Z/2Z)[x]/<1+x^2+x^3+x^4+x^8>$.

Ниже в табл. 1 приводится сравнение производительности решения уравнения (3) в поле $GF(2^m)$ в полиномиальном базисе по формуле Ченя (с оптимизацией из замечания 3) и методом неопределенных коэффициентов.

Таблица 1. **Сравнение эффективности формулы Ченя и метода неопределенных коэффициентов**

m	n_1	$p_1(x)$	n_2	$p_2(x)$
4	8	$1+x+x^4$	4	$1+x+x^4$
5	14	$1+x^2+x^5$	5	$1+x^3+x^5$
6	15	$1+x+x^6$	7	$1+x+x^6$
7	31	$1+x+x^2+x^3+x^4+x^5+x^7$	9	$1+x^3+x^7$
8	33	$1+x^3+x^5+x^7+x^8$	14	$1+x^2+x^3+x^4+x^8$
9	33	$1+x+x^4+x^5+x^6+x^8+x^9$	12	$1+x^5+x^9$

В табл. 1 n_1 – количество битовых операций, требуемых для решения уравнения (3) по формуле Ченя в поле $(Z/2Z)[x]/<p_1(x)>$, p_1 – примитивный многочлен, по которому строится поле, в котором решение уравнения (3) по формуле Ченя оптимально среди остальных примитивных многочленов над $Z/2Z$ такой же степени, n_2 – количество битовых операций, требуемых для решения уравнения (3) методом неопределенных коэффициентов в поле $(Z/2Z)[x]/<p_2(x)>$, p_2 – примитивный многочлен, по которому строится поле, в котором решение уравнения (3) методом неопределенных коэффициентов оптимально среди остальных примитивных многочленов над $Z/2Z$ такой же степени. Из табл. 1 и *замечаний* 2 и 4 видно, что метод неопределенных коэффициентов имеет более высокую эффективность для решения квадратных уравнений в полях Галуа характеристики 2, чем метод, основанный на формуле Ченя.

***Замечание* 6**. В [6] над полями $GF(2^m)$ с нечетным m рассмотрено применение метода неопределенных коэффициентов, приводящее к более громоздким вычислениям.

Норменный метод

В [4] предложен довольно нестандартный метод решения уравнения (2), при котором даже не требуется переход к уравнению (3). Суть его заключается в тесной связи между уравнениями над $GF(2^m)$ и двоичными БЧХ-кодами [3]. Известно [3], что декодирование БЧХ-кодов C_{2t+1}, способных исправлять t-кратные ошибки, сводится к решению алгебраического уравнения степени t над полем Галуа. В [10] разработана теория норм синдромов, позволяющая не прибегать к решению уравнений для декодирования БЧХ-кодов. Согласно [4], норма синдрома для двоичного БЧХ-кода C_5 длиной $n = 2^m - 1$, исправляющего двойные ошибки, определяется как величина $N = s_2 / s_1^3 \in GF(2^m)$, где (s_1, s_2) – синдром принятого сообщения. Алгоритм декодирования такого кода норменным методом заключается в следующем [4].

1. Строится список $T=\{N_0,N_1,\ldots,N_\theta\}$, где $N_i=N(e_i)$ – норма образующей вектор-ошибки [10] $e_i=(1,i)$, $0\le i\le\theta=2^{m-1}-1$.

2. Вычисляется синдром $S=(s_1,s_2)$, $s_1,s_2\in GF(2^m)$ очередного принятого сообщения.

3. Если $S=(s_1,s_2)\neq\overline{0}$, вычисляется норма данного синдрома $N=N(S)=s_2/s_1^3$.

4. Находится номер k полученного значения N в списке T, для которого $N_k=N$. Соответствующей ему образующей вектором-ошибкой будет $e_k=(1,k)$.

5. Вычисляется $s_1/s_1^k=\alpha^\mu\in GF(2^m)$, $0\le\mu\le 2^m-1$, α – примитивный элемент поля $GF(2^m)$.

6. При помощи найденного значения μ вычисляется $e=\sigma^\mu(e_k)=(t_1,t_2)$ – искомый вектор ошибки, где t_1,t_2 – локаторы ошибочных позиций, σ – оператор циклического сдвига вправо.

***Замечание* 7.** Для применения на практике норменного метода декодирования БЧХ-кода список T из пункта 1 достаточно вычислить однажды и сохранить в ПЗУ декодирующего устройства. Таким образом, нахождение ошибочных позиций в принятом сообщении сводится буквально к нескольким арифметическим операциям в поле Галуа.

Опишем теперь, как можно применить норменный метод для решения квадратных уравнений в конечном поле характеристики 2. Пусть над полем $GF(2^m)$ задан двоичный БЧХ-код C_5 длиной $n=2^m-1$. Пусть $S=(s_1,s_2)$ – синдром принятого сообщения, $s_1,s_2\in GF(2^m)$. Согласно [4], если $x=\alpha^u$, $y=\alpha^v\in GF(2^m)$ [4], α – примитивный элемент поля $GF(2^m)$ удовлетворяют следующей системе уравнений:

$$\begin{cases} x+y=s_1,\\ x^3+y^3=s_2. \end{cases}$$

то $u+1, v+1$ – номера ошибочных позиций в принятом сообщении. Так как $x^3+y^3=(x+y)(x^2-xy+y^2)=s_1(s_1^2+xy)=s_2$, то исходная система может быть преобразована к более простому виду

$$\begin{cases} x+y=s_1,\\ xy=s_1^2+s_2/s_1. \end{cases}$$

Данная система, исходя из формул Виета, эквивалентна следующему квадратному уравнению $t^2+s_1t+s_1^2+s_2/s_1=t^2+at+b=0$ над полем $GF(2^m)$. Так как корни данного уравнения являются локаторами ошибочных позиций, соответствующих синдрому (s_1,s_2), то, с учетом выше приведенного метода декодирования, получаем следующий алгоритм решения уравнения (2) [4].

1. Вычисляется $N=1+b/a^2$.
2. В списке T находится $N_k=N$.
3. $t_1=a/(1+\alpha^{k+1})$.
4. $t_2=t_1\alpha^{k+1}$.

Пример 3. Решим норменным методом уравнение из примера 1 над тем же полем. В данном случае список T будет иметь следующий вид

Таблица 2. **Показатели норм синдромов двойных ошибок примитивного БЧХ-кода с $n=31$**

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$degN_i$	12	22	24	18	13	21	17	20	5	10	26	9	11	3

В соответствии с предложенным алгоритмом, вычислим норму

$$N = 1 + \frac{b}{a^2} = 1 + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = \alpha^{24}.$$

В табл. 2 $deg N_3 = 24$, следовательно, $k = 3$. Поэтому $t_1 = a/(1+\alpha^4) = 1/(1+\alpha^4) = \alpha^3 + \alpha^4$, $t_2 = (\alpha^3 + \alpha^4)\alpha^4 = 1 + \alpha^3 + \alpha^4$.

При многократном решении квадратных уравнений (2) над полем $GF(2^m)$, норменный метод демонстрирует наибольшую простоту и эффективность применения.

Заключение

Проведено исследование и дана сравнительная оценка четырех основных методов решения квадратных уравнений над полями Галуа характеристики 2. Следует, что формула Ченя имеет скорее теоретическое значение для решения данной задачи. Для практического же применения более эффективными являются метод неопределенных коэффициентов и, особенно, норменный метод. Последний, в свою очередь, может применяться для уравнений более высоких степеней в полях произвольной положительной характеристики и поэтому представляет особенный интерес для дальнейшего изучения.

SOLVING OF QUADRATIC EQUATIONS OVER FINITE FIELDS OF CHARACTERISTIC 2

V.A. BOGRETSOV, V.A. LIPNITSKI

Abstract

There are four solving methods of quadratic equations over Galois finite fields of characteristic 2 considered in this article. Particularly it is proposed to get acquainted with the author`s version of the undetermined coefficients method. There is a contrastive analysis of considered methods efficiency, on which basis are given recommendations to practice the data.

Литература

1. *Лидл Р., Нидеррайтер Г.* Конечные поля. М., 1988.
2. *Davenport H.* // J. London Math. Soc. 1968. Vol. 43. P. 21-39.
3. *Берлекэмп Э.* Алгебраическая теория кодирования. М., 1971.
4. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн., 2007.
5. *Berlekamp E.R.* // Info. and Control. 1967. Vol. 10. P. 553-564.
6. *Болотов А.А., Гашков С.Б., Фролов А.Б.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М., 2012.
7. *Chen C.L.* // IEEE Trans. of inf. Theory. 1982. Vol. 28, №5. P. 792-794.
8. *Болотов А.А., Гашков С.Б., Фролов А.Б. и др.* Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М., 2012.
9. *Муттер В.М.* Основы помехоустойчивой телепередачи информации. Л., 1990.
10. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М., 2004.