изделий, когда на каждой стадии проектирования важно видеть их реальный конструкторский состав [2], что имеет принципиальное значение как для подразделений СПбГЭТУ «ЛЭТИ», осуществляющих выполнение НИР и НИОКР, так и для выполнения работ по заказу предприятий – стратегических партнеров.

С учетом отмеченных выше достоинств, использование программных продуктов ООО «Нанософт разработка» является основой повышения эффективности учебного процесса в рамках дисциплин, реализуемых кафедрой Прикладной механики и инженерной графики – «Инженерная графика», «Прикладная механика», «Биомеханика», программы которых имеют вариативную адаптацию для подготовки студентов по большинству направлений подготовки, реализуемых в СПбГЭТУ «ЛЭТИ», в частности: 11.03.03 «Конструирование и технология электронных средств», 11.03.04 «Электроника и наноэлектроника», 11.05.01 «Радиоэлектронные системы и комплексы», 13.03.02 «Электроэнергетика и электротехника» и другие [3], а также для выполнения НИР и НИОКР в широком диапазоне задач проектирования изделий электронной техники, медицинского приборостроения, систем обеспечения функционирования интеллектуальных пунктов пропуска.

**Список литературы**

1. Афонин П.Н., Титов А.В. Разработка технических средств потокового контроля веса транспортных средств в пунктах пропуска через государственную границу Российской Федерации // Бюллетень инновационных технологий. 2022. Т. 6. № 3 (23). С. 75-77.

2. ООО «Нанософт разработка»: официальный сайт. – Москва,2022 –URL: http:// www.nanocad.ru (дата обращения 12.08.2022)

3. СПбГЭТУ «ЛЭТИ» Первый электротехнический: официальный сайт. – СПб, 2022 – URL: http:// www.etu.ru (дата обращения 12.08.2022).

## МЕТОД НАХОЖДЕНИЯ КОРНЕЙ МНОГОЧЛЕНА НАД РАСШИРЕННЫМ ПОЛЕМ ГАЛУА НА ОСНОВЕ КОРНЕЙ АФФИННОГО МНОГОЧЛЕНА

***Фам Хак Хоан***
*докцент, к.т.н, Технический университет им. Ле Куй Дона, Социалистическая Республика Вьетнам*
***Нгуен Тьен Тхай***
*к.т.н, Технический университет им. Ле Куй Дона, Социалистическая Республика Вьетнам*
***Ву Шон Ха***
*к.т.н, Институт науки и технологии, Социалистическая Республика Вьетнам*

***Pham Khac Hoan***
*Assoc. Prof., PhD, Le Quy Don Technical University, Ha Noi, Vietnam*
***Nguyen Tien Thai***
*PhD, Le Quy Don Technical University, Ha Noi, Vietnam*
***Vu Son Ha***
*PhD, Institute of Science and Technology, Ha Noi, Vietnam*

**АННОТАЦИЯ**

В статье предложен метод нахождения корней многочлена над расширенным полем Галуа на основе корней аффинного многочлена. Предложенный метод позволяет уменьшить задержку вычисления по сравнению с традиционномыми методами, что дает возможность использования в высокоскоростной системе передачи информации.

**ABSTRACT**

The article proposes a method for finding the roots of a polynomial over an extended Galois field based on the roots of an affine polynomial. The proposed method makes it possible to reduce the calculation delay in comparison with traditional methods, which makes it possible to use in a high-speed communication system.

**Ключевые слова**: Поле Галуа; кодирование, контролирующее ошибки; полиномиальный базис; нормальный базис.

**Key words**: Galois field, error control coding, polynomial basis, normal basis.

### 1. ВВЕДЕНИЕ

Конечное поле широко используется в радиотехнике и компьютерной технике, например в помехоустойчивом кодировании, шифровании на основе кодов и шифровании на эллиптических кривых. Не только неполное понимание теоретических основ конечного поля, но и реализация устройства для решения задач над конечным полем вызывают множество трудностей для исследовательского процесса.

Некоторые задачи, связанные с решением уравнения над конечным полем, например необходимо решить ключевое уравнение при декодировании БЧХ-кода, кодов Рида-Соломона,

Гоппы в помехоустойчивом кодировании и в шировании на основе кодов. Берлекэмп один из авторов имеет большой вклад в решении проблем анализа сомножителей над конечным полем [1].

Некоторые методы решения уравнения над конечным полем: циклические алгоритмы на основе процесдуры Ченя, преобразования Фурье над полем Галуа…[2, 3, 4]. Но перечисленные методы имеют большое время задержки, связанное с высокой сложностью вычисления.

Линеаризированный многочлен и аффинный многочлен имеют особенные свойства, позволяющие облегчить процесс их нахождения решений. Но незначительные многочлены являются линеаризированными или аффинными многочленами. На основе алгебраических преобразований и нахождения найменшего аффинного кратного заданного многочлена возможно найти корни исходного многочлена в множестве корней аффинного многочлена [5, 6].

В данной статье исследован метод нахождения корней многочлена над полем GF($p^n$) на основе корней аффинного многочлена, также данно основание создания устройства для эффективного решения задачи. Полученные результаты могут использоваться в других случаях, включая поля с разными размерностями.

Статья включает в себе следующие части: введение; часть 2 – основы конечного поля; часть 3 – исследование классы особенных многочленов: линеаризированные многочлены над конечным полем и проблема нахождения их корней; заключение.

**2. Основы конечного поля**

*2.1. Представление элементов конечного поля*

Пусть простое число $p$, обозначим конечное поле с порядком $p$ как $F_p$ или GF($p$), это множество целых чисел $Z_p$ с операцией mod $p$. Расширенное поле $F_q$ содержит $q = p^n$ элементов является векторным пространством над $F_p$ некоторой размерности $n \geq 1$.

Функция “след” для элемента $c \in F_q$ определяется следующим образом:

$$Tr(c) = c + c^p + c^{p^2} + \ldots + c^{p^{n-1}}. \quad (1)$$

Имеется: $Tr(nc) = n \cdot Tr(c)$.

В частности, при $p = 2$, $Tr(1) = 1$ при $n$ нечетном и $Tr(1) = 0$ при $n$ четном. Отметим, что уравнение $x^2 + x + D = 0$, $D \in \mathrm{GF}(2^n)$ имеет корни тогда и только тогда, когда $Tr(D) = 0$.

Конечное поле GF($p^n$) порождается неприводимым многочленом $\pi(x)$ степени $n$. Особенно когда используется примитивный многочлен $\pi(x)$, то расширенное поле GF($p^n$) построится на основе присоединения к GF($p$) корней $\alpha$ многочлена $\pi(x)$ над GF($p$). На практике существуют два вида представления с использованием полиномиального и нормального базисов.

* *Полиномиальный базис*

Пусть поле GF($p^n$) и $\alpha \in$ GF($p^n$) – корень примитивного неприводимого многочлена степени $n$ над полем GF($p$). Полиномиальным базисом поля GF($p^n$) над GF($p$) является базис {1, $\alpha$, $\alpha^2$ ... $\alpha^{n-1}$}, где $\alpha$ – примитивный элемент поля GF($p^n$).

* *Нормальный базис*

Известно, что всегда существует нормальный базис конечного поля GF($p^n$) над GF($p$). Если $\gamma \in$ GF($p^n$) порождающий элемент над полем GF($p$), то нормальным базисом поля GF($p^n$) называется базис вида $\left\{\gamma, \gamma^{p^1}, \gamma^{p^2} \ldots \gamma^{p^{n-1}}\right\}$.

Например, для поля GF($2^4$) с порождающим многочленом $\pi(x) = x^4 + x + 1$, имеющим 2 нормального базиса, порождающие примитивным элементом $\gamma = \alpha^7$ и непримитивным элементом $\gamma = \alpha^3$.

*2.2. Операции над конечным полем*

Обычные алгебраические операции над полем GF($2^n$) осуществляются по модулю неприводимого многочлена $\pi(x)$ над GF(2). Операции сложения и вычитания по модулю 2. Операция сложения двух многочлена осуществляется с помощью операции XOR, операция умножения над полем GF($2^n$) имеет высокую сложность и большой затрат времени для ее вычисления. Сложность еще зависит от выбора неприводимого многочлена и базиса, используемая для представления конечных элементов.

При реализации устройства, квадрат элемента с нормальным базисом может осуществляться циклическим сдвигом, а операция умножения более сложно реализуется. Умножение двух элементов поля с полимиальным базисом может выполняться как умножение двух обычных многочленов, а результат

получается по модулю порождающего многочлена $\pi(x)$. На практике часто используются устройства умножения использованием логарифмически-антилоарифмической таблицы и функции Зеха. В процессе вычисления, если сложение и умножение чередуются, то необходимо преобразовать векторное представление в степеньное с помощью логарифмической и антилогарифмической [7, 8].

**3. Линеаризированный многочлен и его корни**

Процессдура Ченя и аналитический способ предназначены для нахождения корней многочлена над конечным полем имеет высокую сложность, особенно для поля с большой размерностей и с большой степеней многочлена. Существуется класс особенных многочленов – линеаризированные многочлены, нахождение корней которых является облегченной задачей. В данном разделе рассматриваются линеаризированный многочлен, нахождение линеаризированного многочлена, как наименьшее кратное заданного многочлена, корни которого могут определены на основе анализа корней линеаризированного многочлена.

*3.1. Линеаризированный многочлен*

Многочлен $L(z)$ над полем $\mathrm{GF}(p^n)$ называется линеаризированным, если он имеет вид

$$L(z)=\sum_i L_i z^{p^i} \qquad (2)$$

.

Например, многочлен $L(z)=z+z^2+z^4$ - это линеаризованный многочлен для всех $n.$ Кроме этого, высше приведенная функция “след” тоже является линеаризованным многочленом.

Отметим, что автор в [2] доказал, что пусть корни многочлена $L(z)$ принадлежат расширенному полю $\mathrm{GF}(p^m),\ m>n,$ они образуют векторное подпространство в $\mathrm{GF}(p^m)$. Наоборот, для векторного подпространства $n$ размерности над $\mathrm{GF}(p^m),$ многочленом $L(z)=\prod_{\beta\in U}(z-\beta)$ является линеаризированным над $\mathrm{GF}(p^m)$, т. е.

$$L(z)=\sum_i L_i z^{p^i}=L_0 z+L_1 z^p+\ldots+L_{n-1}z^{p^{n-1}}+z^{p^n}. \qquad (3)$$

Корни линеаризированного многочлена $L(z)$ образуют подпространство $M$ над $\mathrm{GF}(p^n)$. Если $\gamma\in M$ то $\gamma^p\in M$ так $L^p(\gamma)=L(\gamma^p).$ Если векторное подпространство обладает этим свойством, то оно называется модулем. Если $L_0\neq 0$, то $L(z)$ не имеет кратные корни, и в дальнейшем мы будем рассматривать только этот случай.

*3.2. Корни линеаризированного многочлена*

Учитывая, что линеаризированный многочлен $L(z)$ над $\mathrm{GF}(p^n)$, описываемый выражением (2), предполагая $\gamma$ его примитивный корень, $L(z)$ является многочленом степени $p^n$, корни этого многочлена имеют вид:

$$\delta_0\gamma+\delta_1\gamma^p+\ldots+\delta_{n-1}\gamma^{p^{n-1}}, \qquad (4)$$

где $\delta_i\in\mathrm{GF}(p)$ и эти корни образуют модуль с нормальным базисом $\left\{\gamma,\gamma^p,\ldots,\gamma^{p^{n-1}}\right\}$.

Рассмотрим задачу нахождения корней линеаризированного многочлена.

Пусть $\alpha^0,\alpha^1,\ldots,\alpha^{n-1}$ - полимиальный базис поля $\mathrm{GF}(p^n)$.

*Теорема 1 [2]*

$L(z)$ - линеаризированный многочлен над $\mathrm{GF}(p^n)$, элемент $z$ представляется следующим образом $z=\sum_k Z_k\alpha^k,\ \ Z_k\in\mathrm{GF}(p)$ тогда

$$L(z) = \sum_k Z_k L(\alpha^k) \quad (5)$$

Используя представление элементов $L(\alpha^i) = \sum_{j=0}^{m-1} C_{i,j}\alpha^j$, тогда коэффициент разложения многочлена по базисом многочлена рассчитывается следующим образом:

$$[L_0, L_1, ..., L_{n-1}] = [Z_0, Z_1, ..., Z_{n-1}].C, \quad (6)$$

где

$$C = \begin{bmatrix} C_{0,0} & C_{0,1} & C_{0,1} & \cdot & \cdot & \cdot & C_{0,n-1} \\ C_{1,0} & C_{1,1} & C_{1,2} & \cdot & \cdot & \cdot & C_{1,n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ C_{n-1,0} & C_{n-1,1} & C_{n-1,2} & \cdot & \cdot & \cdot & C_{n-1,n-1} \end{bmatrix}. \quad (7)$$

Многочлен $A(z)$ над $\mathrm{GF}(p^n)$ называется аффинным, если $A(z) = L(z) - u,$ где $L(z)$ линеаризированный многочлен и $u \in \mathrm{GF}(p^n).$ Корни аффинного многочлена можно найти, решая систему линейных уравнений, как показано в примере 1.

Основные свойства линеаризировнных и аффинных многочленов [2].

1. Многочлен $L(z)$ является линеаризированным тогда и только тогда, когда его корни образуют линейное пространство над $\mathrm{GF}(p)$, их корни имеют одинаковые кратные и являются степенями $p$.

2. Многочлен $A(z)$ является аффинным тогда и только тогда, когда его корни образуют аффинное пространство над $\mathrm{GF}(p)$, их корни имеют одинаковые кратные и являются степенями $p$.

3. Наибольший общий делитель двух линеаризированных многочленов является линеаризированным многочленом.

4. Наибольший общий делитель двух аффинных многочленов является аффинным многочленом.

Частный случай аффинного полинома 2-ой степени над $\mathrm{GF}(2^n)$ позволяет вычислить его корни без решения системы линейных уравнений. Квадратное уравнение можно привести к каноническому виду

$$y^2 + y = u. \quad (8)$$

Уравнение (8) имеет корни над $\mathrm{GF}(2^n)$ тогда и только тогда, когда $Tr(u) = 0.$ Обозначая $\alpha \in \mathrm{GF}(2^n)$ - произвольный элемент со степенью $n$, $g = \alpha^k$ - элемент, при котором $Tr(g) = 1.$ Тогда с $i = 0,1,...,n-1$, можно найти $y_i$ такое, что:

$$y_i^2 + y_i = \begin{cases} \alpha^i \quad при \quad Tr(\alpha^i) = 0; \\ \alpha^i + \alpha^k \quad при \quad Tr(\alpha^i) = 1. \end{cases} \quad (9)$$

Для решения уравнения $y^2 + y = u = \sum_{i=0}^{n-1} U_i \alpha^i, U_i \in \mathrm{GF}(2)$, предположим

$$y = \sum_{i=0}^{n-1} U_i y_i \quad (10)$$

Тогда имеем:

$$y^2 + y = \sum_{i=0}^{n-1} U_i (y_i^2 + y_i) = u + \alpha^k \sum_{i=0}^{n-1} U_i Tr(\alpha^i) = \\ = u + \alpha^k Tr\left( \sum_{i=0}^{n-1} U_i \alpha^i \right) = u + \alpha^k Tr(u). \quad (11)$$

Поэтому корни уравнения (8) являются $y' = \sum_{i=0}^{n-1} U_i y_i$ и $y'' = 1 + \sum_{i=0}^{n-1} U_i y_i$.

Половина элементов поля $\mathrm{GF}(2^n)$ имеет след равен 0, а другая половина имеет след равен 1. Разделив поле на циклотомические смежные классы, можно хранить корни более эффективно, зачем используя формулы (9) - (11) для нахождения корней. При использовании орбитального представления по циклотомическим смежным классам сохроняются только ведущие элементы, образующие циклотомические классы. Следовательно, количество рассматриваемых элементов уменьшается от $2^n$ примерно до $n$, что значительно снижает объем памяти, необходимый для хранения приблизительно $2^n / n$ раз. В табл. 1 представлены орбиты с параметром $u$, соответствующим смежным классом, и соответствующие корни $y', y''$ над GF(2ⁿ) с порождающими многочленами $x^3 + x + 1$; $x^4 + x + 1$; $x^5 + x^2 + 1$; $x^6 + x + 1$; $x^7 + x + 1$. Параметры $u$ соответствуют элементам (их следы равны нулями), ведущим циклотомическими классами. Аналогичным образом можно строить орбиты для поля большего размера и хранить их в памяти, используемой для вычисления корней квадратных уравнений. Обратите внимание, что в этой таблице элементы поля представлены десятичными числами $N$, называются модифицированными логарифмами:

$$N = \log_\alpha(\alpha^i) + 1 = i + 1 = \mathrm{Log}(\alpha^i). \quad (12)$$

Таблица 1.

**Орбитальное представление по параметру $u$ над GF(2ⁿ) и корни**

| n | $u$ | $y'$ | $y''$ | n | $u$ | $y'$ | $y''$ | n | $u$ | $y'$ | $y''$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 3 | 7 | | 1 | 22 | 43 | | 2 | 17 | 113 |
| | 1 | 6 | 11 | | 2 | 18 | 48 | | 4 | 26 | 106 |
| 4 | 2 | 8 | 10 | | 4 | 15 | 53 | | 6 | 7 | 127 |
| | 6 | 2 | 5 | 6 | 8 | 2 | 7 | | 10 | 27 | 111 |
| | 2 | 4 | 30 | | 10 | 23 | 57 | 7 | 12 | 45 | 95 |
| 5 | 8 | 3 | 6 | | 14 | 31 | 47 | | 16 | 37 | 107 |
| | 16 | 22 | 26 | | 28 | 37 | 55 | | 24 | 72 | 80 |
| | | | | | | | | | 30 | 43 | 115 |
| | | | | | | | | | 56 | 81 | 103 |

*3.3. Кратный аффинный многочлен*

Большинство многочленов над $\mathrm{GF}(p^n)$ не являются аффинными. Например, при $p$=2 многочлен 3-ой степени не является аффинным, однако можно найти аффинный многочлен 4-ой степени, кратный многочлену 3-ой степени. Корни многочлена 3-ей степени можно найти через корни многочлена 4-ой степени. В общем случае для многчлена $f(z)$ $d$-ой степени мы можем использовать следующий алгоритм для нахождения кратного аффинного $L(z) - u$ этого многочлена.

*Алгоритм 1 [2]*

1. Вычисление $z^k \bmod f(z)$ с $k = d, d+1, ..., (d-1)p$;

2. На основе результатов вычисления на первом шаге вычислить остатки $r^{(0)}(z), r^{(1)}(z), ..., r^{(i)}(z)$, с $r^{(i)}(z) = z^{p^i} \bmod f(z)$;

3. Решение системы линейных уравнений

$$\left[u, L_0, L_1, ..., L_{d-1}\right]\begin{bmatrix} 0 & 0 & ... & 0 & -1 \\ r_{(d-1)}^{(0)} & ... & ... & r_1^{(0)} & r_0^{(0)} \\ r_{(d-1)}^{(1)} & ... & ... & r_1^{(1)} & r_0^{(1)} \\ ... & ... & ... & ... & ... \\ r_{(d-1)}^{(d-1)} & ... & ... & r_1^{(d-1)} & r_0^{(d-1)} \end{bmatrix}. \quad (13)$$

Рассмотрим решение уравнения 3-ей степени с момощью кратного аффинного многочлена 4-ой степени.

Пусть многочлен $f(z) = z^3 + \alpha^{13} z^2 + z + \alpha^3$, с $\alpha^4 + \alpha + 1 = 0$. Найти аффинный многочлен, который является кратным $f(z)$. Вычисляем:

$$z^3 \bmod f(z) = \alpha^{13} z^2 + z + \alpha^3;$$

$$\begin{aligned} z^4 \bmod f(z) &= \alpha^{13} z^3 + z^2 + \alpha^3 z = \\ &= \alpha^{26} z^2 + \alpha^{13} z + \alpha^{16} + z^2 + \alpha^3 z = \\ &= (\alpha^{11} + 1) z^2 + (\alpha^{13} + \alpha^3) z + \alpha = \\ &= \alpha^{12} z^2 + \alpha^8 z + \alpha. \end{aligned}$$

Вычисляем $r^{(i)}(z) = z^{2^i} \bmod f(z)$;

$$r^{(0)}(z) = z^1 \bmod f(z) = z;$$

$$r^{(1)}(z) = z^2 \bmod f(z) = z^2;$$

$$r^{(2)}(z) = z^4 \bmod f(z) = \alpha^{12} z^2 + \alpha^8 z + \alpha.$$

Имеем систему уравнений

$$\left[u, L_0, L_1, L_2\right]\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ \alpha^{12} & \alpha^8 & \alpha \end{bmatrix} = 0.$$

Предположим, что выбраны корни $u = \alpha^2, L_0 = \alpha^8, L_1 = \alpha^{12}, L_2 = 1$ и $L(z) = \alpha^8 z + \alpha^{12} z^2 + z^4$.

Для нахождения корней этого линеаризированного многочлена, мы вычисляем значения:

$$\begin{aligned} L(1) &= \alpha^8 + \alpha^{12} + 1 = 1 + \alpha + \alpha^3; \\ L(\alpha) &= \alpha^9 + \alpha^{14} + \alpha^4 = 0; \\ L(\alpha^2) &= \alpha^{10} + \alpha^{16} + \alpha^8 = 0; \\ L(\alpha^3) &= \alpha^{11} + \alpha^{18} + \alpha^{12} = 1 + \alpha^3. \end{aligned}$$

Отсюда можно найти корни уравнения $L(z) = \alpha$, решив систему уравнений

$$[Z_0, Z_1, Z_2, Z_3]\begin{bmatrix}1 & 1 & 0 & 1\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 1\end{bmatrix} = [0100].$$

Выше упомянутая система уравнений имеет корни $Z = [1011] = \alpha^{13}$; $Z = [1111] = \alpha^{12}$. Корень $\alpha^{13}$ - ненужный посторонний корень, $\alpha^{12}$ корень многочлена $f(z)$, который можно разложить на множители:

$$f(z) = z^3 + \alpha^{13}z^2 + z + \alpha^3 = (z + \alpha^{12})(z^2 + \alpha z + \alpha^6).$$

Осуществляя нахождение корней многочлена $z^2 + \alpha z + \alpha^6$ по изложенной выше методике, находим две корней $\alpha^7, \alpha^{14}$.

Кроме того, для многочлена третьей степени вида $f(z) = z^3 + az^2 + bz + c$ проще найти кратный аффинный многочлен вида:

$$A(z) = (z^3 + az^2 + bz + c)(z + a) = z^4 + (a^2 + b)z^2 + (ab + c)z + ac.$$

**4. Решение уравнения четвертой степени**

Поле $\mathrm{GF}(2^n)$ комбинированый метод алгебраического преобразования и аффинного многочлена реализован для более эффективного поиска решения следующим образом.

Рассмотрим уравнение 4-ой степени над GF($2^n$)

$$x^4 + Ax^3 + Bx^2 + Cx + D = 0. \quad (14)$$

Подстановка $x = y^{-1} + \sqrt{C/A}, \quad A \neq 0,$ можно получить уравнение

$$a_3y^4 + a_2y^2 + a_1y + a_0 = 0, \quad (15)$$

где

$$a_3 = D + BC/A + (C/A)^2; \quad a_2 = B + \sqrt{AC}, a_1 = A, a_0 = 1. \quad (16)$$

При $a_3$, $a_2 \neq 0$ заменяя $y = z\sqrt{a_2/a_3}$ получим уравнение

$$z^4 + z^2 + E_1z + E_2 = 0, \quad (17)$$

где $E_1 = a_1\sqrt{a_3/a_2^3}; \quad E_2 = a_3/a_2^2.$

В этом случае левая часть (17) является аффинным многочленом и его решение можно найти на основе решения системы линейных уравнений, описанного в разделе 3.2. Как только решение найдено, используя обратные замены для нахождения корней исходного уравнения.

**5. Заключение**

В статье представлено улучшение формулы расчета корней уравнения 2-ой степени для уменьшения объема памяти таблиц в примерно $2^n/n$ раз за счет орбитального представления в циклотомическом смежном классе. В статье также предлагается метод решения уравнений 3-ой и 4-ой степеней над конечным полем за счет нахождения корней аффинных многочленов 4-ой степени. Метод решения уравнений над конечным полем с помощью процедуры Ченя (путем перебора всех элементов поля) использует $O(2^n t^2)$ умножений. С помощью нахождения корня аффинного многочлена сложность вычисления составляет примерно $O(nt)$. Таким образом, предлагаемый метод позволяет значительно снизить сложность при решении уравнения не слишком большой степени, тем самым повысит

быстродействие в схемах декодирования кодов БЧХ и Рида-Соломона.

**Литература**

1. Bijan Ansari, *Finite field arithmetic and its* application in cryptography / Dissertation for the degree Doctor of Philosophy in Electrical Engineering, University of California, Los Angeles, 2012.

2. Elwyn R Berlekamp, Algebraic Coding Theory (Revised Edition), World Scientific Publishing Co. Pte. Ltd., 2015.

3. Муттер, В.М. Основы помехоустойчивой телепередачи информации, Л.: Энергоатомиздат, Ленинградское отделение, 1990.

4. Конопелько, В.К. и др. Теория прикладного кодирования. Мн.: БГУИР, 2004.

5. F. J. MacWilliams, N. J. A.Sloane, The theory of error correction codes, Elselvier, 1977.

6. Fedorenko S. V., Trifonov P. V. Finding roots of polynomials over finite fields, IEEE Transactions on Communications, 2002, Vol. 50, Issue 11, pp. 1709–1711

7. Johann Groβschadl, A low-power bit serial multiplier for finite fields GF($2^m$). $34^{th}$ IEEE International symposium on ciruits and system, vol. IV, 2001.

8. Chin-Chin Chen, Chiou Yng Lee, Erl-Huei Lu, Scalable and systolic montgomery multipliers over GF($2^m$), IEICE Transaction Fundamentals, Vol. E91, No.7 July 2008.