ЧИСЛЕННЫЕ МЕТОДЫ И АНАЛИЗ ДАННЫХ

Параллельная машинная арифметика для рекуррентных систем счисления в неквадратичных полях

В.М. Чернов [1 2]
[1] *ИСОИ РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН,*
443001, Россия, Самарская область, г. Самара, ул. Молодогвардейская, д. 151,
[2] *Самарский национальный исследовательский университет имени академика С.П. Королёва,*
443086, Россия, Самарская область, г. Самара, Московское шоссе, д. 34

Аннотация

В работе предлагается новый метод синтеза систем машинной арифметики для «безошибочных» параллельных вычислений. Отличием предлагаемого подхода от вычислений в традиционных системах остаточных классов для прямой суммы модулярных колец является параллелизация вычислений в неквадратичных расширениях простых конечных полей, элементы которых представлены в системах счисления, порождёнными последовательностями степеней корней характеристического полинома рекуррентной последовательности. Работа продолжает и обобщает исследования автора, в которых, в частности, рассматривались рекуррентные соотношения *n*-боначчи (трибоначчи, тетрабоначчи и т.д.).

Ключевые слова: конечные поля, рекуррентная система счисления, параллельная машинная арифметика.

Цитирование: **Чернов, В.М.** Параллельная машинная арифметика для рекуррентных систем счисления в неквадратичных полях / В.М. Чернов // Компьютерная оптика. – 2020. – Т. 44, № 2. – С. 274-281. – DOI: 10.18287/2412-6179-CO-666.

Citation: Chernov VM. Parallel machine arithmetic for recurrent number systems in non-quadratic fields. Computer Optics 2020; 44(2): 275-282. DOI: 10.18287/2412-6179-CO-666.

Введение

Целью работы является введение и исследование нового класса параллельных систем «безошибочных» вычислений, связанных не со структурной разложимостью («параллелизуемостью») алгебры, в которой производятся вычисления (как, например, при вычислениях в системах остаточных классов (СОК)) [1, 2], а с представлением элементов этой алгебры в специальных позиционных системах счисления в виде, адаптированном к проведению параллельных вычислений. Кроме того, вычисления проводятся в конечных полях, что позволяет при разумном выборе параметров этих полей избежать накопления неконтролируемой вычислительной погрешности, характерной при вычислениях с обычными рациональными аппроксимациями вещественных или комплексных чисел.

Несмотря на то, что арифметические операции ($\mathrm{mod}\, p$) не являются для большинства вычислительных устройств элементарными компьютерными операциями, для некоторых простых чисел p арифметика конечного поля $\mathbf{F}_p$ может быть более «дружественной компьютеру». Наиболее известными примерами таких простых чисел являются:

- простые числа Мерсенна $p = 2^q - 1$,
- простые числа Ферма $p = 2^{2^k} + 1$,
- простые числа Голомба $p = 3 \cdot 2^q + 1$.

В этих и некоторых других случаях [3 – 5], например, при «естественном» для полей Мерсенна и Ферма представлении элементов полей в (редуцированной) двоичной системе счисления, умножения сводятся к сложениям представляющих элементы бинарных кодов и к их (циклическим) регистровым сдвигам. Для упомянутых классов простых чисел разработаны как алгоритмические, так и аппаратные средства вычислений в соответствующих модулярных кольцах (полях) [3, 6].

К сожалению, простых чисел Мерсенна, находящихся в «пользовательском диапазоне» специалиста-прикладника, очень мало (простых чисел Ферма ещё меньше). Использование в качестве модулей составных чисел добавляет к непосредственно вычислительным проблемам принципиальные теоретические трудности, связанные с существованием в модулярных кольцах по составным модулям делителей нуля и, как следствие, с возможной необратимостью некоторых элементов соответствующих колец.

Некоторым паллиативом является метод распараллеливания вычислений в СОК [1, 2], синтез которых в настоящее время представляет собой скорее чисто технологическую, а не теоретическую задачу, так как тезис: ***«если алгебраическая структура*** $\mathbf{A}$ ***изоморфна прямой сумме структур той же категории*** $\mathbf{A} \cong \mathbf{A}_1 \oplus \mathbf{A}_2 \oplus \ldots \mathbf{A}_r$***, то вычисления в структуре*** $\mathbf{A}$ ***можно распараллелить и заменить «покомпонент-***

ными» вычислениями в подструктурах $\mathbf{A}_1, \mathbf{A}_2, ..., \mathbf{A}_r$***»,*** является давно известным, хрестоматийным фактом, частные случаи систематического использования которого восходят едва ли не к методу координат Р. Декарта, несмотря на то, что при вычислениях в СОК этот факт используется в весьма специфической версии «китайской теоремы об остатках».

К относительным недостаткам СОК относится тот факт, что характерные преимущества «битовой» реализации арифметических операций в кольцах, например, по модулям простых чисел Мерсенна не наследуются при распараллеливании вычислений в случае составного числа Мерсенна по модулям *сомножителей* чисел такого вида, так как эти сомножители уже числами Мерсенна не являются.

Таким образом, как достоинства, так и недостатки вычисления в СОК вполне определяются самим принципом распараллеливания, связанным с разложением основной вычислительной структуры в прямую сумму подструктур той же категории. То есть определяются *«хорошим» представлением (разложением) множества, в котором производятся вычисления, и использованием структурных алгебраических свойств такого представления.*

В данной работе предлагается принципиально иной подход к распараллеливанию вычислений, связанный с представлением/разложением не вычислительной *структуры в целом*, а с представлением/разложением *каждого отдельного элемента* этой структуры в конечном множестве систем счисления с возможностью эффективных и параллельных реализаций арифметических операций в таких синтезированных системах счисления.

Подобный подход для ряда частных случаев некоторых квадратичных полей был предложен автором впервые в [7] для квадратичных полей и в сочетании с традиционной идеей «СОК-распараллеливания» (см. также [8 – 11]). В настоящей работе исследуется более общий случай систем счисления, порождённых линейными рекуррентными соотношениями n-го порядка в неквадратичных кольцах.

1. Синтез основной вычислительной структуры

Будем рассматривать последовательности, порожденные линейным рекуррентным соотношением

$$L(k+n) = \varepsilon_1 L(k+(n-1)) + ... + \varepsilon_n L(k),\ \varepsilon_n = \pm 1 \qquad (1)$$

n-го порядка с условием $\varepsilon_i \in \{-1, 0 +1\} = \Omega$.

Хорошо известно (например, [12 – 13]), что если все корни α_i характеристического полинома

$$f_n(x) = x^n - \varepsilon_1 x^{n-1} - \varepsilon_2 x^{n-2} - ... - \varepsilon_n x^0 \qquad (2)$$

различны, то общим решением уравнения (1) является функция

$$L(k) = \sum_{j=o}^{n-1} C_j \alpha_j^k ,$$

где константы C_i взаимно-однозначно определяются начальными значениями последовательности (1)

$$\big(L(0), ..., L(n-1)\big) \leftrightarrow (C_0, ..., C_{n-1}) .$$

Замечание 1. Далее в работе будем рассматривать исключительно рекуррентные функции – решения соотношения (1) – с такими начальными условиями, что

$$\big(L(0), \dots, L(n-1)\big) \leftrightarrow (C_0, \dots, C_{n-1}) = (1,1 \dots ,1), \qquad (3)$$

то есть для которых справедливо равенство

$$L(k) = \sum_{j=o}^{n-1} \alpha_j^k . \qquad (4)$$

■

Пусть простое число p таково, что характеристический полином (2) рекуррентного соотношения (1) неприводим над конечным полем $\mathbf{F}_p$ из p элементов. Будем искать возможность представления и целых чисел, и элементов конечных полей в форме

$$z = \sum_{k=0}^{d(z)} \xi_k L\big(k\big), \quad \xi_k \in \Omega \subset \mathbf{Z}.$$

Рассмотрим фактор-кольцо кольца полиномов $\mathbf{Q}[x]$ над $\mathbf{Q}$ по главному идеалу, порождённому полиномом $f_n(x) \in \mathbf{Q}[x]$:

$$\mathbf{Q}\big[x\big] \Big/ \Big[f_n\left(x\right) \Big] \to \mathbf{K} \supset \mathbf{Q}.$$

В случае неприводимости $f_n(x)$ кольцо $\mathbf{K}$ является полем алгебраических чисел – *полем разложения полинома* $f_n(x)$, в котором данный полином имеет n корней $a_1, \dots, a_n$ с учётом их кратности.

Рассмотрим также фактор-кольцо кольца полиномов $\mathbf{F}_p[x]$ над $\mathbf{F}_p$ по главному идеалу, порождённому полиномом $f_n(x) \in \mathbf{F}_p[x]$:

$$\begin{gathered} \mathbf{F}_p\left[x\right] \Big/ \Big[f_n\left(x\right) \Big] \to \mathbf{F}_q = \mathbf{F}_{p^n} = \\ = \left\{ z = \sum\nolimits_{i=0}^{n-1} \mu_i \omega^i : \mu_i \in \mathbf{F}_p ; f_n\left(\omega\right) = 0 \right\} . \end{gathered} \qquad (5)$$

По построению поля $\mathbf{F}_{p^n} = \mathbf{F}_q$ как фактор-кольца элемент ω равен одному из корней γ полинома (2) в поле $\mathbf{F}_q$, остальные корни γ_j в поле $\mathbf{F}_q$ получаются действием автоморфизма Фробениуса $\theta : z \to z^p$ на элемент γ:

$$\gamma_0 = \gamma, \gamma_1 = \theta\big(\gamma\big) = \gamma^p, ..., \gamma_{n-1} = \big(\theta \circ ... \circ \theta\big)\big(\gamma\big) = \gamma^{p^{n-1}} .$$

Так как мультипликативная группа элементов конечного поля циклична, то мультипликативные порядки $Ord(\gamma_i) = d$ корней γ_i совпадают и равны одному из де-

лителей порядка мультипликативной группы $\mathbf{F}_q^*$, равного

$$Ord\left(\mathbf{F}_q^*\right) = p^n - 1 = q - 1,\ d \left| (q-1). \right.$$

Замечание 2. Вопрос о нахождении мультипликативных порядков конкретных элементов конечных полей в конкретных полях является самостоятельной непростой теоретической и вычислительной задачей (см. [14]). ■

Далее, исходя из наличия априорной информации о диапазоне обрабатываемых целочисленных данных в конкретной решаемой прикладной задаче и характеристик используемых вычислительных средств (разрядность, допустимая степень распараллеливания и т.п.), выберем рекуррентное соотношение (1) и простое число p с условием неприводимости характеристического полинома $f_n(x)$ в поле $\mathbf{F}_p$.

В соответствии с выбранными параметрами n, p рассмотрим расширение $\mathbf{F}_q = \mathbf{F}_{p^n}$ поля $\mathbf{F}_p$, а именно фактор-кольцо кольца полиномов $\mathbf{F}_p[x]$ над $\mathbf{F}_p$ по главному идеалу, порождённому полиномом $f_n(x)$. Это фактор-кольцо далее будем рассматривать как основную структуру, в которой будем синтезировать (параллельные) алгоритмы вычислений.

Осторожный оптимизм по отношению к такому выбору указанного класса алгебраических структур базируется на следующих неформальных соображениях.

• *Если допустить,* что простое p и d настолько велики, что все целые числа z, участвующие в вычислительной процедуре в качестве входных и выходных данных, допускают представление в форме (то есть в «L – системе счисления»)

$$z = \sum_{k=0}^{d-1} \xi_k \hat{L}(k), \tag{6}$$

где $\hat{L}(k)$ – последовательность-образ $L(k)$ при редукции $\mathbf{Z} \to \mathbf{Z}/(p)$, то для элемента z, наряду с представлением (6), справедливо и представление

$$z = \sum_{k=0}^{d-1} \xi_k \hat{L}(k) = \sum_{k=0}^{d-1} \xi_k \sum_{j=0}^{n-1} (\alpha_j)^k = \sum_{j=0}^{n-1} \left(\sum_{k=0}^{d-1} \xi_k (\alpha_j)^k \right). \tag{7}$$

Таким образом, переход от представления (6) к представлению (7) даёт возможность вычислять не в «неканонической» L*–системе счисления,* а параллельно в n системах счисления более традиционного вида с экспоненциальными базисами γ_j ($j = 0, 1, ..., n-1$).

• Так как все $\gamma = \gamma_j \in \mathbf{F}_q$ есть корни уравнения

$$\gamma^n = \varepsilon_1 \gamma^{n-1} + \varepsilon_2 \gamma^{n-2} + ... + \varepsilon_n \gamma^0,$$

то при возникновении при выполнении арифметических операций «недопустимых» коэффициентов

$$\pm 2 \notin \{-1, 0, +1\} = \Omega,$$

соответствующее слагаемое в результирующей сумме относительно просто преобразуется к «допустимому» виду. Действительно, если

$$\gamma^n - \varepsilon_1 \gamma^{n-1} - ... - \varepsilon_{n-1} \gamma^1 - 1 \cdot \gamma^0 = 0,$$

то

$$\gamma^n - \varepsilon_1 \gamma^{n-1} - ... - \varepsilon_{n-1} \gamma^1 + 1 \cdot \gamma^0 = 2.$$

Поэтому

$$2 = \begin{cases} \gamma^n - \varepsilon_1 \gamma^{n-1} - ... - \varepsilon_{n-1} \gamma^1 + 1 \cdot \gamma^0, & \text{при } \varepsilon_n = 1; \\ -\gamma^n + \varepsilon_1 \gamma^{n-1} + ... + \varepsilon_{n-1} \gamma^1 + 1 \cdot \gamma^0, & \text{при } \varepsilon_n = -1. \end{cases} \tag{8}$$

Замечание 3. В дальнейшем, если из контекста ясна принадлежность элемента кольцу целых чисел или его модулярной редукции $\mathbf{Z}/(p)$, автор не будет подчеркивать эту разницу в обозначениях. ■

2. О представлении чисел в системе счисления с базисами L(k)

Рассмотрим возможность представления целых чисел в позиционной системе счисления с базисом $\{L(k) : k = 0, 1, ...\}$ и цифрами $\Omega = \{-1, 0, +1\}$.

В работе мы сознательно ограничиваемся относительно важными практически случаями рекуррентных последовательностей (1) и множеством цифр Ω.

Определение 1. Целочисленная последовательность называется *полной последовательностью*, если любое положительное целое число может быть выражено в виде суммы значений из последовательности, при этом каждое значение можно использовать только один раз. ■

Наиболее известным результатом относительно представления целых чисел суммами членов фиксированной последовательности является теорема Броуна [15].

Теорема. (Brown, [15]). Пусть целочисленная последовательность y_m неубывающая и

$$Y(\mu) = \sum_{m=0}^{\mu} y_m .$$

Тогда условия

$$y_0 = 1;\ Y(\mu - 1) \geq y_\mu - 1\ \forall \mu \geq 1 \tag{9}$$

являются необходимыми и достаточными для последовательности y_m, чтобы она была полной. ■

Последнее утверждение позволяет находить представление элементов $z \in \mathbf{Z}$ в форме

$$z = \sum_{k=0}^{t} \xi_k L(k),\ \xi_k \in \{0, 1\}$$

в случае полноты последовательности $L(k)$ с помощью так называемого *жадного* алгоритма, а именно: от числа z последовательно шаг за шагом отщепляются слагаемые таким образом, что

$$z \doteq z_t = L(t) + z_{t-1},\ \text{где}\ L(t) > \sum_{k=0}^{t-1} \xi_k L\left(k\right)$$

и так далее.

К сожалению, непосредственное применение критерия Теоремы для представления целого числа в системе счисления с рассматриваемыми базисами $\{L(k): k = 0, 1, ...\}$ и множеством цифр $\Omega = \{-1, 0, +1\}$ невозможно по ряду причин, в частности:

(a) для последовательности (1) n-го порядка с условиями (3) справедливо равенство $L(0) = n \neq 1$;

(b) последовательность $L(k)$ может быть немонотонной;

(c) последовательность $L(k)$ может быть и знакопеременной;

(d) неравенство $\sum_{m=0}^{\mu-1} L(m) \geq L(\mu) - 1$ может не выполняться для некоторых μ;

(e) утверждение 1 ориентировано на представление элементов с использованием бинарного множества «цифр» $\Delta = \{0,1\}$.

2.1. Неформальные аргументы для обобщения критерия Броуна

Приводимые ниже соображения (a*)–(e*) являются некоторыми контраргументами по отношению к сформулированным выше проблемам (a)–(e), имеют неформальный характер и могут корректироваться в конкретных случаях.

(a*) Если в (1) $\varepsilon_1 = \pm 1$ то $L(1) = \pm 1$ и представление для $z \in \mathbf{Z}$ в форме (6) начинается не с $L(0)$, а с $L(1)$.

(b*) Если хоть один корень полинома (2) лежит вне единичного круга комплексной плоскости, то последовательность абсолютных величин $|L(k)|$, начиная с некоторого k_0, образует монотонно возрастающую последовательность.

(c*) Так как в работе рассматриваются *тернарные* системы счисления с цифрами $\Omega = \{-1, 0, +1\}$, то в представлении (6) отрицательность слагаемых $L(k) \leq 0$ может быть скомпенсирована отрицательностью соответствующей цифры $\xi_k = -1$.

(d*) Если последовательность $L(k)$ возрастает асимптотически как геометрическая прогрессия $\{q^k, k \in \mathbf{Z}\}$, то для выполнения условия

$$\sum_{m=0}^{\mu-1} q^m = \frac{q^\mu - 1}{q - 1} \geq q^\mu - 1$$

достаточно выполнения неравенства $1 < q < 2$. Применительно к вопросу о представлении чисел в системе счисления с базисом $L(k)$ модуль набольшего корня $|\alpha_{\max}|$ полинома (2) (см. выше (b)) также должен удовлетворять неравенству $1 < |\alpha_{\max}| < 2$.

(e*) В определении полноты системы имеется в виду бинарное множество цифр, которое включено в множество цифр, используемое в настоящей работе:

$$\Omega = \{-1, 0 + 1\} \supset \{0, +1\}.$$

2.2. Некоторые примеры

В табл. 1 приводятся сведения обо всех неприводимых над полем **Q** полиномах (2) третьей степени, рассматриваемых в качестве характеристических полиномов рекуррентного соотношения (1) с условиями $\varepsilon_i \in \{-1, 0 + 1\} = \Omega$.

Рассмотрим несколько примеров, в которых изложенные выше неформальные соображения (a*)–(e*) позволяют в конкретных случаях решить типовые проблемы (a)–(e), связанные с невыполнимостью условий теоремы Броуна, и найти представления (6) и (7) элементов колец **Z** и $\mathbf{F}_p$.

*Табл. 1. Неприводимые над полем **Q** кубические характеристические полиномы и некоторые их свойства*

	Неприводимые над **Q** кубические характеристические полиномы $f_3(x)$	$\max\|\alpha_j\|$ $0 \leq j \leq n-1$	Конечные поля, над которыми полином $f_3(x)$ неприводим ($\mathbf{F}_p : p = ...$)	Рекуррентное соотношение с характеристическим полиномом $f_3(x)$	Генерируемая последовательность (начальные значения $L(0)$, $L(1)$, $L(2)$ выделены)
1	$x^3 - x^2 - x - 1$	1,683	3,5,23,31,…	$L(k+3) = L(k+2) + L(k+1) + L(k)$	**3,1,3;**7,11,21,39,71,…
2	$x^3 + x^2 - x + 1$	1,839	3,5,23,31,…	$L(k+3) = -L(k+2) + L(k+1) - L(k)$	**3,-1,3;**-7,11,-21,39,…
3	$x^3 + x^2 + x - 1$	1,355	3,5,23,31,…	$L(k+3) = -L(k+2) - L(k+1) + L(k)$	**3,-1,3;**1,-5,7,-1,-11,…
4	$x^3 - x^2 + x + 1$	1,361	3,5,23,31,…	$L(k+3) = L(k+2) - L(k+1) - L(k)$	**3,1,0;**-4-5-2,7,14,9,-12…
5	$x^3 - x^2 - 1$	1,466	2,5,7,19,…	$L(k+3) = L(k+2) + L(k)$	**3,1,1;**4,5,6,10,15,21…
6	$x^3 - x^2 + 1$	1,149	2,3,13,29,31,	$L(k+3) = L(k+2) - L(k)$	**3,1,1;**-2,-3,-4,-2,1,5,7…
7	$x^3 + x^2 - 1$	1,149	2,3,13,29,31,	$L(k+3) = -L(k+2) + L(k)$	**3,1,1;**2,-3,4,2,1,-5, -7…
8	$x^3 + x^2 + 1$	1,466	2, 5,7, 19,…	$L(k+3) = -L(k+2) - L(k)$	**3,1,1;**-4,3,-4,-8,5,-,9…
9	$x^3 - x - 1$	1,324	2,3,13,29,31,	$L(k+3) = L(k+1) + L(k)$	**3,0,2;**3,2,5,5,7,10,12…
10	$x^3 - x + 1$	1,324	2,3,13,29,31,	$L(k+3) = L(k+1) - L(k)$	**3,0,2;**-3,2,-5,5,-7,…
11	$x^3 + x - 1$	1,207	2,5,7,19, ...	$L(k+3) = -L(k+1) + L(k)$	**3,0,-2;**3,2,-5,1,7,…

Пример 2.1. Пусть $f_3(x) = x^3 - x^2 + 1$.

Проблемы (см. табл. 1.):

(a) $L(0) = 3 \neq 1$, но $1 = L(7)$.

(b) Последовательность $L(k)$ монотонно возрастает, начиная с $L(7) = 1$, и условие (9) выполняется при суммировании, начиная с $m = 7$.

Решение. Представление (6) для элемента z начинается со слагаемого $L(7)=1$, а $\varepsilon_0, ..., \varepsilon_6 = 0$. ■

Пример 2.2. Пусть $f_3(x)=x^3+x^2+1$.

Проблемы (см. табл. 1.):

(b) – (c) Рекуррентная последовательность немонотонна и знакопеременна, но выполняется условие (9) для последовательности абсолютных величин, начиная с $m=6$.

(a) $L(0)=3\neq 1$, но $1=L(1)$.

Решение. Так как $L(6)=-4$, то результат стандартного *жадного* алгоритма, выполненного до получения слагаемого $(-1)L(6)=4$, должен быть дополнен при необходимости учетом равенств

$$1=L(1)=L(2),$$
$$2=L(1)+L(2)=L(0)-L(2),$$
$$3=L(0).$$

■

3. О параллельной реализации арифметических операций

Отметим ряд особенностей параллельной реализации арифметических операций.

Пусть (арифметическая) вычислительная процедура $\mathfrak{I}$ отображает множество X входных данных во множество Y:

$$X=\{x\}\subset \mathbf{Z}\to \mathfrak{I}\{x\}\to Y=\{y\}\subset \mathbf{Z}.$$

Пусть далее p – простое число; относительно множеств X, Y известно, что

$$0\le x,y\le M<p\ \forall (x,y): x\in X, y\in Y.$$

Пусть также для данной рекуррентной последовательности (1) с условиями (3) и (4) число d определено таким образом (обычное требование при применении модулярных методов [16, 17]), что все $(x,y): x\in \mathrm{X}, y\in \mathrm{Y}$ представимы в L-системе счисления не более чем d-членной суммой и:

$$\sum_{k=0}^{d-1}\left|L(k)\right|\le M<p. \tag{10}$$

$$\text{Тогда}\quad z=\sum_{k=0}^{d-1}z_k L(k)\triangleq \langle z\rangle_L, \tag{11}$$
$$z_k\in\Omega=\{-1,0,+1\},\quad z\in X\cup Y.$$

Сумму для z в (10) будем называть *представлением элемента z в L-кодах* и обозначать $\langle z\rangle_L$. Так как при выбранных согласно (3) начальных значениях $L(k)$ справедливо равенство (7), то понятным образом вводятся обозначения $\langle z\rangle_{aj}$ для *частичных кодовых представлений*. Равенство (7) тогда принимает вид

$$\langle z\rangle_L=\sum_{k=0}^{d-1}\xi_k L(k)=\sum_{k=0}^{d-1}\xi_k\sum_{j=0}^{n-1}(a_j)^k=\sum_{j=0}^{d-1}\langle z\rangle_{a_j}. \tag{12}$$

Аналогичный смысл имеют обозначения и редуцированных кодовых представлений $\langle z\rangle_{\gamma j}$ для элементов поля $\mathbf{F}_q=\mathbf{F}_{p^n}$.

Замечание 4. Принципиально важно отметить, что векторы цифр $(\xi_0, ..., \xi_{d-1})$ как (формальные) векторы с тернарными компонентами одинаковые и для $\langle z\rangle_L$, и для частичных кодовых представлений $\langle z\rangle_{aj}$, и для редуцированных частичных кодовых представлений $\langle z\rangle_{\gamma j}$. ■

3.1. Реализация операции сложения

Пусть $z, \nu\in \mathbf{Z}$:

$$z=\langle z\rangle_L=\sum_{j=0}^{n-1}\langle z\rangle_{\gamma_j};\ v=\langle v\rangle_L=\sum_{j=0}^{n-1}\langle v\rangle_{\gamma_j}.$$

Тогда, с учётом (7) и (8), получаем

$$z+v=\langle z\rangle_L+\langle v\rangle_L=\sum_{j=0}^{n-1}\langle z\rangle_{\gamma_j}+\sum_{j=0}^{n-1}\langle v\rangle_{\gamma_j}=$$
$$=\sum_{j=0}^{n-1}\langle z+v\rangle_{\gamma_j}=\langle z+v\rangle_L.$$

Следует отметить, что в силу Замечания 4, векторы цифр в кодовом представлении $\langle z+\nu\rangle_{\gamma j}$ одинаковые при всех γ_i. Поэтому различие γ_i учитывается только на финальном этапе получения результата – при суммировании

$$L(k)=\sum_{j=0}^{n-1}\gamma_j^k.$$

Несколько иначе и намного сложнее реализуется операция умножения.

3.2. Реализация операции умножения

Пусть $z, \nu\in \mathbf{Z}$.

$$z=\sum_{j=0}^{n-1}\sum_{k=0}^{d-1}\xi_k\gamma_j^k,\ v=\sum_{j=0}^{n-1}\sum_{k=0}^{d-1}\eta_k\gamma_j^k.$$

Непосредственно имеем:

$$z\cdot v=\left(\sum_{j=0}^{n-1}\sum_{k=0}^{d-1}\xi_k\gamma_j^k\right)\cdot\left(\sum_{i=0}^{n-1}\sum_{m=0}^{d-1}\eta_k\gamma_i^m\right)=$$
$$=\sum_{i,j=0}^{n-1}\left(\sum_{k=0}^{d-1}\xi_k\gamma_j^k\right)\cdot\left(\sum_{m=0}^{d-1}\eta_k\gamma_i^m\right). \tag{13}$$

Формально внешняя сумма по множеству пар (i,j) содержит n^2 слагаемых, пронумерованных, как и пары корней полинома $f_n(x)$ в поле $\mathbf{F}_q=\mathbf{F}_{p^n}$. Но именно в силу того, что полином $f_n(x)$ неприводим над полем $\mathbf{F}_p$, точнее – в силу цикличности мультипликативной группы $\mathbf{F}^*_q$, число слагаемых в (13), вычисляемых независимо нетривиальным образом, можно существенно сократить. Действительно, при $\gamma=\gamma_0$ имеем для слагаемого с $j=0$:

$$S_0 = \sum_{i,j=0}^{n-1}\left(\sum_{k=0}^{d-1}\xi_k\gamma_j^k\right)\cdot\left(\sum_{m=0}^{d-1}\eta_m\gamma_i^m\right)\Bigg|_{j=0} = \\ = \sum_{i=0}^{n-1}\left(\sum_{k=0}^{d-1}\xi_k\gamma^k\right)\cdot\left(\sum_{m=0}^{d-1}\eta_m\left(\chi^{(i)}(\gamma)\right)^m\right), \quad (14)$$

где χ – автоморфизм Фробениуса поля $\mathbf{F}_q$: $\chi: z \to z^p$, $\chi^{(m)}$ – его m-итерация.

Пусть нумерация корней полинома $f_n(x)$ установлена так, что $\gamma_m = \chi^{(m)}(\gamma_0)$. Пусть далее σ – перестановка индексов, индуцированная автоморфизмом Фробениуса: $\sigma(m) = pm \pmod d$. Тогда выражение (14) для S_0 можно записать в виде

$$S_0 = \sum_{i=0}^{n-1}\left(\sum_{k=0}^{d-1}\xi_k\gamma^k\right)\cdot\left(\sum_{\sigma(m)=0}^{d-1}\eta_{\sigma(m)}\left(\gamma^{\sigma(m)}\right)^i\right).$$

Таким образом, для вычисления S_0 достаточно вычислить n (а не n^2!) раз произведение многочленов с аргументами γ с коэффициентами из $\Omega = \{-1, 0, +1\}$. Вычисление остальных S_i сводится к действию автоморфизма Фробениуса и индуцированной перестановки, то есть не требует выполнения нетривиальных арифметических операций.

4. Особенности и рекомендации при исследовании общего случая

При росте степени многочленов (2), то есть при увеличении порядка рекуррентности (1), увеличивается не только количество параллельных ветвей при вычислениях, но и вариативность структуры параллельных систем вычислений. Связано это с тем, что полином степени выше кубической, неразложимый на линейные множители над **Q**, может разлагаться на нелинейные множители-полиномы над **Q**. Для рекуррентностей (1) с *неприводимыми* над **Q** полиномами (2) структура параллельных вычислений отличается от рассмотренной выше только количеством ветвей. В табл. 2 приведены данные всех таких многочленов четвёртой степени.

Отметим также, что в рассмотренном в параграфе 3 кубическом случае условие неприводимости полинома (2) не только над полем **Q**, но и над некоторым конечным полем $\mathbf{F}_p$, в расширении которого $\mathbf{F}_q = \mathbf{F}_{p^n}$ и производятся вычисления, не является необходимым. Это условие введено исключительно для гарантии цикличности мультипликативной группы $\mathbf{F}^*_q$ и следующей из этого связи между корнями полинома $f_n(x)$, индуцируемой действием автоморфизма Фробениуса.

В отдельных случаях даже при нарушении условий неприводимости эта связь может быть хотя и более сложной, но всё же с вычислительной точки зрения не очень обременительной. Тем не менее, многообразие таких «иррегулярных» ситуаций (степени полиномов-сомножителей, их взаимная простота и т.д.) вынуждает ограничиться только рассмотрением ряда наиболее типичных иллюстративных примеров ситуаций, с которыми можно столкнуться при исследовании общего случая L-систем счисления с факторизуемыми характеристическими полиномами.

Пример 4.1. Пусть $p = 11$, $f(x) = x^4 - x^3 + x^2 - x^1 - 1$. В этом случае полином $f_4(x)$ разлагается над $\mathbf{F}_{11}$ в произведение двух взаимно-простых и неприводимых над $\mathbf{F}_{11}$ полиномов второй степени:

$$f(x) = \left(x^2 + 4x^1 + 7\right)\left(x^2 + 6x^1 + 3\right) = \phi_1(x)\phi_2(x).$$

Для фактор-кольца $\mathbf{W} \cong \mathbf{F}_{11}[x]/[f(x)]$ имеет место изоморфизм:

$$\mathbf{F}_{11}[x]\Big/[f(x)] \cong \mathbf{F}_{11}[x]\Big/[\phi_1(x)] \oplus \mathbf{F}_{11}[x]\Big/[\phi_2(x)] = \\ = \mathbf{W}_1 \oplus \mathbf{W}_2.$$

Табл. 2. Неприводимые над полем **Q** *характеристические полиномы рекуррентностей (1) четвёртого порядка*

№	Характеристические полиномы $f_4(x)$, неприводимые над полем **Q**	Простые числа, p, для которых $f_4(x)$ неприводим над $\mathbf{F}_p$
1	$x^4-x^3-x^2-x^1-1$	2, 5, 31,…
2	$x^4-x^3-x^2-x^1+1$	2, 5, 11,…
3	$x^4-x^3-x^2+x^1-1$	2, 3, 7, 11,…
4	$x^4-x^3-x^2+x^1+1$	2, 5, 11,…
5	$x^4-x^3+x^2-x^1-1$	2, 5, 31 ,…
6	$x^4-x^3+x^2-x^1+1$	2, 7, 13, 17,…
7	$x^4-x^3+x^2+x^1-1$	2, 3, 7, 11,…
8	$x^4-x^3+x^2+x^1+1$	2, 7, 13,…
9	$x^4+x^3-x^2-x^1-1$	2, 3, 7, 11,…
10	$x^4+x^3-x^2-x^1+1$	2, 5, 11,…
11	$x^4+x^3-x^2+x^1-1$	2, 5, 31,…
12	$x^4+x^3-x^2+x^1+1$	2, 5, 11,…
13	$x^4+x^3+x^2-x^1-1$	2, 3, 7, 11,…
14	$x^4+x^3+x^2-x^1+1$	2, 7, 13, 17,…
15	$x^4+x^3+x^2+x^1-1$	2, 5, 31,…
16	$x^4+x^3+x^2+x^1+1$	2, 3, 7,…
17	$x^4-x^3+x^2+1$	3, 5, 7,…
18	$x^4+x^3+x^2+1$	3, 5, 7,…
19	$x^4+x^2-x^1+1$	3, 5, 7,…
20	$x^4+x^2+x^1+1$	3, 5, 7,…
21	x^4-x^3-1	2, 3, 5,…
22	x^4-x^3+1	2, 7, 13,…
23	x^4+x^3-1	2, 3, 5,…
24	x^4+x^3+1	2, 7, 13,…
25	x^4-x^2-1	3, 7, 23,…
26	x^4+x^2-1	3, 7, 23,…
27	x^4-x-1	2, 3, 5,…
28	x^4-x+1	2, 3, 5,…
29	x^4+x-1	2, 3, 5,…
30	x^4+x+1	2, 3, 5,…

Как обычно, для вариантов китайской теоремы об остатках справедливо представление элементов кольца $\mathbf{W}$ парами элементов $z \leftrightarrow (z_1, z_2)$; $z_k \in \mathbf{W}_k$ с покомпонентными сложением и умножением, а явная связь $z \leftrightarrow (z_1, z_2)$ определяется соотношениями $z = \sigma_1 z_1 \phi_2(\omega) + \sigma_2 z_2 \phi_1(\omega)$, где

$$\sigma_1\phi_2(\omega) \equiv 1\left(\bmod \phi_1(\omega)\right),$$
$$\sigma_2\phi_1(\omega) \equiv 1\left(\bmod \phi_2(x)\right),$$

где

$$\sigma_1 \equiv \left(5\cdot\omega+8\right)\left(\mathrm{mod}\,\phi_1(\omega)\right),$$
$$\sigma_2 \equiv \left(0\bullet\omega+1\right)\left(\mathrm{mod}\,\phi_2(\omega)\right).$$

Соответствующее рекуррентное соотношение имеет вид

$$L(k+4)=L\left(k+3\right)-L\left(k+2\right)+$$
$$+L\left(k+1\right)+L\left(k\right)\left(\mathrm{mod}11\right)$$

с начальными значениями

$$L(0)=4,\quad L(1)=1,\quad L(2)=3,\quad L(3)=7,$$

вычисляемыми по формулам Ньютона–Жирара, которые связывают суммы степеней корней полинома и элементарные симметрические функции корней полинома. ■

Пример 4.2. Пусть $p=11, f(x)=x^4-x^3+x^2-x^1+1$.

В этом случае над $\mathbf{F}_{11}$ полином полностью факторизуется:

$$f(x)=x^4-x^3+x^2-x^1+1=\left(x+3\right)\left(x+4\right)\left(x+5\right)\left(x+9\right).$$

Тогда соответствующее рекуррентное соотношение имеет вид

$$L(k+4)=L\left(k+3\right)-L\left(k+2\right)+$$
$$+L\left(k+1\right)-L\left(k\right)\left(\mathrm{mod}11\right).$$

Так как в случае полной факторизации полинома $f(x)$ имеет место изоморфизм

$$\mathbf{W}=\mathbf{F}_{11}\left[x\right]\Big/\left[f(x)\right]\cong\mathbf{F}_{11}\oplus\mathbf{F}_{11}\oplus\mathbf{F}_{11}\oplus\mathbf{F}_{11},$$

то типичный элемент z фактор-кольца $\mathbf{W}$ имеет вид

$$z\leftrightarrow\left\langle\zeta_{1`},\zeta_2,\zeta_3,\zeta_4\right\rangle,\quad \zeta_{j`}\in\mathbf{F}_{11},$$

и операции над элементами кольца $\mathbf{W}$ выполняются покомпонентно. При условиях (3) элементы $L(k)$ рекуррентной последовательности, как элементы прямой суммы колец, представимы в данном случае в форме

$$L(k)\leftrightarrow\left\langle\left(-3\right)^k,\left(-4\right)^k,\left(-5\right)^k,\left(-9\right)^k\right\rangle\leftrightarrow$$
$$\leftrightarrow\left\langle 8^k,\ 7^k,6^k,2^k\right\rangle\left(\mathrm{mod}11\right)$$

с также покомпонентным представлением элементов кольца $\mathbf{W}$. ■

Пример 4.3. Пусть $p=5, f(x)=x^4-x^3+x^2-x^1+1$.

В этом случае над $\mathbf{F}_5$ полином также полностью факторизуется:

$$f(x)=x^4-x^3+x^2-x^1+1=\left(x+1\right)^4,$$

но имеет в $\mathbf{F}_5$ четырёхкратный корень $(-1)\equiv 4\,(\mathrm{mod}5)$.

Тогда соответствующее рекуррентное соотношение имеет вид

$$L(k+4)=L\left(k+3\right)-L\left(k+2\right)+L\left(k+1\right)-L\left(k\right).$$

При условиях (3) элементы $L(k)$ рекуррентной последовательности – базиса системы счисления в данном случае в силу кратности корня имеют вид

$$L\left(k\right)=4^k+k4^k+k^2 4^k+k^3 4^k\,(\mathrm{mod}\,5),$$
$$L(0)=4, L(1)=1, L(2)=0, L(3)=0\,(\mathrm{mod}\,5).$$

Фактор-кольцо $\mathbf{W}$ в этом примере изоморфно кольцу классов вычетов по степени простого числа: $\mathbf{W}\cong\mathbf{Z}\,(\mathrm{mod}625)$ и арифметические операции производятся согласно обычным правилам модулярных колец. ■

Ясно, что полное исследование рекуррентных систем счисления с факторизуемыми характеристическими полиномами и выработка «универсальных» полезных рекомендаций для синтеза рассматриваемых параллельных систем безошибочных вычислений в общем случае является задачей нереалистичной трудоёмкости, так как неприводимые полиномы являются во множестве всех полиномов такой же экзотикой, как и целые простые числа во множестве всех целых. Ясно также, что пользуясь евклидовостью кольца полиномов над полем и, как следствие, его факториальностью, несложно указать вид разложения в прямую сумму фактор-кольца $\mathbf{W}\cong\mathbf{F}_p[x]/[f(x)]$ в зависимости от факторизации полинома $f(x)$ (аналог «Основной теоремы арифметики»), представляющий в контексте обсуждаемых приложений лишь общетеоретический интерес. Действительно, несмотря на ясную *структуру* фактор-колец $\mathbf{W}\cong\mathbf{F}_p[x]/[f(x)]$ при известной факторизации полиномов $f(x)$ в общем случае, нахождение для данного полинома этой факторизации (причём над произвольным конечным полем!) представляется всё же непростой, хотя и интенсивно исследуемой вычислительной задачей [18] с неочевидной перспективой на получение полезной именно для рассматриваемых конкретных приложений *арифметической* информации.

Заключение

Если коротко характеризовать отличие подхода настоящей работы к синтезу компьютерных систем параллельных вычислений, то оно заключается в следующем:

- в хорошо известном методе вычислений в системе остаточных классов параллелизация достигается за счёт представления элементов алгебр, в которых производятся вычисления, как *объектов,* распараллеливание вычислений с которыми индуцируется структурной разложимостью этой алгебры;
- в предложенном новом методе параллелизация происходит на уровне *представления* объектов, которое индуцируется свойствами специфических систем счисления.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования РФ в рамках выполнения работ по Государственному заданию ФНИЦ «Кристаллография и фотоника» РАН (соглашение № 007-ГЗ/Ч3363/26) в части исследования систем счисления и Российского фонда фундаментальных исследований (проекты РФФИ №19-07-00357 А № 18-29-03135_ мк) в части исследования машинной арифметики.

Литература

1. **Ananda Mohan, P.V.** Residue number systems / P.V. Ananda Mohan. – Basel: Birkhäuser, 2016. – 351 p. ISBN: 978-3-319-41383-9.
2. Embedded systems design with special arithmetic and number systems / ed. by A.S. Molahosseini, L.S. de Sousa, Ch.-H. Chang. – Cham: Springer, 2017. – 389 p. – ISBN: 978-3-319-49741-9.
3. **Вариченко, Л.В.** Абстрактные алгебраические системы и цифровая обработка сигналов / Л.В. Вариченко, В.Г. Лабунец, М.А. Раков. – Киев: Наукова думка, 1986.
4. **Нуссбаумер, Г.** Быстрое преобразование Фурье и алгоритмы вычисления сверток / Г. Нуссбаумер; пер. с англ. – М.:Радио и связь, 1985. – 248 с.
5. **Golomb, S.W.** Properties of the sequence $3 \cdot 2^n+1$ / S.W. Golomb // Mathematics of Computation. – 1976. – Vol. 30, Num. 135. – P. 657-663.
6. **Alfredson, L.-I.** VLSI Architectures and arithmetic operations with application to the Fermat number transform / L.-I. Alfredson. – Linköping: Linköping University, 1996.
7. **Chernov, V.M.** Fast algorithm for “error-free” convolution computation using Mersenne-Lucas codes / V.M. Chernov // Chaos, Solitons and Fractals. – 2006. – Vol. 29. – P. 372-380. – DOI: 10.1016/j.chaos.2005.08.081.
8. **Чернов, В.М.** Квазипараллельный алгоритм для безошибочного вычисления свёртки в редуцированных кодах Мерсенна–Люка / В.М. Чернов // Компьютерная оптика. – 2015. – Т. 39, № 2. – С. 241-248. – DOI: 10.18287/0134-2452-2015-39-2-241-248.
9. **Чернов, В.М.** Системы счисления в модулярных кольцах и их приложения к «безошибочным» вычислениям / В.М. Чернов // Компьютерная оптика. – 2019. – Т. 43, № 5. – С. 901-911. – DOI: 10.18287/2412-6179-2019-43-5-901-911.
10. **Чернов, В.М.** Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов. – М.: Физматлит, 2007. – 264 с. – ISBN: 978-5-9221-0940-6.
11. **Чернов, В.М.** Фибоначчи, трибоначчи,…, гексаначчи и параллельная безошибочная машинная арифметика / В.М. Чернов // Компьютерная оптика. – 2019. – Т. 43, № 6. – С. 1072-1078. – DOI: 10.18287/2412-6179-2019-43-6-1072-1078.
12. **Гельфонд, А.О.** Исчисление конечных разностей / А.О. Гельфонд. – 4-е изд. – М.: URSS, 2006.
13. **Wimp, J.** Computations with recurrence relations / J. Wimp. – Boston, MA: Pitman, 1984.
14. **Шпарлинский, И.Е.** О некоторых вопросах теории конечных полей / И.Е. Шпарлинский // Успехи математических наук. – 1991. – Т. 46, Вып. 1(277). – С. 165-200.
15. **Brown, J.L.** Note on complete sequences of integers / J.L. Brown // The American Mathematical Monthly. – 1961. – Vol. 68, Issue 6. – P. 557-560. – DOI: 10.2307/2311150.
16. **Грегори, Р.** Безошибочные вычисления. Методы и приложения / Р. Грегори, Е. Кришнамурти; пер. с англ. – М.: Мир, 1988. – 207 с.
17. **Дэвенпорт, Дж.** Компьютерная алгебра / Дж. Дэвенпорт, И. Сирэ, Э. Турнье. – М.: Мир, 1991. – 352 с.
18. **Von Zur Gathen, J.** Factoring polynomials over finite fields: A survey / J. Von Zur Gathen, D. Panario // Journal of Symbolic Computation. – 2001. – Vol. 31, Issues 1-2. – P. 3-17.

Сведения об авторе

Чернов Владимир Михайлович. Доктор физико-математических наук. Главный научный сотрудник лаборатории математических методов обработки изображений Института систем обработки изображений РАН (филиал ФНИЦ «Кристаллография и фотоника» РАН); профессор кафедры геоинформатики и информационной безопасности Самарского национального исследовательского университета имени академика С.П. Королева. Область научных интересов: алгебраические методы в цифровой обработке сигналов, криптография, машинная арифметика. E-mail: *vche@smr.ru* .

ГРНТИ:27.41.41 .
Поступило в редакцию 10 ноября 2019 г. Окончательный вариант – 15 января 2020 г.

Parallel machine arithmetic for recurrent number systems in non-quadratic fields

V.M.Chernov [1,2]
[1]*IPSI RAS – Branch of the FSRC "Crystallography and Photonics" RAS, Molodogvardeyskaya 151, 443001, Samara, Russia,*
[2]*Samara National Research University, Moskovskoye Shosse 34, 443086, Samara, Russia*

Abstract

The paper proposes a new method of synthesis of computer arithmetic systems for "error-free" parallel calculations. The difference between the proposed approach and calculations in traditional systems of Residue Number Systems for the direct sum of modular rings is the parallelization of calculations in non-quadratic extensions of simple finite fields whose elements are represented in number systems generated by sequences of powers of roots of the characteristic polynomial of the recurrent sequence.

Keywords: finite fields, recurrent number system, parallel machine arithmetic.

Citation: Chernov VM. Parallel machine arithmetic for recurrent number systems in non-quadratic fields. Computer Optics 2020; 44(2): 274-281. DOI: 10.18287/2412-6179-CO-666.

Acknowledgements: The work was partly funded by the Russian Federation Ministry of Science and Higher Education within a state contract with the "Crystallography and Photonics" Research Center of the RAS under agreement 007-ГЗ/Ч3363/26 ("Number systems") and by the Russian Foundation for Basic Research under grants 19-07-00357 A and 18-29-03135_мк ("Machine arithmetic").

References

[1] Ananda Mohan PV. Residue number systems. Basel: Birkhäuser; 2016. ISBN: 978-3-319-41383-9.

[2] Molahosseini AS, de Sousa LS, Chang Ch-H, eds. Embedded systems design with special arithmetic and number systems. Cham: Springer; 2017. ISBN: 978-3-319-49741-9.

[3] Varichenko LV, Labunets VG, Rakov MA. Abstract algebraic systems and digital signal processing [In Russian]. Kyiv: "Naukova Dumka" Publisher; 1986.

[4] Nussbaumer HJ. Fast Fourier transform and convolution algorithms. Berlin, Heidelberg: Springer Verlag; 1982.

[5] Golomb SW. Properties of the sequence $3 \cdot 2^n+1$. Math Comput 1976; 30(135): 657-663.

[6] Alfredson L-I. VLSI Architectures and arithmetic operations with application to the Fermat number transform. Linköping: Linköping University Publisher; 1996.

[7] Chernov V. Fast algorithm for "error-free" convolution computation using Mersenne-Lucas codes. Chaos, Solitons and Fractals 2006; 29: 372-380. DOI: 10.1016/j.chaos.2005.08.081.

[8] Chernov VM. Quasiparallel algorithm for error-free convolution computation using reduced Mersenne–Lucas codes. Computer Optics 2015; 39(2): 241-248. DOI: 10.18287/0134-2452-2015-39-2-241-248.

[9] Chernov VM. Number systems in modular rings and their applications to "error-free" computations. Computer Optics 2019; 43(5): 901-911. DOI: 10.18287/2412-6179-2019-43-5-901-911.

[10] Chernov VM. Arithmetic methods for fast algorithms of discrete orthogonal transforms synthesis [in Russian]. Moscow: "Fizmatlit" Publisher, 2007. ISBN: 978-5-9221-0940-6.

[11] Chernov VM. Fibonacci, tribonacci, ..., hexanacci and parallel "error-free" machine arithmetic. Computer Optics 2019; 43(6): 1072-1078. DOI: 10.18287/2412-6179-2019-43-6-1072-1078.

[12] Gel'fond AO. Calculus of finite differences [In Russian]. 4th ed. Moscow: "URSS" Publisher, 2006.

[13] Wimp J. Computations with recurrence relations. Boston, MA: Pitman; 1984.

[14] Shparlinski E. On some problems in the theory of finite fields. Russian Math Surveys 1991; 46(1:277): 199-240.

[15] Brown JL. Note on complete sequences of integers. The American Mathematical Monthly 1961; 68(6): 557-560. DOI: 10.2307/2311150.

[16] Gregory RT, Krishnamurty EV. Method and applications of error-free computation. New York: Springer-Verlag; 1984.

[17] Davenport JH, Siret Y, Tournier E. Computer algebra: Systems and algorithms for algebraic computation. London: Academic Press; 1988.

[18] Von Zur Gathen J, Panario D. Factoring polynomials over finite fields: A survey. J Symb Comput 2001; 31(1-2): 3-17.

Author's information

Vladimir Mikhailovich Chernov. Doctor of Physical and Mathematical Sciences. Chief researcher of the Image Processing Systems Institute of the RAS (Branch of the FSRC "Crystallography and Photonics" RAS) and a professor of Geo-Information Science and Information Protection department at Samara National Research University (SSAU). Research interests are algebraic methods in digital signal processing, cryptography, computer arithmetic.

Received November 10, 2019. The final version – January 15, 2020.