Новый подход к синтезу систем параллельных «безошибочных» вычислений

В.М. Чернов[1,2]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086
[2]Институт систем обработки изображений РАН - филиал ФНИЦ «Кристаллография и фотоника» РАН, Молодогвардейская 151, Самара, Россия, 443001

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, порожденными последовательностями степеней корней характеристического полинома рекуррентной последовательности.

1. 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 (кольцах), что позволяет при разумном выборе параметров этих полей избежать накопления неконтролируемой вычислительной погрешности, характерной при вычислениях с обычными аппроксимациями вещественных или комплексных чисел.

Не вызывает сомнения тот факт, что эффективность возможности параллелизации вычислений с помощью программных или аппаратных средств должна обеспечиваться учетом глубоких структурных свойств алгебры, в которой производятся вычисления. Метод распараллеливания вычислений в системах остаточных классов (СОК) [1],[2] базируется на в хрестоматийном факте, частные случаи систематического использования которого восходят, едва ли ни к методу координат Р.Декарта: ***«если алгебраическая структура*** $\mathbf{A}$ ***изоморфна прямой сумме структур той же категории*** $\mathbf{A} \cong \mathbf{A}_1 \oplus \mathbf{A}_2 \oplus ... \mathbf{A}_r$***, то вычисления в структуре*** $\mathbf{A}$ ***можно распараллелить и заменить «покомпонентными» вычислениями в подструктурах*** $\mathbf{A}_1, \mathbf{A}_2, ..., \mathbf{A}_r$***»,*** несмотря не то, что в СОК этот факт используется в весьма специфической версии «китайской теоремы об остатках». Тем не менее, этот общий факт с упорством, достойным лучшего применения, успешно «переоткрывается» новыми поколениями исследователей, часто ссылающимися при декларировании новизны

исследований исключительно на актуальность и/или социальную значимость решаемых прикладных задач.

К относительным недостаткам вычислений в СОК относится тот факт, что характерные преимущества «битовой» реализации арифметических операций в кольцах, например, по модулям простых чисел Мерсенна или Ферма с «дружественной» машинной арифметикой не наследуются для вычислений в полях по модулям простых сомножителей составных чисел такого вида, так как эти сомножители уже числами Мерсенна или Ферма 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]).

2. Синтез основной вычислительной структуры

Будем рассматривать последовательности, порожденные линейным рекуррентным соотношением $n-$го порядка

$$L(k+n)=\varepsilon_1 L(k+(n-1))+...+\varepsilon_n L(k), \varepsilon_n=\pm 1 \ (1) \ \varepsilon_j \in \{-1,0,+1\}=\Omega \ . \quad (1)$$

Как известно (например, [12]-[13]), что если все корни α_j характеристического полинома

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

различны, то общим решением уравнения (1) является функция $L(k)=\sum_{j=o}^{n-1} C_j \alpha_j^k$, где константы C_j взаимно-однозначно определяются начальными значениями последовательности (1).

Замечание 1. Далее в работе будем рассматривать исключительно рекуррентные функции – решения соотношения (1) – с такими начальными условиями, что $(L(0),...,L(n-1)) \leftrightarrow (C_0,...,C_{n-1})=(1,1...,1)$ и, следовательно, для которых справедливо равенство

$$L(k)=\sum_{j=o}^{n-1} \alpha_j^k. \quad (3)$$

■

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

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

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

$$\lambda : \mathbf{Q}[x] \Big/ [f_n(x)] \to \mathbf{K} \supset \mathbf{Q}. \quad (4)$$

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 $a_1,...,a_n$ с учетом их

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

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

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

Так как мультипликативная группа элементов конечного поля циклична, то мультипликативные порядки $Ord(\gamma_j) = d$ корней γ_j совпадают и равны одному из делителей порядка мультипликативной группы $\mathbf{F}_q^*$, равного $Ord\left(\mathbf{F}_q^*\right) = p^n - 1 = q - 1,\ d \left| (q-1) \right.$.

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, порожденному полиномом $f_n(x)$, которое 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 *«$L-$ системе счисления»*

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

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

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

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

•Так как все $\gamma = \gamma_j \in \mathbf{F}_q$ - суть 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 с учетом того, что

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

Замечание 2. В дальнейшем, в случаях, когда 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 $\Omega = \{-1, 0 + 1\}$ (т.е., *в* $L-$ *системе счисления*).

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

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

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. ■

Утверждение 1. Пусть целочисленная последовательность $\{y_m\}$ неубывающая и $Y(\mu) = \sum_{m=0}^{\mu} y_m$. Тогда условия $y_0 = 1; Y(\mu - 1) \geq y_\mu - 1 \; \forall \mu \geq 1$ (8) являются необходимыми и достаточными для полноты последовательности y_m. ■

Последнее утверждение позволяет в случае полноты последовательности $L(k)$ находить представление элементов $z \in \mathbf{Z}$ в форме $z = \sum_{k=0}^{d(z)} \xi_k L(k), \xi_k \in \{0,1\}$ с помощью так называемого жадного алгоритма: от числа z последовательно шаг за шагом отщепляется слагаемые, равные наибольшему члену последовательности, не превосходящие $z_t = \sum_{k=0}^{t} \xi_k L(k)$. К сожалению, непосредственное применение критерия Утверждения 1 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:

(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. Полуэвристические аргументы для обобщения критерия Броуна

Приводимые ниже соображения (a*)-(e*) являются некоторыми контраргументами к приведенным 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 модулей $|L(k)|$, начиная с некоторого k_0, образуют 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 компенсирована 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 Таблице 1 приводятся некоторые сведения о всех неприводимых над полем **Q** полиномах (2) третьей степени, рассматриваемыми как характеристическое полиномы рекуррентности (1).

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

#	Неприводимые над **Q** кубические характеристические полиномы $f_3(x)$	$\max_{0 \le j \le n-1} \lvert\alpha_j\rvert$	Конечные поля, над которыми полином $f_3(x)$ неприводим ($\mathbf{F}_p : p = \ldots$)	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,…

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

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 $\varepsilon_o, \ldots, \varepsilon_6 = 0.$

■

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 алгоритм, 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 $\Im$ отображает множество X входных данных во множество Y: $X=\{x\}\subset\mathbf{Z}\to\Im\{x\}\to Y=\{y\}\subset\mathbf{Z}$.

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, что все $(x,y): x\in X, y\in Y$ представимы в $L-$ системе счисления не более, чем $d-$членной суммой и $\sum_{k=0}^{d-1}|L(k)|\le M<p$.

Тогда

$$z=\sum_{k=0}^{d-1}z_kL(k)\ \square\ \langle z\rangle_L,\ z_k\in\Omega=\{-1,0,+1\},\ z\in X\cup Y \quad . \tag{9}$$

Сумму для z в (9) 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 $\langle z\rangle_{a_j}$ для «частичных» кодовых представлений. Равенство (7) принимает вид

$$\langle z\rangle_L=\sum_{k=0}^{d-1}\xi_kL(k)=\sum_{k=0}^{d-1}\xi_k\sum_{j=0}^{n-1}(a_j)^k=\sum_{j=0}^{d-1}\langle z\rangle_{a_j} \tag{10}$$

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

Замечание 3. Принципиально важно отметить, что векторы цифр $(\xi_0,\dots,\xi_{d-1})$ как (формальные) векторы с тернарными компонентами одинаковые и для $\langle z\rangle_L$, и для частичных кодовых представлений $\langle z\rangle_{a_j}$, и для редуцированных частичных кодовых представлений $\langle z\rangle_{\gamma_j}$. ■

Сложение. Пусть $z,v\in\mathbf{Z}$: $z=\langle z\rangle_L=\sum_{j=0}^{n-1}\langle z\rangle_{\gamma_j}$; $v=\langle v\rangle_L=\sum_{j=0}^{n-1}\langle v\rangle_{\gamma_j}$. Тогда, с учетом (7) и (8), получаем

$$z+v=\langle z\rangle_L+\langle v\rangle_L=\sum_{j=0}^{n-1}\langle z\rangle_{\gamma_j}+\sum_{j=0}^{n-1}\langle v\rangle_{\gamma_j}=\sum_{j=0}^{n-1}\langle z+v\rangle_{\gamma_j}=\langle z+v\rangle_L. \tag{11}$$

Следует отметить, что «полноценных» параллельных вычислений почти не требуется. Действительно, в силу Замечания 4, векторы цифр в кодовом представлении $\langle z+v\rangle_{\gamma_j}$ одинаковые при всех γ_j. Поэтому различие γ_j учитывается только на финальном этапе получения результата - при суммировании $L(k)=\sum_{j=0}^{n-1}\gamma_j$.

Несколько иначе и намного сложнее реализуется операция умножения.

Умножение. Пусть $z,v \in \mathbf{Z}$. $z = \sum_{j=0}^{n-1}\sum_{k=0}^{d-1} \xi_k \gamma_j^k$, $v = \sum_{j=0}^{n-1}\sum_{k=0}^{d-1} \eta_k \gamma_j^k$. Непосредственно имеем:

$$z \cdot v = \left(\sum_{j=0}^{n-1}\sum_{k=0}^{d-1} \xi_k \gamma_j^k\right) \cdot \left(\sum_{i=0}^{n-1}\sum_{m=0}^{d-1} \eta_k \gamma_i^m\right) = \sum_{i,j=0}^{n-1} \left(\sum_{k=0}^{d-1} \xi_k \gamma_j^k\right) \cdot \left(\sum_{m=0}^{d-1} \eta_k \gamma_i^m\right). \qquad (12)$$

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 (12), вычисляемых независимо нетривиальным образом можно существенно сократить. Действительно при $\gamma = \gamma_0$ имеем для слагаемого с $j = 0$:

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

где $\chi -$ 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: $\sigma(m) = pm(\mathrm{mod}\, d)$. 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 от γ с коэффициентами из $\Omega = \{-1, 0, +1\}$. Вычисление остальных S_j сводится к действию автоморфизма Фробениуса и индуцированной перестановки компонент кодов, 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. Для рекуррентностей (1) с неприводимыми над $\mathbf{Q}$ полиномами (2) структура параллельных вычислений отличается от рассмотренной выше только количеством ветвей.

В частности, в рассмотренном в Разделе 3 кубическом случае, условие неприводимости полинома (2) не только над полем $\mathbf{Q}$, но и над некоторым конечным полем $\mathbf{F}_p$, в расширении которого $\mathbf{F}_q = \mathbf{F}_{p^3}$ 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:

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

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, как обычно, соотношениями

$$z=\sigma_1 z_1\phi_2(\omega)+\sigma_2 z_2\phi_1(\omega),\ \ \sigma_1\phi_2(\omega)\equiv1\left(\mathrm{mod}\,\phi_1(\omega)\right),\sigma_2\phi_1(\omega)\equiv1\left(\mathrm{mod}\,\phi_2(x)\right),$$

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

$$L(k+4)=L(k+3)-L(k+2)+L(k+1)+L(k)\left(\mathrm{mod}11\right),\ L(0)=4,L(1)=1,L(2)=3,L(3)=7.$$ ■

Таблица 2. Неприводимые над полем $\mathbf{Q}$ характеристические полиномы для рекуррентностей (1) четвертого порядка.

	Характеристические полиномы $f_4(x)$, неприводимые над полем $\mathbf{Q}$	Простые p для которых $f_4(x)$ неприводим над $\mathbf{F}_p$		Характеристические полиномы $f_4(x)$, неприводимые над полем $\mathbf{Q}$	Простые p для которых $f_4(x)$ неприводим над $\mathbf{F}_p$
1	$x^4-x^3-x^2-x^1-1$	2,5,31,…	16	$x^4+x^3+x^2+x^1+1$	2,3,7,…
2	$x^4-x^3-x^2-x^1+1$	2,5,11,…	17	$x^4-x^3+x^2+1$	3,5,7,…
3	$x^4-x^3-x^2+x^1-1$	2,3,7,11,…	18	$x^4+x^3+x^2+1$	3,5,7,…
4	$x^4-x^3-x^2+x^1+1$	2,5,11,…	19	x^4+x^2-x+1	3,5,7,…
5	$x^4-x^3+x^2-x^1-1$	2,5,31 ,…	20	x^4+x^2+x+1	3,5,7,…
6	$x^4-x^3+x^2-x^1+1$	2,7,13,17,…	21	x^4-x^3-1	2,3,5,…
7	$x^4-x^3+x^2+x^1-1$	2,3,7,11,…	22	x^4-x^3+1	2,7,13,…
8	$x^4-x^3+x^2+x^1+1$	2,7,13,…	23	x^4+x^3-1	2,3,5,…
9	$x^4+x^3-x^2-x^1-1$	2,3,7,11,…	24	x^4+x^3+1	2,7,13,…
10	$x^4+x^3-x^2-x^1+1$	2,5,11,…	25	x^4-x^2-1	3,7,23,…
11	$x^4+x^3-x^2+x^1-1$	2,5,31,…	26	x^4+x^2-1	3,7,23,…
12	$x^4+x^3-x^2+x^1+1$	2,5,11,…	27	x^4-x-1	2,3,5,…
13	$x^4+x^3+x^2-x^1-1$	2,3,7,11,…	28	x^4-x+1	2,3,5,…
14	$x^4+x^3+x^2-x^1+1$	2,7,13,17,…	29	x^4+x-1	2,3,5,…
15	$x^4+x^3+x^2+x^1-1$	2,5,31,…	30	x^4+x+1	2,3,5,…

Пример 4.2. Пусть $p=3$, $f(x)=x^4+x^3-x^2-x^1+1$.В этом случае над $\mathbf{F}_3$ полином есть точный квадрат квадратного трехчлена: $f(x)=(x^2+2x+2)^2$ и элементы $z\in\mathbf{W}\cong\mathbf{F}_3[x]/[f(x)]$ представимы в форме $z=(a\cdot\omega+b)(\omega^2+2\omega+2)+(c\cdot\omega+d);\ a,b,c,d\in\mathbf{F}_3$.

Рекуррентное соотношение имеет вид $L(k+4)=-L(k+3)+L(k+2)+L(k+1)-L(k)\left(\mathrm{mod}3\right)$ с начальными значениями $L(0)=4,L(1)=1,L(2)=3,L(3)=-1$. ■

Пример 4.3. Пусть $p=11$, $f(x)=x^4-x^3+x^2-x^1+1$. В этом случае над $\mathbf{F}_{11}$ полином полностью факторизуется: $f(x)=x^4-x^3+x^2-x^1+1=(x+3)(x+4)(x+5)(x+9)$. Тогда соответствующее рекуррентное соотношение имеет вид $L(k+4)=L(k+3)-L(k+2)+L(k+1)-L(k)\left(\mathrm{mod}11\right)$. Так как в случае полной факторизации полинома $f(x)$ имеет место изоморфизм

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

то типичный элемент z фактор-кольца $\mathbf{W}$ представим как $z \leftrightarrow \langle \zeta_{1^`}, \zeta_2, \zeta_3, \zeta_4 \rangle, \zeta_{j^`} \in \mathbf{F}_{11}$, 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 $L(k) \leftrightarrow \langle (-3)^k, (-4)^k, (-5)^k, (-9)^k \rangle \leftrightarrow \langle 8^k, 7^k, 6^k, 2^k \rangle (\mathrm{mod}11)$ с также покомпонентным представлением элементов кольца $\mathbf{W}$. ■

Пример 4.4. 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: $f(x)=x^4-x^3+x^2-x^1+1=(x+1)^4$, но имеет в $\mathbf{F}_5$ четырехкратный корень $(-1)\equiv 4(\mathrm{mod}5)$. Тогда соответствующее рекуррентное соотношение, имеет вид $L(k+4)=L(k+3)-L(k+2)+L(k+1)-L(k)$. При условиях (3) элементы $L(k)$ рекуррентной последовательности в данном случае в силу кратности корня представимы в форме

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

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» рекомендаций для синтеза рассматриваемых параллельных систем безошибочных вычислений в общем случае является задачей нереалистичной трудоемкости, так как неприводимые полиномы, связанные с наиболее просто устроенными параллельными системами вычислений рассмотренного вида 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 понятную 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 его факторизации (причем, над произвольным конечным полем!) представляется всё же непростой, хотя и интенсивно исследуемой, вычислительной задачей [9], с неочевидной перспективой на получение полезной именно для рассматриваемых конкретных приложений арифметической информации.

5. 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 (СОК) параллелизация достигается за счет представления элементов алгебр, в которых производятся вычисления, как объектов, распараллеливание вычислений с которыми индуцируется структурной разложимостью этой алгебры;
- в предложенном методе параллелизация происходит на уровне представления объектов, которое индуцируется свойствами специфических систем счисления.

6. 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.

7. Литература

[1] Ananda Mohan, P.V. Residue Number Systems / P.V. Ananda Mohan – Springer Verlag, 2016. – 351 p.
[2] Sabbagh, A. Embedded Systems Design with Special Arithmetic and Number Systems / A. Sabbagh, L. Seabra de Sousa, Ch.-H. Chang – Springer Verlag, 2017. – 389 p.
[3] Гельфонд, А.О. Исчисление конечных разностей / А.О. Гельфонд – М., URSS, 2006.
[4] Чернов, В.М. Синтез параллельных алгоритмов преобразований Фурье-Галуа в прямых суммах конечных колец // Известия Самарского научного центра Российской Академии Наук. – 2000. – № 2(1). – С. 128-134.
[5] 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.
[6] 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.
[7] Чернов, В.М. Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов – М.: Физматлит, 2007. – 264 с.
[8] 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.
[9] Von Zur Gathen, J. Factoring Polynomials Over Finite Fields: A Survey / J. Von Zur Gathen, D. Panario // Journal of Symbolic Computation. – 2001. – Vol. 31(1-2). – P. 3-17.

A new approach to the synthesis of parallel error-free computing systems

V.M. Chernov[1,2]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086
[2]Image Processing Systems Institute of RAS - Branch of the FSRC "Crystallography and Photonics" RAS, Molodogvardejskaya street 151, Samara, Russia, 443001

Abstract. This paper proposes a new method for synthesizing machine arithmetic systems for "error-free" parallel calculations. The difference between the proposed approach and calculations in traditional systems of residual classes 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 notation systems generated by sequences of degrees of roots of the characteristic polynomial of a recurrent sequence.