КВАЗИПАРАЛЛЕЛЬНЫЙ АЛГОРИТМ БЕЗОШИБОЧНОГО ВЫЧИСЛЕНИЯ СВЁРТКИ В РЕДУЦИРОВАННЫХ КОДАХ МЕРСЕННА–ЛЮКА

Чернов В.М.
Институт систем обработки изображений РАН,
Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет) (СГАУ)

Аннотация

В работе предложен новый «безошибочный» алгоритм вычисления дискретной циклической свёртки. Алгоритм основан на применении нового класса дискретных ортогональных преобразований, для которых существуют эффективные реализации без умножений. Структура этих преобразований связана с представлением данных в избыточной системе счисления с базисом, состоящим из чисел Люка.

Ключевые слова: дискретная циклическая свёртка, теоретико-числовые преобразования, числа Фибоначчи и Люка, алгоритмы безошибочных вычислений.

Цитирование: Чернов, В.М. Квазипараллельный алгоритм безошибочного вычисления свёртки в редуцированных кодах Мерсенна–Люка / В.М. Чернов // Компьютерная оптика. – 2015. – Т. 39, № 2. – С. 241-248.

Введение

Вычисление дискретной циклической свёртки последовательностей с периодом N

$$z(k) = (x * h)(k) = \sum_{n=0}^{N-1} x(n)\, h(k-n), \quad (k = 0,\ 1, \ldots,\ N-1) \tag{1}$$

является одной из наиболее типичных задач в цифровой обработке сигналов.

Для вычисления массива $z(m)$ непосредственно последовательности с помощью уравнения (1) требуется $O(N^2)$ сложений и умножений членов последовательностей $x(n)$ и $h(n)$. Для многих длин свёрток N существуют эффективные «спектральные» методы вычисления $z(m)$, которые основаны на применении дискретного преобразования Фурье (ДПФ) [1–3].

Если члены последовательностей $x(n)$ и $h(n)$ являются целыми неотрицательными числами, то для «безошибочного» вычисления свёртки можно использовать преимущества модулярных аналогов комплексных ДПФ:

$$\hat{x}(m) = \sum_{n=0}^{N-1} x(n)\, \omega^{mn} \pmod{p}, \tag{2}$$

где p – достаточно большое простое число, ω – элемент конечного поля $GF(p)$ из p элементов и мультипликативный порядок $Ord(\omega)$ (то есть такое минимальное число k, что $\omega^k = 1 \in GF(p)$) равен N.

Теоретико-числовое преобразование, ТЧП (2), имеет ряд недостатков, в частности, существуют определённые ограничения на длину преобразования и модуль, а именно, соотношение делимости: $N \mid (p-1)$. Кроме того, арифметические операции $(\bmod p)$ не являются элементарными компьютерными операциями. Но для некоторых простых p арифметика поля $GF(p)$ может быть более «дружественной компьютеру» (например, если $p = 2^q - 1$ – простое число Мерсенна, если $p = 2^{2^k} + 1$ – простое число Ферма, и так далее) [2, 3, 6]. Более того, если $\omega \equiv 2 (\bmod p)$, то умножения в (2) могут быть заменены циклическими сдвигами бинарных векторов, то есть бинарных кодов элементов. К сожалению, так как для чисел Мерсенна $Ord(2) = q$, то возможно вычислить теоретико-числовое преобразование (2) с использованием арифметики Мерсенна без умножений только при $N = q$, то есть при

$$q = 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31, \ldots .$$

Ещё большие трудности возникают в случае вычисления (2), когда N является «немерсенновским» простым числом. Несмотря на известный метод Рейдера–Винограда [5] вычисления ДПФ (или ТЧП), существуют, как показано в [11], «плохие» простые числа, для которых применение метода Рейдера–Винограда приводит к «быстрым» алгоритмам, мультипликативная сложность которых даже выше тривиальной $O(N^2)$.

В работе [11] был введён класс дискретных преобразований, которые могут быть реализованы «без умножений». Эти дискретные преобразования основываются на альтернативном представлении данных, то есть на представлении данных не в традиционной позиционной бинарной системе счисления, а, например, в избыточной «системе счисления Люка». Такие системы счисления сохраняют достоинства мерсенноподобной арифметики для более широкого спектра длин ТЧП. Применение этих преобразований позволяет существенно уменьшить вычислительную сложность алгоритмов вычисления свёртки: количество умножений в таких алгоритмах равно $O(N)$.

Объективным недостатком метода работы [11] является то, что модулей дискретных преобразований и длин N свёртки (1), для которых возможна реализация предложенного в этой работе алгоритма, очень мало. Кроме того, на одном из этапов вычислений необходимо умножать числа, представленные в системе счисления Люка. Поэтому приходится конвертиро-

вать представление чисел в системе счисления Люка в более традиционную систему счисления.

В настоящей работе мы сохраняем общую идею работы [11] вычисления свёртки в кодах, связанных с «фибоначчиевыми» системами счисления, но предлагаем версию, свободную от недостатков, связанных с «нефибоначчиевостью» произведений чисел Фибоначчи.

1. Основные идеи

Использование в качестве модулей в преобразовании (2) составных чисел p добавляет к описанным непосредственно вычислительным проблемам принципиальные теоретические трудности, связанные с существованием в модулярных кольцах по составным модулям делителей нуля и, как следствие, с необратимостью некоторых элементов соответствующих колец и/или с неортогональностью базисных функций преобразования (2). Действительно, доказательство ортогональности базисных функций дискретного преобразования Фурье длины N сводится к проверке равенства

$$\sum_{n=0}^{N-1}\omega^{mn}\omega^{-nk}=\begin{cases}\dfrac{1-\omega^{N(m-k)}}{1-\omega^{(m-k)}}=0, & \text{при } m\neq k \pmod N;\\ N, & \text{при } m\equiv k \pmod N.\end{cases} \quad (3)$$

Доказательство последнего соотношения представляет собой тривиальное упражнение на суммирование геометрической прогрессии и остаётся справедливым и для случая конечного поля, в котором существует корень степени N из единицы. Условие «быть полем», то есть простота модуля в (2), существенно . В поле только нулевой элемент необратим, что гарантирует возможность «деления» на элемент $\left(1-\omega^{(m-k)}\right)$ в верхней строчке правой части равенства (3).

При составном модуле элемент $\left(1-\omega^{(m-k)}\right)$ в соотношении (3) может быть необратимым и для $m\neq k\left(\bmod N\right)$. При распараллеливании вычислений в системе остаточных классов по модулям-сомножителям характерные преимущества «битовой» реализации арифметических операций в полях по модулям чисел Мерсенна не наследуются для вычислений в полях по модулям простых целых сомножителей составных чисел Мерсенна

$$m=2^q-1=p_1p_2\ldots p_d, \quad (4)$$

так как сомножители $p_1,p_2,\ldots,p_d$ уже не являются числами Мерсенна.

В настоящей работе предлагается следующая схема вычислений дискретной свёртки (1) с помощью ТЧП по составному модулю mod$M$.

Для целого составного числа M определяются числа $p_1,p_2,\ldots,p_d$ с условиями

$$M=p_1p_2\ldots p_d, \quad (5)$$

$$p_j\equiv\alpha_j^k-1\left(\bmod M\right),\ \alpha_j\in\mathbf{W},\ k\in\mathbf{Z}. \quad (6)$$

Фактор-кольцо $\mathbf{W}\cong\mathbf{Z}/M\mathbf{Z}$ представляется в виде прямой суммы фактор-колец

$$\mathbf{W}\cong\mathbf{Z}/\left[\alpha_1^k-1\right]\oplus\mathbf{Z}/\left[\alpha_2^k-1\right]\oplus\ldots\oplus\mathbf{Z}/\left[\alpha_t^k-1\right]=$$
$$=\mathbf{W}_{\alpha_1}\oplus\ldots\oplus\mathbf{W}_{\alpha_t},$$

где $\left[\alpha_j^k-1\right]$ есть главные идеалы, порождённые элементами $\left(\alpha_j^k-1\right)$.

Вычисление свёртки может быть произведено по обычной параллельной схеме с применением семейства дискретных преобразований (аналогов ТЧП) в кольцах $\mathbf{W}_{\alpha_j}$ с последующей реконструкцией значения свёртки (mod M) по китайской теореме об остатках. Базисные функции $h_m^j(n)$ семейства этих преобразований выбираются в форме

$$h_m^j(n)=\alpha_j^{nm}.$$

Если входные данные преобразований в кольцах $\mathbf{W}_{\alpha_j}$ представлены в кодах, связанных с системой счисления «с основанием α_j», то умножение при вычислении таких дискретных преобразований реализуется сдвигами этих кодов.

Эффективность предложенной схемы вычислений связана, естественно, с возможностью эффективной реализации вычислений при представлении данных в «нетрадиционных» системах счисления. В качестве таких систем счисления для преобразований в фактор-кольцах $\mathbf{W}_{\alpha_j}$ в работе рассматриваются системы счисления «золотого сечения».

Отметим, что, несмотря на кажущуюся «параллельность» такой схемы вычислений, как будет показано ниже, реально параллельных процессоров не требуется. Этим и объясняется термин «квазипараллельное» в названии работы.

2. Предварительные сведения

Напомним некоторые сведения из теории чисел Люка [7, 8].

1. Пусть L_q есть число Люка, то есть, q-й член последовательности

$$L_k=L_{k-1}+L_{k-2} \quad (7)$$

с начальными условиями $L_0=2,\quad L_1=1$.

Пусть

$$\alpha=\frac{1+\sqrt{5}}{2},\quad \beta=\frac{1-\sqrt{5}}{2},$$

тогда

$$L_q=\alpha^q+\beta^q=\left(\frac{1+\sqrt{5}}{2}\right)^q+\left(\frac{1-\sqrt{5}}{2}\right)^q.$$

Заметим, что число α, являющееся, наряду с β, одним из корней характеристического уравнения для рекуррентности (7), – знаменитое «золотое сечение». породившее «в поисках гармонии мироустройства» значительное число работ, находящихся, по мнению автора, «по ту сторону разума».

2. Хорошо известно [7–8], что для любого положительного целого числа x существует представление в «системе счисления Люка»

$$Y = \sum_{j=0}^{\nu(Y)-1} y_j L_j = \sum_{j=0}^{\nu(Y)-1} y_j \alpha^j + \sum_{j=0}^{\nu(Y)-1} y_j \beta^j = Y_\alpha + Y_\beta, \quad (8)$$

где

$$y_j = 0,1; \quad y_{\nu(x)-1} = 1, \ u \ y_j = 1 \Rightarrow y_{j+1} = 0.$$

Если рассмотреть последовательность (7) с начальными значениями $L_0 = 1, \ L_2 = \alpha$, то каждое целое число представимо в виде конечной суммы

$$Y = \sum_{j=0}^{\nu(Y)-1} y_j \alpha^j + \sum_{j=1}^{\mu(Y)-1} y_{-j} \alpha^{-j}, \quad (9)$$

где также

$$y_j = 0,1; \text{ и } y_j = 1 \Rightarrow y_{j+1} = 0.$$

Представление (9) будем называть представлением целых чисел в кодах золотого сечения, а вектор $\left(y_{\nu-1}, y_{\nu-2}, ...y_0; y_{-1}, ..., y_{-\mu+1}\right)$ – кодом золотого сечения числа Y и обозначать $\langle Y \rangle_\alpha$. Отметим, что код золотого сечения целого числа содержит цифры, соответствующие как положительным, так и отрицательным степеням α.

Например,

$$\langle 1 \rangle_\alpha = (1;0) = (0;1,1), \langle 2 \rangle_\alpha = (1;1,1) = (1,0;0,1),$$

$$\langle 3 \rangle_\alpha = (1,1;0,1) = (1,0,0;0,1).$$

Кроме того, правила сложения чисел, представленных в системе счисления с базовой последовательностью, являющейся решением рекуррентности (7), индуцируют одинаковые правила «сложения кодов» вне зависимости от начальных значений L_0, L_1.

3. Редуцированные коды «золотого сечения»

Пусть $\mathcal{L}$ – множество бинарных векторов

$$\mathbf{x} = (x_{s-1}, \ldots, x_1, x_0) \quad (10)$$

длины s таких, что в любом векторе $\mathbf{x}$ нет двух соседних ненулевых компонент. Определим операцию «сложения» векторов из множества $\mathcal{L}$ по правилам, согласованным с правилом сложения элементов некоторого фактор-кольца, представленных в специфической системе счисления.

Пусть g есть решение сравнения

$$g^2 \equiv g + 1 \left(\mathrm{mod}\left(g^s - 1\right)\right).$$

Рассмотрим представление элемента

$$X \in \mathbf{Z} \Big/ \left(g^s - 1\right)\mathbf{Z} \triangleq \mathbf{W}(g,s)$$

в форме

$$X \equiv x_{s-1} g^{s-1} + \ldots + x_1 g + x_0 \left(\mathrm{mod}\left(g^s - 1\right)\right). \quad (11)$$

Операции над элементами кольца $\mathbf{W}(g,s)$ в форме (11) осуществляются по обычным правилам бинарной арифметики Зеккендорфа [9] с дополнительным правилом

$$g^s \equiv g^0 \left(\mathrm{mod}\left(g^s - 1\right)\right).$$

Сложение элементов (11) индуцирует «правило сложения» векторов (10). Вектор (10) будем называть редуцированным кодом элемента (11) и обозначать $\langle X \rangle_g = (x_{s-1}, \ldots, x_1, x_0)$.

Умножению элемента $X \in \mathbf{W}(g,s)$ на элемент g соответствует циклический сдвиг кода:

$$\langle gX \rangle_g = (x_{s-2}, \ldots, x_1, x_0, x_{s-1}).$$

Умножение элементов кольца $\mathbf{W}(g,s)$ сводится в кодах к сложениям кодов и циклическим сдвигам.

4. Нормальные числа Люка

Определение 1. Пусть последовательность $\psi(k)$ определена соотношениями:

$$\psi(k) = \begin{cases} -L_k, & \text{если } k - \text{нечетное;} \\ -L_k + 2, & \text{если } k - \text{четное.} \end{cases} \quad (12)$$

Число Люка $L_s = -\left(\alpha^s - 1\right)\left(\beta^s - 1\right)$, где s – нечётное, есть нормальное число Люка, если выполняются следующие условия:

(a) при всех $0 < k < s$ числа L_s и $\psi(k)$ взаимно просты:

$$\text{Н.О.Д.}\left(L_s, \ \psi(k)\right) = 1; \quad (13)$$

(b) элемент s обратим в кольце $\mathbf{Z} \Big/ L_s \mathbf{Z}$.

Очевидно, что если при нечётном s число L_s есть простое число, то оно нормальное число Люка. Укажем ещё несколько необходимых условий нормальности чисел Люка.

Лемма 1. Если число Люка L_s есть нормальное число, то s есть простое число.

Доказательство. Если $s = ab$, где $a,b > 1$, есть нечётные числа, то

$$-L_s = \left(\alpha^{ab} - 1\right)\left(\beta^{ab} - 1\right) = \left(\alpha^a - 1\right)\left(\beta^a - 1\right)\sum_{\tau=0}^{b} \alpha^{\tau a} \sum_{\mu=0}^{b} \beta^{\mu a} =$$

$$= -L_a \sum_{\tau=0}^{b} \alpha^{\tau a} \sum_{\mu=0}^{b} \beta^{\mu a},$$

что противоречит условию (a) Определения 1.

Лемма 2. Если число Люка L_s есть нормальное число, то целое число 5 является квадратичным вычетом $\left(\mathrm{mod}\, L_s\right)$.

Доказательство. Вычисляя символ Лежандра с использованием квадратичного закона взаимности, имеем:

$$\left(\frac{5}{L_s}\right) = (-1)^{(5-1)(L_s-1)/4} \left(\frac{l_s}{5}\right) = \left(\frac{l_s}{5}\right),$$

где $L_s \equiv l_s \left(\mathrm{mod}\, 5\right), \quad 0 \le l_s < 5.$

Рассмотрим последовательность

$L_s \pmod 5$, $s = 0,1,\ldots$:

$L_s \pmod 5 = \{2,1,3,4;\ 2,1,3,4;\ \ldots\}$.

При нечётных s справедливы сравнения $L_s \equiv 1 \pmod 5$ или $L_s \equiv 4 \pmod 5$. Но

$$\left(\frac{l_s}{5}\right) = \begin{cases} +1, & \text{if } l_s = 1,4; \\ -1, & \text{if } l_s = 2,3, \end{cases}$$

что и доказывает Лемму.

Непосредственные вычисления показывают, что для простых индексов s<100 все числа Люка L_s являются нормальными (простыми или составными). В табл. 1 приведены все нормальные числа Люка L_s для простых 5≤s≤83.

Отметим, что далее обоснование корректности рассматриваемых алгоритмов и их структура несколько различаются для простых и составных нормальных чисел Люка, поэтому мы рассмотрим эти случаи отдельно.

Табл. 1

s	L_s	Разложение на множители	Тип
5	11	11	простое
7	29	29	простое
11	199	199	простое
13	521	521	простое
17	3571	3571	простое
19	9349	9349	простое
23	64079	139×461	составное, нормальное
29	1149851	59×19489	составное, нормальное
31	3010349	3010349	простое
37	54018521	54018521	простое
41	370248451	370248451	простое
43	969323029	6709×144481	составное, нормальное
47	6643838879	6643838879	простое
53	119 218851371	119 218851371	простое
59	2139295485799	709×8969×336419	составное, нормальное
61	5600748293801	5600 748293801	простое
67	100501350283429	4021×24 994118449	составное, нормальное
71	688846502588399	688846 502588399	простое
73	1803423556807921	151549×11 899937029	составное, нормальное
79	32361122672259149	32361122 672259149	простое
83	221806434537978679	35761381×6202401259	составное, нормальное

5. *Первый случай: L_s есть составное нормальное число*

Лемма 3. Если L_s есть составное нормальное число Люка, то ненулевые главные идеалы $A = \left[\alpha^s - 1\right]$, $B = \left[\beta^s - 1\right]$ взаимно просты в кольце **Z**.

Доказательство. Так как справедливы равенства:

$$\alpha^s\left(\beta^s - 1\right) = -\left(\left(\alpha^s - 1\right) + 2\right),\ \beta^s\left(\alpha^s - 1\right) = -\left(\left(\beta^s - 1\right) + 2\right), \quad (14)$$

то

$$\left(\alpha^s\left(\beta^s - 1\right) + \left(\alpha^s - 1\right)\right)\left(\beta^s\left(\alpha^s - 1\right) + \left(\beta^s - 1\right)\right) = (-2)(-2) = 4. \quad (15)$$

Из (15) следует, что неединичный общий делитель чисел $\left(\alpha^s - 1\right), \left(\beta^s - 1\right)$ может быть только чётным числом, что противоречит тому, что $\left(\alpha^s - 1\right)\left(\beta^s - 1\right) = -L_s \neq 0 \pmod 2$.

Лемма 4. Если L_s есть нормальное число Люка и главные идеалы $A = \left[\alpha^s - 1\right]$, $B = \left[\beta^s - 1\right]$ ненулевые, то для любого $X \in \mathbf{Z}/L_s\mathbf{Z}$ существуют эффективно определяемые элементы

$$X_1 \in \mathbf{Z}/\left[\alpha^s - 1\right], \quad X_2 \in \mathbf{Z}/\left[\beta^s - 1\right]$$

и константы $a, b \in \mathbf{Z}/L_s\mathbf{Z}$ такие, что:

$$X \equiv a\left(\beta^s - 1\right)X_1 + b\left(\alpha^s - 1\right)X_2 \pmod{L_s}, \quad (16)$$

причём

$$X \equiv X_1 \left(\mathrm{mod}\left[\alpha^s - 1\right]\right), \quad X \equiv X_2 \left(\mathrm{mod}\left[\beta^s - 1\right]\right). \quad (17)$$

Доказательство. Так как идеалы $A = \left[\alpha^s - 1\right]$ и $B = \left[\beta^s - 1\right]$ взаимно просты по Лемме 3, то существование представления (16) является следствием китайской теоремы об остатках. Определим константы a, b в (16) таким образом, чтобы выполнялись соотношения:

$$a\left(\beta^s-1\right)\equiv 1\left(\mathrm{mod}\left[\alpha^s-1\right]\right),$$
$$b\left(\alpha^s-1\right)\equiv 1\left(\mathrm{mod}\left[\beta^s-1\right]\right). \quad (18)$$

Заметим, что при нечётных значениях s справедливы равенства

$$\left(\beta^s-1\right)\equiv-\alpha^{-s}\left(\left(\alpha^s-1\right)+2\right)\equiv$$
$$\equiv-2\alpha^{-s}\left(\mathrm{mod}\left[\alpha^s-1\right]\right),$$
$$\left(\alpha^s-1\right)\equiv-\beta^{-s}\left(\left(\beta^s-1\right)+2\right)\equiv \quad (19)$$
$$\equiv-2\beta^{-s}\left(\mathrm{mod}\left[\beta^s-1\right]\right).$$

Поэтому соотношения (18), определяющие константы a,b, можно переписать в форме

$$-2a\alpha^{-s}\equiv 1\left(\mathrm{mod}\left[\alpha^s-1\right]\right),\ -2b\beta^{-s}\equiv 1\left(\mathrm{mod}\left[\beta^s-1\right]\right),$$
$$a\equiv-2^{-1}\alpha^s\left(\mathrm{mod}\left[\alpha^s-1\right]\right),\ b\equiv-2^{-1}\beta^s\left(\mathrm{mod}\left[\beta^s-1\right]\right)$$

или

$$a\equiv\left(-2^{-1}\left(\alpha^s-1\right)-2^{-1}\right)\left(\mathrm{mod}\left[\alpha^s-1\right]\right)\equiv$$
$$\equiv-2^{-1}\left(\mathrm{mod}\left[\alpha^s-1\right]\right),$$
$$b\equiv\left(-2^{-1}\left(\beta^s-1\right)-2^{-1}\right)\left(\mathrm{mod}\left[\beta^s-1\right]\right)\equiv$$
$$\equiv-2^{-1}\left(\mathrm{mod}\left[\beta^s-1\right]\right).$$

Так как в силу нечётности L_s элемент $2\in\mathbf{Z}/L_s\mathbf{Z}$ обратим и

$$\left(\alpha^s-1\right)\left(\beta^s-1\right)=-L_s,$$

то в соотношении (16) достаточно положить

$$a=b\equiv-2^{-1}\left(\mathrm{mod}\,L_s\right),$$

откуда следует сравнение

$$X\equiv-2^{-1}\left[\left(\beta^s-1\right)X_1+\left(\alpha^s-1\right)X_2\right]\left(\mathrm{mod}\,L_s\right), \quad (20)$$

что и доказывает Лемму.

Пример 1. Пусть $s=23$, $L_{23}=64079=139\times461$. Тогда сравнение $W^2\equiv5\left(\mathrm{mod}\,64079\right)$ имеет четыре решения $W_{1,2}\equiv\pm16553\left(\mathrm{mod}\,64079\right)$ и $W_{3,4}\equiv\pm39603\left(\mathrm{mod}\,64079\right)$.

Положим

$$\alpha_1\equiv2^{-1}\left(1+16553\right)\left(\mathrm{mod}\,64079\right)\equiv8277\left(\mathrm{mod}\,64079\right),$$
$$\beta_1\equiv2^{-1}\left(1-16553\right)\left(\mathrm{mod}\,64079\right)\equiv-8276\left(\mathrm{mod}\,64079\right).$$

Аналогично:

$$\alpha_3\equiv2^{-1}\left(1+39603\right)\left(\mathrm{mod}\,64079\right)\equiv19802\left(\mathrm{mod}\,64079\right),$$
$$\beta_3\equiv2^{-1}\left(1-16553\right)\left(\mathrm{mod}\,64079\right)\equiv-19801\left(\mathrm{mod}\,64079\right).$$

Тогда

$$\left(\alpha_1^{23}-1\right)\equiv55320\left(\mathrm{mod}\,64079\right),$$
$$\left(\beta_1^{23}-1\right)\equiv-55322\left(\mathrm{mod}\,64079\right),$$
$$\left(\alpha_3^{23}-1\right)\equiv0\left(\mathrm{mod}\,64079\right),$$
$$\left(\beta_3^{23}-1\right)\equiv-2\left(\mathrm{mod}\,64079\right).$$

Кроме того, $2^{-1}\equiv32040\left(\mathrm{mod}\,64079\right)$. Пара решений $W_{3,4}\equiv\pm39603\left(\mathrm{mod}\,64079\right)$ сравнения $W^2\equiv5\left(\mathrm{mod}\,64079\right)$ порождает нулевой главный идеал $\left[\alpha_3^{23}-1\right]$ и соответствует тривиальной факторизации числа $L_{23}=64079=1\times L_{23}$. Пара решений $W_{1,2}\equiv\pm16553\left(\mathrm{mod}\,64079\right)$ порождает представление элементов кольца $\mathbf{Z}/L_{23}\mathbf{Z}$ в форме

$$X\equiv-2^{-1}\left[\left(\beta_1^{23}-1\right)X_1+\left(\alpha_1^{23}-1\right)X_2\right]\left(\mathrm{mod}\,L_{23}\right)\equiv$$
$$\equiv32040\cdot\left[-55322\cdot X_1+55320\cdot X_2\right]\left(\mathrm{mod}\,64079\right),$$

где

$$X\equiv X_1\left(\mathrm{mod}\,55320\right),\quad X\equiv X_2\left(\mathrm{mod}(-55322)\right).$$

Лемма 5. Если L_s есть нормальное число Люка и главные идеалы $A=\left[\alpha^s-1\right]$, $B=\left[\beta^s-1\right]$ ненулевые, то функции

$$h_m^{\alpha}(n)\equiv\alpha^{mn}\left(\mathrm{mod}\left[\alpha^s-1\right]\right),$$
$$h_m^{\beta}(n)\equiv\beta^{mn}\left(\mathrm{mod}\left[\beta^s-1\right]\right)$$

образуют ортогональные семейства:

$$\sum_{n=0}^{s-1}h_m^{\gamma}(n)\ \ h_k^{\gamma}(s-n)\equiv s\cdot\delta_{mk}\left(\mathrm{mod}\left[\gamma^s-1\right]\right).$$

$$\left(\gamma=\alpha,\ \beta\right)$$

Доказательство. Причиной нарушения условия ортогональности этих семейств может быть только необратимость элементов $\left(1-\alpha^{m-k}\right)$ и $\left(1-\beta^{m-k}\right)$ при суммировании геометрических прогрессий в соотношении (3). Но если при $1<\left(m-k\right)<s$ элемент $\left(1-\alpha^{m-k}\right)$ есть делитель нуля в кольце $\mathbf{Z}/L_s\mathbf{Z}$, то элемент

$$\left(1-\alpha^{m-k}\right)\left(1-\beta^{m-k}\right)\equiv\psi\left(m-k\right)\left(\mathrm{mod}\,L_s\right)$$

также есть делитель нуля в кольце $\mathbf{Z}/L_s\mathbf{Z}$, что влечёт существование неединичного общего делителя чисел $\psi\left(m-k\right)$ и L_s. Это противоречит условию нормальности чисел L_s. Но при $1=\left(m-k\right)$ справедливо равенство

$$\left(1-\alpha\right)\left(1-\beta\right)\equiv-1\left(\mathrm{mod}\,L_s\right),$$

откуда следует обратимость элементов $\left(1-\alpha\right),\left(1-\beta\right)$ в кольце $\mathbf{Z}/L_s\mathbf{Z}$.

6. Второй случай: L_s есть простое число

Пусть L_s есть простое число. Тогда для сомножителей в соотношении

$$L_s = -\left(\alpha^s - 1\right)\left(\beta^s - 1\right)$$

справедливо сравнение

$$\alpha^s - 1 \neq 0 \left(\mathrm{mod}\, L_s\right), \beta^s - 1 \equiv 0 \left(\mathrm{mod}\, L_s\right).$$

Действительно:

$$\left(\alpha^s - 1\right) \equiv -\beta^{-s}\left(\left(\beta^s - 1\right) + 2\right)\left(\mathrm{mod}\left[\beta^s - 1\right]\right) \equiv$$

$$\equiv -2 \left(\mathrm{mod}\, L_s\right).$$

Поэтому справедливо равенство (20) в форме

$$X \equiv -2^{-1}\left[\left(\beta^s - 1\right) X_1 + \left(\alpha^s - 1\right) X_2\right]\left(\mathrm{mod}\, L_s\right) \equiv$$

$$\equiv -2^{-1}\left[L_s X_1 + (-2) X_2\right]\left(\mathrm{mod}\, L_s\right) \equiv X_2 \left(\mathrm{mod}\, L_s\right).$$

Несмотря на то, что вычисления с компонентами $X_2 \left(\mathrm{mod}\left[\beta^s - 1\right]\right)$ равносильны вычислениям, производимым с элементами $X \left(\mathrm{mod}\, L_s\right)$, мы будем иметь в виду справедливость равенства (20) и в случае простого числа L_s для обоснования корректности вычислений в редуцированных кодах Люка.

Лемма 6. Пусть L_s есть простое число Люка и $\alpha^s - 1 \neq 0 \left(\mathrm{mod}\, L_s\right), \beta^s - 1 \equiv 0 \left(\mathrm{mod}\, L_s\right)$, тогда функции

$$h_m^{\alpha}(n) \equiv \alpha^{mn} \left(\mathrm{mod}\left[\alpha^s - 1\right]\right)$$

образуют ортогональные семейства:

$$\sum_{n=0}^{s-1} h_m^{\alpha}(n)\ \ h_k^{\alpha}(s-n) \equiv s \cdot \delta_{mk} \left(\mathrm{mod}\left[\alpha^s - 1\right]\right).$$

Доказательство. Единственной причиной нарушения условия ортогональности может быть необратимость элементов $\left(1 - \alpha^{m-k}\right)$ при суммировании геометрических прогрессий в соотношении (3), что при $m \neq k \left(\mathrm{mod}\, L_s\right)$ противоречит простоте числа L_s.

Пример 2. Пусть $s = 7$, $L_7 = 29$. Тогда сравнение $W^2 \equiv 5 \left(\mathrm{mod}\, 29\right)$ имеет два решения

$$W_{1,2} \equiv \pm 11 \left(\mathrm{mod}\, 29\right).$$

Положим

$$\alpha \equiv 2^{-1}(1+11)\left(\mathrm{mod}\, 29\right) \equiv 6 \left(\mathrm{mod}\, 29\right),$$

$$\beta \equiv 2^{-1}(1-11)\left(\mathrm{mod}\, 29\right) \equiv -5 \left(\mathrm{mod}\, 29\right).$$

Тогда

$$\left(\alpha^7 - 1\right) \equiv -2 \left(\mathrm{mod}\, 29\right), \quad \left(\beta^7 - 1\right) \equiv 0 \left(\mathrm{mod}\, 29\right).$$

Поэтому при $s = 7$ равенство (20) можно переписать в форме:

$$X \equiv -2^{-1}\left[\left(\beta^7 - 1\right) X_1 + \left(\alpha^7 - 1\right) X_2\right]\left(\mathrm{mod}\, 29\right) \equiv$$

$$\equiv -2^{-1}\left[0 \cdot X_1 + (-2) X_2\right]\left(\mathrm{mod}\, 29\right) \equiv X_2 \left(\mathrm{mod}\, 29\right)$$

и вычисление $X \left(\mathrm{mod}\, 29\right)$ равносильно вычислению компоненты $X_2 \left(\mathrm{mod}\left[\beta^7 - 1\right]\right)$.

7. Представление данных в редуцированных кодах Люка

Для практической реализации рассматриваемого алгоритма вычисления свёртки желательно располагать простыми алгоритмами нахождения компонент X_1, X_2 для $X \in {}^{\mathbf{Z}}\!/_{L_s \mathbf{Z}} \triangleq \mathbf{W}_s$ и кодов этих компонент X_1, X_2 в редуцированных $\left(\mathrm{mod}\left(\alpha^s - 1\right)\right)$, $\left(\mathrm{mod}\left(\beta^s - 1\right)\right)$ системах счисления с основаниями α, β соответственно.

Определённые трудности нахождения кодов связаны с тем, что если процесс определения «цифр» y_j для представления элемента кольца $\mathbf{W}_s$ в системе счисления Люка (8) сводится к последовательному делению с остатком целого числа на числа L_t, $0 \le t \le s$ из конечного множества, то представление целых чисел в системах счисления с основаниями α, β содержит отрицательные степени α, β.

Однако для редуцированных $\left(\mathrm{mod}\left(\alpha^s - 1\right)\right)$, $\left(\mathrm{mod}\left(\beta^s - 1\right)\right)$ систем счисления процесс нахождения кодов может быть связан с представлением элементов кольца $\mathbf{W}_s$ в редуцированной $\left(\mathrm{mod}\, L_s\right)$ системе счисления Люка, которое для нахождения требует исключительно деления с остатком целых чисел.

Действительно, пусть элемент $X \equiv X_2 \left(\mathrm{mod}\, L_s\right)$ представлен в редуцированной бинарной системе счисления с основанием α (то есть в редуцированных кодах «золотого сечения»).

$$X \equiv X_2 \equiv x_0 \alpha^0 + x_1 \alpha^1 + \ldots + x_k \alpha^k \left(\mathrm{mod}\, L_s\right), \quad x_j \in \{0,1\}.$$

Рассмотрим $\mathbf{M}_s$-линейное отображение τ, являющееся автоморфизмом кольца $\mathbf{M}_s\left(\sqrt{5}\right)$:

$$\tau : \mathbf{M}_s\left(\sqrt{5}\right) \to \mathbf{M}_s\left(\sqrt{5}\right), \quad \tau : \alpha \mapsto \beta.$$

Тогда справедливо равенство

$$X \equiv \tau(X) \equiv \tau\left(x_0 \alpha^0 + x_1 \alpha^1 + \ldots + x_k \alpha^k\right) \equiv$$

$$\equiv x_0 \beta^0 + x_1 \beta^1 + \ldots + x_k \beta^k \left(\mathrm{mod}\, L_s\right) \qquad (21)$$

То есть если известно представление элемента $X \in \mathbf{M}_s$ в системе счисления с основанием α, то представление этого элемента в системе счисления с основанием β имеет те же самые цифры $x_j \in \{0,1\}$ и остаётся только указать простой способ их определения.

Складывая равенства (20) и (21), получаем:

$$2X \equiv \left(x_0 \alpha^0 + x_1 \alpha^1 + \ldots + x_k \alpha^k\right) +$$

$$+ \left(x_0 \beta^0 + x_1 \beta^1 + \ldots + x_k \beta^k\right)\left(\mathrm{mod}\, L_s\right) \equiv$$

$$\equiv x_0 L_0 + x_1 L_1 + \ldots + x_k L_k \left(\mathrm{mod}\, L_s\right).$$

Таким образом, для определения цифр $x_j \in \{0,1\}$ представления элемента $X \in \mathbf{M}_s$ в редуцированных $\left(\mathrm{mod}\left(\alpha^s - 1\right)\right)$, $\left(\mathrm{mod}\left(\beta^s - 1\right)\right)$ системах счисления с

основаниями α,β достаточно определить цифры представления элемента $2X \in \mathbf{M}_s$ в редуцированной $(\mathrm{mod}\, L_s)$ системе счисления Люка.

8. Дискретное преобразование в кодах золотого сечения

Обозначим левый циклический сдвиг редуцированного кода:

$$< x >_g = (x_{s-1},\ \ldots,\ x_1,\ x_0)\ ,$$

$$\mathcal{M} < x >_g = (x_{s-2},\ \ldots,\ x_1,\ x_0,\ x_{s-1})\ . \qquad (22)$$

Пусть $\mathcal{M}^{-1}$ – обратный оператор (то есть правый циклический сдвиг), пусть $\mathcal{M}^2 = \mathcal{M} \circ \mathcal{M}$ и так далее.

Пусть $x(n)$ – последовательность целых чисел с периодом N, такая что

$$0 \le x(n) < W_q, \quad N = q\ .$$

Определение 2. Преобразование

$$< \hat{x}(m) >_g = \sum_{n=0}^{N-1} \mathcal{M}^{mn} < x(n) >_g\ , \qquad (23)$$

$$g = \alpha,\beta; \quad m = 0,\ldots,N-1$$

будем называть дискретным преобразованием в кодах золотого сечения последовательности $x(n)$.

Лемма 6. Дискретное преобразование

$$< N \cdot x(n) >_g = \sum_{m=0}^{N-1} \mathcal{M}^{-mn} < \hat{x}(m) >_g \qquad (24)$$

является обратным к преобразованию (22).

Доказательство. Из (23) получаем

$$\sum_{m=0}^{N-1} \mathcal{M}^{-mn} < \hat{x}(m) >_g = \left\langle \sum_{m=0}^{N-1} g^{-mn} \hat{x}(m) \left(\mathrm{mod}\left(g^s - 1\right)\right) \right\rangle_g =$$

$$= \left\langle \sum_{m=0}^{N-1} g^{-mn} \sum_{k=0}^{N-1} g^{mk} x(k) \left(\mathrm{mod}\left(g^s - 1\right)\right) \right\rangle_g =$$

$$= \left\langle \sum_{k=0}^{N-1} x(k) \left(\sum_{m=0}^{N-1} g^{m(k-n)} \right) \left(\mathrm{mod}\left(g^s - 1\right)\right) \right\rangle_g =$$

$$= \left\langle N \cdot x(n) \left(\mathrm{mod}\left(g^s - 1\right)\right) \right\rangle_g\ .$$

9. Вычисление дискретной циклической свёртки

Пусть элементы последовательностей $x(n)$ и $h(n)$ в (1) есть положительные целые числа, такие что

$$0 \le s\ \max_n \{x(n)\}\ \max_n \{h(n)\}\ \le L_s\ ,$$

где $N = s$.

Так как выше обосновано представление кольца $\mathbf{Z}/L_s\mathbf{Z}$ в форме прямой суммы

$$\mathbf{Z}/L_s\mathbf{Z} \cong \mathbf{Z}/\left[\alpha^s - 1\right] \oplus \mathbf{Z}/\left[\beta^s - 1\right],$$

при известных $\hat{x}_\alpha(n), \hat{x}_\beta(n), \hat{h}_\alpha(n), \hat{h}_\beta(n)$ реконструкция значений (1) свёртки $z(t)$ осуществляется несложным применением китайской теоремы об остатках с линейной мультипликативной сложностью $O(N)$.

Заключение

Представленная работа базируется на двух связанных идеях:

(a) возможности такого расширения модулярного кольца, в котором существует альтернативное разложение на сомножители (взаимно простые идеалы);

(b) существования в прямых суммах слагаемых – фактор-кольцах – систем счисления для элементов этих подколец с относительно несложной программной или аппаратной реализациями арифметических операций.

Впервые такой подход предложен автором в [12] для альтернативных разложений составных чисел Мерсенна и оснований систем счисления, равных $\pm\sqrt{2}$. Дальнейшее развитие теории систем счисления в полях алгебраических чисел [13] позволило экстраполировать описанный подход на случай канонических и т.н. квазиканонических систем счисления (в том числе и небинарных) в квадратичных полях.

Благодарности

Работа выполнена при поддержке Министерства образования и науки РФ и грантов РФФИ и 13-01-97007-р_поволжье_а и 15-07-05576_а.

Литература

1. **Stein, J.Y**. Digital Signal Processing: A Computer Science Perspective / J.Y. Stein. - New York: John Wiley & Sons, Inc., 2002.
2. **Naudin, C**. Algorithmique Algébrique / C. Naudin. – Paris: Masson; 1992. – (In French).
3. **Nussbaumer, H.J.** Fast Fourier Transform and Convolution Algorithms / H.J. Nussbaumer. – Berlin: Springer-Verlag, 1982. – (In French).
4. **Schoenhage, A.** Schnelle multiplikation grosser Zahlen / A. Schoenhage, V. Strassen // Computing. – 1966. – Vol. 7(3/4). – P. 281-292. – (In German).
5. **Blahut, R.E.** Fast Algorithms for Digital Signal Processing / R.E. Blahut. – Reading:Addison-Wesley Inc, 1985.
6. **Rader, C.M**. Discrete convolution via Mersenne transform / C.M. Rader // IEEE Transactions on Computers. – 1972. – Vol. C-21. – P. 1269-1273.
7. **Hoggatt, V.E**. Fibonacci and Lucas Numbers / V.E. Hoggatt. – Fibonacci Association Edition, 1972.
8. **Vajda, S.** Fibonacci&Lukas numbers and Golden Section. Theory and applications / S. Vajda. – Chichester: Elis Horwood Ltd, 1989.
9. **Zeckendorf, E**. Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas / E. Zeckendorf // Fibonacci Quarterly – 1972. – V. 10. – P. 179-182. – (In French).
10. **Freitag, H.T**. Phillips G.M, Elements of Zeckendorf Arithmetic / H.T. Freitag, G.M. Phillips //Applications of Fibonacci Numbers. – 1998. – V. 7. – P. 129-132.
11. **Chernov, V.** Fast algorithm for "error-free" convolution computation using Mersenne-Lucas codes / V. Chernov // Chaos, Solitons and Fractals. – 2006. – V. 29. – P. 372-380.
12. **Chernov. V.M.** "Error-free" calculation of the convolution using generalized Mersenne and Fermat transforms over al-

gebraic fields / V.M. Chernov, M.V. Pershina // Lecture Note Computer Science. – 1997. – V. 1296. – P. 621-628.
13. **Katai, I**. Kanonische Zahlensysteme in der Theorie der Quadratischen Zahlen / I. Katai, B. Kovacs // Acta Scientiarum Mathematicarum (Szeged). – 1980. – V. 42. – P. 99-107. – (In German).

References

[1] Stein JY. Digital Signal Processing: A Computer Science Perspective. New York: John Wiley & Sons, Inc; 2002.
[2] Naudin C. Algorithmique Algébrique [In French]. Paris: Masson; 1992.
[3] Nussbaumer HJ. Fast Fourier Transform and Convolution Algorithms. Berlin: Springer-Verlag; 1982.
[4] Schoenhage A, Strassen V. Schnelle multiplikation grosser Zahlen [In German]. Computing 1966; 7(3/4): 281-92.
[5] Blahut RE. Fast Algorithms for Digital Signal Processing. Reading:Addison-Wesley Inc; 1985.
[6] Rader CM. Discrete convolution via Mersenne transform. IEEE Trans Comp 1972; C-21: 1269-1273.
[7] Hoggatt VE. Fibonacci and Lucas Numbers. Fibonacci Association Edition; 1972.
[8] Vajda S. Fibonacci&Lukas numbers and Golden Section. Theory and applications. Chichester: Elis Horwood Ltd; 1989.
[9] Zeckendorf E. Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas [In French]. Fibonacci Quarterly 1972; 10, 179-182
[10] Freitag HT, Phillips GM. Elements of Zeckendorf Arithmetic, Applications of Fibonacci Numbers 1998; 7; 129-132.
[11] Chernov V. Fast algorithm for "error-free" convolution computation using Mersenne-Lucas codes. Chaos, Solitons and Fractals 2006; 29;. 372-380.
[12] Chernov VM., Pershina MV. "Error-free" calculation of the convolution using generalized Mersenne and Fermat transforms over algebraic fields.1997. Lecture Notes in Computer Science. 1296, LNCS, pp. 621-628.
[13] Katai I, Kovacs B. Kanonische Zahlensysteme in der Theorie der Quadratischen Zahlen [In German]. Acta Scientiarum Mathematicarum (Szeged) 1980; 42; 99-107.

QUASIPARALLEL ALGORITHM FOR ERROR-FREE CONVOLUTION COMPUTATION USING REDUCED MERSENNE–LUCAS CODES

V.M. Chernov
Image Processing Systems Institute,
Russian Academy of Sciences,
Samara State Aerospace University

Abstract

In this paper a new “error-free” algorithm for discrete circular convolution calculation is proposed. The algorithm is based on a new type of discrete orthogonal transforms for which there exist efficient multiplication-free implementations. The structure of these transforms is associated with the representation of data in the redundant number system associated with Lucas numbers.

Keywords: discrete cyclic convolution, number-theoretical transforms Fibonacci and Lucas numbers, “error-free” calculations.

Citation: Chernov VM. Quasiparallel algorithm for error-free convolution computation using reduced Mersenne–Lucas codes. Computer Optics 2015; 39(2): 241-8.

Сведения об авторе

Чернов Владимир Михайлович, 1949 года рождения, математик, доктор физико-математических наук. Главный научный сотрудник Института систем обработки изображений РАН. Профессор кафедры геоинформатики и информационной безопасности Самарского государственного аэрокосмического университета имени академика С.П. Королёва. Область научных интересов: алгебраические методы в цифровой обработке сигналов, криптография, машинная арифметика.

E-mail: *vche@smr.ru* .

Vladimir Mikhailovich Chernov (b. 1949) is mathematician, Doctor of Physical and Mathematical Sciences. Chief researcher of the Image Processing Systems Institute of the RAS. Professor of Geo-Information Science and Information Security department of S. P. Korolyov Samara State Aerospace University (SSAU). Research interests are algebraic methods in digital signal processing, cryptography, computer arithmetic.

Поступила в редакцию 30 марта 2015 г.
Окончательный вариант – 13 апреля 2015 г.