АЛГОРИТМ БЕЗОШИБОЧНОГО ВЫЧИСЛЕНИЯ СВЕРТКИ В РАСШИРЕНИЯХ КОНЕЧНЫХ ПОЛЕЙ

А.Н. Калугин
Самарский государственный аэрокосмический университет

Аннотация

В работе рассматривается алгоритм безошибочного вычисления дискретной круговой свертки с помощью теоретико–числовых преобразований в системе остаточных классов при альтернативной факторизации составного модуля в расширении кольца классов вычетов. Дополнительный вычислительный выигрыш обеспечивается за счет представления входных данных и параметров преобразования в канонических системах счисления

Введение

В связи с ростом объемов глобальных коммуникаций проблемы хранения и эффективной передачи информации становятся все более актуальными. В настоящее время большое значение приобретает цифровая обработка информации, в частности фильтрация, механизм действия которой основан на вычислении свертки входного сигнала и импульсной характеристики фильтра

$$y(k) = (x * h)(k) = \sum_{n=0}^{N-1} x(n)h(k-n)\,,$$

$$k = 0,..., N-1\ . \qquad (1)$$

Также в ряде криптографических задач в качестве одного из этапов алгоритма возникает необходимость умножения двух чисел с величинами, превышающими границы, в которых возможна аппаратная реализация операций на базе существующей вычислительной техники. Данные числа могут быть рассмотрены как значения соответствующих многочленов в точке равной основанию системы счисления. Значение свертки $y(j)$ в этом случае равно коэффициенту при j-ой степени произведения многочленов, заданных векторами $x(n)$, $h(m)$ коэффициентов при соответствующих степенях.

Стоит отметить, что вычисление свертки «прямым» способом требует чрезмерных вычислительных затрат. Существующие методики, основанные на дискретном преобразовании Фурье (ДПФ),

$$X(m) = \sum_{n=0}^{N-1} x(n) f_m(n) \qquad (2)$$

$$f_m(m) = \cos(\frac{2\pi m}{N} n) + i\sin(\frac{2\pi m}{N} n) \qquad (3)$$

позволяют для определенных значений длины свертки N уменьшить сложность вычислений благодаря существованию эффективных (быстрых) алгоритмов вычисления ДПФ.

Относительным недостатком применения ДПФ является то, что в ряде реальных задач $x(n)$, $h(m)$ и, следственно, $y(j)$ – суть числа с фиксированной точкой или, после понятного масштабирования, целые числа. В то же время значения базисных функций (3) ДПФ являются иррациональными числами и при вычислениях могут быть представлены лишь с ограниченной точностью, в связи с конечностью разрядной сетки вычислительной машины.

Существует круг задач (задачи криптографии [1], [2]), в которых потеря точности недопустима, что обуславливает необходимость использования вместо ДПФ его модулярного аналога – теоретико-числового преобразования (ТЧП).

$$X(m) = \sum_{n=0}^{N-1} x(n)\omega^{mn} (\mathrm{mod}\ p)\,,\ \omega^N \equiv 1(\mathrm{mod}\ p)\ . \qquad (4)$$

при

$$p > \max_{0\le n<N}\{x(n)\} \max_{0\le n<N}\{h(n)\} N \quad x(n), h(n) > 0\,.$$

К сожалению, явные «точностные» преимущества ТЧП вступают в конфликт с фактом «неэлементарности» реализации арифметических операций в конечном поле $\mathbf{Z}/p\mathbf{Z}$.

Паллиативным решением является использование таких простых p, для которых операции сложения и умножения в соответствующем модулярном кольце реализовывались бы наиболее дружественным образом по отношению к «стандартным» процессорам. Выбор p помимо прочего ограничивается условиями существования в конечном поле корней только степени N с условием делимости:

$N \mid (p\text{-}1)$.

К сожалению, простые числа p с «дружественными» для машинной реализации свойствами модулярных операций (простые числа Мерсенна, Ферма, Голомба и т.п.) встречаются в натуральном ряду достаточно редко. Прямое использование ТЧП по модулю составных чисел наталкивается на серьезные трудности, связанные с возможной неортогональностью базисных функций ТЧП, обусловленной наличием в соответствующих модулярных кольцах делителей нуля.

При распараллеливании вычислений в системе остаточных классов характерные преимущества «битовой» реализации арифметических операций в полях по модулям чисел Мерсенна и Ферма не наследуются для вычислений в полях по модулям целых делителей составных чисел Мерсенна или Ферма

$$m = 2^q \pm 1 = p_1 \quad p_2 \dots p_d$$

В самом деле, например, для пятого числа Ферма справедливо разложение на простые множители

$f_5 = 2^{32} + 1 = 641 \bullet 6\ 700\ 417$.

Эти сомножители уже не являются числами Ферма. Все вышесказанное относится в значительной степени и к составным числам Мерсенна.

В работах [3], [4] показано, что для чисел Ферма $f_t = 2^B + 1$, $B = 2^t$, в том числе и составных, при наложении определенных ограничений, возможно построение структурно-простых алгоритмов вычисления свертки длины $N = 2B$ с использованием ТЧП и реализаций операций в $\mathbf{Z}/f_t\mathbf{Z}$ в виде циклических сдвигов. Аналогичные алгоритмы, позволяющие вычислять свертку длины q, описаны и для чисел (составных) Мерсенна $p=2^q-1$.

В цитированных работах были разработаны алгоритмы для вычисления свертки с применением составных чисел Мерсенна и Ферма, базирующиеся на *альтернативной факторизация* элементов алгебраических полей $\mathbf{Q}\left(\sqrt{2}\right)$ и $\mathbf{Q}(\sqrt[3]{-2})$, соответственно. В основе методов работ [3], [4] лежала следующая схема вычислений.

1. Кольцо классов вычетов $\mathbf{Z}/m\mathbf{Z}$ по, вообще говоря, составному модулю m вкладывается в некоторое кольцо **W**, которое в ряде случаев является алгебраическим расширением кольца классов вычетов $\mathbf{Z}/m\mathbf{Z}$.
2. Кольцо **W** выбирается так, чтобы разложение модуля m на простые элементы кольца **W** содержало только сомножители вида $p_j = \alpha_j^{k_j} \pm 1$.
3. Вычисление свертки проводится по обычной параллельной схеме с применением семейства некоторых дискретных преобразований (аналогов ТЧП) в системе остаточных классов $\left(\mathrm{mod}\ p_j\right)$ с последующей реконструкцией значения свертки $\left(\mathrm{mod}\ m\right)$ по китайской теореме об остатках.
4. Базисные функции $h_m^j(n)$ семейства этих преобразований выбираются в форме $h_m^j(n) = \alpha_j^{nm}$; если входные данные преобразований $\left(\mathrm{mod}\ p_j\right)$ представлены в позиционной системе счисления «с основанием α_j», то вычисление ТЧП, как и, например, в мерсенновском случае, не требует умножений.

Эффективность реализации предложенной схемы вычислений связана, естественно, с возможностью эффективной реализации вычислений при представлении данных в «нетрадиционных» системах счисления.

Отметим также, что предлагаемые параллельные алгоритмы, использующие «альтернативное» разложение целых чисел в кольце **W,** остаются справедливыми и для простых чисел Мерсенна и/или Ферма, для которых в кольце целых чисел нет нетривиального разложения на множители.

Однако выбор чисел Мерсенна и Ферма также достаточно ограничен.

В данной работе предлагается расширить класс чисел, порождающих модулярные кольца с сохранением преимуществ «мерсенноподобной» или «фермаподобной» арифметики, в которых операция умножения реализуется посредством циклических сдвигов.

Канонические системы счисления

Предлагаемая методика основывается на понятии канонических систем счисления (canonical number systems), введенных в работе [5] и исследовавшихся далее, в частности, в работах [6], [7].

Пусть **Q** поле рациональных чисел. Обозначим $\mathbf{Q}(\xi)$ квадратичное расширение поля **Q**, порожденное ξ, $\xi \neq ka^2$, ($k \in \mathbf{Z}, a \in \mathbf{N}$):

$$\mathbf{Q}(\xi) = \left\{\gamma \mid \gamma = a + b\sqrt{\xi},\ a,b \in \mathbf{Q}\right\}.$$

Пусть, как обычно, норма $\mathrm{N}(\gamma)$ элемента $\gamma \in \mathbf{Q}(\xi)$ определяется соотношением

$$\mathrm{N}(\gamma) = a^2 - \xi b^2;. \qquad (5)$$

кольцом целых чисел $\mathbf{Q}[\xi]$ поля $\mathbf{Q}(\xi)$ называется множество,

$$\mathbf{Q}[\xi] = \left\{\gamma \mid \mathrm{N}(\gamma) \in \mathbf{Z}\right\}.$$

Целыми алгебраическими числами мнимого поля $\mathbf{Q}\left(i\sqrt{N}\right)$ являются числа:

$$z = \begin{cases} a + bi\sqrt{N},\ a,b \in Z\ при\ N \equiv -2,-3 (\mathrm{mod}\, 4); \\ a + \dfrac{1}{2}b(i\sqrt{N} - 1),\ a,b \in Z\ при\ N \equiv -1 (\mathrm{mod}\, 4). \end{cases}$$

Если для любого $\gamma \in \mathbf{Q}[\xi]$ задать множество N_0, $N_o = N_o(\gamma) = \{0,1,...,\left|\mathrm{N}(\gamma)\right| - 1\}$, то корректно следующее определение.

Определение 1. Канонической системой счисления называется пара $\{\gamma, N_o\}$, такая, что для любого элемента $\alpha \in \mathbf{Q}[\xi]$ существует и, причем, единственное конечное представление в виде

$$\alpha = a_0 + a_1\gamma + ... + a_n\gamma^n,\ (a_i \in N_0,\ i = 0,...,n) \qquad (6)$$

Для различных ξ вопросы существования канонических систем счисления и их свойств рассмотрены в работах [5], [6], [7]. В данной работе ограничимся рассмотрением случая $N_0=\{0,1\}$, то есть слу-

чая, когда каноническая система счисления является «бинарной», в частности, система счисления с основанием $\gamma = \pm i\sqrt{2}$ в поле $\mathbf{Q}[i\sqrt{2}]$, существование которой следует из следующей леммы, доказанной в работе [5]

Лемма 1. *Для любого натурального числа M, не представимого в виде $M = ka^2$, где k, a – натуральные, и удовлетворяющего равенству $M \equiv 1 \bmod 4$, пара $\{i\sqrt{M}, N_0(i\sqrt{M})\}$ будет являться канонической системой счисления в кольце $\mathbf{Q}[i\sqrt{N}]$.*

Данная система счисления описана, например, в монографии [8], однако только для альтернативного бинарного представления *всех* комплексных чисел, что порождала трудности связанные с представлением мнимой единицы в виде бесконечного непериодического разложения. Если ограничиваться лишь кольцом $\mathbf{Q}[i\sqrt{2}]$, то подобные трудности, как показано ниже, вполне преодолимы.

Алгоритм определения представления числа (цифр числа) в данных системах счисления может быть несложным образом получен путем модификации рекурсивного процесса, изложенного в [7]. А именно.

Алгоритм 1. (определения цифр для $\{\pm i\sqrt{2}, N_0(\pm i\sqrt{2})\}$):

Для любого $z = z_1 + z_2 i\sqrt{2} \in \mathbf{Q}[i\sqrt{2}]$, ($z_1, z_2 \in \mathbf{Z}$), определим $s_k(z) \in \mathbf{Z}$ согласно формул:

$$s_{k+1}(z) = -[\frac{s_{k-1}(z)}{2}], k \geq 0,$$

$$s_{-1}(z) = \mp 2z_2,\ s_0(z) = z_1.$$

Тогда

$$z = \sum_{k \geq 0} a_k(z) b^k,$$

где $a_k(z) \equiv s_k(z) (\bmod 2)$.

Доказательство. Проведем доказательство методом математической индукции по номеру цифры в искомом представлении числа z. Проведем доказательство для случая $\xi = i\sqrt{2}$, случай $\xi = -i\sqrt{2}$ доказывается аналогично.

Пусть

$$z = z_1 + i\sqrt{2}z_2 = -i\sqrt{2}[\frac{2z_2}{2}] + z_1 =$$

$$= -\xi\left[\frac{s_{-1}(z)}{2}\right] + s_0(z).$$

Так как наименьший многочлен, корнем которого является ξ, $m(x) = x^2 + 2$, то норма (5) $\mathrm{N}(\xi) = 2 = i\sqrt{2}(-i\sqrt{2}) = \xi(-i\sqrt{2})$. Следовательно, $\xi \mid \mathrm{N}(\xi)$. И, таким образом, получаем

$$a_0(z) \equiv z_1 \equiv s_0(z) (\bmod \mathrm{N}(\xi))$$

Далее, предполагаем, что выполняется равенство

$$\frac{z - \sum_{j=0}^{k} a_j(z)\,\mathrm{N}(\xi)^j}{\xi^{k+1}} = -\xi\left[\frac{s_k(z)}{\mathrm{N}(\xi)}\right] + s_{k+1}(z). \qquad (7)$$

Из последнего соотношения следует, что $a_{k+1} \equiv s_{k+1} (\bmod \mathrm{N}(\xi))$.

Учитывая, что минимальный многочлен определяется как $m(x) = x^2 + 2$, мы получим, что

$$s_{k+1}(z) = a_{k+1}(z) + \left[\frac{s_{k+1}(z)}{\mathrm{N}(\xi)}\right]\mathrm{N}(\xi) =$$

$$= a_{k+1}(z) + \xi\left(-\xi\left[\frac{s_{k+1}(z)}{\mathrm{N}(\xi)}\right]\right).$$

Следовательно, правая часть равенства (7), примет вид:

$$a_{k+1}(z) + \xi\left(-\left[\frac{s_k(z)}{\mathrm{N}(\xi)}\right] - \xi\left[\frac{s_{k+1}(z)}{N(\xi)}\right]\right) =$$

$$= a_{k+1}(z) + \xi\left(s_{k+2} - \xi\left[\frac{s_{k+1}(z)}{\mathrm{N}(\xi)}\right]\right),$$

то есть равенство (7) выполняется и для случая $k+1$, и, следовательно, для всех $k \geq 0$ ◄

Числа Мерсенна и Ферма в кольце $\mathbf{Q}[\xi]$

Пусть $\xi = i\sqrt{2}$, $\overline{\xi} = -i\sqrt{2}$.

Определение 2. В кольце $\mathbf{Q}[\xi]$ числами Мерсенна будем называть числа

$$M_n^2 = (\xi^n - 1)(\overline{\xi}^n - 1) = 2^n - (\xi^n + \overline{\xi}^n) + 1.$$

Определение 3. В кольце $\mathbf{Q}[\xi]$ числами Ферма будем называть числа

$$F_n^7 = (\xi^n + 1)(\overline{\xi}^n + 1) = 2^n + (\xi^n + \overline{\xi}^n) + 1.$$

Определение 4. При $n \neq 0 (\bmod 2)$ числа F_n^2 [M_n^2] будем называть *нормальными*, если выполняются условия:

- при всех $1 < s < n$ числа F_n^2 [M_n^2] и F_s^2 [M_s^2, соответственно] взаимно просты;
- элемент n обратим в кольце $\mathbf{Z}/F_n^2\mathbf{Z}$ [элемент n в кольце $\mathbf{Z}/M_n^2\mathbf{Z}$ соответственно].

Нормальные числа в таблицах 1,2 выделены.

Несложно показать, что

$F_{2k-1}^2 = M_{2k-1}^2,\ k \in \mathbf{Z}$.

Таблица 1. Факторизация чисел M_n^2 $(1 \le n \le 40)$

N	Факторизация
1	3
2	3x3
3	3x3
4	3x3
5	3x11
6	3x3x3x3
7	3x43
8	3x3x5x5
9	3x3x3x19
10	3x3x11x11
11	3x683
12	3x3x3x3x7x7
13	3x2731
14	3x3x43x43
15	3x3x3641
16	3x3x5x5x17x17
17	3x43691
18	3x3x3x3x3x3x19x19
19	3x174763
20	3x3x11x11x31x31
21	3x3x43x5419
22	3x3x466489
23	3x2796203
24	3x3x3x3x7x7x5x5x13x13
25	3x11x251x4051
26	3x3x2731x2731
27	3x3x19x87211
28	9x9x5461x5461
29	3x59x3033169
30	9x9x3641x3641
31	3x715827883
32	9x289x1285x1285
33	3x3x9544371777
34	3x3x43691x43691
35	3x11x43x281x86171
36	9x9x9x19x19x7x7x73x73
37	3x25781083x1777
38	3x3x174763x174763
39	3x3x22366891x2731
40	3x3x5x5x5x5x11x11x31x31x41x41

Таблица 2. Факторизация чисел F_n^2 $(1 \le n \le 40)$

N	Факторизация
1	3
2	1
3	3x3
4	5x5
5	3x11
6	7x7
7	3x43
8	17x17
9	3x3x3x19
10	31x31
11	3x683
12	3x3x3x3x7x7
13	3x2731
14	127x127
15	3x11x331
16	257x257
17	3x43691
18	7x7x73x73
19	3x174763
20	5x5x5x5x41x41
21	3x3x43x5419
22	23x23x89x89
23	3x2796203
24	17x17x241x241
25	3x11x251x4051
26	8191x8191
27	3x3x3x3x19x87211
28	5x5x29x29x113x113
29	3x59x3033169
30	7x7x31x31x151x151
31	3x715827883
32	65537x65537
33	3x3x9544371777
34	131071x131071
35	3x11x43x281x86171
36	5x5x13x13x37x37x109x109
37	3x25781083x1777
38	524587x524587
39	3x3x22366891x2731
40	17x17x61681x61681

Лемма 2. При $n \neq 0 (\mathrm{mod}\, 2)$, числа $d_1 = \left(\xi^n - 1\right)$ и $d_2 = \left(\overline{\xi^n} - 1\right)$ взаимно просты.

Доказательство. Допустим обратное: пусть существуют $a, b_1, b_2 \in \mathbf{Q}[\gamma]$, не являющиеся единицами в $\mathbf{Q}(\gamma)$, такие что $d_1 = ab_1$, $d_2 = ab_2$.

Так как алгебраическая норма $\mathrm{N}(\gamma)$, $\gamma \in \mathbf{Q}(\xi)$ является мультипликативной функцией: $\mathrm{N}(wz) = \mathrm{N}(w)\,\mathrm{N}(z)$, то из очевидных равенств

$$d_1 + d_2 = -2\,,\ a(b_1 + b_2) = -2\,,$$

следует,

$$4 = \mathrm{N}(-2) = \mathrm{N}\left(a(b_1 + b_2)\right) = \mathrm{N}\left(a\right)\mathrm{N}\left(b_1 + b_2\right).$$

Таким образом, $\mathrm{N}(a)$ является четным числом, что противоречит равенству

$$\mathrm{N}(d_1) = \mathrm{N}(ab_1) = 1 + 2 \cdot 2^{n-1} = \mathrm{N}(a)\,\mathrm{N}(b_1). \qquad \blacktriangleleft$$

В силу доказанной леммы, возможно определить изоморфизм между фактор-кольцом $\mathbf{Z}/M_n^2\mathbf{Z}$ и прямой суммой колец $\mathbf{Z}/(\xi^n - 1) \oplus \mathbf{Z}/(\overline{\xi}^n - 1)$. Далее будем рассматривать лишь случай $n = 2t+1$ и M_{2t+1}^2.

Приведем правила реализации операций, например, в кольце $\mathbf{K} = \mathbf{Z}/(\xi^n - 1)$.

1. Любой элемент кольца $\mathbf{K}$ представляется в форме

$$W = \xi^{2t} a_{2t} + \xi^{2t-1} a_{2t-1} + \xi^{2t-2} a_{2t-2} + \ldots + \xi^1 a_1 + \xi^0 a_0 \ ;$$
$$a_j \in \{0,1\} . \qquad (8)$$

2. Это представление однозначно для всех $0 \neq W \in K$; нулевой элемент представим двумя способами в форме (8):

$$0 \cdot \left(i\sqrt{2}\right)^0 + \ldots + 0 \cdot \left(i\sqrt{2}\right)^{2t} = 1 \cdot \left(i\sqrt{2}\right)^0 + \ldots +$$
$$+1 \cdot \left(i\sqrt{2}\right)^{2t} = \left(i\sqrt{2}\right)^{2t+1} - 1 = 0 \left(\mathrm{mod}(\xi^n - 1)\right)$$

так как $\sqrt{2}^{2t+1} \equiv 1 (\mathrm{mod}\, P)$, то в случае возникновения «бита переполнения» $1 \cdot \xi^{2t+1}$ при вычислениях эта единица переносится в «самый младший разряд» и суммируется с полученным числом.

3. Сложение элементов производится с «двойным переносом через разряд».
Данное правило основывается на соотношении:
$2 \cdot (\pm i\sqrt{2})^j = 1 \cdot (\pm i\sqrt{2})^{j+4} + 1 \cdot (\pm i\sqrt{2})^{j+2}$.

4. Умножение элемента $W \in \mathbf{K}$ на элемент $\xi = i\sqrt{2} \in K$ равносильно циклическому сдвигу «цифр» a_j в представлении (8):
$$\sqrt{2} W = \alpha^{2t+1} a_t^1 + (\alpha^{2t} a_{t-1}^2 + \alpha^{2t-1} a_{t-1}^1 + \ldots + \alpha^2 a_0^2 + \alpha^1 a_0^1) =$$
$$= \alpha^{2t} a_{t-1}^2 + \alpha^{2t-1} a_{t-1}^1 + \ldots + \alpha^2 a_0^2 + \alpha^1 a_0^1 + \alpha^0 a_t^1 .$$

5. Умножение элементов кольца **K** «столбиком» сводится к циклическим перестановкам цифр и сложениям;

6. Мультипликативный порядок элемента $\xi = i\sqrt{2} \in \mathbf{K}$ равен $2t+1$: $\mathrm{Ord}(i\sqrt{2}) = 2t+1$ (следовательно, при $\omega = \sqrt{2} \in \mathbf{s}_1$ возможна реализация ТЧП (4) длины N = 2t+1 без умножений).

Аналогичные правила вычислений могут быть получены для кольца $\bar{\mathbf{K}} = \mathbf{Z} \big/ \left(\bar{\xi}^n - 1\right)$, простой заменой $\xi = i\sqrt{2}$ в формулах для кольца **K** на $\bar{\xi} = -i\sqrt{2}$.

Пусть, далее, (D_1) – главный идеал, порожденный d_1, (D_2) – главный идеал, порожденный d_2.

Лемма 3. Для любого $X = \mathbf{Z} \big/ q\mathbf{Z}$ существуют эффективно определяемые элементы $P_1, P_2 \in \mathbf{Q}[\xi]$ и константы $a, b \in \mathbf{Z} \big/ q\mathbf{Z}$ такие, что справедливо равенство $X = aP_1D_2 + bP_2D_1$, причем $X \equiv P_1 \left(\mathrm{mod}(D_1)\right)$, $X \equiv P_2 \left(\mathrm{mod}(D_2)\right)$;

Доказательство. Данная лемма является непосредственным следствием китайской теоремы об остатках. В качестве коэффициентов a и b можно взять $a = b = 2^{2t+1}$. ◄

Проекции P_1 и P_2 могут быть легко найдены с использованием Алгоритма 1. Действительно, необходимо лишь, найдя разложения числа X в системах счисления с основанием $\xi_1 = i\sqrt{2}$ и $\xi_2 = -i\sqrt{2}$, соответственно для P_1 и P_2, вычислить наименьший неотрицательный вычет. Для этого полученные биты переполнения – «цифры», начиная с a_{2t+1}, нужно добавить к младшим битам, используя свойство $1 \cdot \xi^{2t+1} \equiv 1 \left(\mathrm{mod}\left(\xi^{2t+1} - 1\right)\right)$ и правила сложения в соответствующем кольце. ◄

Вычисление свертки

Поскольку арифметические операции в кольцах **K** и $\bar{\mathbf{K}}$ представляют собой, по сути, операции циклического сдвига и «покоординатного» сложения с двойными переносами, т. е. операции над битовыми векторами, введем определение.

Определение 5. Для любого $W \in \mathbf{s}_1$ [$W \in \bar{\mathbf{K}}$],
$W = \xi^{2t} a_{2t} + \xi^{2t-1} a_{2t-1} + \xi^{2t-2} a_{2t-2} + \ldots + \xi^1 a_1 + \xi^0 a_0$
[$W = \bar{\xi}^{2t} a_{2t} + \bar{\xi}^{2t-1} a_{2t-1} + \bar{\xi}^{2t-2} a_{2t-2} + \ldots + \bar{\xi}^1 a_1 + \bar{\xi}^0 a_0$]
вектор $\langle W \rangle = (a_{2t}, a_{2t-1}, a_{2t-2}, \ldots, a_1, a_0)$ будем называть кодом W. Положим $\langle W(j) \rangle = a_j$.

В работе [3] введены понятия сдвига Мерсенна и шифт-преобразования Мерсенна.

Определение 6. Оператором левого сдвига Мерсенна назовем оператор M такой, что

$$M \langle W \rangle = (a_{2t-1}, a_{2t-2}, \ldots, a_1, a_0, a_{2t}) .$$

Аналогично определяется оператор правого сдвига Мерсенна

$$M^{-1} \langle W \rangle = (a_0, a_{2t}, a_{2t-1}, a_{2t-2}, \ldots, a_1) .$$

Для колец **K**, $\bar{\mathbf{K}}$ данный оператор аналогичен $M \langle W \rangle = \langle \xi W \rangle$, $M \langle W \rangle = \langle \bar{\xi} W \rangle$, соответственно.

Определение 7. Пусть $x(n)$ есть T – периодическая последовательность элементов кольца **K** или **K**; $T = 2t+1$. Определим шифт-преобразование Мерсенна последовательности $x(n)$ равенствами:

$$\langle X_k(m) \rangle = \sum_{n=0}^{T-1} M^{mn} \langle x(n) \rangle \ (m = 0, 1, ..., T-1).$$

В работе [3] доказывается, справедливость равенства

$$\langle T \cdot x(n) \rangle = \sum_{m=0}^{T-1} M^{-mn} \langle X(m) \rangle .$$

Заметим, что *алгоритм 1* определения цифр в системах счисления по основанию $\xi_1 = i\sqrt{2}$ и $\xi_2 = -i\sqrt{2}$ для числа $z \in \mathbf{Q}[\xi]$ даст одинаковые векторы «цифр», то есть, коды $\langle P_1 \rangle$ и $\langle P_2 \rangle$ для обеих систем счисления:

$\langle P_1 \rangle = \langle P_2 \rangle$.

Это позволяет улучшить результат работы [3], сократив количество необходимых вычислений.

Теорема 1. *Если для преобразуемых последовательностей x(n) и h(n) с помощью метода леммы 3 найдены коды проекций* $\langle P_1(n)_X \rangle \langle P_2(n)_X \rangle$ *и* $\langle P_1(n)_H \rangle \langle P_2(n)_H \rangle$ *в кольца* **К** *и* $\overline{\mathbf{K}}$*, соответственно, то для вычисления свертки (1) длины* $T = 2t+1$ *достаточно выполнения:*

- трех шифт-ТЧП Мерсенна (двух прямых и одного обратного типа (2*t*+1;0));
- вычисления произведений компонент спектров шифт-ТЧП в псевдомерсенновской арифметике (в одном из колец);
- реконструкции значений свертки по китайской теореме об остатках.

Сокращение вычислений в данном случае происходит из-за того, что из свойства $\langle P_1 \rangle = \langle P_2 \rangle$ для любой из последовательностей, следует что спектр этой последовательности, коды элементов спектра, будут совпадать. Обозначим через $\tilde{P}_1$ спектр проекции P_1, а через $\tilde{P}_1$ спектр проекции $\tilde{P}_1$ исходной последовательности.

$$\langle \tilde{P}_2(m) \rangle = \sum_{n=0}^{T-1} P_2(n)\overline{\xi}^{mn} \pmod{D_2} = \sum_{n=0}^{T-1} M^{mn} \langle P_2(n) \rangle =$$

$$= \sum_{n=0}^{T-1} M^{mn} \langle P_1(n) \rangle = \sum_{n=0}^{2t} P_1(n)\xi^{mn} \pmod{D_1} = \langle \tilde{P}_1(m) \rangle .$$

Таким образом, нет необходимости в вычислении компонент спектра обеих проекций. Для вычисления свертки достаточно вычисления спектра одной из проекций для каждой из преобразуемых последовательностей: необходимо два прямых шифт-ТЧП Мерсенна для *x(n)* и *h(n)*. Аналогично и для обратного преобразования. Вследствие равенства кодов спектров и совпадения реализации арифметических операций в кольцах **К** и $\overline{\mathbf{K}}$, умножение компонент спектра также проводится лишь в одном из колец. Перед реконструкцией результата, достаточно лишь иначе интерпретировать код проекции полученной последовательности в одном из колец, чтобы получить проекцию во второе кольцо (рис. 1).

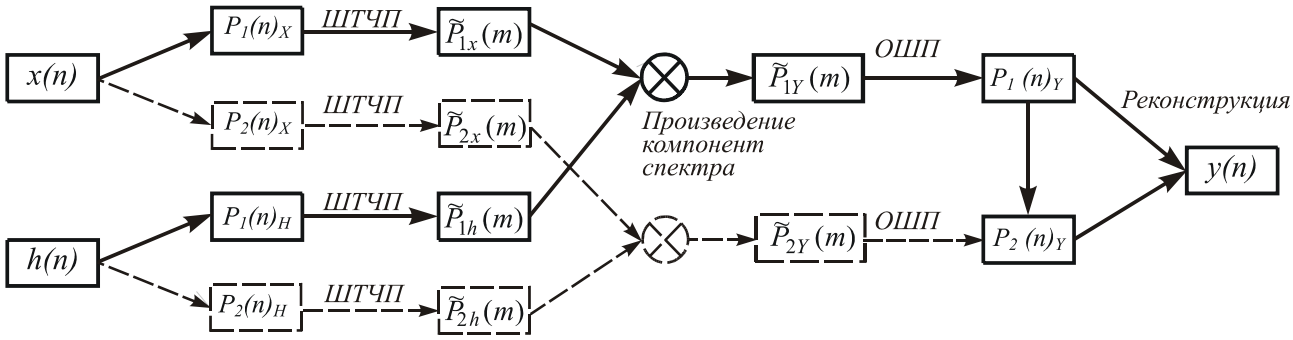

Рис.1. Схема вычисления свертки

Реализации параллельного алгоритма вычисления свертки мешает тот факт, что все числа $M_n^2 (1 \le n \le 40)$ из таблицы 1 имеют общий множитель, равный 3. Взаимная не простота этих чисел может привести к нарушению ортогональности базисных функций теоретико-числового преобразования (4)

$$f_m^{\pm}(t) = (\pm i\sqrt{2})^{mt}$$

дискретных преобразований (4) вычисляемых $\mathrm{mod}(\xi^n - 1)$, $\mathrm{mod}(\overline{\xi}^n - 1)$.

Однако, указанную трудность можно преодолеть. Действительно, пусть $M_N^2 \neq 0 (\mathrm{mod}\, 3)$, а неотрицательные целочисленные последовательности $x(n)$, $h(n)$ и число M_N^2 удовлетворяют неравенству

$$\frac{1}{3} M_N^2 = M > N \max_{0 \le n < N} \{x(n)\} \max_{0 \le n < N} \{h(n)\} .$$

Тогда значения компонент свертки (1) совпадают с их наименьшими неотрицательными вычетами $(\mathrm{mod}\, M)$. Пусть $y_3(k)$ - результат вычисления $(\mathrm{mod}\, 3)$ свертки (9), гипотетически полученный независимым методом. Результат $Y(k)$ - вычисления свертки с помощью шифт-преобразований с распараллеливанием в кольцах классов вычетов по $\mathrm{mod}(\xi^n - 1)$, $\mathrm{mod}(\overline{\xi}^n - 1)$, является «ошибочным» – числа M_n^2 не являются нормальными (нарушается второе условие). Но, по крайней мере, для нечетных значений n (в пределах Таблицы 1) для нормальных чисел M_n^2 числа $\frac{1}{3} M_n^2$ не делятся на 3. Поэтому, по китайской теореме об остатках для $a, b \in \mathbf{Z}$ с условиями $3a \equiv 1 (\mathrm{mod}\, M)$, $3a \equiv 1 (\mathrm{mod}\, M)$, выполняется соотношение

$$Y(k) = 3ay(k) + Mby_3(k) \left(\mathrm{mod}\, M_N^2\right),$$

откуда следует, что независимо от $y_3(k)$, справедливы сравнения

$$Z(k) \equiv 3ay(k) + Mby_3(k) \left(\mathrm{mod}\, M_N^2\right)$$

$$Y(k) = y(k) \left(\mathrm{mod}\, M \right).$$

То есть, истинное значение $y(k)$ свертки получается редуцированием $Y(k)$ по $\left(\mathrm{mod}\, M \right)$.

Заключение

Предлагаемый алгоритм, основан на вычислении свертки *без* использования умножений. Поэтому алгоритм является эффективным и при прямой реализации вычисления свертки, в частности, в случае, когда длина свертки является простым числом.

Предложенная методика позволяет расширить класс используемых чисел для вычисления свертки с применением ТЧП. Реализация алгоритма и возможная его оптимизация зависят от длины вычисляемой свертки, от величины $2t+1$. В работе, были рассмотрены бинарные системы счисления в квадратичном поле. Однако, как показано в работе [9], бинарные системы также возможны в полях алгебраических чисел более высоких степеней. Общая методология синтеза соответствующих параллельных алгоритмов машинной арифметики в таких системах счисления анонсирована в [11].

Благодарности

Работа выполнена при поддержке Российского фонда фундаментальных исследований (Проект 03-01-00736) и российско-американской программы «Фундаментальные исследования и высшее образование» («BRHE»).

Литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си // М.: Издательство ТРИУМФ, 2002. 816 с.
2. Handbook of Applied Cryptography // by A. Menezes, P. Van Oorschot, and S. Vanstone. CRC Press, 1996.
3. Chernov V.M., Pershina M.V. «Error-free» calculation of the convolution using generalized Mersenne and Fermat transforms over algebraic fields // In: G. Sommer, K. Daniilidis, J. Pauli (Eds) "*Computer Analysis of Image and Pattern"*. (CAIP'97). Springer, LNCS 1296. P. 621-628
4. Чернов В.М. Синтез параллельных алгоритмов преобразований Фурье-Галуа в прямых суммах конечных колец // Известия Самарского научного центра Российской Академии Наук, 2000. Вып.1. №2. С. 128-134.
5. Kátai I., Kovács B. Canonical number systems in imaginary quadratic fields // Acta Mathematica Academiae Scientarium Hungaricae. T. 37 (1-3), 1981. P. 159-164.
6. Kátai I., Szabo J. Canonical number systems for complex integers // Acta Sci.Math.(Szeged), 37. 1975. P. 255-260.
7. Thuswardner J. Elementary properties of canonical number systems in quadratic fields // G.E. Bergum et al. (eds.), Applications of Fibonacci Numbers, Volume 7. P. 405-415.
8. Кнут Д. Искусство программирования // Получисленные алгоритмы, 3-е изд. М.: Изд. Дом «Вильямс», 2001. Т.2. 832 с.
9. Kovács A. Generalized binary number systems // Annales Univ. Sci. Budapest, Sect. Comp. 20. 2001. P. 195-206.
10. Чернов В.М. Неоднозначность разложения на множители, канонические системы счисления в квадратичных кольцах и параллельные алгоритмы вычисления свертки // Доклады 11-й конференции Математические методы распознавания образов (ММРО-11), М..: 2003. С. 212-215