УДК 512.643:519.712.2:621.391

СИНТЕЗ ПАРАЛЛЕЛЬНЫХ АЛГОРИТМОВ ПРЕОБРАЗОВАНИЙ ФУРЬЕ-ГАЛУА В ПРЯМЫХ СУММАХ КОНЕЧНЫХ КОЛЕЦ

© 2000 В.М. Чернов

Институт систем обработки изображений РАН, г. Самара

Рассматривается метод синтеза быстрых алгоритмов дискретных преобразований, позволяющих, в частности, безошибочно и с минимальным числом умножений вычислять дискретные свертки целочисленных последовательностей. Предложенный подход базируется на неоднозначности разложения на простые множители в алгебраических кольцах. Выбор подходящего разложения определяется особенностями машинной реализации модулярных вычислений.

Введение

Модулярные аналоги дискретного преобразования Фурье (теоретико-числовые преобразования, ТЧП, преобразования Фурье-Галуа)

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

были впервые введены в работах Р.Г. Фараджиева и Я.З.Ципкина [1, 2], А.Штрассена и В. Шёнхаге [3] и переоткрыты в работе Ч.М. Рейдера [4]. Последняя работа получила наибольшую известность и явилась основой для различных модификаций и обобщений ТЧП. Наибольшая популярность этой тематики приходится на 70-е годы, что объясняется, в основном, вычислительными преимуществами целочисленной арифметики для использовавшихся цифровых устройств и возможностями эффективного решения массовых задач информатики – “безошибочного” вычисления циклической свертки (целочисленных) последовательностей [5] и быстрого умножения больших целых чисел [3]. Возрождение интереса к ТЧП, наметившееся в последние годы, связано с разработкой нового поколения СБИС-устройств, использующих модулярные вычисления для реализации арифметических операций [6 - 9].

Наиболее существенным недостатком ТЧП является то, что простые числа p с “удобной” машинной реализацией (простые числа Мерсенна, Ферма, Голомба и т.п) встречаются в натуральном ряду достаточно редко [10], что существенно ограничивает возможности ТЧП, например, в задачах цифровой обработки многомерных цифровых массивов (в частности, изображений).

В настоящей работе рассматривается метод синтеза параллельных алгоритмов “безошибочного” вычисления сверток целочисленных последовательностей с использованием “ТЧП-подобных” преобразований, реализуемых в кольцах классов вычетов по модулю составных чисел. Метод базируется на двух независимых и хорошо апробированных идеях:

– вложение кольца классов вычетов по (составному) (mod m) в прямую сумму некоторых конечных колец;

– представление данных в «нетрадиционных» системах счисления.

Существенно новым в рассмотренном методе является согласованный выбор конечных колец, способа вложения кольца классов вычетов в прямую сумму этих колец, а также систем счисления «с иррациональным основанием», наследующих свойства двоичной системы счисления в кольцах классов вычетов по модулям простых чисел Ферма. Аналогичная задача для вычислений в кольцах классов вычетов по модулям составных чисел Мерсенна рассмотрена автором в работе [13].

Теоретико-числовое преобразование Ферма

Исторически первым ТЧП, нашедшим эффективные применения в задачах цифровой обработки сигналов, явилось преобразование (1) при

$$p = f_s = 2^{2^s}+1 = 2^B+1, \quad s = 0, 1, 2, 3, 4. \quad (2)$$

Числа f_s называются числами Ферма и

являются простыми только при пяти указанных значениях s. Преобразование (1) при $p = f_s$ называется ТЧП Ферма или просто преобразованием Ферма.

Привлекательность преобразования Ферма обуславливается по меньшей мере двумя факторами:

– существование удобного для машинной реализации "битового" представления элементов поля (mod f_s) с просто реализуемыми операциями сложения и умножения элементов.

– наличие хорошей алгоритмической поддержки вычисления преобразования (1) в виде структурно простых модулярных аналогов классического быстрого алгоритма Кули-Тьюки дискретного преобразования Фурье.

Действительно, любое целое число x из диапазона $0 \le x \le f_s - 1 = 2^B$ может быть представлено (B+1)-битовым разложением

$$x = x_B 2^B + x_{B-1} 2^{B-1} + ... + x_1 2^1 + x_0 2^0, \quad x_j = 0,1. \tag{3}$$

Ассоциированный с разложением (3) (B+1)-битовый вектор

$$< x >= (x_B, x_{B-1}, ... x_1, x_0) \ . \tag{4}$$

будем называть *кодом* элемента x (mod f_s).

Операции в кольце классов вычетов (mod f_s) индуцируют формальные правила преобразования кодов, вполне определяемые соотношением

$$2^B \equiv -1 \pmod{f_s}. \tag{5}$$

Именно, *сложение* производится по почти обычным правилам двоичного сложения "с переносом в старший разряд"; при переполнении B-го разряда "лишняя" единица вычитается из B–разрядной части результата (или, в терминах кодов, "с инвертированным знаком переносится в самый младший разряд кода); *умножение на 2 элемента x* индуцирует преобразование кодов по правилу

$$< X >= (X_B, X_{B-1}, ... X_1, X_0) \mapsto \mapsto < 2X >= (X_{B-1}, ... X_1, X_0, -X_B); \tag{5}$$

умножение элементов общего вида сводится к сложениям и умножением на степени 2.

Заметим, что код в правой части соотношения (5) не обязательно является битовым вектором, но может быть легко преобразован к битовому виду с использованием тривиального соотношения

$$x_{j+1} 2^{j+1} = x_{j+1} 2^j + x_{j+1} 2^j. \tag{6}$$

Такие векторы, преобразованные по правилу (6) к битовому представлению, будем называть *редуцированными кодами* и обозначать $< x >^*$.

Далее, в отличие от поля комплексных чисел, в конечном поле (mod p) существуют корни не любой степени N единицы, а только удовлетворяющие условию делимости:

$$N \,||\, (p\text{-}1). \tag{7}$$

Для чисел Ферма это стеснительное, в общем случае, ограничение (7) гарантирует существование структурно простых быстрых алгоритмов вычисления преобразования (1).

Наиболее просто реализуется преобразование (1) при $\omega \equiv 2 \pmod{f_s}$. В этом случае умножения на фазовые множители в модулярной версии алгоритма Кули-Тьюки (БПФ) реализуются без нетривиальных вещественных умножений [15].

К сожалению, в силу соотношения (5), элемент $\omega \equiv 2 \pmod{f_s}$ является корнем степени $N = 2B \pmod{f_s}$, что ограничивает максимальную длину преобразования Ферма, реализуемого без умножений, числом $N = 32$.

Кроме того, для "безошибочного" вычисления свертки спектральным методом с использованием ТЧП, число p должно быть достаточно велико [16]. В частности, при решении типичной для цифровой обработки изображений задачи вычисления двумерной свертки двух целочисленных массивов размера (512×512) с динамическими диапазонами $0 \div 255$, для числа p должно выполняться неравенство:

$$p > (512)^2 \ (256)^2 = 2^{34} > f_4 = 2^{16} + 1.$$

Это существенно ограничивает возможности применения ТЧП Ферма в задачах обработки многомерной цифровой информации. Использование в качестве модулей в преобразовании (1) составных чисел Ферма доставляет серьезные 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 (1). Кроме того, даже при условии частичной компенсации отмеченных проблем, например, при распараллеливании вычислений в системе остаточных классов [11, 12], характерные преимущества "битовой" реализации арифметических операций именно в полях по модулям чисел Мерсенна и Ферма не наследуются для вычислений в полях по модулям целых делителей составных чисел Мерсенна или Ферма. Действительно,

$$f_5 = 2^{32} + 1 = 641 \cdot 6\,700\,417$$

и сомножители уже не являются числами Ферма.

Альтернативное разложение чисел Ферма

Пусть, для определенности, число Ферма f имеет вид

$$f = 2^B + 1, \quad B = 2^r = 3t + 1 \qquad (8)$$

и обладает свойствами:

(a) при всех $1 < s < 3t + 1$ числа f и $2^s - 1$ взаимно просты;

(b) элемент $2(3t + 1)$ обратим в фактор-кольце $\mathbf{Z}/(f)$;

(c) число f не делится на 3, то есть $f \neq 0 \pmod 3$.

Рассмотрим кольцо S целых элементов поля F разложения полинома $\varphi(z) = z^3 + 2$ над Q. В кольце $S \supset Z$ для числа f наряду с обычным представлением составного числа в виде произведения целых рациональных чисел возможно представление в форме

$$f = \left(2^t \sqrt[3]{2} + 1\right)\left(2^t \gamma \sqrt[3]{2} + 1\right)\left(2^t \bar{\gamma} \sqrt[3]{2} + 1\right). \quad (9)$$

где γ - примитивный корень третьей степени из единицы.

Лемма 3.1. Элементы $f_1, f_2, f_3 \in$ S:

$$f_1 = \left(2^t \sqrt[3]{2} + 1\right), \quad f_2 = \left(2^t \gamma \sqrt[3]{2} + 1\right), \quad f_3 = \left(2^t \bar{\gamma} \sqrt[3]{2} + 1\right)$$

попарно взаимно просты в кольце S.

Доказательство. Допустим, что существуют $a, b_1, b_2 \in$ **S,** не являющиеся единицами кольца S, такие что $f_1 = a\,b_1$, $f_2 = ab_2$. Нормальным полем для многочлена $\varphi(z)$ является поле $F=Q(\gamma, \sqrt[3]{2})$. Пусть $\mathrm{Norm}_\gamma(x)$ есть относительная норма элемента $x \in$ F в поле $\mathbf{Q}(\gamma)$. Трехэлементная группа Галуа полинома $\varphi(z)$ над подполем $\mathbf{Q}(\gamma)$ циклична и действует тождественно на Q. Относительная норма элемента

$$z = x + y\sqrt[3]{2} \in \mathrm{S}$$

равна $\mathrm{Norm}_\gamma(z) = x^3 + 2y^3$. Поэтому из очевидных равенств

$$f_2 = \gamma f_1 + 1 - \gamma, \quad f_2 - f_1 = (f_1 - 1)(\gamma - 1)$$

следует

$$\begin{aligned} &\mathrm{Norm}_\gamma(f_1 - 1)\,\mathrm{Norm}_\gamma(\gamma - 1) = \\ &= \mathrm{Norm}_\gamma(a)\,\mathrm{Norm}_\gamma(b_1 - b_2), \\ &2^B(\gamma\gamma - 1)^3 = \\ &= \mathrm{Norm}_\gamma(a)\,\mathrm{Norm}_\gamma(b_1 - b_2). \end{aligned} \qquad (10)$$

Так как $\mathrm{Norm}_\gamma(a)$ не может быть четным числом, что противоречило бы равенству

$$\begin{aligned} &\mathrm{Norm}_\gamma(f_1) = \mathrm{Norm}_\gamma(ab_1) = \\ &= f = 2^B + 1 = \mathrm{Norm}_\gamma(a)\,\mathrm{Norm}_\gamma(b_1), \end{aligned}$$

то равенство (10) может выполняться только при условии делимости

$$\mathrm{Norm}_\gamma(a) \mid\mid (\gamma - 1)^3. \qquad (11)$$

Так как $\mathrm{Norm}_\gamma(a) \in Q(\gamma)$, то вычисляя норму элементов (11) над Q, получаем:

$$\mathrm{Norm}\,(\mathrm{Norm}_\gamma(a)) \mid\mid \mathrm{Norm}\,(\gamma - 1)^3 = 27,$$

что противоречит условию $f \neq 0 \pmod 3$. Аналогично доказывается взаимная простота остальных элементов в условии леммы.

Пусть элементы f_1, f_2, f_3 определены в лемме 3.1. Введем для удобства новые обозначения: $P = f_1$, $Q = f_2$, $R = f_3$.

Лемма 3.1 гарантирует возможность представления фактор-кольца $\mathbf{S}/\mathbf{f}$ в виде прямой суммы

$$\mathbf{S}/\mathbf{f} \equiv \mathbf{S}/\mathbf{p} \oplus \mathbf{S}/\mathbf{q} \oplus \mathbf{S}/\mathbf{r}$$

фактор-колец $\mathbf{S}/\mathbf{p}$, $\mathbf{S}/\mathbf{q}$, $\mathbf{S}/\mathbf{r}$, где f = (*f*), p =(*P*), q =(*Q*), r =(*R*) - главные идеалы, порожденные элементами *f, P, Q, R*, и возможность вложения подкольца $\mathbf{Z}/f\mathbf{Z} \subset \mathbf{S}/\mathbf{f}$ в эту

прямую сумму. Поэтому следующая лемма является частным случаем китайской теоремы об остатках [14]. Её доказательство приводится только для явного описания такого вложения.

Лемма 3.2. Для любого $W \in \mathbf{Z}/f\mathbf{Z}$ существуют эффективно определяемые элементы $X, Y, Z \in \mathbf{S}/(f)$ и константы $a, b, c \in \mathbf{Z}/f\mathbf{Z}$ такие, что:

(а) справедливо равенство

$$W = aXQR + bYPR + cZPQ, \qquad (12)$$

причем

$$X \equiv W \pmod{(P)},\ Y \equiv W \pmod{(Q)},$$
$$Z \equiv W \pmod{(R)};$$

(б) числа X, Y, Z допускают представления в форме:

$$\begin{aligned} X &= X_1 + X_2\sqrt[3]{2} + X_3\sqrt[3]{4};\\ Y &= Y_1 + Y_2\sqrt[3]{2} + Y_3\sqrt[3]{4};\\ Z &= Z_1 + Z_2\sqrt[3]{2} + Z_3\sqrt[3]{4};\\ 0 \le X_1, Y_1, Z_1 &< 2^{t+1};\\ 0 \le X_2, Y_2, Z_2, X_3, Y_3, Z_3 &< 2^t. \end{aligned} \qquad (13)$$

Доказательство. Соотношение (12) является следствием китайской теоремы об остатках. Для доказательства свойства (а) необходимо доказать, что $a,b,c \in \mathbf{Z}/f\mathbf{Z}$. Непосредственно проверяются равенства:

$$RQ = (P - 3)P + 3, \quad PR = (Q - 3)Q + 3,$$
$$PQ = (R - 3) + 3.$$

Поэтому для выполнения равенств

$$aQR \equiv 1 \pmod{P},\ bPR \equiv 1 \pmod{Q},$$
$$cPQ \equiv 1 \pmod{R}$$

достаточно положить

$$a \equiv 3^{-1} \pmod{f},\ b \equiv 3^{-1} \pmod{f},$$
$$c \equiv 3^{-1} \pmod{f}.$$

Опуская рутинные выкладки, связанные с применением метода неопределенных коэффициентов, приведем выражения для X_j, Y_j, Z_j ($j = 1, 2, 3$) в форме:

$$\begin{aligned} X_1 + (-X_3)\,2^{t+1} + X_2\,2^{2t+1} &= (3a)^{-1}\,W,\\ Y_1 + (-Y_3)\,2^{t+1} + Y_2\,2^{2t+1} &= (3b)^{-1}\,W,\\ Z_1 + (-Z_3)\,2^{t+1} + Z_2\,2^{2t+1} &= (3c)^{-1}\,W. \end{aligned} \qquad (14)$$

Из соотношений (14) эффективно определяются значения X_j, Y_j, Z_j. Действительно, пусть χ есть наименьший неотрицательный вычет для $(3a)^{-1}\,W \pmod{f}$. Пусть далее quot $(u \,//\, v)$ и exc $(u \,//\, v)$ – неполное частное и остаток от деления числа u на v, соответственно. Тогда, например, для X_j имеем:

$$X_1 = \text{exc}\,(\chi \,//\, 2^{t+1}),\ X_2 = \text{quot}\,(\chi - X_1 \,//\, 2^{2t+1}),\ (-X_3) = (\chi - X_1)\,2^{-t-1} - X_2\,2^t.$$

Нетрудно заметить, что элементы X_2, X_3 допускают t-битовое представление, а элемент X_1 допускает $(t+1)$-битовое представление.

Рассмотрим первое из равенств (13). Пусть

$$X_1 = X_t^1 2^t + \ldots + X_0^1 2^0,\ X_2 = X_{t-1}^2 2^{t-1} + \ldots$$
$$+ \ldots + X_0^2 2^0,\ X_3 = X_{t-1}^3 2^{t-1} + \ldots + X_0^3 2^0$$

есть битовые представления элементов X_1, X_2, X_3. Тогда соотношение (13) для X можно переписать в виде:

$$X = X_t^1\left(\sqrt[3]{2}\right)^{3t} + X_{t-1}^2\left(\sqrt[3]{2}\right)^{3t-1} + X_{t-1}^3\left(\sqrt[3]{2}\right)^{3t-2} + \\ + X_{t-1}^1\left(\sqrt[3]{2}\right)^{3t-3} + \ldots + X_0^1\left(\sqrt[3]{2}\right)^0. \qquad (15)$$

Равенство (15) можно интерпретировать как представление элемента X “в системе счисления с основанием $\left(\sqrt[3]{2}\right)$”, равенства, аналогичные (15), для Y и Z - как представления элементов Y и Z “в системах счисления с основанием $\gamma\left(\sqrt[3]{2}\right)$ и $\bar{\gamma}\left(\sqrt[3]{2}\right)$”, соответственно.

Замечание 3.1. Несмотря на не вполне привычную терминологию (“системы счисления с иррациональным основанием”), никаких “приближенных” вычислений в данной работе не производится. Элементы, обозначенные $\left(\sqrt[3]{2}\right)$, $\gamma\left(\sqrt[3]{2}\right)$ и $\bar{\gamma}\left(\sqrt[3]{2}\right)$, есть просто три различных корня уравнения $W^3 = 1$ в фактор кольце $\mathbf{S}/\mathbf{f}$. Как будет показано ниже, такая (неформальная) интерпретация равенства (15) позволяет ввести простые правила преобразований ассоциированных кодов

$$< X >= (X_t^1, X_{t-1}^2, X_{t-1}^3, X_{t-1}^1, \ldots, X_0^1). \qquad (16)$$

Отметим также, что существует необходимый математический формализм для придания корректности понятию “системы счисления с иррациональным основанием”. Такие системы счисления достаточно давно и успешно применяются в информатике [17, 18].

Арифметические действия над элементами кольца $\mathbf{S}/_{\mathbf{f}}$ индуцируют правила преобразования кодов (16): при *сложении* элементов коды преобразуются по правилу “перенос в старший разряд через две позиции”; *умножение элемента X на* $\left(\sqrt[3]{2}\right)$ равносильно циклическому сдвигу кода с инвертированием знака младшего бита и т.д. Как и в случае обычной арифметики кольца вычетов (mod f_s), в результате таких преобразований получаются не обязательно битовые векторы, которые, тем не менее, могут быть легко преобразованы к битовому виду с использованием соотношения (6). Такие векторы, преобразованные по правилу (6) к битовому представлению, будем также называть *редуцированными кодами* компонентов элемента кольца $\mathbf{S}/_{\mathbf{f}}$ и обозначать $<X>^*$, $<Y>^*$, $<Z>^*$.

Шифт-преобразования Ферма

Определение 4.1. Оператор $\Im$, определенный на множестве (k+1)-мерных редуцированных кодов, такой что

$$\Im: <X>^* = (X_k, X_{k-1},\ldots,X_1, X_0)^* \rightarrow$$
$$<\Im\, X>^* = (X_{k-1},\ldots,X_1, X_0, -X_k)^* \qquad (17)$$

будем называть *оператором левого сдвига Ферма*. Аналогично определяется оператор правого сдвига Ферма, являющийся обратным к $\Im$.

Следующие два утверждения, сформулированные как леммы, приводятся без доказательств.

Лемма 4.1. Для любого (k+1)-мерного битового вектора X период последовательности $<\Im^n X>^*$ является делителем числа $2(k+1)$.

Определение 4.2. Пусть $<X(n)>^*$ есть N-периодическая последовательность (k+1)-мерных редуцированных кодов. Определим *шифт-преобразование Ферма* соотношением

$$< \hat{X}(m) >^* = \sum_{n=0}^{N-1} \Im^{mn} < X(n) >^*, \qquad (18)$$

где m = 0,1,…, N-1.

Замечание 4.1. При интерпретации редуцированных кодов как битовых представлений элементов поля классов вычетов по модулю f простого числа Ферма введенное шифт-преобразование совпадает с ТЧП Ферма при $\omega \equiv 2 \pmod f$. В этом случае при $m \neq k \pmod{2B}$ равенство

$$0 = \sum_{n=0}^{T-1} \Im^{-mk} < \Im^{mn} < E >^* >^*. \qquad (19)$$

равносильно очевидному равенству

$$0 \equiv \sum_{n=0}^{2B-1} 2^{n(m-k)} \pmod f. \qquad (20)$$

При $m \equiv k \pmod{2B}$ значение сумм (19) и (20) равны $2B \pmod f$. В общем случае шифт-преобразований значение суммы (19) определяется конкретной интерпретацией действий над кодами, связанной с арифметическими операциями в ассоциированном конечном кольце.

Лемма 4.2. Пусть $<E>^* = (0, 0,\ldots, 0, 1)$, $T = 2B$ есть период последовательности $<\Im^n E>^*$. Тогда для колец $\mathbf{K} = \mathbf{S}/_{\mathbf{p}}$, $\mathbf{S}/_{\mathbf{q}}$, $\mathbf{S}/_{\mathbf{r}}$ при $m \neq k \pmod{2B}$ справедливо соотношение (19). При $m \equiv k \pmod{2B}$ значение суммы (19) равно $2B \pmod{\mathbf{p}}$, $\pmod{\mathbf{q}}$, $\pmod{\mathbf{r}}$, соответственно.

Доказательство. Если рассматривать соотношение (17) как преобразование, индуцированное умножениями на элементы $\left(\sqrt[3]{2}\right)$, $\gamma\left(\sqrt[3]{2}\right)$ и $\bar{\gamma}\left(\sqrt[3]{2}\right)$ соответственно, то единственной причиной нарушения равенства (19) может служить, например, для кольца $\mathbf{S}/_{\mathbf{p}}$ необратимость элементов $\left(\sqrt[3]{2}\right)^{m-k} - 1 = \left(\sqrt[3]{2}\right)^{\tau} - 1$ при суммировании членов геометрической прогрессии. Этого не происходит, если $\mathrm{Norm}\gamma_\gamma\left(\left(\sqrt[3]{2}\right)^{\tau} - 1\right)$ есть число, взаимно простое с f.

Но при $\tau \neq 0 \pmod 3$ имеем

$$\mathrm{Norm}\gamma_\gamma \times$$

$$\times\left(\left(\sqrt[3]{2}\right)^\tau - 1\right) = \left(\left(\sqrt[3]{2}\right)^\tau - 1\right)\left(\gamma\left(\sqrt[3]{2}\right)^\tau - 1\right)\left(\bar{\gamma}\left(\sqrt[3]{2}\right)^\tau - 1\right) = 2^\tau - 1.$$

При $\tau \equiv 0 \pmod 3$ имеем

$$\mathrm{Norm}\gamma_\gamma\left(\left(\sqrt[3]{2}\right)^\tau - 1\right) = \left(2^{\tau/3} - 1\right)^3,$$

и существование нетривиального общего делителя чисел $\mathrm{Norm}\gamma_\gamma\left(\left(\gamma^u \sqrt[3]{2}\right)^\tau - 1\right)$ невозможно при u =0, 1, 2 и $\tau > 3$. При τ = 1, 2, 3 элементы $\left(\left(\gamma^u \sqrt[3]{2}\right)^\tau - 1\right)$ являются единицами кольца **S** и, следовательно, обратимы в соответствующих фактор-кольцах**.**

Лемма 4.2 позволяет рассматривать "правое" шифт-преобразование как обратное по отношению к "левому" шифт преобразованию (18) и наоборот.

Вычисление свертки

Рассмотренные выше шифт-преобразования позволяют вычислять циклическую свертку целочисленных *2B*-периодических последовательностей с помощью *(B+1)* –битовых процессоров по обычной спектральной схеме (см., например, [16]). Опуская детали описания такой схемы, сформулируем окончательный результат.

Теорема. Если для числа Ферма (8) выполняются условия (a)-(c),то для вычисления циклической свертки длины $N = 2(3t + 1)$ достаточно выполнения:

1. девяти (шести левых и трех обратных) шифт-преобразований;

2. вычисления произведений компонентов спектров шифт-преобразований;

3. реконструкции значений свертки по китайской теореме об остатках в форме (12).

Если число Ферма имеет вид

$$f = 2^B + 1, \quad B = 2^r = 3t - 1$$

и обладает свойствами:

(d) при всех $1 < s < 3t$ -1 числа f и 2^s -1 взаимно просты;

(e) элемент $2(3t$ -1) обратим в фактор-кольце $\mathbf{Z}/(f)$;

(f) число f не делится на 3, то есть $f \neq 0 \pmod 3$,

то достаточно рассмотреть разложение числа f на множители в кольце S целых элементов поля разложения полинома $\psi(z) = 2z^3 + 1$ над Q.

В S для числа f наряду с представлением в виде произведения целых рациональных чисел возможно представление в форме, аналогичной (9):

$$f = \left(2^t \sqrt[3]{1/2} + 1\right)\left(2^t \gamma \sqrt[3]{1/2} + 1\right)\left(2^t \bar{\gamma} \sqrt[3]{1/2} + 1\right),$$

где γ - примитивный корень третьей степени из единицы. Как и в лемме 3.1, доказывается взаимная простота элементов

$$\left(2^t \sqrt[3]{1/2} + 1\right), \quad \left(2^t \gamma \sqrt[3]{1/2} + 1\right), \quad \left(2^t \bar{\gamma} \sqrt[3]{1/2} + 1\right)$$

Доказательства аналогов соответствующих лемм и теоремы также существенно не отличаются от приведенных выше.

Непосредственная численная проверка показывает, что числа Ферма f_5 , f_6 , f_7 удовлетворяют условиям (a)-(c) или (d)-(f), что позволяет вычислять свертки длин 64, 128, 256 с помощью описанного метода.

Заключение

Возможности рассмотренного метода, по мнению автора, не ограничиваются задачей «безошибочного» вычисления свертки. Представляется перспективным его использование, например, при быстром параллельном возведении в степень в конечных полях (массовая криптографическая задача), при сжатии информации и т.п.

В этой связи основную техническую трудность при обобщении на случай иррациональностей высших порядков представляет отыскание *явного* вида вложения кольца вычетов (mod f) в прямую сумму колец (лемма 3.2).

Экстраполяция результатов на случай модулей p более общего вида $p = b^k \pm 1$ также не вызывает принципиальных затруднений. В [19] приведены разложения чисел p на простые множители. Практическая целесообразность такого обобщения ограничивается ис-

ключительно возможностями вычислительных средств, ориентированных на недвоичное представление информации [10].

СПИСОК ЛИТЕРАТУРЫ

1. *Фараджиев Р.Г.* Аналитические способы вычисления процессов в линейных последовательных машинах // Известия АН СССР. Техническая кибернетика. 1965. N 5.
2. *Фараджиев Р.Г., Ципкин Я.З.* Преобразование Лапласа-Галуа в теории последовательных машин // Доклады Академии наук СССР. 1966. Т.166. N 36.
3. *Schoenhage A., Strassen V.* Schnelle Multiplikation grosser Zahlen // Computing. B.7. 1966. N.3/4.
4. *Rader C.M.* Discrete convolution via Mersenne transorm // IEEE Trans. Comp. C-21. 1972.
5. *Rader C.M.* On the application of the number theoretic methods of high-speed convolution to two-dimensional filtering // IEEE Trans. on Circuits and Systems.1975. V.22.
6. *Alfredson L.-I.* A fast Fermat number transform for long sequences // Proc. EUSIPCO-94, Edinburg, Scotland. 1994. V.111.
7. *Alfredson L.-I.* VLSI architectures and arithmetic operations with application to the Fermat number transform. Link»oping Studies in Sci. and Technology, Dissertation. 1996. N.425.
8. *Boussakta S., Holt A.G.J.* Calculation of the discrete Hartley transform via Fermat number transform using VLSI chip // IEE Proc. 1988. V.135. N 3.
9. *Towers P.J., Pajayakrit A., Holt A.G.J.* Cascadable NMOS VLSI circuit for implementing a fast convolver using the Fermat number transform // IEE Proc. 1987. V.135. N 2.
10. *Вариченко Л. В., Лабунец В. Г., Раков М. А.* Абстрактные алгебраические системы и цифровая обработка сигналов. Киев: Наукова думка, 1986.
11. *Дэвенпорт Дж., Сирэ И., Турнье Э.* Компьютерная алгебра. М.: Мир, 1991.
12. *Торгашев В.А.* Система остаточных классов и надежность ЦВМ. М: Сов. радио,1973.
13. *Chernov V.M.,Pershina M.V.* «Error-free» calculation of the convolution using generalized Mersenne and Fermat transforms over algebraic fiels // Proc. CAIP'97. Springer. LNCS. 1296.
14. *Ленг С.* Алгебра. М.: Мир, 1965.
15. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. М.: Мир, 1987
16. *Нуссбаумер Г.* Быстрое преобразование Фурье и алгоритмы вычисления сверток. М.: Радио и связь, 1985.
17. *Кнут Д.* Искусство программирования для ЭВМ. Т. 2. М.: Мир, 1977
18. *Стахов А.П.* Коды золотой пропорции. М.: Радио и связь, 1984.
19. *Brillart J., Lehmer D.H., Selfridge J.L., Tuckerman B., Wagstaff S.S.* Factorization of b^k+1, b=2,3,5,6,7,10,11, 12 up high powers // Contemp.Math. AMS. 1988. V.22.

THE PARALLEL ALGORITHMS OF FOURIER-GALOIS TRANSFORMS SYNTHESIS IN DIRECT SUMS OF FINITE RINGS

© 2000 V.M. Chernov

Image Processing System Institute of Russian Academy of Sciences, Samara

The method of fast algorithms of discrete transforms synthesis is considered. The algorithms synthesized with this method are the algorithms of «error-free» calculations of integer-valued discrete convolutions. The approach proposed in the paper is based on the following fact. The factorization of the elements in algebraic rings is can be performed in a number of ways. The choice of factorization is determined by the way in which the modular calculations are organized.