

ОБРАБОТКА ИЗОБРАЖЕНИЙ

БЫСТРОЕ ВЫЧИСЛЕНИЕ ДИСКРЕТНОЙ СВЕРТКИ В РЕДУЦИРОВАННЫХ СИСТЕМАХ СЧИСЛЕНИЯ ДЛЯ КОМПЛЕКСНЫХ ПОЛЕЙ МЕРСЕННА

В.М. Чернов, О.В. Бесполитов*

Институт систем обработки изображений РАН
Самарский государственный аэрокосмический университет

*Самарский государственный университет

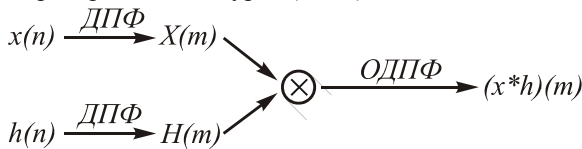
В работе рассматривается задача быстрого безошибочного вычисления целочисленной свертки с помощью теоретико-числовых преобразований в комплексных полях Мерсенна. Снижение вычислительной сложности достигается за счет замены умножений сдвигами массива «цифр» при представлении элементов поля Мерсенна в (редуцированной) системе счисления «с комплексным основанием».

1. Постановка задачи

Вычисление свертки двух N -периодических последовательностей

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

является массовой задачей цифровой обработки сигналов. В частности, метод Шенхаге-Штраассена сводит умножение больших целых чисел именно к вычислению свертки (1) последовательностей, ассоциированных с массивами цифр их представления в выбранной позиционной системе счисления. Традиционное вычисление свертки с помощью дискретного преобразования Фурье (ДПФ) по схеме:



для больших длин сворачиваемых последовательностей может приводить к вычислительной погрешности, связанной с конечноразрядным машинным представлением иррациональных значений базисных функций ДПФ, иногда весьма значительной.

Для ряда задач цифровой обработки сигналов (задач криптографии, в частности) принципиально не допускается «приближенный» ответ. Либо точный, либо – не ответ. Паллиативным решением в этом случае является использование вместо дискретного преобразования Фурье его «модулярных аналогов» – теоретико-числовых преобразований (ТЧП, преобразований Фурье-Галуа):

$$\begin{aligned} \mathfrak{F}(m) &= \sum_{n=0}^{N-1} x(n) \omega^{mn} \pmod{p}, \\ \omega^N &\equiv 1 \pmod{p}. \end{aligned} \quad (2)$$

Теорема о свертке остается справедливой и в этом случае, но для свертки (1), понимаемой не в целочисленной арифметике кольца \mathbf{Z} , а в арифметике конечного поля $(\text{mod } p)$, существенно отли-

чающейся от арифметики кольца \mathbf{Z} . Однако если взять простое число p достаточно большим, а именно:

$$p > \max_{0 \leq n < N} \{x(n)\} \max_{0 \leq n < N} \{h(n)\} N, \quad (3)$$

и считать, что выполняются неравенства

$$0 < x(n), h(n) \in \mathbf{Z},$$

то наименьший неотрицательный вычет значения целочисленной свертки, вычисляемой непосредственно по формуле (1), равен значению этой свертки.

При вычислении свертки (1) с помощью теоретико-числовых преобразований (ТЧП) результаты промежуточных вычислений могут превзойти число p , и полученные значения компонент свертки оказываются «вычисленными с ошибкой», с точностью до слагаемого, делящегося на число p . Выбор числа p с условием (3) в сочетании с (грубой) априорной информацией о диапазоне изменения значений сворачиваемых функций позволяет утверждать, что найденные значения свертки являются точными (следующее целое число, отличающееся от найденного слагаемым, делящимся на p , «слишком велико»).

Отметим, что спектральные методы вычисления (1) с помощью ТЧП содержат ряд вполне объективных трудностей, связанных с арифметическими особенностями конечных полей:

- арифметические операции $(\text{mod } p)$ не являются «элементарными компьютерными операциями», а простые числа p с «дружественными» для машинной реализации свойствами модулярных операций встречаются в натуральном ряду достаточно редко;
- в отличие от поля комплексных чисел, в конечном поле $\mathbf{GF}(p)$ существуют корни не любой степени N единицы, а только удовлетворяющие условию делимости $N|(p-1)$.

К сожалению, эти особенности отчасти конфликтуют между собой: «хорошие» для машинной реализации операций простые числа имеют «плохие» делители числа $(p-1)$, что несколько осложняет

алгоритмическую поддержку вычислений ТЧП, и наоборот. Поэтому основной задачей статьи является разработка неких компромиссных решений, базирующихся на использовании представления элементов конечных полей в специальных системах счисления.

2. Арифметика в полях Мерсенна

Простым числом Мерсенна называется простое число вида $p = 2^q - 1$. Из вида числа Мерсенна сразу следует необходимое (но не достаточное) ограничение на число q , которое также должно быть простым. Числа Мерсенна встречаются в натуральном ряду достаточно редко. К настоящему времени известно только 39 чисел Мерсенна для

$$q = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127,$$

$$521, 607, \dots, 13466917.$$

Тем не менее, вычислительная привлекательность чисел Мерсенна заключается в том, что арифметические операции в полях классов вычетов по модулю таких чисел реализуются достаточно просто.

Сформулируем основные правила вычислений в поле $\mathbf{M} \cong \mathbf{Z}/p\mathbf{Z}$, $p = 2^q - 1$ (см., например, [1]):

- любой элемент поля \mathbf{M} представляется в форме

$$x = x_0 2^0 + x_1 2^1 + \dots + x_{q-1} 2^{q-1}, \quad x_j \in \{0, 1\}; \quad (4)$$

- это представление однозначно для всех $0 \neq x \in \mathbf{M}$; нулевой элемент представим двумя способами в форме (4):

$$\begin{aligned} 0 \cdot 2^0 + \dots + 0 \cdot 2^{q-1} &\equiv 1 \cdot 2^0 + \dots + 1 \cdot 2^{q-1} \equiv \\ &\equiv 2^q - 1 \equiv 0 \pmod{p}; \end{aligned}$$

- так как $2^q \equiv 1 \pmod{p}$, то в случае возникновения «бита переполнения» $1 \cdot 2^q$ при вычислениях эта единица «самого старшего разряда» переносится в «самый младший разряд» и суммируется с полученным числом;
- умножение элемента $x \in \mathbf{M}$ на элемент $2 \in \mathbf{M}$ равносильно циклическому сдвигу «цифр» x_j в представлении (4):

$$2x = x_{q-1} 2^0 + x_0 2^1 + \dots + x_{q-2} 2^{q-1};$$

- умножение элементов поля \mathbf{M} «столбиком» сводится к циклическим перестановкам цифр и сложениям;
- мультипликативный порядок элемента $2 \in \mathbf{M}$ равен q : $\text{Ord}(2) = q$ (следовательно, при $\omega = 2 \in \mathbf{M}$ возможна реализация ТЧП (2) длины $N = q$ без умножений);
- мультипликативный порядок элемента $(-2) \in \mathbf{M}$ равен $2q$: $\text{Ord}(-2) = 2q$ (следовательно, при $\omega = (-2) \in \mathbf{M}$ возможна реализация ТЧП (2) длины $N = 2q$ без умножений);

- максимальная степень двойки, делящая число $(p-1)$, равна единице.

Следует заметить, что последнее свойство чисел Мерсенна несколько осложняет задачу эффективного вычисления ТЧП Мерсенна, так как требование делимости $N \mid (p-1)$ приводит к необходимости синтеза быстрых алгоритмов таких преобразований для весьма «экзотических» длин N .

Например,

$$(2^{31} - 1) - 1 = 2 \cdot (2^{30} - 1) = 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$$

и так далее.

Паллиативным способом преодоления указанной трудности является рассмотрение ТЧП в комплексном поле Мерсенна

$$\mathbf{M}(i) = \{z : a + bi; a, b \in \mathbf{M}, i^2 \equiv -1 \pmod{p}\}. \quad (5)$$

В этом случае условие делимости имеет вид $N \mid (p^2 - 1)$ в силу равенства

$$(p^2 - 1) = (p-1)(p+1) = 2^{q+1} (2^{q-1} - 1).$$

Следовательно, в поле $\mathbf{M}(i)$ существуют корни степени

$$N = 2^t, \quad (t = 1, 2, \dots, q+1).$$

Следует отметить, что арифметические действия в поле $\mathbf{M}(i)$ совершено аналогичны операциям в комплексном поле \mathbf{C} и отличаются лишь необходимостью вычисления остатков по $(\text{mod } p)$. В работе мы рассматриваем специфические системы счисления в поле $\mathbf{M}(i)$, позволяющие еще более упростить некоторые операции над элементами этого поля.

3. Редуцированные системы счисления в комплексном поле Мерсенна

В монографии [2] рассмотрена система счисления в комплексном поле \mathbf{C} с основанием, равным $2i$, названная, по аналогии с «четверичной» системой счисления, «мнимо-четверичной» (негачетверичной) ввиду того, что каждое комплексное число может быть представлено в этой системе при помощи цифр 0, 1, 2 и 3, причем тех же цифр, взятых со знаком минус, не требуется.

Аналогичные системы счисления с «нетрадиционными» основаниями могут быть рассмотрены и для алгебраических расширений конечных полей. Мы будем называть их «редуцированными системами счисления».

Пусть $\mathbf{M} \cong \mathbf{Z}/p\mathbf{Z}$, и $p = 2^q - 1$ является простым числом Мерсенна. Рассмотрим «модулярный» аналог этой системы счисления для «комплексного поля Мерсенна» (5).

Лемма 1. Любой элемент $z \in \mathbf{M}(i)$ может быть представлен в форме

$$z = a_{-1}(2i)^{-1} + a_0(2i)^0 + a_1(2i)^1 + \dots + a_v(2i)^v, \quad a_j = 0, 1, 2, 3, \quad (6)$$

где $v = v(q) \leq q + 1$.

Доказательство. Положим

$$z = x - (2i)^{-1}(2y') = x - (2i)^{-1}y; \quad x, y \in \mathbf{M}, \quad (7)$$

где

$$\begin{aligned} x &\equiv x_0(-4)^0 + x_2(-4)^1 + \dots + x_{2t}(-4)^t \pmod{p}, \\ y &\equiv y_0(-4)^0 + y_2(-4)^1 + \dots + y_{2t}(-4)^t \pmod{p}, \quad (8) \\ x_j, y_j &\in \{0, 1, 2, 3\}. \end{aligned}$$

Тогда доказательство леммы сводится к доказательствам:

(а) принципиальной возможности представления элементов поля \mathbf{M} в форме (8);

(б) определению минимального натурального $t = t(p)$, при котором возможно такое представление.

Для доказательства утверждений (а)-(б) достаточно заметить, что представление произвольного элемента поля \mathbf{M} в четверичной системе счисления возможно и требует не более $t = \frac{(q+1)}{2}$ слагаемых.

Далее, так как

$$\begin{aligned} x &\equiv x_0(-4)^0 + x_2(-4)^1 + \dots + x_{2t}(-4)^t \pmod{p} \equiv \\ &\equiv (x_0(4)^0 + x_4(4)^2 + \dots) - \\ &- 4(x_2(4)^0 + x_6(4)^2 + \dots) \pmod{p} \equiv \\ &\equiv X^{(+)} - 4X^{(-)} \pmod{p}, \quad X^{(+)}, X^{(-)} \in \mathbf{M}, \end{aligned}$$

то и для элемента $X^{(+)} - 4X^{(-)} \in \mathbf{M}$ также требуется не более $t = \frac{(q+1)}{2}$ слагаемых.

Находя для элементов $x, y \in \mathbf{M}$ их представление в «негачетверичной» системе счисления (системе счисления с основанием, равным (-4)) и полагая далее в соответствии с равенством (7)

$$a_{-1} = y_0, \quad a_0 = x_0, \quad a_1 = y_1, \quad a_2 = x_1 \dots,$$

получаем утверждение Леммы 1.

Лемма 2. Мультипликативный порядок элемента $2i$ в поле $\mathbf{M}(i)$ равен $\text{Ord}(2i) = 4q$.

Доказательство. Вычисляя последовательно, получаем:

$$(2i)^2 = -4, \quad (2i)^4 = 16.$$

Далее, в силу того, что н.о.д. $(16, 2^q - 1) = 1$, мультипликативный порядок элемента $16 = 2^4$ равен мультипликативному порядку элемента 2, и, следовательно, для элемента $2i$ в поле $\mathbf{M}(i)$ справедливо соотношение:

$$\text{Ord}(2i) = 4\text{Ord}(16) = 4\text{Ord}(2) = 4q.$$

Таким образом, для $\omega = 2i$ возможна реализация ТЧП длины $N = 4q$ без умножений в поле $\mathbf{M}(i)$.

Как и в комплексном случае, при сложении и умножении элементов поля $\mathbf{M}(i)$ в редуцированной мнимо-четверичной системе счисления в промежуточных результатах могут возникнуть «цифры», не являющиеся элементами множества $\{0, 1, 2, 3\}$. Другими словами, необходимо сформулировать «правила переноса» в старшие разряды для действий, производимых над элементами в форме (6). Сформулируем эти непосредственно проверяемые правила в виде леммы.

Лемма 3. В поле $\mathbf{M}(i)$ справедливы равенства:

$$\begin{aligned} 4 &= 1 \cdot (2i)^4 + 3 \cdot (2i)^2 = 1 \cdot (-4)^2 + 3 \cdot (-4)^1, \\ 5 &= 1 \cdot (2i)^4 + 3 \cdot (2i)^2 + 1 \cdot (2i)^0 = \\ &= 1 \cdot (-4)^2 + 3 \cdot (-4)^1 + 1 \cdot (-4)^0, \\ 6 &= 1 \cdot (2i)^4 + 3 \cdot (2i)^2 + 2 \cdot (2i)^0 = \\ &= 1 \cdot (-4)^2 + 3 \cdot (-4)^1 + 2 \cdot (-4)^0, \\ 7 &= 1 \cdot (2i)^4 + 3 \cdot (2i)^2 + 3 \cdot (2i)^0 = \\ &= 1 \cdot (-4)^2 + 3 \cdot (-4)^1 + 3 \cdot (-4)^0, \\ 8 &= 1 \cdot (-4)^2 + 2 \cdot (-4)^1, \\ 9 &= 1 \cdot (-4)^2 + 2 \cdot (-4)^1 + 1 \cdot (-4)^0. \end{aligned}$$

Несмотря на «четверичность» рассмотренной системы счисления, вычисления в ней легко реализуются на обычной «бинарной» вычислительной технике, если рассмотреть для каждого из возможных значений «цифр» $a_j = 0, 1, 2, 3$ их двухбитовое представление.

«Бинарную» редуцированную систему счисления для поля $\mathbf{M}(i)$ можно также получить, используя основание $(i-1)$, предложенное У. Пенни и также рассмотренное для комплексного поля в книге [2].

Лемма 4. Любой элемент $z \in \mathbf{M}(i)$ может быть представлен в форме

$$z = a_0(i-1)^0 + a_1(i-1)^1 + \dots + a_v(i-1)^v, \quad (9)$$

$$a_j = 0, 1,$$

где $v = v(q) \leq 2q$.

Доказательство. Положим $i-1 = \alpha$. Так как $\alpha^4 = -4$, то для элементов $x, y \in \mathbf{M}$: $x + iy = z \in \mathbf{M}(i)$, согласно Лемме 2 справедливо представление в негачетверичной системе счисления

$$\begin{aligned} x &= b_0(-4)^0 + b_1(-4)^1 + \dots + b_\mu(-4)^\mu, \\ y &= c_0(-4)^0 + c_1(-4)^1 + \dots + c_\mu(-4)^\mu, \\ b_j &= 0, 1, 2, 3, \end{aligned}$$

где $\mu = \left\lceil \frac{q}{4} \right\rceil + 1$. В свою очередь, «цифры» b_j, c_j представляются в виде сумм степеней элемента $i-1 = \alpha$:

$$\begin{aligned} 0 &= 0 \cdot \alpha^0 + 0 \cdot \alpha^1 + 0 \cdot \alpha^2 + 0 \cdot \alpha^3, \\ 1 &= 1 \cdot \alpha^0 + 0 \cdot \alpha^1 + 0 \cdot \alpha^2 + 0 \cdot \alpha^3, \\ 2 &= 0 \cdot \alpha^0 + 0 \cdot \alpha^1 + 1 \cdot \alpha^2 + 1 \cdot \alpha^3, \\ 3 &= 1 \cdot \alpha^0 + 0 \cdot \alpha^1 + 1 \cdot \alpha^2 + 1 \cdot \alpha^3. \end{aligned} \quad (10)$$

Кроме того, справедливо равенство

$$i = 1 \cdot \alpha^0 + 1 \cdot \alpha^1 + 0 \cdot \alpha^2 + 0 \cdot \alpha^3. \quad (11)$$

Преобразуя «цифры» b_j, c_j согласно (10)-(11), получаем утверждение Леммы 4.

Как и для случая мнимо-четверичной системы счисления, при сложении и умножении элементов поля $\mathbf{M}(i)$ в редуцированной системе счисления в промежуточных результатах может возникнуть «цифра», не являющаяся элементом множества $\{0,1\}$. В этом случае «правило переноса» в старшие разряды для действий, производимых над элементами поля $\mathbf{M}(i)$, определяется соотношением

$$2 \cdot (i-1)^0 = (i-1)^3 + (i-1)^2.$$

Лемма 5. Мультипликативный порядок элемента $(i-1) = \omega$ в поле $\mathbf{M}(i)$ равен $\text{Ord}(i-1) = 8q$.

Доказательство. Так как $(i-1)^2 = -2i$, то справедливо равенство

$$\text{Ord}(i-1) = 2\text{Ord}(-2i) = 2 \cdot 4q = 8q.$$

Таким образом, для $\omega = i-1$ возможна реализация теоретико-числовых преобразований длины $N = 8q$ без умножений в поле $\mathbf{M}(i)$.

Заключение

Таким образом, рассмотренный в работе метод вычисления дискретной круговой свертки обладает следующим вычислительным преимуществом:

- за счет представления данных в редуцированных системах счисления в комплексном поле Мерсенна удастся расширить множество тех длин N , для которых алгоритмы вычисления ассоциированного теоретико-числового преобразования свободны от модулярных умножений.

Литература

1. Нуссбаумер П. Быстрое преобразование Фурье и алгоритмы вычисления свертки // М.: Радио и связь, 1985.
2. Кнут Д.Е. Искусство программирования для ЭВМ // М.: Мир, 1977. Т. 2.