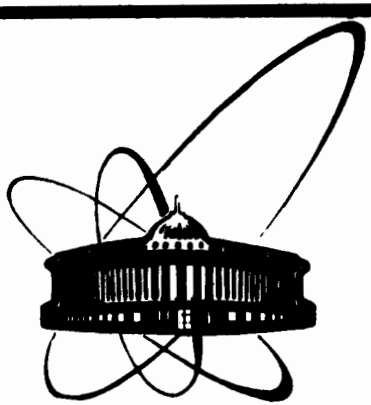

объединенный
институт
ядерных
исследований
дубна

Р11-88-320

В.А.Калинников

ДИНАМИЧЕСКИЙ СПЕКТРАЛЬНЫЙ АНАЛИЗ В АЛГЕБРЕ КОНЕЧНЫХ ПОЛЕЙ

Направлено в журнал "Приборы и техника эксперимента"

1988

ВВЕДЕНИЕ

В основе действия всех цифровых анализаторов спектра лежит разложение исследуемого сигнала в гармонический ряд на базе быстрых алгоритмов дискретного преобразования Фурье (ДПФ)[1-4]. Для данных алгоритмов характерны следующие недостатки: значительные ошибки округления, возникающие из-за операций над комплексными числами; необходимость хранения или генерирования базовых значений экспоненциальных функций; все еще значительный объем умножений[4-6].

В цифровой обработке входные данные могут быть представлены с некоторой конечной точностью и поэтому без потери общности их можно рассматривать как целые числа с вполне определенной верхней границей. При такой интерпретации поле комплексных чисел, непрерывное по своей природе, может быть заменено некоторым конечным полем. В этом конечном поле преобразования, аналогичные ДПФ, могут быть выполнены эффективно и без ошибок округления[7,8]. Такие преобразования были предложены в 1970-1971 годах и получили название теоретико-числовых преобразований (ТЧП). Показано, что ТЧП в алгебре конечных полей идеально подходят для спектральных измерений, так как квантование по амплитуде и дискретизация по времени непосредственно входят в их определение, а эффективность и точность существенно выше, чем у аналогичных результатов, полученных с помощью алгоритмов ДПФ[1,6,7]. Так, например, выполнение цифровой свертки с применением ТЧП на ЭВМ IBM 370/155 дает выигрыш по времени вычислений в 3-5 раз по сравнению с вычислениями на базе алгоритмов ДПФ[5]. Кроме того, выбрав определенным образом параметры конечного поля, можно получить ТЧП, аналогичное ДПФ, в котором выполняются только операции сложения и сдвига и отсутствуют операции умножения. Это существенно упрощает аппаратурную реализацию алгоритмов ДПФ, а экономический эффект может быть значительным[5-8].

Таким образом, применение ТЧП в алгебре конечных полей при вычислении динамических спектральных характеристик позволит повысить быстродействие системы обработки, избежать ошибок округления в ко-

нечных результатах вычислений, сократить объем аппаратурных или программных затрат.

ПРЕОБРАЗОВАНИЕ ФУРЬЕ НАД КОНЕЧНЫМ ПОЛЕМ

Пусть поле Галуа $GF(p^n)$ состоит из p^n элементов, где p - простое, а n -положительное целое число. Пусть N является делителем p^n-1 (возможно $N=p^n-1$), а α -первообразный элемент степени N в поле $GF(p^n)$. Тогда ТЧП, аналогичное ДПФ, можно определить следующим образом [9]:

$$A_i = \sum_{j=0}^{N-1} a_j \alpha^{ij}, \qquad (1)$$

а обратное ТЧП, позволяющее определить a_j через A_i, имеет вид

$$a_j = -N' \sum_{i=0}^{N-1} A_i \alpha^{-ij}, \qquad (2)$$

где N' -целое число, удовлетворяющее условию $N'N = p^n-1$. Полларда показано, что данное ТЧП обладает структурой и свойствами ДПФ в том случае, если в поле $GF(p^n)$ существует инверсный элемент N', а α является корнем N степени из единицы, такой, что для наименьшего целого положительного α справедливо $\alpha^N = 1$ [10,12]. Эти условия выполнимы, если длина последовательности N и модуль M не имеют общих сомножителей, а α выбирается таким образом, чтобы он имел порядок N и был взаимно простым с M [1,12,13]. Хотя на первый взгляд класс возможных ТЧП кажется очень большим, однако, сравнительно мало ТЧП удовлетворяет вышеприведенным условиям [8,14-18]. Так, например, в кольце целых чисел не существует первообразный корень N степени из единицы, то же самое относится и к полю рациональных чисел [5,8].

В работах [5,8-10] показано, что большинство свойств ТЧП в алгебре конечных полей аналогично свойствам ДПФ.

Свойство симметрии. Если сигнал является симметричным, т.е.

$$a(n) = a(-n) = a(N-n),$$

то преобразованная последовательность также симметрична, т.е.

$$A(k) = A(-k) = A(N-k).$$

Если сигнал является антисимметричным, т.е. $a(n) = -a(-n) = -a(N-n)$, то преобразованная последовательность также антисимметрична, т.е.

$$A(k) = -A(-k) = -A(N-k).$$

Свойство периодичности. $A(k)$ может быть периодически продолжена точно так же, как и $a(n)$:

$$a(n+N) = a(n),$$
$$A(k+N) = A(k).$$

Теорема сдвига. Если $ТЧП\{a(n)\} = A(k)$, то

$$ТЧП\{a(n+m)\} = A(k)\cdot\alpha^{-mk}.$$

Свойство свертки. Преобразование циклической свертки двух последовательностей равно произведению их преобразований, т.е. если $y = x * h$, то $ТЧП\{y\} = ТЧП\{x\}\cdot ТЧП\{h\}$.

Теорема Парсеваля. Пусть $X(k) = ТЧП\{x(n)\}$. Тогда

$$N\sum_{n=0}^{N-1} x^2(n) = \sum_{k=0}^{N-1} X(k)\cdot X(-k),$$

$$N\sum_{n=0}^{N-1} x(n)\cdot x(-n) = \sum_{k=0}^{N-1} X^2(k).$$

Свойство растяжения. Свойство растяжения существует, если в этом кольце существует преобразование более длинной последовательности.

Таким образом, теоретико-числовые преобразования в алгебре конечных полей обладают структурой и свойствами ДПФ.

СКОЛЬЗЯЩИЙ СПЕКТРАЛЬНЫЙ АНАЛИЗ В АЛГЕБРЕ КОНЕЧНЫХ ПОЛЕЙ

Рекуррентные методы измерения динамических спектральных характеристик в скользящем режиме наблюдения цифровых сигналов превосходят по эффективности все известные алгоритмы БПФ [19,20]. Кроме того, они обладают наименьшими частотными искажениями и позволяют проводить спектральные измерения для быстроизменяющихся процессов [2]. В этой связи выведем рекуррентные выражения на базе ТЧП для динамического спектрального анализа, которые, в отличие от аналогичных, значительно эффективнее с вычислительной точки зрения и не имеют ошибок округления.

Известны два вида рекуррентных выражений для ДПФ. Первое из них имеет вид [19]

$$F'_{m+1}(k) = \exp(-j\omega)\left[F'_m(k) + \Delta f\right],$$

где $\Delta f = f(N) - f(0)$, $f(N)$ -вновь сформированное дискретное значение сигнала; $f(0)$ -значение сигнала, выходящего из наблюдаемой выборки при дополнении её значением $f(N)$; N -размер окна выборки наблюдения; k, m -соответственно идентификаторы номера коэффициента Фурье и номера дискретного значения сигнала в обрабатываемой выбор-

ке; $\omega = \frac{2\pi K \cdot m}{N}$, $K = \{0, 1, 2, \ldots, \frac{N}{2}-1\}$.

Известна другая формула рекуррентного ДПФ [20]:

$$F_{m+1}(K) = F_m(K) + \Delta f \exp(-j\omega_1),$$

где $\omega_1 = \frac{2\pi K(m+1)}{N}$. Для данных выражений число комплексных умножений при вычислении коэффициентов Фурье не превышает $2N$ и N соответственно.

Выведем аналогичное ТЧП для динамического скользящего спектрального анализа в алгебре конечных полей. Пусть поле $GF^*(p^n)$ порождено первообразным корнем α, т.е. $\{GF^*(p^n)\} \equiv \{\alpha, \alpha^2, \ldots, \alpha^{N-1}, 1\}$ [21]. Тогда для любого цифрового сигнала $f(m)$, область значений которого определена на наборе элементов поля $\{0, 1, \ldots, p^n-1\}$, в тех же самых элементах, справедливо ТЧП вида

$$F(K) = \sum_{m=0}^{N-1} f(m) \cdot \alpha^{Km} \qquad (3)$$

для всех $K, m \equiv \{0, 1, \ldots, p^n-1\}$, а $F(K) \in GF^*(p^n)$. При организации скользящего спектрального измерения необходимо в соответствии с выражением (3) вычислять спектральные характеристики на каждом текущем значении дискретного сигнала $f(m)$, т.е. вычислять последовательность $F_0(K)$, $F_1(K)$, $F_2(K)$ и т.д. [1]. С учетом сказанного обобщенный спектр сигнала $f(m)$ на ℓ-й выборке в точке α можно определить как

$$F_\ell(\alpha) = f(\ell) + f(\ell-1)\alpha + f(\ell-\alpha)\alpha^2 + \ldots + f(\ell-N)\alpha^{N-1},$$

где N – число отсчетов временного окна, по которым находится оценка спектра. Следующее текущее спектральное измерение обеспечивается за счет смещения временного окна на один отсчет и повторения измерения, т.е.

$$F_{\ell+1}(\alpha) = f(\ell+1) + f(\ell)\alpha + \ldots + f(\ell-N+1)\alpha^{N-1}.$$

Проанализировав выражения для двух последовательных спектральных измерений $F_\ell(\alpha)$ и $F_{\ell+1}(\alpha)$, можно получить следующую рекуррентную формулу:

$$F_{\ell+1}(\alpha) = F_\ell(\alpha) + [f(\ell+1) - f(\ell+1-N)]\alpha^{-1}. \qquad (4)$$

Для произвольной точки $K \in GF(p^n)$ рекуррентное выражение (4) принимает следующий вид:

$$F_{\ell+1}(K) = F_\ell(K) + [f(\ell+1) - f(\ell+1-N)]\alpha^{-K(\ell+1)},$$

где $\alpha^{-K(\ell+1)}$ – сдвиг временного окна для последовательности $f(m)$ в начало отсчета. Обозначив разность значений дискретного сигнала на границах временного окна как Δf, получаем формулу рекуррентного теоретико-числового преобразования (РТЧП) для скользящего спектрального анализа в алгебре конечных полей

$$F_{\ell+1}(K) = F_\ell(K) + \Delta f \cdot \alpha^{-K(\ell+1)}.$$

Отрицательный знак в показателе степени α означает, что члены периодической степенной последовательности имеют обратные им числа.

Поскольку вычисления в РТЧП выполняются в модулярной арифметике, следовательно, данное преобразование не имеет ошибок округления, а единственным источником погрешностей будет преобразование "аналог-цифра". Кроме того, арифметические операции в алгебре конечных полей могут быть выполнены значительно эффективнее, чем аналогичные операции в поле комплексных чисел. Все это позволяет утверждать, что организация измерений динамических спектральных характеристик на базе РТЧП наиболее привлекательна с вычислительной точки зрения, а достигаемый при этом выигрыш в объеме аппаратурных затрат и быстродействии может быть существенным, по сравнению с аналогичными результатами измерений на базе рекуррентных алгоритмов ДПФ.

Основным недостатком ТЧП является зависимость между длиной последовательности N и требуемой длиной кодового слова B. Это может привести к тому, что для больших N длина кодового слова может быть больше, чем это возможно или практически реализуемо [5,8].

В этой связи Рейдером было предложено отображать длинную одномерную последовательность в многомерный массив и вычислять многомерное ТЧП от сформированного массива [8]. Число вычислений при этом увеличивается, но требуемая длина кодового слова существенно уменьшается. Так, например, для двумерного ТЧП разрядность кодового слова уменьшается пропорционально $\sqrt{N}$. Этот метод может оказаться очень эффективным, поскольку для вычисления многомерного ТЧП требуется только многократно произвести вычисление одномерных ТЧП от более коротких последовательностей.

Выведем рекуррентное ТЧП для многомерного цифрового сигнала. В работе [8] показано, что если длина последовательности N разбивается на произведение μ взаимно простых множителей, т.е.

$$N = \prod_{i=1}^{\mu} n_i, \quad (n_i, n_j) = 1, \text{ при } i \neq j,$$

то одномерная последовательность может быть преобразована в μ-мерный массив $f(m_1, \ldots, m_\mu)$ на базе китайской теоремы об остатках. Этот алгоритм основан на модулярном представлении входного индекса m, где каждая i-я цифра связана с представляемым числом через вычет по модулю n_i, т.е.

$$\{m\} \equiv \{\langle m \rangle_{n_1}, \langle m \rangle_{n_2}, \ldots, \langle m \rangle_{n_\mu}\} \equiv \{m_1, \ldots, m_\mu\}.$$

Обратный переход от μ-мерной последовательности к одномерной для выходного индекса записывается в виде

$$m = \left\langle \sum_{i=1}^{\mu} m_i N_i M_i \right\rangle_N,$$

где $M_i = \frac{N}{n_i}$, а $\langle M_i N_i \rangle_{n_i} = 1$.

Например, при использовании приведенного алгоритма отображение двумерного ДПФ записывается в виде

$$F(k_1,k_2) = \sum_{m_1=0}^{n_1-1} \sum_{m_2=0}^{n_2-1} f(m_1,m_2)\, W_1^{m_1 k_1} W_2^{m_2 k_2},$$

где $W_1 = \exp(-j\,2\pi/n_1)$ и $W_2 = \exp(-j\,2\pi/n_2)$.

Двумерное преобразование реализуется как последовательное вычисление n_1 ДПФ длины n_2

$$y(m_1,k_2) = \sum_{m_2=0}^{n_2-1} f(m_1,m_2)\, W^{m_2 k_2}$$

и n_2 ДПФ длины n_1

$$F(k_1,k_2) = \sum_{m_1=0}^{n_1-1} y(m_1,k_2)\, W^{m_1 k_1}.$$

Поскольку основная идея такого преобразования заключается в представлении входного индекса m в классе вычетов по модулю n_i, следовательно, этот алгоритм может быть применим и для ТЧП в конечном поле. Пусть $d_1, d_2, \ldots, d_\mu$ делят p^n-1, где p -простое, а n - целое положительное число. Тогда классы вычетов по модулю некоторого простого числа $q = p^n-1$ образуют поле Галуа $GF(p^n)$, состоящее из p^n элементов [9,11]. Если цифровая последовательность $f(m)$ определена на наборе элементов поля $GF(p^n)$, в тех же самых элементах, то эту последовательность можно преобразовать в μ-мерный массив на базе китайского соответствия, а ТЧП от этого массива будет иметь вид

$$F(k_1,k_2,\ldots,k_\mu) = \sum_{m_1=0}^{d_1-1} \cdots \sum_{m_\mu=0}^{d_\mu-1} f(m_1,\ldots,m_\mu)\, \alpha^{m_1 k_1 + \ldots + m_\mu k_\mu}.$$

Данное выражение справедливо и для μ-мерного цифрового сигнала $f(m_1,\ldots,m_\mu)$, заданного на наборе элементов поля $GF(p^n)$, поскольку всегда можно построить расширенное поле $GF(p^n)^\mu$, которое изоморфно полю $GF(p^n)$, такое, что $d_1, d_2, \ldots, d_\mu$ делят $(p^n)^\mu - 1$ [21]. Таким образом, μ-мерное ТЧП сводится к μ-одномерным ТЧП по каждому i-му измерению.

По аналогии с одномерным преобразованием выводим рекуррентное ТЧП для μ-мерного цифрового сигнала:

$$F_{\ell_1+1,\ell_2+1,\ldots\ell_\mu+1}(k_1,\ldots,k_\mu) = F_{\ell_1,\ell_2,\ldots\ell_\mu}(k_1,\ldots,k_\mu) +$$

$$+ [f(\ell_1+1) - f(\ell_1+1-d_1)]\alpha^{-k_1(\ell_1+1)} + \ldots + [f(\ell_\mu+1) -$$

$$- f(\ell_\mu+1-d_\mu)]\cdot\alpha^{-k_\mu(\ell_\mu+1)} =$$

$$= F_{\ell_1,\ell_2,\ldots\ell_\mu}(k_1,\ldots,k_\mu) + \sum_{i=1}^{\mu} [f(\ell_i+1) - f(\ell_i+1-d_i)]\alpha^{-k_i(\ell_i+1)}.$$

Таким образом, путем выбора достаточно большого числа взаимно простых множителей можно вычислять РТЧП на какой угодно длине выборки N. Кроме того, метод вычисления РТЧП на многомерном представлении более эффективен по сравнению с прямым методом, т.к. число умножений при этом значительно уменьшается.

АППАРАТУРНАЯ РЕАЛИЗАЦИЯ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ ДЛЯ ЦИФРОВОГО СПЕКТРАЛЬНОГО АНАЛИЗА С ИСПОЛЬЗОВАНИЕМ АЛГЕБРЫ КОНЕЧНЫХ ПОЛЕЙ

В связи с тем, что эффективность скользящего спектрального измерения зависит от конкретной аппаратурной реализации выбранного алгоритма преобразования, рассмотрим, как выполняются арифметические операции в конечном поле $GF(p^n)$. Представим элементы поля полиномами $n-1$ степени с коэффициентами из поля $GF(p)$. Например, элементы поля $GF(2^3)$ образуют множество $\{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}$, где X - неприводимый полином, порождающий данное поле. Пусть полином имеет вид x^2+1 [19]. Найдем сумму и произведение для элементов поля $GF(2^3)$. Если $a+bx$, $c+dx \in GF(2^3)$, то $(a+bx)+(c+dx) = (a+c)+(b+d)x$; $(a+bx)\cdot(c+dx) = (ac+bd)+(ad+bc)x$. Эти формулы соответствуют правилам умножения и сложения в алгебре комплексных чисел, но не удовлетворяют условию замкнутости для поля Галуа $GF(p^n)$. Поэтому операции сложения и умножения в поле $GF(p^n)$ корректируют по модулю данного поля. Для сложения корректировка заключается в приведении каждого коэффициента к множеству значений $\{0,1,\ldots,p^n-1\}$. Следовательно, для того чтобы сложить два элемента поля $GF(p^n)$, необходимо сложить элементы поля как полиномы и заменить каждый коэффициент в полином-сумме его вычетом по модулю поля $GF(p^n)$. Для умножения корректировка более сложна, т.к. необходимо корректировать не только значения коэффициентов, но и показатели степеней. При аппаратурной реализации операции умножения элементы поля удобнее представлять в виде степеней порождающего много-

члена. Например, для поля $GF(2^3)$, порожденного полиномом x^3+x+1, справедливо:

степенное	многочленное	двоичное
I	I	001
α	α	010
α^2	α^2	100
α^3	$\alpha+1$	011
α^4	$\alpha^2+\alpha$	110
α^5	$\alpha^2+\alpha+1$	111
α^6	α^2+1	101
α^7	1	001

В случае степенного представления произведение для двух любых элементов поля α^i, α^j определяется следующим образом:

$$\alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^{J_M(i+j)},$$

где $J_M(i+j)$ – остаток от деления $i+j$ на M. Таким образом, операция умножения сводится к операции сложения показателей степеней с последующей корректировкой по модулю поля. Такая процедура легко может быть выполнена методом поиска по таблице значений, записанной в элементах памяти. Для большинства практических приложений арифметические операции легко выполняются, если модулем поля является число 2 или кратное степени 2. Тогда сложение элементов в поле $GF(2^n)$ сводится к операции суммирования по $mod\,2$, т.е. равносильно двоичному сложению без переносов в старшие разряды. На рис. I представлена функциональная схема такого сумматора в поле $GF(2^n)$.

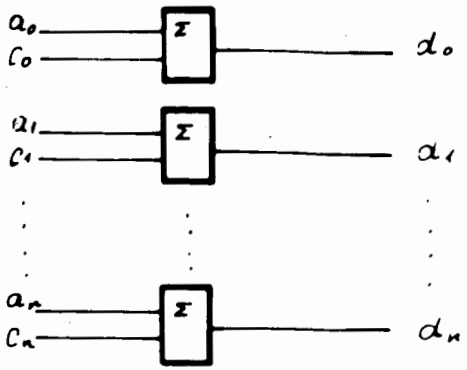

Рис.I. Сумматор в поле $GF(2^n)$. $a_0, a_1, \ldots, b_{n-1}, b_n$ – коэффициенты суммируемых полиномов.

Рассмотрим аппаратурную реализацию операции умножения в поле $GF(2^n)$. Пусть величина $N = 2^n - I$ не слишком велика. Тогда умножение можно заменить операцией сложения степеней элементов поля с последующей корректировкой. Этот прием хорошо известен и реализован в вычислительных машинах, работающих в классах вычетов [6,8]. На рис.2 представлена функциональная схема такого умножителя. Данный подход позволяет получать высокое быстродействие, но требует для реализации

быстродействующих микросхем памяти на n входов, что ограничивает разрядность перемножаемых чисел.

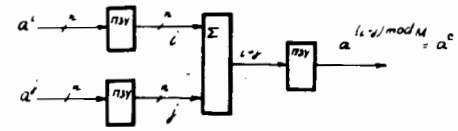

Рис.2. Умножитель в поле $GF(2^n)$.

Другой способ реализации операции умножения в поле $GF(P^n)$ позволяет избежать применения микросхем памяти на n входов, но имеет более низкое быстродействие. Пусть $R_M(X)$ – кольцо полиномов от переменной X над полем $GF(P)$ и пусть $g(x) \in R_M(X)$ – неприводимый полином степени n. Элементы поля $GF(P^n)$ могут быть представлены классами вычетов по $mod\,g(x)$ кольца $R_M(X)$. Пусть в регистре сдвига, состоящего из n ячеек памяти, записано n элементов поля, которые можно рассматривать как коэффициенты многочлена

$$z(x) = z_{n-1} x^{n-1} + z_{n-2} x^{n-2} + \ldots + z_0$$

степени $n-1$ или меньшей. При сдвиге регистра на единицу вправо этот многочлен переходит в многочлен $z'(x) = z(x) \cdot x - z_{n-1} g_n^{-1}(x)$. Последнее слагаемое появляется из-за обратной связи. В работах /II,2I/ показано, что многочлены $z'(x)$ и $z(x) \cdot x$ лежат в одном и том же классе вычетов по $mod\,g(x)$, а поскольку степень многочлена $z'(x)$ меньше чем n, то многочлен $z'(x)$ должен совпадать с единственным многочленом в классе вычетов $\langle z(x) \cdot x \rangle$. Это утверждение можно сформулировать следующим образом: если через S обозначить класс вычетов, содержащий x, то $\langle z(x) \cdot x \rangle = S z(S)$ и $\langle z(x) \rangle = z(S)$. Поэтому сдвиг регистра вправо на единицу соответствует умножению на S. Рассмотрим это на примере. Пусть $g(x) = x^4 + x + 1$, а α – примитивный элемент поля $GF(2^4)$. Соответствующий умножитель показан на рис.3.

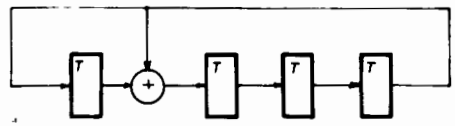

Рис.3. Умножитель в поле $GF(2^4)$. $\oplus$ – сумматор по $mod\,2$. T – триггер.

Если в ячейку младшего разряда поместить единицу, то последовательные сдвиги дадут все степени элемента α, т.е. все элементы по-

ля $GF(2^4)$. Заметим, что единице, сдвигаемой из старшего разряда, соответствует элемент α^4, а наличие обратной связи заменяет его на $\alpha+1$. Сдвиг регистра влево соответствует делению на α.

Данный способ позволяет значительно упростить аппаратурную реализацию операции умножения, но уступает предыдущему способу в быстродействии. В силу обратимости операций в поле $GF(p^n)$, на схемах умножения и сложения можно выполнять операции деления и вычитания. Для этого необходимо один из элементов в операции заменить его инверсным или обратным элементом соответственно /2I/.

Вопросы технической реализации рекуррентных алгоритмов ТЧП приводят к необходимости поиска оптимальных параметров данных преобразований, которые позволяют реализовать эффективные вычислительные структуры. С этой точки зрения следует рассмотреть три основных требования, предъявляемые к ТЧП при аппаратурной реализации /5/.

Во-первых, N должно быть существенно составным, чтобы можно было организовать быстрые алгоритмы типа БПФ.

Во-вторых, так как умножение комплексных чисел при вычислении БПФ требует больших затрат времени, важно, чтобы умножение на степень α было бы достаточно простой операцией. Это возможно, если α занимает мало двоичных разрядов и может быть представлено степенью числа 2. В этом случае умножение сводится к операции сдвига кодового слова.

В-третьих, для облегчения выполнения арифметических операций по модулю M M должно иметь двоичное представление.

Так как аппаратурная реализация ТЧП требует операций сложения и умножения чисел по модулю M, то выбор M в виде 2^B, 2^B-1 или 2^B+1 существенно упрощает положение. Выбор $M=2^B$ не приводит к полезному преобразованию (N равняется единице)/5/. Выбор $M=2^B-1$ приводит к числовому преобразованию Мерсена, где B – простое число. Корень из единицы $\alpha=-2 \bmod M$ имеет порядок $2B$. Тогда длина преобразования не представляется в виде произведения большого числа множителей и, следовательно, не существует алгоритма типа БПФ. Выбор $M=2^B+1$ при $B=2^t$ приводит к ТЧП по модулю F_t (где F_t – означает число Ферма $F_t=2^{2^t}+1$). В этом случае может быть определено преобразование длины $N=2^t+1$ с $\alpha=2 \bmod F_t$, которое может быть разложено на произведение взаимно простых множителей. В работе /8/ показано, что длина преобразования может быть увеличена до $N=2^{2^t}+2$ за счет выбора $\alpha=\sqrt{2}$. Этот случай представляет определенный интерес, но выбор $\alpha=\sqrt{2}$ требует двухразрядного двоичного представления α^i в кольце целых чисел по $mod\ F_t$ /8/.

Арифметические операции по $mod\ F_t$ могут выполнятся B-разрядными двоичными числами. К сожалению не существует регулярного эффективного

метода для выбора оптимального набора параметров M, N и α. На практике прибегают к эмпирическому подбору параметров. Сначала выбирается модуль поля из условия $B_{max} \geq \frac{M}{2}$, затем исследуются возможные значения N и α /5/.

ЗАКЛЮЧЕНИЕ

Алгоритмы обработки в конечных математических структурах, аналогичные БПФ, представляют интересную область исследований. Так как в устройствах, использующих алгоритмы ДПФ, на операцию умножения приходится значительная доля затрат, то возможность удешевления и увеличения быстродействия таких систем открывается в применении алгоритмов теоретико-числовых преобразований.

В данной работе предложен и исследован алгоритм рекуррентного теоретико-числового преобразования, использование которого в системах цифровой обработки позволит значительно повысить быстродействие и точность вычислений и снизит объем аппаратурных или программных затрат.

Поскольку данный алгоритм не имеет ошибок округления, его целесообразно использовать в таких областях, как динамический спектральный анализ, расчет и реализация цифровых фильтров, вычисление корреляционных функций и кросс-спектров и т.д.

ЛИТЕРАТУРА

I. Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. М.: Мир, I978.

2. Гоулд Б., Рейдер Ч. Цифровая обработка сигналов. М.: Советское радио, I973.

3. Рошаль А.С. Быстрое преобразование Фурье для вычислительной техники. – Известия вузов, сер. Радиофизика, №I0, I976, с.I425-I484.

4. Оппенгейм Э. Применение цифровой обработки сигналов. М.: Мир, I980.

5. **Agarwal R.C. Burrus C.S. Number theoretic transforms to implement fast digital convolution. –IEEE Trans. on Acoust., Speach and Signal Processing. ASSP-24, 1976, p.216-225.**

6. **McClenan J.H. Hardware realization of a Fermat number transform. – IEEE, Proc. No.63, 1975, p. 556-560.**

7. **Reed I.S., Truong T.K. The use of finite fields to compute convolutions. –IEEE Trans. on Inform. Theory, IT-21, p.208-225.**

8. Макклеллан Д.Х., Рейдер Ч.М. Применение теории чисел в цифровой

обработке сигналов. М.: Радио и связь, 1983.
9. Pollard J.M. The fast Fourier Transform in Finite Fields.- Mathematic of Comp., 1976, No.25, p.356-374.
10. Reed I.S. Complex integer convolutions over a direct sum of Galois Fields.- IEEE Trans. on Inform. Theory, vol. IT-21, No.1, 1975, p.657-661.

11. Касами Т.,Токура Н., Ивадари Е.,Инагаки Я. Теория кодирования. М.: Мир, 1978.
12. Rader C.M. Discrete convolution via Mersenne transform.- IEEE Trans. on Comput., vol. C-21, 1972, p. 1269-1273.
13. Bergland G.D. A quided of tour of fast Fourier Transform.- IEEE Spectrum, vol. C-6, No.7,1969,p.41-53.
14. Menger K.S. A transform for logic networks.- IEEE Trans. on Comp.,vol. C-25, No.3,1969, p.241-250.
15. Reed I.S.,Benjantthrit B. Galois switching and their aplications. IEEE Trans. on Comp., vol. C-25, No. 1, 1976,p. 78-86.
16. Bartee T.C., Schender D.I. Computation with Finite Field information and control.- IEEE Trans. on Comp. vol.C-28,No.8,1978,p. 7516760.
17. Benjanthrit B., Reed I.S. On the fundamental structure of Galoies switching functions.-IEEE Trans. on Comp.,1978, vol.C-23.No.6, p.78-92.
18. Reed I.S. A decoding procedure for polynomial codes. MIT,1975,p.6.
19. Чайковский В.И.,Коваль В.Ф. и др. Анализатор спектра Фурье. А.с. 560232 (СССР).- Опубликовано в ОИ №20, 1977, с.84.
20 Калинников В.А. Цифровой динамический амплитудно-частотный анализатор спектра. Препринт ОИЯИ Р10-88-275, Дубна, 1988.
21. Питерсон У.,Уэлдон Э. Коды, исправляющие ошибки.М.: Мир, 1976.

Рукопись поступила в издательский отдел
12 апреля 1988 года.

Калинников В.А. P11-88-320
Динамический спектральный анализ в алгебре конечных полей

Описывается новый метод рекуррентного вычисления динамических спектральных характеристик на базе теоретико-числовых преобразований в алгебре конечных полей. Дается оценка его быстродействия и точности. Рассматриваются вопросы выполнения арифметических операций над элементами поля Галуа и их аппаратурная реализация.

Работа выполнена в Общеинститутском научно-методическом отделе ОИЯИ.

Препринт Объединенного института ядерных исследований. Дубна 1988

Перевод А.В.Дмитренко

Kalinnikov V.A. P11-88-320
Dynamic spectral analysis in Finite Field Algebras

A new method of requrent calculation dynamic spectral characteristics on the base of Fast Number-Theoretic Transforms over a Finite Fields is discribed. The estimate of its speed and accuracy is given. The question of execution of arithmetic operations on the Galois Field elements and their hardware implementation are considered.

The investigation has been performed at the Scientifical-Methodical Division, JINR.

Preprint of the Joint Institute for Nuclear Research. Dubna 1988