ОБОБЩЕННОЕ ДИСКРЕТНОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ ДЛЯ КОЛЕЦ НЕПРИВОДИМЫХ ПОЛИНОМОВ

Калмыков И.А., Емарлукова Я.В., Тимошенко Л.И., Гахов В.Р.

Ставропольский военный институт связи Ракетных войск,

Северо-Кавказский государственный технический университет

г. Ставрополь, Россия

kia762@yandex.ru

При решении многих практических задач цифровой обработки сигналов (ЦОС) необходимо осуществлять ортогональные преобразования над входной последовательностью дискретных отсчетов. Такие преобразования, как правило, определены над полем комплексных чисел и называются дискретным преобразованием Фурье (ДПФ), которое определяется выражениями:

$$X(k) = \sum_{n=0}^{N-1} x(n) \cdot W^{kn} \ ; \tag{1}$$

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

где $W = exp\left(- j \cdot \frac{2p}{N} \right)$- поворачивающий коэффициент; $x(n)$- количество отсчетов, $k = 0,...,N-1$, $n = 0,1,...,N-1$.

Известно, что реализация прямого и обратного ДПФ предопределяет значительные погрешности при вычислении значений спектральных коэффициентов в поле комплексных чисел. Это, прежде всего, обусловлено тем, что поворачивающие коэффициенты W^{kn} представляют собой иррациональные числа, а это при значительных значениях N приводит к существенной аддитивной арифметической погрешности. Поэтому для уменьшения среднеквадратической погрешности необходимо определить алгоритм ортогонального преобразования входного вектора $x(n)$, в котором бы не использовались операции поля комплексных чисел.

С этой точки зрения наиболее привлекательными являются преобразования, определенные над расширенным полем Галуа $GF(p^n)$, где p – простое, а n - положительное целое число. Известно [1], что данное поле содержит $p^n - 1$ ненулевых элемента, которые образуют циклическую мультипликативную группу. Следовательно, в этой группе должен существовать хотя бы один элемент d, который являлся бы делителем. Если $p^n - 1$ представляет собой простое число, то значение $d = p^n - 1$.

Пусть b является элементом порядка k в мультипликативной группе ненулевых элементов $GF(p^n)$. Тогда выражение (1) можно преобразовать к виду

$$X(k) = \sum_{n=0}^{d-1} x(n) b^{kn}, \; k = 0,1,...,d-1. \qquad (3)$$

Выражение (3) описывает преобразование входной последовательности отсчетов $x(n)$, являющихся элементами расширенного поля Галуа $GF(p^n)$ в последовательность «частотных» составляющих $X(k)$, определенных над этим же полем.

Преобразование обратное (3), то есть эквивалентное множество уравнений, позволяющих определить входной вектор $x(n)$ через совокупность спектральных составляющих $X(k)$, определяется выражением

$$x(n) = -d^* \sum_{k=0}^{d-1} X(k) b^{-kn}, \; n = 0,1,...,d-1, \qquad (4)$$

где d^* - целое число, удовлетворяющее условию

$$d^* d = p^n - 1. \qquad (5)$$

Анализ выражений (3) и (4) показывает, что полученное преобразование аналогично ДПФ комплексной области и действует в пространстве циклической группы порядка d, определенной полем $GF(p^n)$. Так как b^{kn} и $x(n)$ представляют собой целочисленные элементы расширенного поля Галуа, то при реализации выражений (3) и (4) будут полностью отсутствовать шумы округления.

В подавляющем большинстве приложений задача ЦОС сводится к нахождению значений ортогонального преобразования конечной реализации сигнала для большого числа точек, что предопределяет повышенные требования к разрядности вычислительного устройства.

Рассмотрим возможность выполнения обобщенного ДПФ в расширенных полях Галуа с использованием конечных полиномиальных колец, полученных с помощью неприводимых полиномов.

Пусть имеем конечное кольцо полиномов $P(z)$, с коэффициентами в виде элементов поля $GF(p)$, определяющего точность вычисления ортогональных преобразований сигналов. Положим, что данное кольцо разлагается в виде $P(z) = P_1(z) + P_2(z) + ... + P_k(z)$, где $P_l(z)$ – локальное кольцо полиномов, образованных неприводимым полиномом $p_l(z)$ над полем $GF(p)$; $l=1, \ldots, k$.

Тогда справедлива следующая теорема.

Теорема: Пусть $P(z)$ – конечное кольцо полиномов с коэффициентами поля $GF(p)$ представляет собой прямую сумму локальных колец полиномов

$$P(z) = P_1(z) + P_2(z) + ... + P_m(z). \qquad (6)$$

Тогда в данной системе существует ортогональное преобразование, представляющее собой обобщенное ДПФ, если выполняются следующие условия:

1. $b_i(z)$ - первообразный элемент порядка d для локального кольца $P_l(z)$, где $l=1, \ldots, m$.

2. d имеет мультипликативный обратный элемент d^*.

Доказательство: Ортогональное преобразование является обобщенным ДПФ для кольца вычетов $P(z)$ если существуют преобразования вида

$$X_l^k(z) = \sum_{n=0}^{d-1} x_l^n(z) b_l^{kn}(z), \qquad (7)$$

где $\{ X_l^k(z), x_l^n(z), b_l^{kn}(z) \} \in P_l(z)$, $l=1,2,\ldots,m$; $k=0,1,\ldots d-1$,

над конечным кольцом $P_l(z)$.

Полученная циклическая группа имеет порядок d. Поэтому дискретное преобразование Фурье над $P_l(z)$ можно обобщить над кольцом $P(z)$, если ко-

нечное кольцо $P_l(z)$ содержит корень d-ой степени из единицы и d имеет мультипликативный обратный элемент d^*, такой что справедливо

$$d^* d = p^n - 1. \quad (8)$$

Доказательство закончено.

Основным преимуществом доказанной теоремы является то, что существует возможность организации ортогональных преобразований сигналов на основе обобщенного ДПФ в расширенных полях Галуа при различных значениях разрядности сетки, задаваемой значением конечного кольца $P(z)$. При этом вычисления организуются параллельно, независимо друг от друга, что значительно повышает быстродействие арифметических устройств ЦОС.

Проведенные исследования показали, что применение ортогональных преобразований в $GF(2^5)$ на основе обобщенного ДПФ позволило повысить производительность вычислительного устройства более чем в 1,5 раза. Таким образом, полученные результаты имеют важное практическое значение, так как позволяют поднять аппаратные средства для ЦОС на качественно более высокую ступень.

Литература.

Литература

1. Абстрактные алгебраические системы и цифровая обработка сигналов / Вариченко Л.В., Лабунец В.Г., Раков М.А. – Киев: Наук. думка, 1986.- 248 с.
2. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов/ Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2005. - 276 с.
3. Элементы применения компьютерной математики и нейроинформатики /Н.И. Червяков, И.А. Калмыков И.А., В.А. Галкина, Ю.О. Щелку-

нова, А.А. Шилов; Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 216с.