РЕАЛИЗАЦИЯ ОРТОГОНАЛЬНЫХ ПРЕОБРАЗОВАНИЙ СИГНАЛОВ В РАСШИРЕННЫХ ПОЛЯХ ГАЛУА

Калмыков И.А., Тимошенко Л.И., Лободин М.В., Сагдеев А.К.

Ставропольский военный институт связи Ракетных войск,

г. Ставрополь, Россия

kia762@yandex.ru

При анализе сигналов и цифровых методах их обработки особое внимание привлекают ортогональные преобразования благодаря простоте вычисления координат разлагаемых функций в пространстве. Такие преобразования определены над полем комплексных чисел,

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

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

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. С этой точки зрения наиболее привлекательными являются преобразования, определенные над расширенным полем Галуа $GF(p^n)$. Пусть b является элементом порядка k в мультипликативной группе ненулевых элементов $GF(p^n)$. Тогда выражение (1) имеет вид

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

Преобразование обратное (3), определяется выражением

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

где d^* - целое число, удовлетворяющее условию

$$d^* \cdot d = p^n - 1. \tag{5}$$

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. Поэтому оценка спектральных составляющих с помощью (3) и (4) будет более точной по сравнению с ДПФ.

Пусть дана последовательность $x(n)=\{0,1,2,0,1,0,0\}$. Представим её в двоичном виде $x(n)=\{000,001,010,000,001,000,000\}$. Исходя из условия возможности представления квантованных значений $x(n)$ в виде элементов расширенного поля Галуа b, получаем входной вектор $x(n)=\{0,b^0,b,0,b^0,0,0\}$.

Преобразуем выражение (3) к матричному виду. Тогда значения спектральных составляющих можно представить

$$X(k)=\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & b & b^2 & b^3 & b^4 & b^5 & b^6\\ 1 & b^2 & b^4 & b^6 & b & b^3 & b^5\\ 1 & b^3 & b^6 & b^2 & b^5 & b & b^4\\ 1 & b^4 & b & b^5 & b^2 & b^6 & b^3\\ 1 & b^5 & b^3 & b & b^6 & b^4 & b^2\\ 1 & b^6 & b^5 & b^4 & b^3 & b^2 & b\end{bmatrix}\times\begin{bmatrix}0\\ b^5\\ b\\ 0\\ b^0\\ 0\\ 0\end{bmatrix}=\begin{bmatrix}b\\ b^5\\ b^0\\ b^6\\ b^4\\ b^2\\ b^3\end{bmatrix}. \qquad (6)$$

Следует отметить, что операции сложения при вычислении выходного вектора $X(k)=\begin{bmatrix}b & b^5 & b^0 & b^6 & b^4 & b^2 & b^3\end{bmatrix}^T$ выполнялись по модулю 2, а операции умножения – по модулю порождающего полинома $f(z)=z^3+z+1$.

Для осуществления обратного преобразования необходимо воспользоваться выражением (4), предварительно определив значение обратного элемента d^*. Согласно равенству (5) он равен единице, т.е. $d^*=1$. Тогда выражение (4) в матричной форме примет следующий вид:

$$x(n)=1\cdot\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & b^6 & b^5 & b^4 & b^3 & b^2 & b^1\\ 1 & b^5 & b^3 & b & b^6 & b^4 & b^2\\ 1 & b^4 & b & b^5 & b^2 & b^6 & b^3\\ 1 & b^3 & b^6 & b^2 & b^5 & b & b^4\\ 1 & b^2 & b^4 & b^6 & b & b^3 & b^5\\ 1 & b^1 & b^2 & b^3 & b^4 & b^5 & b^6\end{bmatrix}\times\begin{bmatrix}b\\ b^5\\ b^0\\ b^6\\ b^4\\ b^2\\ b^3\end{bmatrix}=\begin{bmatrix}0\\ b^0\\ b\\ 0\\ b^0\\ 0\\ 0\end{bmatrix}. \qquad (7)$$

Для повышения эффективности реализации задач ЦОС целесообразно обработку одномерных сигналов свести к обработке многомерных сигналов [1,3]. Отправной точкой при решении данной проблемы является изоморфизм, порожденный теоремой теории чисел, называемой китайской теоремой об остатках (КТО). Согласно данной теореме, если $P = p_1 \cdot p_2 \cdot \mathbf{K} \cdot p_n = \prod_{i=1}^{n} p_i$ и p_i - простые числа, то кольцо Z_P класса вычетов по модулю P изоморфно прямой сумме $GF(p_1)+GF(p_2)+\mathbf{K}+GF(p_5)$ конечных полей $GF(p_i)$:

$$Z_p \sim GF(p_1)+GF(p_2)+\mathbf{K}+GF(p_5). \qquad (8)$$

Основным преимуществом $GF(p_1)+GF(p_2)+\mathbf{K}+GF(p_5)$ - арифметики является возможность организации параллельных вычислений и, следовательно, значительное повышение быстродействия арифметических устройств.

Если в качестве оснований новой алгебраической системы выбрать минимальные многочлены $p_i(z)$ поля $GF(p^n)$, то любой полином $A(z)$, удовлетворяющий условию

$$A(z) \in P_{пол},$$

где $P_{пол} = \prod_{i=1}^{n} p_i(z) = z^{p^n-1} - 1,$ (9)

можно представить в виде n-мерного вектора

$$A(z) = \left(a_1(z), a_2(z), ..., a_n(z)\right), \qquad (10)$$

где $a_i(z) = rest\left(A(z) \big/ p_i(z) \right),\ i = 1,2,...,n.$

Так как сравнения по одному и тому же модулю можно почленно складывать, вычитать и умножать [2], то для суммы, разности и произведения

$A(z)$ и $B(z)$, имеющих соответственно модулярные коды $(a_1(z),a_2(z),...,a_n(z))$ и $(b_1(z), b_2(z),..., b_n(z))$ справедливо:

$$|A(z)+B(z)|^+_{p(z)} = \left(|a_1(z)+b_1(z)|^+_{p_1(z)}, |a_2(z)+b_2(z)|^+_{p_2(z)},..., |a_n(z)+b_n(z)|^+_{p_n(z)}\right), \quad (11)$$

$$|A(z)-B(z)|^+_{p(z)} = \left(|a_1(z)-b_1(z)|^+_{p_1(z)}, |a_2(z)-b_2(z)|^+_{p_2(z)},..., |a_n(z)-b_n(z)|^+_{p_n(z)}\right), \quad (12)$$

$$|A(z)\cdot B(z)|^+_{p(z)} = \left(|a_1(z)\cdot b_1(z)|^+_{p_1(z)}, |a_2(z)\cdot b_2(z)|^+_{p_2(z)},..., |a_n(z)\cdot b_n(z)|^+_{p_n(z)}\right). \quad (13)$$

Таким образом, выполнение операций над операндами в $GF(p^n)$ производятся независимо по каждому из модулей $p_i(z)$, что указывает на параллелизм данной алгебраической системы.

Рассмотрим пример. Пусть задано расширенное поле Галуа $GF(2^3)$. Для данного поля определены минимальные многочлены $p_1(z) = z+1$; $p_2(z) = z^3+z^2+1$; $p_3(z) = z^3+z+1$. Найдем сумму и произведение двух полиномов $A(z) = z^4+z^3+z$ и $B(z) = z^2+z+1$. Данные полиномы принадлежит диапазону $P(z)$, который определяется следующим выражением:

$$P(z) = \prod_{i=1}^{3} p_i(z) = (z+1)\cdot(z^3+z^2+1)\cdot(z^3+z+1) = z^7+1.$$

Представим исходные полиномы в виде модулярного кода по основаниям $p_1(z)$, $p_2(z)$, $p_3(z)$. Тогда $A(z) = (1,\ 0,\ z^2+z+1)$, а $B(z) = (1,\ z^2+z+1,\ z^2+z+1)$.

Сумма двух полиномов в $GF(2^3)$ равна

$$C(z) = A(z)+B(z) = (z^4+z^3+z)+(z^2+z+1) = z^4+z^3+z^2+1 = (0,\ z^2+z+1,\ 0).$$

Реализуем данную операцию, используя выражение (11).

$$\begin{array}{l} A(z) = (1,\ 0,\ z^2+z+1) \\ + \\ \underline{B(z) = (1,\ z^2+z+1,\ z^2+z+1)} \\ C(z) = (0,\ z^2+z+1,\ 0) \end{array}$$

Следует отметить, что операции сложения и вычитания в расширенных полях Галуа $GF(p^n)$ выполняются по модулю p, то есть в рассмотренном примере по модулю 2.

Выполним операцию умножения данных полиномов

$$C(z) = \left|A(z) \cdot B(z)\right|^{+}_{p(z)} = (z^4 + z)$$

$$C(z) = \left|A(z) \cdot B(z)\right|^{+}_{p(z)} = (z^4 + z^3 + z) \cdot (z^2 + z + 1) = z^6 + z^2 + z = (1,0, z+1).$$

Реализуем данную операцию, воспользовавшись выражением (13). Тогда

$$\begin{array}{l} A(z) = (1, \quad 0, \quad z^2 + z + 1) \\ \times \\ \underline{B(z) = (1, \quad z^2 + z + 1, \quad z^2 + z + 1)} \\ C(z) = (1,0, z+1) \end{array},$$

где $\left|(z^2 + z + 1) \cdot (z^2 + z + 1)\right|^{+}_{p_3(z)} = \left|z^4 + z^2 + 1\right|^{+}_{p_3(z)} = z + 1.$

Из приведенного примера видно, что выполнение операции сложения и умножения в полиномиальном виде и в виде кода ПСКВ дает один и тот же результат. При этом порядок операндов $A(z)$ и $B(z)$ был уменьшен более чем в 2 раза, что является базовой предпосылкой для построения высокоскоростных вычислительных устройств ЦОС.

Таким образом, применение полиномиальной системы классов вычетов позволяет осуществлять ортогональные преобразования сигналов с использованием параллельных вычислений.

Литература

1. 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

2. Калмыков И.А., Чипига А.Ф. Структура нейронной сети для реализации цифровой обработки сигналов повышенной разрядности/Вестник Ставропольского Государственного Университета,2004, Выпуск №38 с.46-50.

3. Элементы применения компьютерной математики и нейроинформатики/Н.И. Червяков, И.А. Калмыков И.А., В.А. Галкина, Ю.О. Щелкунова, А.А. Шилов; Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 216с.