УДК 681.3

АЛГОРИТМ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ ХААРА В КОНЕЧНОМ ПОЛЕ

Калмыков И.А., Ложечкин А.А., Гапочкин А.В., Калмыков М.И.

ФГАОУ ВПО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Использование модулярной арифметики позволило эффективно решить задачи, связанные с цифровой обработкой сигналов (ЦОС), с реализацией криптографических преобразований, с вычислениями псевдослучайных функций повышенной эффективности. Одним из наиболее эффективных методов анализа сигналов в настоящее время выступает вейвлет-преобразования. Использование крупномасштабного анализа позволяет оценить сигнал как с точки зрения спектрального содержания, так и временного изменения. В работе предлагается реализовать вейвлет-преобразования Хаара в конечном поле. Применение модулярной арифметики позволит повысить точность проводимых исследований сигналов.

Ключевые слова: модулярная арифметика, крупномасштабная обработка сигналов, вейвлеты, преобразование Хаара, базисные функции Хаара конечное поле

LARGE SCALE PROCESSING SIGNALS BASED ON HAAR TRANSFORM

Kalmykov I.A., Lozhechkin A.A., Gapochkin A.V., Kalmykov M.I.

Federal state Autonomous educational institution higher professional education «North-Caucasian federal university», Stavropol, e-mail: kia762@yandex.ru

For the organization of digital signal processing, usually used the discrete Fourier transform (DFT) and its fast algorithms. However, this mathematical formalism is not always possible to ensure the maximum requirements for signal analysis. Using DFT and fast Fourier transform (FFT) in an environment where signals have certain local features, the resulting spectral components weakly reflect those characteristics. To solve this problem by carrying out a large-scale processing using wavelet transformation. The paper discusses examples of Haar wavelet transformation.

Keywords: large-scale signal processing, wavelets transform Haar Haar basis functions

Известно, что применение алгебраических структур, обладающих свойством кольца и поля, позволяет выполнить алгоритмы цифровой обработки сигналов (ЦОС) в реальном масштабе времени. Так как базовыми операциями ЦОС являются операции сложения, вычитания и умножения, то эти операции можно эффективно реализовать с использованием модулярной арифметики. Именно такие операции составляют основу алгоритмов крупномасштабного анализа сигналов. Поэтому реализация дискретного вейвлет-преобразований в поле является актуальной задачей.

Постановка и решение задачи исследований

Модулярная арифметика в настоящее время расширяет сферу своего использования. В настоящее время в качестве основных направлений применения алгебраических структур, обладающих свойством кольца и поля, можно выделить:

– Цифровая обработка сигналов. В данной области достаточно много трудов связано с использованием математических моделей ортогональных преобразований сигналов в поле комплексных чисел, которые реализуются на основе системы остаточных классов (СОК). Использование модулярных кодов позволяет, кроме повышения производительности специализированных процессоров (СП) ЦОС, обеспечить высокую отказоустойчивость вычислительных устройств [1, 2]. С целью повышения точности обработки сигналов в ряде работ [3–5] предлагается выполнение алгоритмов ЦОС в кольце полиномов. Использование полиномиальной системы классов вычетов способствует повышению снижения погрешности при проведении ортогональных преобразований сигналов. Кроме того, подобно кодам СОК, полиномиальная система классов вычетов позволяет осуществлять поиск и коррекцию ошибок, возникающих в процессе функционирования спецпроцессоров ЦОС.

– Защита информации от несанкционированного доступа (НСД) на основе криптографических алгоритмов. Использование математических особенностей полей Галуа позволяет отказаться от операции суммирования по модулю и использовать мультипликативные операции по модулю и их комбинации [6–8]. Использование модулярных полиномиальных кодов позволяет обеспечить защиту потока данных в реальном масштабе времени.

– Построение псевдослучайных функций (ПСФ) повышенной эффективности.

В работе [9] представлен алгоритм и основные сферы применения разработанной ПСФ, реализованной в конечном поле. Данная псевдослучайная функция в качестве аргумента использует входную последовательность $(x_1,\ldots,x_n)$ и ключи $(g,s_1,\ldots,s_n)$. В результате алгоритм ее вычисления определяется

$$F((s_1,...,s_n,h),(x_1,...,x_n)) = g^{\left(\prod_{i=1}^{n}(s_i+x_i)\right)_{-1}}, \quad (1)$$

где h – первообразный элемент мультипликативной группы.

Проведенные исследования показали, что для области определения размером 2^m значение $n = m/\log_2 l$. Вследствие этого при вычислении данной функции требуется в $\log_2 l$ раз меньше умножений. Основным преимуществом данной ПСФ является использование меньшего объема памяти для вычисления значения функция, так как она использует ключ в $\log_2 l$ раз меньший размером по сравнения с ПСФ Наора-Рейнголда. При этом стойкость данной ПСФ основывается на предположении о сложности решения λ-DDH проблемы.

Одним из наиболее перспективных направлением применения модулярной арифметики, реализованной в конечном поле, является крупномасштабный анализ сигналов. Известно, что дискретное преобразование Фурье (ДПФ), а также быстрое преобразование Фурье (БПФ) не используют для проведения анализа нестационарных сигналов, локализованных в некотором интервале времени. Это обусловлено тем, что ДПФ и БПФ не позволяют получить информацию о динамике изменения сигнала во временной области. Таким образом, ортогональные преобразования сигналов, проводимых в поле комплексных чисел, не позволяют правильно оценить изменения частотно-временных характеристик сигнала.

Данного недостатка лишены вейвлет-преобразования, которые положены в основу крупномасштабного анализа сигналов. Использование дискретного вейвлет-преобразования (ДВП) позволяет получить истинную картину при анализе сигнала, так как это преобразование производится как во временной области, так и в частотной области.

Одним из первых дискретных вейвлет-преобразований является преобразование Хаара, которое относится к разделимым, и может быть представлено в виде матриц

$$\mathbf{T} = \mathbf{HFH}^T, \quad (2)$$

где **F** – матрица сигнала; **H** – матрица преобразования; **T** – результат преобразования сигнала.

Для построения матрицы преобразования Хаара используются базисные функции Хаара $h_k(z)$. Следует отметить, что данные функции задаются на непрерывном замкнутом интервале $z\in[0, 1]$. Используемые при этом значения переменной k, располагаются в пределе от 0 до $N-1$, где $N = 2^n$. При этом для каждого индекса k, определяется пара значений q и l, для которых справедливо,

$$0 \le l \le n-1, \quad (3)$$

так чтобы выполнялось условие

$$k = 2^l + q - 1. \quad (4)$$

В работе [10] представлен алгоритм выбора значения индекса, согласно которому

$$q = \begin{cases} 0,1 & \text{при } l = 0 \\ 1 \le q \le 2^l & \text{при } l \ne 0 \end{cases} \quad (5)$$

Вычисленные, согласно выражения (5), значения индексов l и q используются для вычисления базисных функции Хаара. Если $k = 0$, то базисная функция имеет вид

$$h_0(z) = h_{00}(z) = \frac{1}{\sqrt{N}}, \quad (6)$$

где $z\in[0, 1]$.

При этом для вычисления остальных базисных функций используется выражение

$$h_k(z) = h_{lq}(z) = \frac{2^{\frac{l}{2}}}{\sqrt{N}} \begin{cases} 1 & \text{при } \frac{q-1}{2^l} \le z < \frac{q-0,5}{2^l} \\ -1 & \text{при } \frac{q-0,5}{2^l} \le z < \frac{q}{2^l} \\ 0 & \text{в остальных случаях} \end{cases}, \quad (7)$$

где $z\in[0, 1]$.

Рассмотрим выполнение вейвлет преобразования Хаара для 8 точек. Тогда матрица преобразования Хаара будет иметь следующий вид

$$W = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\ 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \end{bmatrix} \quad (8)$$

Анализ выражения (8) показывает, что преобразование Хаара можно реализовать в конечном поле *GF(p)*, где $p \neq 2$. Это обусловлено тем, что матрица содержит целые числа. Однако в ней присутствует и корень из двух. Переход к вычислению вейвлет Хаара возможно, если конечное поле сможет обеспечить целочисленное вычисление $\sqrt{2} \bmod p$. Данное свойство позволит осуществить переход от позиционного вычисления вейвлет-преобразования Хаара к преобразованию Хаара в конечном поле.

Выберем конечное поле *GF(17)*, в котором существует $\sqrt{2} \bmod 17 \equiv 6$. При этом значение нормирующего множителя в данном поле будет равно $\left(\sqrt{8}\right)^{-1} \bmod 17 \equiv 10$. В этом случае получаем следующую матрицу вейвлет-преобразования Хаара

$$H_8 = 10 \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 16 & 16 & 16 & 16 \\ 6 & 6 & 11 & 11 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 6 & 11 & 11 \\ 2 & 15 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 15 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 15 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 15 \end{bmatrix} \quad (9)$$

Для удобства работы в конечном поле произведем нормализацию 8×8 матрицы преобразования H_8 в поле *GF(17)*

$$H_8^{норм} = \begin{bmatrix} 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\ 10 & 10 & 10 & 10 & 7 & 7 & 7 & 7 \\ 9 & 9 & 8 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 9 & 8 & 8 \\ 3 & 14 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 14 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 14 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 14 \end{bmatrix} \quad (10)$$

В данной матрице выполняются все требования, предъявляемые к вейвлет-преобразованию

$$\sum_{i=0}^{N-1} h_{ij}(z) \equiv 0 \bmod p . \qquad (11)$$

$$\sum_{i=0}^{N-1} h_{ij}^2(z) \equiv 1 \bmod p . \qquad (12)$$

$$\sum_{i=0}^{N-1} h_{ij}(z) h_{ab}(z) \equiv 0 \bmod p , \qquad (13)$$

где $\forall\, i \neq a \; or \; j \neq b$.

Произведем выполнение крупномасштабного анализа сигнала с использованием нормализованной матрицы Хаара в конечном поле *GF(17)*.

$$W(i) = H_8^{норм} x(i) = \begin{bmatrix} 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\ 10 & 10 & 10 & 10 & 7 & 7 & 7 & 7 \\ 9 & 9 & 8 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 9 & 8 & 8 \\ 3 & 14 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 14 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 14 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 14 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \\ 4 \\ 4 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \qquad (14)$$

Проведем прямое преобразование Хаара для входной последовательности отсчетов сигнала $f(x) = [1, 1, 4, 4, 0, 0, 0, 1]$. Тогда, используя математический аппарат, который связан с крупномасштабной теорией, имеем

$$W_\phi(0,0) = \sum_{x=0}^{7} f(x)\phi_{00}(x) = \left|10\cdot 1 + 10\cdot 1 + 10\cdot 4 + 10\cdot 4 + 10\cdot 1\right|_{17}^{+} = \left|110\right|_{17}^{+} = 8$$

$$W_\psi(1,0) = \sum_{x=0}^{7} f(x)\psi_{01}(x) = \left|10\cdot 1 + 10\cdot 1 + 4\cdot 10 + 4\cdot 10 + 7\cdot 1\right|_{17}^{+} = 5$$

$$W_\psi(2,0) = \sum_{x=0}^{7} f(x)\psi_{2,0}(x) = \left|9\cdot 1 + 9\cdot 1 + 4\cdot 8 + 4\cdot 8\right|_{17}^{+} = 14$$

$$W_\psi(2,1) = \sum_{x=0}^{7} f(x)\psi_{2,1}(x) = \left|8\cdot 1\right|_{17}^{+} = 8$$

$$W_\psi(4,0) = \sum_{x=0}^{7} f(x)\psi_{4,0}(x) = \left|3\cdot 1 + 14\cdot 1\right|_{17}^{+} = 0$$

$$W_\psi(4,3) = \sum_{x=0}^{7} f(x)\psi_{4,3}(x) = \left|3\cdot 4 + 14\cdot 4\right|_{17}^{+} = 0$$

$$W_\psi(4,2) = \sum_{x=0}^{7} f(x)\psi_{4,2}(x) = 0$$

$$W_\psi(4,1) = \sum_{x=0}^{7} f(x)\psi_{4,1}(x) = \left|14\cdot 1\right|_{17}^{+} = 14$$

Таким образом, результатом вейвлет-преобразования имеем

$$W(i) = \left[8, 5, 14, 8, 0, 0, 0, 14\right].$$

Произведем обратное преобразование с целью восстановления исходного сигнала. Для этого необходимо воспользоваться транспонированной матрицей Хаара H_8^T, которая в конечном поле *GF(17)* имеет следующий вид

$$H_8^T = \begin{bmatrix} 10 & 10 & 9 & 0 & 3 & 0 & 0 & 0 \\ 10 & 10 & 9 & 0 & 14 & 0 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 3 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 14 & 0 & 0 \\ 10 & 7 & 0 & 9 & 0 & 0 & 3 & 0 \\ 10 & 7 & 0 & 9 & 0 & 0 & 14 & 0 \\ 10 & 7 & 0 & 8 & 0 & 0 & 0 & 3 \\ 10 & 7 & 0 & 8 & 0 & 0 & 0 & 14 \end{bmatrix}. \quad (15)$$

Воспользуемся данной матрицей и произведем вычисление обратного преобразования. В качестве входного вектора используем

$$W(i) = [8, 5, 14, 8, 0, 0, 0, 14].$$

Тогда имеем

$$f(x) = H_8^T W(x) = \begin{bmatrix} 10 & 10 & 9 & 0 & 3 & 0 & 0 & 0 \\ 10 & 10 & 9 & 0 & 14 & 0 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 3 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 14 & 0 & 0 \\ 10 & 7 & 0 & 9 & 0 & 0 & 3 & 0 \\ 10 & 7 & 0 & 9 & 0 & 0 & 14 & 0 \\ 10 & 7 & 0 & 8 & 0 & 0 & 0 & 3 \\ 10 & 7 & 0 & 8 & 0 & 0 & 0 & 14 \end{bmatrix} \times \begin{bmatrix} 8 \\ 5 \\ 14 \\ 8 \\ 0 \\ 0 \\ 0 \\ 14 \end{bmatrix}. \quad (16)$$

Согласно (16) получаем

$$x(0T) = \sum_i W_\phi(i)\phi_{00}(x) + \sum_j W_\psi(i,j)\psi_{i,j} = |10\cdot 8 + 10\cdot 5 + 14\cdot 9|_{17}^{+} = |256|_{17}^{+} = 1$$

$$x(1T) = \sum_i W_\phi(i)\phi_{00}(x) + \sum_j W_\psi(i,j)\psi_{i,j} = |10\cdot 8 + 10\cdot 5 + 14\cdot 9|_{17}^{+} = |256|_{17}^{+} = 1$$

$$x(2T) = |10\cdot 8 + 10\cdot 5 + 14\cdot 8|_{17}^{+} = |242|_{17}^{+} = 4$$

$$x(3T) = |10\cdot 8 + 10\cdot 5 + 14\cdot 8|_{17}^{+} = |242|_{17}^{+} = 4$$

$$x(4T) = |10\cdot 8 + 7\cdot 5 + 9\cdot 8|_{17}^{+} = |187|_{17}^{+} = 0$$

$$x(5T) = |10\cdot 8 + 7\cdot 5 + 9\cdot 8|_{17}^{+} = |187|_{17}^{+} = 0$$

$$x(6T) = |10\cdot 8 + 7\cdot 5 + 8\cdot 8 + 14\cdot 3|_{17}^{+} = |221|_{17}^{+} = 0$$

$$x(7T) = |10\cdot 8 + 7\cdot 5 + 8\cdot 8 + 14\cdot 14|_{17}^{+} = |375|_{17}^{+} = 1$$

Таким образом, получена исходная входная комбинация, которую подвергали крупномасштабному анализу. Рассмотрим представление исходной последовательностив базисевейвлет-преобразования

$$x(nT) = \left| 8\phi_{0,0} + 5\psi_{1,0} + 14\psi_{2,0} + 8\psi_{2,1} + 0\psi_{4,0} + 0\psi_{4,3} + 0\psi_{4,2} + 14\psi_{4,1} \right|_{17}^{+}, \quad (17)$$

Таким образом, выражение (17) можно представить в виде

$$x(nT) = \left| \underbrace{\underbrace{\underbrace{8\phi_{0,0}}_{V_0} + \underbrace{5\psi_{1,0}}_{W_0}}_{V_1=V_0\oplus W_0} + \underbrace{14\psi_{2,0} + 8\psi_{2,1}}_{W_1}}_{V_2=V_1\oplus W_1} + \underbrace{0\psi_{4,0} + 0\psi_{4,3} + 0\psi_{4,2} + 14\psi_{4,1}}_{W_2} \right|_{17}^{+}. \quad (18)$$

Проведенные исследования свидетельствуют о том, что использование вейвлет-преобразований в конечном поле представляет собой обратимые преобразования. При этом такое преобразование не имеет ошибок округления, которые определяются позиционной системой счисления.

Выводы

В работе рассмотрены вопросы применения вейвлет-преобразований для анализа сигнала. В качестве такого преобразования предлагается использовать преобразования Хаара. Показана целесообразность реализации данного преобразования в конечном поле. Приведены примеры прямого преобразования Хаара, а также реализация обратного преобразования в поле Галуа GF(17). Полученные результаты позволяют сделать вывод о том, что использование алгебраических структур, обладающих свойством поля, позволяет снизить ошибки округления при выполнении крупномасштабного анализа сигналов.

СПИСОК ЛИТЕРАТУРЫ

1. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Ряднов С.А Модулярные параллельные вычислительные структуры нейросетевых систем / под ред. Н.И. Червякова. – М.: Физматлит., 2003. – 303 с.

2. Червяков Н.И. Обобщенная вычислительная модель модулярного нейропроцессора цифровой обработки сигналов на основе программируемых логических интегральных схем // Нейрокомпьютеры: разработка и применение. – 2006. – № 10. – С. 37–40.

3. Калмыков И.А., Воронкин Р.А., Резеньков Д.Н, Емарлукова Я.В., Фалько А.А. Генетические алгоритмы в системах цифровой обработки сигналов // Нейрокомпьютеры: разработка и применение. – 2011. – № 5. – С. 20–27.

4. Калмыков И.А., Калмыков М.И. Структурная организация параллельного спецпроцессора цифровой обработки сигналов, использующего модулярные код// Теория и техника радиосвязи. – 2014. – № 2. – С. 60-66.

5. Калмыков И.А., Саркисов А.Б., Макарова А.В. Технология цифровой обработки сигналов с использованием модулярного полиномиального кода [Текст] // Известия ЮФУ Технические науки. – 2013. – № 12 (149). – С. 234–241.

6. Калмыков И.А., Зиновьев А.В., Резеньков Д.Н., Гахов В.Р. Применение систолических ортогональных преобразований в полиномиальной системе классов вычетов для повышения эффективности цифровой обработки сигналов // Инфокоммуникационные технологии. – 2010. – Т .8, № 3. – С. 4–11.

7. Калмыков И.А., Чипига А.Ф., Кихтенко О.А., Барильская А.В. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем // Известия ЮФУ Технические науки. – 2009. – Т. 100, № 11. – С. 210–220.

8. Калмыков И.А., Стрекалов Ю.А., Щелкунова Ю.О., Кихтенко О.А., Барильская А.В. Технология нелинейного шифрования данных в высокоскоростных сетях связи // Инфокоммуникационные технологии. – 2010. – Т.8, № 2. – С. 14–22.

9. Калмыков И.А., Дагаева О.И. Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции // Известия ЮФУ Технические науки. – 2012. – Т. 137, № 12 (137). – С. 218–224.

10. Червяков Н.И., Чумаков Д.В., Мальцев Н.А. Применение нейронных сетей для реализации целочисленного вейвлет анализа сигналов, заданных конечным числом отсчетов-преобразований [Текст] / Н.И. Червяков // Нейрокомпьютеры: разработка и применение. – 2008. – № 1-2. – С. 43–50.