УДК 517.9

СЕТЕВОЕ КОДИРОВАНИЕ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

А.А. ОХРИМЕНКО, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 3 сентября 2012

Рассматривается метод сетевого кодирования группового сигнала на основе применения вейлет преобразований над конечными полями. Показана возможность применения дискретных вейвлет-преобразований Хаара и Добеши, формируемых над конечными полями, для кодирования и декодирования информации в сетевой структуре.

Ключевые слова: сетевой код, конечное поле, дискретное вейвлет-преобразование.

Модель системы сетевого кодирования

Рассмотрим канал сети, состоящий из нескольких элементов сети N_1, N_2, …, N_L, которые обмениваются между собой информацией через промежуточный, ретрансляционный элемент сети N_R. Промежуточный узел запоминает в буферной памяти пакеты, поступившие по входным линиям, образует их линейные комбинации, а затем рассылает их копии по тем своим выходным линиям, которые могут через другие узлы доставить их получателям [1-3].

Предполагается, что элементы сети поддерживают режим полудуплексного взаимодействия. Имеются две фазы взаимодействия элементов сети в канале. В первой фазе элементы N_1, …, N_L передают пакеты $\{X_i, i=1,...L\}$ на элемент N_R, который принимает сигнал

$$y_R = \sum_{i=1}^{L} h_{i,R} x_i + v_R,\ x_i \in X_i, \qquad (1)$$

где $h_{i,j}$ – комплексный коэффициент, характеризующий свойства канала; v_3 – комплексный, гауссовский, внутренний шум с нулевым математическим ожиданием и единичной дисперсией принимающей части элемента сети N_R.

Предполагается нормализация мощности и синхронизация сигналов передаваемых пакетов. Также предполагается возможность оценки коэффициентов $h_{i,j}$ для каждого элемента сети.

Во второй фазе элемент сети N_R формирует на основе принятых сообщений пакет X_R, сигнал которого x_R в широковещательном формате передается на элементы сети. Последние принимают сигналы

$$y_1 = h_{R,1} x_R + v_1, \ldots, y_L = h_{R,L} x_L + v_L, \qquad (2)$$

где $x_R = f(x_1,...x_L)$ является функцией от $\{x_i, i=1,...,L\}$.

Кодирование $f(x_1, ..., x_L)$ может быть выполнено различными способами [1-2].

Помехоустойчивые методы кодирования используют ортогональные сигналы. Для сетевых структур важным аспектом является разнообразие массивов ортогональных сигналов и преобразований.

Вейвлет-преобразования над конечными полями

Вейвлет-функции могут быть определены над конечными полями $GF(q)$. Базисная (материнская) вейвлет-функция над конечным полем (ВФКП) представляется в виде N-мерного вектора [4]:

$$\boldsymbol{\psi}_{1,0} = (\psi_{1,0}(0), \psi_{1,0}(1), ..., \psi_{1,0}(N-1)), \tag{3}$$

где каждая компонента ψ принадлежит расширенному полю $GF(p^s)$, p – простое число, s – целое положительное число.

Рассмотрим вначале случай простого поля $GF(p)$. Пусть N будет целым и $D(N)$ – дивизор, который объединяет множество делителей N. Структура конечного поля не позволяет выполнить такую же операцию масштабирования (шкалирования), какая производится для непрерывных вейвлет-функций в поле действительных чисел. Операцию масштабирования в конечном поле выполняет дивизор длины.

Введем следующие операции.

1. Операция шкалирования $\boldsymbol{\psi}_{j,0}$, где

$$\psi_{j,0}(i) = \psi_{1,0}(ji) \quad \forall j \in D(N/2) := \{ j \text{ таких, что } j \mid N/2 \}. \tag{4}$$

2. Операция сдвига $\boldsymbol{\psi}_{j,k}$:

$$\psi_{j,k}(i) = \psi_{j,0}(i + \frac{Nk \bmod N}{j}), \ \forall k = 0,1,...,N-1. \tag{5}$$

Вейвлет-функция может быть записана в виде

$$\boldsymbol{\psi}_{j,k} = (\psi_{j,k}(0), \psi_{j,k}(1), \psi_{j,k}(2), ..., \psi_{j,k}(N-1)), \tag{6}$$

где масштабирование и/или сдвиг выполняются по версии базисной ВФКП.

Свойство. ВФКП $\boldsymbol{\psi}_{j,k}$ подчиняются соотношению

$$\sum_{i=0}^{N-1} \boldsymbol{\psi}_{j,k}(i) \equiv 0 \bmod p, \ (\forall j,k). \tag{7}$$

Вейвлет-преобразование над конечным полем. Пусть задан вектор-сигнал $\mathbf{v} = (v_0, v_1, \ldots, v_{N-1})$ длины N над полем $GF(p)$ характеристики $p \neq 2$ и вейвлет-функции $\boldsymbol{\psi}_{j,k}$ над полем $GF(p^s)$.

Вейвлет-преобразование над конечным полем (ВПКП) сигнала $\mathbf{v}$ определяется как

$$\Psi_F(j,k) \equiv \sum_{i=0}^{N-1} v_i \psi_{j,k}(i) \bmod p = < \mathbf{v}, \boldsymbol{\psi}_{j,k} >. \tag{8}$$

Преобразование Хаара над конечным полем. Базис Хаара в конечных полях можно записать следующим образом:

$$\psi_{1,0}(i) = \begin{cases} 1, & \text{если } 0 \le \dfrac{i}{N} < \dfrac{1}{2} \\ p-1, & \text{если } \dfrac{1}{2} \le \dfrac{i}{N} < 1 \\ 0, & \text{в остальных случаях} \end{cases} \tag{9}$$

или в форме

$$\psi_{j,0}(i) = \begin{cases} (p-1)^{\left\lfloor \frac{i \bmod N}{N/2} \right\rfloor}, & \text{если } 0 \le \dfrac{i}{N} < 1 \\ 0, & \text{в остальных случаях} \end{cases}. \tag{10}$$

Пример. Предположим, требуется построить функции Хаара длиной $N = 8$ над конечным полем $GF(p)$. Возможные коэффициенты масштабирования $j \in D(4) = \{1,2,4\}$. Воспользовавшись вышеприведенной формулой, получаем:

$j = 1 \to \boldsymbol{\psi}_{1,0} = (1,1,1,1, p-1, p-1, p-1, p-1)$,

$j = 2 \to \boldsymbol{\psi}_{2,0} = (1,1, p-1, p-1, p-1, 0, 0, 0, 0)$,

$j = 4 \to \boldsymbol{\psi}_{4,0} = (1, p-1, 0, 0, 0, 0, 0, 0)$.

Полученные функции удовлетворяют операции сдвига. Так, функция $\boldsymbol{\psi}_{2,0}$ после сдвига образует вектор

$\boldsymbol{\psi}_{2,1} = (0,0,0,0,1,1, p-1, p-1)$.

Свойство. Исходная версия функции $\boldsymbol{\psi}_{j,0}$ позволяет получить j различных сдвигов функции $\boldsymbol{\psi}_{j,k}$.

Нормализация энергии. Поскольку N является степенью двойки и j принадлежит $D(N/2)$, то (N/j) также степень двойки. Предположим теперь, что $p \equiv \pm 1 \bmod 8$, тогда $\sqrt{N/j} \in GF(p)$. Тогда нормализованное преобразование может быть записано как

$$V_{FW}(j,k) = \frac{1}{\sqrt{(N/j) \bmod p}} \sum_{i=0}^{N-1} v_i \psi_{j,k}(i) \bmod p. \qquad (11)$$

Определим подмножество $S \subseteq D(N/2)$ такое, что

$$\sum_{j \in S \subseteq D(N/2)} j = N - 1. \qquad (12)$$

Положим $N = 2^m$, тогда $D(N/2)=\{1, 2, 4, 8, \ldots, 2^{m-1}\}$ и $\sum_{j \in D(n/2)} j = \sum_{j=1}^{m-1} 2^j = N - 1$. В этом случае $j \in D(N/2)$ и все значения индекса j могут быть использованы для построения базисных вейвлетов. Построенные таким образом функции вместе с последовательностью из всех единиц (1, 1, …, 1) образуют ортогональное множество N сигналов над полем $GF(p)$ или, другими словами, ортогональный базис Хаара.

Пример. Над полем $GF(7)$ ВФКП Хаара и нормализованные ВФКП Хаара имеют вид

(1 1 1 1 1 1 1 1)	(1 1 1 1 1 1 1 1)
(1 1 1 1 6 6 6 6)	(6 6 6 6 1 1 1 1)
(1 1 6 6 0 0 0 0)	(4 4 3 3 0 0 0 0)
(0 0 0 0 1 1 6 6)	(0 0 0 0 4 4 3 3)
(1 6 0 0 0 0 0 0)’	(5 2 0 0 0 0 0 0)
(0 0 1 6 0 0 0 0)	(0 0 5 2 0 0 0 0)
(0 0 0 0 1 6 0 0)	(0 0 0 0 5 2 0 0)
(0 0 0 0 0 0 1 6)	(0 0 0 0 0 0 5 2)

Для построенных функций справедливы следующие соотношения:

$\sum_{i=0}^{N-1} \psi_{j,k}(i) \equiv 0 \bmod p$, $\sum_{i=0}^{N=1} \psi_{j,k}^2(i) \equiv 1 \bmod p$,

$\sum_{i=0}^{N-1} \psi_{j,k}(i) \psi_{j',k'}(i) \equiv 0 \bmod p, \forall j \neq j'$ или $k \neq k'$.

Если N не является степенью двойки, то могут быть вычислены не ортогональные вейвлет-функции. Например, если $N = 24$, то над полем $GF(7)$ получаем следующее множество сдвигов $D(12) = \{1, 2, 3, 4, 6, 12\}$. Вейвлет-функции имеют вид

	Число возможных сдвигов	
$j = 1$	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1
$j = 2$	1 1 1 1 1 1 1 1 1 1 1 1 6 6 6 6 6 6 6 6 6 6 6 6	1
$j = 6$	1 1 1 6 6 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	4
$j = 12$	1 1 6 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	6
	1 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12

Полученные сигналы не образуют ортогонального множества, так, например, $\langle \boldsymbol{\psi}(2,1), \boldsymbol{\psi}(6,0) \rangle \neq 0 \bmod p$.

Структура вейвлет-функции Хаара над конечным полем позволяет строить пирамидально-фильтровые алгоритмы.

Пример. Двухэлементные фильтры (1, 1) для преобразования Хаара над полем $GF(7)$ имеют следующие импульсные характеристики:

$h = [5, 5]$, $h^*[5, 5]$; $g = [2, 5]$, $g^* = [5, 2]$.

Вейвлет-функции Добеши над простыми конечными полями. Рассмотрим стандартную постановку задачи Добеши построения ортогональных вейвлет-функций. Функция прототип имеет вид

$$\psi_{j,k}(i) = \left(\sqrt{2}\right)^j \psi\left(2^j i - k\right). \tag{13}$$

Анализ с разным разрешением использует масштабные функции. В нашем случае в качестве масштабных функций можно определить такие функции φ, которые удовлетворяют сравнению

$$\varphi_{j,k}(i) \equiv \left(2\right)^{j/2} \varphi(2^j i - k), \tag{14}$$

причем выполняется условие $\varphi_{j,k}(i) \equiv \sqrt{2}\varphi(2i - k) \bmod p$.

Дискретный вейвлет-анализ использует понятие зеркальных квадратурных фильтров с импульсными характеристиками, соответственно $\mathbf{h} = (h_0, h_{1,}\ldots, h_{N-1})$ и $\mathbf{g} = (g_0, g_{1,}\ldots, g_{N-1})$. Применим такой подход при решении нашей задачи. Уравнения, обеспечивающие детализацию спектра, с использованием импульсных характеристик квадратурных зеркальных фильтров $\mathbf{h}$ можно записать как

$$\varphi(i) \equiv \sqrt{2} (\bmod p) \sum_{k=0}^{N-1} h_k \varphi(2i - k) \bmod p. \tag{15}$$

Соответственно, вейвлет-функции используют альтернативный фильтр $\mathbf{g}$ следующим образом:

$$\psi(i) \equiv \sqrt{2} (\bmod p) \sum_{k=0}^{N-1} g_k \varphi(2i - k) \bmod p. \tag{16}$$

Импульсные характеристики фильтров определяются из соотношений

$$\sum_{k=0}^{N-1} h_k \equiv \sqrt{2} \bmod p,\ \sum_{k=0}^{N-1} g_k \equiv 0 \bmod p,\ g_k \equiv (-1)^k h_{N-1+k} \bmod p,\ \sum_{k=0}^{N-1} h_k h_{k+2m} \equiv 0 \bmod p, m \neq 0. \tag{17}$$

Пример. Построим фильтры для вейвлет-функций Добеши конечного поля *GF*(97), $N = 4$.

Квадратурные зеркальные фильтры определяются как

- сглаживающий (нижних частот) фильтр **h** = [92, 47, 12, 57];
- детализирующий (высоких частот) фильтр **g** =[57, 85, 47, 5].

Значения импульсных характеристик фильтров связаны соотношениями

$g_k \equiv (-1)^k h_{3-k} \mod 97$, $\sum_{k=0}^{3} h_k \equiv 14 \mod 97$, $14^2 = 196 \equiv 2 \mod 97$;

$\sum_{k=0}^{3} g_k \equiv 0 \mod 97$, и $\sum_{k=0}^{3} h_k h_{k+2} \equiv 0 \mod 97$.

Синтез сложных сигналов на основе вейвлет-функций Хаара конечных полей

Ортогональные вейвлет-функции конечного поля можно использовать для формирования сигналов при сетевом кодировании. В таких системах каждый элемент сети использует для передачи информации свой сигнал – кодовую последовательность. В качестве таких кодовых последовательностей можно предложить использовать сигналы, которые получаются путем масштабирования/сдвига базисного вейвлета.

Рассмотрим пример кодирования сигналов для N=8 и поля $GF(7)$.

Оператор суммы в y_R выполняет операцию векторного суммирования по mod p. Информационный сигнал в каждом канале состоит из N одинаковых символов, которые смешиваются с канальной вейвлет-функцией. Например, пусть для третьего канала информационный символ равен 2, а канальная вейвлет-функция имеет вид $\boldsymbol{\psi}_{2,0}$ = (4 4 3 3 0 0 0 0). Тогда канальный сигнал имеет вид

(2 2 2 2 2 2 2 2) $\otimes$ (4 4 3 3 0 0 0 0) = (1 1 6 6 0 0 0 0) mod 7

или в сокращенной записи

$2^{(8)} \otimes 4^{(2)}3^{(2)}0^{(4)} = 1^{(2)}6^{(2)}0^{(4)} \mod 7$.

Теперь рассмотрим случай, когда информация передается сразу по всем 8 каналам. Пусть информационный вектор $\mathbf{a} = [3, 0, 2, 1, 6, 5, 5, 4]^T$. Вектор опорных вейвлет-функций имеет вид $[\boldsymbol{\psi}_{0,0}, \boldsymbol{\psi}_{1,0}, \boldsymbol{\psi}_{2,0}, \boldsymbol{\psi}_{2,1}, \boldsymbol{\psi}_{4,0}, \boldsymbol{\psi}_{4,1}, \boldsymbol{\psi}_{4,2}, \boldsymbol{\psi}_{4,3}]$. После перемножения в каналах символов информационных и вейвлет-последовательностей, на входе сумматора Σ получим

$\mathbf{r} = 3^{(8)} \oplus 0^{(8)} \oplus 1^{(2)}6^{(2)}0^{(4)} \oplus 0^{(4)}4^{(2)}3^{(2)} \oplus 2^{(1)}5^{(1)}0^{(6)} \oplus 0^{(2)}4^{(1)}3^{(1)}0^{(4)} \oplus 0^{(4)}4^{(1)}3^{(1)}0^{(2)} \oplus 0^{(6)}6^{(1)}1^{(1)} \equiv$

$\equiv (6, 2, 6, 5, 4, 3, 5, 0) \mod 7$.

Так как вейвлет-функции ортогональны, то на приемной стороне информация однозначно выделяется с помощью операции скалярного произведения векторов над конечным полем $GF(p)$:

- канал $3 \rightarrow < \mathbf{r}, \boldsymbol{\psi}_{2,0} > \equiv 2 \mod 7$;
- канал $8 \rightarrow < \mathbf{r}, \boldsymbol{\psi}_{4,3} > \equiv 4 \mod 7$, и т.д.

Заключение

Описаны методы построения дискретных вейвлет-преобразований в конечных полях и модулярных вычислениях. Показаны перспективы использования рассмотренных преобразований для решения задач сетевого кодирования.

NETWORK CODING ON THE USE OF WAVELET TRANSFORM IN FINITE FIELDS

A.A. OKHRIMENKO, S.B. SALOMATIN

Abstract

A method of network coding based on the use of wavelet transform in finite fields is presented. Algorithms of wavelet transforms Haar and Daubechies in finite fields for network coding has been considered.

Литература

1. *Габидулин Э.М., Пилипчук Н.И., Колыбельников А.И. и др*. // Сетевое кодирование. ТРУДЫ МФТИ. 2009. Т. 1, №2. С. 3-28.
2. Physical layer network coding [Электронный ресурс]. Режим доступа: http://arxiv.org/ftp/arxiv/papers/0704/0704.2475.pdf
3. *Li Y.R., Yeung R.W., Cai N.* // IEEE Trans. on Inform. 2003. Vol. 49 (2). P. 371-381.
4. *Фрейзер М.* Введение в вейвлеты в свете линейной алгебры. М., 2008.