КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

УДК 621.391

ВЕЙВЛЕТНЫЕ ФИЛЬТРЫ ТРЕТЬЕГО ПОРЯДКА В ПРОСТЫХ ПОЛЯХ ГАЛУА

THIRD ORDER WAVELET FILTERS OVER PRIME GALOIS FIELDS

Н.И. Червяков, П.А. Ляхов, Н.Ф. Семенова, К.С. Шульженко
N.I. Chervyakov, P.A. Lyakhov, N.F. Semyonova, K.S. Shulzhenko

Северо-Кавказский федеральный университет, Россия, 355009, Ставрополь, ул. Пушкина, 1
North-Caucasus Federal University, 1 Pushkina St, Stavropol, 355009, Russia

e-mail: ljahov@mail.ru

Аннотация. В работе исследован вопрос о построении вейвлетных фильтров третьего порядка над конечными полями с простым числом элементов. Предложен метод построения всех фильтров такого типа, основанный на свойствах квадратичных вычетов. Использование предложенного подхода позволяет значительно сократить время построения вейвлетных фильтров конечного поля по сравнению с известными методами, основанными на вычислительно сложном алгоритме Берлекэмпа. Разработанный метод построения вейвлетных фильтров третьего порядка над конечным полем может быть использован для цифровой обработки сигналов и для задач защиты информации.

Resume. We investigated the problem of third order wavelet filters construction over finite fields with the prime number of elements. There was proposed a method for design all filters of this type based on the properties of quadratic residues. Using the proposed approach can significantly reduce the time of wavelet filters construction over finite fields in comparison with known methods based on the computationally complicated Berlekamp algorithm. The developed method of third order wavelet filters construction over finite field can be used for digital signal processing tasks and for information protection.

Ключевые слова: цифровая обработка сигналов, вейвлет-преобразование, алгоритм, конечное поле.
Keywords: digital signal processing, wavelet transform, algorithm, finite field.

Введение

Разработка моделей, методов и алгоритмов цифровой обработки сигналов (ЦОС) в конечных полях вызывает в последнее время повышенный интерес у исследователей. Данный факт объясняется особенностями строения конечного поля как алгебраической структуры [1]. В конечных полях, так же как и в полях действительных и комплексных чисел, сохраняется возможность выполнения арифметических операций сложения, вычитания, умножения и деления. С другой стороны, дискретная природа конечных полей эффективна при обработке квантованных величин, возникающих в ЦОС [2, 3].

В настоящее время получило широкое распространение применение вейвлетов для решения разнообразных задач ЦОС. Вейвлет-преобразование возникло как альтернатива преобразованию Фурье. Обработка с использованием вейвлетов позволяет получать не только частотную информацию о сигнале, но еще и его локальные особенности. В настоящее время вейвлеты широко применяются для задач сжатия сигнала [4], очистки от шума [5, 6], анализа временных рядов [7], обработки данных в медицине [8] и во многих других областях. Однако в большинстве случаев на практике используются вейвлеты, построенные над полями действительных и комплексных чисел. Особенностью этих вейвлетов является относительная

простота построения и применения на практике. Однако вейвлет-преобразование над полями действительных и комплексных чисел не лишено недостатков, к которым прежде всего следует отнести высокую вычислительную сложность обработки, а также неизбежное возникновение ошибок округления.

Для устранения этих недостатков был разработан математический аппарат ЦОС с использованием вейвлетов конечного поля [9]. Предложены методы и алгоритмы кодирования [10, 11], криптографической защиты информации [12, 13] и обработки изображений [14] с использованием вейвлетов конечного поля. Одним из главных препятствий на пути использования вейвлетов конечного поля на практике является высокая сложность их построения, так как в настоящее время для этой цели используется алгоритм Берлекэмпа или его модификации [9]. В данной статье исследованы вейвлетные фильтры третьего порядка над конечными полями GF_p, построенные с использованием линейных двучленов. Показаны алгоритмы построения таких фильтров и приведен пример проектирования.

Вейвлет-преобразование в конечных полях

Конечные поля (поля Галуа) делятся на два типа: простые поля GF_p и полиномиальные поля GF_{p^n}, $n>1$, $n\in N$. Простое конечное поле GF_p содержит число элементов, равное простому числу p. Любое конечное поле из p элементов изоморфно полю классов вычетов по модулю p, поэтому операции сложения, умножения и вычитания в GF_p могут рассматриваться как аналогичные операции над целыми числами, взятые по $\bmod p$. Арифметика полиномиальных полей GF_{p^n} является более сложной и основана на свойствах многочленов над GF_p. В данной работе будут рассмотрены лишь простые поля GF_p.

Пусть мы имеем конечное поле GF_p. Определим векторное пространство V, элементы которого – вектора над полем GF_p. Предположим, что это пространство можно представить в виде прямой суммы двух подпространств

$$V = V_0 \oplus W_0,\ V_0 \cap W_0 = \{0\}. \quad (1)$$

Если обозначить через $\overline{span\{\alpha_1, \alpha_2, \ldots, \alpha_n\}}$ линейную оболочку над векторами $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, то материнский вейвлет $\psi(x)$ и скейлинг-функция $\varphi(x)$, определяющие вейвлет-преобразование в конечном поле GF_p, должны удовлетворять следующим соотношениям [9]

$$V_0 = \overline{span\{\varphi(n-2j)\}},\ \forall j \in Z, \quad (2)$$

$$W_0 = \overline{span\{\psi(n-2j)\}},\ \forall j \in Z, \quad (3)$$

и, кроме того, условиям ортонормированности базиса

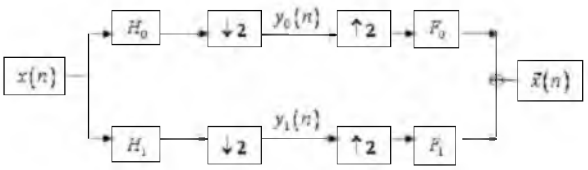
$$\langle \varphi(n-2m), \varphi(n-2k) \rangle = \delta(m-k),\ \forall m,k \in Z, \quad (4)$$

$$\langle \psi(n-2m), \psi(n-2k) \rangle = \delta(m-k),\ \forall m,k \in Z, \quad (5)$$

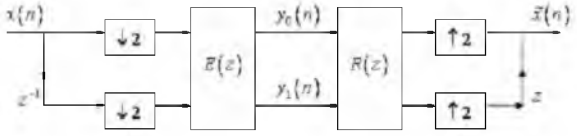
$$\langle \varphi(n-2m), \psi(n-2k) \rangle = 0,\ \forall m,k \in Z. \quad (6)$$

Вейвлет-преобразованием в конечном поле GF_p является отображение, ставящее в соответствие вектору $x(m)$ последовательность коэффициентов $\langle x(m), \psi(m-2k) \rangle$. Обратное преобразование осуществляется по формуле

$$x(n) = \sum_{k\in Z} \langle x(m), \varphi(m-2k) \rangle \varphi(n-2k) + \sum_{k\in Z} \langle x(m), \psi(m-2k) \rangle \psi(n-2k). \quad (7)$$



а



б

Рис. 1. Двухканальный набор фильтров дискретного вейвлет-преобразования:
а) обычное изображение, б) изображение в многофазной форме

Fig. 1. Two-channel discrete wavelet transform filter bank: a) direct form, b) polyphase form

На практике вейвлет-преобразование реализуется при помощи наборов фильтров. На рисунке 1а показан двухканальный набор фильтров дискретного вейвлет-преобразования. Здесь H_0 и H_1 - анализирующие фильтры, $\downarrow 2$ - оператор децимации, $\uparrow 2$ - оператор разрежающей выборки, F_0 и F_1 - синтезирующие фильтры. Этот же набор фильтров может быть представлен в многофазной форме (рисунок 1б) [15, 16]. С таким набором фильтров ассоциирована матрица

$$E(z)=\begin{pmatrix} E_{00}(z) & E_{01}(z) \\ E_{10}(z) & E_{11}(z) \end{pmatrix}, \tag{8}$$

элементы которой принадлежат кольцу многочленов $F(z)$. В конечных полях, так же как и в полях действительных и комплексных чисел, порядок фильтров, соответствующих материнскому вейвлету $\psi(x)$ и скейлинг-функции $\varphi(x)$ должен быть нечетным [9]. Для того, чтобы набор фильтров обладал свойством точного восстановления сигнала, необходимо, чтобы матрица $E(z)$ была параунитарной, то есть выполнялось соотношение

$$E^T(z^{-1})E(z)=I, \tag{9}$$

где I – единичная матрица [17]. Необходимым и достаточным условием точного восстановления сигнала является выполнение соотношения

$$E_{00}(z)E_{00}(z^{-1})+E_{01}(z)E_{01}(z^{-1})=I \tag{10}$$

между элементами матрицы (8).

Пусть порядок фильтра определяется целым числом $2N+1$ и M – положительное число, такое что $M \le N$. Тогда многочлены $E_{00}(z)$ и $E_{01}(z)$ определяются следующими соотношениями:

$$E_{00}(z)=\sum_{i=0}^{M} e_{0i}z^{-i},\ e_{00}\neq 0,\ e_{0i}\in GF_p, \tag{11}$$

$$E_{01}(z)=\sum_{i=0}^{N} e_{1i}z^{-i},\ e_{1N}\neq 0,\ e_{1i}\in GF_p, \tag{12}$$

а многочлены $E_{10}(z)$ и $E_{11}(z)$ матрицы (8) находятся по формулам

$$E_{10}(z)=z^{-N}E_{01}(z^{-1}),\ E_{11}(z)=-z^{-N}E_{00}(z^{-1}). \tag{13}$$

Фильтры H_0 и H_1 можно найти по формулам

$$H_0(z)=E_{00}(z^2)+z^{-1}E_{01}(z^2), \tag{14}$$

$$H_1(z)=E_{10}(z^2)+z^{-1}E_{11}(z^{-2}). \tag{15}$$

Фильтры F_0 и F_1 находятся из условий точного восстановления сигнала [2]

$$F_0(z)=H_1(-z),\ F_1(z)=-H_0(-z). \tag{16}$$

Построение набора фильтров на рисунке 1 сводится к отысканию многочленов $A(z)=\sum_{i=0}^{M} a_i z^i$, $a_0\neq 0$ и $B(z)=\sum_{i=0}^{M} b_i z^i$, $b_M\neq 0$ из кольца многочленов $F(z)$, удовлетворяющих условию

$$A(z)A(z^{-1})+B(z)B(z^{-1})=1. \tag{17}$$

Каждая такая пара многочленов $A(z)$ и $B(z)$ определяет многочлены E_{00} и E_{01} по формулам

$$a_i=e_{0i},\ e_{1i}=0, \text{ для } i=0,\ldots,N-M-1. \tag{18}$$
$$b_i=e_{1(N-M+i)}, \text{ для } i=0,\ldots,M.$$

Основной сложностью при построении вейвлетных фильтров конечного поля является поиск многочленов $A(z)$ и $B(z)$, удовлетворяющих условию (17). Далее будет исследован вопрос о нахождении линейных двучленов $A(z)$ и $B(z)$ в полях GF_p для построения вейвлетных фильтров наименьшего нетривиального (третьего) порядка.

Построение вейвлетных фильтров третьего порядка в полях GF_p

Рассмотрим задачу о построении многочленов $A(z)=a_0+a_1z$ и $B(z)=b_0+b_1z$ из $GF_p[z]$, для которых выполняется соотношение $A(z)A(z^{-1})+B(z)B(z^{-1})=1$.

Задача будет решаться в предположении, что: $a_0\neq 0$, $a_1\neq 0$, $b_0\neq 0$, $b_1\neq 0$.

Сформулируем и докажем вспомогательные теоремы, которые будут необходимы нам для решения поставленной задачи.

Теорема 1. Пусть $A_1(z)=a_0+a_1z$, $A_2(z)=a_1+a_0z$, $A_3(z)=(p-a_0)+(p-a_1)z$, $A_4(z)=(p-a_1)+(p-a_0)z$, $B_1(z)=b_0+b_1z$, $B_2(z)=b_1+b_0z$, $B_3(z)=(p-b_0)+(p-b_1)z$, $B_4(z)=(p-b_1)+(p-b_0)z$, $C_1(z)=a_0+(p-a_1)z$, $C_2(z)=(p-a_1)+a_0z$, $C_3(z)=(p-a_0)+a_1z$, $C_4(z)=a_1+(p-a_0)z$, $D_1(z)=b_0+(p-b_1)z$, $D_2(z)=(p-b_1)+b_0z$, $D_3(z)=(p-b_0)+b_1z$, $D_4(z)=b_1+(p-b_0)z$ – линейные двучлены в поле GF_p.

Если для $A_1(z)=a_0+a_1z$ и $B_1(z)=b_0+b_1z$ из $GF_p[z]$ выполняется соотношение $A_1(z)A_1(z^{-1})+B_1(z)B_1(z^{-1})=1$, то $A_l(z)A_l(z^{-1})+B_k(z)B_k(z^{-1})=1$ и $C_l(z)C_l(z^{-1})+D_k(z)D_k(z^{-1})=1$, при $k=1,2,3,4$ и $l=1,2,3,4$.

Доказательство.

Непосредственное нахождение произведений дает: $A_1(z)A_1(z^{-1})=a_1a_0z+a_1^2+a_0^2+a_1a_0z^{-1}$.

$A_2(z)A_2(z^{-1})=a_0a_1z+a_0^2+a_1^2+a_0a_1z^{-1}=A_1(z)A_1(z^{-1})$.

$A_3(z)A_3(z^{-1})=(p-a_1)(p-a_0)z+(p-a_1)^2+(p-a_0)^2+(p-a_1)(p-a_0)z^{-1}=a_1a_0z+a_1^2+a_0^2+a_1a_0z^{-1}=A_1(z)A_1(z^{-1})$.

$A_4(z)A_4(z^{-1})=(p-a_0)(p-a_1)z+(p-a_0)^2+(p-a_1)^2+(p-a_0)(p-a_1)z^{-1}=a_0a_1z+a_0^2+a_0^2++a_0a_1z^{-1}=A_1(z)A_1(z^{-1})$.

Отсюда, $A_1(z)A_1(z^{-1})=A_2(z)A_2(z^{-1})=A_3(z)A_3(z^{-1})=A_4(z)A_4(z^{-1})$.

Аналогично, $B_1(z)B_1(z^{-1})=B_2(z)B_2(z^{-1})=B_3(z)B_3(z^{-1})=B_4(z)B_4(z^{-1})$

Следовательно, $A_l(z)A_l(z^{-1})+B_k(z)B_k(z^{-1})=A_1(z)A_1(z^{-1})+B_1(z)B_1(z^{-1})=1$ для $l=1,2,3,4$ и $k=1,2,3,4$.

Так как

$A_1(z)A_1(z^{-1})+B_1(z)B_1(z^{-1})=(a_1a_0+b_1b_0)z+a_1^2+a_0^2+b_1^2+b_0^2+(a_1a_0+b_1b_0)z^{-1}=1$, то $a_1a_0+b_1b_0=0$ и $a_1^2+a_0^2+b_1^2+b_0^2=1$. $C_1(z)C_1(z^{-1})=(p-a_1)a_0z+(p-a_1)^2+a_0^2+(p-a_1)a_0z^{-1}=(p-a_1a_0)z+a_1^2+a_0^2+(p-a_1a_0)z^{-1}$

Легко показать, что $C_1(z)C_1(z^{-1})=C_2(z)C_2(z^{-1})=C_3(z)C_3(z^{-1})=C_4(z)C_4(z^{-1})$.

Аналогично, $D_1(z)D_1(z^{-1})=(p-b_1b_0)z+b_1^2+b_0^2+(p-b_1b_0)z^{-1}$ и $D_1(z)D_1(z^{-1})=D_2(z)D_2(z^{-1})=D_3(z)D_3(z^{-1})=D_4(z)D_4(z^{-1})$.

Ясно,что $C_1(z)C_1(z^{-1})+D_1(z)D_1(z^{-1})=(p-a_1a_0-b_1b_0)z+a_1^2+a_0^2+b_1^2+b_0^2+(p-a_1a_0-b_1b_0)z^{-1}=$

$=(p-0)z+1+(p-0)z^{-1}=1$

Следовательно, для $l=1,2,3,4$ и $k=1,2,3,4$ имеем $C_l(z)C_l(z^{-1})+D_k(z)D_k(z^{-1})=C_1(z)C_1(z^{-1})+D_1(z)D_1(z^{-1})=1$.

Теорема 1 доказана.

Если a_0, $p-a_0$, a_1, $p-a_1$, b_0, $p-b_0$, b_1, $p-b_1$ – различные элементы поля GF_p, то из теоремы 1 следует, что зная пару многочленов $A_1(z)=a_0+a_1z$ и $B_1(z)=b_0+b_1z$ из $GF_p[z]$, для которых $A_1(z)A_1(z^{-1})+B_1(z)B_1(z^{-1})=1$, можно построить ещё 15 пар многочленов вида $A_l(z)$ и $B_k(z)$, для которых $A_l(z)A_l(z^{-1})+B_k(z)B_k(z^{-1})=1$, и 16 пар многочленов вида $C_l(z)$ и $D_k(z)$, для которых $C_l(z)C_l(z^{-1})+D_k(z)D_k(z^{-1})=1$. Если же среди указанных элементов поля GF_p встретятся одинаковые, то удастся построить меньше 32 пар интересующих нас многочленов.

Теорема 2. Если $a_0^2+b_0^2\neq 0$ и $\left(\frac{1}{a_0^2+b_0^2}-1\right)$ - квадратичный вычет по модулю p, то для

$$A_1(z)=a_0+\left(p-b_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}\right)z \text{ и } B_1(z)=b_0+a_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}z \quad (19)$$

из $GF_p[z]$ выполняется соотношение $A_1(z)A_1(z^{-1})+B_1(z)B_1(z^{-1})=1$, а для

$$C_1(z)=a_0+b_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}z \text{ и } D_1(z)=b_0+\left(p-a_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}\right)z \quad (20)$$

из $GF_p[z]$ выполняется соотношение $C_1(z)C_1(z^{-1})+D_1(z)D_1(z^{-1})=1$.

Доказательство.

Если $A(z)A(z^{-1})+B(z)B(z^{-1})=1$ для $A(z)=a_0+a_1z$ и $B(z)=b_0+b_1z$ из $GF_p[z]$, то $(a_1a_0+b_1b_0)z+a_1^2+a_0^2+b_1^2+b_0^2+(a_1a_0+b_1b_0)z^{-1}=1$.

Следовательно, $\begin{cases}a_1a_0+b_1b_0=0\\ a_1^2+a_0^2+b_1^2+b_0^2=1\end{cases}$. Отсюда, $a_1=p-\frac{b_0}{a_0}b_1$. Так как $a_1^2=\frac{b_0^2}{a_0^2}b_1^2$, то $\frac{b_0^2}{a_0^2}b_1^2+a_0^2+b_1^2+b_0^2=1$. Значит, $\frac{a_0^2+b_0^2}{a_0^2}b_1^2=1-(a_0^2+b_0^2)$. Если $a_0^2+b_0^2\neq 0$, то $b_1^2=\frac{a_0^2}{a_0^2+b_0^2}-a_0^2$ или $b_1^2=a_0^2\left(\frac{1}{a_0^2+b_0^2}-1\right)$. Если $\left(\frac{1}{a_0^2+b_0^2}-1\right)$ квадратичный вычет по модулю p [18], то получаем $b_1=a_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}$ или $b_1=p-a_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}$. Откуда, $a_1=p-b_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}$ или $a_1=b_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}$.

Таким образом, имеем две пары многочленов из $GF_p[z]$, удовлетворяющие поставленным условиям:

$$A_1(z)=a_0+\left(p-b_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}\right)z \text{ и } B_1(z)=b_0+a_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}z;$$

$$C_1(z)=a_0+b_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}z \text{ и } D_1(z)=b_0+\left(p-a_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}\right)z.$$

Теорема 2 доказана.

Покажем на примере применение теорем 1 и 2 для нахождения вейвлетных фильтров 3-го порядка над GF_p.

Пример. Рассмотрим поле GF_{13}. Квадратичными вычетами по модулю 13 являются числа 1, 3, 4, 9, 10, 12, так как $1\equiv 1^2 \bmod 13$, $3\equiv 4^2 \bmod 13$, $4\equiv 2^2 \bmod 13$, $9\equiv 3^2 \bmod 13$, $10\equiv 6^2 \bmod 13$, $12\equiv 5^2 \bmod 13$. Условию теоремы 2 удовлетворяют, например, числа $a_0=3$ и $b_0=5$, так как $a_0^2+b_0^2=3^2+5^2\equiv 8 \bmod 13\neq 0$ и $\frac{1}{a_0^2+b_0^2}-1=8^{-1}-1\equiv 4 \bmod 13$ квадратичный вычет по модулю 13. По формуле (19) имеем:

$$A(z)=a_0+\left(p-b_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}\right)z=3+3z \text{ и } B(z)=b_0+a_0\sqrt{\frac{1-a_0^2-b_0^2}{a_0^2+b_0^2}}z=5+6z.$$

По теореме 1 получаем еще 15 пар линейных двучленов над полем GF_{13}, удовлетворяющих условию (17): $3+3z$ и $6+5z$; $3+3z$ и $8+7z$; $3+3z$ и $7+8z$; $10+10z$ и $5+6z$; $10+10z$ и $6+5z$; $10+10z$ и $8+7z$; $10+10z$ и $7+8z$; $3+10z$ и $5+7z$; $3+10z$ и $7+5z$; $3+10z$ и $8+6z$; $3+10z$ и $6+8z$; $10+3z$ и $5+7z$; $10+3z$ и $7+5z$; $10+3z$ и $8+6z$; $10+3z$ и $6+8z$.

На рисунке 2 схематично показан принцип расчета коэффициентов при построении вейвлетных фильтров третьего порядка в поле GF_{13} из двучленов $A(z)=3+3z$ и $B(z)=5+6z$.

Таким образом, построение вейвлетных фильтров третьего порядка над полем GF_p сводится к проверке простого условия для элементов поля на квадратичный вычет по модулю. Это улучшает результат из [9], в котором для построения таких фильтров предлагается использовать вычислительно сложные модификации алгоритма Берлекэмпа для разложения на множители многочленов из GF_p. Кроме того, доказанные теоремы 1 и 2 позволяют строить все возможные вейвлетные фильтры третьего порядка над полем GF_p.

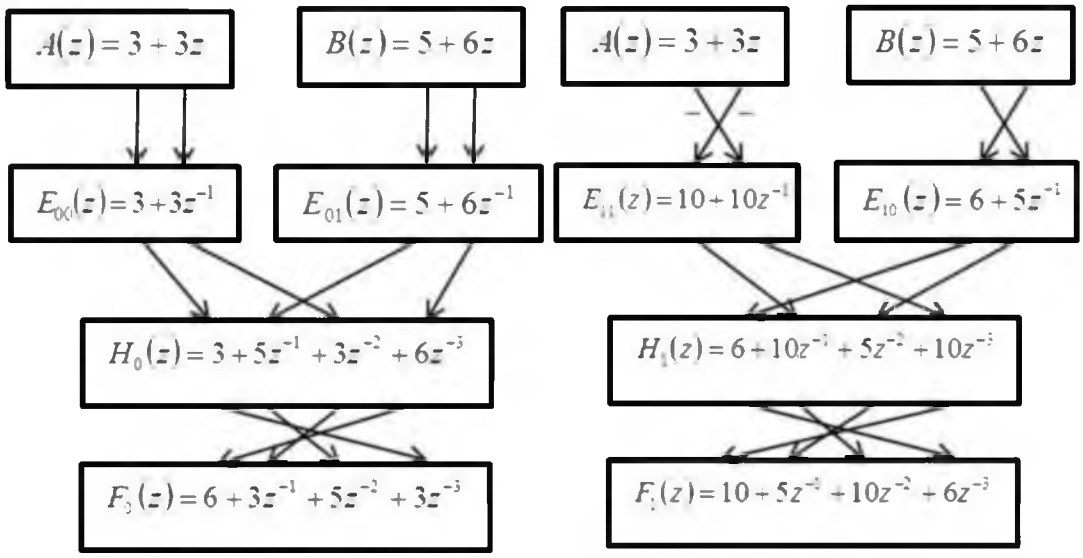


Рис. 2. Схема расчета коэффициентов вейвлетных фильтров над полем GF_{13}

Fig. 2. Computing scheme for coefficients of wavelet filters over GF_{13}

Заключение

В работе исследован метод построения вейвлетных фильтров третьего порядка над полями GF_p. Использование теорем 1 и 2 позволяет значительно сократить время построения вейвлетных фильтров конечного поля по сравнению с известными подходами, основанными на вычислительно сложном алгоритме Берлекэмпа. Кроме того, применение доказанных теорем позволяет строить все возможные вейвлетные фильтры третьего порядка над полем GF_p.

Перспективным направлением дальнейших исследований является исследование практического применения вейвлетных фильтров третьего порядка для задач ЦОС, а также в кодировании и шифровании. Кроме того, интерес представляет разработка быстрых алгоритмов проектирования вейвлетных фильтров другого порядка над GF_p а также фильтров над полями GF_{p^n}.

Благодарности

Работа выполнена при финансовой поддержке РФФИ, грант № 14-07-31004-мол-а.

Список литературы
References

1. Vigila S.A.M.C., Muneeswaran K., Antony W.T.B.A. Biometric security system over finite field for mobile applications // IET Information Security. 2015. V. 9. No. 2. P. 119-126.

Vigila S.A.M.C., Muneeswaran K., Antony W.T.B.A. Biometric security system over finite field for mobile applications // IET Information Security. 2015. V. 9. No. 2. P. 119-126.

2. Cooklev T., Nishihara A., Sablatash M. Theory of filter banks over finite fields // Proc. IEEE Asia-Pacific Conf. On Circuits and Systems, Taipei, 1994. P. 260-265.

Cooklev T., Nishihara A., Sablatash M. Theory of filter banks over finite fields // Proc. IEEE Asia-Pacific Conf. On Circuits and Systems, Taipei, 1994. P. 260-265.

3. Jeronimo da Silva G., de Souza R.M.C. Design method for two-channel cyclic filter banks over fields of characteristic two // IET Electronics Letters. 2009. V. 45. No. 6. P. 332-334.

Jeronimo da Silva G., de Souza R.M.C. Design method for two-channel cyclic filter banks over fields of characteristic two // IET Electronics Letters. 2009. V. 45. No. 6. P. 332-334.

4. Usevitch B.E. A tutorial on modern lossy wavelet image compression: foundations of JPEG 2000 // IEEE Signal Processing Magazine. 2001. V. 18. No. 5. P. 22-35.

Usevitch B.E. A tutorial on modern lossy wavelet image compression: foundations of JPEG 2000 // IEEE Signal Processing Magazine. 2001. V. 18. No. 5. P. 22-35.

5. Zhang D., Bao P., Xiaolin Wu. Multiscale LMMSE-based image denoising with optimal wavelet selection // IEEE Transactions on Circuits and Systems for Video Technology. 2005. V. 15. No. 4. P. 469-481.

Zhang D., Bao P., Xiaolin Wu. Multiscale LMMSE-based image denoising with optimal wavelet selection // IEEE Transactions on Circuits and Systems for Video Technology. 2005. V. 15. No. 4. P. 469-481.

6. Shukla K.K., Tiwari A.K. Efficient Algorithms for Discrete Wavelet Transform With Applications to Denoising and Fuzzy Inference Systems Series. SpringerBriefs in Computer Science, 2013.

Shukla K.K., Tiwari A.K. Efficient Algorithms for Discrete Wavelet Transform With Applications to Denoising and Fuzzy Inference Systems Series. SpringerBriefs in Computer Science, 2013.

7. Fu-Chiang Tsui, Li C.-C., Mingui Sun, Sclabassi R.J. A comparative study of two biorthogonal wavelet transforms in time series prediction // Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics, Computational Cybernetics and Simulation, Orlando, 1997. V. 2. P. 1791-1796.

Fu-Chiang Tsui, Li C.-C., Mingui Sun, Sclabassi R.J. A comparative study of two biorthogonal wavelet transforms in time series prediction // Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics, Computational Cybernetics and Simulation, Orlando, 1997. V. 2. P. 1791-1796.

8. Brechet L., Lucas M.-F., Doncarli C., Farina D. Compression of Biomedical Signals With Mother Wavelet Optimization and Best-Basis Wavelet Packet Selection // IEEE Transactions on Biomedical Engineering. 2007. V. 54. No. 12. P. 2186-2192.

Brechet L., Lucas M.-F., Doncarli C., Farina D. Compression of Biomedical Signals With Mother Wavelet Optimization and Best-Basis Wavelet Packet Selection // IEEE Transactions on Biomedical Engineering. 2007. V. 54. No. 12. P. 2186-2192.

9. Fekri F., Mersereau R.M., Shafer R.W. Theory of wavelet transform over finite fields // Proc. IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, Phoenix, 1999. V. 3. P. 1213-1216.

Fekri F., Mersereau R.M., Shafer R.W. Theory of wavelet transform over finite fields // Proc. IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, Phoenix, 1999. V. 3. P. 1213-1216.

10. Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W. Block error correcting codes using finite-field wavelet transforms // IEEE Transactions on Signal Processing. 2006. V. 54. No. 3. P. 991-1004.

Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W. Block error correcting codes using finite-field wavelet transforms // IEEE Transactions on Signal Processing. 2006. V. 54. No. 3. P. 991-1004.

11. Sartipi M., Delgosha F., Fekri F. Two-Dimensional Half-Rate Codes Using Two-Dimensional Finite-Field Filter Banks // IEEE Transactions on Signal Processing. 2007. V. 55. No. 12. P. 5846-5853.

Sartipi M., Delgosha F., Fekri F. Two-Dimensional Half-Rate Codes Using Two-Dimensional Finite-Field Filter Banks // IEEE Transactions on Signal Processing. 2007. V. 55. No. 12. P. 5846-5853.

12. Delgosha F., Fekri F. Stream cipher using finite-field wavelets // Proc. IEEE Int. Conf. On Acoustics, Speech, and Signal Processing. 2005. V. 5. P. 689-692.

Delgosha F., Fekri F. Stream cipher using finite-field wavelets // Proc. IEEE Int. Conf. On Acoustics, Speech, and Signal Processing. 2005. V. 5. P. 689-692.

13. Delgosha F., Fekri F. Public-key cryptography using paraunitary matrices // IEEE Transactions on Signal Processing. 2006. V. 54. No. 9. P. 3489-3504.

Delgosha F., Fekri F. Public-key cryptography using paraunitary matrices // IEEE Transactions on Signal Processing. 2006. V. 54. No. 9. P. 3489-3504.

14. Chervyakov N.I., Lyakhov P.A., Babenko M.G. Digital filtering of images in a residue number system using finite-field wavelets // Automatic Control and Computer Sciences. 2014. V. 48. No. 3. P. 180-189.

Chervyakov N.I., Lyakhov P.A., Babenko M.G. Digital filtering of images in a residue number system using finite-field wavelets // Automatic Control and Computer Sciences. 2014. V. 48. No. 3. P. 180-189.

15. Vaidyanathan P.P. Multirate Systems and Filter Banks. Englewood Cliffs, NJ: Prentice-Hall, 1993.

Vaidyanathan P.P. Multirate Systems and Filter Banks. Englewood Cliffs, NJ: Prentice-Hall, 1993.

16. Червяков, Н.И. Реализация многофазных фильтров в системе остаточных классов / Н.И. Червяков, П.А. Ляхов // Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. – 2011. . – №13(108). – Вып. 19/1. – С. 204-210.

Chervjakov, N.I. Realizacija mnogofaznyh fil'trov v sisteme ostatochnyh klassov / N.I. Chervjakov, P.A. Ljahov // Nauchnye vedomosti BelGU. Ser. Istorija. Politologija. Jekonomika. Informatika. – 2011. . – №13(108). – Vyp. 19/1. – S. 204-210.

17. Phoong S., Vaidyanathan P.P. Paraunitary filter banks over finite fields // IEEE Transactions on Signal Processing. 1997. V. 45. No. 6. P. 1443-1457.

Phoong S., Vaidyanathan P.P. Paraunitary filter banks over finite fields // IEEE Transactions on Signal Processing. 1997. V. 45. No. 6. P. 1443-1457.

18. Montgomery H.L., Vaughan R.C. Multiplicative number theory I: Classical Theory. Cambridge University Press, 2006, 572 p.

Montgomery H.L., Vaughan R.C. Multiplicative number theory I: Classical Theory. Cambridge University Press, 2006, 572 p.