ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

ПОСТРОЕНИЕ В КОНЕЧНЫХ ПОЛЯХ ВЕЙВЛЕТНЫХ ФИЛЬТРОВ ТРЕТЬЕГО ПОРЯДКА С ИСПОЛЬЗОВАНИЕМ ДВУЧЛЕНОВ СПЕЦИАЛЬНОГО ВИДА

Червяков Н.И., Ляхов П.А., Семенова Н.Ф.
Северо-Кавказский Федеральный университет, Ставрополь, РФ
E-mail: k-fmf-primath@stavsu.ru

В работе исследован метод построения вейвлетных фильтров третьего порядка над конечными полями с использованием двучленов специального вида. Использование предложенного подхода позволяет значительно сократить время построения вейвлетных фильтров конечного поля по сравнению с известными методами, основанными на применении алгоритма Берлекэмпа или его модификаций.

Ключевые слова: цифровая обработка сигналов, вейвлет-преобразование, алгоритм, конечное поле.

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. 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 [1].

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 [2], очистки от шума [3-4], анализа временных рядов [5], обработки данных в медицине [6] 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 [7]. Предложены методы и алгоритмы кодирования [8-9], криптографической защиты информации [10-11] и обработки изображений [12] 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 [7]. В данной статье исследованы вейвлетные фильтры третьего порядка над конечными полями, построенные с использованием линейных двучленов специального вида. Представлены алгоритмы построения таких фильтров и приведены примеры.

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 осно-

вана 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

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

Если обозначить через $\overline{span\{\alpha_1, \alpha_2, ..., \alpha_n\}}$ линейную оболочку над векторами $\{\alpha_1, \alpha_2, ..., \alpha_n\}$, то материнский вейвлет $\psi(x)$ и скейлинг-функция $\varphi(x)$, определяющие вейвлет-преобразование в конечном поле $GF(p)$, должны удовлетворять следующим соотношениям [7]

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

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

и, кроме того, условиям ортонормированности базиса

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

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

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

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

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

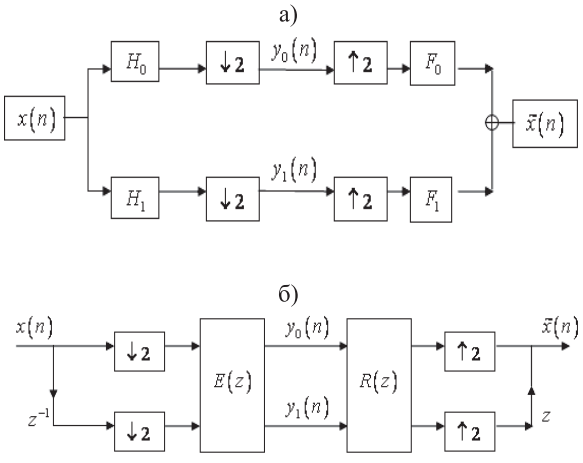

Рис. 1. Двухканальный набор фильтров дискретного вейвлет-преобразования: а) обычное изображение, б) изображение в многофазной форме.

На практике вейвлет-преобразование реализуется при помощи наборов фильтров. На рис. 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 (см. рис. 1б) [13]. С таким набором фильтров ассоциирована матрица

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

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 [7]. Для того, чтобы набор фильтров обладал свойством точного восстановления сигнала, необходимо, чтобы матрица $E(z)$ была параунитарной, то есть выполнялось соотношение

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

где I – единичная матрица [14]. Необходимым и достаточным условием точного восстановления сигнала является выполнение соотношения

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

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:

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

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

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

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

Фильтры H_0 и H_1 можно найти по формулам

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

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

Фильтры F_0 и F_1 находятся из условий точного восстановления сигнала [1]

$$F_0(z)=H_1(-z),\ F_1(z)=-H_0(-z). \quad (16)$$

Построение набора фильтров на рис. 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

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

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

$$\begin{gathered} a_i=e_{0i};\\ e_{1i}=0, \text{ для } i=0\ \ldots\ N-M-1;\\ b_i=e_{1(N-M+i)}, \text{ для } i=0\ \ldots\ M. \end{gathered} \quad (18)$$

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 многочленов $A(z)$ и $B(z)$ вида $1+\alpha z$ 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 $A(z)=1+az$ и $B(z)=1+bz$ из $GF_p[z]$, для которых выполняется соотношение $A(z)A(z^{-1})+B(z)B(z^{-1})=1$. Сформулируем и докажем вспомогательное утверждение, которое будет необходимо нам для решения поставленной задачи.

Утверждение 1. Число $\frac{p-1}{2}$ является квадратичным вычетом по модулю p для простых чисел вида $p=8k+1$ и $p=8k+3$, а для простых чисел вида $p=8k+5$ и $p=8k+7$ является квадратичным невычетом по модулю p.

Доказательство. Пусть простое число p имеет вид $p=8k+1$. Согласно основной теореме арифметики, любое целое число $k\geq 1$ представляется в виде

$$k=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}, \quad (19)$$

где $p_1,\ldots,p_n$ различные простые числа, а $\alpha_i\geq 0, \alpha_i\in Z$. Равенство (19) можно переписать в виде $k=2^m$, $(m\geq 0)$ или $k=2^m(2l+1)$, $(m\geq 0,\ l\geq 1)$. Следовательно, $p=2^{m+3}+1$ или $p=2^{m+3}(2l+1)+1=2^{m+4}l+2^{m+3}+1$. Тогда $\frac{p-1}{2}=2^{m+2}$ или $\frac{p-1}{2}=2^{m+2}(2l+1)$. Рассмотрим каждый из этих случаев.

1. Пусть $\frac{p-1}{2}=2^{m+2}$. Если $m+2$ четное число, то $\frac{p-1}{2}$ является квадратичным вычетом по модулю p. Если $m+2$ нечетное число, то символ Лежандра $\left(\frac{2^{m+2}}{p}\right)=\left(\frac{2}{p}\right)=1$, так как $p=8k+1$ [15]. Следовательно, $\frac{p-1}{2}$ является квадратичным вычетом по модулю p и при $m+2$ нечетном.

2. Пусть $\frac{p-1}{2}=2^{m+2}(2l+1)$. Тогда символ Якоби [16] равен

$$\left(\frac{2^{m+2}(2l+1)}{p}\right)=\left(\frac{2^{m+2}}{p}\right)\left(\frac{2l+1}{2^{m+3}(2l+1)+1}\right)=$$
$$=(-1)^{2^{m+2}(2l+1)l}\left(\frac{1}{2l+1}\right)=1,$$

учитывая, что $\left(\frac{2^{m+2}}{p}\right)=1$ при $p=8k+1$. Следовательно, и в этом случае $\frac{p-1}{2}$ является квадратичным вычетом по модулю p.

Таким образом, $\frac{p-1}{2}$ является квадратичным вычетом по модулю p для любых простых чисел вида $p=8k+1$.

Если простое число p имеет вид $p=8k+3$, то $\frac{p-1}{2}=4k+1$. Символ Якоби для этого случая равен $\left(\frac{4k+1}{8k+3}\right)=(-1)^{2k(4k+1)}\left(\frac{1}{4k+1}\right)=1$.

Если простое число p имеет вид $p=8k+5$, то $\frac{p-1}{2}=4k+1$. Символ Якоби для этого случая равен $\left(\frac{4k+2}{8k+5}\right)=\left(\frac{2}{8k+5}\right)\left(\frac{2k+1}{8k+5}\right)=$ $=-(-1)^{k(4k+2)}\left(\frac{1}{2k+1}\right)=-1$, учитывая что 2 является квадратичным невычетом по модулю $p=8k+5$.

Если простое число p имеет вид $p=8k+7$, то $\frac{p-1}{2}=4k+3$. Символ Якоби для этого случая равен $\left(\frac{4k+3}{8k+7}\right)=(-1)^{(2k+1)(4k+3)}\left(\frac{1}{4k+3}\right)=-1$.

Обобщая все результаты, описанные выше, заключаем, что $\frac{p-1}{2}$ является квадратичным вычетом по модулю p для простых чисел вида $p=8k+3$ и квадратичным невычетом по модулю p для простых чисел вида $p=8k+5$ и $p=8k+7$. Утверждение доказано.

Используя доказанное утверждение, сформулируем и докажем следующую теорему.

Теорема 1. Для простых чисел вида $p=8k+5$ и $p=8k+7$ не существует пар многочленов $A(z)=1+az$ и $B(z)=1+bz$ из $GF_p[z]$, таких, что $A(z)A(z^{-1})+B(z)B(z^{-1})=1$. Для простых чисел вида $p=8k+1$ и $p=8k+3$ многочлены

$$A(z)=1+\sqrt{\frac{p-1}{2}}z \text{ и } B(z)=1+\left(p-\sqrt{\frac{p-1}{2}}\right)z \quad (20)$$

из $GF_p[z]$ обладают свойством $A(z)A(z^{-1})+B(z)B(z^{-1})=1$.

Доказательство. Если $A(z)=1+az$ и $B(z)=1+bz$, то $A(z)A(z^{-1})=az+a^2+1+az^{-1}$, а $B(z)B(z^{-1})=bz+b^2+1+bz^{-1}$. Следовательно,

$$A(z)A(z^{-1})+B(z)B(z^{-1})=$$
$$=(a+b)z+a^2+b^2+2+(a+b)z^{-1}.$$

Если $A(z)A(z^{-1})+B(z)B(z^{-1})=1$, то

$$\begin{cases}a+b=0\\a^2+b^2+2=1\end{cases} \text{ или } \begin{cases}b=p-a\\a^2+b^2+1=0\end{cases}.$$

Из равенства $b=p-a$ следует, что $b^2=a^2$. С учетом равенства $a^2+b^2+1=0$ имеем, что $2a^2=p-1$ или $a^2=\frac{p-1}{2}$. Последнее равенство возможно в том и только в том случае, если $\frac{p-1}{2}$ является квадратичным вычетом по модулю p.

Используя утверждение 1, заключаем, что если $p=8k+5$ и $p=8k+7$, то многочлены $A(z)=1+az$ и $B(z)=1+bz$ из $GF_P[z]$, для которых $A(z)A(z^{-1})+B(z)B(z^{-1})=1$ не существуют. Если же $p=8k+1$ и $p=8k+3$, то многочлены $A(z)=1+az$ и $B(z)=1+bz$ из $GF_p[z]$, для которых $A(z)A(z^{-1})+B(z)B(z^{-1})=1$, существуют. В этом случае имеем две пары чисел a и b, удовлетворяющие поставленному требованию: $a_1=\sqrt{\frac{p-1}{2}}$ и $b_1=p-\sqrt{\frac{p-1}{2}}$, а также $a_2=p-\sqrt{\frac{p-1}{2}}$ и $b_2=\sqrt{\frac{p-1}{2}}$.

Окончательно (с учетом порядка следования) имеем пару многочленов $A(z)=1+\sqrt{\frac{p-1}{2}}z$ и $B(z)=1+\left(p-\sqrt{\frac{p-1}{2}}\right)z$, удовлетворяющих соотношению $A(z)A(z^{-1})+B(z)B(z^{-1})=1$ для $p=8k+1$ и $p=8k+3$. Теорема доказана.

Рассмотрим на примере процедуру построения вейвлетных фильтров третьего порядка с использованием теоремы 1.

Пример 1. С помощью теоремы 1 найдем многочлены $A(z)=1+az$ и $B(z)=1+bz$ из $GF_n[z]$, для которых выполняется соотношение $A(z)A(z^{-1})+B(z)B(z^{-1})=1$. Полученные многочлены приведены в таблице 1.

Таблица 1. Многочлены $A(z)$ и $B(z)$ из $GF_n[z]$

$p=8k+r$	$A(z)=1+az$	$B(z)=1+bz$
$3=8\cdot0+3$	$1+z$	$1+2z$
$5=8\cdot0+5$	не существует	не существует
$7=8\cdot0+7$	не существует	не существует
$11=8\cdot1+3$	$1+4z$	$1+7z$
$13=8\cdot1+5$	не существует	не существует
$17=8\cdot2+1$	$1+5z$	$1+12z$
$19=8\cdot2+3$	$1+3z$	$1+16z$

Обратим внимание, что если число p имеет вид $p=2c^2+1$, например $p=3,19,73,163,883,...$, то в этом случае $\frac{p-1}{2}=c^2$ и многочлен $A(z)=1+az=1+cz$. В таблице 1 этот случай встречается при $p=3=2\cdot1^2+1$ и при $p=19=2\cdot3^2+1$.

Построим теперь вейвлетный фильтр в поле $GF(19)$ с использованием многочленов $A(z)=1+3z$ и $B(z)=1+16z$. Процесс последовательного построения многочленов $E_{ij}(z)$, $i=0,1$, $j=0,1$ из формул (11)-(13), а также анализирующих (H_0 и H_1) и синтезирующих (F_0 и F_1) фильтров схематично изображен на рис. 2.

Многочлены $A(z)$ и $B(z)$ из теоремы 1 могут быть использованы для построения других пар многочленов, обладающих свойством $A(z)A(z^{-1})+B(z)B(z^{-1})=1$.

Теорема 2. Пусть $A_1(z)=1+az$, $A_2(z)=a+z$, $A_3(z)=(p-1)+(p-a)z$, $A_4(z)=(p-a)+(p-1)z$, $B_1(z)=1+bz$, $B_2(z)=b+z$, $B_3(z)=(p-1)+(p-b)z$, $B_4(z)=(p-b)+(p-1)z$. Тогда если для многочленов $A_l(z)$ и $B_l(z)$ из $GF_n[z]$ выполняется соотношение $A_1(z)A_1(z^{-1})+B_1(z)B_1(z^{-1})=1$, то для $A_l(z)$ и $B_k(z)$, где $k=1,2,3,4$ и $l=1,2,3,4$ выполняется соотношение $A_l(z)A_l(z^{-1})+B_k(z)B_k(z^{-1})=1$.

Доказательство. Преобразуем выражения $A_1(z)A_1(z^{-1})$, $A_2(z)A_2(z^{-1})$ и $A_3(z)A_3(z^{-1})$:

$$A_1(z)A_1(z^{-1}) = az + 1 + a^2 + az^{-1} = A_2(z)A_2(z^{-1});$$

$$A_3(z)A_3(z^{-1}) = (p-1)(p-a)z +$$

$$+ (p-1)^2 + (p-a)^2 + (p-1)(p-a)z^{-1} =$$

$$= az + 1 + a^2 + az^{-1} = A_1(z)A_1(z^{-1}).$$

Аналогично доказывается, что $A_4(z)A_4(z^{-1}) = A_1(z)A_1(z^{-1})$. Из этих равенств следует, что $A_l(z)A_l(z^{-1}) = az + 1 + a^2 + az^{-1}$ для $l = 1,2,3,4$. Аналогично доказывается, что $B_k(z)B_k(z^{-1}) = bz + 1 + b^2 + bz^{-1}$ для $k = 1,2,3,4$. Так как $A_1(z)A_1(z^{-1}) + B_1(z)B_1(z^{-1}) = 1$, то и $A_l(z)A_l(z^{-1}) + B_k(z)B_k(z^{-1}) = 1$ для $A_l(z)$ и $B_k(z)$, где $k = 1,2,3,4$ и $l = 1,2,3,4$. Теорема доказана.

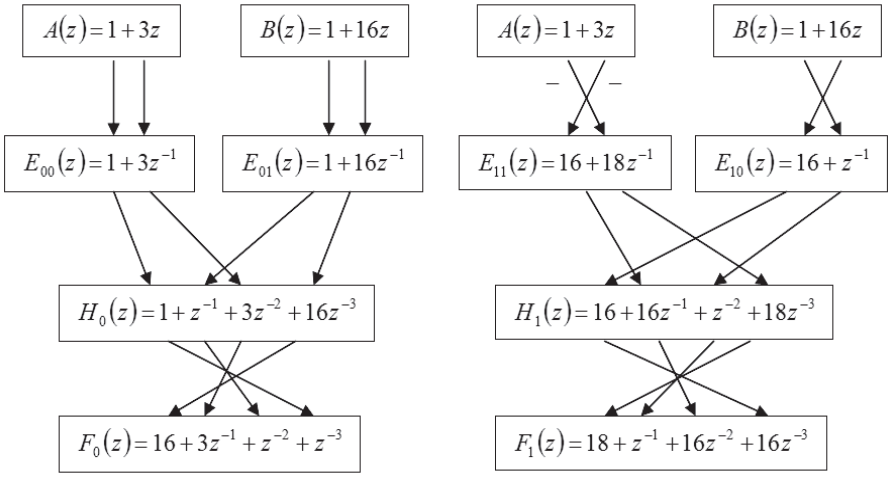

Рис. 2. Схема построения анализирующих (H_0 и H_1) и синтезирующих (F_0 и F_1) вейвлетных фильтров из многочленов $A(z)$ и $B(z)$ в поле $GF(19)$

Теорема 2 дает возможность, имея пару многочленов $A_1(z) = 1 + az$ и $B_1(z) = 1 + bz$, для которых $A_1(z)A_1(z^{-1}) + B_1(z)B_1(z^{-1}) = 1$, построить с ее помощью еще 15 пар многочленов $A_l(z)$ и $B_k(z)$, для которых $A_l(z)A_l(z^{-1}) + B_k(z)B_k(z^{-1}) = 1$.

Пример 2. В примере 1 было найдено, что в $GF(19)$ для $A_1(z) = 1 + 3z$ и $B_1(z) = 1 + 16z$ выполняется соотношение $A_1(z)A_1(z^{-1}) + B_1(z)B_1(z^{-1}) = 1$. Используя теорему 2, получим, что $A_2(z) = 3 + z$, $A_3(z) = 18 + 16z$, $A_4(z) = 16 + 18z$, $B_2(z) = 16 + z$, $B_3(z) = 18 + 3z$, $B_4(z) = 3 + 18z$. Комбинируя разными способами $A_l(z)$ и $B_k(z)$, где $k = 1,2,3,4$ и $l = 1;2;3;4$, получим 16 пар многочленов, удовлетворяющих условию $A_l(z)A_l(z^{-1}) + B_k(z)B_k(z^{-1}) = 1$. Каждая из таких пар может быть использована для построения вейвлетных фильтров третьего порядка над $GF(19)$ аналогично схеме, показанной в примере 1.

Заключение

В работе исследован метод построения вейвлетных фильтров третьего порядка над полями $GF(p)$ с использованием двучленов специального вида. Показано, как предложенный подход может быть использован для построения вейвлетных фильтров над полями $GF(p)$ при $p = 8k + 1$ и $p = 8k + 3$. Использование теорем 1 и 2 позволяет значительно сократить время построения вейвлетных фильтров конечного поля по сравнению с известными подходами, основанными на примененииии алгоритма Берлекэмпа или его модификаций.

Дальнейшая работа в данном направлении может быть направлена на исследование практического применения вейвлетных фильтров третьего порядка для задач ЦОС, а также в кодировании и шифровании. Перспективным подходом к использованию вейвлетов над полями $GF(p)$ является использование модулярной арифметики в системе остаточных классов с простыми модулями.

Благодарности

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

Литература

1. 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.

2. Usevitch B.E. A tutorial on modern lossy wavelet image compression: foundations of JPEG 2000 // IEEE Signal Processing Magazine. V.18, No.5, 2001. – P. 22-35.
3. Zhang D., Bao P., Xiaolin Wu. Multiscale LMMSE-based image denoising with optimal wavelet selection // IEEE Transactions on Circuits and Systems for Video Technology. V.15, No.4, 2005. – P. 469-481.
4. 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.
5. 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. V.2, 1997. – P. 1791-1796.
6. 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. V.54, No.12, 2007. – P. 2186-2192.
7. 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. V.3, 1999. – P. 1213-1216.
8. 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, 2007. – P. 5846-5853.
9. 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. V.54, No.3, 2006. – P. 991-1004.
10. Delgosha F., Fekri F. Stream cipher using finite-field wavelets // Proc. IEEE Int. Conf. On Acoustics, Speech, and Signal Processing. V.5, 2005. – P. 689-692.
11. Delgosha F., Fekri F. Publickey cryptography using paraunitary matrices // IEEE Transactions on Signal Processing. V.54, No.9, 2006. – P. 3489-3504.
12. 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. V.48, No.3, 2014. – P. 180-189.
13. Vaidyanathan P.P. Multirate Systems and Filter Banks. Englewood Cliffs, NJ: Prentice-Hall, 1993.
14. Phoong S., Vaidyanathan P.P. Paraunitary filter banks over finite fields // IEEE Transactions on Signal Processing. V.45, No.6, 1997. – P. 1443-1457.
15. Виноградов И.М. Основы теории чисел. СПб.: Лань, 2009. – 176 с.
16. Сизый С.В. Лекции по теории чисел. М.: Физматлит, 2007. – 192 с.

Получено 15.01.2015

Червяков Николай Иванович, Заслуженный деятель науки РФ, д,т.н., профессор, заведующий Кафедрой прикладной математики и математического моделирования (ПМ и ММ) Северо-Кавказского Федерального университета (СКФУ). Тел. 8-865-235-48-61. E-mail: k-fmf-primath@stavsu.ru

Ляхов Павел Алексеевич, к.ф-м.н., доцент Кафедры ПМ и ММ СКФУ. Тел. 8-962-028-72-14. E-mail: ljahov@mail.ru

Семенова Наталия Федоровна, к.ф-м.н., доцент Кафедры высшей алгебры и геометрии СКФУ. Тел. 8-962-449-62-14.

DESIGN OF THIRD ORDER WAVELET FILTERS OVER FINITE FIELDS BY USING SPECIAL BINOMIALS

Chervyakov N.I., Lyakhov P.A., Semyonova N.F.
North-Caucasus Federal University, Stavropol, Russian Federation
E-mail: k-fmf-primath@stavsu.ru

This work concerns on research of method for design of third order wavelet filters in finite fields by using special binomials. Finite field wavelets have many advantages in comparison with real or complex field wavelets. The main two of them are high rate data processing and lack of rounding error. However, the main disadvantage of finite field wavelets is high complexity of design based on using of polynomial properties and para-unitary matrixes over finite fields. The most known methods for design of finite filed wavelets utilize computing system based on Berlekamp algorithm or its modifications for polynomial expansion over finite field. We propose new method for design of third

order wavelet filters over finite field. Presented method is based on using of special type binomials over those fields. We derived and proved analytical formulas for filter coefficient and demonstrated some examples.

Keywords: *digital signal processing, wavelet transform, algorithm, finite field.*

DOI: 10.18469/ikt.2015.13.2.01.

Chervyakov Nikolay Ivanovich, Doctor of Technical Science, Professor, the Head of Department of Applied Mathematics and Mathematical Modeling, North-Caucasus Federal University, Stavropol, Russian Federation. Tel.: +78652354861. E-mail: k-fmf-primath@stavsu.ru.
Lyakhov Pavel Alekseyevich, PhD in Physico-Mathematical Sciences, Assistant Professor of the Department of Applied Mathematics and Mathematical Modeling, North-Caucasus Federal Univer-sity, Stavropol, Russian Federation. Tel.: +79620287214. E-mail: ljahov@mail.ru
Semyonova Nataliya Fyodorovna, PhD in Physico-Mathematical Sciences, Assistant Professor of the Department of Higher Algebra and Geometry, North-Caucasus Federal University, Stavropol, Russian Federation. Tel.: +79624496214

References

1. Cooklev T., Nishihara A., Sablatash M. Theory of filter banks over finite fields. *Proc. IEEE Asia-Pacific Conf. On Circuits and Systems, Taipei,* 1994. pp. 260-265. doi: 10.1109/APCCAS.1994.514560.
2. Usevitch B.E. A tutorial on modern lossy wavelet image compression: foundations of JPEG 2000. *IEEE Signal Processing Magazine, 2001,* vol. 18, no. 5, pp. 22-35. doi: 10.1109/79.952803.
3. 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, vol. 15, no. 4, pp. 469-481. doi: 10.1109/TCSVT.2005.844456.
4. Shukla K.K., Tiwari A.K. *Efficient Algorithms for Discrete Wavelet Transform With Applications to Denoising and Fuzzy Inference Systems Series.* Springer-Verlag London, 2013. 91 p. doi: 10.1007/978-1-4471-4941-5.
5. 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 Cyber-netics, Computational Cybernetics and Simulation,* Orlando, 1997, vol. 2, pp. 1791-1796. doi: 10.1109/ICSMC.1997.638292.
6. 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 Bio-medical Engineering,* 2007, vol. 54, no. 12, pp. 2186-2192. doi: 10.1109/TBME.2007.896596.
7. 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, vol. 3, pp. 1213-1216. doi: 10.1109/ICASSP.1999.756196.
8. Sartipi M., Delgosha F., Fekri F. Two-Dimensional Half-Rate Codes Using Two-Dimensional Finite-Field Filter Banks. *IEEE Transactions on Signal Processing, 2007,* vol. 55, no. 12, pp. 5846-5853. doi: 10.1109/TSP.2007.899388.
9. 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, vol. 54, no. 3, pp. 991-1004. doi: 10.1109/TSP.2005.863011.
10. Delgosha F., Fekri F. Stream cipher using finite-field wavelets. *Proc. IEEE Int. Conf. On Acoustics, Speech, and Signal Processing,* 2005, vol. 5, pp. 689-692. doi: 10.1109/ICASSP.2005.1416397.
11. Delgosha F., Fekri F. Public-key cryptography using para-unitary matrices. *IEEE Transactions on Signal Processing,* 2006, vol. 54, no. 9, pp. 3489-3504. doi: 10.1109/TSP.2006.877670.
12. 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, vol. 48, no. 3, pp. 180-189. doi: 10.3103/S0146411614030031.
13. Vaidyanathan P.P. *Multirate Systems and Filter Banks*. Englewood Cliffs, NJ, Prentice-Hall, 1993.
14. Phoong S., Vaidyanathan P.P. Para-unitary filter banks over finite fields. *IEEE Transactions on Signal Processing,* 1997, vol. 45, no. 6, pp. 1443-1457. doi: 10.1109/78.599956
15. Vinogradov I.M. *Osnovy teorii chisel* [Foundations of Numbers Theory]. St. Petersburg, Lan' Publ., 2009. 176 p.
16. Sizyi S.V. *Lektsii po teorii chisel* [Lectures on Numbers Theory]. Moskow, FIZMATLIT Publ., 2007. 192 p.

Received 15.01.2015