АВТОМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА. – 2012. – No.5. – С.48-57.

АЛГЕБРАИЧЕСКИЙ МЕТОД СИНТЕЗА БЫСТРЫХ АЛГОРИТМОВ ДИСКРЕТНОГО КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ ПРОИЗВОЛЬНОГО РАЗМЕРА

М.И. ВАШКЕВИЧ, *аспирант*
А.А. ПЕТРОВСКИЙ, *доктор технических наук, профессор*
кафедра «Электронных вычислительных средств»
Белорусского государственного университета информатики и радиоэлектроники
ул. П. Бровки 6, 220013 Минск, Беларусь
E-mail: vashkevich@bsuir.by, palex@bsuir.by

Предлагается алгебраический метод синтеза быстрых алгоритмов дискретного косинусного преобразования (ДКП) произвольного размера. В основе метода лежит использование полиномиальной алгебры $\mathbb{F}[x]/p(x)$, связанной с ДКП. Быстрый алгоритм ДКП получается в результате поэтапной декомпозиции данной алгебры. В свою очередь выполнение декомпозиции требует поэтапной факторизации полинома $p(x)$. Эта задача решается с привлечением теории Галуа, которая позволяет найти все подполя поля разложения полинома $p(x)$, в которых $p(x)$ имеет разложение на множители.

Ключевые слова: быстрый алгоритм, дискретное косинусное преобразование, теория Галуа

1. ВВЕДЕНИЕ

Дискретное косинусное преобразование (ДКП) играет важную роль во многих практических приложениях цифровой обработки сигналов, таких как сжатие изображений/видео, распознавание образов, кодировании речи, записи медицинских сигналов (ЭЭГ, ЭКГ) и т.д. [1]. Широкое распространение ДКП вызывает большой интерес к построению эффективных алгоритмов его вычисления [2]. Поскольку в таких популярных областях применения ДКП как кодирование изображений и видео блоки данных имеют размерность 4×4, 8×8 или 16×16, то большинство разработанных быстрых алгоритмов (БА) вычисления ДКП применимы, когда размер преобразования равен $n = 2^k$ [3]. В то же время, в других приложениях существует большой интерес к построению БА ДКП, когда размер преобразования отличен от степени двойки.

Быстрое развитие вычислительных платформ (таких как FPGA – *Field-programmable gate array*) сопровождается созданием программных систем автоматической генерации структур процессоров ДКП [4-5]. Подобные системы позволяют определить оптимальную в некотором смысле структуру процессора ДКП заданного размера для заданной вычислительной платформы.

Проблема автоматического поиска структуры процессора ДКП решается как оптимизационная задача над пространством альтернативных алгоритмов вычисления ДКП. Таким образом, качество получаемого решения существенно зависит от того, какое количество альтернативных быстрых алгоритмов ДКП существует для конкретного размера преобразования. Для расширения возможности подобных систем в настоящей работе предлагается метод, позволяющий получать быстрые алгоритмы ДКП произвольного размера. В ряде случаев для одного размера преобразования метод позволяет получить несколько альтернативных быстрых алгоритмов ДКП.

В основе предлагаемого метода лежит подход, использующий *полиномиальную алгебру* $\mathbb{F}[x]/\,p(x)$, связанную с ДКП [6]. Отметим, что эффективность использования математического аппарата абстрактной алгебры для синтеза быстрых алгоритмов дискретных преобразований показана ещё в работах советских ученых [7-9].

Полиномиальная алгебра представляет собой векторное пространство:

$$\mathcal{A} = \mathbb{F}[x]/\,p(x)\,. \tag{1}$$

Элементами алгебры является множество полиномов, коэффициенты которых принадлежат полю $\mathbb{F}$, а степень меньше $n = \deg(p(x))$. Операция «/» в (1) означает, что в полиномиальной алгебре операции сложения и умножения элементов выполняются с последующим приведением результата по модулю полинома $p(x)$:

$$r_1(x) = [v_1(x) + v_2(x)] \mod p(x),$$
$$r_2(x) = [v_1(x) \times v_2(x)] \mod p(x),$$

где

$$v_1(x),\, v_2(x),\, r_1(x),\, r_2(x) \in \mathbb{F}[x]/\,p(x)\ .$$

В [6] показано, что синтез быстрых алгоритмов ДКП происходит в результате поэтапной декомпозиции полиномиальной алгебры (1), для чего требуется выполнить поэтапную факторизацию полинома $p(x)$.

Выбор поля констант $\mathbb{F}$ в (1) является важной частью процесса синтеза быстрых алгоритмов ДКП. Например, в [10] в качестве $\mathbb{F}$ выбиралось поле комплексных чисел $\mathbb{C}$. Это удобно, поскольку в $\mathbb{C}$ любой полином раскладывается в произведение линейных многочленов [11]. Тем не менее, выбор $\mathbb{C}$ в качестве основного поля не дает ответа на вопрос, каким образом выполнить поэтапную факторизацию $p(x)$, необходимую для синтеза быстрых алгоритмов. Для решения этой проблемы предлагается ввести в рассмотрение поле разложения полинома $p(x)$. Для выполнения последовательной факторизации $p(x)$ необходимо найти все подполя поля разложения полинома $p(x)$, для чего используется теория Галуа. В каждом подполе полином $p(x)$ имеет уникальную факторизацию, которая может быть использована для синтеза БА. Поскольку коэффициенты полиномов Чебышева, которые входят в определение алгебры, отвечающей ДКП, имеют целые коэффициенты, то в качестве исходного поля предлагается выбрать поле рациональных чисел $\mathbb{Q}$. При выполнении поэтапной факторизации $p(x)$, поле $\mathbb{Q}$ постепенно дополняется числами, не содержащимися в $\mathbb{Q}$. На последнем этапе результирующее поле является полем разложения полинома $p(x)$.

Поскольку известны полиномиальные алгебры для всех восьми типов дискретных косинусных и синусных преобразований [10], то предлагаемый метод применим к синтезу быстрых алгоритмов любого преобразования из данного класса. В качестве практического применения метода показан пример синтез двух быстрых алгоритмов 7-точечного ДКП 4-го типа.

2. СИНТЕЗ БЫСТРЫХ АЛГОРИТМОВ С ИСПОЛЬЗОВАНИЕМ ПОЛИНОМИАЛЬНОЙ АЛГЕБРЫ

В данном разделе рассматриваются теоретические основы синтеза быстрых алгоритмов ДКП с использованием понятия полиномиальной алгебры.

Применяя Китайскую теорему об остатках (КТО) полиномиальную алгебру (1) можно разложить в прямую сумму одноразмерных подалгебр [10]:

$$\mathcal{F}: \quad \mathbb{F}[x]/\,p(x) \to \bigoplus_{0\le k<n} \mathbb{F}[x]/(x-\alpha_k), \tag{2}$$

при условии, что $\alpha=(\alpha_0,\ldots,\alpha_{n-1})$ попарно различные нули $p(x)$ и $\alpha_k \in \mathbb{F}$. Если в алгебре $\mathbb{F}[x]/\,p(x)$ выбрать базис $b=(p_0(x),\ldots,p_{n-1}(x))$, а в каждой подалгебре $\mathbb{F}[x]/(x-\alpha_k)$ установить единичный базис $(x^0)=(1)$, тогда отображение $\mathcal{F}$ записывается в матричном виде следующим образом:

$$\mathcal{F}=\mathcal{P}_{b,\alpha}=[p_\ell(\alpha_k)]_{k,\ell}\,, \tag{3}$$

где $0\le k<n$, $0\le \ell<n$. $\mathcal{P}_{b,\alpha}$ называют *полиномиальным преобразованием*. Если в каждой подалгебре $\mathbb{F}[x]/(x-\alpha_k)$ выбраны различные базисы β_k, то получающееся полиномиальное преобразование называют *масштабированным*

$$\mathcal{F}=\operatorname{diag}(1/\beta_0,\ldots,1/\beta_{n-1})\cdot\mathcal{P}_{b,\alpha}\,. \tag{4}$$

Хорошо известно, что широко используемые в цифровой обработке сигналов дискретные преобразования, такие как дискретное преобразование Фурье и ДКП, можно представить в виде произведения входного вектора $\mathbf{x}$ на матрицу:

$$\mathbf{y}=\mathcal{P}_{b,\alpha}\,\mathbf{x}\,.$$

Быстрый алгоритм преобразования можно записать в виде факторизации матрицы $\mathcal{P}_{b,\alpha}$ в произведение слабозаполненных, структурированных матриц. Такой подход отражает структуру быстрого алгоритма и упрощает работу при получении различных его вариантов.

Как указывалось выше, быстрый алгоритм получается путем факторизации матрицы преобразования $\mathcal{P}_{b,\alpha}=B_m\cdot B_{m-1}\cdot\ldots\cdot B_1$, где B_k – слабозаполненная матрица. Если учесть, что фактически $\mathcal{P}_{b,\alpha}$ представляет собой матрицу смены базиса, то задача синтеза БА сводится к определению последовательности базисов $b \xrightarrow{B_1} b_1 \xrightarrow{B_2} \ldots \xrightarrow{B_m} \alpha$. В терминах преобразования (2) быстрый алгоритм получается, если декомпозицию $\mathbb{F}[x]/\,p(x)$ в сумму одноразмерных подалгебр выполнить в несколько этапов [10].

Один из способов выполнения поэтапной декомпозиции $\mathbb{F}[x]/\,p(x)$ состоит в использовании факторизации $p(x)=q(x)r(x)$. Если $\deg(q)=k$, а $\deg(r)=m$, то

$$\mathcal{F}: \quad \mathbb{F}[x]/p(x) \to \mathbb{F}[x]/q(x) \oplus \mathbb{F}[x]/r(x) \tag{5}$$

$$\to \left(\underset{0 \le i < k}{\oplus} \mathbb{F}[x]/(x-\beta_i) \right) \oplus \left(\underset{0 \le j < m}{\oplus} \mathbb{F}[x]/(x-\gamma_i) \right) \tag{6}$$

$$\to \underset{0 \le i < n}{\oplus} \mathbb{F}[x]/(x-\alpha_i), \tag{7}$$

где β_i и γ_j – нули полиномов $q(x)$ и $r(x)$, соответственно, $\oplus$ – операция прямой суммы алгебр. Если в подалгебре $\mathbb{F}[x]/q(x)$ выбрать базис *c*, а в $\mathbb{F}[x]/r(x)$ – базис *d*, тогда поэтапную декомпозицию (5)-(7) можно записать в виде произведения матриц:

$$\mathcal{P}_{b,\alpha} = P\left(\mathcal{P}_{c,\beta} \oplus \mathcal{P}_{d,\gamma}\right) B, \tag{8}$$

где $A \oplus B = \begin{bmatrix} A & \\ & B \end{bmatrix}$ обозначает прямую сумму матриц. Матрица *B* отображает базис *b* в конкатенацию базисов (c,d) и соответствует выражению (5). Преобразованию (6), выполняющему декомпозицию $\mathbb{F}[x]/q(x)$ и $\mathbb{F}[x]/r(x)$ с использованием КТО, соответствует прямая сумма матрица $\mathcal{P}_{c,\beta}$ и $\mathcal{P}_{d,\gamma}$. На этапе (7) происходит перестановка одноразмерных алгебр. В выражении (8) этому шагу отвечает матрица перестановки *P*, выполняющая отображение $(\beta,\gamma) \mapsto \alpha$. Если *B* – слабозаполненная матрица, тогда (8) представляет собой быстрый алгоритм, поскольку оставшиеся матрицы-сомножители являются слабозаполненными по определению. Описанная выше процедура применяется в дальнейшем для синтеза быстрых алгоритмов ДКП.

3. АЛГЕБРАИЧЕСКИЙ МЕТОД СИНТЕЗА БЫСТРЫХ АЛГОРИТМОВ ДКП

3.1 Описание метода

Предлагаемый алгебраический метод синтеза быстрых алгоритмов ДКП состоит в выполнении следующих шагов.

Шаг 1. Определение полиномиальной алгебры $\mathbb{Q}[x]/p(x)$ (и базиса в ней), отвечающей заданному типу ДКП.

Шаг 2. Получения всех подполей $\mathbb{L}_i$ поля разложения $\mathbb{E}$ полинома $p(x)$ с использованием теории Галуа.

Шаг 3. Получение поэтапной факторизации полинома $p(x)$, отвечающей башне вложенных подполей $\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_r = \mathbb{E}$.

Шаг 4. Синтез БА ДКП с использованием факторизации, полученной на шаге 3 и выражений (5)-(8).

Полиномиальные алгебры, отвечающие всем 8 типам дискретных косинусных и синусных преобразований, можно найти в работах [6-10]. Необходимые для понимания метода сведения из теории Галуа приведены в **Приложении** (в конце статьи).

3.2 Синтез БА ДКП-4 размера 7

Для конкретизации предлагаемого метода ниже рассматривается задача синтеза БА ДКП четвертого типа. Традиционные методы синтеза БА ДКП, как правило, применимы в случае, когда размер преобразования равен составному числу [10]. Чтобы показать преимущество предлагаемого метода, выполним синтез БА ДКП-4, размер которого равен простому числу 7.

Шаг 1. Рассмотрим полиномиальную алгебру, отвечающую ДКП-4 [10]:

$$\mathcal{A} = \mathbb{Q}[x] / 2T_n(x), \quad b = (V_0(x), \ldots, V_{n-1}(x)) , \tag{9}$$

где $T_k(x)$ и $V_k(x)$ – полиномы Чебышева первого и третьего рода *k*-го порядка, соответственно $(x = \cos\ \psi)$:

$$T_n(x) = \cos(n\psi), \quad V_n(x) = \cos(n + \tfrac{1}{2})\psi \,\big/\, \cos(\tfrac{1}{2}\psi) .$$

Поскольку корни $2T_n(x)$ равны $\alpha_k = \cos(k + \frac{1}{2})\frac{\pi}{n}$, $0 \le k < n$, то в соответствии с (3) полиномиальное преобразование для (9) определяется как

$$\mathcal{P}_{b,\alpha} = [V_\ell(\alpha_k)]_{0 \le k, \ell < n} = \left[\frac{\cos(k + \frac{1}{2})(\ell + \frac{1}{2})\frac{\pi}{n}}{\cos(k + \frac{1}{2})\frac{\pi}{2n}} \right]_{0 \le k, \ell < n} . \tag{10}$$

Если (10) умножить слева на масштабирующую диагональную матрицу

$$D_n^{(\mathrm{C4})} = \mathrm{diag}_{\,0 \le k < n}\ (\cos(k + \tfrac{1}{2})\tfrac{\pi}{2n}) , \tag{11}$$

то в результате получим матрицу ДКП-4:

$$\text{DCT-4}_n = D_n^{(\mathrm{C4})}\, \mathcal{P}_{b,\alpha} = \left[\cos(k + \tfrac{1}{2})(\ell + \tfrac{1}{2})\tfrac{\pi}{n} \right]_{0 \le k, \ell < n} . \tag{12}$$

Таким образом, выражения (10)-(12) демонстрируют, что ДКП-4 представляет собой масштабированное полиномиальное преобразование вида (4).

Шаг 2. Полиномиальная алгебра, соответствующая 7-точечному ДКП-4 имеет вид

$$\mathcal{A} = \mathbb{Q}[x] / 2T_7(x), \quad b = (V_0(x), \ldots, V_6(x)) . \tag{13}$$

Корни полинома $2T_7(x)$ равны $\alpha_k = \cos\dfrac{\pi(1+2k)}{14}$, $k = 0,1,\ldots,6$. Над полем $\mathbb{Q}$ данный полином имеет факторизацию

$$2T_7(x) = 2x\, P_6(x) , \tag{14}$$

поскольку корень $\alpha_3 = 0$. Данная факторизация будет использована при получении БА.

Полином $P_6(x)$ неприводим над полем $\mathbb{Q}$. Его полем разложения служит $\mathbb{Q}_{\cos(\frac{\pi}{14})}$, поскольку все корни $P_6(x)$ могут быть выражены через примитивный элемент $\theta = \cos(\frac{\pi}{14})$ следующим образом

$$\alpha_k = T_{1+2k}(\theta) , \quad k = 0,1,2,4,5,6 . \tag{15}$$

Согласно описанному методу синтеза БА необходимо определить подполя поля $\mathbb{Q}_{\cos(\frac{\pi}{14})}$, в которых $P_6(x)$ может быть разложен на множители. Для этого определим группу Галуа $\mathrm{Gal}(P_6)$. Воспользуемся методом, описанным в [11], для отыскания всех автоморфизмов поля $\mathbb{Q}_{\cos(\frac{\pi}{14})}$, которые и составляют группу $\mathrm{Gal}(P_6)$. Введем следующие обозначения $\theta_0 = \alpha_0$, $\theta_1 = \alpha_1$, $\theta_2 = \alpha_2$, $\theta_3 = \alpha_4$, $\theta_4 = \alpha_5$, $\theta_5 = \alpha_6$. Поскольку элементы $\theta_0, \ldots, \theta_5$ являются числами, сопряженными с θ (и могут быть выражены через θ см. (15)), тогда подстановки

$$\theta \mapsto \theta_k , \tag{16}$$

$k = 0, \ldots, 5$ исчерпывают всю группу Галуа $\mathrm{Gal}(P_6)$. Таким образом, каждый элемент группы Галуа переводит систему корней $P_6(x)$ в себя. Подстановки (16) удобно представлять матрицами перестановок $\{\sigma_0, \ldots, \sigma_5\}$ – которые имеют разряженную структуру (рис.1).

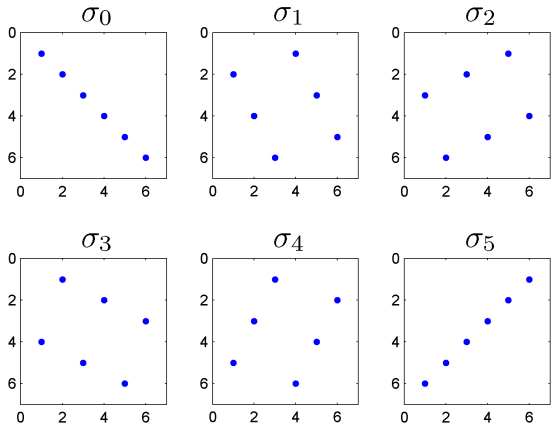

Рис.1. Группа Галуа $\mathrm{Gal}(P_6)$, представленная матрицами перестановок $\{\sigma_0, \ldots, \sigma_5\}$. Кружками обозначены положения единиц в матрице.

Таким образом, установлено, что $\mathrm{Gal}(P_6)$ представляет собой циклическую группу шестого порядка ($\mathbb{Z}_6$). Как известно, $\mathbb{Z}_6$ имеет две подгруппы – циклическую подгруппу порядка 2: $\mathbb{Z}_2 = \{\sigma_0, \sigma_5\}$, и циклическую подгруппу порядка 3: $\mathbb{Z}_3 = \{\sigma_0, \sigma_1, \sigma_3\}$. На рис.2(*a*) группа $\mathrm{Gal}(P_6)$ показана в виде решетки подгрупп. Согласно соответствию Галуа должно существовать аналогичная решетка подполей поля $\mathbb{Q}_{\cos(\frac{\pi}{14})}$ (рис.2(*b*)).

Возникает следующий вопрос: как найти подполе $\mathbb{F}$, соответствующее некой подгруппе H группы Галуа? В [11] предлагается следующее решение. Если задана подгруппа $H = \{\sigma_0, \ldots, \sigma_{h-1}\}$, то необходимо составить произведение

$$(x - \sigma_0\,\theta)(x - \sigma_1\,\theta)\ldots(x - \sigma_{h-1}\,\theta) , \tag{17}$$

коэффициенты этого многочлена согласно основной теореме теории Галуа должны принадлежать полю $\mathbb{F}$ и даже порождать его.

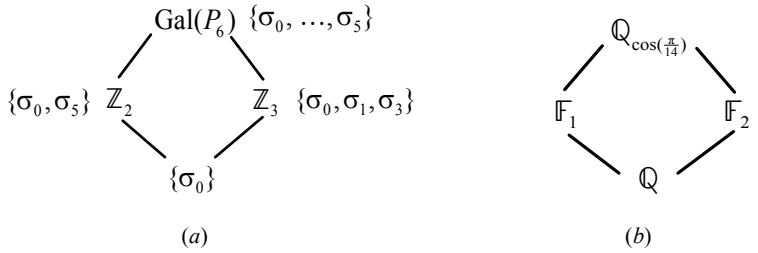

Рис.2. (*a*) подгруппы группы Галуа $\mathrm{Gal}(P_6)$;
(*b*) подполя поля разложения $P_6(x)$.

Применим данный способ для нахождения подполей $\mathbb{F}_1$ и $\mathbb{F}_2$ (рис.2(*b*)). Рассмотрим полином

$$(x-\sigma_0\theta)(x-\sigma_5\theta)=x^2-\tfrac{1}{2}\cos(\tfrac{6\pi}{7}), \tag{18}$$

коэффициенты которого принадлежат полю $\mathbb{Q}_{\cos(\frac{\pi}{7})}$. Это и есть искомое поле $\mathbb{F}_1$. Поле $\mathbb{F}_2$ определяется аналогичным образом, если рассмотреть полином

$$(x-\sigma_0\theta)(x-\sigma_1\theta)(x-\sigma_3\theta)=x^3+(\cos\tfrac{\pi}{14}+\cos\tfrac{3\pi}{14}+\cos\tfrac{9\pi}{14})x^2-\tfrac{1}{4}(\cos\tfrac{\pi}{14}+\cos\tfrac{3\pi}{14}+\cos\tfrac{9\pi}{14}), \tag{19}$$

чьи коэффициенты лежат в поле $\mathbb{Q}_{\cos\frac{\pi}{14}+\cos\frac{3\pi}{14}+\cos\frac{9\pi}{14}}\cong\mathbb{Q}_{\sqrt{7}}$, которое соответствует полю $\mathbb{F}_2$.

Шаг 3. Используя две башни полей на рис.2(*b*) получаются два различных способа поэтапной факторизации полинома $P_6(x)$

$$2T_7(x)=\underbrace{2xP_6(x)}_{\mathbb{Q}}=\underbrace{2x(2T_2-2\cos\tfrac{6\pi}{7})(2T_2-2\cos\tfrac{4\pi}{7})(2T_2-2\cos\tfrac{2\pi}{7})}_{\mathbb{Q}_{\cos\left(\frac{\pi}{7}\right)}}=\underbrace{2\prod_{i=0}^{6}(x-\alpha_i)}_{\mathbb{Q}_{\cos\left(\frac{\pi}{14}\right)}}, \tag{20}$$

$$2T_7(x)=\underbrace{2xP_6(x)}_{\mathbb{Q}}=\underbrace{2x(2T_3-2\sqrt{7}\,T_2+6T_1-\sqrt{7})(2T_3+2\sqrt{7}\,T_2+6T_1+\sqrt{7})}_{\mathbb{Q}_{\sqrt{7}}}=\underbrace{2\prod_{i=0}^{6}(x-\alpha_i)}_{\mathbb{Q}_{\cos\left(\frac{\pi}{14}\right)}}, \tag{21}$$

Шаг 4. На основе факторизаций (20)-(21) и метода синтеза БА, описанного в подразделе 3.2, получены два БА 7-точечного ДКП-4. Детали процедуры получения БА по известной факторизации полинома можно найти в работах [10, 12].

На рис.3 показана граф-схема БА 7-точечного ДКП-4, полученная с использованием факторизации (20). Красным цветом обозначены сигналы, которые в блоках суммирования берутся с отрицательным знаком. Пунктирной линией обозначены внутренние сигналы, которые умножаются на константу (соответствующая константа приведена рядом). Сумматор рядом с входом x_0 суммирует 7 слагаемых и поэтому для его реализации требуется 6 двухвходовых сумматоров.

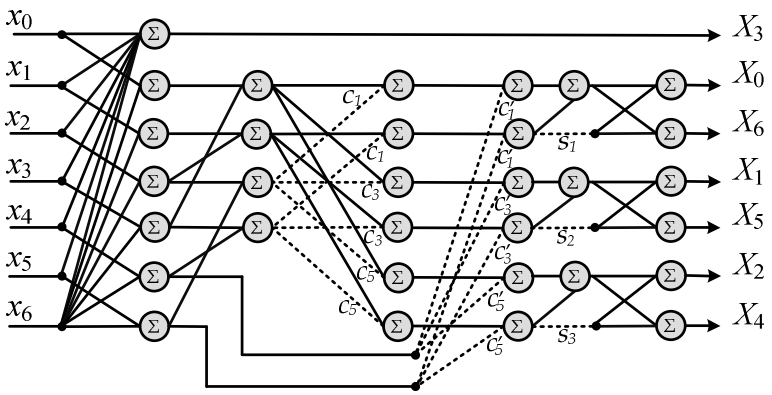

Рис.3. Граф-схема быстрого алгоритма ДКП-4 размера 7,
$c_k = 2\cos\frac{k\pi}{7}$, $c'_k = c_k^2 - 1$ и $s_k = 2\cos\frac{k\pi}{14}$.

На рис.3 не показана операция масштабирования выходных данных, которая соответствует умножению выходных данных на диагональную матрицу $D_7^{(C4)}$. Без учета масштабирующих множителей БА 7-точечного ДКП-4 (рис.3) требует 15 операций умножения и 37 сложений.

Быстрый алгоритм, полученный с использованием факторизации (21), представлен в виде произведения слабозаполненных матриц:

$$\mathrm{DCT4}_7 = D_7^{(C4)} \times P \times B_5 \times B_4 \times B_3 \times B_2 \times B_1, \tag{22}$$

где

$$B_1 = \begin{bmatrix} 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & & & & & & 1 \\ & 1 & & & & & -1 \\ & & 1 & & & & -1 \\ & & & 1 & & & 1 \\ & & & & 1 & & 1 \\ & & & & & 1 & -1 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 1 & & & & & & \\ & 1 & & -3 & 4 & -6 & \\ & & 1 & -3 & 6 & -8 & \\ & & & 1 & -1 & 4 & -4 \\ & & & & 1 & -2 & 2 \\ & & & & 1 & -2 & 3 \\ & & & & 1 & -1 & 2 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & a & & \\ & & & & & a & \\ & & & & & & a \end{bmatrix},$$

$$B_4 = \begin{bmatrix} 1 & & & & & & \\ & 1 & & 1 & & & \\ & & 1 & & 1 & & \\ & & & 1 & & & 1 \\ & 1 & & -1 & & & \\ & & 1 & & -1 & & \\ & & & 1 & & & -1 \end{bmatrix}, \quad B_5 = \begin{bmatrix} 1 & & & & & & \\ & 1 & b_1 & d_1 & & & \\ & 1 & b_3 & d_3 & & & \\ & 1 & b_9 & d_9 & & & \\ & & & & 1 & b_5 & d_5 \\ & & & & 1 & b_{11} & d_{11} \\ & & & & 1 & b_{13} & d_{13} \end{bmatrix}, \quad P = \begin{bmatrix} & 1 & & & & & \\ & & 1 & & & & \\ & & & & 1 & & \\ 1 & & & & & & \\ & & & 1 & & & \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix},$$

где $a = \sqrt{7}$, $b_k = 2\cos\frac{k\pi}{14} - 1$, $d_k = 8\cos^2\frac{k\pi}{14} - 4\cos\frac{k\pi}{14} - 1$. Если не учитывать умножения на матрицу $D_7^{(C4)}$, то для выполнения алгоритма (22) необходимо выполнить 15 умножения и 49 сложений. Таким образом, второй вариант алгоритма 7-точечного ДКП-4 требует на 12 сложений больше, чем первый.

4. ЗАКЛЮЧЕНИЕ

Предложен алгебраический метод синтеза БА ДКП произвольного размера. В методе используется представление ДКП как матрицы декомпозиции определенной полиномиальной алгебры $\mathbb{F}[x]/p(x)$. Быстрый алгоритм получается в результате выполнения поэтапной декомпозиции данной алгебры. В свою очередь декомпозиция тесно связана с выполнением факторизации полинома $p(x)$. Для решения этой задачи используется математический аппарат теории Галуа, при помощи которого находятся все подполя поля разложения полинома $p(x)$. В данных подполях полином $p(x)$ имеет факторизацию, которая используется для получения быстрого алгоритма. В качестве практического применения получены два варианта БА 7-точечного ДКП-4, которые требуют одинакового количества операций умножения (15), но отличаются по числу операций сложения (37 и 49, соответственно). Предложенный метод можно использовать в системах автоматического синтеза структур процессоров ДКП [13] для расширения пространства альтернативных быстрых алгоритмов ДКП.

СПИСОК ЛИТЕРАТУРЫ

[1] *Айфичер Э., Джервис Б.* Цифровая обработка сигналов: практический подход; пер. с англ. – М.: Вильямс, 2004.

[2] *Britanak V., Yip P., Rao K*. Discrete cosine and sine transforms: general properties, fast algorithms and integer approximations. London: Academic Press, 2007.

[3] *Миано Дж*. Форматы и алгоритмы сжатия изображений в действии; пер. с англ. – М.: Триумф, 2003.

[4] *Püschel M., et al.* SPIRAL: Code generation for DSP transforms // Processing of IEEE. 2005. V. 93, no. 2. P. 232–275.

[5] *Bartholma R., et al*. A systematic approach for synthesizing VLSI architecture of lifting-based filter bank and transforms // IEEE Transactions on Circuits and systems – I. V. 55, no. 7. P. 1939–1952.

[6] *Püschel M., Moura J.M.F.,* The algebraic approach to the discrete cosine and sine transform // SIAM Journal on Computing. 2003. V. 32. P. 1280–1316.

[7] *Вайрадян А.С., Пчелинцев И.П., Челышев М.М*. Алгоритмы вычисления цифровых сверток // Зарубежная радиоэлектроника. 1982. №3. С. 3–34.

[8] *Лабунец В.Г.,* Алгебраическая теория сигналов и систем: цифровая обработка сигналов. – Красноярск: Издательство Красноярского университета, 1984.

[9] *Крот А.М*. Дискретные модели динамических систем на основе полиномиальной алгебры – Мн.: Наука и техника, 1990.

[10] *Püschel M., Moura J.M.F*., Algebraic signal processing theory: Coole-Tukey type algorithms for DCTs and DSTs // IEEE Transactions on Signal Processing. 2008. V. 54, no. 4. P. 1502–1521.

[11] *Ван дер Варден Б.Л.* Алгебра; под ред. Ю.И. Мерзлякова. М.: «Наука», 1978.

[12] *Вашкевич М.И., Петровский А.А*., Применение полиномиальных алгебр и теории Галуа для синтеза быстрых алгоритмов дискретных косинусных преобразований // Цифровая обработка сигналов. 2011. № 3. С. 2–10.

[13] *Петровский Ал.А, Станкевич А.В., Петровский А.А*. Быстрое проектирование систем мультимедиа от прототипа. – Мн.: «Бестпринт», 2011.

Рукопись получена 03.07.2012,
финальная версия – 31.07.2012.

ПРИЛОЖЕНИЕ

Краткие сведения из теории Галуа

Множество всех полиномов от x с коэффициентами из поля $\mathbb{F}$ обозначают как $\mathbb{F}[x]$. Пусть $p(x) \in \mathbb{F}[x]$, *полем разложения* $\mathbb{E}$ полинома $p(x)$ считается наименьшее расширение поля $\mathbb{F}$, содержащее все корни $p(x)$. Например, $\mathbb{Q}_{\sqrt{2}}$ – поле разложения полинома $p(x) = x^2 - 2$. $\mathbb{Q}_{\sqrt{2}}$ получается присоединением числа $\sqrt{2}$ к $\mathbb{Q}$. Взаимно-однозначное отображение поля $\mathbb{E}$ на себя называется *автоморфизмом*. $\mathbb{F}$*-автоморфизмом* поля $\mathbb{E}$ называется такой автоморфизм φ, для которого $\varphi(x) = x, \forall x \in \mathbb{F}$. Группу $\mathbb{F}$-автоморфизмов поля $\mathbb{E}$ называют группой Галуа полинома $p(x)$ и обозначают $\mathrm{Gal}(p)$ или $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$. В качестве примера определим функцию $\varphi\colon \mathbb{Q}_{\sqrt{2}} \to \mathbb{Q}_{\sqrt{2}}$ такую, что

$$\varphi(a + b\sqrt{2}) = a - b\sqrt{2},$$

тогда φ представляет собой $\mathbb{Q}$-автоморфизм поля $\mathbb{Q}_{\sqrt{2}}$. Группа автоморфизмов $\mathrm{Gal}(p) = \{\mathrm{id}, \varphi\}$ представляет собой циклическую группу второго порядка, где id – $\mathbb{Q}$-автоморфизм, который оставляет все элементы поля $\mathbb{Q}_{\sqrt{2}}$ на своих местах. Очевидно, что $\varphi \cdot \varphi = \mathrm{id}$.

Важным результатом теории Галуа является установление связи между структурой подполей поля разложения полинома $p(x)$ и структурой подгрупп группы Галуа $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Каждой подгруппе H группы $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ отвечает подполе $\mathbb{L} \subset \mathbb{E}$, состоящее из элементов $\mathbb{E}$, неподвижных под действием автоморфизмов из H. Аналогично, каждому подполю $\mathbb{L} \subset \mathbb{E}$ отвечает подгруппа H группы Галуа, оставляющая элементы $\mathbb{L}$ на месте. В результате изучение всех подполей поля $\mathbb{E}$ сводится к изучению всех подгрупп группы $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$. При этом каждой башне (цепочке вложенных) полей

$$\mathbb{F} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_r = \mathbb{E}, \tag{23}$$

отвечает нормальный ряд вложенных (в обратном направлении) групп

$$\mathrm{Gal}(\mathbb{E}/\!\!/\mathbb{F}) = \mathrm{G}_0 \supset \mathrm{G}_1 \supset \cdots \supset \mathrm{G}_r = \{1\},$$

и наоборот (соответствие Галуа).

Таким образом, соответствие Галуа позволяет определить все подполя поля разложения полинома $p(x)$. В каждом подполе $p(x)$ раскладывается единственным образом в произведение неприводимых над этим подполем полиномов. Используя (23) можно выполнить поэтапную факторизацию $p(x)$, которая необходима для синтеза БА ДКП.