

## ПРИМЕНЕНИЕ ПОЛИНОМИАЛЬНЫХ АЛГЕБР И ТЕОРИИ ГАЛУА ДЛЯ СИНТЕЗА БЫСТРЫХ АЛГОРИТМОВ ДИСКРЕТНЫХ КОСИНУСНЫХ ПРЕОБРАЗОВАНИЙ

**Вашкевич М.И.**, аспирант кафедры «Электронных вычислительных средств» Белорусского государственного университета информатики и радиоэлектроники, г. Минск, e-mail: vashkevich@bsuir.by.

**Петровский А.А.**, зав. кафедрой «Электронных вычислительных средств» Белорусского государственного университета информатики и радиоэлектроники, г. Минск, д.т.н., профессор, e-mail: palex@bsuir.by.

**Ключевые слова:** дискретные преобразования, полиномиальная алгебра, теория Галуа, быстрые алгоритмы, модели сигнала.

### Введение

Для описания и синтеза быстрых алгоритмов дискретных преобразований, таких как дискретное косинусное преобразование (ДКП) и дискретное преобразование Фурье (ДПФ) в настоящее время используются различные математические системы обозначений [1]:

- алгебраическая система обозначений, предложенная Кули и Тьюки, используется для получения коротких рекурсивных уравнений, которые оказываются удобными при составлении программ и исследовании ошибок округления;
- матричная система обозначений, в которой быстрый алгоритм преобразования представляется в виде произведения структурированных матриц;
- полиномиальные алгебры. Позволяют перейти от матрицы преобразования к рассмотрению полиномиальных алгебр и использовать для синтеза быстрых алгоритмов математический аппарат теории групп и колец [2-4];
- модель сигнала. Понятие модели сигнала обобщает использование полиномиальных алгебр для синтеза быстрых алгоритмов преобразований и позволяет с единых позиций рассматривать различные дискретные преобразования и их быстрые алгоритмы [5].

В данной работе используется подход на основе понятия модели сигнала [5]. Однако, в отличие от [5], в качестве основного выбирается поле рациональных, а не комплексных чисел. Это изменение приводит к тому, что для синтеза быстрого алгоритма приходится вводить в рассмотрение расширения поля рациональных чисел, что в свою очередь ведёт к новой структуре быстрых алгоритмов. Упомянутая особенность также позволяет найти применение в ЦОС изящного математического аппарата теории Галуа.

В качестве практического применения предлагаемого алгебраического подхода разработан быстрый алгоритм 8-точечного ДКП-2, содержащий в ядре своей структуры только 5 операций умножения и 29 операций сложения.

Статья имеет следующую структуру. В первом разделе, для удобства читателя, приводятся основные сведения из АТОС. Во втором разделе описываются модели сигнала соответствующие ДКП-2 и ДКП-4. Третий раздел содержит описание предлагаемого метода синтеза быстрых алгоритмов ДКП-2 и ДКП-4 с использованием теории Галуа, а также практические примеры. Ниже приведены некоторые пояснения по поводу используемых обозначений.

Предлагается систематический подход к синтезу быстрых алгоритмов дискретных косинусных преобразований второго и четвертого типов (ДКП-2/ДКП-4), основанный на алгебраической теории обработки сигналов (АТОС). В рамках АТОС, быстрый алгоритм преобразования получается не путем действий с коэффициентами матрицы преобразования, а как пошаговая декомпозиция полиномиальной алгебры, отвечающей данному преобразованию. Декомпозиция предполагает пошаговую факторизацию полинома, для чего предлагается использовать подполя поля разложения полинома, получаемые с использованием основной теоремы теории Галуа.

**Представление алгоритма.** Традиционно в ЦОС линейное преобразование записывается в виде

$$y_k = \sum_{0 \leq \ell < n} t_{k,\ell} s_\ell,$$

где  $s = (s_0, \dots, s_{n-1})^T$  – входной сигнал,  $y = (y_0, \dots, y_{n-1})^T$  – выходной сигнал, а  $t_{k,\ell}$  – коэффициенты преобразования. Тем не менее, часто более удобной является векторно-матричная форма записи преобразования:  $y = Ts$ , где  $T = [t_{k,\ell}]_{0 \leq k, \ell < n}$

В этом случае быстрый алгоритм для преобразования представляется в виде факторизации матрицы  $T$  в произведение слабозаполненных, структурированных матриц [6].

**Обозначения.** Ниже приведены используемые в статье типы матриц

$$I_n = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}, J_n = \begin{bmatrix} & & 1 \\ & \ddots & \\ 1 & & \end{bmatrix}.$$

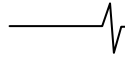
Все матрицы, как правило, обозначаются заглавными латинскими буквами (например  $A_n$  – квадратная матрица порядка  $n$ ), а вектора – строчными латинскими буквами (полуужирное начертание шрифта). Диагональные матрицы записываются как  $diag(\alpha_0, \dots, \alpha_{n-1})$ . Также используется оператор прямой суммы матриц

$$A \oplus B = \begin{bmatrix} A & \\ & B \end{bmatrix}.$$

Полиномы обозначаются строчными латинскими буквами, например  $p(x), q(x)$ . Часто для удобства и экономии пространства аргумент  $x$  опускается.

### 1. Алгебраическая теория обработки сигналов: обзор Полиномиальная алгебра

В [5] показано, что любое дискретное тригонометрическое преобразование (в том числе ДПФ и ДКП) связано с определённой полиномиальной алгеброй. Под алгеброй здесь понимается векторное пространство  $\mathcal{A}$  над числовым полем  $\mathbb{F}$ , в котором установлена операция умножения, приводящая в соответствие каждой паре элементов  $p, q$  из  $\mathcal{A}$  элемент  $r \in \mathcal{A}$  [7]. Примером алгебр могут служить система комплексных чисел, кватернио-



нов или  $\mathbb{F}[x]$  (множество всех полиномов с коэффициентами из поля  $\mathbb{F}$ ).

Практическую значимость для ЦОС представляет полиномиальная алгебра, определяемая как

$\mathcal{A} = \frac{\mathbb{F}[x]}{p(x)} = \{q(x) \mid \deg q < \deg p\}$ , множество всех полиномов со степенью меньше  $\deg p$  и операциями сложения и умножения, выполняемыми по модулю  $p(x)$ .

**Концепция модели сигнала**

Развитие понятия полиномиальной алгебры привело к появлению алгебраической теории обработки сигналов (АТОС) (от англ. «algebraic signal processing theory»), в которой нашли применение многие понятия современной алгебры [8].

АТОС – это общий аксиоматический подход к ЦОС, который строится на концепции модели сигнала, определяемой тройкой  $(\mathcal{A}, \mathcal{M}, \mathcal{Z})$ , где  $\mathcal{A}$  – это пространство фильтров (алгебра),  $\mathcal{M}$  – пространство сигналов ( $\mathcal{A}$ -модуль) и  $\mathcal{Z}$  – обобщенная концепция z-преобразования. Модель сигнала  $(\mathcal{A}, \mathcal{M}, \mathcal{Z})$  устанавливает связь векторно-матричных операций, в которых выражаются дискретные линейные преобразования, с их алгебраической структурой (можно сказать, что существуют две изоморфные области – область алгебраических структур и область их векторно-матричного представления).

Множество сигналов  $\mathcal{M}$  представляет собой векторное пространство. Таким образом, сигналы можно складывать и умножать на константы из основного поля. В ЦОС сигналы обрабатываются линейными системами, которые, как правило, называют фильтрами. В АТОС фильтрацию представляют, как умножение

$$s' = h \cdot s, \tag{1}$$

где  $s, s' \in \mathcal{M}$ , а  $h$  принадлежит пространству фильтров  $\mathcal{A}$ . Пространство фильтров имеет более сложную структуру, чем пространство сигналов, в нём определены следующие операции:  $h + h' \in \mathcal{A}$ ;  $\alpha h \in \mathcal{A}$ , где  $\alpha$  константа из основного поля;  $h \cdot h' \in \mathcal{A}$ .

Первые две операции определяют  $\mathcal{A}$ , как векторное пространство, а третья делает  $\mathcal{A}$  алгеброй.

Таким образом, пространство фильтров является алгеброй  $\mathcal{A}$ , которая действует в векторном пространстве  $\mathcal{M}$ , образуя в нем структуру левого  $\mathcal{A}$ -модуля. По определению левым  $\mathcal{A}$ -модулем называется векторное пространство  $\mathcal{M}$  с операцией умножения слева на элементы алгебры  $\mathcal{A}$ , обладающей следующими свойствами:

$$\begin{aligned} h \cdot (s + s') &= h \cdot s + h \cdot s', \\ (h + h') \cdot s &= h \cdot s + h' \cdot s, \\ (h \cdot h') \cdot s &= h \cdot (h' \cdot s), \end{aligned} \tag{2}$$

для любых  $h, h' \in \mathcal{A}$  и  $s, s' \in \mathcal{M}$ .

В [8] показано, что если модель сигнала строится для конечномерных сигналов  $s = (s_0, \dots, s_{n-1}) \in \mathbb{F}^n$  и ей свойственна инвариантность к сдвигу, то  $\mathcal{A}$  обязана быть полиномиальной алгеброй  $\mathbb{F}[x]/p(x)$ . Далее, если в  $\mathbb{F}[x]/p(x)$  задан базис  $b = (p_0, \dots, p_{n-1})$ , то  $\mathcal{A} = \mathcal{M} = \mathbb{F}[x]/p(x)$  с отображением

$$\mathcal{Z}: \mathbb{F}^n \rightarrow \mathcal{M}, s \mapsto s = s(x) = \sum_{0 \leq \ell < n} s_\ell p_\ell,$$

определяют модель сигнала, где  $\mathcal{Z}$  это «z-преобразование» для данной модели. Можно сказать, что  $\mathcal{Z}$  выполняет отображения конечномерного сигнала  $s \in \mathbb{F}^n$  в пространство  $\mathcal{M}$ . Заметим, что  $\mathcal{Z}$  зависит от выбора базиса  $b$  в  $\mathcal{M}$ . Выражение  $\mathcal{A} = \mathcal{M}$  показывает, что базисное множество у алгебры  $\mathcal{A}$  и векторного пространства  $\mathcal{M}$  совпадают, в этом случае  $\mathcal{M}$  называют *регулярным*  $\mathcal{A}$ -модулем. Тем не менее, даже, если множества  $\mathcal{A}$  и  $\mathcal{M}$  равны, их алгебраическая структура различна. Так, например, для элементов из  $\mathcal{M}$  не определена операция умножения.

**Матричное представление алгебр**

Свойства (2) показывают, что каждый фильтр  $h \in \mathcal{A}$  определяет линейное преобразование  $\mathcal{M} \rightarrow \mathcal{M}$  (см. выражение (1)). При любом выборе базиса  $b = (p_0, \dots, p_{n-1})$  в  $\mathcal{M}$  линейному преобразованию  $h$  будет отвечать матрица  $M_h$  размера  $n \times n$ , которая называется (матричным) представлением фильтра  $h$ . Применяя  $h$  к каждому базисному вектору  $p_j$ , можно найти матрицу

$$M_h = [m_{ij}]_{0 \leq i, j < n} \tag{3}$$

$$h \cdot p_j = \sum_{i=0}^{n-1} m_{ij} p_i, m_{ij}, m_{ij} \in \mathbb{C}^n.$$

Определяя, таким образом,  $M_h$  для каждого  $h \in \mathcal{A}$ , получаем отображение алгебры  $\mathcal{A}$  в алгебру матриц  $\mathbb{F}^{n \times n}$ :  $\phi: \mathcal{A} \rightarrow \mathbb{F}^{n \times n}, h \mapsto \phi(h) = M_h$ .

Отображение  $\phi$  является гомоморфизмом алгебр, т.е. таким отображением, которое сохраняет структуру алгебры:  $\phi(h + h') = \phi(h) + \phi(h')$ , и  $\phi(hh') = \phi(h)\phi(h')$ .

$\phi$  называют (матричным) представлением  $\mathcal{A}$ , отвечающим  $\mathcal{A}$ -модулю  $\mathcal{M}$  с базисом  $b$ .

Если каждому элементу  $s$  пространства сигналов  $\mathcal{M}$  соответствует сигнал  $s$  из  $\mathbb{F}^n$ , то каждому элементу  $h$  пространства фильтров  $\mathcal{A}$  соответствует матрица некоторого линейного оператора из  $\mathbb{F}^{n \times n}$ . В случае, когда  $\mathcal{A} = \mathbb{F}[x]/p(x)$  для установления связи между  $\mathcal{A}$  и  $\mathbb{F}^{n \times n}$  достаточно определить линейный оператор, который будет играть роль умножения на  $x$  т.е.

$$\phi: \mathcal{A} \rightarrow \mathbb{F}^{n \times n}, x \mapsto \phi(x) = A.$$

Тогда любому (фильтру) полиному  $h(x) \in \mathcal{A} = \mathbb{F}[x]/p(x)$  будет соответствовать операторный полином в  $\mathbb{F}^{n \times n}$ :  $\phi: h(x) = h_{n-1}x^{n-1} + \dots + h_1x + h_0 \mapsto h(A) = h_{n-1}A^{n-1} + \dots + h_1A + h_0I$ .

В [8] доказывается, что  $x \in \mathcal{A}$  является оператором сдвига и порождающим элементом алгебры  $\mathcal{A} = \mathbb{F}[x]/p(x)$ , а  $\phi(x)$  – матричным представлением оператора сдвига.

**Инвариантность к сдвигу.** В ЦОС важным является понятие инвариантности линейной системы к сдвигу. В АТОС это свойство принимает весьма простую форму. А именно, если  $x$  оператор сдвига,  $h$  любой фильтр, то инвариантность к сдвигу имеет место, если для любого  $s \in \mathcal{M}$  выполняется тождество  $h(xs) = (hx)s$ , что эквивалентно:

$$x \cdot h = h \cdot x, \forall h \in \mathcal{A}. \tag{4}$$

В случае если  $x$  – порождающий элемент  $\mathcal{A}$ , то алгебра  $\mathcal{A}$  является коммутативной и, следовательно, выполнение (4) гарантировано. Тем самым доказывается, что если модель сигнала  $(\mathcal{A}, \mathcal{M}, \mathcal{Z})$  поддерживает свойство инвариантности к сдвигу, то соответствующая алгебра  $\mathcal{A}$  является коммутативной.

**Пример: модель сигнала дискретного времени.** В качестве примера рассмотрим модель сигнала  $\mathcal{A} = \mathcal{M} = \mathbb{F}[x]/(x^3 - 1)$  с базисом  $b = (x^0, x^1, x^2)$  в  $\mathcal{M}$ , тогда для сигнала  $s = (s_0, s_1, s_2) \in \mathbb{F}^3$  получим:

$$\mathcal{Z}: s \mapsto s = s(x) = s_0 + s_1x + s_2x^2 \in \mathbb{F}[x]/(x^3 - 1).$$

Операция умножения, которая соответствует фильтрации, в данной модели для  $h(x) \in \mathcal{A}$  и  $s(x) \in \mathcal{M}$  определяется как

$$h(x)s(x) \text{ mod } (x^3 - 1), \tag{5}$$

что соответствует вычислению круговой свёртке коэффициентов  $h$  и  $s$ . Далее, используя (3), построим матричное представление простейшего фильтра  $h(x) = x \in \mathcal{A}$ :

$$\begin{aligned} x \cdot x^0 \text{ mod } (x^3 - 1) &= x^1, \\ x \cdot x^1 \text{ mod } (x^3 - 1) &= x^2, \\ x \cdot x^2 \text{ mod } (x^3 - 1) &= x^0, \end{aligned}$$

откуда

$$\phi(x) = A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}. \quad (6)$$

В (6) легко узнать матрицу оператора циклического сдвига. Применяя (6) к фильтру  $h(x) = h_0 + h_1x + h_2x^2 \in \mathcal{A}$ , получим его матричное представление:

$$\begin{aligned} h(x) &= h_0 + h_1x + h_2x^2 \xrightarrow{\phi} h(A) = h_2A^2 + h_1A + h_0I = \\ &= h_2 \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} + h_1 \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} + \\ &+ h_0 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} h_0 & h_2 & h_1 \\ h_1 & h_0 & h_2 \\ h_2 & h_1 & h_0 \end{bmatrix}. \end{aligned}$$

Таким образом, операции умножения (5), производимой в  $\mathcal{A}$ -модуле  $\mathcal{M}$ , соответствует умножение вектора на матрицу, результатом которого является циклическая свёртка векторов  $h$  и  $s$ :

$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \end{bmatrix} = \begin{bmatrix} h_0 & h_2 & h_1 \\ h_1 & h_0 & h_2 \\ h_2 & h_1 & h_0 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \end{bmatrix}.$$

### Полиномиальное преобразование

**Основные определения.** Пусть задана полиномиальная алгебра  $\mathcal{A} = \mathbb{C}[x]/p(x)$ , где  $\mathbb{C}$  – поле комплексных чисел. Предположим, что все корни  $\alpha = (\alpha_0, \dots, \alpha_{n-1})$  полинома  $p(x)$  попарно различны. Тогда любой полином из  $\mathcal{A}$  можно разложить согласно Китайской теореме об остатках (КТО) следующим образом

$$\mathcal{F}: \mathbb{C}[x]/p(x) \rightarrow \bigoplus_{0 \leq k < n} \mathbb{C}[x]/(x - \alpha_k), \quad (7)$$

$$s(x) \mapsto (s(\alpha_0), \dots, s(\alpha_{n-1})).$$

Преобразование (7) линейно и имеет простую интерпретацию [9]: полином степени  $n - 1$  полностью определяется либо своими коэффициентами, либо списком своих значений в  $n$  различных точках. Преобразование (выполняет переход от коэффициентов полинома к его значениям в точках  $\alpha = (\alpha_0, \dots, \alpha_{n-1})$ . Как векторное пространство  $\mathcal{A} = \mathbb{C}[x]/p(x)$  под действием  $\mathcal{F}$  раскладывается в прямую сумму одномерных подпространств  $\mathbb{C}[x]/(x - \alpha_k)$ . Следовательно, если зафиксировать базис  $b = (p_0, \dots, p_{n-1})$  в  $\mathcal{A}$  и выбрать базис (с единичной нормой)  $\|x^0\| = 1$  в каждом подпространстве  $\mathbb{C}[x]/(x - \alpha_k)$ , то преобразование  $\mathcal{F}$  приобретёт матричную форму:

$$\mathcal{F} = \mathcal{P}_{b,\alpha} = [p_\ell(\alpha_k)]_{0 \leq k, \ell < n} \quad (8)$$

$\mathcal{P}_{b,\alpha}$  называют полиномиальным преобразованием для  $\mathcal{A} = \mathbb{C}[x]/p(x)$  с базисом  $b$ . Если в подпространствах  $\mathbb{C}[x]/(x - \alpha_k)$  выбрать базисы с нормой отличной от единицы  $\|x^0\| = \beta_k$ , то получаемое преобразование  $\mathcal{F} = \text{diag}(1/\beta_0, \dots, 1/\beta_{n-1}) \cdot \mathcal{P}_{b,\alpha}$  называют *масштабированным полиномиальным преобразованием*. Часто (8) также называют преобразованием Фурье для модуля  $\mathcal{M}$ .

### Пример: полиномиальное преобразование для модели сигнала дискретного времени.

Рассмотрим модель сигнала  $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/(x^n - 1)$  с базисом  $b = (x^0, \dots, x^{n-1})$  в  $\mathcal{M}$ . Корнями полинома  $(x^n - 1)$  являются  $\alpha = (\omega_n^0, \dots, \omega_n^{n-1})$ , где  $\omega_n = e^{-j2\pi/n}$ . Таким образом, преобразование Фурье для данной модели задается как  $\mathcal{F}: \mathbb{C}[x]/(x^n - 1) \rightarrow \bigoplus_{0 \leq k < n} \mathbb{C}[x]/(x - \omega_n^k)$ , что в точности совпадает с матрицей ДПФ и объясняет, почему модель названа моделью дискретного времени.

### Синтез быстрых алгоритмов с использованием концепции модели сигнала

Важнейшим применением понятия модели сигнала является изучение, вывод и классификация быстрых алгоритмов преобразований. Имеется большое число различных преобразований, широко используемых в ЦОС, таких как ДПФ и ДКП, для которых разработаны быстрые алгоритмы. Получение большинства этих алгоритмов заключается в

искусном обращении с коэффициентами преобразования. Тем не менее, подобные способы не помогают уяснить ни структуру, ни суть быстрых алгоритмов.

В АТОС основная идея заключается в получении быстрого алгоритма по модели сигнала, описывающего преобразование, а не из самого преобразования. Рассмотрим модель сигнала  $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/p(x)$ , для которого  $\mathcal{F}$  является преобразованием Фурье. Преобразование  $\mathcal{F}$  раскладывает модуль  $\mathcal{M}$  на неприводимые компоненты, называемые спектром. С точки зрения линейной алгебры  $\mathcal{M}$  (как векторное пространство) раскладывается на инвариантные подпространства относительно линейного оператора, играющего роль умножения на  $x$ . В случае полиномиальной алгебры преобразование  $\mathcal{F}$  является частным случаем КТО

$$\mathcal{F}: \mathbb{C}[x]/p(x) \rightarrow \bigoplus_{0 \leq k < n} \mathbb{C}[x]/(x - \alpha_k), \quad (9)$$

где  $\text{deg}(p) = n$  и  $\alpha_k$  корни полинома  $p$ . Заметим, что каждое слагаемое в правой части имеет размерность равную единице. Суть быстрого алгоритма заключается в поэтапном выполнении (9). Как правило, рассматриваются два основных способа поэтапной декомпозиции (9):

- факторизация  $p: p(x) = q(x) \cdot r(x)$ ;
- декомпозиция  $p: p(x) = q(r(x))$ .

Получение быстрого алгоритма путём факторизации состоит в рекурсивном разбиении полинома  $p$ . Если  $p = q \cdot r$ , то

$$\mathbb{C}[x]/p(x) \rightarrow \mathbb{C}[x]/q(x) \oplus \mathbb{C}[x]/r(x) \rightarrow \quad (10)$$

$$\rightarrow \bigoplus_{0 \leq i < k} \mathbb{C}[x]/(x - \beta_i) \oplus \bigoplus_{0 \leq j < m} \mathbb{C}[x]/(x - \gamma_j) \rightarrow \quad (11)$$

$$\rightarrow \bigoplus_{0 \leq i < n} \mathbb{C}[x]/(x - \alpha_i). \quad (12)$$

В приведённых выражениях  $\text{deg}(q) = k$ ,  $\text{deg}(r) = m$ ,  $\beta_i$  – корни полинома  $q$ ,  $\gamma_j$  – корни полинома  $r$ , очевидно, что  $\beta_i$  и  $\gamma_j$  подмножества корней  $\alpha_i$  полинома  $p$ . Шаги (10) и (11) используют КТО, в то время как (12) является простым переупорядочиванием компонент спектра. В [5] доказывается следующая

**Теорема 1.** Пусть  $p(x) = q(x) \cdot r(x)$ , выберем  $c$  и  $d$  в качестве базисов для модулей  $\frac{\mathbb{C}[x]}{q(x)}$  и  $\frac{\mathbb{C}[x]}{r(x)}$ , соответственно, тогда, обозначив через  $\beta$  и  $\gamma$  множества корней  $q$  и  $r$  соответственно, получаем

$$\mathcal{P}_{b,\alpha} = P(\mathcal{P}_{c,\beta} \oplus \mathcal{P}_{d,\gamma})B. \quad (13)$$

Матрица  $B$  отвечает переходу (10), т.е. отображению базиса  $b$  в конкатенированный базис  $(c, d)$ , а  $P$  является матрицей перестановки, которая отображает конкатенацию  $(\beta, \gamma)$  в список корней  $\alpha$  в выражении (12).

**Пример: 4-точечное БПФ.** Рассмотрим модель сигнала  $\mathcal{A} = \mathcal{M} = \mathbb{C}[x]/(x^4 - 1)$  с базисом  $b = (1, x^1, x^2, x^3)$  в  $\mathcal{M}$ . Полиномиальным преобразованием данной модели служит ДПФ. Заметим, что  $x^4 - 1 = (x^2 - 1)(x^2 + 1)$ , тогда, используя теорему 1, получаем следующую декомпозицию

$$\mathbb{C}[x]/(x^4 - 1) \rightarrow \mathbb{C}[x]/(x^2 - 1) \oplus \mathbb{C}[x]/(x^2 + 1) \rightarrow \quad (14)$$

$$\rightarrow \bigoplus_{0 \leq i < 2} \mathbb{C}[x]/(x - \beta_i) \oplus \bigoplus_{0 \leq j < 2} \mathbb{C}[x]/(x - \gamma_j) \rightarrow \quad (15)$$

$$\rightarrow \bigoplus_{0 \leq i < 4} \mathbb{C}[x]/(x - \alpha_i). \quad (16)$$

Выберем  $c = d = (1, x)$  в качестве базисов меньших модулей  $\mathbb{C}[x]/(x^2 - 1)$  и  $\mathbb{C}[x]/(x^2 + 1)$ . Вначале получим матрицу смены базиса  $B$ . Для этого необходимо выразить элементы  $x^\ell \in b$  в базисе  $(c, d)$ :

$$\begin{aligned} 1 &\equiv 1 \pmod{x^2 - 1}, 1 \equiv 1 \pmod{x^2 + 1}, \\ x &\equiv x \pmod{x^2 - 1}, x \equiv x \pmod{x^2 + 1}, \end{aligned}$$

$$x^2 \equiv 1 \pmod{x^2 - 1}, x^2 \equiv -1 \pmod{x^2 + 1},$$

$$x^3 \equiv x \pmod{x^2 - 1}, x^3 \equiv -x \pmod{x^2 + 1}.$$

Таким образом, получаем отображение:  
 $1 \mapsto (1, 1), x \mapsto (x, x), x^2 \mapsto (1, -1), x^3 \mapsto (x, -x)$ ,  
 которое определяет матрицу  $B$ :

$$B = \begin{bmatrix} I_2 & I_2 \\ I_2 & -I_2 \end{bmatrix},$$

Полиномиальные преобразования  $\mathcal{P}_{c,\beta}$  и  $\mathcal{P}_{d,\gamma}$  можно найти исходя из (8) и учитывая, что  $\beta = \{1, -1\}$ , а  $\gamma = \{j, -j\}$ ,

$$\mathcal{P}_{c,\beta} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \mathcal{P}_{d,\gamma} = \begin{bmatrix} 1 & j \\ 1 & -j \end{bmatrix}.$$

Поскольку корни  $(x^4 - 1)$  образуют упорядоченное множество  $\alpha = (1, j, -1, -j)$ , то переходу (16) соответствует матрица

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

которая отображает конкатенацию  $(\beta, \gamma)$  в множество корней  $\alpha$ . Используя (13), запишем полиномиальное преобразование для данной модели сигнала:

$$\mathcal{P}_{b,\alpha} = \text{DFT}_4 = P \begin{bmatrix} \mathcal{P}_{c,\beta} & \\ & \mathcal{P}_{d,\gamma} \end{bmatrix} B =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ & 1 & j \\ & 1 & -j \end{bmatrix} \quad (17)$$

$$\cdot \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}.$$

Выражение (17) представляет собой факторизацию матрицы 4-точечного ДПФ. Каждая матрица-сомножитель является слабозаполненной, из чего следует, что (17) определяет быстрый алгоритм для  $\text{DFT}_4$ .

## 2. Модели сигналов дискретных тригонометрических преобразований

### Дискретные тригонометрические преобразования.

Шестнадцать типов дискретных тригонометрических преобразований (ДТП) (восемь косинусных и восемь синусных преобразований) являются преобразованиями Фурье для соответствующих моделей одномерного конечно-пространства [5]. Наиболее широкое распространение получило ДКП-2, применяемое в стандарте кодирования изображений JPEG [10], а также ДКП-4, применяемое в стандарте кодирования аудио MP3, а также при построении косинусно-модулированных банков фильтров.

В отличие от дискретной модели времени, которая определяет ДПФ, для моделей конечно-пространства базисными полиномами являются полиномы Чебышева первого ( $T_\ell$ ), второго ( $U_\ell$ ), третьего ( $V_\ell$ ) и четвертого ( $W_\ell$ ) рода.

### Полиномы Чебышева

Полиномы Чебышева [11] образуют специальный класс ортогональных многочленов и играют важную роль во многих областях математики. В данном подразделе рассматриваются только те свойства полиномов Чебышева, которые будут использованы в дальнейшем изучении.

Обозначим через  $C_0(x) = 1$  и  $C_1(x)$  полиномы нулевой и первой степени, тогда  $C_n(x)$  для  $n > 1$  определяется рекуррентной формулой  $C_n(x) = 2xC_{n-1}(x) - C_{n-2}(x)$ .

Данный ряд полностью определяется условием  $C_0 = 1$  и выбором  $C_1$ . Для ЦОС практическую значимость имеют четыре частных случая полиномов Чебышева [5]. Они обозначаются, как  $C \in \{T, U, V, W\}$  и называются полиномами Чебышева первого, второго, третьего и четвертого рода (Таблица 1).

В дальнейшем рассмотрении понадобятся сведения факторизации полиномов Чебышева над полем рациональных чисел [4]. В [12] доказываются теоремы, которые будут нами использованы в дальнейшем.

Таблица 1  
Полиномы Чебышева 1-4 рода.

	Первые члены ряда	Аналитический вид ( $\cos \theta = x$ )	Вид симметрии	Корни, $0 \leq k < n$
$T_n$	$1, x$	$\cos(n\theta)$	$T_{-n} = T_n$	$\cos \frac{(k+\frac{1}{2})\pi}{n}$
$U_n$	$1, 2x$	$\frac{\sin(n+1)\theta}{\sin \theta}$	$U_{-n} = -U_{n-2}$	$\cos \frac{(k+1)\pi}{n+1}$
$V_n$	$1, 2x - 1$	$\frac{\cos(n+\frac{1}{2})\theta}{\cos \frac{1}{2}\theta}$	$V_{-n} = V_{n-1}$	$\cos \frac{(k+\frac{1}{2})\pi}{n+\frac{1}{2}}$
$W_n$	$1, 2x + 1$	$\frac{\sin(n+\frac{1}{2})\theta}{\sin \frac{1}{2}\theta}$	$W_{-n} = -W_{n-1}$	$\cos \frac{(k+1)\pi}{n+\frac{1}{2}}$

**Теорема 2.** Пусть  $n > 1$  целое число, тогда

$$T_n(x) = 2^{n-1} \prod_h D_h(x),$$

$$D_h(x) = \prod_{\substack{k=1 \\ (2k-1)n=h}}^n \left( x - \cos \frac{(k+\frac{1}{2})\pi}{n} \right), \quad (18)$$

где  $h \leq n$  пробегает через все положительные делители  $n$  и  $D_h(x)$  – неприводимый полином над полем рациональных чисел.

**Теорема 3.** Пусть  $n \geq 2$  целое число, тогда

$$U_n(x) = \prod_h E_h(x),$$

$$E_h(x) = 2^{l_h} \prod_{\substack{k=1 \\ (k, 2n+2)=h}}^n \left( x - \cos \frac{(k+1)\pi}{n+1} \right), \quad (19)$$

где  $h \leq n$  пробегает все положительные делители числа  $(2n+2)$  и  $E_h(x)$  – неприводимые полиномы над полем рациональных чисел, через  $(k, n)$  обозначается наибольший общий делитель чисел  $k$  и  $n$ . В последнем выражении  $l_h = \phi((2n+2)/h)/2$  ( $\phi$  – функция Эйлера).

### Модели сигнала для ДКП-2 и ДКП-4

В [5] показано, что ДКП-2 отвечает модель сигнала  $\mathcal{M} = \mathcal{A} = \mathbb{C}[x]/2(x-1)U_{n-1}$  с обобщенным z-преобразованием, которое в данном случае носит название конечно- $V$ -преобразования

$$\mathcal{Z}: \mathbb{C}^n \rightarrow \mathcal{M}, \quad s \mapsto \sum_{0 \leq \ell < n} s_\ell V_\ell \in \mathcal{M}, \quad \text{где } s \in \mathbb{C}^n.$$

После того, как определена модель сигнала  $(\mathcal{A}, \mathcal{M}, \mathcal{Z})$  остальные концепции, такие как преобразование Фурье и свертка выводятся автоматически. Покажем, что для рассматриваемой модели сигнала преобразование Фурье совпадает с ДКП-2. Согласно таблице 1, корни полинома  $2(x-1)U_{n-1}$  задаются выражением  $\alpha_k = \cos k\pi/n, 0 \leq k < n$ . Таким образом, преобразование Фурье для  $\mathcal{M}$  в соответствии с (8)

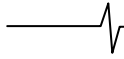
$$\mathcal{P}_{b,\alpha} = [V_\ell(\alpha_k)]_{0 \leq \ell, k < n} = \left[ \frac{1}{\cos k\pi/2n} \cdot \cos \frac{k(\ell + \frac{1}{2})\pi}{n} \right]_{0 \leq \ell, k < n}.$$

Для получения ДКП-2 необходимо выполнить масштабирование полученного преобразования

$$\text{DCT}_{2n} = \text{diag}_{0 \leq k < n} (\cos k\pi/(2n)) \cdot [V_\ell(\alpha_k)]_{0 \leq \ell, k < n}. \quad (20)$$

Тем самым показывается, что  $\text{DCT}_{2n}$  является преобразованием Фурье для регулярного модуля  $\mathcal{M} = \mathbb{C}[x]/(x-1)U_{n-1}$ .





ДКП-4 соответствует модель сигнала  $\mathcal{M} = \mathcal{A} = \mathbb{C}[x]/2T_n$  с базисом  $\mathbf{b} = (V_0, \dots, V_{n-1})$  и обобщённым z-преобразованием таким же, как и у ДКП-2. Корнями полинома  $2T_n(x)$  являются числа  $\alpha_k = \cos(k+\frac{1}{2})\pi/n$ . Следовательно, полиномиальное преобразование данной модели сигнала задаётся как

$$\mathcal{P}_{b,a} = [V_\ell(\alpha_k)]_{0 \leq \ell, k < n} = \left[ \frac{1}{\cos(k+\frac{1}{2})\pi/(2n)} \cdot \cos \frac{(k+\frac{1}{2})(\ell+\frac{1}{2})\pi}{n} \right]_{0 \leq \ell, k < n} \quad (21)$$

ДКП-4 получается из (21) умножением на диагональную матрицу

$$\text{DCT}4_n = \text{diag}_{0 \leq k < n} \left( \cos \frac{(k+\frac{1}{2})\pi}{2n} \right) \cdot [V_\ell(\alpha_k)]_{0 \leq \ell, k < n} \quad (22)$$

Каждому дискретному тригонометрическому преобразованию ДТТ отвечает полиномиальное преобразование, которое обозначается как  $\overline{\text{ДТТ}}$ . Например  $\overline{\text{DCT}}2_n$  соответствует матрица (20).

### 3. Синтез быстрых алгоритмов ДКП-2 и ДКП-4

#### Основная идея

В разделе 1 было показано, что синтез быстрого алгоритма преобразования, связанного с алгеброй  $\mathcal{A} = \mathbb{C}[x]/p(x)$ , строится на основе факторизации полинома  $p(x)$ . Для ДКП-2 и ДКП-4 в роли  $p(x)$  выступают полиномы  $2(x-1)U_{n-1}(x)$  и  $2T_n(x)$ , соответственно. Основная идея состоит в использовании для синтеза быстрых алгоритмов факторизации  $U_{n-1}(x)$  и  $T_n(x)$  соотношений (19) и (18) соответственно. При этом в качестве основного поля изначально выбирается поле рациональных чисел  $\mathbb{Q}$ :

$$\mathbb{Q}[x]/2(x-1)U_{n-1}(x) \rightarrow \mathbb{Q}[x]/2(x-1) \oplus \bigoplus_h \mathbb{Q}[x], \quad (23)$$

$$\mathbb{Q}[x]/2T_n(x) \rightarrow \bigoplus_h \mathbb{Q}[x]/D_h(x). \quad (24)$$

Разложения (23) и (24) требуют операции умножения на элементы из поля рациональных чисел, которые, как правило, имеют простую аппаратную реализацию. Отсутствие нетривиальных умножений обусловлено тем, что полиномы  $U_{n-1}(x)$  и  $T_n(x)$  имеют разложение над  $\mathbb{Q}$ .

Поскольку полиномы  $E_h$  и  $D_h$  неприводимы над  $\mathbb{Q}$ , то для выполнения декомпозиции подмодулей  $\mathbb{Q}[x]/E_h(x)$  и  $\mathbb{Q}[x]/D_h(x)$  необходимо расширить основное поле  $\mathbb{Q}$  до поля разложения полинома  $E_h$  и  $D_h$  соответственно. Такое расширение выполняется последовательно, используя башню полей, которая строится с использованием основной теоремы теории Галуа [13].

В следующем разделе приводится описание основных понятий из теории групп и теории Галуа, которые используются при описании процедуры синтеза быстрых алгоритмов.

#### Основные понятия теории групп и теории Галуа

**Определение группы.** Группой  $G$  называется совокупность элементов, на которой задана групповая операция « $\cdot$ », сопоставляющая любой паре элементов  $g_1, g_2 \in G$  некоторый элемент  $g_3$  из той же совокупности  $G$ . При этом групповая операция должна удовлетворять трём условиям:

- ассоциативность:  $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ ;
- существование единицы: в группе есть такой элемент  $e$  (иногда обозначается «1»), что  $e \cdot g = g, e = g$  для всех  $g \in G$ ;
- существование обратного элемента: для любого  $g \in G$  существует такой  $g^{-1} \in G$ , что  $g \cdot g^{-1} = g^{-1} \cdot g = e$ .

**Поле разложение полинома.** Для полинома  $p(x) \in \mathbb{F}[x]$  полем разложения называют наименьшее расширение  $\mathbb{F}$ , которое содержит все корни  $p(x)$ . Например, для  $p(x) =$

$x^2 - 2$  полем разложения является  $\mathbb{Q}(\sqrt{2})$ . Поле  $\mathbb{Q}(\sqrt{2})$  есть расширение поля  $\mathbb{Q}$ , которое образуется из  $\mathbb{Q}$  присоединением числа  $\sqrt{2}$ . Все элементы поля  $\mathbb{Q}(\sqrt{2})$  имеют вид:  $a + b\sqrt{2}$ , где  $a, b \in \mathbb{Q}$ ,

**Аutomорфизмы полей.** Взаимнооднозначное отображение  $\mathcal{B}: G \rightarrow G$  группы на себя, сохраняющее групповую операцию, называют автоморфизмом. Группа автоморфизмов обозначается  $\text{Aut } G$ . Автоморфизмы полей  $\mathcal{B}: \mathbb{F} \rightarrow \mathbb{F}$  определяются аналогично, с тем уточнением, что взаимнооднозначное отображение  $\mathcal{B}$  поля на себя обязано сохранять обе операции [12],

$$\mathcal{B}(x+y) = \mathcal{B}(x) + \mathcal{B}(y), \mathcal{B}(xy) = \mathcal{B}(x)\mathcal{B}(y), x, y \in \mathbb{F}.$$

**Пример: определим функцию  $f: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$**

**следующим образом**

$$f(a + b\sqrt{2}) = a - b\sqrt{2}, \quad (25)$$

тогда  $f$  – автоморфизм поля  $\mathbb{Q}(\sqrt{2})$ . Таким образом, суть идеи автоморфизма полей состоит в перенумерации элементов поля, без изменения его структуры в целом.

Пусть  $\mathbb{E}$  нормальное расширение поля  $\mathbb{F}$  (т.е.  $\mathbb{E} \supset \mathbb{F}$ ). В группе автоморфизмов  $\text{Aut } \mathbb{E}$  выделим подгруппу  $\text{Aut } \mathbb{E}/\mathbb{F}$  тех автоморфизмов  $\mathcal{B}: \mathbb{E} \rightarrow \mathbb{E}$ , которые поле  $\mathbb{F}$  оставляют на месте, т.е.  $\mathcal{B}(x) = x$ , если  $x \in \mathbb{F}$ . Элементы группы  $\text{Aut } \mathbb{E}/\mathbb{F}$  называют автоморфизмами поля  $\mathbb{E}$ . Например, автоморфизм (25) определяет  $\mathbb{Q}$ -автоморфизм поля  $\mathbb{Q}(\sqrt{2})$ .

Рассмотрим полином  $p(x) \in \mathbb{F}[x]$ , не имеющий кратных корней, полем разложения которого является расширение  $\mathbb{E}$ , тогда группу  $\text{Aut } \mathbb{E}/\mathbb{F}$  называют группой Галуа полинома  $p(x)$  (или соответствующего расширения  $\mathbb{E}$ ) и обозначают  $\text{Gal}(\mathbb{E}/\mathbb{F})$ . Возьмём полином  $p(x) = x^2 - 2$ , полем разложения которого является  $\mathbb{Q}(\sqrt{2})$ . Группа Галуа полинома  $p(x)$  состоит из двух элементов  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{f, g\}$ , где  $f$  определена в (25), а  $g(a + b\sqrt{2}) = a + b\sqrt{2}$ . Очевидно, что  $g$  – единичный элемент группы (оставляет все на своих местах), также справедливо тождество  $f \cdot f = g$ . Полученная группа является циклической группой второго порядка.

**Соответствие Галуа.** Стержнем теории Галуа является соответствие между структурой расширения полей и структурой подгрупп автоморфизмов. Каждой подгруппе  $H \subset \text{Gal}(\mathbb{E}/\mathbb{F})$  отвечает подполе  $\mathbb{L} \subset \mathbb{E}$ , состоящее из элементов  $\mathbb{F}$ , неподвижных под действием автоморфизмов из  $H$ . И наоборот, каждому подполю  $\mathbb{L} \subset \mathbb{E}$  отвечает подгруппа  $H$  автоморфизмов, оставляющих элементы  $\mathbb{L}$  на месте. В результате изучение всех подполей поля  $\mathbb{E}$  сводится к изучению всех подгрупп группы  $\text{Gal}(\mathbb{E}/\mathbb{F})$ . При этом каждой башне (цепочке вложенных) полей

$$\mathbb{F} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \dots \subset \mathbb{L}_r = \mathbb{E}, \quad (26)$$

отвечает нормальный ряд вложенных (в противоположном направлении) групп

$$\text{Gal}(\mathbb{E}/\mathbb{F}) = G_0 \supset G_1 \supset \dots \supset G_r = \{1\}, \quad (27)$$

и наоборот (соответствие Галуа).

Если имеется неприводимый полином  $p(x)$  с коэффициентами из поля  $\mathbb{F}$ , полем разложения которого является  $\mathbb{E}$ , то используя соответствие Галуа для него, можно построить башню полей (26). Причём в каждом поле  $\mathbb{L}_i$   $p(x)$  будет распадаться в произведение неприводимых полиномов, а в поле  $\mathbb{E}$  разложиться в произведение линейных сомножителей. Таким образом, использование (26) позволяет выполнить поэтапную факторизацию полинома  $p(x)$ , что и требуется при синтезе быстрого алгоритма дискретного тригонометрического преобразования.

#### Быстрый алгоритм 4-точечного ДКП-2

В данном разделе подробно рассматривается пример синтеза быстрого алгоритма 4-точечного ДКП-2 на базе теоретического материала изложенного в предыдущих разделах. Исходным пунктом является модель

сигнала для ДКП-2:

$$\mathcal{A} = \mathcal{M} = \frac{\mathbb{Q}[x]}{V_4 - V_3} = \frac{\mathbb{Q}[x]}{2(x-1)U_3}, \quad (3)$$

$$\mathbf{b} = (V_0, \dots, V_3)$$

Рассмотрим полином  $p(x) = 2(x-1)U_3(x)$ , используя выражение (19) для факторизации  $U_3(x)$  над полем  $\mathbb{Q}$ , получаем

$$p(x) = (2x-2)(2x)(4x^2-2), \quad (29)$$

откуда, объединив на время сомножители, взятые в фигурную скобку, находим

$$p(x) = V_4(x) - V_3(x) = (4x^2 - 4x)(4x^2 - 2) = (V_2(x) - V_1(x))(V_2(x) + V_1(x)). \quad (30)$$

Согласно таблице 1, корни полинома  $p(x)$  равны  $\alpha_k = \cos k\pi/4, k = 0, \dots, 3$ . Поскольку для исходного модуля  $\mathcal{M}$  задан базис  $\mathbf{b} = (V_0, \dots, V_3)$ , нам важно факторизовать полином  $p$  в том же базисе. Теперь, используя (30) и КТО, получаем:

$$\mathbb{Q}[x]/(V_4 - V_3) \rightarrow \mathbb{Q}[x]/(V_2 - V_1) \oplus \mathbb{Q}[x]/(V_2 + V_1). \quad (31)$$

Преобразованию (31) соответствует матрица смены базиса  $B_4$ . Для определения  $B_4$  необходимо выразить базисные элементы  $V_\ell \in \mathbf{b}$  в базисе  $(c, d)$ , где  $c$  и  $d$  – это базис подмодуля  $\mathbb{Q}[x]/(V_2 - V_1)$  и  $\mathbb{Q}[x]/(V_2 + V_1)$ , соответственно. В таблице 2 производятся необходимые вычисления.

Используя последний столбец таблицы 2, получаем матрицу  $B_4$  смены базиса

$$\mathbf{b} \mapsto (c, d): B_4 = \begin{bmatrix} I_2 & J_2 \\ I_2 & -J_2 \end{bmatrix}.$$

Важно отметить тот факт что, разложение полинома  $p = V_4 - V_3 = (V_2 - V_1)(V_2 + V_1)$  над полем  $\mathbb{Q}$  приводит к тому, что переход (31), реализуемый в виде матрицы  $B_4$ , не требует умножения на числа не из поля  $\mathbb{Q}$ .

Таблица 2

Переход от базиса  $\mathbf{b}$  к базису  $(c, d)$ , где  $c = d = (V_0, V_1)$

Номер базисного элемента $\ell$	$V_\ell \bmod (V_2 - V_1)$	$V_\ell \bmod (V_2 + V_1)$	$\mathbf{b} \mapsto (c, d)$
0	$V_0 \bmod (V_2 - V_1) = V_0,$	$V_0 \bmod (V_2 + V_1) = V_0,$	$V_0 \mapsto (V_0, V_0)$
1	$V_1 \bmod (V_2 - V_1) = V_1,$	$V_1 \bmod (V_2 + V_1) = V_1,$	$V_1 \mapsto (V_1, V_1)$
2	$V_2 \bmod (V_2 - V_1) = V_1,$	$V_2 \bmod (V_2 + V_1) = -V_1,$	$V_2 \mapsto (V_1, -V_1)$
3	$V_3 \bmod (V_2 - V_1) = V_0,$	$V_3 \bmod (V_2 + V_1) = -V_0,$	$V_3 \mapsto (V_0, -V_0)$

Отметим, что слагаемые в правой части (31) соответствуют алгебрам для 2-точечных ДКП-2 и ДКП-4, соответственно. Тем самым задача синтеза быстрого алгоритма 4-точечного ДКП-2 распадается на две подзадачи синтеза быстрых алгоритмов для 2-точечных ДКП-2 и ДКП-4.

Продолжим рассмотрение модуля  $\mathbb{Q}[x]/(V_2 - V_1)$ , который раскладывается на два неприводимых модуля (размерности один), используя соотношение  $V_2(x) - V_1(x) = (2x-2)(2x) = (V_1(x) - 1)(V_1(x) + 1)$  следующим образом

$$\mathbb{Q}[x]/(V_2 - V_1) \rightarrow \mathbb{Q}[x]/(V_1 - 1) \oplus \mathbb{Q}[x]/(V_1 + 1). \quad (32)$$

Преобразованию (32) отвечает матрица

$$B_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Шаги (31)-(32) позволяют выполнить частичную декомпозицию исходного модуля  $\mathcal{M}$ :

$$\mathbb{Q}[x]/(V_4 - V_3) \rightarrow \mathbb{Q}[x]/(V_1 - 1) \oplus \mathbb{Q}[x]/(V_1 + 1) \oplus \mathbb{Q}[x]/(V_2 + V_1), \quad (33)$$

которой соответствует факторизация (29). Наша конечная цель состоит в полном разложении  $\mathcal{M}$  на неприводимые подмодули размерности один. Чтобы продолжить разложение (33), необходимо расширить основное поле  $\mathbb{Q}$ .

Рассмотрим полином  $V_2(x) + V_1(x) = 4x^2 - 2$ , очевидно, что полем его разложения является  $\mathbb{Q}(\sqrt{2})$ , которое для краткости обозначим  $\mathbb{Q}_{\sqrt{2}}$ :

$$V_2(x) + V_1(x) = (2x - \sqrt{2})(2x + \sqrt{2}) = (V_1(x) + (1 - \sqrt{2}))(V_1(x) + (1 + \sqrt{2})).$$

Воспользуемся данной факторизацией для разложения модуля  $\mathbb{Q}[x]/(V_2 + V_1)$ :

$$\mathbb{Q}[x]/(V_2 + V_1) \rightarrow \mathbb{Q}_{\sqrt{2}}[x]/(V_1 - (1 - \sqrt{2})) \oplus \mathbb{Q}_{\sqrt{2}}[x]/(V_1 + (1 + \sqrt{2})), \quad (34)$$

учитывая, что

$$V_0 \bmod (V_1 + (1 - \sqrt{2})) = V_0 \equiv 1,$$

$$V_1 \bmod (V_1 + (1 - \sqrt{2})) = \sqrt{2} - 1,$$

$$V_0 \bmod (V_1 + (1 + \sqrt{2})) = V_0 \equiv 1,$$

$$V_1 \bmod (V_1 + (1 + \sqrt{2})) = -\sqrt{2} - 1,$$

матрица перехода, отвечающая (34), запишется как

$$T_2 = \begin{bmatrix} 1 & \sqrt{2} - 1 \\ 1 & -\sqrt{2} - 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ & \sqrt{2} \end{bmatrix}. \quad (35)$$

Из (35) легко заметить, что умножение на матрицу  $T_2$  требует только одной операции умножения.

Выполнение (34) завершает полное (позатупное) разложение модуля  $\mathcal{M} = \mathbb{Q}[x]/(V_4 - V_3)$ , описывающего 4-точечное ДКП-2, на неприводимые подмодули размерности один (Рис. 1).

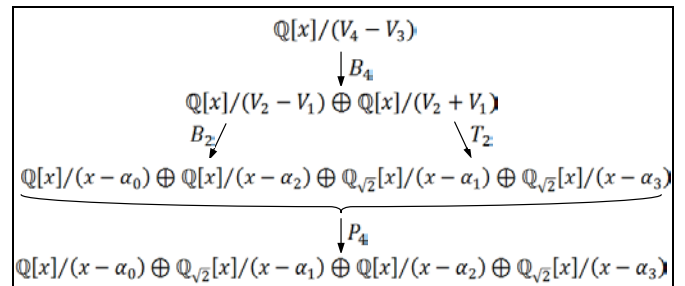


Рис. 1 – Общая схема разложения модуля  $\mathcal{M} = \mathbb{Q}[x]/(V_4 - V_3)$

На рис. 1 учитывается, что

$$\mathbb{Q}[x]/(V_1 - 1) \cong \mathbb{Q}[x]/(x - 1) = \mathbb{Q}[x]/(x - \alpha_0),$$

$$\mathbb{Q}[x]/(V_1 + 1) \cong \mathbb{Q}[x]/(x - 0) = \mathbb{Q}[x]/(x - \alpha_2),$$

$$\mathbb{Q}_{\sqrt{2}}[x]/(V_1 - (1 - \sqrt{2})) \cong$$

$$\cong \mathbb{Q}_{\sqrt{2}}[x]/(x - \sqrt{2}/2) = \mathbb{Q}_{\sqrt{2}}[x]/(x - \alpha_1),$$

$$\mathbb{Q}_{\sqrt{2}}[x]/(V_1 + (1 + \sqrt{2})) \cong$$

$$\cong \mathbb{Q}_{\sqrt{2}}[x]/(x + \sqrt{2}/2) = \mathbb{Q}_{\sqrt{2}}[x]/(x - \alpha_3).$$

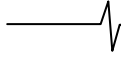
Матрица  $P_4$  отвечает за перестановку неприводимых подмодулей в нужном порядке

$$P_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Полиномиальное преобразование для модели сигнала (28), описывающей 4-точечное ДКП-2, имеет вид  $DCT\mathbf{2}_4 = \mathcal{P}_{b,\alpha} = P_4(B_2 \oplus T_2)B_4$ .

В соответствии с (20), для получения матрицы ДКП-2 необходимо  $\overline{DCT}\mathbf{2}_4$  умножить на масштабирующую диагональную матрицу:  $DCT\mathbf{2}_4 = \text{diag}_{0 \leq k < 4}(\cos k\pi/8) \cdot \overline{DCT}\mathbf{2}_4$ .

В итоге получен быстрый алгоритм 4-точечного ДКП-2,



требующий четырёх операций умножения (одно умножение для  $\overline{\text{DCT}}_4$  и три умножения для  $\text{diag}_{0 \leq k < 4}(\cos k\pi/8)$ ).

#### Быстрый алгоритм 4-точечного ДКП-4

В качестве ещё одного примера рассмотрим синтез быстрого алгоритма 4-точечного ДКП-4, модель сигнала которого приведена ниже

$$\mathcal{A} = \mathcal{M} = \frac{\mathbb{Q}[x]}{V_4 + V_3} = \frac{\mathbb{Q}[x]}{2T_4}, \mathbf{b} = (V_0, \dots, V_3).$$

Анализ полинома  $p(x) = 2T_4(x)$  с использованием выражения (18) показывает, что  $T_4(x)$  неприводим над полем  $\mathbb{Q}$ . Поэтому для его поэтапной факторизации необходимо расширить основное поле  $\mathbb{Q}$ . Корнями полинома  $T_4(x)$  являются  $\alpha_k = \cos(k + \frac{1}{2})\pi/4$ ,  $k = 0, \dots, 3$ , поэтому  $\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$  – поле разложения полинома  $p(x)$ . Если заметить, что

$$\alpha_0 = \cos \frac{\pi}{8} = -\alpha_3 = -\cos \frac{7\pi}{8} = \frac{1}{2}\sqrt{2+\sqrt{2}},$$

$$\alpha_1 = \cos \frac{3\pi}{8} = -\alpha_2 = -\cos \frac{5\pi}{8} = \frac{1}{2}\sqrt{2-\sqrt{2}},$$

то поле разложения полинома  $p(x)$  запишется как  $\mathbb{Q}(\alpha_0, \alpha_1) \cong \mathbb{Q}(\sqrt{2+\sqrt{2}})$ . Поле  $\mathbb{Q}(\alpha_0, \alpha_1)$  можно рассматривать, как четырехмерное векторное пространство, поскольку любой элемент  $\theta \in \mathbb{Q}(\alpha_0, \alpha_1)$  представим в виде  $\theta = a + b\alpha_0 + c\alpha_1 + d\alpha_0\alpha_1$ , где  $a, b, c, d \in \mathbb{Q}$ . Группа  $\text{Aut } \mathbb{Q}(\alpha_0, \alpha_1)/\mathbb{Q}$  является группой Галуа полинома  $p(x)$ . Элементами группы Галуа являются следующие автоморфизмы:

$$g_0(\theta) = \theta, g_1(\theta) = a + c\alpha_0 + b\alpha_1 + d\alpha_0\alpha_1,$$

$$g_2(\theta) = a + b\alpha_0 + c\alpha_1 - d\alpha_1\alpha_0,$$

$$g_3(\theta) = a + c\alpha_0 + b\alpha_1 - d\alpha_1\alpha_0.$$

Приведём таблицу Кэли для данной группы автоморфизмов (таблица 3).

Таблица 3  
Таблица Кэли группы  $\text{Gal}\left(\frac{\mathbb{Q}(\alpha_0, \alpha_1)}{\mathbb{Q}}\right) = \text{Aut}\frac{\mathbb{Q}(\alpha_0, \alpha_1)}{\mathbb{Q}}$

$\circ$	$g_0$	$g_1$	$g_2$	$g_3$
$g_0$	$g_0$	$g_1$	$g_2$	$g_3$
$g_1$	$g_1$	$g_0$	$g_3$	$g_2$
$g_2$	$g_2$	$g_3$	$g_0$	$g_1$
$g_3$	$g_3$	$g_2$	$g_1$	$g_0$

Из таблицы 3 видно, что  $H \in \{g_0, g_1\}$  образует подгруппу группы  $\text{Gal}(\mathbb{Q}(\alpha_0, \alpha_1)/\mathbb{Q})$ , которая определяет подполе  $\mathbb{Q}_H$  такое, что

$$\mathbb{Q}_H = \{\theta \in \mathbb{Q}(\alpha_0, \alpha_1) | g(\theta) = \theta \forall g \in H\}.$$

В рассматриваемом случае  $\mathbb{Q}_H = \mathbb{Q}(\alpha_0, \alpha_1) \cong \mathbb{Q}(\sqrt{2})$ . Таким образом, согласно теории Галуа (26)-(27), получаем нормальный ряд вложенных групп  $\text{Gal}(\mathbb{Q}(\alpha_0, \alpha_1)/\mathbb{Q}) \supset H \supset \{1\}$ , которому отвечает башня полей  $\mathbb{Q} \subset \mathbb{Q}(\alpha_0, \alpha_1) \subset \mathbb{Q}(\alpha_0, \alpha_1)$ . (36)

На основании (36) можно предложить следующую схему факторизации полинома  $p(x)$ ,

$$p = \frac{V_4 + V_3}{\mathbb{Q}} = \frac{(V_2 + V_1 - \sqrt{2})(V_2 + V_1 + \sqrt{2})}{\mathbb{Q}(\alpha_0, \alpha_1)} =$$

$$= \underbrace{\left( V_1 + \left( 1 - \sqrt{2 + \sqrt{2}} \right) \right) \left( V_1 + \left( 1 + \sqrt{2 + \sqrt{2}} \right) \right) \left( V_1 + \left( 1 - \sqrt{2 - \sqrt{2}} \right) \right) \left( V_1 + \left( 1 + \sqrt{2 - \sqrt{2}} \right) \right)}_{\mathbb{Q}(\alpha_0, \alpha_1)}, \quad (37)$$

где над фигурными скобками указаны соответствующие поля разложения.

Руководствуясь (37), предлагается следующая схема разложения модуля  $\mathcal{M} = \mathbb{Q}[x]/p$

$$\begin{aligned} \mathbb{Q}[x]/(V_4 + V_3) &\xrightarrow{R_4} \mathbb{Q}_{\alpha_0, \alpha_1}[x]/(V_2 + V_1 - \sqrt{2}) \oplus \\ &\quad \oplus \mathbb{Q}_{\alpha_0, \alpha_1}[x]/(V_2 + V_1 + \sqrt{2}) \\ &\xrightarrow{R_2 \oplus S_2} \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/\left(V_1 + (1 - \sqrt{2 + \sqrt{2}})\right) \oplus \\ &\quad \oplus \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/\left(V_1 + (1 + \sqrt{2 + \sqrt{2}})\right) \oplus \\ &\quad \oplus \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/\left(V_1 + (1 - \sqrt{2 - \sqrt{2}})\right) \oplus \\ &\quad \oplus \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/\left(V_1 + (1 + \sqrt{2 - \sqrt{2}})\right) \\ &\xrightarrow{P_4} \bigoplus_{0 \leq i < 4} \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(x - \alpha_i). \end{aligned} \quad (38)$$

Над стрелками в (38) указаны матрицы, отвечающие за соответствующий переход, также во всех подмодулях предполагается, что базис состоит из полиномов Чебышева третьего рода  $V_\ell$ . В таблице 4 приведены вычисления, необходимые для определения матрицы  $R_4$ .

Таблица 4.

Вычисление матрицы  $R_4$

Номер базисного элемента $\ell$	$V_\ell \text{ mod } (V_2 + V_1 - \sqrt{2})$	$V_\ell \text{ mod } (V_2 + V_1 + \sqrt{2})$
0	$V_0$	$V_0$
1	$V_1$	$V_1$
2	$-V_1 + \sqrt{2}V_0$	$-V_1 - \sqrt{2}V_0$
3	$\sqrt{2}V_1 - V_0$	$-\sqrt{2}V_1 - V_0$

Используя таблицу 4, можно записать матрицу

$$\begin{aligned} R_4 &= \begin{bmatrix} 1 & \sqrt{2} & -1 \\ & 1 & -1 & \sqrt{2} \\ 1 & -\sqrt{2} & -1 \\ & 1 & -1 & -\sqrt{2} \end{bmatrix} = \\ &= \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ 1 & & & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & & & \\ & 1 & -1 & \\ & & \sqrt{2} & \\ & & & \sqrt{2} \end{bmatrix}. \end{aligned}$$

Исходя из соотношений:

$$V_0 \text{ mod } \left( V_1 + (1 - \sqrt{2 + \sqrt{2}}) \right) = V_0 \equiv 1,$$

$$V_1 \text{ mod } \left( V_1 + (1 - \sqrt{2 + \sqrt{2}}) \right) = \sqrt{2 + \sqrt{2}} - 1,$$

$$V_0 \text{ mod } \left( V_1 + (1 + \sqrt{2 + \sqrt{2}}) \right) = V_0 \equiv 1,$$

$$V_1 \text{ mod } \left( V_1 + (1 + \sqrt{2 + \sqrt{2}}) \right) = -\sqrt{2 + \sqrt{2}} - 1,$$

определяется матрица  $R_2$

$$R_2 = \begin{bmatrix} 1 & \sqrt{2 + \sqrt{2}} - 1 \\ 1 & -\sqrt{2 + \sqrt{2}} - 1 \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ & \sqrt{2 + \sqrt{2}} \end{bmatrix}.$$

Аналогично из

$$V_0 \text{ mod } \left( V_1 + (1 - \sqrt{2 - \sqrt{2}}) \right) = V_0 \equiv 1,$$

$$V_1 \text{ mod } \left( V_1 + (1 - \sqrt{2 - \sqrt{2}}) \right) = \sqrt{2 - \sqrt{2}} - 1,$$

$$V_0 \text{ mod } \left( V_1 + (1 + \sqrt{2 - \sqrt{2}}) \right) = V_0 \equiv 1,$$

$$V_1 \text{ mod } \left( V_1 + (1 + \sqrt{2 - \sqrt{2}}) \right) = -\sqrt{2 - \sqrt{2}} - 1,$$

находится матрица

$$S_2 = \begin{bmatrix} 1 & \sqrt{2-\sqrt{2}} - 1 \\ 1 & -\sqrt{2-\sqrt{2}} - 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ \sqrt{2-\sqrt{2}} \end{bmatrix}.$$

Поскольку

$$\mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(v_1 + (1 - \sqrt{2 + \sqrt{2}})) \cong \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(x - \alpha_0),$$

$$\mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(v_1 + (1 + \sqrt{2 + \sqrt{2}})) \cong \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(x - \alpha_3),$$

$$\mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(v_1 + (1 - \sqrt{2 - \sqrt{2}})) \cong \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(x - \alpha_1),$$

$$\mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(v_1 + (1 + \sqrt{2 - \sqrt{2}})) \cong \mathbb{Q}_{(\alpha_0, \alpha_1)}[x]/(x - \alpha_2),$$

то матрица перестановки в (38) определяется как

$$P_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Полиномиальное преобразование 4-точечного ДКП-4, согласно пошаговой декомпозиции (38), имеет вид

$$\overline{\text{DCT}}_4 = \mathcal{P}_{b,\alpha} = P_4(R_2 \oplus S_2)R_4.$$

Матрица ДКП-4 получается из  $\overline{\text{DCT}}_4$ , согласно (22), умножением на масштабирующую диагональную матрицу:

$$\text{DCT}_4 = \text{diag}_{0 \leq k < 4}(\cos(k + \frac{1}{2})\pi/8) \cdot \overline{\text{DCT}}_4.$$

В итоге получен быстрый алгоритм 4-точечного ДКП-4, требующий восемь операций умножения (четыре умножения для  $\overline{\text{DCT}}_4$  и четыре умножения для  $\text{diag}_{0 \leq k < 4}(\cos k\pi/8)$ ).

### Быстрый алгоритм 8-точечного ДКП-2

Самое широкое распространение в последнее время получил алгоритм 8-точечного ДКП-2, что связано с его применением в стандарте кодирования изображений JPEG [10]. Применим предлагаемый в статье подход к синтезу быстрого алгоритма 8-точечного ДКП-2. Как и в предыдущих примерах, начальным пунктом является модель сигнала, описывающего ДКП-2:

$$\mathcal{A} = \mathcal{M} = \frac{\mathbb{Q}[x]}{V_8 - V_7} = \frac{\mathbb{Q}[x]}{2(x-1)U_7}, \mathbf{b} = (V_0, \dots, V_7)$$

Рассмотрим полином  $p(x) = 2(x-1)U_7(x)$ , используя выражение (19) для факторизации  $U_7(x)$  над полем  $\mathbb{Q}$ , получаем  $p(x) = (2x-2)(2x)(4x^2-2)(16x^4-16x+2)$ ,

откуда, объединив на время сомножители, взятые в фигурную скобку, находим

$$p(x) = (16x^4 - 16x^3 - 8x^2 + 8x)(16x^4 - 16x + 2) = (V_4(x) - V_3(x))(V_4(x) + V_3(x)). \quad (39)$$

Согласно таблице 1, корни полинома  $p(x)$  равны  $\alpha_k = \cos k\pi/8, k = 0, \dots, 7$ . Теперь, используя (39) и КТО, можно перейти от исходного модуля  $\mathcal{M}$  размерности восемь к прямой сумме двух подмодулей размерности четыре:

$$\mathbb{Q}[x]/(V_8 - V_7) \xrightarrow{B_8} \mathbb{Q}[x]/(V_4 - V_3) \oplus \mathbb{Q}[x]/(V_4 + V_3) \quad (40)$$

Преобразованию (40) соответствует матрица смены базиса  $B_8$ . Для определения  $B_8$  необходимо выразить базисные элементы  $\mathbf{b}$  в базисе  $(c, d)$ , где  $c = d = (V_0, \dots, V_3)$  это базис подмодуля  $\mathbb{Q}[x]/(V_4 - V_3)$  и  $\mathbb{Q}[x]/(V_4 + V_3)$ , соответственно. Выполняя действия, аналогичные выполненным в таблице 3, получаем

$$B_8 = \begin{bmatrix} I_4 & J_4 \\ I_4 & -J_4 \end{bmatrix}.$$

Алгебры в правой части (40) соответствуют 4-точечным ДКП-2 и ДКП-4, соответственно. Тем самым задача синтеза быстрого алгоритма 8-точечного ДКП-2 распадается на две подзадачи синтеза быстрых алгоритмов 4-точечных ДКП-2 и ДКП-4, которые были решены в предыдущих разделах. Таким образом, общая схема разложения модуля  $\mathbb{Q}[x]/(V_8 - V_7)$  запишется как

$$\mathbb{Q}[x]/(V_8 - V_7) \xrightarrow{B_8} \mathbb{Q}[x]/(V_4 - V_3) \oplus \mathbb{Q}[x]/(V_4 + V_3)$$

$$\xrightarrow{\overline{\text{DCT}}_4 \oplus \overline{\text{DCT}}_4} \bigoplus_{i=0,2,4,6} \frac{\mathbb{Q}_{(\alpha_2)}[x]}{(x-\alpha_i)} \oplus \quad (41)$$

$$\oplus \bigoplus_{i=1,3,5,7} \mathbb{Q}_{(\alpha_1, \alpha_3)}[x]/(x-\alpha_i)$$

$$\xrightarrow{P_8} \bigoplus_{0 \leq i < 8} \mathbb{Q}_{(\alpha_1, \alpha_3)}[x]/(x-\alpha_i).$$

В (41)  $P_8$  – матрица перестановки неприводимых подмодулей в соответствии с индексами корней полинома  $p = V_8 - V_7$ . Отметим также, что  $\mathbb{Q}_{(\alpha_2)} \cong \mathbb{Q}_{\sqrt{2}}$  является подполем  $\mathbb{Q}_{(\alpha_1, \alpha_3)} \cong \mathbb{Q}_{(\sqrt{2+\sqrt{2}})}$ . Используя (41) получаем быстрый алгоритм полиномиального 8-точечного ДКП-2  $\overline{\text{DCT}}_8 = \mathcal{P}_{b,\alpha} = P_8(\overline{\text{DCT}}_4 \oplus \overline{\text{DCT}}_4)B_8$ .

Для получения матрицы ДКП-2 умножим  $\overline{\text{DCT}}_8$  на масштабирующую диагональную матрицу:

$$\text{DCT}_8 = \text{diag}_{0 \leq k < 8}(\cos k\pi/16) \cdot \overline{\text{DCT}}_8. \quad (42)$$

В итоге получен быстрый алгоритм для 8-точечного ДКП-2. Схема алгоритма, соответствующего (42), приводится на рис. 2. Алгоритм требует 29 сложений и 12 умножений (или 5 умножений, если не выполнять масштабирования).

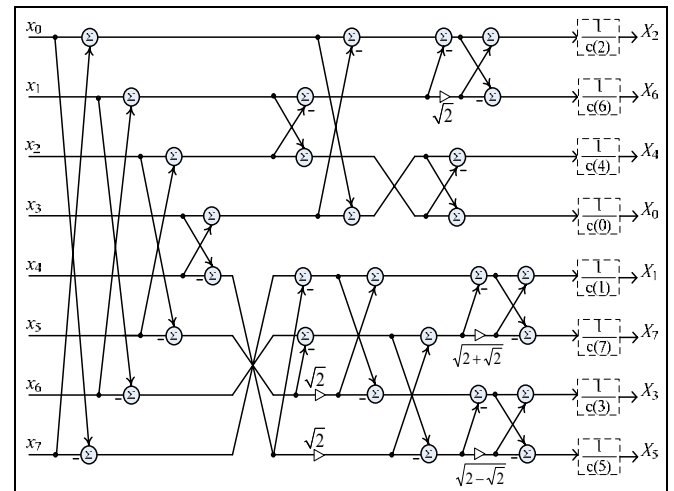


Рис. 2 – Граф-схема быстрого алгоритма 8-точечного ДКП-2,  $c(k) = \cos \frac{\pi k}{16}, k = 0, \dots, 7$

### Заключение

Представлен систематический подход к синтезу быстрых алгоритмов дискретных тригонометрических преобразований на основе алгебраической теории обработки сигналов. Основное внимание уделено дискретным косинусным преобразованием второго и четвертого типов. Используемый в статье подход упрощает синтез быстрых алгоритмов и даёт лучшее представление об их алгебраической структуре. Ключевым является соответствие между дискретным тригонометрическим преобразованием и полиномиальной алгеброй  $\mathbb{Q}[x]/p(x)$ . Быстрый алгоритм получается в результате действий над алгеброй, а не над матрицей преобразования. По сути, быстрый алгоритм сводится к нахождению пошаговой факторизации полинома  $p(x)$ . Для этой цели великолепно подходит теория Галуа, позволяющая определить башню полей, в которых  $p(x)$  раскладывается на сомножители меньшей степени.

В качестве практического результата получен быстрый алгоритм 8-точечного ДКП-2, содержащий в ядре своей структуры только 5 операций умножения и 29 операций сложения.



## Литература

1. Белый А.А., Бовбель Е.И., Микулович В.И. Алгоритмы быстрого преобразования Фурье и их свойства // Зарубежная радиоэлектроника. – 1979. – №2. – С. 3-29.
2. Вайрадян А.С., Пчелинцев И.П., Челышев М.М. Алгоритмы вычисления цифровых сверток // Зарубежная радиоэлектроника. – 1982. – № 3. – С. 3-34.
3. Нуссбаумер, Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток – М.: Радио и связь, 1985. – С. 248.
4. Крот А.М. Дискретные модели динамических систем на основе полиномиальной алгебры – Мн.: Наука и техника, 1990. – С. 312.
5. Püschel M., Moura J.M.F. Algebraic Signal Processing Theory: Cooley-Tukey Type Algorithms for DCTs and DSTs // IEEE Transactions on Signal Processing. – 2008. – Vol. 56, № 4. –1502-1521 pp.
6. Трахтман А.М., Трахтман В.А. Основы теории дискретных сигналов на конечных интервалах – М.: Советское радио, 1975. – С. 208.
7. Шиллов Г.Е. Математический анализ. Конечномерные линейные пространства – М.: Наука, 1969 – С. 421.
8. Püschel M., Moura J.M.F. Algebraic Signal Processing Theory: foundation and 1-D time // IEEE Transactions on Signal Processing. – 2008. – Vol. 56, № 8. – 3572-3585 pp.
9. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов – М.: Мир, 1979. – С. 536.
10. Миано Дж., Форматы и алгоритмы сжатия изображений в действии – М.: Триумф, 2003. – С. 336.
11. Данилов Ю.А., Многочлены Чебышева – Мн.: Вышшая школа, 1984. – С. 160.
12. Rayes M., Trevisan V., Wang P.S. Factorization properties of Chebyshev polynomials // Computers and mathematics with applications. – 2005. – vol. 50. – 1231-1240 pp.
13. Босс В., Теория Групп – М: «Либроком», 2009. – С. 216.

### Application of polynomial algebras and Galois theory for synthesis of fast algorithm of discrete cosine transform

M.I. Vashkevich, A.A. Petrovsky

The systematic approach to synthesis of fast algorithm of discrete cosine transform of type 2 and 4 (DCT-2/DCT-4) based on algebraic signal processing theory (ASP) is proposed. In the ASP framework fast algorithm are not derived by manipulating with the entries of transform matrix, but by stepwise decomposition of polynomial algebra associated with given transform. This decomposition assumes stepwise factorization of polynomial. For that purpose we suggest to use intermediate fields of splitting field of polynomial that obtained by using fundamental theorem of Galois theory.

## 14-я Международная Конференция и Выставка ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ И ЕЁ ПРИМЕНЕНИЕ

28 марта – 30 марта 2012 г., Москва, Россия

The 14<sup>th</sup> International Conference

DIGITAL SIGNAL PROCESSING AND ITS APPLICATIONS

### ИНФОРМАЦИОННОЕ ПИСЬМО

Уважаемый коллега!

Приглашаем Вас принять участие в работе 14-й Международной конференции «Цифровая обработка сигналов и её применение- DSPA'2012», которая состоится в ИПУ РАН 28 марта – 30 марта 2012 года

#### ОРГАНИЗАТОРЫ:

- Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова
- IEEE Signal Processing Society
- Российская секция IEEE
- Институт радиотехники и электроники РАН
- Институт проблем управления РАН
- Институт проблем передачи информации РАН
- Московский научно-исследовательский телевизионный институт (ЗАО МНИТИ)
- Компания AUTEX Ltd. (ЗАО «АВТЭКС»)

#### ПРИ УЧАСТИИ:

- Федеральное агентство по промышленности РФ
- Министерство образования и науки РФ
- Международный союз приборостроителей и специалистов по информационным и телекоммуникационным технологиям
- ФГУП ГКРЧ
- ГСКБ «АЛМАЗ-АНТЕЙ»
- ЗАО «Инструментальные системы»
- НТЦ «МОДУЛЬ»
- ЗАО «СКАН Инжиниринг Телеком»
- ГУП НПЦ «Элвис»
- Владимирский государственный университет
- Московский авиационный институт
- Московский государственный технический университет им. Н.Э. Баумана
- Московский институт радиотехники, электроники и автоматики
- Московский технический университет связи и информатики
- Московский энергетический институт
- Рязанский государственный радиотехнический университет
- Санкт-Петербургский государственный университет телекоммуникаций
- Санкт-Петербургский государственный электротехнический университет – ЛЭТИ
- Ульяновский государственный технический университет
- Ярославский Государственный Университет
- Московский Физико-технический институт (университет)