УДК 539.3

ДИСКРЕТНЫЕ ОРТОГОНАЛЬНЫЕ ПРЕОБРАЗОВАНИЯ С "ХАОТИЧЕСКИМИ" БАЗИСНЫМИ ФУНКЦИЯМИ[1]

© 2005 О.В. Бесполитов[2]

Работа посвящена дискретным ортогональным преобразованиям, базисные функции которых имеют "шумоподобный" характер. В процессе передачи информации возможны потери "энергетически важных" компонент. Поэтому предлагаются такие преобразования, которые не обладают свойствами концентрации энергии в нескольких спектральных компонентах.

Введение

Одним из важных свойств "классических" дискретных ортогональных преобразований

$$\widehat{x}(m) = \sum_{n=0}^{N-1} x(n) h_m(n); \quad m = 0, 1, \ldots, N-1; \tag{1}$$

$$< h_u, h_v >= \sum_{n=0}^{N-1} h_u(n),\ h_v(n) = \delta_{uv}, \tag{2}$$

определяющим возможность их эффективного применения к задачам кодирования цифровой видеоинформации, является концентрация энергии спектра в относительно небольшом числе спектральных компонент. В задачах, например, компрессии изображений это свойство во многом определяет эффективность конкретных алгоритмов компрессии. С другой стороны, при передаче кодированной видеоинформации по реальному каналу возникают помехи, искажения, зависящие от физической природы канала. И если специфика канала такова, что какая-то часть передаваемой информации *случайным образом* утрачивается ("канал с пропусками"), то при утрате "энергетически значимых" компонент спектра на изображение накладываются

[1]Представлена доктором физико-математических наук профессором В.М. Черновым.

[2]Бесполитов Олег Владимирович (gelo@ssu.samara.ru), кафедра безопасности информационных систем Самарского государственного университета, 443011, Россия, г. Самара, ул. Акад. Павлова, 1.

Рис. 1. Исходное изображение

Рис. 2. Искажение изображения при применении преобразования Хартли

"структурированные помехи", к которым зрительная система человека более чувствительна, чем к точечному шуму. На рис. 2–4 показаны примеры таких структурированных помех, отличающиеся от точечного шума.

В связи с этим целесообразно рассматривать такие преобразования, которые не обладают свойством концентрации энергии в нескольких спектральных компонентах и позволяли бы эффективно удалять несущественную информацию. В частности, желательно, чтобы влияние канальных ошибок было бы менее заметно, чем при применении классических дискретных ортогональных преобразований Фурье, Уолша, Хартли и др. Другими словами, мы намерены рассматривать дискретные ортогональные преобразования, базисные функции которых имеют "шумоподобный" характер. Для таких преобразований спектральные компоненты "энергетически равноправны".

Такие одномерные преобразования (1), базисные функции $h_m(n)$ которых принимают "хаотическим" образом два различных значения, введены в [1]. В работах [2–4] рассмотрены приложения таких преобразований к кодированию видеоинформации. Различные обобщения основной конструкции работы [1] рассматривались авторами в [5–7] для случая k-значных функций $h_m(n)$.

Основой для построения семейства базисных функций исследуемых дискретных ортогональных преобразований является линейная рекуррентная последовательность

$$y(n) = a_1 y(n-1) + \ldots + a_r y(n-r); \quad a_j \in \mathbf{F}_q, a_r \neq 0 \tag{3}$$

элементов конечного поля $\mathbf{F}_q$ из $q = p^s$ элементов (p — простое число) с максимально возможным периодом $N = q^r - 1$ (m — последовательность [8, 9]).

Рис. 3. Искажение изображения при применении преобразования Адамара

Рис. 4. Искажение изображения при применении M-преобразования

При построении базисных функций преобразования (1) члены последовательности $y(n) \in \mathbf{F}_q$ заменяются вещественными числами $h_m(n)$ таким образом, чтобы для функций $h_m(n)$ выполнялось условие ортогональности (2).

Одной из основных проблем, препятствующих экстраполяции методов цитированных работ на двумерный случай, является проблема построения "хорошей" одномерной нумерации двумерного массива $\{(n_1, n_2);\ n_1, n_2 \in \mathbf{Z}\}$.

В работах [10, 11] введено понятие канонической системы счисления в кольце $\mathbf{S}(\sqrt{d})$ целых элементов квадратичного поля

$$\mathbf{Q}(\sqrt{d}) = \{z = a + b\sqrt{d};\quad a, b \in \mathbf{Q}\},$$

позволяющих представить элементы $z \in \mathbf{S}(\sqrt{d})$ в форме конечной суммы

$$z = \sum_{j=0}^{k(z)} z_j \alpha^j, \tag{4}$$

где "цифры" z_j принадлежат некоторому конечному подмножеству $N \subset \mathbf{Z}$, а элемент α (основание системы счисления) есть некоторый элемент кольца $\mathbf{S}(\sqrt{d})$.

В настоящей работе мы устанавливаем взаимнооднозначное соответствие между элементами "гусеницы"

$$\begin{aligned} &Y_0 = (y(0), \ldots, y(r-1)),\\ &Y_1 = (y(1), \ldots, y(r)),\\ &\ldots\\ &Y_{N-1} = (y(N-1), \ldots, y(N-1+r)) \end{aligned} \tag{5}$$

N-периодической m-последовательности (3) и элементами кольца $\mathbf{S}(\sqrt{d})$, представимыми r-членными суммами (5). На основе такого соответствия

мы вводим двумерные ортогональные преобразования

$$\widehat{x}(m_1, m_2) = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} x(n_1, n_2) h_{m_1,m_2}(n_1, n_2) \tag{6}$$

с условием ортогональности

$$\langle h_{m_1,m_2}, h_{k_1,k_2} \rangle = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} h_{m_1,m_2}(n_1, n_2) h_{k_1,k_2}(n_1, n_2) = \delta_{k_1,n_1} \cdot \delta_{k_2,n_2} \tag{7}$$

и с "хаотическим" поведением значений базисных функций $h_{m_1,m_2}(n_1, n_2)$.

1. Некоторые вспомогательные сведения

Содержание данного раздела играет вспомогательную роль. Доказательства сформулированных ниже свойств последовательностей, удовлетворяющих линейному рекуррентному соотношению в конечном поле, можно найти, например, в [8, 9], а свойства канонических систем счисления в [10, 11].

1.1. Рекуррентные функции в конечных полях

Пусть $\mathbf{F}_q$ есть конечное поле из $q = p^s$ элементов, p — простое число.

Определение 1. Функцию, являющуюся решением линейного рекуррентного соотношения (3), где

$$a_1, \ldots, a_r \in \mathbf{F}_q, \quad a_r \neq 0, \quad Y = (y(0), \ldots, y(r-1)),$$

будем называть линейной рекуррентной последовательностью порядка r с начальными значениями $Y = (y(0), \ldots, y(r-1))$.

Определение 2. Рекуррентная последовательность (3) с максимально возможным периодом, равным $N = q^r - 1$, называется m-последовательностью.

Для удобства ссылок простейшие свойства m-последовательностей сформулируем в форме леммы.

Лемма 1. Пусть рекуррентная последовательность (3) с ненулевыми начальными условиями $Y = Y_0 = (y(0), \ldots, y(r-1))$ является m-последовательностью. Тогда справедливы следующие утверждения:

1) если n пробегает полный период последовательности (3), равный $N = q^r - 1$, то элемент $0 \neq a \in \mathbf{F}_q$; встретится q^{r-1} раз, нулевой элемент $0 \in \mathbf{F}_q$ встретится $q^{r-1} - 1$ раз;

2) в полном периоде "гусеницы" (5) последовательности (3) все ненулевые r-мерные векторы пространства $(\mathbf{F}_q)^r$ встретятся ровно по одному разу;

3) если $y_1(n), y_2(n)$ есть два различных решения рекуррентного соотношения (3) с различными начальными условиями

$$Y_{0,1} = (y_1(0), \ldots, y_1(r-1)), \; Y_{0,2} = (y_2(0), \ldots, y_2(r-1)), \tag{8}$$

то последовательность

$$y_3(n) = y_1(n) + y_2(n)$$

также есть решение рекуррентного соотношения (3) и является либо m-последовательностью, либо нулевой последовательностью;

4) если $y_1(n), y_2(n)$ есть два различных решения рекуррентного соотношения (3) с различными начальными условиям (8), то существует такое натуральное τ, что

$$y_1(n) = y_2(n + \tau);$$

5) если $\mathbf{F}_q$ есть конечное поле из $q = p$ элементов (p — простое число), $\omega = \exp\{2\pi i/p\}$, то справедливо равенство

$$\sum_{n=0}^{N-1} \omega^{y(n)} = -1.$$

1.2. Канонические системы счисления в квадратичных полях

Введем обозначения.

Квадратичное поле $\mathbf{Q}(\sqrt{d})$:

$$\mathbf{Q}(\sqrt{d}) = \{z = a + b\sqrt{d};\ a, b \in \mathbf{Q}\},$$

$$z = a + b\sqrt{d} = \mathrm{Rat}(z) + \sqrt{d}\ \mathrm{Irr}(z),$$

где d есть свободное от квадратов целое число.

Кольцо $\mathbf{S}(\sqrt{d})$ целых элементов поля $\mathbf{Q}(\sqrt{d})$:

$$\mathbf{S}(\sqrt{d}) = \{z \in \mathbf{Q}(\sqrt{d}) : \mathrm{Norm}(z) = a^2 - db^2,\ \mathrm{Tr}(z) \in \mathbf{Z}\}.$$

Подкольцо $\mathbf{Z}(\sqrt{d})$ целых элементов с целыми компонентами:

$$\mathbf{Z}(\sqrt{d}) = \{z = a + b\sqrt{d} : a, b \in \mathbf{Z}\} \subseteq \mathbf{S}(\sqrt{d}) \subset \mathbf{Q}(\sqrt{d}).$$

Определение 3. Целое алгебраическое число $\alpha = A + \sqrt{d}$ есть основание канонической системы счисления в кольце $\mathbf{S}(\sqrt{d})$ целых элементов поля $\mathbf{Q}(\sqrt{d})$, если любой элемент $z \in \mathbf{S}(\sqrt{d})$ представляется в форме конечной суммы (5), где "цифры" z_j принадлежат конечному подмножеству

$$N = \{0, 1, \ldots, |\mathrm{Norm}(\alpha)| - 1\},\ \mathrm{Norm}(\alpha) = A^2 - d. \tag{9}$$

В зависимости от того, является ли поле $\mathbf{Q}(\sqrt{d})$ вещественным ($d > 0$) или мнимым ($d < 0$), исчерпывающее описание канонических систем счисления дается следующими утверждениями, доказанными в [9, 10], которые мы сформулируем в форме леммы.

Лемма 2. (а) Пусть поле $\mathbf{Q}(\sqrt{d})$ вещественное, $0 < d \equiv 2, 3 \pmod 4$. Тогда алгебраическое число $\alpha = A \pm \sqrt{d}$ является основанием канонической системы счисления в кольце $\mathbf{S}(\sqrt{d}) = \mathbf{Z}(\sqrt{d})$ тогда и только тогда, когда $A \in Z$ и

$$0 < -2A \leqslant A^2 - d \geqslant 2. \tag{10}$$

(b) Пусть поле $\mathbf{Q}(\sqrt{d})$ вещественное, $0 < d \equiv 1 \pmod 4$. Тогда алгебраическое число $\alpha = (B \pm \sqrt{d})/2$ является основанием канонической системы счисления в кольце $\mathbf{S}(\sqrt{d}) \supset \mathbf{Z}(\sqrt{d})$ тогда и только тогда, когда $B \in \mathbf{Z}$ нечетно и

$$0 < -B \leqslant \frac{1}{4}(B^2 - d) \geqslant 2. \tag{11}$$

(c) Пусть поле $\mathbf{Q}(i\sqrt{\Delta})$ мнимое, $\Delta \equiv -2, -3 \pmod 4$. Тогда алгебраическое число $\alpha = A + i\sqrt{\Delta}$ является основанием канонической системы счисления в кольце $\mathbf{S}(i\sqrt{\Delta}) = \mathbf{Z}(i\sqrt{\Delta})$ тогда и только тогда, когда $A \in \mathbf{Z}$ and

$$0 \leqslant -2A \leqslant A^2 + \Delta \geqslant 2, \tag{12}$$

(d) Пусть поле $\mathbf{Q}(\sqrt{d})$ мнимое, $\Delta \equiv -1 \pmod 4$. Тогда алгебраическое число $\alpha = (B \pm i\sqrt{\Delta})/2$ является основанием канонической системы счисления в кольце $\mathbf{S}(\sqrt{d}) \supset \mathbf{Z}(\sqrt{d})$ тогда и только тогда, когда $B \in \mathbf{Z}$ нечетно и

$$0 \leqslant -B \leqslant \frac{1}{4}(B^2 + \Delta) \geqslant 2. \tag{13}$$

Пример 1. Пусть $\mathrm{Norm}(\alpha) = 2$, тогда существует ровно три мнимых квадратичных поля, в кольцах целых элементов которых существуют бинарные канонические системы счисления, а именно:

(a) кольцо целых гауссовых чисел $\mathbf{Z}(i) \subset \mathbf{Q}(i)$ с основаниями, равными $\alpha = -1 \pm i$;

(b) кольцо $\mathbf{S}(i\sqrt{7}) \subset \mathbf{Q}(i\sqrt{7})$ с основаниями, равными $\alpha = (-1 \pm i\sqrt{7})/2$;

(c) кольцо $\mathbf{S}(i\sqrt{2}) \subset \mathbf{Q}(i\sqrt{2})$ с основаниями, равными $\alpha = \pm i\sqrt{2}$.

Пример 2. Пусть $\mathrm{Norm}(\alpha) = 3$, тогда существуют только три мнимых квадратичных поля, в кольцах целых элементов которых существуют тернарные канонические системы счисления, а именно:

(a) поле $\mathbf{Q}(i\sqrt{2})$ с основаниями $\alpha = -1 \pm i\sqrt{2}$;

(b) поле $\mathbf{Q}(i\sqrt{3})$ с основаниями $\alpha = (-3 \pm i\sqrt{3})/2$;

(c) поле $\mathbf{Q}(i\sqrt{11})$ с основаниями $\alpha = (-1 \pm i\sqrt{11})/2$.

Пример 3. Рассмотрим кольцо целых элементов $\mathbf{S}(\sqrt{d}) \subset \mathbf{Q}(\sqrt{d})$ вещественного квадратичного поля. Если $d \equiv 1 \pmod 4$ и $\alpha = (B \pm \sqrt{d})/2$ является основанием канонической системы счисления в кольце $\mathbf{S}(\sqrt{d})$, то из соотношения (15) получаем

$$0 < -B \leqslant \frac{1}{4}(B^2 - d) = \mathrm{Norm}(\alpha),$$

откуда легко следует, что минимально возможное значение нормы в правой части (15), для которого существуют основания $\alpha = (B \pm \sqrt{d})/2$ канонической системы счисления, равно пяти. В этом случае соответствующим полем и основаниями системы счисления являются $\mathbf{Q}(\sqrt{5})$ и $\alpha = (-5 \pm \sqrt{5})/2$ соответственно. Если $0 < d \equiv 2, 3 \pmod 4$, и $\alpha = A \pm \sqrt{d}$ является основанием канонической системы счисления в кольце $\mathbf{S}(\sqrt{d}) = \mathbf{Z}(\sqrt{d})$. Тогда из соотношения (11) получаем

$$0 < -2A \leqslant A^2 - d = \mathrm{Norm}(\alpha),$$

откуда легко следует, что минимально возможное значение нормы, для которого существуют основания канонической системы счисления $\alpha = A \pm \sqrt{d}$ равно 6. В этом случае соответствующим полем и основаниями системы счисления являются $\mathbf{Q}(\sqrt{3})$ и $\alpha = -3 \pm \sqrt{3}$ соответственно.

2. M-преобразования

В работе [1] введено понятие дискретного ортогонального M-преобразования [1], значения базисных функций $h_m(n)$ которого имеют "шумоподобный" характер. Именно функции $h_m(n)$ принимают "случайным" образом два значения с (почти) равными относительными частотами. Основой для построения семейства базисных функций в работе [1] являлась m-последовательность (3) при $p = 2$.

Построение базисных функций такого преобразования состоит в следующем.

При построении функции $h_0(n)$ члены последовательности $y(n)$ заменяются вещественными числами

$$\varphi : y(n) \mapsto h_0(n) = \begin{cases} A, & y(n) = 1 \in F_2; \\ B, & y(n) = 0 \in F_2. \end{cases} \tag{14}$$

Функции $h_m(n)$ получаются из $h_0(n)$ циклическим сдвигом:

$$h_m(n) = h_0(m + n); \;\; m = 0, 1, \ldots, N-1; \;\; N = (2^r - 1). \tag{15}$$

Числа A и B выбираются таким образом, чтобы для функций $\{h_m(n)\}$ выполнялось условие ортогональности в форме (2).

Основная техническая сложность заключается в получении (простых) соотношений для определения A и B. Мы докажем теорему, обобщающую результат работы [1] на случай произвольного простого p.

Теорема 1. Пусть p — простое число, $N = p^r - 1$, числа $A_0, \ldots, A_{p-1}$ удовлетворяют соотношению

$$A_k = k\lambda + A_0, \;\; \lambda = \frac{A_{p-1} - A_0}{p-1}, \;\; (k = 0, \ldots, p-1).$$

Пусть функции $h_m(n)$ определены соотношениями

$$\begin{cases} h_0(n) = A_k, \;\; y(n) = k; \\ h_m(n) = h_0(m + n). \end{cases}$$

Тогда существуют эффективно вычисляемые константы A_0 и λ такие, что семейство функций

$$\{h_m(n); \;\; m, n = 0, 1, \ldots, N-1\}$$

(a) образует ортонормированный базис;

(b) константы $A = A_0$ и λ являются решением системы уравнений

$$\begin{cases} N = A^2\left(\dfrac{N+1}{p} - 1\right) + \left(\dfrac{N+1}{p}\right)\displaystyle\sum_{k=1}^{p-1}(A+\lambda k)^2, \\ 0 = \displaystyle\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}(A+Ci)(A+Cj)S_{ij}(\tau), \end{cases} \tag{16}$$

где

$$S_{ij}(\tau) = \begin{cases} \dfrac{N+1}{p^2} - 1, & (i,j) = (0,0); \\ \dfrac{N+1}{p^2}, & (i,j) \neq (0,0). \end{cases}$$

Доказательство. Представим функцию $h_0(n) = h(n)$ в форме

$$h(n) = \sum_{k=0}^{p-1} A_k \chi_k(n),$$

где функции $\chi_k(n)$ определены как

$$\chi_k(n) = \begin{cases} 0, & y(n) \neq k; \\ 1, & y(n) = k. \end{cases}$$

Так как функции $h_m(n)$ получаются из функции $h_0(n)$ циклическим сдвигом, то соотношения (20) достаточно доказать для пары функций $h_0(n)$ и $h_m(n)$ при $m = 0, \ldots, N-1$.

При $m = 0$ условие ортогональности имеет вид

$$\begin{aligned} N = \sum_{n=0}^{N-1}\left(\sum_{k=0}^{p-1} A_k\chi_k(n)\right)^2 = \sum_{k=0}^{p-1} A_k^2 \sum_{n=0}^{N-1}\chi_k(n) = \\ = A^2\left(\frac{N+1}{p} - 1\right) + \left(\frac{N+1}{p}\right)\sum_{k=1}^{p-1}(A+\lambda k)^2, \end{aligned}$$

то есть первое уравнение системы (20).

При $m \neq 0$ условие ортогональности имеет вид

$$\begin{aligned} 0 = \sum_{n=0}^{N-1}\left(\sum_{k=0}^{p-1} A_k\chi_k(n)\right)\left(\sum_{j=0}^{p-1} A_j\chi_j(n+m)\right) = \\ = \sum_{k=0}^{p-1}\sum_{j=0}^{p-1} A_kA_j \sum_{n=0}^{N-1}\chi_k(n)\chi_j(n+m) = \sum_{k=0}^{p-1}\sum_{j=0}^{p-1} A_kA_j\sum_{n=0}^{N-1} S_{kj}(m). \end{aligned} \tag{17}$$

Так как

$$\chi_k(n) = \frac{1}{p}\sum_{a=0}^{p-1}\exp\left\{\frac{2\pi i}{p}(y(n)-k)a\right\},$$

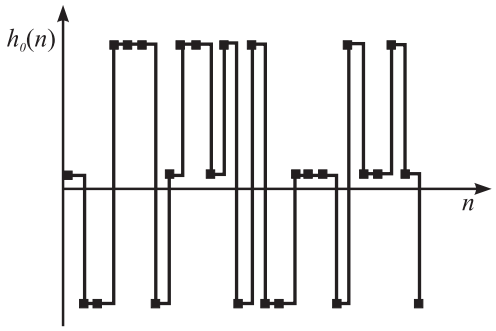

Рис. 5. Базисная функция $N = 27$, $p = 3$, $r = 3$

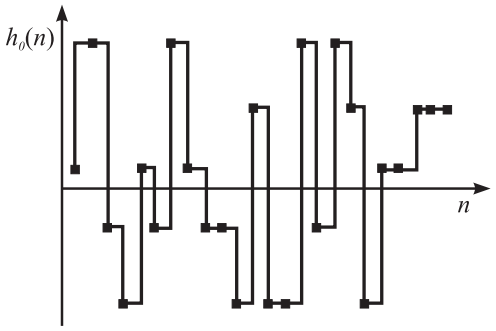

Рис. 6. Базисная функция $N = 25$, $p = 5$, $r = 2$

то

$$S_{kj}(m) = \frac{1}{p^2}\sum_{n=0}^{N-1}\sum_{a,b=0}^{p-1}\exp\left\{\frac{2\pi i}{p}(y(n)-k)a\right\}\exp\left\{\frac{2\pi i}{p}(y(n+m)-j)b\right\} =$$
$$= \frac{1}{p^2}\sum_{a,b=0}^{p-1}\exp\left\{-\frac{2\pi i}{p}(ka+jb)\right\}\sum_{n=0}^{N-1}\exp\left\{\frac{2\pi i}{p}(y(n)a+y(n+m)b)\right\}. \tag{18}$$

Так как $m \neq 0$, то при всех $(a,b) \neq (0,0)$ последовательность

$$z_{ab}(n,m) = y(n)a + y(n+m)b$$

является m-последовательностью и $z_{00}(n,m) = 0$. Поэтому из (19) следует

$$S_{kj}(m) = \frac{N}{p^2} - \frac{1}{p^2}\sum_{\substack{a,b=0\\(a,b)\neq(0,0)}}^{p-1}\exp\left\{-\frac{2\pi i}{p}(ka+jb)\right\}. \tag{19}$$

Для $k = j = 0$ имеем

$$p^2 S_{kj}(m) = N - (p^2 - 1).$$

А для $(k,j) \neq (0,0)$ имеем

$$p^2 S_{kj}(m) = N - \sum_{\substack{a,b=0\\(a,b)\neq(0,0)}}^{p-1}\exp\left\{-\frac{2\pi i}{p}(ka+jb)\right\} =$$
$$= N + 1 - \left(\sum_{a=0}^{p-1}\exp\left\{-\frac{2\pi i}{p}ka\right\}\right)\left(\sum_{b=0}^{p-1}\exp\left\{-\frac{2\pi i}{p}jb\right\}\right) = N + 1.$$

Подстановка найденных значений $S_{kj}(m)$ в равенство (20) дает второе уравнение системы (17) для определения параметров $A = A_0$ и λ.

На рис. 5, 6 приведены примеры базисных функций M-преобразования при различных значениях p.

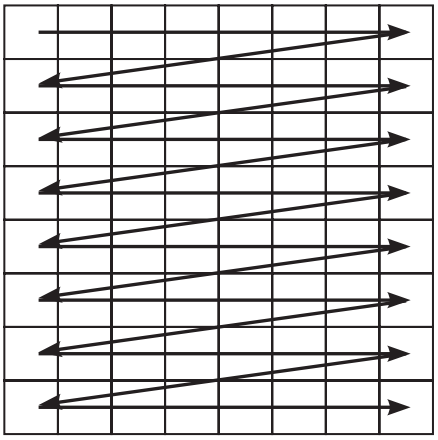

Рис. 7. "Последовательная" развертка

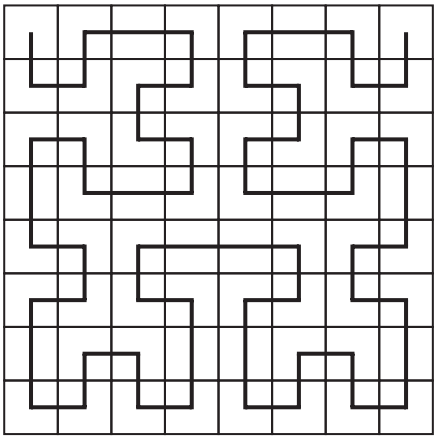

Рис. 8. Развертка Гильберта—Пеано

3. Двумерные M-преобразования

3.1. Синтез базисов двумерных M-преобразований

Для применений описанных выше M-преобразований к задачам обработки двумерной информации требуется представление двумерного обрабатываемого массива в одномерном виде.

Пусть $N = p^{2r} - 1$. Тогда

$$N = p^{2r} - 1 = (p^r - 1)(p^r + 1) = M \times K.$$

Элементы двумерного массива размера $(M \times K)$ можно упорядочить линейно различными способами (рис. 7). Если добавить к обрабатываемому массиву еще один отсчет $x(-1) = 0$, а к базисным функциям также еще одно нулевое значение, то получим массивы размера $N + 1 = (p^r)^2$, которые можно занумеровать, например, при $p = 2$ с помощью развертки Гильберта—Пеано (рис. 8).

В данной работе мы нумеруем точки квадрата размера $(p^r \times p^r)$ с одной выколотой точкой и определяем значения базисных функций, используя канонические системы счисления по следующей схеме.

ШАГ 1. Рассмотрим рекуррентную m-последовательность (3) порядка $2r$ с периодом $N = p^{2r} - 1$ периода с "гусеницей":

$$\begin{aligned} &Y_0 = (y(0), \dots, y(2r-1)),\\ &Y_1 = (y(1), \dots, y(2r)),\\ &\dots,\\ &Y_{N-1} = (y(N-1), \dots, y(N-1+2r)) \end{aligned} \tag{20}$$

и выберем p-значную систему счисления с основанием α в подходящем квадратичном поле $\mathbf{Q}(\sqrt{d})$.

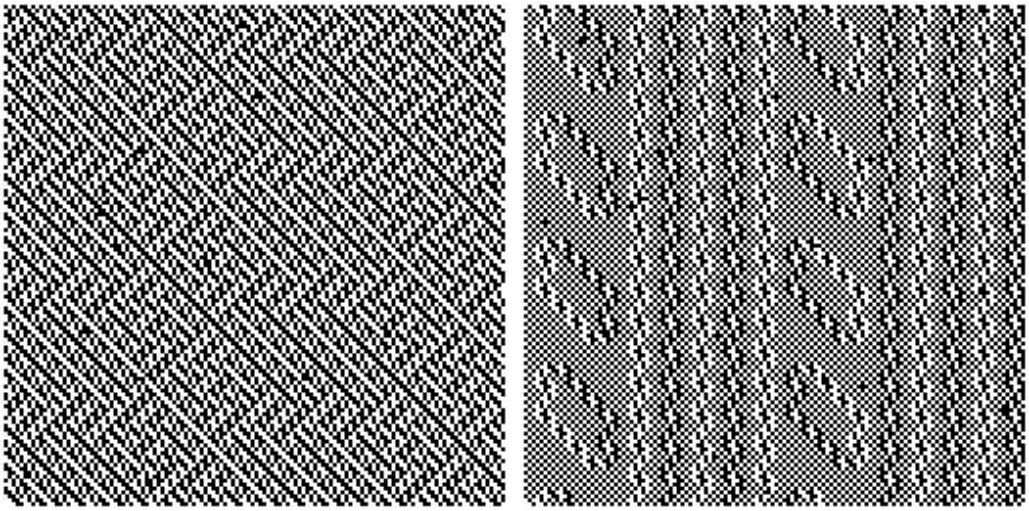

Рис. 9. Базисные функции двумерных M-преобразований

ШАГ 2. Координаты точки $\mathbf{Z}^2$ будем понимать как пару $(\mathrm{Rat}(z), \mathrm{Irr}(z))$, определяемую элементом кольца $\mathbf{S}(\sqrt{d})$, имеющим представление $z = a + b\sqrt{d} = \mathrm{Rat}(z) + \sqrt{d}\ \mathrm{Irr}(z)$.

ШАГ 3. Положим для последовательности (21)

$$z(k) = y(k)\alpha^0 + y(k+1)\alpha^1 + \ldots + y(2r-1)\alpha^{2r-1}. \tag{21}$$

В этом случае последовательность (25) изобразится на плоскости

$$(\mathrm{Rat}(z), \mathrm{Irr}(z)) = L$$

в виде некоторой "фундаментальной" области, сдвиги которой с соответствующими параметрами покроют $\mathbf{Z}^2$.

ШАГ 4. Определим значения "двумерных" базисных функций

$$H_m(\mathrm{Rat}(k), \mathrm{Irr}(k)) = H_m(z(k)),$$

определенных на фундаментальной области плоскости $(\mathrm{Rat}(z), \mathrm{Irr}(z))$ соотношениями

$$H_m(\mathrm{Rat}(k), \mathrm{Irr}(k)) = H_m(z(k)) = A_t, \quad y(k+m) = A_t$$

и продолжим эти значения по периодичности на всю плоскость L.

ШАГ 5. Ограничим определенные выше функции на точки $(n_1, n_2) \in \mathbf{Z}^2$, лежащие в квадрате $0 \leqslant n_1, n_2 \leqslant p^r - 1$, и будем понимать такое ограничение построенных функций как двумерные базисные функции M-преобразования.

Примеры таких базисных функций приведены на рис. 9.

3.2. О совместном распределении значений базисных функций M-преобразования

Доказываемая ниже теорема показывает, что значения различных базисных функций являются в некотором смысле "независимыми".

Теорема 2. Пусть

$$D_{u,v} = \operatorname{card}\{n : h_u(n) \neq h_v(n);\ \ 0 \leqslant n \leqslant N-1\}. \tag{22}$$

Тогда существует $\theta = \theta_p > 1/2$, такое, что при $u \neq v$ справедливо неравенство

$$D_{u,v} \geqslant \theta N. \tag{23}$$

Доказательство. Так как функции $h_m(n)$ получаются из функции $h_0(n)$ циклическим сдвигом, то неравенство (24) достаточно доказать для пары функций $h_0(n)$ и $h_m(n)$ при $m = 1, \ldots, N-1$. Пусть

$$M_{m,k} = \operatorname{card}\{n :\ \ h_0(n) = h_m(n) = k; \quad 0 \leqslant n \leqslant N-1\},$$

тогда при $k \neq 0$ имеем:

$$\begin{aligned}
M_{m,k} &= \frac{1}{p^2}\sum_{n=0}^{N-1}\left(\sum_{a=0}^{p-1}\exp\left\{\frac{2\pi i}{p}(y(n)-k)a\right\}\right)\left(\sum_{b=0}^{p-1}\exp\left\{\frac{2\pi i}{p}(y(n+m)-k)b\right\}\right) = \\
&= \frac{1}{p^2}\sum_{a=0}^{p-1}\sum_{b=0}^{p-1}\exp\left\{-\frac{2\pi i}{p}(a+b)k\right\}\sum_{n=0}^{N-1}\exp\left\{\frac{2\pi i}{p}(y(n)a+y(n+m)b)\right\} = \\
&= \frac{1}{p^2}\sum_{\substack{a,b=0\\(a,b)\neq(0,0)}}^{p-1}\exp\left\{-\frac{2\pi i}{p}(a+b)k\right\}\sum_{n=0}^{N-1}\exp\left\{\frac{2\pi i}{p}(y(n)a+y(n+m)b)\right\} + \frac{N}{p^2} = \\
&= \frac{1}{p^2}\sum_{a,b=0}^{p-1}(-1)\exp\left\{-\frac{2\pi i}{p}(a+b)k\right\} + \frac{1}{p^2} + \frac{N}{p^2} = \\
&= \frac{(-1)}{p^2}\left(\sum_{a=0}^{p-1}\exp\left\{-\frac{2\pi i}{p}ak\right\}\right)\left(\sum_{b=0}^{p-1}\exp\left\{-\frac{2\pi i}{p}bk\right\}\right) + \frac{1}{p^2} + \frac{N}{p^2} = \frac{1}{p^2}(N+1) = p^{r-2}.
\end{aligned} \tag{24}$$

При $k = 0$ имеем

$$\begin{aligned}
M_{m,0} &= \frac{1}{p^2}\sum_{a,b=0}^{p-1}\sum_{n=0}^{N-1}\exp\left\{\frac{2\pi i}{p}(y(n)a+y(n+m)b)\right\} = \\
&= \frac{1}{p^2}\sum_{a,b=0}^{p-1}(-1) + \frac{1}{p^2} + \frac{N}{p^2} = \\
&= p^{-2}(N+1) - 1 = p^{r-2} - 1.
\end{aligned} \tag{25}$$

Из равенств (24), (25) следует

$$D_m = D_{0,m} = N - \sum_{k=0}^{p-1} M_{m,k} = N\left(1-\frac{1}{p}\right) + \left(1+\frac{1}{p}\right) > N\left(1-\frac{1}{p}\right).$$

Теорема, таким образом, доказана.

Автор благодарит д.ф.-м.н. проф. В.М. Чернова за постоянное внимание к работе.

Литература

[1] Grallert H.J. Application of orthonormalized *m*-sequences for data reduced and error protected transmission of pictures. Proc. IEEE Int Symp. on Electromagnetic Compability. Baltimore, MD, 1980. P. 282–287.

[2] Grallert H.J. Source encoding and error protected transmission of pictures with help of orthonormalized *m*-sequences. Proc. 12^{th} Int. Television Symp. Montreux, Switzerland, 1981. P. 441–454.

[3] Keesen W.G., Riemann U., Grallert H.J. Codierung von Farbensehsignalen mittels modifizierten *M*-Transformationen für die Ubertragung über 34-M-bit/s-Kanaele. Frequenz. V. 38. No. 10. P. 238–243.

[4] Musmann H.G., Pirsch P., Grallert H.J. Advances in picture coding // IEEE Proc.. 1985. V. 73. No. 4. P. 523–548.

[5] Chernov V.M., Dmitriyev A.G. Image Compression Using Discrete Orthogonal Transforms with the "Noise-Like" Basis Functions. // Компьютерная оптика. 1999. №19. P. 184–187.

[6] Dmitriyev A.G., Chernov V.M. Two-dimensional Discrete Orthogonal Transforms with the "Noise-like" Basis Functions. Proc. Int. Conf. GraphiCon 2000. P. 36–41.

[7] Dmitriyev A.G., Chernov V.M. Generating Pseudostochastic Basis Function for Discrete Orthogonal Transforms. Pattern Recognition and Image Analysis. 2001. V. 11. No. 1. P. 155–157.

[8] Биркгофф Г., Барти. Т. Современная прикладная алгебра. М.: Мир, 1976. 400 с.

[9] Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988.

[10] Katai I., Kovacs B. Kanonische Zahlensysteme in der Theorie der quadratischen Zahlen. Acta Sci. Math. (Szeged) 42. 1980. P. 99–107.

[11] Katai I., Kovacs B. Canonical Number Systems in Imaginary Quadratic Fields // Acta Math. Acad. Sci. Hungaricae. 1981. V. 37. P. 159–164.

Поступила в редакцию 18/ *V*/2005;
в окончательном варианте — 28/ *VI*/2005.

DISCRETE ORTHOGONAL TRANSFORMATIONS WITH "NOISE-LIKE" BASIS FUNCTIONS[3]

© 2005 O.V. Bespolitov[4]

The paper is devoted to discrete orthogonal transformations with noise-like basis functions. During information transfer energetically important components loss is possible. Thus transformations which don't posses properties of energy concentration in several spectral components are proposed.

Paper received 18/*V*/2005.
Paper accepted 28/*VI*/2005.

[3]Communicated by Dr. Sci. (Phys. & Math.) Prof. V.M. Chernov.

[4]Bespolitov Oleg Vladimirovich (gelo@ssu.samara.ru), Dept. of Information Systems Security, Samara State University, Samara, 443011, Russia.