УДК 621.391.14

КОРРЕЛЯЦИОННЫЕ СПЕКТРЫ И КОДОВЫЕ РАССТОЯНИЯ МАЖОРИТАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А.И. МИТЮХИН, П.Н. ЯКУБЕНКО

Институт информационных технологий
Козлова 28, Минск, 220037, Беларусь

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 14 ноября 2014

Рассматривается задача выбора множества бинарных последовательностей корректирующего кода с заданным минимальным расстоянием. Исследуются диадные корреляционные свойства мажоритарных последовательностей. Представлены экспериментальные данные о корреляционных спектрах нелинейных последовательностей. Предложена нелинейная кодовая конструкция, позволяющая получить большее значение кодового расстояния.

Ключевые слова: кодовое расстояние, мажоритарная последовательность, базис Уолша, диадный сдвиг, корреляция, корреляционный спектр, шум.

Введение

Решения таких задач как обнаружении и различение сигналов в шумах, низкоскоростное кодирование-декодирование, распознавание, сегментация динамических объектов связаны с использованием оптимальных или близких к оптимальным алгоритмов обработки на множествах сигналов (кодовых слов) со сравнительно большим среднеквадратическим расстоянием между ними. Степень различия между двумя кодовыми словами (векторами) $\boldsymbol{g}=(g_0, g_1, ..., g_{N-1})$ и $\boldsymbol{x}=(x_0, x_1, ..., x_{N-1})$ оценивается коэффициентом корреляции

$$r_{g,x}=\frac{1}{N}\sum_{n=0}^{N-1} g_n x_n = \frac{A-D_x}{N}, \qquad (1)$$

где A – число совпадений соответствующих элементов обоих векторов; D_x – расстояние Хэмминга между векторами; N – длина слова. Для любой пары конечных последовательностей кода G функция $r_{g,x}, 0 \le n \le N-1, g \in G, x \in G, g \ne x$ должна быть мала. В этом случае достигается хорошая корректирующая способность кода в каналах с шумами. На практике уже сравнительно давно используются линейные трансортогональные и симплексные коды, у которых максимальный коэффициент корреляции между всеми словами минимизирован [1]. В работе исследуется усеченная нелинейная кодовая конструкция (N, M, D)-кода с минимальным расстоянием D на множестве из M мажоритарных последовательностей.

Мажоритарные последовательности

Класс этих последовательностей получается мажоритарным сложением функций Уолша $\{\mathrm{wal}_i(t)\}, i=0,1,...,N-1$ [2]. Для построения мажоритарных последовательностей необходимо выбрать из множества функций Уолша $\{\mathrm{wal}_i(t)\}$ l функций, где l – нечетное число.

Выделенные функции обозначим $\left\{\mathrm{wal}_{i_j}(t)\right\}$, $j = 0,1,\ldots,l$. Пусть $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_l$ обозначают произвольные векторы с компонентами $(b_1, b_2, \ldots, b_l)$, $b_i \in \{1, -1\}$. Мажоритарная последовательность образуется путем суммирования бинарных символов по следующему правилу [3]:

$$a(t) = \mathrm{sign}\sum_{j=1}^{l} b_j \mathrm{wal}_{i_j}(t) = \begin{cases} 1, \sum\limits_{j=1}^{l} b_j(t)\mathrm{wal}_{i_j}(t) \ge 0; \\ 0, \sum\limits_{j=1}^{l} b_j(t)\mathrm{wal}_{i_j}(t) < 0. \end{cases} \qquad (2)$$

Обозначим $\{a_i\} = \{a_0, a_1, \ldots, a_{N-1}\}$ множество последовательностей циклической группы, на котором определена операция диадного сдвига на конечных интервалах. Все множество последовательностей $\{a_i\}$ получается заданием координат векторов $\mathbf{b} = (b_1, b_2, \ldots, b_l)$. Диадный сдвиг последовательности a_i переводит ее в последовательность $a_i(t \oplus \tau) = a_\tau(t)$, $\tau = 0,1,\ldots,N-1$. Далее воспользуемся следующей теоремой.

Теорема [3]. При фиксированном векторе $\mathbf{b}$ множество последовательностей $\{a_i\}$ инвариантно относительно диадного сдвига аргумента. Тогда все множество $\{a_i\}$ получается вычислением диадных сдвигов только одной последовательности, соответствующей фиксированному вектору $\mathbf{b}$.

Множество $\{a_i\}$ можно представить в виде матрицы $\mathbf{A}$. Строки матрицы $\mathbf{A}$ это последовательности $a_\tau(t)$, упорядоченные по возрастанию значения диадного сдвига τ. Проиллюстрируем применение теоремы на примере.

Пример 1. Пусть вектор $\mathbf{b} = (11111)$. Вектору соответствует мажоритарная последовательность

$$a_0(t) = (1111111-1111-11-1-1-1111-11-1-1-11-1-1-1-1-1-1-1), \tau = 0.$$

Для τ = 1 получаем

$$a_1(t) = (111111-1111-11-11-1-111-11-11-1-1-11-1-1-1-1-1-1).$$

На рис.1 показана структура неполного множества последовательностей матрицы $\mathbf{A}$.

1	1	1	1	1	1	1	-1	1	1	1	-1	1	-1	-1	-1	1	1	1	-1	1	-1	-1	-1	1	-1	-1	-1	-1	-1	-1	-1
1	1	1	1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	1	1	-1	1	-1	1	-1	-1	-1	1	-1	-1	-1	-1	-1	-1
1	1	1	1	1	-1	1	1	1	-1	1	1	-1	-1	1	-1	1	-1	1	1	-1	-1	1	-1	-1	-1	1	-1	-1	-1	-1	-1
1	1	1	1	-1	1	1	1	-1	1	1	1	-1	-1	-1	1	-1	1	1	1	-1	-1	-1	1	-1	-1	-1	1	-1	-1	-1	-1
1	1	1	-1	1	1	1	1	1	-1	-1	-1	1	1	1	-1	1	-1	-1	-1	1	1	1	-1	-1	-1	-1	-1	1	-1	-1	-1
1	1	-1	1	1	1	1	1	-1	1	-1	-1	1	1	-1	1	-1	1	-1	-1	1	1	-1	1	-1	-1	-1	-1	-1	1	-1	-1
1	-1	1	1	1	1	1	1	-1	-1	1	-1	1	-1	1	1	-1	-1	1	-1	1	-1	1	1	-1	-1	-1	-1	-1	-1	1	-1
-1	1	1	1	1	1	1	1	-1	-1	-1	1	-1	1	1	1	-1	-1	-1	1	-1	1	1	1	-1	-1	-1	-1	-1	-1	-1	1
1	1	1	-1	1	-1	-1	-1	1	1	1	1	1	1	1	-1	1	-1	-1	-1	-1	-1	-1	-1	1	1	1	-1	1	-1	-1	-1
1	1	-1	1	-1	1	-1	-1	1	1	1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	-1
1	-1	1	1	-1	-1	1	-1	1	1	1	1	1	-1	1	1	-1	-1	1	-1	-1	-1	-1	-1	1	-1	1	1	-1	-1	1	-1
-1	1	1	1	-1	-1	-1	1	1	1	1	1	-1	1	1	1	-1	-1	-1	1	-1	-1	-1	-1	-1	1	1	1	-1	-1	-1	1
1	-1	-1	-1	1	1	1	-1	1	1	1	-1	1	1	1	1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	-1	-1	1	1	1	-1
-1	1	-1	-1	1	1	-1	1	1	1	-1	1	1	1	1	1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	-1	1	1	-1	1
-1	-1	1	-1	1	-1	1	1	1	-1	1	1	1	1	1	1	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	-1	1	1

Рис. 1. Кодовые слова мажоритарного (32, 15, 12)-кода

Если A_i обозначает число последовательностей веса *i*, то весовой спектр этого кода определяется вектором $(A_1, A_2, \ldots, A_{32}) = (0, 0, \ldots, A_{16} = 32, \ldots, 0)$.

Минимальное кодовое расстояние множества последовательностей матрицы $\mathbf{A}$ равно D = 12 Код может исправлять все конфигурации пятикратных ошибок. Этот код может быть использован для построения блоков нелинейных кодов, исправляющих большее число ошибок.

Диадная корреляция

Ниже рассмотрены диадные корреляционные свойства мажоритарных последовательностей матрицы **A**. В качестве опорной выбрана последовательность $a_0(t)$ примера 1. Коэффициенты диадной корреляции вычисляются по формуле

$$r(\tau) = \sum_{t=0}^{N-1} a(t) a(t \oplus \tau), \tau = 0,1,\ldots, N-1. \qquad (3)$$

Пример 2. На рис. 2 и 3 показаны графики диадных корреляционных функций последовательностей $a_0(t)$ и $a_7(t)$.

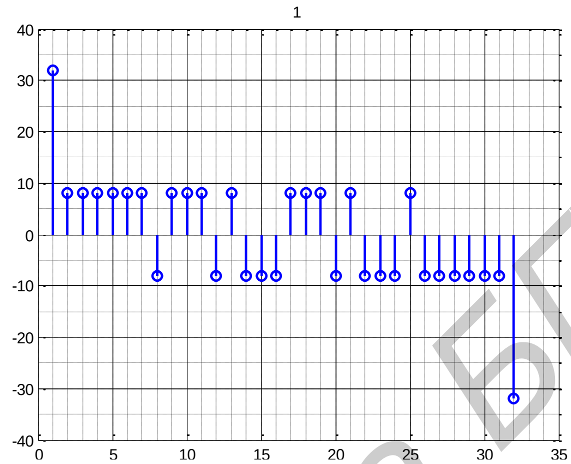

Рис. 2. Диадная корреляционная функция последовательности $a_0(t)$

Число коэффициентов корреляции с положительными и отрицательными значениями уравновешено. Как видно, последовательности обладают четырехуровневым корреляционным спектром, в котором значение 32 встречается 1 раз, значение –32 встречается 1 раз, значение 8 встречается 15 раз, значение –8 встречается 15 раз.

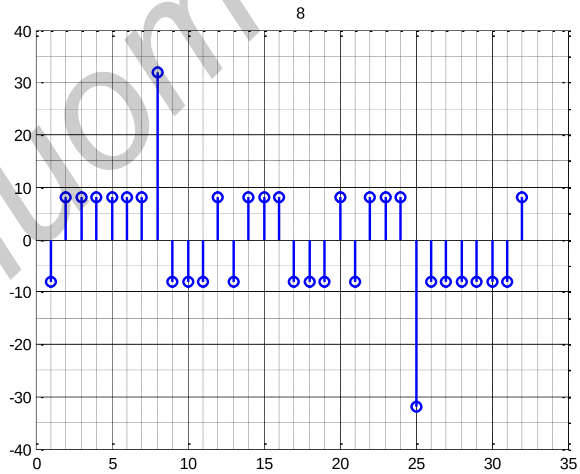

Рис. 3. Диадная корреляционная функция последовательности $a_7(t)$

Корреляционный спектр пары последовательностей $a_i(t)$ и $a_j(t)$ совпадает со спектром диадно сдвинутых последовательностей $a_i(t \oplus l)$ и $a_j(t \oplus l)$. Отличительной особенностью корреляционного спектра является его инвариантность относительно номеров мажоритарных последовательностей матрицы $\mathbf{A}$.

Усеченная нелинейная конструкция кода

Она представляет собой способ увеличения минимального расстояния кода. Выявление подмножеств последовательностей с большим кодовым расстоянием основывается на анализе полученного корреляционного спектра и форм всех 32-х корреляционных функций диадно сдвинутых мажоритарных последовательностей. Выражению (3) соответствует матричная запись вида $\mathbf{R} = \mathbf{A}\mathbf{a}^{\mathrm{T}}$.

Вектор $\mathbf{a} = (a_0, a_1, ..., a_{N-1}), a \in (-1, 1)$ совпадает с одной из строк матрицы $\mathbf{A}$. Координаты вектора $\mathbf{R} = (r_0, r_1, ..., r_{N-1})^{\mathrm{T}}$ – это коэффициенты диадной корреляционной функции последовательности $a_i(t)$. Из формул (1), (3) и рис. 2 и 3 следует, что отрицательные значения коэффициентов корреляции соответствуют парам $(a_i(t), a_j(t))$ мажоритарных последовательностей с большим минимальным расстоянием, чем D. Напомним, значение D – это кодовое расстояние полного множества $\{a_i\}$. Расстояние Хэмминга $D^x{}_{i,j}$ между двумя векторами $\mathbf{a}_i$ и $\mathbf{a}_j$ усеченного кода определяется как $D^x{}_{i,j} = D + |-r_{i,j}|$, где $(-r_{i,j})$ обозначает отрицательное значение коэффициента корреляции между векторами $\mathbf{a}_i$ и $\mathbf{a}_j$. Свойство инвариантности и структурная регулярность корреляционных спектров диадно сдвинутых мажоритарных последовательностей позволяют сформировать сравнительно большое число новых множеств нелинейных последовательностей, состоящих из четырех слов с расстоянием $D = 20$. На рис. 4 показаны рассчитанные номера последовательностей, образующих такие множества. Компьютерные расчеты проведены в программной системе MATLAB (нумерация слов соответствует принятой в MATLAB).

1 8 26 31	1 8 27 30	1 8 28 29	1 12 22 31	1 12 23 30	1 12 24 29	1 14 20 31	1 14 23 28	1 14 24 27	1 15 20 30	1 15 22 28	1 15 24 26	1 16 20 29	1 16 22 27	1 16 23 26
2 7 25 32	2 7 27 30	2 7 28 29	2 11 21 32	2 11 23 30	2 11 24 29	2 13 19 32	2 13 23 28	2 13 24 27	2 15 19 30	2 15 21 28	2 15 24 25	2 16 19 29	2 16 21 27	2 16 23 25
3 6 25 32	3 6 26 31	3 6 28 29	3 10 21 32	3 10 22 31	3 10 24 29	3 13 18 32	3 13 22 28	3 13 24 26	3 14 18 31	3 14 21 28	3 14 24 25	3 16 18 29	3 16 21 26	3 16 22 25
4 5 25 32	4 5 26 31	4 5 27 30	4 9 21 32	4 9 22 31	4 9 23 30	4 13 17 32	4 13 22 27	4 13 23 26	4 14 17 31	4 14 21 27	4 14 23 25	4 15 17 30	4 15 21 26	4 15 22 25
5 10 19 32	5 10 20 31	5 10 24 27	5 11 18 32	5 11 20 30	5 11 24 26	5 12 18 31	5 12 19 30	5 12 24 25	5 16 18 27	5 16 19 26	5 16 20 25	6 9 19 32	6 9 20 31	6 9 23 28
6 11 17 32	6 11 20 29	6 11 23 26	6 12 17 31	6 12 19 29	6 12 23 25	6 15 17 28	6 15 19 26	6 15 20 25	7 9 18 32	7 9 20 30	7 9 22 28	7 10 17 32	7 10 20 29	7 10 22 27
7 12 17 30	7 12 18 29	7 12 22 25	7 14 17 28	7 14 18 27	7 14 20 25	8 9 18 31	8 9 19 30	8 9 21 28	8 10 17 31	8 10 19 29	8 10 21 27	8 11 17 30	8 11 18 29	8 11 21 26
8 13 17 28	8 13 18 27	8 13 19 26	9 16 18 23	9 16 19 22	9 16 20 21	10 15 17 24	10 15 19 22	10 15 20 21	11 14 17 24	11 14 20 21	11 14 18 23	12 13 17 24	12 13 18 23	12 13 19 22

Рис. 4. Номера нелинейных мажоритарных последовательностей, образующих 120 блоков кодов с расстоянием D = 20

Пример 3. На рис. 5 приведен блок последовательностей с номерами: 5, 12, 19, 30. Легко убедиться в том, что минимальное расстояние кода равно $D = 20$. Код исправляет все конфигурации девятикратных ошибок. Такое же множество известного линейного симплексного m-кода с параметрами [31, 2, 16] корректирует только семикратные ошибки.

1 1 1–1 1 1 1 1 1–1–1–1 1 1 1–1 1–1–1–1 1 1 1–1–1–1–1–1 1–1–1–1
–1 1 1 1–1–1–1 1 1 1 1 1 -1 1 1 1–1–1–1 1–1–1–1–1–1 1 1 1–1–1–1 1
1–1 1 1–1–1 1–1–1–1 1–1–1–1–1–1 1 1 1 1 1–1 1 1 1–1 1 1–1–1 1–1
–1–1–1–1–1 1–1–1–1 1–1–1 1 1–1 1–1 1–1–1 1 1–1 1 1 1–1 1 1 1 1 1

Рис. 5. Последовательности нелинейного (32, 4, 20)-кода

Заключение

Исследованы корреляционные спектры и минимальные расстояния нелинейного мажоритарного кода длиной $N = 32$ и его подмножеств. Вычеркивание координат (32, 32, 12)-кода, отражающее структурные особенности корреляционных спектров, позволило получить 120 блоков последовательностей, корректирующих ошибки кратностью $t = 9$.

CORRELATION SPECTRA AND CODE DISTANCE OF THE MAJORITY SEQUENCES

A.I. MITSIUKHIN, P.N. YAKUBENKO

Abstract

The correlation properties of the majority of sequences are investigated. Experimental data on the correlation spectra of non-linear sequences is presented. A nonlinear code design that allows to get more distance with the code is given.

Список литературы

1. *Ипатов В.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М., 2007.
2. *Tanner R., Woodward J.* WCDA – Requirements and Practical Design. Chichester, 2003.
3. *Лосев В.В., Бродская Е.Б., Коржик В.И.* Поиск и декодирование сложных дискретных сигналов. М., 1988.