Доклады БГУИР
2003 *июль–сентябрь* *Том 1, № 3*

УДК 621. 391. 26

ОРТОГОНАЛЬНЫЕ КОДЫ НА ОСНОВЕ БЕНТ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В.Д. ДВОРНИКОВ

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

Поступила в редакцию 26 сентября 2003

В статье рассмотрен низкоскоростной ортогональный код, множество кодовых слов которого образовано диадными сдвигами одной бент-последовательности. Доказано, что код является ортогональным и нелинейным. Определено количество различных кодовых множеств. Для декодирования кода предложено использовать алгоритм вычисления диадной корреляции в спектральной области Уолша–Адамара.

Ключевые слова: ортогональные коды, бент-последовательности, диадный сдвиг, диадная корреляция, спектр Уолша–Адамара.

Известны нелинейные кодовые конструкции, являющиеся смежными классами кодов Рида–Маллера высоких порядков (коды Кердока, коды Препараты) [1]. Свойства нелинейности позволяют обеспечить определенную степень криптографической защиты сообщений. При этом желательно иметь большое число различных кодовых ансамблей, а сами коды должны иметь быстрые алгоритмы декодирования. Перспективными в этом отношении являются бент-последовательности [2]. Ниже рассмотрен метод синтеза ортогональных нелинейных кодов на основе бент-последовательностей и устройства их быстрого декодирования.

Кодовое слово длины n записывается в виде последовательности

$$\{b_i(j)\} = [b_0(j), b_1(j), ..., b_{n-1}(j)],$$

где $n = 2^{2m}$ — длина кодового слова, m — любое целое число, j — $2m$-разрядное двоичное число, представляющее собой блок информационных символов, $j = 0,...,2^{2m+1} - 1$.

Кодовое слово для $j = 0$ вычисляется по формуле

$$\{b_i(0)\} = (-1)^{i_1 \cdot i_2},$$

здесь $i_1 = (i) \bmod 2^m$, $i_2 = (i - i_1)2^{-m}$, а $i_1 \cdot i_2$ — скалярное произведение.

Последовательность $\{b_i(0)\}$ является бент-последовательностью длины n [3]. Остальные кодовые слова образуются диадным сдвигом (перестановкой) символов исходной последовательности в соответствии с параметром сдвига j [4,5]:

$$\{b_i(j)\} = \{b_i(0 \oplus j)\}.$$

Для этого текущие номера символов i в двоичной форме суммируются по модулю два информационными символами j. Тогда можно записать

$$\{b_i(j)\} = (-1)^{(i_1 \oplus j_1)\cdot(i_2 \oplus j_2)}.$$

Здесь $j_1 = (j) \bmod 2^m$, $j_2 = (j - j_1)2^{-m}$.

Так как j изменяется в диапазоне от 0 до $2^{2m} - 1$, то полученный ансамбль будет содержать 2^{2m} кодовых слов. Пусть множество B содержит все кодовые слова.

Утверждение 1. B является ортогональным множеством.

Под ортогональностью понимается следующее свойство кода:

$$R(j,l) = \sum_{i=0}^{n-1} b_i(j) b_i(l) = \begin{cases} n, j = l \\ 0, j \neq l. \end{cases}$$

Покажем, что это справедливо для рассмотренного ансамбля. Если $i = j$, то справедливость утверждения доказывается вычислением

$$R(j,j) = \sum_{i=0}^{n-1} b_i(j) b_i(j) = \sum_{i=0}^{n-1} [(-1)^{(i_1 \oplus j_1)\cdot(i_2 \oplus j_2)}]^2 = n.$$

Для $j \neq l$ запишем

$$R(j,l) = \sum_{i=0}^{n-1} b_i(j) b_i(l) = \sum_{i=0}^{n-1} (-1)^{(i_1 \oplus j_1)\cdot(i_2 \oplus j_2)} (-1)^{(i_1 \oplus l_1)\cdot(i_2 \oplus l_2)} =$$

$$= \sum_{i=0}^{n-1} (-1)^{(i_1 \oplus j_1)\cdot(i_2 \oplus j_2) \oplus (i_1 \oplus l_1)\cdot(i_2 \oplus l_2)} = (-1)^{j_1 \cdot j_2 \oplus l_1 \cdot l_2} \sum_{i_2=0}^{2^m-1} (-1)^{i_2 \cdot (j_1 \oplus l_1)} \sum_{i_1=0}^{2^m-1} (-1)^{i_1 \cdot (j_2 \oplus l_2)}.$$

Если $i_2 \neq l_2$, то внутренняя сумма $\sum_{i=0}^{n-1} (-1)^{i_1 \cdot (j_2 \oplus l_2)}$ равна нулю, так как $(-1)^{i_1 \cdot (j_2 \oplus l_2)}$ представляет собой строку матрицы Уолша–Адамара с номером $j_2 \oplus l_2 \neq 0$. Если $i_2 = l_2$, а $i_1 \neq l_1$, то $\sum_{i=0}^{n-1} (-1)^{i_1 \cdot (j_2 \oplus l_2)} = \pm 2^m$. При этом сумма $\sum_{i_2=0}^{2^m-1} (-1)^{i_2 \cdot (j_1 \oplus l_1)} = 0$, поскольку $(-1)^{i_2 \cdot (j_1 \oplus l_1)}$ представляет собой строку с номером $j_1 \oplus l_1 \neq 0$. Поэтому если $j \neq l$, то в любом случае $R(j,l) = 0$.

Утверждение 2. B — нелинейный код.

Под нелинейностью (негрупповые свойства) понимается свойство, когда не выполняется условие замкнутости множества B относительно операции умножения. Если $j \neq l$, $\{b_i(j)\} \in B$, $\{b_i(l)\} \in B$, то

$\{b_i(j)\}\{b_i(l)\} = \{b_i(p)\}$ и $\{b_i(p)\} \notin B$.

Достаточно показать, что это условие выполняется хотя бы в одном случае. Пусть $l = j \oplus s$, где $s = 00...01$ — $2m$-разрядное двоичное число, равное единице. Тогда

$$\{b_i(p)\} = \{b_i(j)\}\{b_i(j \oplus s)\} = (-1)^{(i_1 \oplus j_1)\cdot(i_2 \oplus j_2)} (-1)^{(i_1 \oplus j_1 \oplus s_1)\cdot(i_2 \oplus j_2)} = (-1)^{s_1 (i_2 \oplus j_2)}.$$

В результате получилась последовательность длины n, которая является строкой матрицы Уолша–Адамара с номером, равным m. Поскольку множество B не содержит подобной последовательности, то условие замкнутости не выполняется. Следовательно, код нелинейный.

Подобным образом можно построить несколько ансамблей кодовых последовательностей, отличающихся друг от друга, если использовать в качестве исходного кодового слова $\{b_i(0)\}$ любую бент-последовательность. В общем случае можно образовать не менее чем $M_a = 2^m! \, 2^{2^m - 2m - 1}$ различных ансамблей биортогональных нелинейных кодов [3]. В качестве примера ниже приведены два кодовых слова предложенного кода длины 16:

$\{b_i(0)\}$=(1,1,1,–1,1,1,–1,1,1,–1,1,1,1,–1,–1,–1),

$\{b_i(1)\}$=(1,1,–1,1,1,1,1,–1,–1,1,1,1,–1,1,–1,–1).

Для повышения помехоустойчивости ортогональные коды декодируются методом максимального правдоподобия. Для этого вектор $\boldsymbol{X}$, образованный символами принятого кодового слова, умножается на кодовую матрицу и в произведении находится максимальная компонента. Основной объем вычислений при этом тратится на вычисление корреляционного вектора, поэтому рассмотрим только эту операцию. Поскольку все кодовые слова образуются диадным сдвигом $\{b_i(0)\}$, то для декодирования целесообразно использовать алгоритм вычисления диадной корреляции [4, 5]. Процесс вычисления корреляционного вектора описывается следующим выражением:

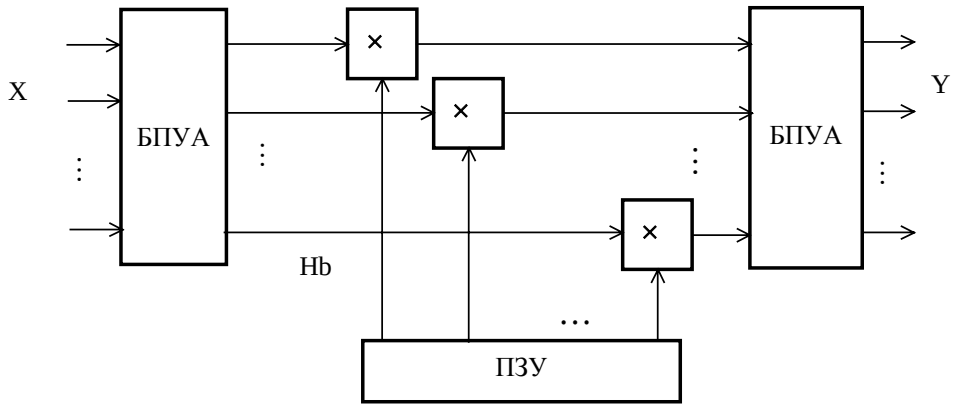
$$\mathbf{Y} = n^{-1}\mathbf{H}(\mathbf{Hb})(\mathbf{HX}),$$

где $\mathbf{H}$ — матрица преобразования Уолша–Адамара размерности $n \times n$; $\mathbf{b}$ — вектор-столбец, образованный символами $\{b_i(0)\}$.

В общем случае для нахождения $\mathbf{Y}$ необходимо три раза вычислить преобразование Уолша–Адамара и перемножить спектры векторов $\mathbf{X}$ и $\mathbf{b}$. Все вычисления производятся над действительными числами, а при вычислении спектров используются только операции типа сложение-вычитание. Для экономии результаты вычисления спектра $\mathbf{Hb}$ используются многократно. Дополнительная экономия получается при перемножении спектров. Во-первых, все компоненты $\mathbf{Hb}$ равны $\pm 2^m$, поэтому можно использовать следующую форму записи выражения для вычисления корреляционного вектора:

$$\mathbf{Y} = 2^{-m}\mathbf{H}(2^{-m}\mathbf{Hb})(\mathbf{HX}).$$

В этом случае $2^{-m}\mathbf{Hb} = \pm 1$ и, следовательно, умножения вообще исключаются. В результате потребуется $4mn$ операций типа сложение. Структурная схема декодера, реализующего данный алгоритм, представлена на рисунке.



Структурная схема декодера

Декодер содержит два блока вычисления быстрого преобразования Уолша–Адамара, постоянное запоминающее устройство для хранения спектральных коэффициентов кодового слова $\{b_i(0)\}$ и n умножителей. При умножении фактически происходит только изменение знаков спектральных коэффициентов вектора $\boldsymbol{X}$, следовательно, умножители можно исключить, а изменение знаков выполнять при загрузке второго блока быстрого преобразования Уолша–Адамара.

Предложенные нелинейные ортогональные коды обладают большим ансамблем, высокой помехоустойчивостью и структурной сложностью, декодируются при помощи быстрых преобразований, поэтому они могут найти применение в защищенных высокоскоростных телекоммуникационных системах с обработкой сигнала в реальном масштабе времени.

ORTHOGONAL CODES ON THE BASES OF BENT-SEQUENCES

V.D. DVORNIKOV

Abstract

The paper considers low-rate orthogonal code, which code words get, is formed by dyadic shifts of a bent-sequence. It is proved that the code is orthogonal and nonlinear. The number of different code sets is defined. The algorithm of calculation of dyadic correlation in spectrums Walsh-Hadamard domain is proposed for decoding.

Литература

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М., 1979.
2. *Rothaus O.S.* On Bent Functions // J. Combinatorial Theory. Ser. A. 1979. Vol. 20. P. 300–305.
3. *Prenel B., VanLeekwijck W., VanLinden L., Govaerts R., Vandewalle J.* Propagation characteristics of Boolean functions // Advances in Cryptology. Proc. Eurocrypt ’90. Lecture Notes in Computer Science. Vol. 473. Berlin, Heidelberg, New York: Springer–Verlag, 1991.
4. *Трахтман А.М., Трахтман В.А.* Основы теории дискретных сигналов на конечных интервалах. М., 1975.
5. *Лосев В.В., Бродская Е.Б., Коржик В.И.* Поиск и декодирование сложных дискретных сигналов. М., 1988.