УДК 621.391.26

МЕТОД ФОРМИРОВАНИЯ 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 рассматривается метод формирования бент-последовательностей, использующий свойство инвариантности преобразования Уолша-Адамара и двумерный алгоритм вычисления спектра Уолша-Адамара. Количество различных последовательностей, которые позволяет получить предложенный метод, почти в два раза больше количества, определяемого известной нижней границей. Описано устройство формирования бент-последовательностей, реализующее рассмотренный метод.

Ключевые слова: бент-последовательности, матрицы Уолша–Адамара, спектр Уолша–Адамара, границы числа последовательностей.

Двоичные бент-последовательности (БП), задаваемые при помощи бент-функций (булевых максимально-нелинейных функций), являются смежными классами кодов Рида–Маллера высоких порядков по коду Рида–Маллера первого порядка. Бент-последовательности интенсивно исследуются в теории кодирования [1], связи [2, 3] и криптографии [4–6]. Одной из важнейших теоретических задач является перечисление всех существующих БП длин, превышающих 64. Для этих случаев известны приближенные нижние и верхние границы [5], а решение этой задачи прямым перебором осложняется чрезмерно большим требуемым объемом вычислений. Ниже описывается метод синтеза БП, число которых почти в два раза превышает известную нижнюю границу.

Для описания метода используется представление БП, основанное на свойстве равномерности ее спектра Уолша–Адамара. Пусть имеется последовательность $\{b_i\} = (b_0, b_1, ..., b_{n-1})$, $n = 2^{2m}$, а $b_i = \pm 1$, $i = 0,...,n-1$, и представляется двоичным числом длины $2m$. Тогда $\{b_i\}$ является БП, если

$$\left| b(j) \right| = \sum_{i=0}^{n-1} b_i (-1)^{i \cdot j} = 2^m, \qquad (1)$$

где $j = 0,...,n-1$ — двоичное число длины $2m$, а скалярное произведение $i \cdot j$ вычисляется как сумма по модулю два вида $i_0 j_0 + i_1 j_1 + ... + i_{2m-1} j_{2m-1}$.

В [4] для синтеза БП используется матрица преобразования Уолша–Адамара размерности $2^m \times 2^m$ — $\mathbf{H}_{2^m}$, задаваемая следующей формулой:

$$\boldsymbol{H}_{2^m} = [(-1)^{i \cdot j}], \qquad (2)$$

где $i = 0,...,2^{m-1}$, $j = 0,...,2^m$ — соответственно номера столбца и строки, в которых находится элемент матрицы.

Последовательность $\{b_i\}$ получается конкатенацией в любом порядке взятых с любыми знаками всех строк матрицы $\mathbf{H}_{2^m}$. Нетрудно убедиться, что для любой полученной таким образом последовательности выполняется свойство (1), а общее их число равно $M = (2^m)!\,2^{2^m}$. Данное число и является нижней границей количества различных БП длины 2^{2m}.

Получим из матрицы (2) БП, описываемую выражением

$$\{b_i^0\} = (-1)^{i_1 \cdot i_2}, \tag{3}$$

где $i = i_1 + 2^m i_2$, i_1 и i_2 – соответственно остаток и частное от деления i на 2^m: $i_1 = (i) \bmod 2^m$, $i_2 = (i - i_1)2^{-m}$.

Все возможные последовательности получаются преобразованиями выражения (3).

$$\{b_i^j\} = (b_0^0, b_1^0, ..., b_{n-1}^0)[\boldsymbol{I} \otimes \boldsymbol{P}\boldsymbol{C}], \tag{4}$$

где $j = 0,...,M-1$, $\boldsymbol{I}$ — единичная, $\boldsymbol{P}$ — перестановочная и $\boldsymbol{C}$ — диагональная матрицы размерностью $2^m \times 2^m$, $\otimes$ — символ кронекеровского произведения, а $\boldsymbol{C} = \mathrm{diag}(\pm 1, \pm 1, \pm 1, ..., \pm 1)$.

Всего существует $(2^m)!$ различных матриц $\boldsymbol{P}$ и 2^{2^m} различных матриц $\boldsymbol{C}$. Произведение этих чисел и дает нижнюю границу M [5]. Для $m = 2$ ниже приведены матрицы $\boldsymbol{I}$, $\boldsymbol{P}$ и $\boldsymbol{C}$:

$$\boldsymbol{I} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \boldsymbol{P} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \boldsymbol{C} = \begin{bmatrix} \pm 1 & 0 & 0 & 0 \\ 0 & \pm 1 & 0 & 0 \\ 0 & 0 & \pm 1 & 0 \\ 0 & 0 & 0 & \pm 1 \end{bmatrix}.$$

Произведение матриц вычисляется последовательно:

$$\boldsymbol{I} \otimes \boldsymbol{P}\boldsymbol{C} = \boldsymbol{I} \otimes \begin{bmatrix} \pm 1 & 0 & 0 & 0 \\ 0 & 0 & \pm 1 & 0 \\ 0 & \pm 1 & 0 & 0 \\ 0 & 0 & 0 & \pm 1 \end{bmatrix} = \begin{bmatrix} \pm \mathrm{I} & 0 & 0 & 0 \\ 0 & 0 & \pm \mathrm{I} & 0 \\ 0 & \pm \mathrm{I} & 0 & 0 \\ 0 & 0 & 0 & \pm \mathrm{I} \end{bmatrix}.$$

Вычисления одномерного спектра (1) целесообразно выполнять при помощи двумерного преобразования и воспользоваться свойством инвариантности преобразования Уолша–Адамара. Результатом этих действий будет еще одно выражение для формирования БП:

$$\{b_i^j\} = (b_0^0, b_1^0, ..., b_{n-1}^0)[\boldsymbol{P}\boldsymbol{C} \otimes \boldsymbol{I}]. \tag{5}$$

Формула (5) тоже позволяет получить M различных БП, так как количество разных матриц $\boldsymbol{P}$ и $\boldsymbol{C}$ не изменилось. Для демонстрации метода при $m = 2$ используем матрицу $\mathbf{P}$, рассмотренную выше, $\boldsymbol{C} = \mathrm{diag}(1,1,1,-1)$, а $\{b_i\} = (1,1,1,1,1,-1,1,-1,1,1-1,-1,1,-1,-1,1)$. Тогда получаем

$$\boldsymbol{P}\,\boldsymbol{C}\otimes\boldsymbol{I}=\begin{bmatrix}\boldsymbol{PC} & 0 & 0 & 0\\ 0 & \boldsymbol{PC} & 0 & 0\\ 0 & 0 & \boldsymbol{PC} & 0\\ 0 & 0 & 0 & \boldsymbol{PC}\end{bmatrix},\ \{b_i^j\}=(1,1,1,-1,1,1,-1,1,1,-1,1,1,1,-1,-1,-1).$$

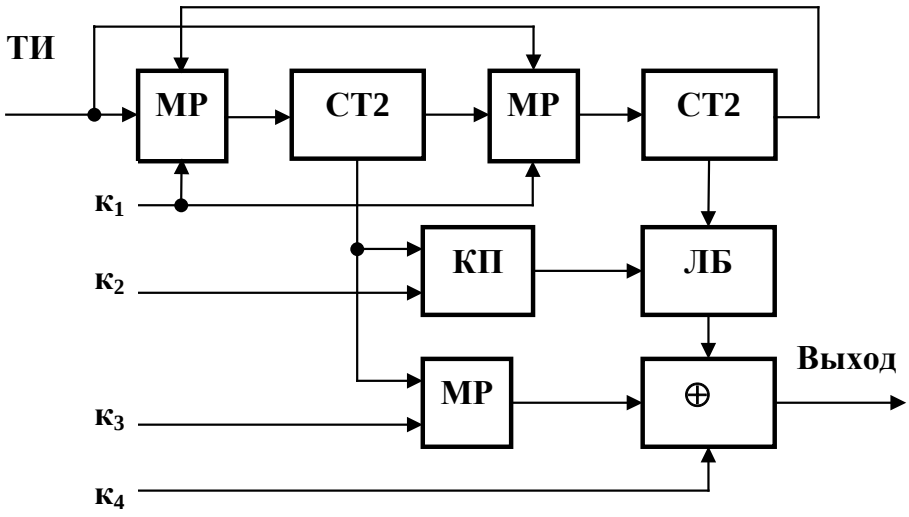
Нетрудно убедиться, что полученная последовательность является БП, так как обладает свойством (1). Кроме того, ее нельзя получить из выражения (4). Совокупное использование формул (4) и (5) позволяет увеличить количество БП, получаемых из $\boldsymbol{H}_{2^m}$. Однако следует учитывать, что этим методом не удается удвоить общее число формируемых последовательностей, поскольку некоторые из них повторяются. Число совпадающих БП легко определить из сравнительного анализа выражений (4) и (5). Оно равно

$$M_c = 2^{2m+1}\prod_{r=0}^{m-1}(2^m-2^r).$$

Следовательно, общее число не повторяющихся последовательностей, которые можно получить, определяется выражением

$$M_{\acute{i}} = 2M - M_c = (2^m)!\,2^{2^m+1} - 2^{2m+1}\prod_{r=0}^{m-1}(2^m-2^r).$$

На рисунке приведено устройство для формирования бент-последовательностей, общее число которых равно $(2^m)!\,2^{2^m+1}$.



Структурная схема устройства формирования бент-последовательностей

Устройство содержит два m-разрядных двоичных счетчика, объединенных при помощи мультиплексоров, кодопреобразователь (КП), логический блок (ЛБ), сумматор по модулю два и мультиплексор. Совокупность управляющих сигналов $К_1$, $К_2$, $К_3$ и $К_4$ обеспечивает получение $(2^m)!\,2^{2^m+1}$ различных БП. При этом $К_1$ позволяет формировать группу последовательностей, описываемых выражениями (4) или (5), а $К_4$ управляет их инверсией. Кодопреобразователь использует выходные сигналы счетчика и сигналы $К_2$ для реализации перестановочных матриц $\boldsymbol{P}$, а $К_3$ и мультиплексор — матриц $\boldsymbol{C}$.

Предложенный метод позволяет не только увеличить мощность ансамбля генерируемых БП, но и уточнить нижнюю границу их количества.

METHOD OF FORMING BENT-SEQUENCES

V.D. DVORNIKOV

Abstract

The paper considers a method of forming bent-sequences using the invariance feature of Walsh-Hadamard transform and two-dimensional algorithm of calculation of Walsh-Hadamard spectrums. The number of different sequences that allows us to obtain the proposed method is twice more the number defined by the known low bound. The device of bent-sequences forming realizing the method is described.

Литература

1. Rothaus O.S. On Bent Functions // J. Combinatorial Theory. Ser. A. 1979. Vol. 20, P. 300–305.
2. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М., 1979.
3. Лосев В.В., Бродская Е.Б., Коржик В.И. Поиск и декодирование сложных дискретных сигналов. М., 1988.
4. Adams C.M., Tavares S.E. // IEEE Trans. Inform. Theory. 1990. Vol. IT–36, № 5. P. 1170–1173.
5. 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.
6. Olsen J.D., Scholtz R.A., Welch L.R. // IEEE Trans. Inform. Theory. 1982. Vol. IT–28, №6. P. 858–864.