

УДК 519.7

КЛАССИФИКАЦИЯ ГРАФОВ АНФ КВАДРАТИЧНЫХ БЕНТ-ФУНКЦИЙ ОТ ШЕСТИ ПЕРЕМЕННЫХ

Е. П. Корсакова

В математике часто возникает задача построения булевых функций, обладающих свойством нелинейности. Особенный интерес представляют функции, для которых эти свойства экстремальны. Такие булевы функции от четного числа переменных называются бент-функциями. Определим понятие бент-функции более строго. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция W_f , заданная на множестве $\mathbb{Z}_2^n$ равенством $W_f(v) = \sum_{u \in \mathbb{Z}_2^n} (-1)^{\langle u, v \rangle \oplus f(u)}$.

Бент-функцией называется булева функция от n переменных (n четно), такая, что модуль каждого коэффициента Уолша — Адамара этой функции равен $2^{n/2}$.

Несмотря на то, что масштабы исследования бент-функций велики, в настоящее время они изучены довольно плохо. Например, задача описания всех бент-функций от n переменных решена лишь при малых значениях n . При $n \geq 10$ класс бент-функций не описан, его мощность неизвестна.

Обратимся к вопросу классификации бент-функций степени 2 от 6 переменных. Известно [1], что все квадратичные бент-функции аффинно эквивалентны между собой. Введем для таких функций понятие более сильной эквивалентности, а именно графовой эквивалентности. Каждой функции сопоставим граф на шести вершинах. Вершины графа отождествим с переменными булевой функции, ребрами соединим те вершины, которые образуют слагаемое в квадратичной части алгебраической нормальной формы (АНФ) функции. Для каждого графа определим его тип — упорядоченный по убыванию набор степеней его вершин. Две функции назовем *графово эквивалентными*, если соответствующие им графы изоморфны. В данной работе решена задача графовой классификации всех квадратичных бент-функций от 6 переменных.

Все квадратичные бент-функции аффинно эквивалентны функции $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$. Поэтому для нахождения графов использовались аффинные преобразования этой функции, заданные верхнетреугольными матрицами с 1 на диагонали, 0 или 1 над диагональю, а именно вида

$$\begin{pmatrix} 1 & * & * & * & * & * \\ 0 & 1 & * & * & * & * \\ 0 & 0 & 1 & * & * & * \\ 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

где на местах $*$ стоят 0 или 1. Написана программа на С, которая, перебирая все возможные матрицы данного вида, определяет типы графов. В результате получено 37 типов и 50 графово неэквивалентных бент-функций. В таблице приведены все типы в левой колонке и соответствующие им бент-функции — в правой. Функция задана вектором лексикографически упорядоченных коэффициентов в квадратичной части АНФ (в скобках указан возможный способ её построения из бент-функции от четырех переменных).

№ п/п	Тип	Функция	№ п/п	Тип	Функция
1	1 1 1 1 1 1	100000000100001 (iter1)	14	4 3 3 2 1 1	100001101100011
2	2 2 1 1 1 1	100001000100001 (iter1)	15	4 3 3 2 2 2	111011000100101
3	2 2 2 2 1 1	100001000100101 (iter2)	16	4 3 3 3 2 1	111100001110100 (iter3)
4	3 2 2 1 1 1	100001001001100 (iter1) 100001001100001 (iter3)	17	4 3 3 3 3 2	110011000110111
5	3 2 2 2 2 1	100001001100101 100001000010111	18	4 4 3 2 2 1	100001101100111
6	3 3 2 2 1 1	100001001110001 (iter1) 100001000110101 (iter2)	19	4 4 3 3 1 1	100001101101110 (iter2)
7	3 3 2 2 2 2	011001011100001 101101001100001	20	4 4 3 3 2 2	110001011110011
8	3 3 3 1 1 1	100001010110001 (iter2)	21	4 4 3 3 3 1	100001100111111
9	3 3 3 2 2 1	100001001100111 (iter2) 100001001110101 100001001100111	22	4 4 3 3 3 3	111011001110101
10	3 3 3 3 1 1	100001010110110 (iter2) 111001100100001 (iter1) 111000000110101 (iter1)	23	4 4 4 3 3 2	011101001110111
11	3 3 3 3 2 2	110011100100101 110101001100101 111001001100101 101101001100101	24	4 4 4 4 3 1	100001101111111
12	4 2 2 2 1 1	100001101100001 (iter3)	25	4 4 4 4 3 3	111001100010111 110101101100111
13	4 3 2 2 2 1	100001101100101 100001100100111	26	5 2 2 2 2 1	100001111100001
			27	5 3 3 2 2 1	100001111100101
			28	5 3 3 3 2 2	110001000111111
			29	5 3 3 3 3 3	110101001111110
			30	5 4 3 3 2 1	100001111111100
			31	5 4 4 3 2 2	110111000111101
			32	5 4 4 4 3 2	111101000111111
			33	5 4 4 4 4 1	100001111111111
			34	5 5 3 3 3 3	111001100111111
			35	5 5 4 4 3 3	111001111111011
			36	5 5 5 4 4 3	111101111111110
			37	5 5 5 5 5 5	111111111111111

Поясним обозначения. Конструкция iter1 означает, что к бент-функции от четырёх переменных добавляется слагаемое x_5x_6 ; iter2 — слагаемое $x_ix_5 \oplus x_jx_6$, где $i, j \in \{1, 2, 3, 4\}$; iter3 — слагаемое $x_ix_5 \oplus x_5x_6$, где $i \in \{1, 2, 3, 4\}$. Пример: АНФ функции, заданной вектором 100001101100011, имеет вид $x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_4x_6 \oplus x_5x_6$. Данное исследование помогает выявить общие закономерности построения бент-функций от $(n + 2)$ переменных с помощью бент-функций от n переменных.

ЛИТЕРАТУРА

1. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.

УДК 519.7

СЛАБОЦЕНТРАЛЬНЫЕ КЛОНЫ И ПРОБЛЕМА ПОЛНОТЫ В НИХ¹

Н. Г. Парватов

Проблема полноты и критериальные системы. Пусть E — конечное множество. Через P_E обозначается множество функций $f : E^n \rightarrow E$ при всевозможных целых положительных n . Классы таких функций, замкнутые операциями суперпозиции и

¹Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).