6. *Куценко А. В.* Спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда // Дискретный анализ и исследование операций. 2018. Т. 25. № 1. С. 98–119.
7. *Danielsen L. E., Parker M. G., and Solé P.* The Rayleigh quotient of bent functions // LNCS. 2009. V. 5921. P. 418–432.
8. *Марков А. А.* О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2003. С. 70–93.
9. *Tokareva N. N.* The group of automorphisms of the set of bent functions // Discr. Math. Appl. 2010. No. 20 (5). P. 655–664.

УДК 519.7 DOI 10.17223/2226308X/12/17

О КЛАССАХ БУЛЕВЫХ ФУНКЦИЙ ОГРАНИЧЕННОЙ СЛОЖНОСТИ[1]

А. И. Метальникова, И. А. Панкратова

Рассматриваются классы булевых функций от n переменных, имеющих короткое (по сравнению с 2^n) представление. Подсчитаны мощности этих классов, приведены тесты на принадлежность функции классам и алгоритм доопределения частично заданной булевой функции до функции ограниченной степени.

Ключевые слова: *существенная зависимость функции от переменной, степень булевой функции, алгебраическая нормальная форма.*

Во многих шифрсистемах используются булевы функции. Если функция является ключом, как, например, в [1, 2], то она должна зависеть от большого числа переменных. Поскольку длина вектора значений булевой функции от n переменных равна 2^n и формула (в любом базисе) произвольной функции имеет ту же длину (порядка 2^n), представляют интерес классы функций, которые зависят от большого числа переменных, но имеют короткое задание. В связи с этим возникают следующие задачи: подсчёт количества функций в классе; разработка теста на принадлежность функции классу; разработка алгоритма доопределения частичной функции до функции из заданного класса.

Обозначим $P_2(n)$ множество всех булевых функций от n переменных; будем рассматривать следующие классы функций в $P_2(n)$ и называть их классами ограниченной сложности:

— $C_{n,k}$ — с заданным (равным k) числом существенных переменных;
— $C_{n,\leqslant k}$ — с ограниченным (не больше k) числом существенных переменных;
— $D_{n,k}$ — заданной степени ($\deg f = k$);
— $D_{n,\leqslant k}$ — ограниченной степени ($\deg f \leqslant k$);
— $L_{n,k}$ — с заданной (равной k) длиной алгебраической нормальной формы (АНФ);
— $L_{n,\leqslant k}$ — с ограниченной (не больше k) длиной АНФ;
— NR_n — имеющие бесповторную АНФ (каждая переменная входит в АНФ не более одного раза).

В таблице приведены мощности этих классов, здесь $\mathbb{S}_k$ — количество функций от k переменных, существенно зависящих от всех своих переменных (последовательность A000371 из [3]), $\mathbb{S}_k = \sum\limits_{i=0}^{k}(-1)^i\binom{k}{i}2^{2^{k-i}}$; $\mathbb{B}_k$ — число Белла, или количество всех

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

неупорядоченных разбиений k-элементного множества (последовательность A000110 из [3]), задаваемое рекуррентной формулой $\mathbb{B}_0 = 1$, $\mathbb{B}_{k+1} = \sum\limits_{i=0}^{k} \binom{k}{i} \mathbb{B}_i$.

Класс	Мощность
$C_{n,k}$	$\binom{n}{k}\mathbb{S}_k$
$C_{n,\leqslant k}$	$\sum\limits_{i=0}^{k} \lvert C_{n,i}\rvert = \sum\limits_{i=0}^{k} \binom{n}{i}\mathbb{S}_i$
$D_{n,k}$	$2^{\sum\limits_{i=0}^{k}\binom{n}{i} - \sum\limits_{i=0}^{k-1}\binom{n}{i}}$
$D_{n,\leqslant k}$	$2^{\sum\limits_{i=0}^{k}\binom{n}{i}}$
$L_{n,k}$	$\binom{2^n}{k}$
$L_{n,\leqslant k}$	$\sum\limits_{i=0}^{k}\binom{2^n}{i}$
NR_n	$2\mathbb{B}_{n+1}$

Принадлежность функции f классу ограниченной сложности определяется свойствами её АНФ, например, $\deg f$ равна длине самого длинного слагаемого в АНФ; количество существенных переменных — количеству переменных, входящих в АНФ. АНФ, в свою очередь, строится с помощью преобразования Мёбиуса $\mu : P_2(n) \to P_2(n)$ [4]:

$$f(x) = \bigoplus_{a \in \mathbb{Z}_2^n} g(a)x^a, \quad g = \mu(f),$$
$$g(a) = \bigoplus_{x \leqslant a} f(x). \tag{1}$$

Для $g = \mu(f)$ обозначим $\{a_1, \ldots, a_r\}$ множество всех векторов, на которых $g(a_i) = 1$, $i = 1, \ldots, r$; единичным компонентам в a_i соответствуют переменные, входящие в i-е слагаемое АНФ функции f. Через $\mathrm{w}(x)$ ($\mathrm{w}(f)$) обозначим вес булева вектора x (функции f). Тогда $t = \mathrm{w}\left(\bigvee\limits_{i=1}^{k} a_i\right)$ — количество существенных переменных функции f; $d = \max\limits_{i=1,\ldots,r} \mathrm{w}(a_i)$ — её степень. Получаем следующие тесты принадлежности функции f классам ограниченной сложности:

— если $t = k$, то $f \in C_{n,k}$; если $t \leqslant k$, то $f \in C_{n,\leqslant k}$;
— если $d = k$, то $f \in D_{n,k}$; если $d \leqslant k$, то $f \in D_{n,\leqslant k}$;
— если $\mathrm{w}(g) = k$, то $f \in L_{n,k}$; если $\mathrm{w}(g) \leqslant k$, то $f \in L_{n,\leqslant k}$.

Чуть сложнее проверяется принадлежность функции классу NR_n. Составим матрицу A размера $r \times n$, строками которой являются векторы a_i, $i = 1, \ldots, r$. Тогда $f \in NR_n$, если и только если веса всех столбцов матрицы A не больше 1; другими словами, $f \notin NR_n$, если и только если какой-либо столбец матрицы A содержит хотя бы две единицы. Соответствующая проверка выполняется в алгоритме 1.

Задача доопределения функции до функции из заданного класса $\mathcal{C} \subseteq P_2(n)$ ставится так: частично определённая функция $f \in P_2(n)$ задана множествами $M_0 = \{x \in \mathbb{Z}_2^n : f(x) = 0\}$ и $M_1 = \{x \in \mathbb{Z}_2^n : f(x) = 1\}$, $M_0 \cap M_1 = \varnothing$; найти все такие функции $g \in \mathcal{C}$, что $g(x) = f(x)$ для всех $x \in M_0 \cup M_1$. Рассмотрим случай $\mathcal{C} = D_{n,\leqslant k}$.

АНФ функции $f \in D_{n,\leqslant k}$ обладает следующим свойством: $g(x) = 0$ для всех x, таких, что $\mathrm{w}(x) > k$, где $g = \mu(f)$. Обозначим вектор значений функции f как $\mathbf{b} =$

Алгоритм 1. Тест на принадлежность функции f классу NR_n

Вход: Функция $f \in P_2(n)$; матрица A со строками $\{a_1, \ldots, a_r\}$.

1: $x := a_1$.
2: **Для** $i = 2, \ldots, r$
3: $\quad y := x \oplus a_i$.
4: $\quad$ **Если** $x\&\bar{y} = \mathbf{0}$, **то**
$\qquad$ выход, ответ: $f \notin NR_n$.
5: $\quad x := y$.
6: Ответ: $f \in NR_n$.

$= (b_0 b_1 \ldots b_{2^n-1})$, $b_i = f(i)$ (здесь мы не различаем число в диапазоне от 0 до $2^n - 1$ и его представление в виде булева вектора длины n).

В самом общем виде (если $M_0 = M_1 = \varnothing$) решение задачи состоит в следующем: для каждого x, такого, что $\mathrm{w}(x) > k$, в соответствии с формулой (1) составляем уравнение $\bigoplus\limits_{i \leqslant x} b_i = 0$. Обозначим матрицу полученной системы линейных однородных уравнений (СЛОУ) $B_{n,k}$. Все решения получившейся СЛОУ

$$B_{n,k}\mathbf{b} = \mathbf{0} \tag{2}$$

являются векторами значений функций из $D_{n,\leqslant k}$.

Для поиска доопределений частично заданной функции (если $M_0 \neq \varnothing$ или $M_1 \neq \varnothing$) решаем ту же систему относительно переменных множества $\{b_i : i \notin M_0 \cup M_1\}$, объявив константами 0 и 1 переменные b_i с номерами из множеств M_0 и M_1 соответственно. Таким образом, СЛОУ (2) преобразуется к системе уже не обязательно однородных уравнений.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
2. *Агибалов Г. П.* SIBCiphers — симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // Прикладная дискретная математика. Приложение. 2014. № 7. С. 43–48.
3. *Sloan N. J. A.* The On-line Encyclopedia of Integer Sequences. `https://oeis.org/`
4. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

УДК 519.7 DOI 10.17223/2226308X/12/18

О СВЯЗИ НЕЛИНЕЙНЫХ И ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

А. В. Милосердов

Исследуются связи таблиц линейного приближения (LAT) и распределения разностей (DDT) векторных булевых функции. Доказано, что наличие совпадающих строк в DDT и LAT является инвариантом относительно аффинной эквивалентности, а также относительно EA-эквивалентности для нормированных DDT- и

[1]Работа поддержана грантами РФФИ, проекты № 18-07-01394 и 18-31-00374.