11. *Коломеец Н. А.* Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. 2014. №3. С. 28–39.

УДК 519.719.1 DOI 10.17223/2226308X/8/17

ПЕРЕЧИСЛЕНИЕ ДВОИЧНЫХ ФУНКЦИЙ, ИМЕЮЩИХ ЗАДАННОЕ ЧИСЛО АФФИННЫХ СОМНОЖИТЕЛЕЙ

А. В. Черемушкин

Предлагается рекурсивный способ вычисления числа двоичных функций от n переменных, имеющих заданное число аффинных сомножителей, допускающий введение ограничений на вес или степень нелинейности функций.

Ключевые слова: *двоичные функции, аффинная классификация, формула обращения Мёбиуса.*

1. Случай обычных функций

Пусть $n \geqslant 0$. Подсчитаем число двоичных функций от n переменных заданного веса, имеющих аффинные сомножители. Функция $f : V_n(2) \to \{0, 1\}$ *имеет аффинные сомножители*, если найдутся такие функция $l(x) = (x, a^*) \oplus b$, $x \in V_n(2)$, $0 \neq a^* \in \in V_n(2)^*$ ($V_n(2)^*$ — сопряжённое пространство), $b \in \{0, 1\}$ и функция h, что $f = l \cdot h$.

Пусть $k \in \{0, \ldots, n\}$. Обозначим через $\mathcal{F}_n(k)$ множество всех двоичных функций от n переменных, имеющих ровно k аффинных сомножителей. Функцию $f \equiv 0$ не включаем ни в одно из множеств $\mathcal{F}_n(k)$. Легко видеть, что выполняется равенство

$$\mathcal{F}_n = \bigcup_{k=0}^{n} \mathcal{F}_n(k) \cup \{0\}. \tag{1}$$

Справедливы следующие свойства:

1. Множества $\mathcal{F}_n(k)$ при разных k не пересекаются, $k = 0, \ldots, n$.
2. Множества $\mathcal{F}_n(k)$, $k = 0, \ldots, n$, инвариантны относительно действия полной аффинной группы $\mathbf{AGL}\,(n, 2)$ (и, следовательно, разбиваются на классы эквивалентности относительно этой группы).
3. Каждую функцию $f \in \mathcal{F}_n(k)$ можно привести с помощью некоторого аффинного преобразования к виду

$$h(x) = f(xQ \oplus b) = \overline{x}_1 \ldots \overline{x}_k g(x_{k+1}, \ldots, x_n), \tag{2}$$

   где $g \in F_{n-k}(0)$.
4. Если $k \in \{0, \ldots, n\}$ и $f \in \mathcal{F}_n(k)$, то $1 \leqslant \|f\| \leqslant 2^{n-k}$, где $\|f\|$ — вес функции f.
5. Множество векторов, входящих в область истинности $\{a \in V_n(2) : f(a) = 1\}$ функции f вида (2), порождает смежный класс по подпространству размерности $n - k$.

Теорема 1. Пусть $1 \leqslant k \leqslant n$ и функции $f, h \in \mathcal{F}_n(k)$ и $g \in \mathcal{F}_{n-k}(0)$ удовлетворяют равенству (2). Тогда порядки групп инерции функций f, h и g в группе аффинных преобразований связаны равенством

$$|\mathbf{AGL}\,(n, 2)_f| = |\mathbf{AGL}\,(n, 2)_h| = 2^{k(n-k)} |\mathbf{GL}\,(k, 2)| \cdot |\mathbf{AGL}\,(n-k, 2)_g|. \tag{3}$$

Доказательство вытекает из инвариантности подпространства, порождённого областью истинности функции.

При $n \geqslant 1$ числа

$$\left[\begin{array}{c} n \\ k \end{array} \right]_2 = \begin{cases} \prod\limits_{i=0}^{k-1} \dfrac{2^n - 2^i}{2^k - 2^i}, & \text{если } k \in \{1, \ldots, n\}, \\ 1, & \text{если } k = 0, \end{cases}$$

называются *коэффициентами Гаусса* (индекс 2 для простоты записи далее будем опускать).

Теорема 2. При $1 \leqslant k \leqslant n$ справедливо равенство

$$|\mathcal{F}_n(k)| = 2^k \left[\begin{array}{c} n \\ k \end{array} \right] \cdot |\mathcal{F}_{n-k}(0)|. \tag{4}$$

Доказательство. Для каждой функции $f \in \mathcal{F}_n(k)$ число эквивалентных ей функций совпадает с индексом группы инерции

$$|f^{\mathbf{AGL}\,(n,2)}| = (\mathbf{AGL}\,(n,2) : \mathbf{AGL}\,(n,2)_f),$$

который в силу теоремы 1 равен $2^k \left[\begin{array}{c} n \\ k \end{array} \right] \cdot |g^{\mathbf{AGL}\,(n-k,2)}|$. Применяя данное равенство для всех функций $f \in \mathcal{F}_n(k)$, получаем формулу (4). ■

Наряду с множествами $\mathcal{F}_n$ и $\mathcal{F}_n(k)$, $k = 0, \ldots, n$, рассмотрим $(2^n + 1)$-мерные вектор-столбцы $\mathcal{F}_n^{\downarrow}$ и $\mathcal{F}_n^{\downarrow}(k)$, j-я координата которых равна числу функций из соответствующего множества, имеющих вес j, $j = 0, \ldots, 2^n$. Для этих векторов справедливо аналогичное (1) соотношение

$$\mathcal{F}_n^{\downarrow} = \sum_{k=0}^{n} \mathcal{F}_n^{\downarrow}(k) + \{\varepsilon_0^{\downarrow}\},$$

где $\varepsilon_0^{\downarrow}$ — вектор, у которого первая координата равна 1, а остальные — нули. В силу свойства 4 у векторов $\mathcal{F}_n^{\downarrow}(k)$ первая координата и последние $2^n - 2^{n-k}$ координат равны нулю. Заметим, что в (2) веса функций f, h и g совпадают. Поэтому равенства, аналогичные (4), выполняются между первыми $2^{n-k} + 1$ координатами вектор-столбцов $\mathcal{F}_n^{\downarrow}$ и $\mathcal{F}_{n-k}^{\downarrow}(0)$. Дополним вектор $\mathcal{F}_{n-k}^{\downarrow}(0)$, имеющий длину $2^{n-k} + 1$, до вектора длины $2^n + 1$, полагая координаты с номерами j, $2^{n-k} + 1 \leqslant j \leqslant 2^n$, равными нулю. С учётом этого дополнения можно записать равенство (4) в векторном виде

$$\mathcal{F}_n^{\downarrow}(k) = 2^k \left[\begin{array}{c} n \\ k \end{array} \right] \mathcal{F}_{n-k}^{\downarrow}(0). \tag{5}$$

В силу равенств (4) и (5) для вычисления значений $\mathcal{F}_n^{\downarrow}(k)$, $k = 0, \ldots, n$, достаточно вычислить лишь величины $z_m = |\mathcal{F}_m(0)|$ и $z_{mj} = \mathcal{F}_m^{\downarrow}(0)_j$, $j = 0, \ldots, 2^m$, $m = 0, \ldots, n$.

Воспользуемся равенством

$$2^{2^n} = \sum_{k=0}^{n} |\mathcal{F}_n(k)| + 1,$$

которое непосредственно вытекает из равенства (1) и свойства 1.

Обозначая для краткости

$$h(n,k) = 2^k \left[\begin{array}{c} n \\ k \end{array} \right],$$

с учётом равенства (4) получаем рекуррентное соотношение

$$z_n = 2^{2^n} - 1 - \sum_{k=1}^{n} h(n,k) z_{n-k}. \tag{6}$$

Аналогично, с учётом равенства (5) имеем $z_{n0} = 0$ и для $j = 1, \ldots, 2^n$

$$z_{nj} = \binom{2^n}{j} - \sum_{k=1}^{n} h(n,k) z_{n-k,j}. \tag{7}$$

При этом при всех $n \geqslant 0$ выполнено равенство $\sum\limits_{j=0}^{2^n} z_{nj} = z_n$.

Рекуррентные соотношения (6) и (7) позволяют вычислять значения величин z_n и z_{nj}, $j = 0, \ldots, 2^n$, последовательно для $n = 0, 1, 2, \ldots$ В табл. 1 приведены соответствующие значения при $n = 3$.

Таблица 1

j	$\lvert\mathcal{F}_3\rvert$	$\{0\}$	$\lvert\mathcal{F}_3(3)\rvert$	$\lvert\mathcal{F}_3(2)\rvert$	$\lvert\mathcal{F}_3(1)\rvert$	$\lvert\mathcal{F}_3(0)\rvert$
0	1	1	0	0	0	0
1	8	0	8	0	0	0
2	28	0	0	28	0	0
3	56	0	0	0	56	0
4	70	0	0	0	14	56
5	56	0	0	0	0	56
6	28	0	0	0	0	28
7	8	0	0	0	0	8
8	1	0	0	0	0	1
Всего	256	1	8	28	70	149

Найдём теперь общий вид решений рекуррентных уравнений (6) и (7). Формула обращения Мёбиуса в данном случае принимает следующий вид.

Утверждение 1 [1, 2]. Если последовательности $\{u_n\}$ и $\{w_n\}$ связаны соотношением

$$u_n = \sum_{k=0}^{n} \left[\begin{array}{c} n \\ k \end{array} \right] w_{n-k}, \qquad n \geqslant 0,$$

то

$$w_n = \sum_{k=0}^{n} (-1)^k 2^{k(k+1)/2} \left[\begin{array}{c} n \\ k \end{array} \right] u_{n-k}, \qquad n \geqslant 0.$$

Переписав рекуррентное соотношение (6) в виде $\dfrac{2^{2^n}-1}{2^n} = \sum\limits_{k=0}^{n} \left[\begin{array}{c} n \\ k \end{array} \right] \dfrac{z^{n-k}}{2^{n-k}}$, с помощью формулы обращения получаем следующий окончательный результат.

Теорема 3. При всех $n \geqslant 0$ справедлива формула

$$z_n = |\mathcal{F}_n(0)| = \sum_{k=0}^{n} (-1)^k 2^{k(k+1)/2} \left[\begin{array}{c} n \\ k \end{array} \right] (2^{2^{n-k}} - 1) 2^k.$$

Эта формула позволяет, например, оценить вероятность p_n того, что у функции $f(x_1,\dots,x_n)$ есть аффинные сомножители:

$$p_n = 1 - \frac{z_n}{2^{2^n}}.$$

Значения вероятности p_n при $1 \leqslant n \leqslant 10$ представлены в табл. 2.

Таблица 2

n	p_n	n	p_n
1	0,75	6	$2{,}9 \cdot 10^{-8}$
2	0,6875	7	$1{,}3 \cdot 10^{-17}$
3	0,4218	8	$1{,}4 \cdot 10^{-38}$
4	0,0809	9	$8{,}8 \cdot 10^{-75}$
5	$8{,}9 \cdot 10^{-4}$	10	$1{,}5 \cdot 10^{-151}$

2. Случай сравнения функций по модулю

При $-1 \leqslant s \leqslant n-1$ обозначим $\mathcal{U}_s$ подпространство функций, степень нелинейности которых не превышает s (степень нулевой функции полагаем равной -1).

Аналогично предыдущему случаю, при $k \in \{0,\dots,n\}$ обозначим через $\mathcal{F}_n^{(s)}(k)$ множество всех двоичных функций, имеющих ровно k линейно независимых аффинных сомножителей по модулю $\mathcal{U}_s$. Функции $f \in \mathcal{U}_s$ не включаем ни в одно из множеств $\mathcal{F}_n^{(s)}(k)$, $k = 0,\dots,n$. Легко видеть, что выполняется равенство

$$\mathcal{F}_n = \bigcup_{k=0}^{n} \mathcal{F}_n^{(s)}(k) \cup \mathcal{U}_s.$$

Заметим, что в работе [4] получена точная формула для числа функций от n переменных с алгебраической иммунностью равной 1, т. е. $AI_n(f) = 1$. Этот класс функций можно записать в виде

$$B_1 = \bigcup_{k=1}^{n} \mathcal{F}_n^{(0)}(k).$$

Справедливы следующие свойства:

1. Множества $\mathcal{F}_n^{(s)}(k)$ при разных k не пересекаются, $k = 0,\dots,n$.
2. Множества $\mathcal{F}_n^{(s)}(k)$, $k = 0,\dots,n$, инвариантны относительно действия группы $\mathbf{AGL}\,(n,2)\mathcal{U}_s$ (и, следовательно, разбиваются на классы эквивалентности относительно этой группы).
3. Каждую функцию $f \in \mathcal{F}_n^{(s)}(k)$ можно привести с помощью некоторого аффинного преобразования к виду

$$h(x) = f(xQ \oplus b) \equiv \overline{x}_1 \cdots \overline{x}_k g(x_{k+1},\dots,x_n) \ (\mathrm{mod}\,\mathcal{U}_s), \tag{8}$$

где $g \in F_{n-k}^{(s-k)}(0)$.

Аналогично предыдущему случаю (подробнее см. [3]) доказываются:

Теорема 4. Пусть $s \geqslant 0$, $1 \leqslant k \leqslant n$ и функции $f, h \in \mathcal{F}_n^{(s)}(k)$ и $g \in \mathcal{F}_{n-k}^{(s-k)}(0)$ удовлетворяют равенству (8). Тогда порядки групп инерции функций f, h и g по модулю $\mathcal{U}_s$ связаны равенством

$$|\mathbf{AGL}\,(n,2)_f^{(s)}| = |\mathbf{AGL}\,(n,2)_h^{(s)}| =$$

$$= \begin{cases} 2^{k(n-k+1)}|\mathbf{GL}\,(k,2)| \cdot |\mathbf{AGL}\,(n-k,2)_g^{(s-k)}|, & \text{если } s = \deg f - 1, \\ 2^{k(n-k)}|\mathbf{GL}\,(k,2)| \cdot |\mathbf{AGL}\,(n-k,2)_g^{(s-k)}|, & \text{если } s \leqslant \deg f - 2. \end{cases}$$

Теорема 5. При всех $s \geqslant 0$, $1 \leqslant k \leqslant n$ справедливо равенство

$$|\mathcal{F}_n^{(s)}(k)| = \begin{cases} \begin{bmatrix} n \\ k \end{bmatrix} |\mathcal{F}_{n-k}^{(s-k)}(0)| \dfrac{|\mathcal{U}_s^{(n)}|}{|\mathcal{U}_{s-k}^{(n-k)}|}, & \text{если } s = \deg f - 1, \\ 2^k \begin{bmatrix} n \\ k \end{bmatrix} |\mathcal{F}_{n-k}^{(s-k)}(0)| \dfrac{|\mathcal{U}_s^{(n)}|}{|\mathcal{U}_{s-k}^{(n-k)}|}, & \text{если } s \leqslant \deg f - 2. \end{cases} \tag{9}$$

Равенство (9) позволяет составить соотношение рекуррентного типа, которое можно решить также с помощью формулы обращения Мёбиуса. Обозначим

$$z_{nj}^{(s)} = |\mathcal{F}_n^{(s)}(0) \cap (\mathcal{U}_j \backslash \mathcal{U}_{j-1})|, \quad j = 0, \ldots, n.$$

Аналогично введём $(n+1)$-мерные векторы $\mathcal{F}_n^{(s)}(k)^{\Downarrow}$, j-я координата которых равна числу функций из множества $\mathcal{F}_n^{(s)}(k)$ степени нелинейности j, $j = 0, \ldots, n$.

Пусть $n > j > s$. Воспользуемся соотношением

$$(2^{\binom{n}{j}} - 1)|\mathcal{U}_{j-1}^{(n)}| = \sum_{k=0}^{n} (\mathcal{F}_n^{(s)}(k)^{\Downarrow})_j,$$

которое непосредственно вытекает из свойства 1. С учётом равенства (9) и теоремы 5 при фиксированных j и s получаем соотношение

$$(2^{\binom{n}{j}} - 1)|\mathcal{U}_{j-1}^{(n)}| = \begin{cases} \displaystyle\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} z_{n-k,j-k}^{(s-k)} \frac{|\mathcal{U}_s^{(n)}|}{|\mathcal{U}_{s-k}^{(n-k)}|}, & \text{если } j = s+1, \\ \displaystyle\sum_{k=0}^{n} 2^k \begin{bmatrix} n \\ k \end{bmatrix} z_{n-k,j-k}^{(s-k)} \frac{|\mathcal{U}_s^{(n)}|}{|\mathcal{U}_{s-k}^{(n-k)}|}, & \text{если } j > s+1. \end{cases}$$

В табл. 3 приведены для примера соответствующие значения при $n = 3$.

Таблица 3

s	$\{\mathcal{U}_s\}$	$\lvert\mathcal{F}_3^{(s)}(3)\rvert$	$\lvert\mathcal{F}_3^{(s)}(2)\rvert$	$\lvert\mathcal{F}_3^{(s)}(1)\rvert$	$\lvert\mathcal{F}_3^{(s)}(0)\rvert$
-1	1	8	28	70	149
0	2	16	56	126	56
1	16	128	112	0	0
2	128	128	0	0	0
3	256	0	0	0	0

ЛИТЕРАТУРА

1. *Comtet M. L.* Nombres de Stirling generaux et fonctions symmetriques // C. R. Acad. Sc. Paris. 1972. V. 275. Ser. A. P. 747–750.
2. *Bender E. A. and Goldman J. R.* On the application of the Möbius inversion in combinatorial analysis // Amer. Math. Monthly. 1975. V. 82. No. 8. P. 789–803.
3. *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. Т. 4. М.: Физматлит, 2001. С. 273–314.
4. *Tu Z. and Deng Y.* Algebraic Immunity Hierarchy of Boolean Functions. Cryptology ePrint Archive, Report 2007/259, 2007. `e-print.iacr.org`. 6 p.