2) $L \overset{n}{\circ} R = \{w_1 \overset{n}{\circ} w_2 : w_1 \in L \text{ и } w_2 \in R\}$;

3) $L^{\overset{n}{+}} = \bigcup\limits_{i=1}^{\infty} L^i$, где $L^1 = L$; $L^{i+1} = L^i \overset{n}{\circ} L$ для всех $i \geqslant 1$.

Рассмотрим семейство алгебр $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$. В случае, когда $n = 0$, операция $\overset{n}{\circ}$ совпадает с операцией конкатенации, а рассматриваемая алгебра является алгеброй регулярных языков.

Регулярные выражения в алгебре $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$ определим следующим образом:

1) $\varnothing$ является регулярным выражением и представляет язык $L(\varnothing) = \varnothing$;
2) x является регулярным выражением и представляет язык $L(x) = \{x\}$ для всех $x \in \bigcup\limits_{0 \leqslant i \leqslant n+1} X^i$;
3) если R и Q — регулярные выражения, представляющие языки $L(R)$ и $L(Q)$ соответственно, то выражения $(R \overset{n}{\circ} Q)$, $(R \cup Q)$, $(R^{\overset{n}{+}})$ также являются регулярными, причем $L(R \overset{n}{\circ} Q) = L(R) \overset{n}{\circ} L(Q)$, $L(R \cup Q) = L(R) \cup L(Q)$, $L(R^{\overset{n}{+}}) = (L(R))^{\overset{n}{+}}$.

Графом с отмеченными дугами (вершинами) назовем четверку $G = (Q, E, X, \mu)$, где Q — конечное множество вершин; $E \subseteq Q \times Q$ — множество дуг; X — конечное множество отметок дуг; $\mu : E \to X$ ($\mu : Q \to X$) — функция отметок дуг (вершин). Отметкой пути будем называть последовательность отметок входящих в этот путь дуг (вершин).

Пусть $I \subseteq Q$ — множество начальных вершин графа G с отмеченными дугами или с отмеченными вершинами, $F \subseteq Q$ — множество финальных вершин. Отметки всех путей в графе G, начальные вершины которых принадлежат множеству I, а конечные — множеству F, назовем языком, допускаемым графом G, и обозначим $L(G)$.

Теорема 1. Язык $L \subseteq X^*$ допустим в графе с отмеченными дугами (вершинами) тогда и только тогда, когда он описывается регулярным выражением любой алгебры из семейства $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$.

Эта теорема в некотором смысле аналогична широко известной теореме Клини для конечных автоматов. В случае, когда $n = 0$ и рассматриваются только графы с отмеченными дугами, теорема 1 совпадает с теоремой Клини. На основе доказательства теоремы разработаны методы анализа и синтеза языков, представимых в отмеченных графах.

ЛИТЕРАТУРА

1. *Капитонова Ю. В., Летичевский А. А.* Математическая теория проектирования вычислительных систем. М.: Наука, 1988.
2. *Anderson J.* Automata Theory with Modern Applications. Cambridge: Cambridge University Press, 2006.

УДК 519.7

ГИПОТЕЗЫ О ЧИСЛЕ БЕНТ-ФУНКЦИЙ[1]

Н. Н. Токарева

Проблема определения числа всех *бент-функций* — булевых функций от четного числа переменных, максимально удаленных от множества аффинных функций, — яв-

[1]Исследование выполнено при поддержке РФФИ (проекты № 09-01-00528, 10-01-00424, 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0429).

ляется одной из фундаментальных в этой области. Известно, что разрыв между существующими нижней и верхней оценками этого числа огромен. В работе исследуется роль класса итеративных бент-функций в решении этой задачи и формулируется серия гипотез о числе бент-функций.

Бент-функция g от n переменных называется *итеративной бент-функцией*, если она получена из четырех бент-функций $f_0,\ f_1,\ f_2,\ f_3$ от $n-2$ переменных с помощью конструкции

$$g(00,x)=f_0(x),\ g(01,x)=f_1(x),\ g(10,x)=f_2(x),\ g(11,x)=f_3(x).$$

При этом необходимым и достаточным условием того, чтобы определенная таким образом булева функция g была бент-функцией, является выполнение равенства $\widetilde{f_0}+\widetilde{f_1}+\widetilde{f_2}+\widetilde{f_3}=1$, где $\widetilde{f}$ обозначает дуальную бент-функцию. Этот способ был предложен А. Канто и П. Шарпин в работе [1], см. также [2].

Пусть $\mathcal{B}_n$ и $\mathcal{BI}_n$ обозначают соответственно множество всех бент-функций и множество всех итеративных бент-функций от n переменных. В [2, 3] показано, что $|\mathcal{B}_{n+2}| \geqslant |\mathcal{BI}_{n+2}| \geqslant \sum\limits_{f'\in\mathcal{B}_n}\sum\limits_{f''\in\mathcal{B}_n} |\ (\mathcal{B}_n+f')\cap(\mathcal{B}_n+f'')\ |$. Продолжим начатое исследование.

Пусть X_n — множество всех булевых функций от n переменных, которые можно представить в виде суммы двух бент-функций, т. е.

$$X_n=\bigcup_{f\in\mathcal{B}_n}(\mathcal{B}_n+f).$$

Кратностью покрытия булевой функции h назовем число бент-функций f от n переменных, таких, что h принадлежит множеству $\mathcal{B}_n+f$. Обозначим кратность функции через $m(f)$. Несложно заметить, что $\sum\limits_{f\in X_n} m(f)=|\mathcal{B}_n|^2$.

Доказаны следующие утверждения.

Теорема 1. Справедливо $|\mathcal{BI}_{n+2}|=\sum\limits_{f\in X_n} m(f)^2$.

Теорема 2. Выполняется $|\mathcal{BI}_{n+2}|\geqslant|\mathcal{B}_n|^4/|X_n|$.

Таким образом, из задачи нахождения числа всех итеративных бент-функций от n переменных возникают следующие вопросы.

Открытые вопросы. Какие булевы функции от n переменных могут быть представлены в виде суммы двух бент-функций? Сколько различных таких представлений имеет булева функция? Как распределены числа $m(f)$?

Заметим, что поскольку степень каждой бент-функции от n переменных не выше $n/2$, то множество X_n также содержит только функции степени не выше $n/2$, т. е. $|X_n|\leqslant 2^{1+n+\binom{n}{2}+\ldots+\binom{n}{n/2}}=2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$. Проверено, что при $n=2,4,6$ множество X_n содержит *все* булевы функции степени не выше $n/2$. Сформулируем следующую сильную гипотезу.

Гипотеза 1. Каждая булева функция от n переменных степени не больше $n/2$ представима в виде суммы двух бент-функций от n переменных.

Если гипотеза 1 верна, то из нее практически сразу следует справедливость следующей гипотезы об асимптотике числа всех бент-функций.

Гипотеза 2. Число всех бент-функций от n переменных асимптотически равно $2^{2^{n-c}+d\binom{n}{n/2}}$, где c, d — некоторые константы, причем $1 \leqslant c \leqslant 2$.

Гипотеза 2 означает, что число всех бент-функций скорее ближе к тривиальной верхней оценке их числа (в грубом приближении 2^{2^n}), чем к нижней (около $2^{2^{(n/2)+\log(n-2)-1}}$).

С другой стороны, возникают гипотезы, отражающие роль множества итеративных бент-функций в классе всех бент-функций. Проверено, что при малых n, равных $2, 4, 6$, оценка теоремы 2 становится всё более точной.

Например, для последнего случая ($n = 6$) с привлечением методов Монте-Карло вычислено с малой погрешностью значение $|\mathcal{BI}_8|$, а именно показано, что с вероятностью 0,999 выполняется $2^{87{,}36} < |\mathcal{BI}_8| < 2^{87{,}38}$, тогда как по оценке теоремы 2 имеем $|\mathcal{BI}_8| > 197\,004\,891\,331\,091\,000\,000\,000\,000 \approx 2^{87{,}35}$.

Гипотеза 3. Оценка теоремы 2 асимптотически точна, т. е. справедливо

$$\lim_{n\to\infty} \frac{\log\log|\mathcal{BI}_{n+2}|}{\log\log(|\mathcal{B}_n|^4/|X_n|)} = 1.$$

Сформулируем также следующую гипотезу, смысл которой неформально сводится к тому, что «поведение» класса всех бент-функций определяется лишь итеративными бент-функциями.

Гипотеза 4. Класс $\mathcal{BI}_n$ является *базовым классом* в множестве $\mathcal{B}_n$, т. е. выполняется

$$\lim_{n\to\infty} \frac{\log\log|\mathcal{BI}_n|}{\log\log|\mathcal{B}_n|} = 1.$$

ЛИТЕРАТУРА

1. *Canteaut A. and Charpin P.* Decomposing Bent Functions // IEEE Trans. Inform. Theory. 2003. V. 49. P. 2004–2019.
2. *Токарева Н. Н.* Новая комбинаторная конструкция бент-функций // Прикладная дискретная математика. Приложение. 2010. № 3. С. 13–14.
3. *Tokareva N.* On the number of bent functions: lower bounds and hypotheses // Crypto Archive 2011, Report 083. `http://eprint.iacr.org/2011/083.pdf`.