Доклады Академии наук СССР
1972. Том 202, № 6

УДК 519.95 *КИБЕРНЕТИКА И ТЕОРИЯ РЕГУЛИРОВАНИЯ*

О. Б. ЛУПАНОВ

О СХЕМАХ ИЗ ПОРОГОВЫХ ЭЛЕМЕНТОВ

(Представлено академиком А. Н. Тихоновым 15 VII 1971)

Функция алгебры логики $f(x_1, \ldots, x_n)$ называется **пороговой**, если существуют вещественные числа $w_1, \ldots, w_n$, h такие, что $f(x_1, \ldots, x_n) = 1$ тогда и только тогда, когда

$$w_1x_1 + \ldots + w_nx_n \geqslant h. \tag{1}$$

Известно, что для любой пороговой функции можно подобрать целые $w_1, \ldots, w_n$, h в определяющем ее неравенстве (1). Функциональный элемент (см., например, [1]), реализующий пороговую функцию, называется **пороговым элементом**. **Схема из пороговых элементов** (с.п.э.) — это схема из функциональных элементов, все элементы которой реализуют пороговые функции. Обычно рассматриваются два определения сложности с.п.э.: $L(S)$ — число элементов в S и $L^0(S)$ — сумма модулей всех коэффициентов w_i всех элементов схемы (при условии, что пороговые функции задаются целочисленными неравенствами (1)). Пусть f — функция или система функций (вектор-функция); обозначим через $L(f)$ ($L(f/g)$) минимальное число элементов в с.п.э., реализующей f (минимальное число элементов в с.п.э., которую надо присоединить к выходам схемы для g, чтобы получить схему для f). Если $\mathfrak{F}$ — (конечное) множество (вектор-) функций, то через $L(\mathfrak{F})$ ($L(\mathfrak{F}/g)$) будем обозначать $\max\limits_{f\in\mathfrak{F}} L(f)$ ($\max\limits_{f\in\mathfrak{F}} L(f/g)$). Если $\mathfrak{F}$ — множество всех функций $f(x_1, \ldots, x_n)$ от n аргументов (всех систем $(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$, которые будем называть (n, m)-функциями), то вместо $L(\mathfrak{F})$ будем употреблять обозначение $L(n)$ ($L(n, m)$). Последние функции получили название функций Шеннона. Аналогично определяются функции $L^0(f)$, $L^0(\mathfrak{F})$, $L^0(n)$ и т. д.

Задачей о сложности с.п.э., реализующих произвольные функции алгебры логики, занимались многие авторы. Для $L^0(n)$ Е. Ю. Захарова [2] установила асимптотику $L^0(n) \sim 2^n/n$. Получение оценок функции $L(n)$ потребовало создания специфических методов. Э. И. Нечипорук [3] установил порядок функции $L(n)$, получив оценки

$$2(2^n/n)^{1/2} \leqslant L(n) \leqslant 2\sqrt{2}(2^n/n)^{1/2}. \tag{2}$$

В направлении получения асимптотики функции $L(n)$ Н. П. Редькиным [4] установлена асимптотика функции $L(\mathfrak{F})$ для некоторого специального класса функций и при некоторых ограничениях на схемы (схемы глубины 3).

Целью настоящей заметки является изложение идеи доказательства асимптотических формул для $L(n)$ и $L(n, m)$.

Теорема 1. *$L(n) \sim 2(2^n/n)^{1/2}$.*

Теорема 2. *Если $m = o(2^n)$, то* *

$$L(n, m) \sim 2\left(\frac{m\cdot 2^n}{n - \log m}\right)^{1/2} \quad **;$$

---

* Заметим, что $L(n, m) \leqslant 2^n + m$. Поэтому при m порядка 2^n и выше имеет место соотношение $L(n, m) \asymp m$.

** Здесь всюду имеются в виду логарифмы по основанию 2.

или в другой форме: *если* $m = 2^n / \varphi$, $\varphi \to \infty$, *то*

$$L(n, m) \sim 2^{n+1} / \sqrt{\varphi \log \varphi}.$$

Нижняя оценка для $L(n)$ доказана Э. И. Нечипоруком ([3]) (см. (2)). Нижняя оценка для $L(n, m)$ доказывается аналогично. Все дальнейшее относится к верхним оценкам.

Пусть $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — набор из нулей и единиц. Обозначим через $|\tilde{\alpha}|$ число $2^0\alpha_1 + 2^1\alpha_2 + \ldots + 2^{n-1}\alpha_n$. Функцию алгебры логики f будем называть квазимонотонной, если она удовлетворяет условию: если $|\tilde{\alpha}| < |\tilde{\beta}|$, то $f(\tilde{\alpha}) \leqslant f(\tilde{\beta})$. Каждая квазимонотонная функция f полностью определяется целым числом (порогом) λ, обладающим тем свойством, что $f(\tilde{\alpha}) = 1$ тогда и только тогда, когда $|\tilde{\alpha}| \geqslant \lambda$. Вектор-функцию будем называть квазимонотонной, если она состоит из квазимонотонных функций. Каждая квазимонотонная (n, m)-функция полностью определяется вектором $(\lambda_1, \ldots, \lambda_m)$, где λ_i — порог i-й функции.

Обозначим через A^a ($\hat{A}^a$) множество квазимонотонных $(a, 2^a)$-функций, векторы которых $(\lambda_1, \ldots, \lambda_{2^a})$ являются перестановками набора $(0, 1, \ldots \ldots, 2^a - 1)$ (набора $(1, 2, \ldots, 2^a)$). Обозначим через $A^{a, b}$ ($\hat{A}^{a, b}$) множество $(a + b, 2^a)$-функций $F(\tilde{x}, \tilde{y})$, удовлетворяющих условию (здесь $\tilde{x}$ имеет длину a, $\tilde{y}$ — длину b) : $F(\tilde{x}, \tilde{\beta}) \in A^a$ ($\in \hat{A}^a$).

Пусть K^b есть $(b, 2^b)$-функция, содержащая все элементарные конъюнкции $y_1^{\sigma_1} y_2^{\sigma_2} \ldots y_b^{\sigma_b}$. Очевидно, что $L(K^b) = 2^b$.

Лемма 1. $L(A^{a, b} / K^b) \leqslant 2^a$, $L(\hat{A}^{a, b} / K^b) \leqslant 2^a$.

Доказательство основано на использовании пороговых функций $F_{c_1, \ldots, c_{2^b}}(x_1, \ldots, x_a, u_1, \ldots, u_{2^b})$, определяемых неравенствами

$$2^0 x_1 + 2^1 x_2 + \ldots + 2^{a-1} x_a - c_1 u_1 - c_2 u_2 - \ldots - c_{2^b} u_{2^b} \geqslant 0.$$

Пусть E^a — множество наборов из нулей и единиц длины 2^a с одной единицей. Пусть $B^{a, b}$ — множество $(a + b, 2^a)$-функций $F(\tilde{x}, \tilde{y})$, удовлетворяющих условиям

$$F(\tilde{\alpha}, \tilde{\beta}) \in E^a; \tag{*}$$

$$\text{если} \quad \tilde{\alpha}_1 \neq \tilde{\alpha}_2, \quad \text{то} \quad F(\tilde{\alpha}_1, \tilde{\beta}) \neq F(\tilde{\alpha}_2, \tilde{\beta}). \tag{**}$$

Лемма 2. $L(B^{a, b} / K^b) \leqslant 3 \cdot 2^a$.

В самом деле, пусть $\varphi(u_1, u_2) = u_1 \bar{u}_2$. Каждая вектор-функция F из $B^{a, b}$ может быть представлена в виде $F = \varphi(F_1, F_2)$, где $F_1 \in A^{a, b}$, $F_2 \in \hat{A}^{a, b}$ (операция φ применяется в каждой компоненте).

Пусть $C^{a, b}$ — множество $(a + b, a)$-функций $F(\tilde{x}, \tilde{y})$, удовлетворяющих условию (**).

Лемма 3. $L(C^{a, b} / K^b) \leqslant 3 \cdot 2^a + a$.

(К схеме для F из $B^{a, b}$ следует присоединить схему, выдающую по набору с одной единицей двоичную запись номера разряда, в котором стоит эта единица; подробнее см. ([5]), стр. 57—59.)

Будем рассматривать $(2^a, a)$-матрицы (2^a строк, a столбцов) из нулей и единиц. Обозначим i-ю строку матрицы M через $\tilde{\mu}_i$. Определим следующие две операции над матрицами:

$M' + M''$ — поэлементное сложение по mod 2;

$M' \square M''$: $\tilde{\mu}_i = \tilde{\mu}_i'$ при $1 \leqslant i \leqslant 2^{a-1}$ и $\tilde{\mu}_i = \tilde{\mu}_i''$ при $2^{a-1} < i \leqslant 2^a$.

Будем называть $(2^a, a)$-матрицу перестановочной, если все ее строки попарно различны.

Лемма 4. *Для любой* $(2^a, a)$-*матрицы* M *найдутся четыре перестановочные* $(2^a, a)$-*матрицы* $M^{(1)}, M^{(2)}, M^{(3)}, M^{(4)}$ *такие, что*

$$M = (M^{(1)} + M^{(2)}) \square (M^{(3)} + M^{(4)}).$$

($\tilde{\mu}_1^{(1)}$ и $\tilde{\mu}_1^{(2)}$ — это любые два набора такие, что $\tilde{\mu}_1^{(1)} + \tilde{\mu}_1^{(2)} = \tilde{\mu}_1$; $\tilde{\mu}_2^{(1)}$ и $\tilde{\mu}_2^{(2)}$ — любые два набора такие, что, $\tilde{\mu}_2^{(1)} + \tilde{\mu}_2^{(2)} = \tilde{\mu}_2$, $\tilde{\mu}_2^{(1)} \neq \tilde{\mu}_1^{(1)}$, $\tilde{\mu}_2^{(2)} \neq \tilde{\mu}_1^{(2)}$ и т. д.).

Пусть $D^{a,b}$ — множество всех $(a+b, a)$-функций.

Лемма 5. $L(D^{a,b}/K^b) \leqslant 12\cdot 2^a + O(a)$.

Доказательство леммы опирается на леммы 4 и 3.

Пусть $D^{a,b,c}$ — множество всех $(a+b, 2^c)$-функций. Очевидно, что если $2^c \leqslant a$, то $L(D^{a,b,c}/K^b) \leqslant L(D^{a,b}/K^b)$.

Лемма 6. *Если* $m = 2^n/\varphi$, $\varphi \to \infty$, *то* $L(n, m) \preccurlyeq \dfrac{2^n}{\sqrt{\varphi \log \varphi}}$.

Приведем набросок доказательства этой леммы. Положим $c = [\log\log\varphi - 2]$, $a = [{}^1/_2(\log\varphi - \log\log\varphi)]$, $b = n - a - c$. Тогда (при достаточно больших n) $2^c \leqslant a$. Переменные произвольной (n, m)-функции $F = (f_1, \ldots, f_m)$ разобьем на три группы: $\tilde{x}$ — длины a, $\tilde{y}$ — длины b, $\tilde{z}$ — длины c. Схема для F состоит из подсхем $\mathfrak{R}_1$, $\mathfrak{R}_2$, $\mathfrak{F}$, $\mathfrak{V}$. Подсхемы $\mathfrak{R}_1$ и $\mathfrak{R}_2$ реализуют K^b и K^c соответственно; $L(\mathfrak{R}_1) = 2^b$, $L(\mathfrak{R}_2) = 2^c$. Пусть $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_{2^c}$ — все наборы длины c, занумерованные в естественном порядке. Пусть $F_i = (f_i(\tilde{x}, \tilde{y}, \tilde{\gamma}_1), \ldots, f_i(\tilde{x}, \tilde{y}, \tilde{\gamma}_{2^c}))$, это $(a+b, 2^c)$-функция. Подсхема $\mathfrak{F}$ реализует вектор-функции F_i $(1 \leqslant i \leqslant m)$; $L(\mathfrak{F}) \preccurlyeq m\cdot 2^a$ (лемма 5). Подсхема $\mathfrak{V}$ выбирает (для каждого i отдельно) тот разряд вектор-функции F_i, который соответствует значению $\tilde{z}$; $L(\mathfrak{V}) \preccurlyeq m\cdot 2^c$.

Из доказательства следует, что порядок функции Шеннона может быть получен на схемах ограниченной глубины. Можно показать, что для этой цели достаточно ограничиться с.п.э. глубины 4.

Определим операцию умножения (p, q)-функции $G(\tilde{x}) = (g_1(\tilde{x}), \ldots, g_q(\tilde{x}))$ на (q, r)-матрицу $M = \|\mu_{ij}\|$, $1 \leqslant i \leqslant q$, $1 \leqslant j \leqslant r$, следующим образом. Пусть $\tilde{\mu}_i = (\mu_{i1}, \ldots, \mu_{ir})$. Функция $F(\tilde{x}) = G(\tilde{x}) \times M$ есть (p, r)-функция, значение которой на произвольном наборе $\tilde{\alpha}$ определяется так:

$$|F(\tilde{\alpha})| = g_1(\tilde{\alpha})\,|\tilde{\mu}_1| + g_2(\tilde{\alpha})\,|\tilde{\mu}_2| + \ldots + g_q(\tilde{\alpha})\,|\tilde{\mu}_q| \pmod{2^r}.$$

Будем называть (q, r)-матрицу M монотонной, если $|\tilde{\mu}_1| \leqslant |\tilde{\mu}_2| \leqslant \ldots \leqslant |\tilde{\mu}_q|$.

Лемма 7. *Для любой (a, a)-функции F существуют $(a, 2^a)$-функция G из A^a и монотонная $(2^a, a)$-матрица M такие, что $F = G \times M$.*

(Сначала берется функция G' из A^a, определяемая вектором $(0, 1, \ldots, 2^a - 1)$, и матрица M' такая, что $F = G' \times M'$. Затем одновременной перестановкой компонент в G' и строк в M' матрица M' превращается в монотонную.)

Кодом монотонной $(2^a, a)$-матрицы M будем называть набор из нулей и единиц длины 2^{a+1}, имеющий 2^a нулей и 2^a единиц, такой, что число единиц, стоящих левее i-го нуля, равно $|\tilde{\mu}_i|$ (см. также ([5]), стр. 64—67).

Набросок доказательства верхней оценки теоремы 2. Пусть $F(f_1, \ldots, f_m)$ — произвольная (n, m)-функция. Набор значений (длины 2^n) каждой функции f_i разбивается на куски длины $a\cdot 2^a$, $a = [{}^1/_2\log\varphi - 4\log\log\varphi]$. Каждый такой кусок определяет некоторую (a, a)-функцию. Пусть F_{ij} — (a, a)-функция, соответствующая j-му куску функции f_i. Значение функции f_i на наборе $\tilde{\sigma}$ есть значение некоторого (h-го) разряда значения некоторой функции F_{ij} на некотором наборе $\tilde{\tau}$; h, j и $\tilde{\tau}$ определяются по $\tilde{\sigma}$ соотношением

$$(j-1)a\cdot 2^a + |\tilde{\tau}|a + h = |\tilde{\sigma}| + 1.$$

Каждая функция F_{ij} представляется в виде $F_{ij} = G_{ij} \times M_{ij}$, где G_{ij} — некоторая $(a, 2^a)$-функция из A^a, а M_{ij} — монотонная $(2^a, a)$-матрица (лемма 7).

Схема для F состоит из нескольких подсхем. Подсхема $\mathfrak{N}$ по $\tilde{\sigma}$ определяет $j-1$, $\tilde{\tau}$ и h. Основной подсхемой является подсхема $\mathfrak{G}$, реализующая некоторым специальным образом все функции G_{ij}. Она состоит из подсхем $\mathfrak{G}_i$ $(1 \leqslant i \leqslant m)$. Подсхема $\mathfrak{G}_i$ состоит из r ярусов $(r \sim \sqrt[4]{8\varphi}/2^{a/2}\sqrt[4]{a})$; l-й ярус состоит из l блоков $B_{il1}, \ldots, B_{ill}$. Блок B_{ilk} состоит из 2^a элементов, каждый из которых имеет входы трех типов:

1) a входов, аналогичных входам $x_1, \ldots, x_a$ элемента для $F_{c_1, \ldots; c_{2^b}}(x_1, \ldots, x_a, u_1, \ldots, u_{2^b})$; на них подается набор τ;

2) t_l «информационных» входов, аналогичных $u_1, \ldots, u_{2^b}$; t_l равно числу элементов во всех блоках всех предыдущих ярусов всех подсхем $\mathfrak{G}_i$, т. е. $t_l = l(l-1)m \cdot 2^{a-1}$; эти входы присоединены к выходам указанных элементов;

3) некоторого числа управляющих входов.

Каждый из блоков B_{ilk} может находиться в одном из двух состояний — активном и пассивном. В активном состоянии находится ровно один блок в каждой подсхеме $\mathfrak{G}_i$. Он реализует одну из функций G_{ij}. Находящиеся в пассивном состоянии блоки вырабатывают набор с одной единицей, подаваемый на информационные входы активного блока.

Дополнительная подсхема управления $\mathfrak{D}$ отправляет выработанный активным блоком набор в определенное место. Подсхема $\mathfrak{M}$ выдает по j коды монотонных матриц $M_{1j}, \ldots, M_{mj}$. Используя лемму 6, имеем $L(\mathfrak{M}) = o(2^n / \sqrt{\varphi \log \varphi})$. Подсхема $\mathfrak{N}$ по кодам монотонных $(2^a, a)$-матриц определяет все их элементы. При этом используется также некоторый аналог сети Ю. П. Офмана (6). Наконец, подсхема $\mathfrak{P}$ осуществляет умножение $G_{ij} \times M_{ij}$ и подсхема $\mathfrak{B}$ выделяет нужные разряды.

Сочетание теоремы 2 (метод синтеза) и принципа локального кодирования (5) позволяет почти механически получать асимптотически наилучшие (наилучшие по порядку) методы синтеза с.п.э. для известных классов функций, допускающих более простую схемную реализацию, чем большинство функций. При этом требуется лишь изменение значений параметров в обычных методах синтеза.

Институт прикладной математики
Академии наук СССР
Москва

Поступило
3 VI 1971

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] О. Б. Лупанов, Сборн. Проблемы кибернетики, в. 7, 61 (1962). [2] Е. Ю. Захарова, Сборн. Проблемы кибернетики, в. 9, 317 (1963). [3] Э. И. Нечипорук, Сборн. Проблемы кибернетики, в. 11, 49 (1964). [4] Н. П. Редькин, Кибернетика, № 5, 6 (1970). [5] О. Б. Лупанов, Сборн. Проблемы кибернетики, в. 14, 31 (1965). [6] Ю. П. Офман, Тр. Московск. матем. общ., 14, 186 (1965).