Доклады Академии наук СССР
1966. Том 169, № 4

УДК 519.95

МАТЕМАТИКА

Э. И. НЕЧИПОРУК

ОБ ОДНОЙ БУЛЕВСКОЙ ФУНКЦИИ

(Представлено академиком П. С. Новиковым 26 III 1965)

Известно ([1-3]), что при $n \to \infty$ почти все булевские функции от n аргументов допускают лишь реализации, сложность которых выше чем $\exp Cn$, где C — некоторая константа. Однако лишь для очень немногих явно задаваемых функций f удается показать, что их сложность $L(f)$ имеет порядок выше линейного. Все эти примеры ([4-7]) связаны с некоторыми ограничениями на базис. До настоящего времени ни для одной функции не было доказано, что она допускает только «нелинейные» реализации в классе суперпозиций над произвольным базисом или в классе произвольных контактных схем. Ниже построен пример функции, заполняющий этот пробел.

1°. Пусть $m = [\log n] + 2$*, $\tilde{x} = \{\tilde{x}_i\}_1^{[n/m]}$, $\tilde{x}_i = \{x_{i,j}\}_1^m$ при $1 \leqslant i \leqslant [n/m]$, $x_{i,j}$ — попарно различные булевские аргументы. Через $\|\tilde{\sigma}\|$ обозначаем число единиц в булевском векторе $\tilde{\sigma}$. Пусть $\tilde{\sigma}_{i,j}$ — попарно различные булевские векторы размерности m такие, что $\|\tilde{\sigma}_{i,j}\| > 1$. Через $K^+_{\tilde{\sigma}_{i,j}}(\tilde{x}_k)$ обозначаем конъюнкцию без инверсий всех аргументов из $\tilde{x}_k$, соответствующих единичным компонентам вектора $\tilde{\sigma}_{i,j}$. Положим при $1 \leqslant i, k \leqslant [n/m]$, $1 \leqslant j \leqslant m$ **

$$f_n(\tilde{x}) = \sum_{i,j} x_{ij} \sum_{\substack{k \\ (k \neq i)}} K^+_{\tilde{\sigma}_{i,j}}(\tilde{x}_k).$$

Лемма. *При всяком i все функции, получающиеся из функции $f_n(\tilde{x})$ замещением всех аргументов из $\tilde{x} \setminus \tilde{x}_i$ произвольными булевскими константами, различны.*

Доказательство следует из единственности получающихся полиномов Жегалкина.

2°. Теорема 1. *Для суперпозиций над всяким конечным невырожденным базисом ([3]) справедлива оценка*

$$L(f_n) \geqslant n^2 / \log n.$$

Доказательство. Пусть $\mathfrak{A}$ — суперпозиция, на которой достигается $L(f_n)$; h — число ее ребер, по которым подаются аргументы. Тогда существует константа C, зависящая только от базиса, такая, что $L(f_n) \geqslant Ch$. Выберем число i_0 такое, что $h \geqslant [n/m] h_0$, где h_0 — число ребер, по которым подаются аргументы из $\tilde{x}_{i_0}$.

Выделим в $\mathfrak{A}$ две непересекающиеся группы элементов: в 1-ю группу отнесем все элементы ***, на каждый вход каждого из которых подается

---

* Логарифмы берутся по основанию 2.

** Символ $\sum$ обозначает сложение по mod2.

*** В частности, элементы без выходов.

аргумент из $\tilde{x} \setminus \tilde{x}_{i_0}$ или выход элемента 1-й группы; во 2-ю группу отнесем все элементы, в каждом из которых на один вход подается аргумент из $\tilde{x}_{i_0}$ или выход элемента 2-й группы, а на каждый из остальных входов подается аргумент из $\tilde{x} \setminus \tilde{x}_{i_0}$ или выход элемента 1-й группы. Элементы 2-й группы образуют непересекающиеся цепочки. Оборвем в $\mathfrak{A}$ все аргументы из $\tilde{x} \setminus x_{i_0}$ и все элементы 1-й группы; образующиеся при этом входы назовем свободными. После этого каждую цепочку элементов 2-й группы * заменим одним элементом с тремя входами, реализующим функцию $x\varphi + \psi$ (рис. 1). Аргумент x здесь тот же, что и в цепочке, а входам φ, ψ (их также назовем свободными) соответствуют функции $\varphi(\tilde{x} \setminus \tilde{x}_{i_0})$, $\psi(\tilde{x} \setminus \tilde{x}_{i_0})$, вырабатываемые свободными входами в цепочке. Полученную суперпозицию обозначим через $\mathfrak{A}_0$.

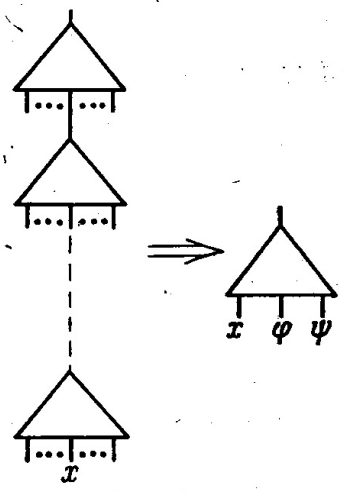

Рис. 1

Каждая функция, получающаяся из функции $f_n(\tilde{x})$ замещением всех аргументов из $\tilde{x} \setminus \tilde{x}_{i_0}$ константами, определяется расстановкой некоторых булевских констант на свободных входах суперпозиции $\mathfrak{A}_0$. В силу леммы число этих функций равно $2^{m[n/m]-m}$, поэтому общее число свободных входов не меньше чем $m[n/m] - m$.

Элемент суперпозиции $\mathfrak{A}_0$ назовем концевым, если по крайней мере на один его вход подается аргумент. Так как в $\mathfrak{A}_0$ нет элементов 1-й и 2-й групп, то, в силу хотомии (цепочки из концевых элементов в счет не идут) доля концевых элементов не меньше чем $1/2$. Поэтому существует константа C, зависящая только от базиса, такая, что число свободных входов не больше чем h_0/C.

Окончательно

$$L(f_n) \geqslant C^2[n/m](m[n/m] - m) \asymp n^2/\log n.$$

3°. Теорема 2. *Для контактных схем справедлива оценка*

$$L(f_n) \gtrsim (n/\log n)^2.$$

Доказательство. Выберем число i_0 такое, что $L(f_n) \geqslant [n/m]h_0$, где h_0 — число контактов из $\tilde{x}_{i_0}$. Каждая функция, получающаяся из функции $f_n(\tilde{x})$ замещением всех аргументов из $\tilde{x} \setminus \tilde{x}_{i_0}$ константами, определяется схемой, состоящей из h_0 контактов. Поэтому, по лемме настоящей работы и лемме 13 из [2]

$$2^{m[n/m]-m} \leqslant (30h_0)^{h_0}(2m)^{h_0},$$

в силу чего

$$h_0 \gtrsim n/\log n,$$

откуда следует утверждение теоремы.

Ленинградский государственный университет
им. А. А. Жданова

Поступило
23 III 1965

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] C. E. Shannon, Bell Syst. Techn. J., 28, 1, 59 (1949). [2] О. Б. Лупанов, Сборн. Проблемы кибернетики, в. 10, М., 1963, стр. 63. [3] Э. И. Нечипорук, Сборн. Проблемы кибернетики, в. 14, «Наука», 1965, стр. 111. [4] Б. А. Субботовская, ДАН, 136, № 3, 553 (1961). [5] А. А. Марков, Сборн. Проблемы кибернетики, в. 8, М., 1962, стр. 117. [6] G. Hansel, C. R., 258, 25, 6037 (1964). [7] Р. Е. Кричевский, Сборн. Проблемы кибернетики, в. 12, «Наука», стр. 45.

* В частности, один элемент.