MATHEMATICAL PROBLEMS IN COMPUTATION THEORY
BANACH CENTER PUBLICATIONS, VOLUME 21
PWN — POLISH SCIENTIFIC PUBLISHERS
WARSAW 1988

О ГЛУБИНЕ БУЛЕВЫХ ФУНКЦИЙ, РЕАЛИЗУЕМЫХ КОНТАКТНЫМИ СХЕМАМИ ЗАДАННОЙ СЛОЖНОСТИ

Н. Н. КУЗЮРИН

Институт Проблем Кибернетики, Москва, СССР

В статье изучается соотношение между сложностью реализации булевых функций и их глубиной. Все используемые и неопределяемые здесь понятия из теории контактных схем и схем из функциональных элементов (сокращенно с.ф.э.) можно найти в работе [2]. *Глубиной схемы из функциональных элементов* будем называть максимальную длину цепи от входов схемы к ее выходам. *Глубиной булевой функции* f (обозначение $D(f)$) называется минимальная из глубин с.ф.э., реализующих булеву функцию f. В работе [4] (см. также [5]) для полного базиса установлено, что если булева функция f реализуется формулой сложности $L(f)$, то выполнено неравенство

$$D(f) \leqslant c \cdot \log L(f).$$

Значение константы c для базиса $\{\&, \vee, \neg\}$ последовательно понижалось рядом авторов (см. [1], [3]). Наилучшая оценка получена в работе [5], где доказано, что $c \leqslant 1.73$. С другой стороны, известно, что если булева функция f реализуется в классе с.ф.э. со сложностью $L(f)$, то справедливо неравенство

$$D(f) \leqslant L(f)/\log L(f).$$

Весьма интересным является вопрос: верно ли, что для всякой булевой функции, имеющей сложность реализации в классе с.ф.э. $L(f)$ справедливо неравенство:

$$D(f) \leqslant P(\log L(f)), \tag{1}$$

где $P(x)$ — некоторый полином.

В настоящей работе на основе весьма простых соображений устанавливается справедливость (1) для функций, допускающих реализацию контактными схемами заданной сложности. Более точно, доказано следующее утверждение.

Теорема. *Для всякой последовательности булевых функций f_n, имеющей сложность реализации контактными схемами $L(f_n)$, выполнено неравенство*:

$$D(f_n) \lesssim \log^2 L(f_n), \tag{2}$$

причем с.ф.э., реализующая f_n с глубиной (2), *имеет сложность по порядку не превосходящую $L^4(f_n)$.*

Приведем схему доказательства теоремы. Контактная схема является мультиграфом с двумя выделенными вершинами, называемыми полюсами схемы (обозначим их соответственно p и q) причем каждому ребру приписан один символ из множества $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$. Всякому пути из p в q сопоставляется конъюнкция переменных, приписанных ребрам этого пути. Контактная схема реализует булеву функцию, равную дизъюнкции конъюнкций, сопоставленных всем путям контактной схемы ведущим из полюса p в полюс q.

Каждой контактной схеме с m вершинами сопоставим матрицу A размера $m \times m$, в которой a_{ij} есть дизъюнкция символов, приписанных ребрам (i, j), если эти ребра есть в схеме, либо нуль — в противном случае. Пусть $L(f_n)$ — число ребер контактной схемы, реализующей f_n, $Z = A \cdot B$ обозначает булевское произведение матриц A и B, причем $z_{ij} = \bigvee_{k=1}^{m} a_{ik} \cdot b_{kj}$. Через $(A)_{pq}$ обозначим элемент матрицы A, стоящий на пересечении p-й строки и q-го столбца.

Доказательство основано на следующем представлении функции f:

$$f = (A \vee A^2 \vee \ldots \vee A^{L(f)})_{pq}. \tag{3}$$

Из свойств булевского произведения матриц вытекает, что $(A^t)_{pq} = 1$ тогда и только тогда, когда в контактной схеме из полюса p в полюс q существует простой путь длины t, всем ребрам которого приписаны значения равные единице (на фиксированном наборе значений переменных). В справедливости (3) нетрудно убедиться непосредственной проверкой: если функция проводимости контактной схемы на некотором наборе значений переменных равна единице, то это означает, что существует путь из p в q целиком состоящий из ребер с приписанными значениями равными единице. Длина этого пути, очевидно, не превосходит $L(f)$. Пусть она равна t. Тогда элемент $(A^t)_{pq}$ равен единице (по определению булевского произведения). Если же значение проводимости на заданном наборе равно нулю, то не существует пути из p в q, целиком состоящего из ребер с приписанными единичными значениями. Поэтому все элементы $(A)_{pq}, (A^2)_{pq}, \ldots, (A^{L(f)})_{pq}$ равны нулю.

Покажем теперь, как на основе представления (3) построить с.ф.э. для f, имеющую глубину $O(\log^2 L(f))$ и сложность $O(L^4(f))$. Одним блоком $P(A, B)$ будем обозначать с.ф.э. для булева умножения матриц A

и B размера $m \times m$, имеющую m^2 входов и m^2 выходов, глубину $O(\log m)$ и сложность $O(m^3)$. Эта схема является реализацией метода сдваивания переменных: сначала каждый элемент a_{ij} матрицы A умножается покомпонентно на j-ю строку матрицы B. Далее независимо реализуются m^2 дизъюнкций по m переменных. Дизъюнкцию m переменных очевидным образом можно выполнить формулой глубины $O(\log m)$ и сложности $O(m)$: на первом ярусе берутся дизъюнкции независимых пар переменных, на втором ярусе то же самое проделывается с результатами, полученными на первом ярусе и т.д.

Пусть $L(f)$ представлено в виде: $L(f) = 2^{t-1} + j_0$, $0 \leqslant j_0 < 2^{t-1}$. Построим требуемую с.ф.э. для f из блоков $P(A, B)$. Сначала вычисляем значение элементов матрицы A (Глубина 1). На первом ярусе вычисляем

$$A^2 = P(A, A).$$

На $(k+1)$-м ярусе вычисляем следующие матрицы:

$$A^{2^k+1} = P(A^{2^k}, A),\ A^{2^k+2} = P(A^{2^k}, A^2), \ldots, A^{2^{k+1}} = P(A^{2^k}, A^{2^k});$$

. . . .

На t-м ярусе вычисляем следующие матрицы:

$$A^{2^{t-1}+1} = P(A^{2^{t-1}}, A), \ldots, A^{L(f)} = P(A^{2^{t-1}}, A^{j_0}).$$

В заключение нужно взять поэлементную дизъюнкцию всех полученных матриц $A, A^2, \ldots, A^{L(f)}$. Это можно сделать с.ф.э. глубины $O(\log L(f))$ и сложности $O(m^2 \cdot L(f))$.

Оценим теперь глубину и сложность построенной с.ф.э. В схеме имеется не более $]\log L(f)[$ ярусов, состоящих из блоков вида $P(A, B)$. Каждый такой блок имеет глубину $O(\log m)$. Поэтому глубина всей схемы не превосходит по порядку $O(\log^2 L(f))$. Заметим также, что на первом ярусе имеется один блок умножения матриц, на втором — 2, на третьем — 4, и.т.д. На последнем ярусе имееется не более $]\frac{1}{2}L(f)[$ блоков умножения матриц. Таким образом, общее число блоков умножения матриц по порядку не превосходит

$$1+2+4+\ldots+]\tfrac{1}{4}L(f)[+]\tfrac{1}{2}L(f)[\leqslant L(f).$$

Поскольку каждый блок имеет сложность по порядку равную m^3, то сложность всей схемы по порядку не превосходит величины $O(L^4(f))$. Отметим, что оценку $O(L^4(f))$ на сложность схемы можно понизить, если в качестве блоков использовать быстрые алгоритмы для булевского произведения матриц, преобразованные в с.ф.э. глубины $O(\log m)$. Теорема доказана.

Будем говорить, что контактные схемы *полиномиально моделируют* схемы из функциональных элементов, если существует полином $P(x)$ такой, что для любой булевой функции f выполнено неравенство:

$$L_k(f) \leqslant P(L_{\text{с.ф.э.}}(f)),$$

где $L_k(f)$ и $L_{\text{с.ф.э.}}(f)$ обозначают соответственно сложность реализации f в классе контактных схем и в классе схем из функциональных элементов.

В связи с вопросом (1) интерес представляет следующее следствие из теоремы.

Следствие. *Либо контактные схемы не моделируют полиномиально схемы из функциональных элементов, либо существует полином $Q(x)$ такой, что любая с.ф.э. сложности $L(f)$ может быть преобразована в эквивалентную с.ф.э. глубины не более $Q(\log L(f))$.*

Литература

[1] A. Barak, E. Shamir, *On the parallel evaluation of boolean expressions*, SIAM J. Computers 4 (1976), 678–681.

[2] О. Б. Лупанов, *О синтезе некоторых классов управляющих систем*, Проблемы кибернетики вып. 10, М., Физматгиз (1963), 63–98.

[3] F. P. Preparata, D. E. Muller, *Efficient parallel evaluation of boolean expressions*, IEEE Trans. Computers 25(5) (1976), 548–549.

[4] P. M. Spira, *On time-hardware complexity tradeoffs for boolean functions*, Proceedings of Fourth Hawaii International Symposium on System Sciences (1971), 525–527.

[5] В. М. Храпченко, *О соотношении между сложностью и глубиной формул*, Сб. *Методы дискретного анализа в синтезе управляющих систем*, Новосибирск 1978, 32, 76–94.

Presented to the semester
Mathematical Problems in Computation Theory
September 16–December 14, 1985