Дискретная математика. Модуль 3. Лекция 1

Лекторий ПМИ ФКН 2015-2016
Бубнова Валерия
Жижин Пётр
Пузырев Дмитрий

18 января 2016

1 Размер схемы. Сложность булевой функции. Верхние и нижние оценки сложности

Размер схемы. Сложность булевой функции

Размер булевой схемы — это количество присваиваний в схеме $g_1, \ldots, g_L$ для вычисления функции $f : \{0,1\}^n \to \{0,1\}$.

Сложность функции f в базисе B — это минимальный размер булевой схемы, вычисляющей функцию f в базисе B. Если базис не указывают – имеют в виду стандартный базис $\{\neg, \vee, \wedge\}$. *Обозначение:* $C(f)$.

Утверждение: Если B – конечный базис, тогда $\exists c : \forall f$ если f вычисляется схемой S в B размера L, тогда существует схема в стандартном базисе размера меньше, чем $c \cdot L$, вычисляющая ту же функцию f.

Доказательство. Пусть f вычисляется схемой S в базисе B путём следующих присваиваний:

$$g_1, \ldots, g_k, \ldots, g_L = f$$

Рассмотрим некоторую g_k как функцию в базисе B от каких-то аргументов.

$$g_k = g(\ldots), g \in B$$

Для этой функции есть некоторая схема в стандартном базисе некоторого размера L'_k (так как в стандартном базисе любая функция вычислима, в том числе и g).

Каждую g_i заменим на соответствующую схему в стандартном базисе размера L'_i. Тогда и вся функция вычислима в стандартном базисе схемой размера:

$$L' = L'_1 + L'_2 + L'_3 + \ldots + L'_L \leqslant L \cdot max(L'_1, L'_2, \ldots L'_L) = L \cdot c_f$$

Для того чтобы теперь подобрать константу c в определении опять возьмем наибольшее из всех c_f. **Q.E.D.**

Верхняя оценка схемной сложности

Теорема. $C(f) = O(n \cdot 2^n)$

Доказательство. Повторим предыдущие рассуждения при доказательстве того, что в стандартном базисе любая функция вычислима. Для этого вспомним:

$$f(x) = \bigvee_{\substack{a : f(a)=1 \\ a \in \{0,1\}^n}} x^a, \; x^a = \bigwedge_{i=1}^{n} x_i^{a_i}$$

Нетрудно посчитать, что схема для вычисления x^a имеет размер $L_a = O(n)$. Тогда итоговый размер схемы $L \leqslant 2^n \cdot O(n) \iff L = O(n \cdot 2^n)$. **Q.E.D.**

Теорема. $C(f) = O(\frac{2^n}{n})$

Доказательство. В доказательстве много возни, желающие могут найти и прочитать. Идея в том, что многие схемы можно повторять примерно n^2 раз. **Q.E.D.**

Нижняя оценка схемной сложности

Теорема. *Существует функция* $f : \{0,1\}^n \to \{0,1\}$ *такая, что* $C(f) \geqslant \frac{2^n}{10n}$ *(в точности то же самое, что* $C(f) = \Omega(\frac{2^n}{n})$*).*

Доказательство. Воспользуемся мощностным методом. Всего булевых функций от n аргументов 2^{2^n}.

Теперь узнаем, сколько булевых схем размера меньше либо равных некоторого фиксированного числа L. Для этого будем кодировать схемы двоичными словами. Посмотрим на какое-то присваивание в схеме S: $g_k = g(g_i, g_j)$. Для кодирования самой функции g нужно 2 бита (так как в стандартном базисе всего три функции). Для кодирования номеров аргументов i и j нужно битов не более, чем $log_2 L$. А значит для всего присваивания g_k нужно не более $2 \cdot (1 + log_2 L)$ бит.

Итого размер одной схемы в битах: $L \cdot 2 \cdot (1 + log_2 L)$. Каждая схема кодирует ровно одну функцию. А значит каждое двоичное слово кодирует не более одной функции (так как некоторые двоичные слова ни одну схему не задают).

Получается и схем размера L не более, чем двоичных слов для схем такой длины, то есть: $2^{2L(1+log_2 L)}$.

Возьмем $L = \frac{2^n}{10n}$. Размер схемы в битах тогда будет равен:

$$L_2 = \frac{2^n}{10n} \cdot 2 \cdot \left(1 + log_2\left(\frac{2^n}{10n}\right)\right) = \frac{2^n}{5n}\left(1 + n - log_2(10n)\right), 1 - log(10n) \leqslant 0 \implies L_2 \leqslant \frac{2^n}{5n} \cdot n = \frac{2^n}{5}$$

А значит функций, задающейся схемой такой длины не более чем $2^{\frac{2^n}{5}}$. Нетрудно заметить, что это число значительно меньше числа функций от n аргументов.

$$2^{\frac{2^n}{5}} < 2^{2^n}$$

А значит существует функция, задающаяся схемой длины больше, чем L. **Q.E.D.**

Всё очень хорошо, но можно ли задать такую функцию явно? К сожалению, с этим есть некоторые проблемы. В 1984 году нашли f такую, что $C(f) \geqslant 3n$. Прорывом 2015 стала функция f такая, что $C(f) \geqslant \left(3 + \frac{1}{86}\right) n$.

Схемы для сложения и умножения двоичных чисел. Схема для проверки графа на связность