Теория дискретных функций

2015/16 уч. год, 2-й семестр

1-й курс, I поток

10 апреля 2016 г.

Лектор — проф. Р. М. Колпаков

Конспект лекции № 7 (24/03/16, проф. В. В. Кочергин)

Сложность булевых функций

Нижние оценки сложности булевых функций

На прошлой лекции мы двумя способами (методом Шеннона и методом каскадов) установили следующую верхнюю оценку функции Шеннона сложности реализации булевых функций от n переменных в базисе $B_0 = \{x \vee y,\, x\&y,\, \overline{x}\}$:

$$L(n) \lesssim 6\,\frac{2^n}{n}.$$

Насколько хороша эта оценка? Чтобы ответить на этот вопрос, нужно получить как можно более высокую нижнюю оценку функции Шеннона $L(n)$. А пока мы имеем только оценку $L(n) \geq n - 1$, так как любая функция от n переменных, существенно зависящая от n переменных, требует для своей реализации в базисе B_0 не менее $n - 1$ двухвходового элемента. Чуть усилим эту оценку функции Шеннона. Заметим, что любая немонотонная функция от n переменных, существенно зависящая от n переменных (например, функция $\overline{x_1 \vee \ldots \vee x_n}$), требует для своей реализации в базисе B_0 не менее $n - 1$ двухвходового элемента и, как

минимум, один инвертор (элемент, реализующий отрицание). Поэтому справедливо следующее утверждение.

Лемма 1. *Для любого натурального n справедливо неравенство*

$$L(n) \geq n.$$

Оценку из леммы 1, конечно, можно усилить. Однако, для конструктивно (явным образом) задаваемых последовательностей булевых функций известны лишь не более чем линейные по числу переменных нижние оценки сложности.

Тем не менее, можно доказать, что верхняя оценка функции Шеннона $L(n)$, доказываемая методом Шеннона или методом каскадов, неулучшаема по порядку роста величины, а для этого нужно установить экспоненциальную нижнюю оценку функции Шеннона. Эта оценка будет неконструктивная и будет получаться из мощностных соображений, идею которых проиллюстрируем на примере одной задачи из теории чисел.

Как доказать, что есть трансцендентные действительные числа (не являющиеся корнями ненулевых многочленов с рациональными коэффициентами)? Да, можно доказать, что $e, \pi, \sin 1, 2^{\sqrt{2}}, \log 3$ трансцендентны. Однако эти доказательства отнюдь не просты. В то же время элементарные мощностные рассуждения — множество действительных чисел континуально, а множество корней ненулевых многочленов с рациональными коэффициентами счетно — дают не только простейшее (правда, некоструктивное) доказательство этого факта, но и устанавливают, что почти все действительные числа трансцендентны.

Аналогичные рассуждения лежат и в основе экспоненциальной нижней оценки функции Шеннона. Сформулируем соответствующий очевидный факт в виде леммы, но сначала напомним определение минимальной схемы.

Схема, реализующая некоторую булеву функцию (или систему функций) в базисе B, называется *минимальной схемой в базисе B*, если никакая схема в базисе B меньшей сложности не реализует ту же самую функцию (систему функций).

Лемма 2. *Если число различных минимальных в базисе B схем S с n входами и одним выходом, удовлетворяющих условию $L_B(S) \leq k$, меньше величины 2^{2^n}, то выполняется неравенство*

$$L_B(n) > k.$$

Это утверждение непосредственно следует из того, что в условиях леммы число булевых функций $f(x_1, \ldots, x_n)$, удовлетворяющих условию

$L_B(f) \le k$, меньше величины 2^{2^n} — числа всех булевых функций от n переменных.

Таким образом, при доказательстве нижней оценки сложности функции Шеннона на первый план выходит задача о получении приемлемых верхних оценок числа минимальных схем, к которой мы и переходим.

Для того, чтобы оценить (сверху) количество минимальных схем оценим количество схем в более широком классе — в классе так называемых приведенных (или правильных) схем.

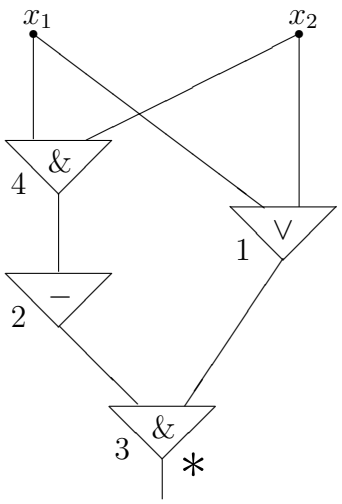
Схему будем называть *приведенной* (*правильной*), если в ней нет двух разных элементов, реализующих одну и ту же функцию. Очевидно, что из любой схемы путем удаления некоторых элементов и «переподключения» выходящих из этих элементов ребер можно получить приведенную схему. Поэтому справедливо такое утверждение.

Лемма 3. *Любая минимальная схема является приведенной.*

Обозначим через $N_=(k,n)$ число приведенных схем в базисе $B_0 = \{x \vee y,\, x\&y,\, \overline{x}\}$ со входами, которым приписаны переменные $x_1, \ldots, x_n$, и одним выходом, имеющих сложность в точности k, а через $N_\le(k,n)$ — число приведенных схем в базисе B_0 со входами, которым приписаны переменные $x_1, \ldots, x_n$, и одним выходом, имеющих сложность не более k.

Пусть S — приведенная схема в базисе B_0 сложности k со входами $x_1, \ldots, x_n$ и одним выходом. Занумеруем в произвольном порядке числами $1, 2, \ldots, k$ элементы схемы S. Обозначим эту нумерацию NUM. Схеме S с выбранной нумерацией элементов NUM сопоставим таблицу $T(S, NUM)$ высоты k и ширины 3 следующим образом. Пусть элемент E схемы S получил номер i. Тогда в i-й строке таблицы $T(S, NUM)$ в первом столбце указывается функция из базиса B_0, приписанная элементу E, а в других столбцах этой строки — символы из множества $\{x_1, \ldots, x_n\} \cup \{1, \ldots, k\}$: в $(j+1)$-й столбец, $j = 1, 2$, этой строки помещается информация о том, из какой вершины ведет ребро, соответствующее j-му входу элемента E (считаем, что входы элементов пронумерованы). Если ребро ведет из входа, помеченного переменной x_i, то в соответствующую клетку помещается символ x_i, а если ребро ведет из элемента с номером k, то — число k. Если у элемента E не два входа, а один (т. е. элемент E — инвертор), то оставшуюся пустой третью клетку i-й строки заполним для определенности так же, как и вторую клетку этой строки. Кроме того, если элемент E является выходом схемы, то i-я строка помечается дополнительно символом $*$ (если выходом является переменная, то помечается эта переменная).

На рис. 1 представлена схема, все элементы которой занумерованы



∨	x_1	x_2
−	4	4
&	2	1
&	x_1	x_2

*

Рис. 1:

в некотором порядке, а также таблица, соответствующая этой схеме с заданной нумерацией элементов.

Лемма 4. *Пусть S — приведенная схема в базисе B_0, а NUM_1 и NUM_2 — две отличные друг от друга нумерации элементов схемы S. Тогда*

$$T(S, NUM_1) \neq T(S, NUM_2).$$

Доказательство. Предположим противное, т. е. $NUM_1 \neq NUM_2$, но при этом $T(S, NUM_1) = T(S, NUM_2)$. Рассмотрим для схемы S еще одну нумерацию ее элементов — монотонную (правильную) нумерацию NUM_0. Нумерация NUM_0 обладает следующим свойством: для любого i, $1 \leq i \leq L(S)$, на каждый вход i-го относительно нумерации NUM_0 элемента подается либо переменная, либо выход элемента с номером (относительно нумерации NUM_0), меньшим i.

Среди всех элементов схемы S, которые имеют разные номера в нумерациях NUM_1 и NUM_2, выделим тот элемент E, который имеет наименьший номер относительно нумерации NUM_0. Пусть элемент E в нумерации NUM_1 имеет номер p, а в нумерации NUM_2 — номер q, $q \neq p$.

В силу выбора элемента E элементы, которые соединены ребрами со входами элемента E (если такие элементы есть), имеют одни и те же номера относительно нумераций NUM_1 и NUM_2, поэтому строка с номером p таблицы $T(S, NUM_1)$ и строка с номером q таблицы $T(S, NUM_2)$ заполнены идентично. Но по предположению, справедливо равенство $T(S, NUM_1) = T(S, NUM_2)$, а значит, строки с номерами p и q таблицы $T(S, NUM_1)$ (а также таблицы $T(S, NUM_2)$) совпадают. Отсюда

непосредственно следует, что в схеме S есть два элемента, вычисляющие одну и ту же функцию, что противоречит неприводимости схемы S. $\square$

Лемма 5. *Найдется $c > 0$, такое что при всех значениях k и n при выполнении условия $k \geq n$ справедливо неравенство*

$$N_{\leq}(k, n) \leq c^k k^k.$$

Доказательство. Оценим сверху число таблиц, которые соответствуют всевозможным нумерациям элементов всех приведенных схем со входами $x_1, \ldots, x_n$ и одним выходом сложности k. Каждую клетку первого столбца можно заполнить не более чем тремя способами, каждую клетку второго и третьего столбцов таблицы — не более чем $k+n$ способами. Кроме того, выбор места для пометки $*$ осуществляется $k+n$ способами. Поэтому всего таких таблиц не более $3^k(k+n)^{2k}(k+n)$ штук. Каждой приведенной схеме сложности k в силу леммы 4 соответствует $k!$ различных таблиц. Следовательно,

$$N_{=}(k, n) \leq \frac{3^k(k+n)^{2k}(k+n)}{k!}.$$

Используя условие $k \geq n$, соотношение $k! \geq (k/3)^k$ и неравенство $2k \leq 2^k$, получаем:

$$N_{=}(k, n) \leq \frac{3^k(2k)^{2k}(2k)}{\left(\frac{k}{3}\right)^k} \leq 72^k k^k.$$

Из последней оценки легко получается верхняя оценка величины $N_{\leq}(k, n)$:

$$N_{\leq}(k, n) = \sum_{l=0}^{\lfloor k \rfloor} N_{=}(l, n) \leq \sum_{l=0}^{\lfloor k \rfloor} 72^l l^l \leq 72^k k^k \left(1 + \frac{1}{2} + \ldots + \frac{1}{2^{\lfloor k \rfloor}}\right) \leq 144^k k^k.$$

$\square$

Теорема 1 (мощностная нижняя оценка)**.** *Для любого $\varepsilon > 0$ доля булевых функций f от n фиксированных переменных, удовлетворяющих условию*

$$L(f) \geq (1 - \varepsilon)\frac{2^n}{n},$$

стремится к 1 при $n \to \infty$.

Доказательство. Положим

$$k_\varepsilon = (1 - \varepsilon)\frac{2^n}{n}.$$

Число функций f от n фиксированных переменных, удовлетворяющих условию $L(f) \leq k_\varepsilon$, не превосходит величины $N_{\leq}(k_\varepsilon, n)$. Поэтому достаточно установить, что при $n \to \infty$

$$\frac{N_{\leq}(k_\varepsilon, n)}{2^{2^n}} \to 0$$

или, что то же самое,

$$\log_2 \frac{N_{\leq}(k_\varepsilon, n)}{2^{2^n}} \to -\infty.$$

Действительно, применяя лемму 5, имеем:

$$\log_2 \frac{N_{\leq}(k_\varepsilon, n)}{2^{2^n}} \leq k_\varepsilon \log_2 c + k_\varepsilon \log_2 k_\varepsilon - 2^n \leq$$
$$\leq (1-\varepsilon)\frac{2^n}{n}\log_2 c + (1-\varepsilon)\frac{2^n}{n}\log_2 (2^n) - 2^n = -\varepsilon 2^n + O\left(\frac{2^n}{n}\right).$$

Последнее выражение стремится к $-\infty$ при $n \to \infty$. □

Следствие 1. *При $n \to \infty$ выполняется асимптотическое неравенство*

$$L(n) \gtrsim \frac{2^n}{n}.$$

Теорема 1 вместе с верхними оценками, полученными методом Шеннона и методом каскадов, устанавливает порядок роста функции Шеннона $L(n)$.

Теперь тем же самым способом на основе леммы 5 с некоторым увеличением технических выкладок усилим доказанную нижнюю оценку функции Шеннона. Покажем, что функция Шеннона $L(n)$ при всех достаточно больших n превосходит величину $2^n/n$ (этот факт не следует ни из теоремы 1, ни из следствия к этой теореме), причем разность этих величин растет экспоненциально.

Теорема 2 (усиленная мощностная нижняя оценка)**.** *Для любого $\varepsilon > 0$ доля булевых функций f от n фиксированных переменных, удовлетворяющих условию*

$$L(f) \geq \frac{2^n}{n}\left(1 + (1-\varepsilon)\frac{\log_2 n}{n}\right),$$

стремится к 1 при $n \to \infty$.

Доказательство. Положим

$$k_\varepsilon = \frac{2^n}{n} + (1-\varepsilon)\frac{2^n \log_2 n}{n^2}.$$

Установим, что при $n \to \infty$

$$\log_2 \frac{N_{\leq}(k_\varepsilon, n)}{2^{2^n}} \to -\infty.$$

Применяя лемму 5, имеем:

$$\log_2 \frac{N_{\leq}(k_\varepsilon, n)}{2^{2^n}} \leq k_\varepsilon \log_2 c + k_\varepsilon \log_2 k_\varepsilon - 2^n \leq$$
$$\leq O\left(\frac{2^n}{n}\right) + \left(\frac{2^n}{n} + (1-\varepsilon)\frac{2^n \log_2 n}{n^2}\right) \log_2 \left(2\,\frac{2^n}{n}\right) - 2^n =$$
$$= -\varepsilon \frac{2^n \log_2 n}{n} + O\left(\frac{2^n}{n}\right).$$

Последнее выражение стремится к $-\infty$ при $n \to \infty$. □

Следствие 2. *При $n \to \infty$ выполняется асимптотическое неравенство*

$$L(n) - \frac{2^n}{n} \gtrsim \frac{2^n \log_2 n}{n^2}.$$

Теперь перейдем к исследованию роста функции Шеннона сложности реализации булевых функций схемами из функциональных элементов в произвольном полном конечном базисе.

Теорема 3. *Пусть B_1 и B_2 — конечные множества булевых функций, причем $[B_1] = [B_2] = P_2$. Тогда найдутся такие положительные константы c_1 и c_2, что для любой булевой функции f выполняются неравенства*

$$c_1 L_{B_1}(f) \leq L_{B_2}(f) \leq c_2 L_{B_1}(f).$$

Доказательство. Положим

$$c_2 = \max_{\varphi \in B_1} L_{B_2}(\varphi).$$

Теперь, если в какой-либо минимальной схеме S, реализующей произвольную функцию f в базисе B_1, заменить все функциональные элементы, соответствующие функциям из базиса B_1, минимальными схемами в

базисе B_2, реализующие те же самые функции, получим схему S', реализующую функцию f в базисе B_2 и имеющую сложность не более $c_2 L(S)$. Следовательно,

$$L_{B_2}(f) \le L(S') \le c_2 L(S) = c_2 L_{B_1}(f),$$

и второе неравенство доказано.

Полагая

$$c_1 = \left(\max_{\varphi \in B_2} L_{B_1}(\varphi) \right)^{-1},$$

можно аналогично установить первое неравенство. □

Из теоремы 3 и полученных оценок функции Шеннона сложности реализации булевых функций схемами из функциональных элементов в базисе $B_0 = \{x \vee y,\, x\&y,\, \overline{x}\}$ непосредственно устанавливается порядок роста функции Шеннона для произвольного полного конечного базиса.

Теорема 4. *Пусть B — конечное множество булевых функций, причем $[B] = P_2$. Тогда найдутся такие положительные константы a и b, что при $n \to \infty$ выполняются асимптотические неравенства*

$$a\frac{2^n}{n} \lesssim L_B(n) \lesssim b\frac{2^n}{n}.$$

Реализация симметрических функций

Как следует из мощностной нижней оценки функции Шеннона почти все булевы функции имеют экспоненциальную по числу переменных сложность. В связи с этим возникает естественная и тесно связанная с практическими применениями задача выявления различных классов булевых функций, допускающих существенно более простую схемную реализацию. Одним из таких классов является множество симметрических булевых функций, к изучению которого со сложностной точки зрения мы и переходим. Но прежде чем непосредственно заняться реализацией симметрических функций, рассмотрим две задачи, вспомогательные для исходной задачи, но имеющие серьезное самостоятельное значение.

Обозначим через Σ_n булев оператор суммирования n-разрядных чисел, т. е. булеву $(2n, n+1)$-функцию (систему из $n+1$ булевой функции от $2n$ переменных), которая по двум n-разрядным двоичным числам вычисляет $(n+1)$-разрядное двоичное представление их суммы, а через N_n — булев оператор подсчета числа единиц в наборе длины n, т. е. булеву $(n, \lceil \log(n+1) \rceil)$-функцию, которая по n-разрядному двоичному набору вычисляет $\lceil \log(n+1) \rceil$-разрядное двоичное представление количества единиц в этом наборе.

Лемма 6. *Для любого конечного полного базиса B при $n \to \infty$ верно равенство*

$$L_B(\Sigma_n) = O(n).$$

Доказательство. Утверждение леммы в силу теоремы 3 достаточно доказать для какого-нибудь конкретного конечного базиса. Пусть базис B содержит функции $x\&y$, $x \oplus y$, $x \oplus y \oplus z$ и $xy \vee xz \vee yz$.

Построим схему S, которая по двум группам входов — $(x_1, \ldots, x_n)$ и $(y_1, \ldots, y_n)$, на которые подаются двоичные n-разрядные числа (младшие разряды x_1 и y_1), вычисляет набор $(z_1, \ldots, z_{n+1})$, представляющий двоичную запись их суммы. Тогда, обозначив через u_i, $i = 2, \ldots, n+1$, значение переноса в i-й разряд, получаем:

$$\begin{gathered} z_1 = x_1 \oplus y_1, \quad u_2 = x_1 y_1 \\ z_i = x_i \oplus y_i \oplus u_i, \quad u_{i+1} = x_i y_i \vee x_i u_i \vee y_i u_i, \qquad i = 2, \ldots, n-1; \\ z_n = x_n \oplus y_n \oplus u_n, \quad z_{n+1} = u_{n+1} = x_n y_n \vee x_n u_n \vee y_n u_n. \end{gathered}$$

Следовательно, $L_B(\Sigma_n) \leq 2n$. □

Лемма 7. *Для любого конечного полного базиса B при $n \to \infty$ верно равенство*

$$L_B(N_n) = O(n).$$

Доказательство. Очевидно, что результат применения оператора N_n равен двоичной записи суммы n подаваемых на входы оператора одноразрядных двоичных чисел. Опишем способ вычисления этой суммы схемой линейной сложности.

Сначала будем считать, что $n = 2^k$ для некоторого k. Построим схему S, имеющую k ярусов. Ярус с номером t, $t = 1, \ldots, k$, будет состоять из 2^{k-t} подсхем, каждая из которых реализует оператор Σ_t и, следовательно, имеет две группы по t входов, а также $t+1$ выходов. Таким образом, считая в силу леммы 6, что $L_B(\Sigma_t) \leq ct$, в случае, когда $n = 2^k$, имеем:

$$L_B(N_n) \leq L_B(S) \leq \sum_{t=1}^{k} 2^{k-t} ct = c2^k \sum_{t=1}^{k} \frac{t}{2^t} < 2c2^k = 2cn.$$

Переходя к общему случаю, полагаем $n' = 2^{\lceil \log n \rceil}$. Очевидно, что $n \leq n' < 2n$. Схему, реализующую оператор N_n, можно получить из схемы S', реализующую оператор $N_{n'}$, подав на $n' - n$ входов схемы S' константу 0. Поэтому

$$L_B(N_n) \leq L_B(0) + L_B(N_{n'}) \leq L_B(0) + 2cn' \leq L_B(0) + 4cn = O(n).$$

□

Конспект лекции № 8 (31/03/16, проф. В. В. Кочергин)

Теперь рассмотрим реализацию симметрических булевых функций. Напомним, что функция $f(x_1, \ldots, x_n)$ называется *симметрической*, если для любой перестановки σ из симметрической группы S_n выполняется равенство $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$.

Теорема 5. *Для произольного конечного полного базиса B найдутся такие положительные константы c_1 и c_2, что для любой симметрической булевой функции $f(x_1, \ldots, x_n)$, отличной от константы, выполняются неравенства*

$$c_1 n \leq L_B(f(x_1, \ldots, x_n)) \leq c_2 n.$$

Доказательство. Нижнюю оценку в силу существенной зависимости от всех своих переменных любой отличной от константы симметрической функции дает неравенство

$$L_B(f) \geq \frac{n-1}{r(B)-1},$$

где $r(B)$ — максимальное число существенных переменных у функций из базиса B.

Переходя к доказательству верхней оценки отметим, что произвольная симметрическая функция f от n переменных может быть задана двоичной последовательностью $\tilde{\pi}(f) = (\pi_0(f), \pi_1(f), \ldots, \pi_n(f))$, где $\pi_k(f)$ — значение функции f на наборах, состоящих из k единиц и $n-k$ нулей. Значение симметрической функции $f(x_1, \ldots, x_n)$ одназначно определяется по числу единиц в наборе $x_1, \ldots, x_n$, а следовательно, по двоичной записи этого числа. На этом и основан метод построения схемы S, вычисляющей функцию $f(x_1, \ldots, x_n)$.

Схема S состоит из подсхем S_1 и S_2. Подсхема S_1 реализует оператор N_n, на выходах подсхемы S_1 вычисляется двоичная запись длины $\lceil \log(n+1) \rceil$ числа единиц во входном наборе. Подсхема S_2 по двоичной записи числа единиц во входном наборе вычисляет значение функции f на этом наборе. В силу леммы 7 и теоремы 4 получаем:

$$L_B(f) \leq L_B(N_n) + L_B(\lceil \log(n+1) \rceil) = O(n) + O\left(\frac{n}{\log n}\right) = O(n).$$

□

Асимптотически наилучший метод О. Б. Лупанова

Теперь на примере базиса $B_0 = \{x \vee y,\ x\&y,\ \overline{x}\}$ рассмотрим предложенный О. Б. Лупановым метод построения схем, который является асимптотически наилучшим для почти всех булевых функций.

Теорема 6 (О. Б. Лупанов). *Пусть $n \to \infty$. Тогда*

$$L(n) \leq \frac{2^n}{n}\left(1 + O\left(\frac{\log n}{n}\right)\right).$$

Доказательство. Опишем метод, который позволяет для произвольной (в том числе и для самой сложной) функции от n переменных построить схему, состоящую не более чем из $\frac{2^n}{n}\left(1 + O\left(\frac{\log n}{n}\right)\right)$ элементов.

Пусть $k = k(n)$ — натуральный параметр, удовлетворяющий при $n \to \infty$ условиям $k \to \infty$ и $n - k \to \infty$. Точное значение этого параметра укажем позже.

Таблицу из 2^n значений произвольной функции $f(x_1, \ldots, x_n)$ представим в виде прямоугольной таблицы высоты 2^k и ширины 2^{n-k} как показано на рис. 2.

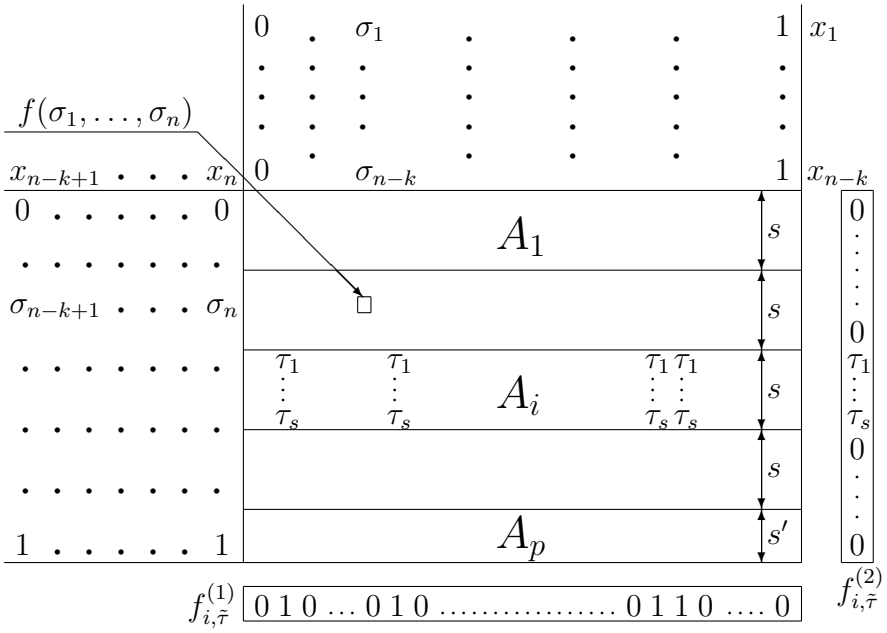


Рис. 2:

Пусть $s = s(n)$ — также некоторый натуральный параметр, удовлетворяющий при $n \to \infty$ условиям $s \to \infty$ и $\frac{2^k}{s} \to \infty$. Точное значение

этого параметра укажем позже. Таблицу разобъем на горизонтальные полосы $A_1, \ldots, A_p$ высоты s (полоса A_p имеет высоту $s' \leq s$), $p = \left\lceil \frac{2^k}{s} \right\rceil$. Для $i = 1, \ldots, p$ через $f_i(x_1, \ldots, x_n)$ обозначим функцию, значения которой совпадают со значениями функции $f(x_1, \ldots, x_n)$ на полосе A_i, и равны 0 на остальных полосах. Тогда

$$f(x_1, \ldots, x_n) = \bigvee_{i=1}^{p} f_i(x_1, \ldots, x_n).$$

Теперь для каждой пары $(i, \tilde{\tau})$, $i = 1, \ldots, p$, $\tilde{\tau} \in \{0,1\}^s$ (или $\tilde{\tau} \in \{0,1\}^{s'}$ при $i = p$), обозначим через $f_{i,\tilde{\tau}}(x_1, \ldots, x_n)$ функцию, таблица которой получается из таблицы функции $f_i(x_1, \ldots, x_n)$ путем обнуления всех столбцов полосы A_i, значения в которых не сопадают с набором $\tilde{\tau}$. Тогда

$$f(x_1, \ldots, x_n) = \bigvee_{i=1}^{p} \bigvee_{\tilde{\tau}} f_{i,\tilde{\tau}}(x_1, \ldots, x_n).$$

Наконец, у каждой функции $f_{i,\tilde{\tau}}(x_1, \ldots, x_n)$ можно разделить переменные, точнее представить эту функцию в виде

$$f_{i,\tilde{\tau}}(x_1, \ldots, x_n) = f^{(1)}_{i,\tilde{\tau}}(x_1, \ldots, x_{n-k}) f^{(2)}_{i,\tilde{\tau}}(x_{n-k+1}, \ldots, x_n),$$

где функция $f^{(1)}_{i,\tilde{\tau}}(x_1, \ldots, x_{n-k})$ обращается в единицу только на таких наборах $(\sigma_1, \ldots, \sigma_{n-k})$, что в соответствующих этим наборам столбцах полосы A_i находится набор $\tilde{\tau}$, а столбец значений функции $f^{(2)}_{i,\tilde{\tau}}(x_{n-k+1}, \ldots, x_n)$ совпадает с набором $\tilde{\tau}$ на полосе A_i, а на наборах вне полосы A_i функция $f^{(2)}_{i,\tilde{\tau}}(x_{n-k+1}, \ldots, x_n)$ равна 0.

Возвращаясь к представлению функции f, окончательно получаем:

$$f(x_1, \ldots, x_n) = \bigvee_{i=1}^{p} \bigvee_{\tilde{\tau}} f^{(1)}_{i,\tilde{\tau}}(x_1, \ldots, x_{n-k}) f^{(2)}_{i,\tilde{\tau}}(x_{n-k+1}, \ldots, x_n).$$

Схема S, реализующая функцию $f(x_1, \ldots, x_n)$, будет состоять из подсхем S_i, $i = 1, \ldots, 6$, — см. рис. 3.

Подсхема S_1, на входы которой подаются переменные $x_1, \ldots, x_{n-k}$, реализует систему функций $\mathcal{K}_{n-k}(x_1, \ldots, x_{n-k})$. В силу леммы о сложности реализации системы элементарных конъюнкций можно считать, что при $n \to \infty$

$$L(S_1) = 2^{n-k} + o\left(2^{n-k}\right) \leq 2 \times 2^{n-k}.$$

Подсхема S_2, на входы которой подаются переменные $x_{n-k+1}, \ldots, x_n$, реализует систему функций $\mathcal{K}_k(x_{n-k+1}, \ldots, x_n)$. Также в силу леммы о

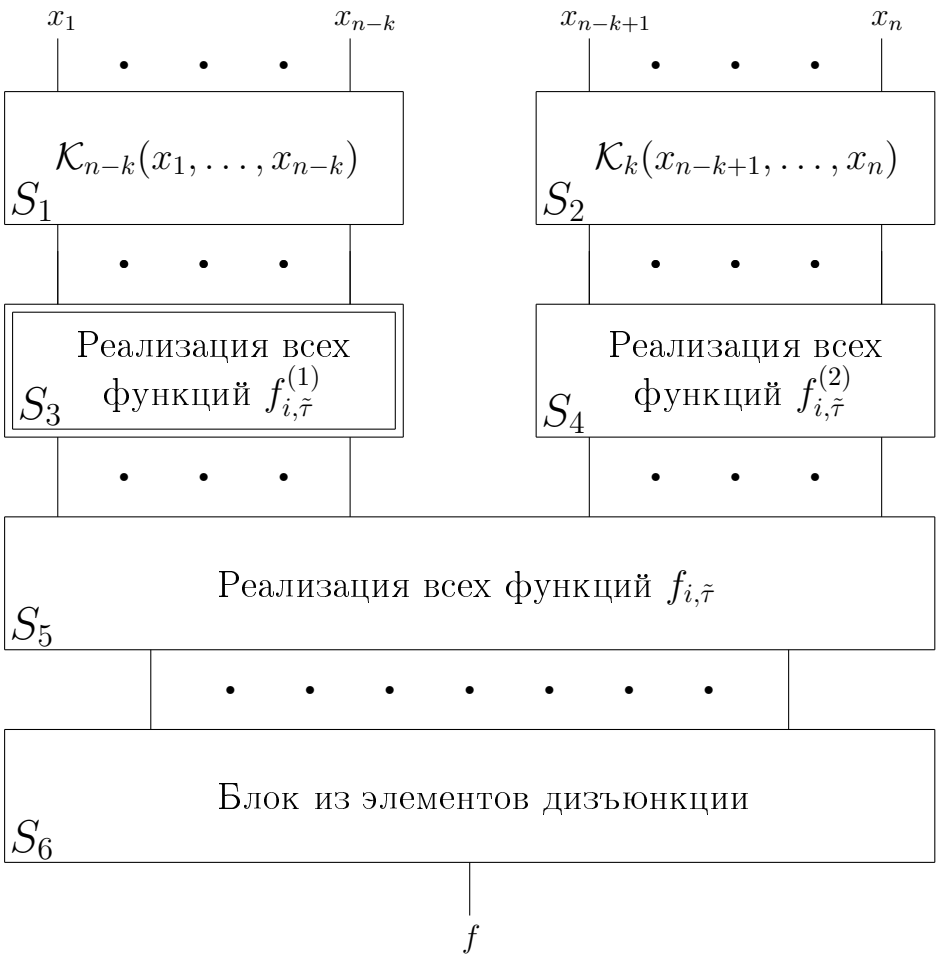


Рис. 3:

сложности реализации системы элементарных конъюнкций можно считать, что при $n \to \infty$

$$L(S_2) = 2^k + o\left(2^k\right) \leq 2 \times 2^k.$$

Подсхема S_3, на входы которой подаются элементарные конъюнкции из системы $\mathcal{K}_{n-k}(x_1, \ldots, x_{n-k})$, состоит только из дизъюнкторов и реализует функции $f^{(1)}_{i,\tilde{\tau}}(x_1, \ldots, x_{n-k})$ для всех i и $\tilde{\tau}$ в соответствии с представлением этих функций в виде совершенной дизъюнктивной нормальной

формы. Учитывая равенство[1]

$$\sum_{\tilde{\tau}} \left| N_{f^{(1)}_{i,\tilde{\tau}}} \right| = 2^{n-k},$$

справедливое для всех $i = 1, \ldots, p$, получаем следующую оценку:

$$L(S_3) \leq p2^{n-k}.$$

Подсхема S_4, на входы которой подаются элементарные конъюнкции из системы $\mathcal{K}_k(x_{n-k+1}, \ldots, x_n)$, состоит только из дизъюнкторов и реализует функции $f^{(2)}_{i,\tilde{\tau}}(x_{n-k+1}, \ldots, x_n)$ для всех i и $\tilde{\tau}$ также в соответствии с представлением этих функций в виде совершенной дизъюнктивной нормальной формы. Используя очевидное равенство

$$\left| N_{f^{(2)}_{i,\tilde{\tau}}} \right| \leq s,$$

выполняющееся для всех допустимых значений i и $\tilde{\tau}$, получаем:

$$L(S_4) \leq p2^s s.$$

Подсхема S_5, на входы которой подаются выходы подсхем S_3 и S_4, состоит только из конъюнкторов и реализует функции $f_{i,\tilde{\tau}}(x_1, \ldots, x_n)$ для всех i и $\tilde{\tau}$. Сложность подсхемы S_5 можно оценить сверху числом различных пар $(i, \tilde{\tau})$:

$$L(S_5) \leq p2^s.$$

Подсхема S_6, на входы которой подаются все функции$f_{i,\tilde{\tau}}(x_1, \ldots, x_n)$ для всех i и $\tilde{\tau}$, состоит только из дизъюнкторов и реализует функцию $f(x_1, \ldots, x_n)$.Сложность подсхемы S_6 также можно оценить сверху числом различных пар $(i, \tilde{\tau})$:

$$L(S_6) < p2^s.$$

Таким образом,

$$\begin{aligned} L(f) \leq L(S) = \sum_{i=1}^{6} L(S_i) \leq \\ \leq 2 \times 2^{n-k} + 2 \times 2^k + p2^{n-k} + p2^s s + 2p2^s \leq \\ \leq \left(\frac{2^k}{s} + 1 \right) 2^{n-k} + \left(\frac{2^k}{s} + 1 \right) 2^s (s+2) + 2^{n-k+1} + 2^{k+1} \leq \\ \leq \frac{2^n}{s} + 2^{s+k} + 3 \times 2^{n-k} + 2 \times 2^k. \end{aligned}$$

[1]Здесь и далее через N_g обозначается множество наборов переменных функции g, на которых эта функция равна 1.

Теперь полагая

$$k = \lfloor 3 \log n \rfloor, \quad s = \lfloor n - 5 \log n \rfloor,$$

легко проверить, что условия $k \to \infty$, $k \to \infty$, $s \to \infty$, $\frac{2^k}{s} \to \infty$ выполнены. Подставляя значения k и s в полученную оценку, имеем:

$$L(f) \leq \frac{2^n}{n} \left(1 + O\left(\frac{\log n}{n}\right)\right).$$

Утверждение теоремы следует из справедливости этой оценки для функции $f(x_1, \ldots, x_n)$, удовлетворяющей условию $L(f) = L(n)$. □

Упражнение 1. Доказать, что при $n \to \infty$ для любого фиксированного $r \geq 2$ справедливо асимптотическое неравенство

$$L_{\{x_1 \& \ldots \& x_r, \overline{x}\}}(n) \sim \frac{1}{r-1} \frac{2^n}{n}.$$

Отметим важный факт, который вытекает из теорем 1 и 6: почти все функции от n переменных имеют сложность, асимптотически совпадающую со сложностью самой сложной функции. Такой эффект называется *эффектом Шеннона.*

Реализация самодвойственных функций

В качестве одного из разнообразных применений теоремы Лупанова рассмотрим задачу о сложности реализации самодвойственных функций в базисе $B_0 = \{x \vee y,\ x \& y,\ \overline{x}\}$.

Определим функцию Шеннона сложности реализации самодвойственных функций в базисе B_0 равенством

$$L^S(n) = \max_{f(x_1, \ldots, x_n) \in S} L(f).$$

Теорема 7. *При $n \to \infty$ справедливо асимптотическое равенство*

$$L^S(n) \sim \frac{2^{n-1}}{n}.$$

Доказательство. Если в доказательстве теоремы 1 положить

$$k_\varepsilon = (1 - \varepsilon) \frac{2^{n-1}}{n}$$

и сравнить величину $N_{\leq}(k_\varepsilon, n)$ не с числом 2^{2^n} всех булевых функций от n переменных, а с числом $2^{2^{n-1}}$ всех самодвойственных функций от n переменных, то получится такая нижняя оценка:

$$L^S(n) \gtrsim \frac{2^{n-1}}{n-1} \sim \frac{2^{n-1}}{n}.$$

Построим схему в базисе $B_0 = \{\vee, \&, {}^-\}$ для произвольной самодвойственной функции $f(x_1, \ldots, x_n)$. Положим

$$g(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0).$$

Тогда

$$f(x_1, \ldots, x_{n-1}, 1) = \overline{f(\overline{x}_1, \ldots, \overline{x}_{n-1}, 0)} = \overline{g(\overline{x}_1, \ldots, \overline{x}_{n-1})}.$$

Таким образом, для реализации функции $f(x_1, \ldots, x_n)$ достаточно при $x_n = 0$ реализовать функцию $g(x_1, \ldots, x_{n-1})$, а при $x_n = 1$ — функцию $\overline{g(\overline{x}_1, \ldots, \overline{x}_{n-1})}$.

Преобразуем минимальную схему S_g, реализующую в базисе B_0 функцию $g(x_1, \ldots, x_{n-1})$, в схему S_f, реализующую функцию $f(x_1, \ldots, x_n)$. На i-й вход схемы, $i = 1, \ldots, n-1$, вместо переменной x_i подадим выход подсхемы, реализующей функцию $x_i \oplus x_n$ (схема для функции $x_1 \oplus x_2$ приведена на рис. 1). Выход схемы S_g, а также переменную x_n, подадим на входы еще одной подсхемы, реализующей сумму по модулю 2 своих входов. Получим схему S_f, реализующую функцию f, причем

$$L(S_f) = L(S_g) + nL(S_\oplus) = L(S_g) + 4n.$$

Применяя для оценки сложности минимальной схемы, реализующей функцию g от $n-1$ переменной, теорему 6, получаем требуемую верхнюю оценку. $\square$