Math-Net.Ru

Общероссийский математический портал

Р. Н. Забалуев, О средней сложности монотонных функций, *Дискрет. матем.*, 2006, том 18, выпуск 2, 71–83

DOI: <https://doi.org/10.4213/dm47>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.81.137.203

26 апреля 2023 г., 15:46:02

О средней сложности монотонных функций

© 2005 г. Р. Н. Забалуев

В работе рассматривается сложность реализации монотонных функций неветвящимися программами с условной остановкой. Показано, что при $n \rightarrow \infty$ средняя сложность каждой монотонной функции n переменных не превосходит величины $a2^n/n^2(1 + o(1))$, а средняя сложность почти каждой монотонной функции n переменных не меньше, чем $b2^n/n^2(1 + o(1))$, где a и b — некоторые постоянные.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 05-01-0099, программой Президента Российской Федерации поддержки ведущих научных школ, грант НШ-1807.2003.1, программой Университеты России, проект УР.04.02.528, и программой фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики», проект «Оптимальный синтез управляющих систем».

1. Введение

В работе рассматривается средняя сложность монотонных функций. Функции вычисляются при помощи неветвящихся программ с условной остановкой, которые введены А. В. Чашкиным в [10]. Рассматриваемые программы обобщают понятие схемы из функциональных элементов и являются естественной моделью неветвящихся вычислений, то есть вычислений в которых нет условного перехода и косвенной адресации, но есть возможность досрочного прекращения работы при выполнении определенного условия.

Сложностью $L(P)$ программы P назовем число операторов этой программы. Временем работы $T_P(x)$ программы P на наборе переменных x назовем число операторов, выполненных до остановки программы. Величину

$$T(P) = 2^{-n} \sum T_P(x),$$

где суммирование производится по всем двоичным наборам x длины n , назовем средним временем работы программы P . Если для некоторой булевой функции f и любого двоичного набора x справедливо равенство $f(x) = P(x)$, то будем говорить, что программа P вычисляет функцию f . Величину

$$T(f) = \min T(P),$$

где минимум берется по всем программам, вычисляющим f , назовем средней сложностью функции f . Программу P , вычисляющую функцию f , для которой справедливо равенство $T(P) = T(f)$, назовем минимальной программой. Пусть $Q(n)$ — некоторый класс функций от n переменных. Будем говорить, что некоторое свойство выполнено для

почти каждой функции из класса $\mathcal{Q}(n)$, если для подкласса $V(n)$ функций, не обладающих этим свойством,

$$\lim_{n \rightarrow \infty} |V(n)|/|\mathcal{Q}(n)| = 0.$$

Сложность реализации монотонных функций схемами из функциональных элементов изучалась специалистами по синтезу управляющих систем в течение многих лет. Пусть $L_B(A)$ — функция Шеннона для сложности реализации схемами в базисе B функций из класса A ; $\rho(B)$ — приведенный вес базиса B . Через $M(n)$ обозначим класс монотонных функций n переменных.

В 1957 г. С. В. Яблонский [13] показал, что

$$L_B(M(n)) = o\left(\frac{2^n}{n}\right). \quad (1)$$

Нижняя оценка для величины $L_B(M(n))$, получаемая из мощностных соображений (см. [4]), имеет вид

$$L_B(M(n)) \geq \frac{1}{n} \rho(B) \binom{n}{\lfloor n/2 \rfloor} (1 + o(1)).$$

Конкретные верхние оценки (хотя и существенно отличающиеся от нижней) получены в [8] и [5]. В. К. Коробков в [2] установил, что

$$\log |M(n)| \asymp \binom{n}{\lfloor n/2 \rfloor};$$

в сочетании с принципом локального кодирования О. Б. Лупанова (см. [4]) это позволило ему найти порядок функции Шеннона

$$L_B(M(n)) \asymp \frac{1}{n} \binom{n}{\lfloor n/2 \rfloor}. \quad (2)$$

В 1966 г. Ж. Ансель, опираясь на свой метод перечисления монотонных функций [14] и принцип локального кодирования, несколько уменьшил константу в верхней оценке работы [2]. В [15] построено асимптотически оптимальное кодирование монотонных функций и показано, что

$$\log |M(n)| \sim \frac{1}{n} \binom{n}{\lfloor n/2 \rfloor}.$$

С использованием перечислительной конструкции работы [3] и принципа локального кодирования в [9] получена асимптотика функции Шеннона

$$L_B(M(n)) \sim \frac{1}{n} \rho(B) \binom{n}{\lfloor n/2 \rfloor}. \quad (3)$$

В [16] был получен следующий аналог последней формулы:

$$L_B(M(n)) - \frac{1}{n} \rho(B) \binom{n}{\lfloor n/2 \rfloor} \asymp \frac{\log n}{n^2} \binom{n}{\lfloor n/2 \rfloor} \quad (4)$$

Отметим также метод доказательства соотношения (2), предложенный в [12], где вычисления монотонных функций несложным образом сводятся к вычислению частичных функций. При доказательстве формул (1)–(4) предполагалось, что базис B полон в множестве всех булевых функций $P_2(n)$.

Помимо задач реализации монотонных функций в полных базисах также рассматривались задачи реализации этих функций в неполных базисах. В [6, 7] была установлена справедливость формулы (2) для собственных базисов класса $M(n)$. В [1] доказана справедливость формулы (4) для собственных базисов класса $M(n)$ с использованием усовершенствованной перечислительную процедуру из [15].

Используя результаты работы [3], легко установить, что для почти каждой монотонной функции $f(x_1, \dots, x_n)$ справедливо соотношение

$$T(f) \leq c \frac{2^n}{n^2} (1 + o(1)). \quad (5)$$

Действительно, из [3] следует, что почти каждая функция $f \in M(n)$ принимает значение нуль на всех наборах, содержащих менее $\lfloor n/2 \rfloor - 1$ единиц, а значение единица на всех наборах, содержащих более $\lfloor n/2 \rfloor + 2$ единиц. Тогда программу P , вычисляющую f , можно записать в виде $P = P_1 P_2$. Программа P_1 по входному набору $\tilde{\sigma}$ вычисляет число единиц $\|\tilde{\sigma}\|$ в этом наборе, и если $\|\tilde{\sigma}\| < \lfloor n/2 \rfloor - 1$ или $\|\tilde{\sigma}\| > \lfloor n/2 \rfloor + 2$, то присваивает выходной переменной значение нуль или единица соответственно и останавливает вычисления. Программа P_2 по входному набору $\tilde{\sigma}$, на котором не остановилась программа P_1 , вычисляет значение $f(\tilde{\sigma})$. Учитывая (2)–(4), программу P_2 можно составить не более чем из $c_1 2^n / n^{3/2} (1 + o(1))$ команд. Пусть E' — множество наборов $\tilde{\sigma}$, у которых число единиц либо меньше $\lfloor n/2 \rfloor - 1$, либо больше $\lfloor n/2 \rfloor + 2$. Тогда выполняется цепочка неравенств

$$\begin{aligned} T(f) &\leq T(P) \leq 2^{-n} \left(\sum_{\tilde{\sigma} \in E'} L(P_1) + \sum_{\tilde{\sigma} \in E^n \setminus E'} (L(P_1) + L(P_2)) \right) \\ &\leq 2^{-n} \left(2^n O(n) + 4 \binom{n}{\lfloor n/2 \rfloor} \frac{c_1 2^n}{n^{3/2}} (1 + o(1)) \right) \\ &\leq c \frac{2^n}{n^2} (1 + o(1)). \end{aligned}$$

В настоящей работе для каждой монотонной функции $f(x_1, \dots, x_n)$ получена оценка (5), а также показана оптимальность по порядку этой оценки для почти каждой рассматриваемой функции. Основным результатом работы является следующая теорема.

Теорема 1. Пусть $n \rightarrow \infty$. Тогда для каждой функции $f \in M(n)$ выполнено соотношение

$$T(f) \leq a \frac{2^n}{n^2} (1 + o(1))$$

и для почти каждой функции $f \in M(n)$ справедливо соотношение

$$T(f) \geq b \frac{2^n}{n^2} (1 + o(1)),$$

где a и b — некоторые положительные постоянные.

Здесь наибольший интерес представляет первое утверждение, составляющее утверждение теоремы 2 раздела 4 данной работы. Для доказательства этой теоремы в разделе 3 строится специальное разбиение множества всех двоичных наборов, зависящее от конкретной монотонной функции. При построении используется лемма 4, рассмотренная в разделе 2, которая представляет собой модификацию одного утверждения из [12]. Упомянутое разбиение и его свойства позволяют привести алгоритм написания программ, вычисляющих монотонные функции, с необходимым средним временем работы и в итоге доказать теорему 2. Второе утверждение теоремы составляет утверждение теоремы 3, которая доказывается в разделе 5.

2. Вспомогательные утверждения о монотонных функциях

Булева функция $f(x_1, \dots, x_n)$ называется монотонной, если $f(\tilde{\alpha}) \leq f(\tilde{\beta})$ для всяких двух наборов $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \dots, \beta_n)$ таких, что $\tilde{\alpha} \leq \tilde{\beta}$, то есть $\alpha_1 \leq \beta_1, \dots, \alpha_n \leq \beta_n$. Через E^n обозначим множество всех n -местных двоичных наборов и назовем это множество n -мерным булевым кубом, через $E^{n,k}$ обозначим множество наборов из E^n , содержащих k единиц. Пусть $\tilde{\alpha}_1, \tilde{\alpha}_2$ — n -местные двоичные наборы, отличающиеся друг от друга в одной компоненте, и $\tilde{\alpha}_1 \leq \tilde{\alpha}_2$. Тогда пара $(\tilde{\alpha}_1, \tilde{\alpha}_2)$ задает ребро n -мерного булевого куба E^n . Ребра $\alpha = (\tilde{\alpha}_1, \tilde{\alpha}_2)$ и $\beta = (\tilde{\beta}_1, \tilde{\beta}_2)$ назовем сравнимыми, если $\tilde{\alpha}_2 \leq \tilde{\beta}_1$ или $\tilde{\beta}_2 \leq \tilde{\alpha}_1$. Будем говорить, что ребра α и β несравнимы, если $\tilde{\alpha}_1 \not\leq \tilde{\beta}_2$ и $\tilde{\alpha}_2 \not\leq \tilde{\beta}_1$. Последовательность вершин и ребер из E^n $\tilde{\alpha}_1, (\tilde{\alpha}_1, \tilde{\alpha}_2), \tilde{\alpha}_2, (\tilde{\alpha}_2, \tilde{\alpha}_3), \dots, \tilde{\alpha}_{k-1}, (\tilde{\alpha}_{k-1}, \tilde{\alpha}_k), \tilde{\alpha}_k$, назовем цепью, если $\tilde{\alpha}_i \leq \tilde{\alpha}_{i+1}$ для $i = 1, 2, \dots, k-1$.

Лемма 1. Пусть N — множество попарно несравнимых ребер в E^n . Тогда справедливо неравенство

$$|N| \leq \left\lceil \frac{n}{2} \right\rceil \binom{n}{\lceil n/2 \rceil}.$$

Доказательство. Через N_k обозначим множество ребер $\alpha = (\tilde{\alpha}_1, \tilde{\alpha}_2) \in N$ таких, что $\tilde{\alpha}_1 \in E^{n,k}$. Оценим число различных цепей в E^n с началом в наборе $(0, 0, \dots, 0)$ и концом в наборе $(1, 1, \dots, 1)$, проходящих через ребра из N_k . В набор $\tilde{\alpha}_1$ входит $k!$ цепей, а из набора $\tilde{\alpha}_2$ выходит $(n-k-1)!$ цепей. Поэтому через ребро α проходит $k!(n-k-1)!$ цепей. Так как число различных цепей, идущих из $(0, 0, \dots, 0)$ в $(1, 1, \dots, 1)$, равно $n!$, а через разные ребра из N_k проходят различные цепи, выполнено неравенство

$$\sum_{k=0}^{n-1} \sum_{\alpha \in N_k} k!(n-k-1)! \leq n!.$$

Перепишем это неравенство в виде

$$\sum_{k=0}^{n-1} \sum_{\alpha \in N_k} \frac{1}{\binom{n-1}{k}} \leq n.$$

Отсюда следует справедливость соотношений

$$\frac{|N|}{\binom{n-1}{\lceil (n-1)/2 \rceil}} \leq \frac{1}{\binom{n-1}{\lceil (n-1)/2 \rceil}} \sum_{k=0}^{n-1} \sum_{\alpha \in N_k} 1 \leq \sum_{k=0}^{n-1} \sum_{\alpha \in N_k} \frac{1}{\binom{n-1}{k}} \leq n.$$

Таким образом, получаем, что

$$|N| \leq n \binom{n-1}{\lceil (n-1)/2 \rceil} = \lceil \frac{n}{2} \rceil \binom{n}{\lceil n/2 \rceil}.$$

Лемма 1 доказана.

Пусть $f(x_1, \dots, x_n)$ — монотонная функция и $\alpha = (\tilde{\alpha}_1, \tilde{\alpha}_2)$ — ребро в E^n . Тогда будем говорить, что α — непостоянное ребро функции f , если $f(\tilde{\alpha}_1) < f(\tilde{\alpha}_2)$.

Лемма 2. Пусть N — множество непостоянных ребер функции $f \in M(n)$. Тогда справедливо неравенство

$$|N| \leq \lceil \frac{n}{2} \rceil \binom{n}{\lceil n/2 \rceil}.$$

Утверждение этой леммы следует из леммы 1 и того факта, что непостоянные ребра монотонной функции f попарно несравнимы.

Через $f_{pqr}^{\delta\gamma\eta}$ обозначим функцию $n-3$ переменных, получающуюся из функции $f(x_1, \dots, x_n)$ подстановкой двоичных значений δ, γ, η вместо переменных x_p, x_q и x_r соответственно, при этом нумерация переменных, в которые значения подставлены не были, не меняется. Пусть $\alpha = (\tilde{\alpha}_1, \tilde{\alpha}_2)$ — ребро в E^n . Будем говорить, что оно имеет направление p , если наборы $\tilde{\alpha}_1$ и $\tilde{\alpha}_2$ отличаются в компоненте с номером p .

Лемма 3. Пусть $f \in M(n)$. Если значения функций f_{pqr}^{111} и f_{pqr}^{000} не равны на N наборах, то у функции f число непостоянных ребер направлений p, q, r не меньше $3N$.

Доказательство этой леммы несложно, и мы его опускаем.

Лемма 4. Пусть $f \in M(n)$. Тогда существуют такие числа p, q, r , что число наборов, на которых функции f_{pqr}^{111} и f_{pqr}^{000} не совпадают, не превосходит величины

$$\frac{n+1}{2n} \binom{n}{\lceil n/2 \rceil}. \quad (6)$$

Доказательство. Будем говорить, что непостоянное ребро функции f соответствует тройке чисел p, q, r , если оно имеет направление либо p , либо q , либо r .

Допустим, что для любой тройки чисел p, q, r число наборов (длины $n-3$), на которых функции f_{pqr}^{111} и f_{pqr}^{000} не совпадают, строго больше чем (6).

При подсчете непостоянных ребер функции f , соответствующих всем тройкам, каждое непостоянное ребро повторится $\binom{n-1}{2}$ раз. Действительно, пусть непостоянное ребро α функции f имеет направление p (заметим, что направления выбираются из множества $\{1, 2, \dots, n\}$). Тогда это ребро соответствует каждой тройке чисел, одним числом из которых является p . Другие два числа (или два направления), отличные от p , в каждой такой тройке принадлежат множеству $\{1, 2, \dots, n\} \setminus \{p\}$. Поэтому количество таких троек равно

$$\binom{n-1}{2} = \frac{(n-1)(n-2)}{2}.$$

Таким образом, с учетом леммы 3, общее число различных непостоянных ребер функции f , соответствующих всем тройкам, строго больше чем

$$\frac{n(n-1)(n-2)}{3 \cdot 2 \cdot (n-1)(n-2)/2} \frac{3(n+1)}{2n} \binom{n}{\lceil n/2 \rceil} = \frac{n+1}{2} \binom{n}{\lceil n/2 \rceil}.$$

Получили противоречие с леммой 2.

Лемма 4 доказана.

3. Об одном разбиении множества двоичных наборов

В данном разделе описано, как из множества $A_0 = E^n$ выделяются зависящие от конкретной монотонной функции подмножества $D_1, D_2, \dots, D_k$ и $A_1, A_2, \dots, A_k$ (k — целочисленный параметр), которые задают разбиение

$$A_0 = A_k \sqcup D_k \sqcup D_{k-1} \sqcup \dots \sqcup D_1, \quad (7)$$

где для множеств D_i и A_i выполняются соотношения

$$A_k \subseteq A_{k-1} \subseteq \dots \subseteq A_1 \subseteq A_0, \quad A_{i-1} = A_i \sqcup D_i, \quad i = 1, \dots, k.$$

Перед описанием множеств D_i и A_i введем вспомогательные множества функций $B_0, B_1, \dots, B_k$, которые задают разбиение и вместе с ним используются в доказательстве теоремы 2.

Пусть f — монотонная функция n переменных. Построим для нее множества $B_0, B_1, \dots, B_k$. На рис. 1 изображена диаграмма (дерево) H_k , где схематично показано, как получаются функции из этих множеств.

Пусть множество B_0 состоит из единственной функции $f_{1,0} = f$. Для функции f по лемме 4 найдутся числа p_1, q_1, r_1 такие, что функции $f_{p_1 q_1 r_1}^{111}$ и $f_{p_1 q_1 r_1}^{000}$ не совпадают не более чем на

$$\frac{n+1}{2n} \binom{n}{\lceil n/2 \rceil} \leq \binom{n}{\lceil n/2 \rceil}$$

наборах длины $n-3$. Символом $f_{1,1}$ обозначим функцию $f_{p_1 q_1 r_1}^{000}$. С функцией $f_{1,1}$ свяжем два набора, набор $v_{1,1}$, состоящий из одного нуля, и набор $w_{1,1}$, состоящий из чисел p_1, q_1, r_1 , то есть $v_{1,1} = (0)$, $w_{1,1} = (p_1 q_1 r_1)$. Также обозначим функцию $f_{p_1 q_1 r_1}^{111}$ символом $f_{2,1}$ и свяжем с этой функцией наборы $v_{2,1} = (1)$ и $w_{2,1} = (p_1 q_1 r_1)$. К множеству B_1 отнесем функции $f_{1,1}$ и $f_{2,1}$. На рис. 1 ребру, соединяющему вершину f с вершиной $f_{1,1}$, приписан нуль, а ребру, соединяющему вершину f с вершиной $f_{2,1}$ — единица, также обоим ребрам приписан набор $(p_1 q_1 r_1)$. Это показывает, что функция $f_{1,1}$ получена из f подстановкой нулей вместо переменных $x_{p_1}, x_{q_1}, x_{r_1}$, а функция $f_{2,1}$ — подстановкой единиц вместо этих же переменных.

Теперь построим множество B_2 . Для функции $g = f_{1,1}$ по лемме 4 найдем числа p_2, q_2, r_2 такие, что функции $g_{p_2 q_2 r_2}^{000}$ и $g_{p_2 q_2 r_2}^{111}$ не совпадают не более чем на $\binom{n-3}{\lceil (n-3)/2 \rceil}$ наборах длины $n-6$. Функцию $(n-6)$ -ти переменных $g_{p_2 q_2 r_2}^{000}$ обозначим символом $f_{1,2}$ и свяжем с этой функцией наборы $v_{1,2} = (v_{1,1} 0) = (00)$, $w_{1,2} = (w_{1,1} p_2 q_2 r_2) = (p_1 q_1 r_1 p_2 q_2 r_2)$, а функцию $g_{p_2 q_2 r_2}^{111}$ обозначим символом $f_{2,2}$ и свяжем с ней наборы $v_{2,2} = (v_{1,1} 1) = (01)$, $w_{2,2} = (w_{1,1} p_2 q_2 r_2) = (p_1 q_1 r_1 p_2 q_2 r_2)$. Для функции $h = f_{2,1}$, как

Рис. 1.

и для функции $f_{1,1}$, по лемме 4 найдем числа p'_2, q'_2, r'_2 такие, что функции $h_{p'_2 q'_2 r'_2}^{000}$ и $h_{p'_2 q'_2 r'_2}^{111}$ не совпадают не более чем на $\binom{n-3}{\lfloor (n-3)/2 \rfloor}$ наборах длины $n-6$. Функцию $(n-6)$ -ти переменных $h_{p'_2 q'_2 r'_2}^{000}$ обозначим символом $f_{3,2}$ и свяжем с этой функцией наборы $v_{3,2} = (v_{1,1}0) = (10)$, $w_{3,2} = (w_{1,1} p_2 q_2 r_2) = (p_1 q_1 r_1 p'_2 q'_2 r'_2)$, а функцию $h_{p'_2 q'_2 r'_2}^{111}$ — символом $f_{4,2}$ и свяжем с ней наборы $v_{4,2} = (v_{1,1}1) = (11)$ и $w_{4,2} = (w_{1,1} p'_2 q'_2 r'_2) = (p_1 q_1 r_1 p'_2 q'_2 r'_2)$.

К множеству B_2 отнесем функции $f_{1,2}, f_{2,2}, f_{3,2}$ и $f_{4,2}$. На рис. 1 ребра, выходящие из вершины $f_{1,1}$ к вершинам $f_{1,2}$ и $f_{2,2}$, помечены одно нулем, другое единицей, также обоим ребрам приписан набор $(p_2 q_2 r_2)$. Аналогично ребра, выходящие из вершины $f_{2,1}$ к вершинам $f_{3,2}$ и $f_{4,2}$, помечены нулем и единицей соответственно, и обоим ребрам приписан набор $(p'_2 q'_2 r'_2)$. Как и для функций из множества B_1 , обозначения показывают, что функция $f_{1,2}$ получена из $f_{1,1}$ подстановкой нулей вместо переменных $x_{p_2}, x_{q_2}, x_{r_2}$, а функция $f_{2,2}$ — подстановкой единиц вместо этих же переменных; функции $f_{3,2}$ и $f_{4,2}$ получены из $f_{2,1}$ подстановкой трех нулей и трех единиц соответственно вместо $x_{p'_2}, x_{q'_2}, x_{r'_2}$.

Допустим, что уже построено множество B_{k-1} . Проследим, как строится множество B_k . Каждая функция $f_{i,k-1} \in B_{k-1}$, $i = 1, \dots, 2^{k-1}$, зависит от $n-3(k-1)$ переменных, и с ней связаны двоичный набор $v_{i,k-1}$ длины $k-1$ и числовой набор $w_{i,k-1}$ длины $3(k-1)$, состоящий из чисел, найденных по лемме 4. Снова по лемме 4 для каждой функции $g = f_{i,k-1}$, $i = 1, \dots, 2^{k-1}$, найдем такие числа $p_k = p_k(i)$, $q_k = q_k(i)$, $r_k = r_k(i)$, что функции $g_{p_k q_k r_k}^{000}$ и $g_{p_k q_k r_k}^{111}$ не совпадают не более чем на $\binom{n-3(k-1)}{\lfloor (n-3(k-1))/2 \rfloor}$ наборах. Функции $(n-3k)$ переменных $g_{p_k q_k r_k}^{000}$ и $g_{p_k q_k r_k}^{111}$ обозначим символами $f_{2i-1,k}$ и $f_{2i,k}$ соответственно. С функцией $f_{2i-1,k}$ свяжем наборы $v_{2i-1,k} = (v_{i,k-1}0)$ и $w_{2i-1,k} = (w_{i,k-1} p_k q_k r_k)$, а с функцией $f_{2i,k}$ — наборы $v_{2i,k} = (v_{i,k-1}1)$ и $w_{2i,k} = (w_{i,k-1} p_k q_k r_k)$. На рис. 1 вершина $f_{i,k-1}$ соединена ребрами с вершинами $f_{2i-1,k}$ и $f_{2i,k}$, ребра помечены

нулем и единицей соответственно, и им приписан набор $(p_k q_k r_k)$.

Итак, каждая функция $f_{i,j}$ из множества B_j задается двоичным набором $v_{i,j}$ длины j и числовым набором $w_{i,j}$ длины $3j$. Эти наборы легко получить, глядя на дерево H_k . Набор $v_{i,j}$ получается, если выписать двоичные значения, которыми помечены ребра пути, идущего из вершины f в вершину $f_{i,j}$. А если расположить друг за другом тройки чисел из наборов, приписанных ребрам этого пути, в том же порядке, в каком следуют ребра, то получится числовой набор $w_{i,j}$.

Функции $f_{2i-1,j}$ и $f_{2i,j}$ будем называть близнецами, а функцию $f_{i,j-1}$ — предком для функций $f_{2i-1,j}$ и $f_{2i,j}$. Очевидно, что у функций-близнецов связанные с ними числовые наборы совпадают, а двоичные наборы отличаются в последнем элементе. Отметим также, что если с функцией $f_{i,j}$ связаны наборы $v_{i,j} = (\gamma_1 \dots \gamma_j)$ и $w_{i,j} = (p_1 q_1 r_1 \dots p_i q_i r_i \dots p_j q_j r_j)$, то $f_{i,j} = f_{p_1 q_1 r_1 \dots p_i q_i r_i \dots p_j q_j r_j}^{\gamma_1 \gamma_1 \gamma_1 \dots \gamma_i \gamma_i \gamma_i \dots \gamma_j \gamma_j \gamma_j}$.

Через $\tilde{\sigma}_{i_1 i_2 \dots i_q}$ обозначим $(n - q)$ -местный двоичный набор, получающийся из n -местного двоичного набора $\tilde{\sigma} = (\sigma_1, \dots, \sigma_n)$ удалением элементов $\sigma_{i_1}, \sigma_{i_2}, \dots, \sigma_{i_q}$, при этом нумерация элементов, которые не были удалены, не меняется. Например, если $\tilde{\sigma}' = (1_1, 0_2, 0_3, 1_4)$, то $\tilde{\sigma}'_{1,3} = (0_2, 1_4)$, то есть не удаленные нуль и единица, стоявшие в наборе $\tilde{\sigma}'$ в разрядах с номерами 2 и 4 соответственно, в наборе $\tilde{\sigma}'_{1,3}$ также стоят в разрядах 2 и 4. Пусть $\tilde{\sigma}$ — n -местный двоичный набор. Тогда значение $f_{i,j}(\tilde{\sigma}_{w_{i,j}})$, $j \geq 0$, будем называть кратким значением функции $f_{i,j}$ на наборе $\tilde{\sigma}$.

Нетрудно видеть, что при совпадении кратких значений функций-близнецов на наборе $\tilde{\sigma}$, то есть при выполнении равенства $f_{2i-1,j}(\tilde{\sigma}_{w_{2i-1,j}}) = f_{2i,j}(\tilde{\sigma}_{w_{2i,j}})$, в силу монотонности функций, краткое значение функции-предка на наборе $\tilde{\sigma}$, равное $f_{i,j-1}(\tilde{\sigma}_{w_{i,j-1}})$, совпадает с этими значениями.

Для каждого $j = 1, \dots, k$ определим функцию $s_j(x_1, \dots, x_n)$, полагая

$$s_j(\tilde{\sigma}) = \begin{cases} 1 & \text{если } f_{1,j}(\tilde{\sigma}_{w_{1,j}}) = f_{2,j}(\tilde{\sigma}_{w_{2,j}}) = \dots = f_{2^j,j}(\tilde{\sigma}_{w_{2^j,j}}), \\ 0 & \text{в противном случае.} \end{cases}$$

Лемма 5. Если $s_j(\sigma) = 1$, то для функции $f(x_1, \dots, x_n) \in M(n)$ справедливо равенство

$$f(\tilde{\sigma}) = f_{1,j}(\tilde{\sigma}_{w_{1,j}}).$$

Доказательство. Так как $s_j(\tilde{\sigma}) = 1$, краткие значения на наборе $\tilde{\sigma}$ всех функций из множества B_j совпадают:

$$f_{1,j}(\tilde{\sigma}_{w_{1,j}}) = f_{2,j}(\tilde{\sigma}_{w_{2,j}}) = \dots = f_{2^j,j}(\tilde{\sigma}_{w_{2^j,j}}).$$

Функция $f_{i,j-1} \in B_{j-1}$, $i = 1, \dots, 2^{j-1}$, является предком для функций $f_{2i-1,j}$ и $f_{2i,j}$. Значит, верны соотношения

$$f_{i,j-1}(\tilde{\sigma}_{w_{i,j-1}}) = f_{2i-1,j}(\tilde{\sigma}_{w_{2i-1,j}}) = f_{2i,j}(\tilde{\sigma}_{w_{2i,j}}).$$

Отсюда следует, что для функций из множества B_{j-1} справедливы равенства

$$f_{1,j-1}(\tilde{\sigma}_{w_{1,j-1}}) = f_{2,j-1}(\tilde{\sigma}_{w_{2,j-1}}) = \dots = f_{2^{j-1},j-1}(\tilde{\sigma}_{w_{2^{j-1},j-1}}) = f_{1,j}(\tilde{\sigma}_{w_{1,j}}).$$

Таким образом, краткие значения на наборе $\tilde{\sigma}$ функций из множества B_{j-1} совпадают между собой и равны значению $f_{1,j}(\tilde{\sigma}_{w_{1,j}})$. Поэтому справедливы равенства

$$f_{1,j}(\tilde{\sigma}_{w_{1,j}}) = f_{1,j-1}(\tilde{\sigma}_{w_{1,j-1}}) = \dots = f_{1,1}(\tilde{\sigma}_{w_{1,1}}) = f(\tilde{\sigma}).$$

Лемма 5 доказана.

Приступим к построению множеств D_i и A_i , $i = 1, \dots, k$. К множеству A_1 отнесем каждый набор $\tilde{\sigma}$ такой, что $s_1(\tilde{\sigma}) = 1$. Если же $s_1(\tilde{\sigma}) = 0$, то отнесем его к множеству D_1 . Тем самым множество A_0 разбивается на два непересекающихся подмножества D_1 и A_1 . Далее, множество A_1 разобьем на два непересекающихся подмножества D_2 и A_2 . К множеству A_2 отнесем каждый набор $\tilde{\sigma} \in A_1$, для которого $s_2(\tilde{\sigma}) = 1$, в ином случае отнесем его к множеству D_2 . Допустим, что уже построены множества D_{k-1} и $A_{k-1} = A_{k-2} \setminus D_{k-1}$. Снова разобьем множество A_{k-1} на непересекающиеся подмножества A_k и D_k : набор $\tilde{\sigma} \in A_{k-1}$ отнесем к множеству A_k , если $s_k(\tilde{\sigma}) = 1$, если же $s_k(\tilde{\sigma}) = 0$, то отнесем его к множеству D_k . Таким образом строятся множества, входящие в разбиение (7).

Лемма 6. Для каждого множества D_j справедливо неравенство

$$|D_j| \leq 2^{4j-1} \binom{n-3(j-1)}{\lceil (n-3(j-1))/2 \rceil},$$

где $1 \leq j \leq k$.

Доказательство. Докажем, что в множество D_j входит каждый набор $\tilde{\sigma}$, для которого выполнены два условия:

- (1') $s_{j-1}(\tilde{\sigma}) = 1$,
- (2') найдется по крайней мере одна пара функций-близнецов из множества B_j , краткие значения которых на наборе $\tilde{\sigma}$ различны.

Установим равносильность условий (1') и (2') условиям

- (1) $\tilde{\sigma} \in A_{j-1}$ или, что то же самое, $s_{j-1}(\tilde{\sigma}) = 1$,

- (2) $s_j(\tilde{\sigma}) = 0$,

определяющим множество D_j .

Очевидно, достаточно доказать, что из условий (1) и (2) следует условие (2'). Допустим, что условия (1) и (2) выполнены, а условие (2') нет. Последнее означает, что в каждой паре функций-близнецов значения этих функций на наборе $\tilde{\sigma}$ совпадают, то есть для каждого $i = 1, \dots, 2^{j-1}$ выполнено равенство

$$f_{2i-1,j}(\tilde{\sigma}_{w_{2i-1,j}}) = f_{2i,j}(\tilde{\sigma}_{w_{2i,j}}) = \gamma_i,$$

где $\gamma_i \in \{0, 1\}$. Функция $f_{i,j-1}$ является функцией предком для $f_{2i-1,j}$ и $f_{2i,j}$, поэтому $f_{i,j-1}(\tilde{\sigma}_{w_{i,j-1}}) = \gamma_i$. По условию (1) все значения γ_i совпадают между собой, но это не верно по условию (2). Итак, условия (1') и (2') равносильны условиям (1) и (2).

Теперь оценим число наборов в множестве D_j . Из условий (1') и (2') следует, что набор $\tilde{\sigma}$ длины n принадлежит множеству D_j , если $\tilde{\sigma}$ входит в множество A_{j-1} и хотя бы для одного $1 \leq i \leq 2^{j-1}$ выполнено неравенство

$$f_{2i-1,j}(\tilde{\sigma}_{w_{2i-1,j}}) \neq f_{2i,j}(\tilde{\sigma}_{w_{2i,j}}).$$

В силу леммы 4 функции-близнецы $f_{2i-1,j}$ и $f_{2i,j}$ не совпадают не более чем на $\binom{n-3(j-1)}{\lceil (n-3(j-1))/2 \rceil}$ наборах длины $n - 3j$. Поэтому число наборов длины n , на которых не совпадают краткие значения $f_{2i-1,j}(\tilde{\sigma}_{w_{2i-1,j}})$ и $f_{2i,j}(\tilde{\sigma}_{w_{2i,j}})$ этих функций, не превосходит величины $2^{3j} \binom{n-3(j-1)}{\lceil (n-3(j-1))/2 \rceil}$. Отсюда, с учетом того, что число пар функций-близнецов из множества B_j равно 2^{j-1} , следует утверждение леммы 6.

4. Верхняя оценка средней сложности

Теорема 2. Для каждой функции $f \in M(n)$ при $n \rightarrow \infty$ выполнено соотношение

$$T(f) \leq a \frac{2^n}{n^2} (1 + o(1)),$$

где a — некоторая положительная постоянная.

Доказательство. Пусть f — произвольная монотонная функция n переменных. Положим $k = \lceil (1/3) \log n \rceil$. Для f построим множества функций $B_0, B_1, \dots, B_k$ и множества наборов $A_1, \dots, A_k$ и $D_1, \dots, D_k$ таких, что

$$E^n = A_0 = A_k \sqcup D_k \sqcup D_{k-1} \sqcup \dots \sqcup D_1.$$

Программа P , вычисляющая функцию f , имеет вид

$$P = P_0 P_1 \dots P_k.$$

В этой записи программа P_0 по входному набору $\tilde{\sigma}$ выясняет, принадлежит ли он к множеству A_k , и если принадлежит, то вычисляет значение $f(\tilde{\sigma})$ и останавливает вычисления. Каждая программа P_j , $j = 1, \dots, k$, по набору $\tilde{\sigma}$ проверяет его вхождение в множество D_{k-j+1} , и если $\tilde{\sigma} \in D_{k-j+1}$, то определяет значение $f(\tilde{\sigma})$ и останавливает вычисления. Программа P_j , $j = 1, \dots, k$, начинает работу только на тех наборах, на которых не остановились программы $P_0, P_1, \dots, P_{j-1}$, то есть на наборах, не вошедших в множество

$$A_{k-j+1} = A_k \sqcup D_k \sqcup D_{k-1} \sqcup \dots \sqcup D_{k-j+2}.$$

Поэтому для проверки вхождения набора $\tilde{\sigma}$ в множество D_{k-j+1} , с учетом равенства $D_{k-j+1} = A_{k-j} \setminus A_{k-j+1}$, программе P_j достаточно проверить вхождение набора $\tilde{\sigma}$ в множество A_{k-j} .

Итак, каждую программу P_j , $j = 0, 1, \dots, k$, можно записать в виде

$$P_j = P'_j P''_j,$$

где программа P'_j вычисляет величины $f_{i,k-j}(\tilde{\sigma}_{w_{i,k-j}})$, $i = 1, \dots, 2^{k-j}$, являющиеся краткими значениями на наборе $\tilde{\sigma}$ функций $f_{i,k-j} \in B_{k-j}$, программа P''_j , используя уже вычисленные значения $f_{i,k-j}(\tilde{\sigma}_{w_{i,k-j}})$, вычисляет величину $s_{k-j}(\tilde{\sigma})$, потом присваивает выходной ячейке z значение $f_{1,k-j}(\tilde{\sigma}_{w_{1,k-j}})$ и останавливает вычисления, если $s_{k-j}(\tilde{\sigma}) = 1$. Набор $\tilde{\sigma}$ входит в множество A_{k-j} , когда $s_{k-j}(\tilde{\sigma}) = 1$. Поэтому подпрограммы работают корректно: P_0 останавливает вычисления на каждом наборе из A_k , а каждая программа P_j , $j = 1, \dots, k$, — на каждом наборе из D_{k-j+1} , при этом значение выходной ячейки после остановки будет совпадать со значением $f(\tilde{\sigma})$ по лемме 5.

Оценим длину каждой программы P_j , $j = 0, 1, \dots, k$. Учитывая (2) или (3), получим, что для вычисления 2^{k-j} монотонных функций $f_{i,k-j}$ из множества B_{k-j} , зависящих от $n - 3(k - j)$ переменных, программе P'_j достаточно не более

$$2^{k-j} c_1 \frac{2^{n-3(k-j)}}{(n-3(k-j))^{3/2}} (1 + o(1)) = c_1 \frac{2^{n-2(k-j)}}{n^{3/2}} (1 + o(1))$$

команд. Также очевидно, что для каждой программы P''_j выполнено соотношение

$$L(P''_j) = O(2^{k-j}). \quad (8)$$

Поэтому длина программы P_j не превосходит величины

$$c_1 \frac{2^{n-2(k-j)}}{n^{3/2}} (1 + o(1)). \quad (9)$$

Отметим, что если два набора $\tilde{\sigma}$ и $\tilde{\sigma}'$ одновременно принадлежат одному из множеств $A_k, D_k, \dots, D_1$, то для этих наборов выполнено соотношение $T_P(\tilde{\sigma}) = T_P(\tilde{\sigma}')$, а также для каждого $j = 1, \dots, k$ время работы программы P на наборе из множества D_{k-j+1} совпадает с величиной $\sum_{i=0}^j L(P_i)$. Откуда следует, что для средней сложности функции f справедливо неравенство

$$T(f) \leq 2^{-n} \left(\sum_{\tilde{\sigma} \in A_k} L(P_0) + \sum_{j=1}^k \sum_{\tilde{\sigma} \in D_{k-j+1}} \sum_{i=0}^j L(P_i) \right).$$

Отсюда, используя (9) и лемму 6, получим, что

$$\begin{aligned} T(f) &\lesssim \frac{1}{2^n} \left(2^n c_1 \frac{2^{n-2k}}{n^{3/2}} + \sum_{j=1}^k 2^{4(k-j+1)-1} \binom{n-3(k-j)}{\lceil (n-3(k-j))/2 \rceil} \sum_{i=0}^j c_1 \frac{2^{n-2(k-i)}}{n^{3/2}} \right) \\ &\sim \frac{1}{2^n} \left(2^n c_1 \frac{2^{n-2k}}{n^{3/2}} + \sum_{j=1}^k 2^{k-j+3} \binom{n}{\lceil n/2 \rceil} \sum_{i=0}^j c_1 \frac{2^{n-2(k-i)}}{n^{3/2}} \right) \\ &\sim c_1 \frac{2^n}{n^{13/6}} + \frac{1}{2^n} \frac{8c_1 2^n}{n^{3/2}} \binom{n}{\lceil n/2 \rceil} \sum_{j=1}^k 2^{k-j} \sum_{i=0}^j 2^{-2(k-i)} \\ &\lesssim \frac{4}{3} \frac{8c_1}{n^{3/2}} \binom{n}{\lceil n/2 \rceil} \sum_{j=1}^k 2^{-k+j} \lesssim \frac{64c_1}{3n^{3/2}} \binom{n}{\lceil n/2 \rceil}. \end{aligned}$$

Теорема 2 доказана.

5. Нижние оценки средней сложности

Теорема 3. Для почти каждой функции $f \in M(n)$ при $n \rightarrow \infty$ выполнено соотношение

$$T(f) \geq b \frac{2^n}{n^2} (1 + o(1)).$$

где b — некоторая положительная постоянная.

Доказательство. Через $N(L, n)$ обозначим число различных программ, которые содержат не более чем L операторов из $P_2(2)$ и имеют n входов. Из [11] следует справедливость неравенства

$$N(L, n) \leq (c(L+n))^{(4/3)L+n}. \quad (10)$$

Пусть f — монотонная функция от n переменных и P — минимальная программа, вычисляющая f . Каждому двоичному набору $\tilde{\sigma}$ длины n , рассматриваемому как двоичная запись натурального числа, поставим в соответствие такой номер $N_P(\tilde{\sigma})$, что

$1 \leq N_P(\tilde{\sigma}) \leq 2^n$, $N_P(\tilde{\sigma}) < N_P(\tilde{\gamma})$ для любого набора $\tilde{\gamma}$ такого, что $T_P(\tilde{\sigma}) < T_P(\tilde{\gamma})$, $N_P(\tilde{\sigma}) < N_P(\tilde{\gamma})$ для любого $\tilde{\gamma}$ такого, что $T_P(\tilde{\sigma}) = T_P(\tilde{\gamma})$ и $\tilde{\sigma} < \tilde{\gamma}$.

Пусть набор $\tilde{\sigma}_0$ таков, что

$$N_P(\tilde{\sigma}_0) = 2^n - \left\lceil \frac{1}{2} \binom{n}{\lfloor n/2 \rfloor} \right\rceil.$$

Через R_f обозначим множество наборов $\tilde{\sigma}$ таких, что $N_P(\tilde{\sigma}) \leq N_P(\tilde{\sigma}_0)$. Тогда

$$|R_f| = 2^n - \left\lceil \frac{1}{2} \binom{n}{\lfloor n/2 \rfloor} \right\rceil.$$

Таким образом, первые $T_P(\tilde{\sigma}_0)$ команд программы P определяют значения функции f на наборах $\tilde{\sigma}$, входящих в множество R_f .

Оценим мощность множества M' монотонных функций n переменных, у каждой из которых для реализующей ее минимальной программы P выполняется неравенство

$$T_P(\tilde{\sigma}_0) < \frac{3 \binom{n}{\lfloor n/2 \rfloor}}{8 \log \binom{n}{\lfloor n/2 \rfloor}}.$$

Каждая монотонная функция f из M' определяется однозначно первыми $T_P(\tilde{\sigma}_0)$ операторами своей минимальной программы и набором значений длины $\lceil \frac{1}{2} \binom{n}{\lfloor n/2 \rfloor} \rceil$, то есть значениями на тех входных наборах, которые не вошли в множество R_f .

Из неравенства (10) следует, что число различных программ N , чья сложность не больше $T_P(\tilde{\sigma}_0)$, оценивается следующим образом

$$N \leq (c(T_P(\tilde{\sigma}_0) + n))^{(4/3)T_P(\tilde{\sigma}_0) + n}. \quad (11)$$

Отсюда, из несложно доказываемого неравенства $|M(n)| \geq 2^{\binom{n}{\lfloor n/2 \rfloor}}$ и из (11) получим, что мощность множества M' намного меньше числа всех монотонных функций:

$$|M'| \leq 2^A,$$

где

$$A = \left\lceil \frac{1}{2} \binom{n}{\lfloor n/2 \rfloor} \right\rceil + \left(\frac{4}{3} \frac{3 \binom{n}{\lfloor n/2 \rfloor}}{8 \log \binom{n}{\lfloor n/2 \rfloor}} + n \right) \log_2 \left(c \left(\frac{3 \binom{n}{\lfloor n/2 \rfloor}}{8 \log \binom{n}{\lfloor n/2 \rfloor}} + n \right) \right),$$

так что

$$|M'| = o(|M(n)|).$$

Поэтому, каждая минимальная программа P почти каждой функции из $M(n)$ удовлетворяет следующему условию: если

$$N_P(\tilde{\sigma}_0) = 2^n - \left\lceil \frac{1}{2} \binom{n}{\lfloor n/2 \rfloor} \right\rceil,$$

то

$$T_P(\tilde{\sigma}_0) \geq \frac{3 \binom{n}{\lfloor n/2 \rfloor}}{8 \log \binom{n}{\lfloor n/2 \rfloor}}.$$

Пусть

$$W = \{\bar{\sigma} \mid N_P(\bar{\sigma}) \geq N_P(\bar{\sigma}_0)\}.$$

Тогда для среднего времени работы $T(P)$ каждой программы P , удовлетворяющей приведенному выше условию, справедливы соотношения

$$\begin{aligned} T(P) &= 2^{-n} \sum_{\bar{\sigma} \in \{0,1\}^n} T_P(\bar{\sigma}) > 2^{-n} \sum_{\bar{\sigma} \in W} T_P(\bar{\sigma}) \geq 2^{-n} T_P(\bar{\sigma}_0) |W| \\ &\geq 2^{-n} \frac{3 \binom{n}{\lfloor n/2 \rfloor}}{8 \log \binom{n}{\lfloor n/2 \rfloor}} \frac{1}{2} \binom{n}{\lfloor n/2 \rfloor} \geq \frac{3}{8\pi} \frac{2^n}{n^2} (1 + o(1)). \end{aligned}$$

Теорема 3 доказана.

Список литературы

1. Андреев А. Е., Синтез схем из функциональных элементов в полных монотонных базисах. *Матем. вопросы киберн.* (1985) **1**, 114–139.
2. Коробков В. К., О монотонных функциях алгебры логики. *Пробл. киберн.* (1965) **13**, 5–28.
3. Коршунов А. Д., О числе монотонных булевых функций. *Пробл. киберн.* (1965) **38**, 5–108.
4. Лупанов О. Б., Об одном подходе к синтезу управляющих систем — принципе локального кодирования. *Пробл. киберн.* (1965) **14**, 31–110.
5. Нечипорук Э. И., О вентильных схемах. В сб.: *Тезисы докл. Международного симпозиума по теории релейных схем и конечных автоматов*. Москва, 1962, с. 42–43.
6. Редькин Н. П., О реализации монотонных булевых функций контактными схемами. В сб.: *Тезисы докл. 4-й Всесоюзной конференции по проблемам теоретической кибернетики*. Новосибирск, 1977, с. 180–181.
7. Редькин Н. П., О реализации монотонных булевых функций схемами из функциональных элементов. *Пробл. киберн.* (1979) **36**, 87–110.
8. Резник В. И., О реализации монотонных функций схемами из функциональных элементов. *ДАН СССР* (1961) **139**, №3, 566–569.
9. Угольников А. Б., О реализации монотонных функций схемами из функциональных элементов. *Пробл. киберн.* (1976) **31**, 167–185.
10. Чашкин А. В., О среднем времени вычисления значений булевых функций. *Дискретный анализ и исследование операций* (1997) **3**, №1, 60–78.
11. Чашкин А. В., Об одном методе вычисления частичных булевых функций. *Матем. вопросы киберн.* (2004) **12**, 231–246.
12. Чашкин А. В., О сложности реализации булевых функций формулами. *Дискретный анализ и исследование операций* (2005) **12**, № 2, 75–91.
13. Яблонский С. В., О классах функций алгебры логики, допускающих простую схемную реализацию. *Успехи матем. наук* (1957) **12**, №6, 189–196.
14. Hansel G., Sur le nombre des fonctions booléennes monotones de n variables. *C. R. Acad. Sci. Paris* (1966) **262**, 1088–1099.
15. Kleitman D., On Dedekind's problem: the number of monotone Boolean functions. *Proc. Amer. Math. Soc.* (1969) **21**, №3, 677–682.
16. Pippenger N., The complexity of monotone-boolean functions. *Math. Syst. Theory* (1978) **11**, 289–316.

Статья поступила 12.05.2005.