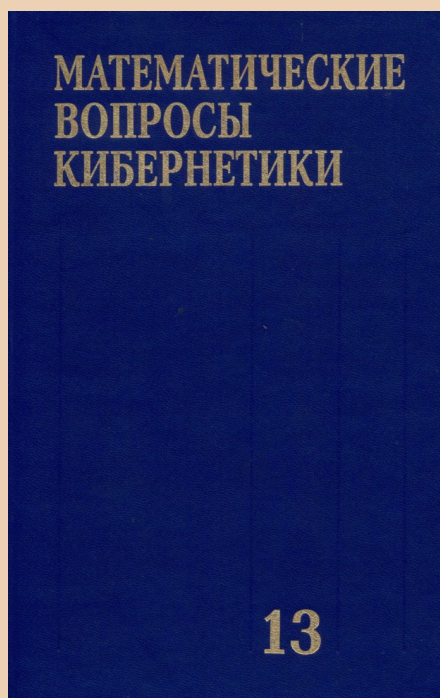




А. В. Кондратов

**Асимптотические
оценки высокой
степени точности для
сложности реализации
функций, связанных с
автоматными
языками, в некоторых
классах схем**

Рекомендуемая форма библиографической ссылки:
Кондратов А. В. Асимптотические оценки высокой степени точности для сложности реализации функций, связанных с автоматными языками, в некоторых классах схем // Математические вопросы кибернетики. Вып. 13. — М.: ФИЗМАТЛИТ, 2004. — С. 279–288. URL: <http://library.keldysh.ru/mvk.asp?id=2004-279>

АСИМПТОТИЧЕСКИЕ ОЦЕНКИ ВЫСОКОЙ СТЕПЕНИ ТОЧНОСТИ ДЛЯ СЛОЖНОСТИ РЕАЛИЗАЦИИ ФУНКЦИЙ, СВЯЗАННЫХ С АВТОМАТНЫМИ ЯЗЫКАМИ, В НЕКОТОРЫХ КЛАССАХ СХЕМ *)

А. В. КОНДРАТОВ

(МОСКВА)

§ 1. Введение

Одна из основных задач математической кибернетики — задача синтеза управляющих систем, — сформулирована С. В. Яблонским в [7]. В общем виде эта задача ставится следующим образом. Имеется некоторый класс схем (контактные схемы, схемы из функциональных элементов, формулы и т. п.), с помощью которых можно реализовать любую функцию алгебры логики (ФАЛ). Сложность схемы характеризуется, обычно, числом элементов, ее составляющих, а под сложностью ФАЛ понимается минимальная из сложностей схем, реализующих эту функцию [5]. Задача синтеза сводится, как правило, либо к изучению сложности отдельных ФАЛ, либо к оценке т. н. функции Шеннона, которая зависит от натурального аргумента n и определяется как максимальная из сложностей ФАЛ от n переменных.

Напомним, что К. Шеннон [10] установил порядок роста функции Шеннона для сложности контактных схем, а О. Б. Лупанов (см., например, [5]) получил асимптотику функций Шеннона для сложности реализации ФАЛ во всех основных классах схем (контактные схемы, схемы из функциональных элементов, формулы, релейно-контактные схемы). В [2, 4] С. А. Ложкин уточнил оценки остаточного члена асимптотического разложения для некоторых функций Шеннона и в целом ряде случаев получил т. н. оценки высокой степени точности, в которых установлена асимптотика второго члена указанного разложения.

В дальнейшем оценки высокой степени точности были получены также для функций Шеннона, связанных с реализацией ФАЛ из некоторых специальных классов. Так в [3] были установлены асимптотические оценки высокой степени точности для сложности реализации функций, связанных с автоматными языками, в классах схем из функциональных элементов и ориентированных контактных схем.

В данной работе получены асимптотические оценки высокой степени точности для сложности реализации функций, связанных с автоматными языками, в определяемом далее классе схем, являющимся расширением класса ориентированных контактных схем.

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 02-01-01110).

§ 2. Основные определения и описание полученных результатов

Положим $B = \{0, 1\}$, и пусть B^* — множество всех слов, включая и пустое слово Λ , составленных из символов элементов множества B . Напомним [9], что языком A называется любое непустое конечное или бесконечное подмножество множества B^* . Для языка A через $A(s)$ обозначим множество слов из A длины не больше s , $s = 1, 2, \dots$, и определим следующую последовательность, характеризующую «мощность» этого языка,

$$\sigma_A(s) = \frac{\log |A(s)|}{s}.$$

Так как язык не пустой, то последовательность $\sigma_A(s)$ будет определена при любом s , большем некоторого s_0 , и при этом, очевидно, что $0 \leq \sigma_A(s) \leq 1$. Язык A будем называть *регулярным*, если существует предел

$$\lim_{s \rightarrow \infty} \sigma_A(s) = \sigma_A.$$

Определим *замыкание* языка A относительно операции взятия подслов как множество тех слов из B^* , которые являются подсловами слов из A , и будем обозначать это множество через $\hat{A}$. Язык A называется *замкнутым*, если $A = \hat{A}$. Пусть A — автоматный язык (см. [1]), т. е. язык, состоящий из всех тех слов в алфавите B , которые переводят заданный конечный автомат $\mathcal{A}$ из начального состояния в одно из его заключительных состояний. Из [9] вытекает следующая лемма.

Лемма 1. *Любой автоматный язык A является регулярным, и в случае $\sigma_A > 0$ имеет место равенство:*

$$|A(s)| = 2^{\sigma_A \cdot s + O(1)}. \quad (1)$$

Пусть A — автоматный язык с параметром $\sigma_A > 0$, который задается автоматом $\mathcal{A}$. Через $Q_A(n)$ обозначим множество тех ФАЛ от булевских переменных (БП) $x_1, \dots, x_n$, столбец значений которых является словом из $\hat{A}$, и определим класс *автоматных ФАЛ*, или, иначе, класс *ФАЛ порождаемых автоматом $\mathcal{A}$* , как последовательность $Q_A = Q_A(1), \dots, Q_A(n), \dots$.

В работе [4] был определен класс функционально проводящих схем — класс схем, построенных из функционально проводящих элементов (ФПЭ), — который обобщает многие известные классы схем [5, 6], реализующих ФАЛ. В данной работе будет рассмотрен некоторый специальный частный случай этих схем.

Схемы строятся из элементов конечного базиса B , $B = \{\mathcal{E}_i\}$, $i = 1, \dots, r$, где ФПЭ $\mathcal{E}_i$ имеет $k_i + 2$ полюсов, пронумерованных числами $0, 1, \dots, k_i + 1$. Полюс с номером 0 называется *выходом* или *стоком*, а полюс с номером j , $1 \leq j \leq k_i + 1$, — j -м *входом* элемента $\mathcal{E}_i$. Вход с номером $k_i + 1$ называется *истоком* или *проводящим входом*, а остальные входы — *управляющими входами*. Элементу $\mathcal{E}_i$ сопоставляется ФАЛ φ_i , существенно зависящая от переменных $x_1, \dots, x_{k_i}$, где переменная x_j связана с j -м входом $\mathcal{E}_i$, и положительное действительное число p_i , называемое *весом* элемента $\mathcal{E}_i$ и характеризующее его сложность. Упорядоченная пара (u, v) , где u — j -й вход, а v — выход $\mathcal{E}_i$, называется j -м *каналом* элемента $\mathcal{E}_i$. Канал с номером $k_i + 1$ называется *проводящим каналом*, а остальные — *управляющими каналами* $\mathcal{E}_i$. Считается, что проводящий канал элемента $\mathcal{E}_i$ *открыт на наборе α* значений переменных $x_1, \dots, x_{k_i}$, если $\varphi_i(\alpha) = 1$. Предполагается, что в этом случае по нему имеет место проводимость от истока к стоку. Можно считать, что ФПЭ $\mathcal{E}_i$ состоит из функционального элемента E_i , реализующего

ФАЛ φ_i , выход которого «управляет» проводимостью ориентрованного контакта K_i (см. рис. 1).

Класс S_B^Π определяется подобно классу $S_B^{\Phi\Pi}$ из [4], только на структуру схемы накладываются некоторые дополнительные ограничения. Будем считать, что каждому элементу $\mathcal{E}_i$ сопоставлено число k'_i , $0 \leq k'_i \leq k_i$, и что первые k'_i входов являются *прямыми входами*, которые при построении схемы могут присоединяться только к входам схемы, а остальные — *итеративными входами* $\mathcal{E}_i$. При изучении класса S_B^Π предполагается, что в базисе B имеются так называемые замыкающий и размыкающий контакты, т. е. элементы с прямым входом x_1 , которым сопоставлены функции x_1 и $\bar{x}_1$ соответственно. В этом случае класс S_B^Π является, очевидно, полным. Для $i = 1, \dots, r$ положим

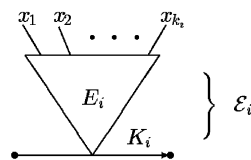


Рис. 1

$$\pi_i = \frac{p_i}{k_i - k'_i + 1}, \quad \Theta_i = \frac{2k_i - 3k'_i + 3}{k_i - k'_i + 1},$$

и пусть

$$\pi_B = \min_{1 \leq i \leq r} \pi_i, \quad \Theta_B = \min_{\pi_i = \pi_B} \Theta_i.$$

Схема Σ принадлежит классу S_B^K , если она строится из ФПЭ таким образом, что на управляющие входы всех ее элементов поступают только входные переменные, а контакты этих элементов образуют ориентированную ациклическую контактную схему с одним входом. Схема Σ принадлежит классу S_B^Π , если она состоит из двух подсхем Σ_1 и Σ_2 , принадлежащих классу S_B^K , но при этом во второй подсхеме Σ_2 (она может быть пустой) на итеративные входы ее элементов могут поступать как входные переменные, так и выходы схемы Σ_1 . Выходами схемы Σ могут быть как выходы схемы Σ_2 , так и выходы схемы Σ_1 . Заметим, что Σ является ациклической схемой, в которой никакая цепочка из последовательно соединенных элементов не может содержать два и более переходов от выхода одного элемента к итеративному входу следующего элемента.

Под *сложностью* $L(\Sigma)$ схемы Σ над базисом B понимается, как обычно, сумма весов всех ее элементов, а *сложность* $L_B^\Pi(f)$ функции f в классе S_B^Π определяется как минимальная из сложностей схем Σ , $\Sigma \in S_B^\Pi$, реализующих f . Для $n = 1, 2, \dots$ обозначим через $P_2(n)$ множество всех ФАЛ от переменных $x_1, x_2, \dots, x_n$, а для класса ФАЛ Q , т. е. последовательности $Q(1), \dots, Q(n), \dots$, где $Q(n) \subset P_2(n)$, введем функцию Шеннона

$$L_B^\Pi(Q(n)) = \max_{f \in Q(n)} L_B^\Pi(f).$$

Основным результатом данной работы является доказательство следующей теоремы.

Теорема. Пусть базис $\hat{B}$ состоит из ФПЭ $\mathcal{E}$ с весом p и функцией проводимости $\varphi(x_1, x_2, \dots, x_k) = x_1^\sigma \bar{\varphi}(x_2, \dots, x_k)$, где x_1 — прямая, а $x_2, \dots, x_k$ — итеративные переменные, а также из обычных замыкающего и размыкающего контактов с весом $p' > p/k$. Тогда для любого автоматного класса ФАЛ Q_A , где $\sigma_A > 0$, справедлива следующая оценка

$$L_B^\Pi(Q_A(n)) = \pi_B \frac{2^n \cdot \sigma_A}{n} \left(1 + \frac{2 \log n}{n} + O\left(\frac{1}{n}\right) \right).$$

§ 3. Нижняя мощностная оценка для рассматриваемой функции Шеннона

Пусть A — язык, задаваемый автоматом $\mathcal{A}$. Тогда через $\mathcal{A}_{ij}$ обозначим автомат, получающийся из исходного автомата $\mathcal{A}$ путем принятия i -й вершины за начальное состояние, а j -й вершины — за заключительное состояние, где i -я вершина достижима из начального состояния, j -я вершина достижима из i -й вершины, а из j -й вершины достижимо одно из заключительных состояний. Пусть A_{ij} — язык, задаваемый автоматом $\mathcal{A}_{ij}$, тогда $\hat{A} = \bigcup A_{ij}$, где объединение берется по всем i и j , удовлетворяющим приведенным выше условиям. Учитывая данное представление для языка $\hat{A}$, из [1] получаем, что $\hat{A}$ является автоматным языком.

Лемма 2. Для любого автоматного языка A справедливо следующее равенство: $\sigma_A = \sigma_{\hat{A}}$.

Доказательство. Из равенства $\hat{A} = \bigcup A_{ij}$ следует, что $\sigma_A \leq \sigma_{\hat{A}}$. Далее заметим, что

$$\sigma_{\hat{A}}(s) \leq \frac{(\log \sum_{ij} |A_{ij}|)}{s} = \frac{\log(\sum_{ij} |2^{\sigma_{A_v} s + O(1)}|)}{s} = \max_{ij} \sigma_{A_v} + \frac{O(1)}{s}.$$

Если перейти к пределу при s стремящемся к бесконечности, то получим неравенство $\sigma_{\hat{A}} \leq \max \sigma_{A_v}$. Теперь заметим, что в силу ограничений, наложенных на вершины i и j , существуют два таких слова β' и β'' , что из принадлежности слова α языку A_{ij} следует, что слово $\beta = \beta' \alpha \beta''$ принадлежит языку A . Значит

$$|A_{ij}(s)| \leq |A(s+d)|,$$

где d — сумма длин слов β' и β'' . Из этого неравенства следует, что

$$\sigma_{A_v}(s) = \frac{\log |A_{ij}(s)|}{s} \leq \frac{\log |A(s+d)|}{s} = \sigma_A(s+d) \frac{s+d}{s}.$$

Перейдя к пределу, получим, что $\sigma_{A_v} \leq \sigma_A$. Так как это неравенство верно для любого A_{ij} , то $\max \sigma_{A_v} \leq \sigma_A$. Объединив это неравенство с полученными выше неравенствами ($\sigma_A \leq \sigma_{\hat{A}}$ и $\sigma_{\hat{A}} \leq \max \sigma_{A_v}$), получим, что

$$\max \sigma_{A_v} \leq \sigma_A \leq \sigma_{\hat{A}} \leq \max \sigma_{A_v},$$

и значит $\sigma_A = \sigma_{\hat{A}}$. Лемма доказана.

Учитывая (1), получаем

С л е д с т в и е.

$$|Q_A(n)| = 2^{\sigma_A 2^n + O(1)}. \quad (2)$$

Рассмотрим итерацию [1] языка A , т. е. язык A^* , в который входят любые цепочки слов из языка A . Заметим, что $\sigma_{A^*} \geq \sigma_A$ и что существуют [9] языки, для которых $\sigma_{A^*} > \sigma_A$. Если A — автоматный язык, то из [1] следует, что язык A^* тоже является автоматным.

Теперь приступим к получению нижней оценки теоремы. Схему Σ , $\Sigma \in S_B^\Pi$, будем называть *минимальной* в классе S_B^Π , если для любой эквивалентной ей схемы Σ' , $\Sigma' \in S_B^\Pi$, справедливо неравенство $L(\Sigma') \geq L(\Sigma)$, причем в случае $L(\Sigma') = L(\Sigma)$ число вершин Σ' не меньше, чем число вершин Σ . Обозначим через $S_B^\Pi(L, n)$ максимальное по включению множество попарно не эквивалентных минимальных схем Σ из класса S_B^Π , функционирование которых описывается одной ФАЛ, зависящей от переменных $X(n)$, $X(n) = \{x_1, \dots, x_n\}$, и для которых $L(\Sigma) \leq L$. Нижняя оценка функции

Шеннона $L_B^\Pi(Q_A(n))$ выводится, учитывая (2), из обычного мощностного неравенства

$$|S_B^\Pi(L_B^\Pi(Q_A(n)), n)| \geq 2^{\sigma_A \cdot 2^n + O(1)}. \quad (3)$$

Для этого используется верхняя оценка величины $|S_B^\Pi(L, n)|$ из леммы 21 работы [2], из которой следует, что в случае $\frac{1}{2}n \leq \log L \leq 2n$ выполняется неравенство

$$|S_B^\Pi(L, n)| \leq (c_1 L n^{1-\Theta_B})^{L/\pi_B}, \quad (4)$$

где c_1 — некоторая константа*), а π_B и Θ_B — определенные в § 2 параметры базиса.

Из (3) и (4) обычным образом получается нижняя оценка для функции Шеннона $L_B^\Pi(Q_A(n))$:

$$L_B^\Pi(Q_A(n)) \geq \pi_B \frac{\sigma_A 2^n}{n} \left(1 + \frac{\Theta_B \log n}{n} + O\left(\frac{1}{n}\right) \right). \quad (5)$$

Нижняя оценка теоремы вытекает из (5) в силу того, что $\Theta_B = 2$ и $\pi_B = p/k$.

§ 4. Построение универсальных матриц для рассматриваемого класса функций

Число строк (столбцов) матрицы будем называть ее *высотой* (соответственно, *длиной*). Матрицу, элементы которой принадлежат множеству Q , будем называть *матрицей над Q* , а множество всех матриц длины n и высоты s над множеством Q будем обозначать через $Q^{s,n}$. Результатом конкатенации матриц одинаковой высоты U' и U'' назовем матрицу U , $U = U' \cdot U''$, которая получается в результате приписывания столбцов матрицы U'' после столбцов матрицы U' . Для матрицы M' , $M' \in B^{n,l}$ и ФАЛ φ , $\varphi = \varphi(y_1, \dots, y_l)$ через $\varphi(M')$ будем обозначать столбец β , $\beta \in B^{n,1}$, получающийся в результате построчного применения φ к M' . Через M^T будем обозначать матрицу, транспонированную по отношению к матрице M .

Матрица M , $M \in B^{n,m}$, называется *универсальной матрицей относительно ФАЛ φ* , $\varphi = \varphi(y_1, \dots, y_l)$, для множества столбцов $\mathfrak{J}$, $\mathfrak{J} \subset B^{n,1}$, если для любого столбца β , $\beta \in \mathfrak{J}$, существует матрица M' , $M' \in B^{n,l}$, составленная из столбцов матрицы M и такая, что $\varphi(M') = \beta$. Универсальную относительно ФАЛ φ матрицу будем называть также *φ -универсальной матрицей* (φ -УМ).

Рассмотрим матрицу $\mu_A(s)$ высоты s , в которой перечислены все столбцы, являющиеся словами длины s из $\hat{A}(s)$. Из леммы 1 вытекает, что длина матрицы $\mu_A(s)$ равна $2^{\sigma_A s + O(1)}$. Легко видеть, что матрица $\mu_A(s)$ является φ -УМ, где $\varphi \equiv x$, для множества столбцов высоты s из $\hat{A}(s)$, так как любой такой столбец содержится среди столбцов $\mu_A(s)$.

Приступим теперь к построению специальной схемы, которая будет использоваться при доказательстве основной теоремы, и оценке ее параметров. Возьмем s элементов $\mathcal{E}$ базиса $\hat{B}$ и построим из них схему $\mathcal{E}^{(s)}$ так, как это показано на рис. 2, где на управляющие входы i -го элемента $\mathcal{E}$

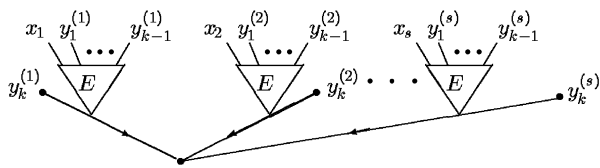


Рис. 2

*) Буквой c с различными индексами будем обозначать константы, зависящие от базиса (класса схем).

поступает прямая БП x_i , $(k-1)$ итеративных БП $y_1^{(i)}, \dots, y_{k-1}^{(i)}$ и еще одна итеративная БП $y_k^{(i)}$ подается на исток контакта этого элемента $\mathcal{E}$.

Напомним, что функция проводимости i -го элемента $\mathcal{E}$ имеет вид:

$$\varphi(x_i, y_1^{(i)}, \dots, y_{k-1}^{(i)}) = x_i^\sigma \widehat{\varphi}(y_1^{(i)}, \dots, y_{k-1}^{(i)}), \quad i = 1, \dots, s, \quad (6)$$

и поэтому схема $\mathcal{E}^{(s)}$ реализует функцию

$$\Phi_{k,s}(Y_1, Y_2) = \bigvee_{i=1}^s x_i \widehat{\varphi}(Y^{(i)}) y_k^{(i)}, \quad (7)$$

где $Y^{(i)} = \{y_1^{(i)}, \dots, y_{k-1}^{(i)}\}$, $Y_1 = \bigcup_{i=1}^s Y^{(i)}$, $Y_2 = \{x_1, \dots, x_s\}$.

Лемма 3. Для определенной выше функции $\Phi_{k,s}$ и для любого натурального s_1 такого, что $s_1 > \log(ks)$, можно построить $\Phi_{k,s}$ -универсальную для множества $\widehat{A}(h)$ матрицу $U = U^{(1)}U^{(2)}$, где $U^{(1)} \in B^{h, \Theta_1}$, $U^{(2)} \in B^{h, \Theta_2}$ и выполнены следующие соотношения

$$\Theta_1 \leq 2^{\sigma_A s_1 + O(1)}, \quad \Theta_2 = s, \quad h \geq ks(s_1 - \log k).$$

Если при этом столбцы матрицы $U^{(1)}$ рассматривать как столбцы значений функций от m БП, то сложность реализации этой системы ФАЛ в классе S_B^K не превосходит

$$c_2 \Theta_1 + O(2^m \cdot k \cdot 2^{\sigma_A s_1/2 + O(1)}),$$

где $m \geq \log h$, а c_2 — константа, зависящая от базиса.

Доказательство. На основе лемм 5 и 6 из работы [4], построим $\Phi_{k,s}$ -универсальную матрицу U , $U \in B^{h, \Theta_1 + \Theta_2}$, вида $U = U^{(1)}U^{(2)}$, где матрицы $U^{(1)}$ и $U^{(2)}$ показаны на рис. 3. Матрица $U^{(1)}$ строится на основе леммы 5 из [4]. Пусть D — разбиение множества Y_1 на компоненты $Y_v = \{y_v^{(1)}, \dots, y_v^{(s)}\}$, $|Y_v| = s$, $v = 1, \dots, k$. Выберем четное число d , которое удовлетворяет условию

$$s_1 - \log k \leq d < s_1 - \log k + 2$$

и в силу $s_1 > \log(ks)$ является положительным числом. Для всех i , $i = 1, \dots, k$, и j , $j = 1, \dots, ks$, обозначим через $W_j^{(i)}$ такую матрицу длины $2^{\sigma_A d + O(1)}$ и высоты d , где $y_j \in Y_v$, которая совпадает с $\mu_A(d)$, если $i = v$, и является константным блоком, если $i \neq v$. Константные блоки выбираются таким образом, чтобы при подаче связанных с ними переменных на вход функции $\Phi_{k,s}$ она принимала вид $\Phi_{k,s}(Y_v, Y_2) = \bigvee_{i=1}^s x_i y_v^{(i)}$. Это возможно в силу того, что функция φ (функция проводимости элемента $\mathcal{E}$) существенно зависит от всех своих переменных и особенности строения схемы $\mathcal{E}^{(s)}$ (схема строится из s одинаковых элементов $\mathcal{E}$). Для всех i , $i = 1, \dots, k$, и j , $j = 1, \dots, ks$, положим

$$W_j = \prod_{v=1}^k W_j^{(v)}, \quad W^{(i)} = \left[\prod_{u=1}^{ks} [W_u^{(i)}]^T \right]^T,$$

и тогда

$$U^{(1)} = \prod_{i=1}^k W^{(i)} = \left[\prod_{j=1}^{ks} [W_j]^T \right]^T.$$

Матрицу W_j (матрицу $W^{(i)}$) будем считать горизонтальной (соответственно, вертикальной) полосой матрицы $U^{(1)}$, связанной с переменной y_j

(соответственно, с компонентой Y_i) функции $\Phi_{k,s}$. Легко видеть, что $U^{(1)} \in B^{h, \Theta_1}$, где

$$\Theta_1 = \sum_{v=1}^k 2^{\sigma_A \sigma_d + O(1)} \leq 2^{\sigma_A s_1 + O(1)}, \quad h = \sum_{v=1}^k sd \geq ks(s_1 - \log k).$$

В силу четности числа σ_d четная и нечетная компоненты матрицы $U^{(1)}$ (матрицы, получающиеся из исходной вычеркиванием всех строк с четными (нечетными) номерами) совпадают с точностью до перестановки столбцов, среди которых имеется не более $k 2^{\sigma_A s_1/2 + O(1)}$ различных. Матрица $U^{(2)}$, учитывая (6), берется специального диагонального вида (см. рис. 3).

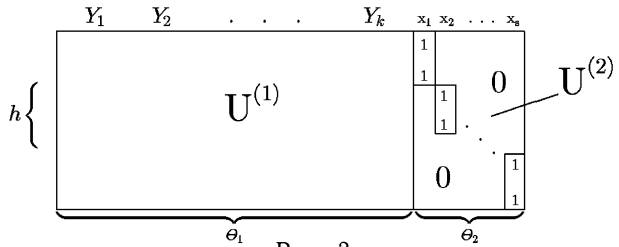


Рис. 3

Из построения следует, что матрица U является $\Phi_{k,s}$ -универсальной для множества $\hat{A}(h)$, а ее размеры удовлетворяют требуемым оценкам.

Далее будем реализовывать построенную матрицу $U^{(1)}$. Пусть столбец матрицы $U^{(1)}$ является некоторой функцией f от m переменных, разложим эту функцию по последней переменной

$$f = x_m g' \vee \bar{x}_m g''. \quad (8)$$

Соберем все столбцы матрицы M и реализуем их в соответствии с (8): возьмем функционально-проводящие элементы, реализующие функции x и $\bar{x}^*$, функции g' и g'' реализуем аналогично методу каскадов (см., например, [5]) со сложностью $O(2^m)$. Величина $k \cdot 2^{\sigma_A s_1/2 + O(1)}$ возникает в силу выбора функций g' и g'' (как было замечено при построении, четная и нечетная компоненты матрицы $U^{(1)}$ совпадают с точностью до перестановки столбцов, среди которых имеется не более $k 2^{\sigma_A s_1/2 + O(1)}$ различных). Лемма полностью доказана.

§ 5. Верхние оценки и поведение рассматриваемой функции Шеннона

В работе [2] была введена операция сложения для слов разной длины. Через B^n будем обозначать единичный n -мерный куб. Для слова (набора) α , $\alpha \in B^*$, через $\lambda(\alpha)$ будем обозначать его длину. Для слов α , $\alpha = \alpha_1 \dots \alpha_n$, и β , $\beta = \beta_1 \dots \beta_n$, из B^n обозначим через $\alpha \oplus \beta$ слово $(\alpha_1 \oplus \beta_1) \dots (\alpha_n \oplus \beta_n)$, через $sort(\alpha, \beta)$ — слово, получающееся из β вычеркиванием тех букв β_j , $j = 1, \dots, n$, для которых $\alpha_j = 0$, а через $\alpha]_m$ — слово, состоящее из m первых букв α . Определим сумму $\alpha \oplus \beta$ для произвольных слов α и β из B^* следующим образом:

- 1) $\alpha \oplus \beta = \alpha]_{\lambda(\beta)} \oplus \beta$, если $1 \leq \lambda(\beta) \leq \lambda(\alpha)$;
- 2) $\alpha \oplus \beta = \beta$;
- 3) $\alpha \oplus \beta = (\alpha \oplus \beta') \cdot (sort(\beta', \alpha) \oplus \beta'')$, если $1 \leq \lambda(\alpha) \leq \lambda(\beta)$,
где $\beta' = \beta]_{\lambda(\alpha)}$ и $\beta = \beta' \cdot \beta''$.

Сумму $M \oplus \alpha$, где $M \in B^{s,m}$, $\alpha \in B^n$, определим как матрицу, i -я строка которой, $i = 1, 2, \dots, s$, получается в результате сложения i -й строки матрицы M с набором α . Особенность операции $M \oplus \alpha$ заключается [2] в том, что любой столбец матрицы $M \oplus \alpha$ либо совпадает с некоторым столбцом

*) См. определение базиса $\hat{B}$ в § 2.

из матрицы M , либо является его отрицанием, и что если в α число 0 не меньше длины матрицы M , то в матрице $M \oplus \alpha$ есть подматрица вида M .

Множество наборов, состоящее из различных строк матрицы M , будем называть ее *базовым множеством*. Базовое множество матрицы M будем обозначать через $\widetilde{M}$, а под базовым множеством $\widetilde{\mathfrak{B}}$ системы $\mathfrak{B}$, состоящей из матриц одинаковой длины, будем понимать объединение их базовых множеств. Матрицы M', M'' над B длины n будем называть *ортогональными*, если $\widetilde{M'} \cap \widetilde{M''} = \emptyset$. Матрицу, все строки которой различны, будем называть *отделимой матрицей*. Систему $\mathfrak{B}$, состоящую из матриц над B длины n , будем называть *отделимой*, если она состоит из попарно ортогональных отделимых матриц, и *полной*, если $\widetilde{\mathfrak{B}} = B^n$. Из работы [4] вытекает следующая лемма.

Лемма 4. Пусть $U \in B^{s,m}$, а W — отделимая матрица из $B^{s,t}$. Тогда система $\mathfrak{B}$ матриц $M_\beta, M_\beta = (U \oplus \beta) \cdot W$, где $\beta \in B^n$, является отделимой, причем $\widetilde{\mathfrak{B}} = B^n \times \widetilde{W}$.

Теперь, когда приведены все необходимые вспомогательные результаты, приступим к доказательству верхней оценки основной теоремы.

Лемма 5. Для сложности реализации автоматных функций в классе S_B^Π справедлива следующая оценка

$$L_B^\Pi(Q_A(n)) \leq \pi_B \frac{2^n \sigma_A}{n} \left(1 + \frac{2 \log n}{n} + O\left(\frac{1}{n}\right) \right).$$

Доказательство. Будем применять технику, подобную используемой в работе [4] при доказательстве леммы 8. Возьмем произвольную функцию $f(\tilde{x})$, где $\tilde{x} = (x_1, \dots, x_n)$, и построим схему $\Sigma_f, \Sigma_f \in S_B^\Pi$, которая реализует f с нужной нам сложностью. Как было определено в (7), схема $\mathcal{E}^{(s)}, \mathcal{E}^{(s)} \in S_B^\Pi$ реализует функцию $\Phi_{k,s}(Y_1, Y_2)$. Наложим на натуральные параметры s, s_1 и q следующие ограничения

$$s_1 > \log ks, \quad 4s \leq n - q, \quad 2^q \leq ks(s_1 - \log k), \quad (9)$$

а их точные значения подберем в конце доказательства.

Из леммы 3 и выбора q следует, что существует $\Phi_{k,s}(Y_1, Y_2)$ -универсальная матрица $U, U \in B^{2^q, \Theta}$, вида

$$U = U^{(1)} U^{(2)}, \quad U^{(1)} \in B^{2^q, \Theta_1}, \quad U^{(2)} \in B^{2^q, s}, \quad \Theta_1 \leq 2^{\sigma_A \cdot s_1 + O(1)}. \quad (10)$$

Пусть a — натуральный параметр такой, что

$$n - q - a \geq 3 \cdot s, \quad (11)$$

и пусть $b = n - q - a$. Разобьем переменные $\tilde{x}$ на три группы:

$$\begin{aligned} \tilde{v} &= (v_1, \dots, v_a) = (x_1, \dots, x_a), \\ \tilde{u} &= (u_1, \dots, u_b) = (x_{a+1}, \dots, x_{a+b}), \\ \tilde{w} &= (w_1, \dots, w_q) = (x_{a+b+1}, \dots, x_n). \end{aligned}$$

Для каждого $\beta, \beta \in B^b$, положим $M_\beta = (U^{(2)} \oplus \beta)W$, где W — матрица, составленная из всех подряд идущих строк длины q , и пусть $\mathfrak{B} = \{M_\beta\}_{\beta \in B^b}$. Будем считать, что

$$X(W) = \tilde{w}, \quad X(U^{(2)}) = \tilde{u},$$

а переменные из множества $X(U^{(1)})$ будем рассматривать как функции от переменных $\tilde{w}$, столбцами значений которых являются соответствующие столбцы матрицы $U^{(1)}$. Обозначим через G множество различных функций $g_i, i = 1, \dots, \Theta_1$, от переменных $\tilde{w}$, соответствующих столбцам $U^{(1)}$.

Из леммы 4 следует, что система $\mathfrak{B}$ является отделимой полной системой матриц для куба B^{b+q} . Обозначим через $\mathcal{R}$ множество всех наборов куба B^b с не менее чем s нулями. В силу (11) получаем, что

$$|B^b \setminus \mathcal{R}| \leq e_1^b 2^b,$$

где $e_1 < 1$.

Для каждого σ , $\sigma = (\sigma_1, \dots, \sigma_s)$, $\sigma \in B^s$, положим

$$\Phi_\sigma(Y_1, Y_2) = \Phi_{k,s}(Y_1, Y_2 \oplus \sigma).$$

Легко видеть, что в классе S_B^Π функцию Φ_σ можно реализовать схемой E_σ , которая при $\sigma = 0^{t_2}$ совпадает с $\mathcal{E}^{(s)}$ и которая при любом σ , $\sigma \in B^{t_2}$ удовлетворяет неравенству

$$L(E_\sigma) \leq c_3 s(k+1). \quad (12)$$

Тогда для каждого α , $\alpha \in B^a$, и каждого β , $\beta \in B^b$, найдется такая функция $F_{\alpha,\beta}(\tilde{u}, \tilde{w})$ вида

$$F_{\alpha,\beta}(\tilde{u}, \tilde{w}) = \Phi_\sigma(g_{i_1}(\tilde{w}), \dots, g_{i_{ks}}(\tilde{w}), u_{j_1}, \dots, u_{j_s}), \quad (13)$$

которая совпадает с функцией $f(\alpha, \tilde{u}, \tilde{w})$ на множестве $\tilde{M}_\beta$, где $g_{i_m} \in G$ при всех m , $m = 1, \dots, ks$, $1 \leq j_m \leq s$ при всех m , $m = 1, \dots, s$, и $\sigma = \sigma(\beta)$. Из § 4 и определения сложения матрицы и слова следует, что матрица $U^{(1)} \cdot (U^{(2)} \oplus \beta)$ является $\Phi_{k,s}$ -универсальной, если $\beta \in \mathcal{R}$, и тогда $\sigma_1 = \dots = \sigma_s = 0$, а при остальных значениях β в силу того, что любой столбец матрицы $U^{(2)} \oplus \beta$ либо совпадает с некоторым столбцом из матрицы $U^{(2)}$, либо является его отрицанием, существует возможность выбора σ таким образом, чтобы $F_{\alpha,\beta}(\tilde{u}, \tilde{w})$ совпадала с $f(\alpha, \tilde{u}, \tilde{w})$ на множестве $\tilde{M}_\beta$.

Через $K_\sigma(z_1, \dots, z_m)$, где $\sigma = (\sigma_1, \dots, \sigma_m)$, обозначается элементарная конъюнкция $z_1^{\sigma_1} \& \dots \& z_m^{\sigma_m}$. Пусть $\chi_\beta(\tilde{u}, \tilde{w})$ — характеристическая функция базового множества матрицы M_β , $\beta \in B^b$. Тогда

$$f(\tilde{x}) = \bigvee_{\alpha \in B^a} \bigvee_{\beta \in B^b} K_\alpha(\tilde{v}) \chi_\beta(\tilde{u}, \tilde{w}) F_{\alpha,\beta}(\tilde{u}, \tilde{w}) = \bigvee_{\beta \in B^b} \chi_\beta(\tilde{u}, \tilde{w}) \psi_\beta(\tilde{x}), \quad (14)$$

где

$$\psi_\beta(X) = \bigvee_{\alpha \in B^a} K_\alpha(\tilde{v}) F_{\alpha,\beta}(\tilde{u}, \tilde{w}). \quad (15)$$

Схема Σ_f строится в соответствии с (13)–(15) следующим образом. Подсхема Σ_G схемы Σ_f для каждой функции g , $g \in G$, реализует ее на выходе подсхемы. Схема Σ_G строится по лемме 3 так, что

$$L(\Sigma_G) \leq c_2 \cdot \Theta_1 + c_4 \cdot 2^{q + \sigma_A s/2} k. \quad (16)$$

Подсхема Σ_F включает в себя схему Σ_G и для каждой пары (α, β) , где $\alpha \in B^a$, $\beta \in B^b$, реализует функцию $F_{\alpha,\beta}$ в соответствии с (13). Для этого используется схема E_σ , входы которой присоединены к соответствующим выходам схемы Σ_G и входам $\tilde{u}$. Схема Σ_F в силу (12) такова, что

$$L(\Sigma_F) \leq L(\Sigma_G) + 2^a (L(\mathcal{E}^{(s)}) \cdot |\mathcal{R}| + c_3 t |B^b \setminus \mathcal{R}|). \quad (17)$$

Подсхема Σ_ψ включает в себя схему Σ_F и для каждого β , $\beta \in B^b$, реализует функцию ψ_β в соответствии с (15). Для этого используется схема, построенная по лемме 7 из работы [4] для системы элементарных конъюнк-

*) Буквой e с различными индексами будем обозначать абсолютные константы.

ций $K_\alpha(\tilde{v})$, $\alpha \in B^a$, итеративные входы которой присоединены к соответствующим выходам схемы Σ_F :

$$L(\Sigma_\psi) \leq L(\Sigma_F) + c_6 2^{a+b}. \quad (18)$$

Схема Σ_f , наконец, реализует функцию f , используя для этого схему, построенную по лемме 7 [4] для системы ортогональных функций χ_β , $\beta \in B^b$, итеративные входы которой подключены к выходам Σ_ψ в соответствии с (14). Таким образом, в силу (16)–(18) с учетом (10)–(12) получим

$$L(\Sigma_f) \leq 2^{a+b} L(\mathcal{E}^{(s)}) + O(k \cdot 2^{q+\sigma_A s_1/2} + 2^{\sigma_A s_1} + 2^{a+b} + 2^{a+b} s(k+1) e_1^b). \quad (19)$$

При $a = [(n-q)/4]$ условие (11) в силу (9) будет выполнено, и поэтому из (19) вытекает

$$L_B^\Pi(n) \leq L(\mathcal{E}^{(s)}) 2^{n-q} + O(2^{n-q}(1 + s(k+1)e_2^{n-q}) + 2^{s_1} + k 2^{q+s_1/2}), \quad (20)$$

где $e_2 = e_1^{3/4}$ (значит $e_2 < 1$ — это следует из определения множества $\mathcal{R}$).

Для получения итоговой оценки выберем следующие значения параметров:

$$s_1 = \left\lceil \frac{n - 2 \log n + \log k + 2}{\sigma_A} \right\rceil, \quad q = [2 \log n + \log k - 7], \quad s = \left\lfloor \frac{\sigma_A 2^q}{k(n - \log n)} \right\rfloor.$$

Напомним, что для схемы $\mathcal{E}^{(s)}$ ее сложность $L(\mathcal{E}^{(s)}) = ps$. При данном выборе параметров условия (9) выполняются, и, значит, мы можем использовать оценку (20). Учитывая, что $\pi_B = p/k$, получим требуемую оценку

$$L_B^\Pi(Q_A(n)) \leq \pi_B \frac{2^n \sigma_A}{n} \left(1 + \frac{2 \log n}{n} + O\left(\frac{1}{n}\right) \right).$$

Лемма полностью доказана.

Полученная верхняя оценка совпадает с полученной в § 3 нижней оценкой до второго члена разложения, что и доказывает основную теорему.

СПИСОК ЛИТЕРАТУРЫ

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. — М.: Изд-во Моск. ун-та, 1978.
2. Ложкин С. А. Асимптотические оценки высокой степени точности для сложности управляющих систем // Диссертация на соискание ученой степени доктора физико-математических наук, Москва, МГУ, 1997.
3. Ложкин С. А. Асимптотические оценки высокой степени точности для сложности функций, связанных с автоматными языками // Проблемы теоретической кибернетики. Тезисы докладов XII Международной конференции. Часть II / Под редакцией О. Б. Лупанова. — М.: Изд-во механико-математического факультета МГУ, 1999. — С. 138.
4. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 189–214.
5. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Моск. ун-та, 1984.
6. Лупанов О. Б. О сложности реализации функции алгебры логики релейно-контактными схемами // Проблемы кибернетики. Вып. 11. — М.: Наука, 1964. — С. 25–48.
7. Яблонский С. В. Основные понятия кибернетики // Проблемы кибернетики. Вып. 2. — М.: Физматгиз, 1959. — С. 7–38.
8. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.
9. Chomsky N., Miller G. A. Finite state languages // Inf. and control. — V. 1, № 2. — 1958. — P. 91–112. [Русский перевод: Хомский Н., Миллер Д. Языки с конечным числом состояний // Кибернетич. сб. Вып. 4. — М.: ИЛ, 1962. — С. 231–255.]
10. Shannon C. E. The synthesis of two-terminal switching circuits // Bell Syst. Techn. J., 1949. — V. 28, № 1. — P. 59–98. [Русский перевод: Шеннон К. Синтез двухполюсных переключаемых схем // Сб. Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 59–106.]