ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 2004. Серия 1. Том 11, № 2, 41–65

УДК 519.6

ОБ ОДНОМ МЕТОДЕ ПОЛУЧЕНИЯ ОЦЕНОК СЛОЖНОСТИ СХЕМ НАД ПРОИЗВОЛЬНЫМ БЕСКОНЕЧНЫМ БАЗИСОМ*)

О. М. Касим-Заде

Предложен метод получения оценок сложности реализации булевых функций схемами из функциональных элементов над произвольным бесконечным полным базисом B, позволяющий при слабых ограничениях оценивать функцию Шеннона $L_B(n)$ с точностью до множителя порядка n.

Введение

Всякое функционально полное множество булевых функций, т. е. такое, что суперпозициями функций из этого множества можно выразить любую булеву функцию, будем называть *базисом*.

Рассмотрим реализацию булевых функций схемами из функциональных элементов над произвольным фиксированным базисом B. Определение понятия схемы из функциональных элементов и других связанных с ним понятий см. в [9, 15].

Всюду в данной работе под *сложностью схемы* понимается число входящих в нее функциональных элементов.

Наименьшее число элементов, достаточное для реализации схемой над базисом B булевой функции f называется *сложностью* функции f и обозначается через $L_B(f)$.

Обычным образом вводится соответствующая базису B *функция Шеннона* $L_B(n)$, определяемая для всех натуральных n соотношением

$$L_B(n) = \max_f L_B(f),$$

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 02-01-00985), программы поддержки ведущих научных школ РФ (проект НШ-1807.2003.1), программы «Университеты России» (проект УР.04.03.007/03) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Оптимальный синтез управляющих систем»).

где максимум берется по всевозможным булевым функциям f от n переменных.

Базис называется *бесконечным*, если содержит функции, существенно зависящие от сколь угодно большого числа переменных (т. е. для всякого m в базисе имеется по крайней мере одна функция, существенно зависящая не менее чем от m переменных). В противном случае базис называется *конечным*.

Известно [18], что для всякого конечного базиса B порядок роста функции Шеннона $L_B(n)$ при $n \to \infty$ равен $2^n/n$. Исчерпывающее описание асимптотического поведения функций Шеннона для всех конечных базисов с положительными весами элементов дано О. Б. Лупановым [9].

Поведение функций Шеннона для бесконечных базисов гораздо разнообразнее. В частности, известны примеры базисов, для которых порядки роста функций Шеннона равны: 1, $\log_2 n$, $(2^n/n)^{1/2}$, $2^{n/2}$ [10–13, 17].

Какого-либо общего метода, позволяющего по произвольному бесконечному базису находить порядок роста соответствующей функции Шеннона (или хотя бы оценивать ее с некоторой разумной точностью, например, с точностью до полиномиальной эквивалентности), не известно.

В работе [4] решена задача о характеризации функций, асимптотически эквивалентных функциям Шеннона, отвечающим произвольным (в том числе бесконечным) базисам с произвольными неотрицательными весами элементов.

Автором [7] установлена общая верхняя оценка функций Шеннона, распространяющаяся на все бесконечные базисы: для всякого бесконечного базиса B при любом натуральном n выполняется соотношение $L_B(n) \leqslant C \cdot 2^{n/2}$, где C — некоторая абсолютная (т. е. не зависящая от базиса) постоянная. С точностью до множителя эта оценка является, вообще говоря, неулучшаемой: существуют базисы, для которых порядок роста соответствующей функции Шеннона равен $2^{n/2}$ [12].

В работе [8] предложен новый подход к получению оценок функций Шеннона для произвольных бесконечных базисов, позволяющий при некоторых ограничениях оценивать рост функций Шеннона с точностью до полиномиальной эквивалентности. Основной результат [8] заключается в следующем.

Для всякого бесконечного базиса B обозначим через $N'_B(r)$ число всех булевых функций от r фиксированных переменных $x_1, \ldots, x_r$, которые получаются из функций базиса B с помощью операций переименования переменных, отождествления переменных и добавления или изъя-

тия несущественных переменных. Фактически, $N'_B(r)$ есть число булевых функций от r переменных, допускающих реализацию схемами сложности 1 над базисом B.

При любом натуральном n обозначим через $l'_B(n)$ наименьшее натуральное число l, удовлетворяющее неравенству

$$(l+1)\log_2 N'_B(n+l) \geqslant 2^n.$$

Основной результат [8] гласит, что для всякого бесконечного базиса B при любом натуральном n выполняются соотношения

$$l'_B(n) \leqslant L_B(n) \leqslant c'(l'_B(n)+n)^2,$$

где c' — некоторая абсолютная постоянная.

Если функция $l'_B(n)$ имеет рост не ниже линейного, т. е. нижний предел $\liminf\limits_{n\to\infty} l'_B(n)/n > 0$, то функция Шеннона $L_B(n)$ с точностью до постоянного множителя (зависящего от базиса) заключена между функциями $l'_B(n)$ и $(l'_B(n))^2$.

При этом, и даже при более слабых условиях, если функция $l'_B(n)$ имеет рост не ниже степенно́го, т. е. для некоторого $\alpha > 0$ выполняется соотношение $\liminf\limits_{n\to\infty} l'_B(n)/n^\alpha > 0$, функция Шеннона $L_B(n)$ полиномиально эквивалентна функции $l'_B(n)$.

Содержательно функция $l'_B(n)$ выражает «мощностную» (или, как еще говорят, «информационную») нижнюю оценку функции Шеннона $L_B(n)$. Таким образом, метод [8] позволяет получать верхние оценки функции Шеннона, сопоставимые с ее мощностной нижней оценкой $l'_B(n)$.

Формальное определение функции Шеннона $L_B(n)$ опирается на рассмотрение совокупности всех схем над базисом B. Оценивая функцию Шеннона $L_B(n)$ через функцию $l'_B(n)$, удается в некотором смысле сводить рассмотрение совокупности всех схем над базисом B к рассмотрению части этой совокупности, — вообще говоря, значительно более узкой, — всех схем сложности 1.

Следует отметить, что для нахождения функции $l'_B(n)$ достаточно знать только связанную с базисом B функцию $N'_B(r)$. Нахождение по базису функции $N'_B(r)$ в точном виде составляет, вообще говоря, трудную задачу. Однако для получения оценок функции $l'_B(n)$ знание точного вида функции $N'_B(r)$ не требуется, достаточно лишь уметь оценивать ее с нужной точностью. Как правило, эта задача решается намного легче.

В настоящей работе метод [8] получает новое развитие. Вводится функция $l_B(n)$, определяемая аналогично $l'_B(n)$, но в некотором смысле

более тонким образом, и устанавливается, что для любого бесконечного базиса B при любом натуральном n выполняются соотношения

$$l_B(n) \leqslant L_B(n) \leqslant cn(l_B(n) + n),$$

где c — некоторая абсолютная постоянная.

Если функция $l_B(n)$ имеет рост не ниже линейного, то функция Шеннона $L_B(n)$ с точностью до постоянного множителя заключена между $l_B(n)$ и $nl_B(n)$. Эти оценки, вообще говоря, точнее оценок [8]. В случае, если функция $l_B(n)$ имеет рост не ниже степенно́го, функция Шеннона $L_B(n)$ также полиномиально эквивалентна функции $l_B(n)$.

Отметим, что с формальной точки зрения предлагаемый метод пригоден для всякого базиса. Поэтому в дальнейшем бесконечность рассматриваемых базисов специально не оговаривается. Следует, однако, иметь в виду, что в применении к конечным базисам этот метод без должной модификации ведет к довольно грубым оценкам.

1. Нижняя оценка

Как уже говорилось, описываемый метод получения нижней оценки функции Шеннона опирается на мощностные (информационные) соображения и восходит к работам [10, 13].

1.1. Расширение базиса. Удобнее работать не с самим базисом B, а с некоторым его расширением. Для любого базиса B обозначим через $G(B)$ множество всех булевых функций, которые можно получить из функций базиса B с помощью следующих операций: переименование переменных, отождествление переменных, добавление или изъятие несущественных переменных, применямых в любом числе и в любом порядке (определения этих операций см. в [15]).

Легко видеть, что $G(B)$ есть фактически множество тех булевых функций, которые реализуются над базисом B схемами сложности 1: функция φ принадлежит множеству $G(B)$ тогда и только тогда, когда $L_B(\varphi) = 1$.

Отсюда, в частности, следует, что любую схему над базисом $G(B)$ без изменения сложности можно преобразовать в эквивалентную (т. е. реализующую ту же функцию) схему над базисом B путем замены каждого базисного элемента из $G(B)$ соответствующей эквивалентной схемой сложности 1 над базисом B. С другой стороны, любая схема над базисом B, очевидно, может рассматриваться как схема над базисом $G(B)$. Поэтому для любого базиса B и любой булевой функции f выполняется равенство $L_{G(B)}(f) = L_B(f)$, и при любом натуральном n — равенство $L_{G(B)}(n) = L_B(n)$.

Таким образом, изучение сложности реализации булевых функций над базисом B сводится к изучению сложности их реализации над базисом $G(B)$ и наоборот.

1.2. Функция $N_B(r,t)$ и ее свойства. Для любого натурального r обозначим через $G^r(B)$ множество всех принадлежащих $G(B)$ булевых функций от r фиксированных переменных $x_1,\dots,x_r$.

Обозначим через B^r множество всех двоичных наборов длины r, т. е. наборов вида $\tilde{\alpha}=(\alpha_1,\dots,\alpha_r)$, где $\alpha_i\in\{0,1\}$.

Пусть A — непустое множество наборов из B^r. Булевы функции f и g от r переменных называются *различимыми на множестве* A, если существует такой набор $\tilde{\alpha}\in A$, что $f(\tilde{\alpha})\neq g(\tilde{\alpha})$.

Множество F булевых функций от r переменных называется *разделимым на множестве* A, если любые две различные функции из F являются различимыми на A.

Для любого множества Q булевых функций от r переменных положим[*)]

$$W(Q,A)=\max_F|F|,$$

где максимум берется по всем разделимым на A подмножествам F множества Q.

Для любого базиса B при любых натуральных r, t таких, что $t\leqslant 2^r$, положим

$$N_B(r,t)=\max_A W(G^r(B),A),$$

где максимум берется по всем t-элементным подмножествам A из B^r.

Говоря содержательно, функция $N_B(r,t)$ выражает наибольшее число частичных булевых функций от r переменных, которое можно получить из булевых функций, реализуемых над базисом B со сложностью 1, путем сужения их на некоторое подмножество наборов мощности t в множестве B^r.

Установим некоторые свойства функции $N_B(r,t)$.

Лемма 1.1. *Для любого базиса B при любых натуральных r, t таких, что $t\leqslant 2^r$, выполняется неравенство $N_B(r+1,t)\geqslant N_B(r,t)$.*

Доказательство. Зафиксируем произвольное t-элементное множество A наборов из B^r, для которого достигается равенство $W(G^r(B),A)=N_B(r,t)$, и произвольное разделимое на A множество функций F из $G^r(B)$, для которого достигается равенство $|F|=W(G^r(B),A)$. К каждому набору из A добавим нулевую $(r+1)$-ю компоненту, и к каждой функции

[*)] Как обычно, через $|F|$ обозначается мощность (число элементов) множества F.

из F — несущественную переменную x_{r+1}. Очевидно, что полученное множество функций остается разделимым на новом множестве наборов. Отсюда вытекает требуемое неравенство. Лемма 1.1 доказана.

Лемма 1.2. *Для любого базиса B при любых натуральных r, t таких, что $r \leqslant t \leqslant 2^r$, выполняется неравенство $N_B(r,t) \geqslant r$.*

Доказательство. Обозначим через A_1^r множество всех двоичных наборов длины r, имеющих одну единичную и $r-1$ нулевых компонент:

$$A_1^r = \{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)\}.$$

Зафиксируем произвольную отличную от константы функцию φ из базиса B. Возможны два случая.

Случай 1: $\varphi(0,\ldots,0) \neq \varphi(1,\ldots,1)$. В этом случае функция $\psi(x) = \varphi(x,\ldots,x)$, полученная из функции φ путем отождествления всех переменных, существенно зависит от x. Рассмотрим функции $\psi(x_1),\ldots,$ $\psi(x_r)$. Добавив к ним недостающие несущественные переменные, получим r функций, принадлежащих множеству $G^r(B)$. Легко проверить, что эти функции попарно различимы на множестве A_1^r.

Случай 2: $\varphi(0,\ldots,0) = \varphi(1,\ldots,1)$. Функция φ не равна константе. Поэтому на некотором наборе функция φ принимает значение, отличное от $\varphi(0,\ldots,0)$. В функцию φ вместо всех переменных, соответствующих нулевым компонентам этого набора, подставим переменную x, а вместо всех остальных — переменную y. Полученную функцию обозначим через $\kappa(x,y)$. По построению $\kappa(0,0) = \kappa(1,1) \neq \kappa(0,1)$.

Рассмотрим функции $\kappa(x_1,x_1),\ldots,\kappa(x_1,x_r)$. Добавив к ним несущественные переменные, снова получим r функций, принадлежащих множеству $G^r(B)$, попарно различимых на A_1^r.

В обоих случаях построено множество из r функций, принадлежащих $G^r(B)$, разделимое на r-элементном множестве A_1^r. Отсюда вытекает, что $N_B(r,r) \geqslant r$. Остается заметить, что $N_B(r,t) \geqslant N_B(r,r)$, ибо разделимость множества функций сохраняется при расширении множества наборов. Лемма 1.2 доказана.

1.3. Оценка числа функций, реализуемых с данной сложностью. При каждом натуральном n и целом l, $l \geqslant 0$, обозначим через $M_B(n,l)$ множество всех булевых функций от переменных x_1, …, x_n, допускающих реализацию схемой сложности не более l над базисом B.

Очевидно, что схемы нулевой сложности реализуют только тривиальные функции x_1, …, x_n. Поэтому при любом n имеет место равенство $|M_B(n,0)| = n$.

Оценим сверху величину $|M_B(n,l)|$ при $l \geqslant 1$. Следуя [10, 13], сведем эту задачу к получению верхней оценки числа схем некоторого специального вида.

Известно [9], что в каждой схеме из функциональных элементов можно занумеровать элементы так, чтобы входы каждого элемента были соединены либо со входами схемы, либо с выходами элементов с меньшими номерами. Такая нумерация элементов схемы называется *правильной*.

Следуя [10, 13], будем говорить, что схема имеет *специальный вид*, если эта схема допускает такую правильную нумерацию элементов, что для любого i элемент схемы с номером i имеет $n+i-1$ входов, которые в порядке возрастания их номеров соединены со всеми входами схемы и с выходами всех элементов с меньшими номерами. Говоря более формально, для любого j, $1 \leqslant j \leqslant n+i-1$, j-й вход элемента с номером i при $j \leqslant n$ присоединен к входу схемы, помеченному символом переменной x_j, а при $j \geqslant n+1$ — к выходу элемента с номером $j-n$. Выходом схемы специального вида, по определению, является выход элемента с наибольшим номером.

Вершинами схемы, как обычно, будем называть входы схемы и выходы ее элементов.

Напомним, что *эквивалентными* называются схемы, реализующие одинаковые функции.

Лемма 1.3. *Для любой схемы над базисом B существует эквивалентная схема той же сложности над базисом $G(B)$, имеющая специальный вид.*

Доказательство. Рассмотрим произвольную схему над базисом B. Для этой схемы зафиксируем произвольную правильную нумерацию элементов. Над всеми элементами схемы последовательно выполним следующие операции.

Если в исходной схеме некоторый элемент не имеет входов, соединенных с выходом какого-либо элемента с меньшим номером или с каким-либо входом схемы, то к базисной функции, приписанной рассматриваемому элементу, добавим несущественную переменную, вход которой соединим с нужной вершиной.

Если несколько входов элемента соединены с одной и той же вершиной, то у приписанной этому элементу базисной функции отождествим переменные, соответствующие таким входам.

Если нумерация входов элемента не соответствует нумерации входов схемы и ее элементов, то переменные базисной функции переименуем так, чтобы установить нужное соответствие.

Во всех случаях после выполнения описанных операций получаются схемы, эквивалентные исходной. Сложность схемы не изменяется. Остается учесть, что при добавлении несущественных переменных, равно как и при отождествлении или переименовании переменных, функции базиса B переходят в функции базиса $G(B)$. Лемма 1.3 доказана.

Из леммы 1.3 следует, что любую функцию из множества $M_B(n,l)$ можно реализовать некоторой схемой специального вида над базисом $G(B)$ сложности не более l. Поэтому величина $|M_B(n,l)|$ не превосходит числа различных функций, реализуемых такими схемами. Оценим это число.

Обозначим через $R_B(n,s)$ множество всех схем специального вида над базисом $G(B)$ сложности s, $1 \leqslant s \leqslant l$, имеющих n входов, помеченных символами переменных $x_1,\ldots, x_n$.

Рассмотрим произвольную схему из множества $R_B(n,s)$. Осуществим правильную нумерацию элементов этой схемы. (Очевидно, что для любой схемы специального вида существует единственная правильная нумерация.)

Обозначим через φ_i базисную функцию из $G(B)$, приписанную элементу схемы с номером i. В соответствии с определением схем специального вида φ_i есть функция от $n+i-1$ переменных.

Функцию от входных переменных, реализуемую на выходе элемента схемы с номером i, обозначим через $f_i(x_1,\ldots,x_n)$.

Очевидно, что при любом i выполняется соотношение

$$f_i(x_1,\ldots,x_n) = \varphi_i(x_1,\ldots,x_n, f_1(x_1,\ldots,x_n),\ldots,f_{i-1}(x_1,\ldots,x_n)). \quad (1)$$

Обозначим через A_i множество всех двоичных наборов

$$\tilde{\beta} = (\alpha_1,\ldots,\alpha_n, f_1(\alpha_1,\ldots,\alpha_n),\ldots,f_{i-1}(\alpha_1,\ldots,\alpha_n))$$

длины $n+i-1$, где $\tilde{\alpha} = (\alpha_1,\ldots,\alpha_n)$ пробегает всевозможные наборы из множества B^n.

Из определения видно, что $\tilde{\beta}$ — это набор, поступающий на входы элемента с номером i при подаче на входы схемы набора $\tilde{\alpha}$ значений входных переменных $x_1,\ldots,x_n$. Соответственно, A_i есть множество всех таких наборов $\tilde{\beta}$, когда $\tilde{\alpha}$ пробегает множество B^n. Очевидно, что $|A_i| = 2^n$ при любом i.

Оценим сверху число различных последовательностей функций $f_1,\ldots,f_s$, соответствующих схемам из множества $R_B(n,s)$. В соответствии с соотношением (1) любую такую последовательность можно построить рекуррентно за s шагов.

Любая схема, принадлежащая множеству $R_B(n,s)$, однозначно задается последовательностью $\varphi_1,\ldots,\varphi_s$ базисных функций из $G(B)$, приписанных ее элементам.

На первом шаге выбирается функция φ_1. Из (1) следует, что $f_1=\varphi_1$. Поэтому число возможностей выбора функции f_1 равно $N_B(n,2^n)$, т. е. числу всех функций в множестве $G^n(B)$.

На каждом последующем шаге i выбирается очередная базисная функция φ_i. К моменту осуществления этого шага уже зафиксированы функции $f_1,\ldots,f_{i-1}$. Поэтому множество A_i известно. Из (1) следует, что различные возможности для функций f_i соответствуют выбору в качестве φ_i функций из $G^{n+i-1}(B)$, различимых на множестве A_i. Поэтому число возможностей выбора функции f_i равно $W(G^{n+i-1}(B),A_i)$, и, следовательно, не превосходит величины $N_B(n+i-1,2^n)$.

Отсюда следует, что число различных последовательностей $f_1,\ldots,f_s$, соответствующих схемам из множества $R_B(n,s)$, не превосходит величины

$$\prod_{i=1}^{s} N_B(n+i-1,2^n).$$

Число различных функций сложности s, $s\geqslant 1$, принадлежащих множеству $M_B(n,l)$, также не превосходит указанной величины, ибо каждая из этих функций в качестве f_s встречается по меньшей мере в одной из последовательностей $f_1,\ldots,f_s$. Отсюда следует, что

$$|M_B(n,l)|\leqslant\sum_{s=1}^{l}\prod_{i=1}^{s}N_B(n+i-1,2^n)+|M_B(n,0)|.$$

Учитывая, что $|M_B(n,0)|=n$, приходим к следующему утверждению.

Лемма 1.4. *Для любого базиса B при любом натуральном n и любом целом l, $l\geqslant 0$, выполняется неравенство*

$$|M_B(n,l)|\leqslant\sum_{s=1}^{l}\prod_{i=1}^{s}N_B(n+i-1,2^n)+n.$$

Это утверждение удобнее применять в другой, несколько более грубой (хотя и несколько более слабой) форме.

Лемма 1.5. *Для любого базиса B при любых натуральных n, l выполняется неравенство*

$$|M_B(n,l)|\leqslant(N_B(n+l,2^n))^{l+1}.$$

Доказательство. В соответствии с леммой 1.1 при любом i выполняется соотношение

$$N_B(n+i-1, 2^n) \leqslant N_B(n+l, 2^n).$$

Поэтому из леммы 1.4 следует, что

$$|M_B(n,l)| \leqslant l(N_B(n+l,2^n))^l + n \leqslant (l+n)(N_B(n+l,2^n))^l.$$

Если $l < 2^n - n$, то в соответствии с леммой 1.2 имеем $l+n \leqslant N_B(n+l, 2^n)$, и требуемое неравенство доказано.

В противном случае $l \geqslant 2^n - n$. При этом в силу леммы 1.1 $N_B(n+l, 2^n) \geqslant N_B(2^n, 2^n)$, а в соответствии с леммой 1.2 $N_B(2^n, 2^n) \geqslant 2^n$. Поэтому в данном случае

$$(N_B(n+l,2^n))^{l+1} \geqslant 2^{n(2^n-n+1)}.$$

С другой стороны, заведомо $|M_B(n,l)| \leqslant 2^{2^n}$. Остается учесть, что при любом натуральном n выполняется неравенство $2^n \leqslant n(2^n-n+1)$. Лемма 1.5 доказана.

1.4. Функция $l_B(n)$. Нижняя оценка функции Шеннона. При любом натуральном n через $l_B(n)$ обозначим наименьшее натуральное l, удовлетворяющее неравенству

$$(l+1)\log_2 N_B(n+l, 2^n) \geqslant 2^n. \tag{2}$$

Определение величины $l_B(n)$ корректно, ибо при любом фиксированном n левая часть неравенства (2) есть неограниченно возрастающая функция от l.

Лемма 1.6. *Для любого базиса B при любом натуральном n выполняется соотношение $L_B(n) \geqslant l_B(n)$.*

Доказательство. По определению любую булеву функцию от n переменных можно реализовать некоторой схемой над базисом B сложности не более $L_B(n)$. Поэтому

$$\log_2 |M_B(n, L_B(n))| = 2^n.$$

С другой стороны, в соответствии с леммой 1.5

$$\log_2 |M_B(n, L_B(n))| \leqslant (L_B(n)+1)\log_2 N_B(n+L_B(n), 2^n).$$

Поэтому

$$(L_B(n)+1)\log_2 N_B(n+L_B(n), 2^n) \geqslant 2^n.$$

Следовательно, число $L_B(n)$ удовлетворяет неравенству (2). Учитывая, что $l_B(n)$ есть наименьшее натуральное число, удовлетворяющее (2), приходим к требуемой оценке $L_B(n) \geqslant l_B(n)$. Лемма 1.6 доказана.

Как обычно, будем говорить, что некоторое соотношение выполняется для *почти всех* булевых функций f от n переменных, если отношение числа функций f от n переменных, удовлетворяющих этому соотношению, к числу всех булевых функций от n переменных стремится к единице с ростом n.

Лемма 1.7. *Для любого базиса B соотношение*

$$L_B(f) \geqslant l_B(n) - 1$$

выполняется для почти всех булевых функций f от n переменных.

Доказательство. Пусть n — натуральное. Если $l_B(n) = 1$, то требуемое неравенство тривиальным образом выполняется для всех булевых функций f от n переменных.

Пусть $l_B(n) \geqslant 2$. Оценим сверху число $|M_B(n, l_B(n) - 2)|$ функций f от n переменных, допускающих реализацию схемой над базисом B сложности не более $l_B(n) - 2$.

В соответствии с леммой 1.5 имеем

$$\log_2 |M_B(n, l_B(n) - 2)| \leqslant (l_B(n) - 1) \log_2 N_B(n + l_B(n) - 2, 2^n). \qquad (3)$$

По определению величина $l_B(n)$ есть наименьшее натуральное число, удовлетворяющее неравенству (2). Поэтому для числа $l_B(n) - 1$ это неравенство не выполняется:

$$l_B(n) \log_2 N_B(n + l_B(n) - 1, 2^n) < 2^n.$$

Учитывая, что $l_B(n) \leqslant 2^n - n$ (число $l = 2^n - n$ заведомо удовлетворяет неравенству (2), ибо $N_B(2^n, 2^n) \geqslant 2^n$), в соответствии с леммой 1.2 имеем

$$N_B(n + l_B(n) - 1, 2^n) \geqslant n + l_B(n) - 1 \geqslant n.$$

Следовательно,

$$(l_B(n) - 1) \log_2 N_B(n + l_B(n) - 1, 2^n) < 2^n - \log_2 n.$$

Отсюда с учетом (3) и леммы 1.1 получаем

$$\log_2 |M_B(n, l_B(n) - 2)| < 2^n - \log_2 n.$$

Из последнего соотношения видно, что при любом n отношение числа булевых функций f от n переменных сложности $L_B(f) \leqslant l_B(n) - 2$, к числу всех булевых функций от n переменных, не превосходит величины n^{-1}. Отсюда и из сказанного вначале доказательства вытекает, что для почти всех функций f от n переменных выполняется неравенство $L_B(f) \geqslant l_B(n) - 1$. Лемма 1.7 доказана.

2. Верхняя оценка

Предлагаемый метод, подобно методу [8], нарпавлен на получение верхней оценки функции Шеннона $L_B(n)$, сопоставимой с ее мощностной (информационной) нижней оценкой $l_B(n)$.

С точки зрения информационных соображений [10, 13] любая схема над базисом B рассматривается как «код» реализуемой ею функции (функция определяется схемой однозначно). Для того чтобы закодировать все булевы функции от n переменных, требуется 2^n двоичных единиц (*бит*) информации. Совокупность всех схем сложности не более l над базисом B, кодирующих функции от n переменных, способна нести не более $(l+1)\log_2 N_B(l+n, 2^n)$ единиц информации. Таким образом, с информационной точки зрения неравенство (2), определяющее функцию $l_B(n)$, выражает соотношение между количеством информации, необходимым для задания произвольной булевой функции от n переменных, и количеством информации о реализуемых функциях, которое способны нести схемы сложности не более l над базисом B. Выполнение этого соотношения составляет необходимое условие возможности реализации всех булевых функций от n переменных схемами над базисом B, сложность которых не превосходит l.

Условие, выраженное неравенством (2), вообще говоря, не является достаточным. Однако можно пытаться использовать его для получения верхней оценки функции Шеннона $L_B(n)$, сопоставимой с информационной нижней оценкой $l_B(n)$, опираясь на следующие соображения.

Если в множестве B^{n+l} зафиксировать произвольное 2^n-элементное подмножество наборов A и в множестве $G^{n+l}(B)$ — произвольное разделимое на A множество функций F такое, что выполняется равенство $|F| = N_B(n+l, 2^n)$, то выбор произвольной функции в множестве F несет $\log_2 N_B(n+l, 2^n)$ единиц информации. В соответствии с этим неравенство (2) можно понимать и так: при любом l, $l \geqslant l_B(n)$, выбор в множестве F произвольной последовательности из $l+1$ функций несет не менее 2^n единиц информации. Такого количества информации, в принципе, достаточно для того, чтобы закодировать все булевы функции от n переменных. Фактически, предлагаемый метод позволяет некоторым

образом извлекать эту информацию с не слишком большими дополнительными затратами сложности. Поэтому и удается получить верхнюю оценку функции Шеннона $L_B(n)$, сопоставимую с информационной нижней оценкой $l_B(n)$.

Если отвлечься от технических деталей, то главные черты описываемого метода получения верхней оценки функции Шеннона, как и в [8], сводятся к следующим: использование универсальных множеств и параметризующих их вектор-функций для представления произвольных булевых функций через базисные, и рекуррентный способ реализации параметризующих вектор-функций в сочетании с известным приемом разложения функций по подмножествам переменных. Рассмотрим все по порядку.

2.1. Универсальные множества. Пусть Q — некоторое множество булевых функций от r переменных. Множество A двоичных наборов длины r назовем Q-*универсальным*, если для каждого отображения $\psi\colon A \to \{0,1\}$ найдется такая функция $g \in Q$, что для любого набора $\tilde{\alpha}$, $\tilde{\alpha} \in A$, выполняется равенство $g(\tilde{\alpha}) = \psi(\tilde{\alpha})$.

Иными словами, множество A является Q-универсальным, если любую частичную булеву функцию с областью определения A можно получить путем сужения на множество A некоторой функции из Q.

Очевидно, что мощность любого Q-универсального множества A удовлетворяет неравенству $|A| \leqslant \log_2 |Q|$.

Каждое непустое подмножество Q-универсального множества также является Q-универсальным. При расширении множества функций универсальность множества наборов сохраняется, т. е. для любого множества Q', $Q \subseteq Q'$, каждое Q-универсальное множество является также Q'-универсальным.

Укажем одно достаточное условие существования Q-универсальных множеств заданной мощности.

Матрицу с a строками и b столбцами, будем называть матрицей *размера* $a \times b$. Матрицу, столбцы которой попарно различны, будем называть *правильной*.

Будем называть *полной* любую правильную двоичную матрицу размера $q \times 2^q$, где q —любое фиксированное натуральное число. Иными словами, полной является любая матрица размера $q \times 2^q$, в которой в качестве столбцов встречаются по одному разу все 2^q двоичных наборов длины q (порядок их расположения в матрице значения не имеет).

Подматрицей матрицы A называется любая матрица, получаемая из A путем вычеркивания каких-либо строк и (или) столбцов.

При любых натуральных a и q, $a \geqslant q$, обозначим через $m(a,q)$ такое наибольшее натуральное число b, что существует хотя бы одна правильная двоичная матрица размера $a \times b$, не содержащая полных подматриц размера $q \times 2^q$.

Например, при любых a и q, $a \geqslant q$, в правильной матрице размера $a \times \sum\limits_{i=0}^{q-1} \binom{a}{i}$, в которой столбцами являются всевозможные двоичные наборы длины n не более чем с $q-1$ единицами, заведомо отсутствуют полные подматрицы размера $q \times 2^q$. Поэтому $m(a,q) \geqslant \sum\limits_{i=0}^{q-1} \binom{a}{i}$. На самом деле, правая часть этого неравенства дает точное значение величины $m(a,q)$.

Известно следующее утверждение, независимо установленное многими авторами [1–3, 16, 19, 20] (насколько можно судить, впервые подобное утверждение опубликовано в [2]).

Лемма 2.1. *При любых натуральных a и q, $a \geqslant q$, выполняется соотношение*

$$m(a,q) = \sum_{i=0}^{q-1} \binom{a}{i}.$$

Отсюда вытекает другое, также известное утверждение [14].

Лемма 2.2. *При любых натуральных a, b, q таких, что $a \geqslant q \geqslant 2$ и*

$$\log_2 b \geqslant q \log_2 a, \tag{4}$$

каждая правильная двоичная матрица размера $a \times b$ содержит хотя бы одну полную подматрицу размера $q \times 2^q$.

Доказательство. Из леммы 2.1 следует, что для любых натуральных a, b, q, где $a \geqslant q$, удовлетворяющих условию

$$b \geqslant \sum_{i=0}^{q-1} \binom{a}{i} + 1, \tag{5}$$

любая правильная двоичная матрица размера $a \times b$ содержит хотя бы одну полную подматрицу размера $q \times 2^q$.

Вместе с тем

$$\sum_{i=0}^{q-1} \binom{a}{i} \leqslant \sum_{i=0}^{q-1} a^i \leqslant a^q - 1.$$

В силу последнего неравенства выполнение условия (4) влечет выполнение условия (5), откуда следует требуемое заключение. Лемма 2.2 доказана.

Лемма 2.3. *Пусть r, t, q — такие натуральные числа, что $2 \leqslant q \leqslant t \leqslant 2^r$, D — t-элементное множество двоичных наборов длины r, Q — множество функций от r переменных, разделимое на множестве D, и пусть выполнено условие*:

$$\log_2 |Q| \geqslant q \log_2 t. \tag{6}$$

Тогда существует q-элементное подмножество A множества D, являющееся Q-универсальным.

Доказательство. Каждой функции из Q поставим в соответствие столбец ее значений на наборах из множества D, упорядоченных каким-либо фиксированным способом, например, лексикографически, и из этих столбцов построим двоичную матрицу размера $|D| \times |Q|$. Ясно, что построенная матрица является правильной.

Применим к этой матрице лемму 2.2, полагая $a = |D|$, $b = |Q|$; из соотношения (6) следует, что для рассматриваемой матрицы условие (4) выполнено.

В соответствии с леммой 2.2 рассматриваемая матрица содержит хотя бы одну полную подматрицу размера $q \times 2^q$. Зафиксируем такую подматрицу. Строки этой подматрицы соответствуют наборам из некоторого q-элементного подмножества $A \subseteq D$, столбцы — функциям из некоторого подмножества $Q'' \subseteq Q$. Из полноты подматрицы следует, что при сужении функций из Q на множество A получаются все частичные булевы функции с областью определения A. Поэтому множество A является Q''-универсальным, а, следовательно, Q-универсальным. Лемма 2.3 доказана.

2.2. Параметризация. Пусть $\tilde{x} = (x_1, \ldots, x_n)$ обозначает набор n переменных. Будем говорить, что булева (n, r)-вектор-функция $\tilde{h}(\tilde{x})$ *параметризует* множество A двоичных наборов длины r, если эта вектор-функция взаимно-однозначно отображает множество B^n всех двоичных наборов длины n на множество A.

Очевидно, что при каждом натуральном n, $n \leqslant r$, для любого 2^n-элементного множества A наборов длины r существует по меньшей мере одна (n, r)-вектор-функция, параметризующая это множество. (На самом деле их может быть намного больше, но для наших целей хватит и одной.) Кроме того, имеет место очевидная

Лемма 2.4. *Пусть n и r — натуральные, Q — такое непустое множество функций от r переменных, A — такое Q-универсальное множество наборов длины r, что $|A| = 2^n$, $\tilde{h}(\tilde{x})$ — (n, r)-вектор-функция, параметризующая множество A. Тогда для любой булевой функции f от n*

переменных в Q найдется такая функция g, что

$$f(\tilde{x}) = g(\tilde{h}(\tilde{x})).$$

2.3. Разложения. При каждом натуральном k двоичным наборам длины k присвоим номера $1, \ldots, 2^k$ так, чтобы набор с номером j изображал число $j-1$, записанное в двоичной системе счисления, причем старшие разряды располагались справа. Набор с номером j обозначим через $\tilde{\sigma}_j^k$ и будем записывать покомпонентно в виде $\tilde{\sigma}_j^k = (\sigma_{j,1}, \ldots, \sigma_{j,k})$.

При любом j обозначим через K_j соответствующую набору $\tilde{\sigma}_j^k$ элементарную конъюнкцию от k переменных, определяемую соотношением

$$K_j(z_1, \ldots, z_k) = z_1^{\sigma_{j,1}} \& \ldots \& z_k^{\sigma_{j,k}}.$$

Известно [15], что любую булеву функцию $f(\tilde{x})$ от n переменных, $\tilde{x} = (x_1, \ldots, x_n)$, при любом k, $1 \leqslant k \leqslant n$, можно представить в виде

$$f(\tilde{x}) = \bigvee_{j=1}^{2^k} f(\tilde{x}_1, \tilde{\sigma}_j^k) \& K_j(\tilde{x}_2). \tag{7}$$

где $\tilde{x}_1 = (x_1, \ldots, x_{n-k})$, $\tilde{x}_2 = (x_{n-k+1}, \ldots, x_n)$, а $f(\tilde{x}_1, \tilde{\sigma}_j^k)$ обозначает функцию, полученную из f путем подстановки компонент набора $\tilde{\sigma}_j^k$ вместо последних k переменных.

Удобно ввести специальные функции, соответствующие таким разложениям.

Определим булеву функцию W_k от $2^k + k$ переменных, полагая

$$W_k(y_1, \ldots y_{2^k}, z_1, \ldots, z_k) = \bigvee_{j=1}^{2^k} y_j \& K_j(z_1, \ldots, z_k). \tag{8}$$

Из сопоставления (7) и (8) вытекает следующая

Лемма 2.5. *Для любой булевой функции $f(\tilde{x})$ от n переменных при любом k, $1 \leqslant k \leqslant n$, выполняется соотношение*

$$f(\tilde{x}) = W_k(f(\tilde{x}_1, \tilde{\sigma}_1^k), \ldots, f(\tilde{x}_1, \tilde{\sigma}_{2^k}^k), \tilde{x}_2).$$

В дальнейшем потребуется верхняя оценка сложности реализации функций W_k схемами в произвольном базисе. Сначала докажем следующий простой факт.

Лемма 2.6. *Для любой булевой функции φ существует такое число $c(\varphi)$, что для любого базиса B выполняется соотношение $L_B(\varphi) \leqslant c(\varphi)$.*

Известно, что любой базис содержит хотя бы одну немонотонную и хотя бы одну нелинейную функцию. Из немонотонной функции путем подстановки констант 0, 1 можно получить функцию отрицания $\bar{x}$, а из нелинейной путем подстановки функций $0, 1, x, y, \bar{x}, \bar{y}$, и, возможно, взятия отрицания от самой функции, — конъюнкцию $x\&y$ от двух переменных [15].

Рассмотрим базис $B_0 = \{\bar{x}, x\&y\}$ и реализуем функцию φ над этим базисом некоторой схемой S сложности $L_{B_0}(\varphi)$. Преобразуем схему S в эквивалентную схему над базисом B, заменив каждый элемент схемы S эквивалентной ему схемой над базисом B, действуя следующим образом.

Сначала реализуем схемой над B систему констант $\{0, 1\}$. Известно, что эта система реализуется над любым базисом с использованием не более трех элементов [15].

Имея константы, каждый элемент отрицания в S заменим одним элементом из B (соответствующим немонотонной функции), и каждый элемент конъюнкции — схемой над B, содержащей не более четырех элементов (один из которых соответствует нелинейной функции, три остальных — немонотонной). Отсюда вытекает, что $L_B(\varphi) \leqslant 4L_{B_0}(\varphi) + 3$. Полагая $c(\varphi) = 4L_{B_0}(\varphi) + 3$, приходим к требуемому заключению. Лемма 2.6 доказана.

Лемма 2.7. *Для любого базиса B при любом натуральном k выполняется соотношение*

$$L_B(W_k) \leqslant c_0(2^k - 1),$$

где c_0 — некоторая абсолютная (т. е. не зависящая от базиса) постоянная.

Доказательство. В соответствии с леммой 2.6 существует такое число $c(W_1)$, что для любого базиса B выполняется неравенство $L_B(W_1) \leqslant c(W_1)$. Положим $c_0 = c(W_1)$.

Легко проверить (например, применив индукцию по k), что при любом k, $k \geqslant 2$, функцию W_k можно выразить через функции W_1 и W_{k-1} в виде

$$W_k(y_1, \ldots, y_{2^k}, z_1, \ldots, z_k) = W_1(W_{k-1}(y_1, \ldots, y_{2^{k-1}}, z_1, \ldots, z_{k-1}), \\ W_{k-1}(y_{2^{k-1}+1}, \ldots, y_{2^k}, z_1, \ldots, z_{k-1}), z_k).$$

Отсюда следует, что при любом k функцию W_k можно реализовать над базисом B схемой сложности не более $L_B(W_1)(2^k - 1) \leqslant c_0(2^k - 1)$.

Лемма 2.7 доказана.

2.4. Вспомогательные утверждения. Обозначим через $L_B(n,m)$ наименьшее число элементов, достаточное для реализации схемой над базисом B любой булевой (n,m)-вектор-функции.

Лемма 2.8. *Для любого базиса B при любых натуральных n, r, t, m, k таких, что $n \geqslant 2$, $k \leqslant n-1$, $2^{n-k} \leqslant t \leqslant 2^r$ и*

$$\log_2 N_B(r,t) \geqslant 2^{n-k} \log_2 t,$$

выполняется соотношение

$$L_B(n,m) \leqslant L_B(n-k,r) + c_1 m 2^k,$$

где c_1 — некоторая абсолютная постоянная.

Доказательство. Рассмотрим произвольную (n,m)-вектор-функцию $\tilde{f}(\tilde{x}) = (f_1(\tilde{x}), \ldots, f_m(\tilde{x}))$, где $\tilde{x} = (x_1, \ldots, x_n)$. Опираясь на лемму 2.5, каждую из компонент f_i вектор-функции $\tilde{f}$ представим в виде

$$f_i(\tilde{x}) = W_k(f_i(\tilde{x}_1, \tilde{\sigma}_1^k), \ldots, f_i(\tilde{x}_1, \tilde{\sigma}_{2^k}^k), \tilde{x}_2),$$

где $\tilde{x}_1 = (x_1, \ldots, x_{n-k})$, $\tilde{x}_2 = (x_{n-k+1}, \ldots, x_n)$. Для сокращения записи введем обозначение: $f_i^j(\tilde{x}_1) = f_i(\tilde{x}_1, \tilde{\sigma}_j^k)$.

В соответствии с определением величины $N_B(r,t)$ существуют: t-элементное множество D двоичных наборов длины r и такое разделимое на D множество функций Q от r переменных, $Q \subseteq G^r(B)$, что $|Q| = N_B(r,t)$.

Применим к множествам D и Q лемму 2.3, полагая $q = 2^{n-k}$. Все условия леммы 2.3 выполнены: $2 \leqslant q \leqslant t \leqslant 2^r$ и $\log_2 |Q| \geqslant q \log_2 t$. В соответствии с этой леммой существует Q-универсальное множество A, $A \subseteq D$, мощности $|A| = 2^{n-k}$. Это множество является также $G^r(B)$-универсальным, ибо $Q \subseteq G^r(B)$.

Зафиксируем произвольное множество A с указанными свойствами, а также произвольную $(n-k,r)$-вектор-функцию $\tilde{h}(\tilde{x}_1)$, параметризующую множество A. В соответствии с леммой 2.4 для каждой функции f_i^j найдется такая функция g_i^j в $G^r(B)$, что выполняется соотношение

$$f_i^j(\tilde{x}_1) = g_i^j(\tilde{h}(\tilde{x}_1)).$$

Отсюда следует, что для любого i компоненту f_i вектор-функции $\tilde{f}$ можно представить в виде:

$$f_i(\tilde{x}) = W_k(g_i^1(\tilde{h}(\tilde{x}_1)), \ldots, g_i^{2^k}(\tilde{h}(\tilde{x}_1)), \tilde{x}_2).$$

Построим схему над базисом B, реализующую вектор-функцию $\tilde{f}$. Сначала реализуем вектор-функцию $\tilde{h}$, использовав не более $L_B(n-k,r)$ элементов. Затем с помощью $m2^k$ базисных элементов, соответствующих функциям g_i^j, реализуем систему всех функций f_i^j. Завершая построение, каждую из компонент f_i вектор-функции $\tilde{f}$ реализуем с помощью отдельной схемы для функции W_k — в соответствии с леммой 2.7 для этого требуется не более $mc_0(2^k-1)$ элементов.

Общая сложность построенной схемы не превосходит величины $L_B(n-k,r)+(c_0+1)m2^k$. Полагая $c_1=c_0+1$, ввиду произвольности вектор-функции $\tilde{f}$ получаем требуемое. Лемма 2.8 доказана.

Замечание. В дополнение к лемме 2.8 отметим, что из лемм 2.5 и 2.7 вытекает также известная грубая верхняя оценка функций Шеннона: для любого базиса B при любом натуральном n выполняется соотношение $L_B(n)\leqslant c_0(2^n-1)+3$ (если в лемме 2.7 положить $k=n$, то функции $f(\tilde{x}_1,\tilde{\sigma}_j^k)$ оказываются константами, а система констант $\{0,1\}$, как уже говорилось, реализуется над любым базисом с использованием не более трех элементов).

Лемма 2.9. *Для любого базиса B при любых натуральных p, r, t таких, что*

$$2^{p-1}\leqslant t\leqslant 2^r, \tag{9}$$

и

$$\log_2 N_B(r,t)\geqslant 2^{p-1}\log_2 t, \tag{10}$$

выполняется соотношение

$$L_B(p,r)\leqslant c_2pr, \tag{11}$$

где c_2 — некоторая абсолютная постоянная.

Доказательство. Положим $c_2=\max(3,2c_1)$. Сначала рассмотрим случай $p=1$. Известно, что для реализации системы всех функций от одной переменной схемой над любым базисом достаточно трех элементов. Поэтому при каждом r выполняется неравенство $L_B(1,r)\leqslant 3$, и, тем более, $L_B(1,r)\leqslant c_2r$.

Из соотношений (9) и (10) следует, что при любом s, $2\leqslant s\leqslant p$, выполняются неравенства $2^{s-1}\leqslant t\leqslant 2^r$ и $\log_2 N_B(r,t)\geqslant 2^{s-1}\log_2 t$. Положим в лемме 2.8 $n=s$, $m=r$ и $k=1$ (оставив значение t без изменения). Тогда все условия леммы 2.8 выполнены, и в соответствии с этой леммой имеем

$$L_B(s,r)\leqslant L_B(s-1,r)+2c_1r.$$

Складывая почленно полученные неравенства, соответствующие значениям $s = 2, \ldots, p$, после очевидных преобразований приходим к соотношению $L_B(p, r) \leqslant L_B(1, r) + c_2(p-1)r$. Отсюда с учетом установленного в начале доказательства неравенства $L_B(1, r) \leqslant c_2 r$ получаем требуемое соотношение. Лемма 2.9 доказана.

Из лемм 2.8 и 2.9 легко выводится

Лемма 2.10. *Для любого базиса B при любых натуральных n, r, t, k таких, что $n \geqslant 2$, $k \leqslant n-1$, $2^{n-k} \leqslant t \leqslant 2^r$ и*

$$\log_2 N_B(r, t) \geqslant 2^{n-k} \log_2 t,$$

выполняется соотношение

$$L_B(n) \leqslant c_2((n-k)r + 2^k),$$

где c_2 — та же абсолютная постоянная, что в лемме 2.9.

3. Основной результат. Оценки функций Шеннона

Основной результат данной работы содержится в следующем утверждении.

Теорема 1. *Для любого базиса B при любом натуральном n выполняются соотношения*

$$l_B(n) \leqslant L_B(n) \leqslant cn(l_B(n) + n),$$

где c — некоторая абсолютная постоянная.

Доказательство. Нижняя оценка установлена в лемме 1.6. Докажем верхнюю оценку. Положим $c = \max(2\max(c_0, 3), 3c_2)$ и рассмотрим два случая.

Случай 1: $n(l_B(n)+1) \geqslant 2^{n-1}$. В этом случае требуемая верхняя оценка вытекает из замечания к лемме 2.8. Действительно, в соответствии с этим замечанием $L_B(n) \leqslant c_0(2^n - 1) + 3$. Поэтому в рассматриваемом случае $L_B(n) \leqslant cn(l_B(n) + n)$.

Случай 2: $n(l_B(n) + 1) < 2^{n-1}$. Применим лемму 2.10, полагая $r = l_B(n)+n$, $t = 2^n$ и $k = \lceil \log_2(n(l_B(n) + 1)) \rceil$. Покажем, что все условия этой леммы выполнены.

Очевидно, что $r, t, k \geqslant 1$ и $2^{n-k} \leqslant t \leqslant 2^r$. Кроме того, в рассматриваемом случае выполняется неравенство $\log_2(n(l_B(n) + 1)) < n - 1$. Следовательно, $k \leqslant n - 1$.

По определению величины $l_B(n)$ имеет место неравенство

$$(l_B(n) + 1) \log_2 N_B(l_B(n) + n, 2^n) \geqslant 2^n.$$

Отсюда с учетом очевидного соотношения $k \geqslant \log_2(l_B(n)+1)+\log_2\log_2 t$ следует, что

$$\log_2 N_B(r,t) \geqslant 2^{n-k}\log_2 t.$$

Все условия леммы 2.10 выполнены. В соответствии с этой леммой имеем $L_B(n) \leqslant c_2((n-k)r+2^k)$. Подставив значения r и k и учитывая, что $k \leqslant \log_2(n(l_B(n)+1))+1$, получаем $L_B(n) \leqslant c_2(n(l_B(n)+n)+2n(l_B(n)+1))$. Окончательно имеем $L_B(n) \leqslant cn(l_B(n)+n)$. Теорема 1 доказана.

Из теоремы 1 и леммы 1.7 вытекает

Следствие. *Для любого базиса B соотношения*

$$l_B(n)-1 \leqslant L_B(f) \leqslant cn(l_B(n)+n)$$

выполняются для почти всех булевых функций f от n переменных (*здесь c — та же абсолютная постоянная, что в теореме* 1).

Если функция $l_B(n)$, связанная с данным базисом B, имеет достаточно быстрый рост, то из теоремы 1 удается извлечь довольно точные оценки функции Шеннона $L_B(n)$.

Будем говорить, что функция $a(n)$ натурального аргумента n имеет рост *не ниже линейного*, если существует такое действительное число $\alpha > 0$, что при любом достаточно большом n выполняется соотношение $a(n) \geqslant \alpha n$.

Из теоремы 1 и относящегося к ней следствия очевидным образом вытекает

Теорема 2. *Если для базиса B функция $l_B(n)$ имеет рост не ниже линейного, то существует такая постоянная c_B (вообще говоря, зависящая от базиса), что при любом натуральном n выполняются соотношения*

$$l_B(n) \leqslant L_B(n) \leqslant c_B n l_B(n),$$

причем для почти всех булевых функций f от n переменных

$$l_B(n)-1 \leqslant L_B(f) \leqslant c_B n l_B(n).$$

Будем говорить, что функция $a(n)$ натурального аргумента n имеет рост *не ниже степенно́го*, если существует такое действительное число $\alpha > 0$, что при любом достаточно большом n выполняется соотношение $a(n) \geqslant n^\alpha$.

Функции $a(n)$ и $b(n)$ натурального аргумента называются *полиномиально эквивалентными*, если существует такой полином $P(x)$ с положительными действительными коэффициентами, что при любом достаточно большом n выполняются соотношения $a(n) \leqslant P(b(n))$ и $b(n) \leqslant P(a(n))$.

Из теоремы 1 вытекает

Теорема 3. *Если для базиса B функция $l_B(n)$ имеет рост не ниже степенно́го, то функция Шеннона $L_B(n)$ полиномиально эквивалентна функции $l_B(n)$.*

В следующем утверждении говорится о сравнении базисов.

Теорема 4. *Если для базисов B_1 и B_2 функции $l_{B_1}(n)$ и $l_{B_2}(n)$ имеют рост не ниже степенно́го, то полиномиальная эквивалентность этих функций влечет полиномиальную эквивалентность функций Шеннона $L_{B_1}(n)$ и $L_{B_2}(n)$.*

Ограничения на рост функций $l_B(n)$ в теоремах 3 и 4 являются существенными. Например, для бесконечного базиса AC, состоящего из всевозможных антицепных булевых функций (т. е. функций, принимающих единичные значения лишь на попарно несравнимых наборах), порядок роста функции $l_{AC}(n)$ равен $\log_2 n$, в то время как порядок роста функции Шеннона $L_{AC}(n)$ заключен между $(n/\log_2 n)^{1/2}$ и n [5, 6]. Здесь функции $L_{AC}(n)$ и $l_{AC}(n)$ не являются полиномиально эквивалентными.

Известен также [4, 9] пример такого бесконечного базиса AM, состоящего из всех антимонотонных булевых функций (т. е. функций, являющихся отрицаниями монотонных), для которого порядки роста функций $l_{AM}(n)$ и $L_{AM}(n)$ совпадают и равны $\log_2 n$. Таким образом, для базисов AM и AC полиномиальная эквивалентность (и даже совпадение порядков роста) функций $l_{AM}(n)$ и $l_{AC}(n)$ не влечет полиномиальной эквивалентности соответствующих функций Шеннона $L_{AM}(n)$ и $L_{AC}(n)$.

4. Заключительные замечания

К предложенному методу получения оценок функции Шеннона можно отнести большинство замечаний, сделанных во введении по отношению к методу [8]. Предложенный метод, как и метод [8], позволяет сводить получение верхней оценки функции Шеннона $L_B(n)$ к нахождению ее мощностной нижней оценки $l_B(n)$, и приводит к верхней оценке, сопоставимой с нижней оценкой $l_B(n)$. Для нахождения функции $l_B(n)$ достаточно знать только связанную с базисом B функцию $N_B(r,t)$, причем для получения приемлемых по точности оценок функции $l_B(n)$ и вытекающих из них верхних оценок функции Шеннона $L_B(n)$ требуется уметь лишь оценивать функцию $N_B(r,t)$ подходящим образом; знание ее точного вида не обязательно.

Функция $N_B(r,t)$ является метрической характеристикой множества $G(B)$ всех булевых функций, реализуемых над базисом B со сложностью

1 и выражает наибольшее число частичных булевых функций от r переменных, которое можно получить из таких функций путем сужения на некоторое подмножество наборов мощности t в множестве B^r. Таким образом, как и в [8], оценивая функцию Шеннона $L_B(n)$ через функцию $l_B(n)$, рассмотрение совокупности всех схем над базисом B удается в некотором смысле свести к рассмотрению схем сложности 1.

Функция $N_B(r,t)$ является более тонкой метрической характеристикой множества $G(B)$, чем использованная в [8] функция $N'_B(r)$. Очевидно, что для любого базиса B при любых r и t выполняется соотношение $N_B(r,t) \leqslant N'_B(r)$. Поэтому при любом n выполняется неравенство $l_B(n) \geqslant l'_B(n)$, т. е. функция $l_B(n)$ во всех случаях доставляет нижнюю оценку функции Шеннона, не худшую чем $l'_B(n)$.

Сравним точность соответствующих двусторонних оценок. Если для данного базиса B функция $l_B(n)$ имеет рост не ниже линейного, то при $n \to \infty$ отношение $(l'_B(n)+n)^2/l'_B(n)$ растет по порядку как $l'_B(n)+n$. При тех же условиях отношение $n(l_B(n)+n)/l_B(n)$ растет как n. Поэтому если $l'_B(n)/n \to \infty$, то метод данной работы дает заведомо более точные оценки функции Шеннона, чем метод [8] (хотя для нахождения этих оценок, вообще говоря, могут потребоваться бóльшие усилия).

Следует сказать, что теоремы 3 и 4 можно вывести также из основного результата [8] и леммы 1.6. В силу соотношений

$$l'_B(n) \leqslant l_B(n) \leqslant L_B(n) \leqslant c'(l'_B(n)+n)^2,$$

справедливых для любого базиса B при любом n (c' — абсолютная постоянная), если хотя бы одна из функций $l'_B(n)$, $l_B(n)$, $L_B(n)$ имеет рост не ниже степенно́го, то все три функции имеют такой рост и полиномиально эквивалентны друг другу. В данной работе теоремы 3 и 4 получены независимо от результатов [8].

Обратим внимание еще на одно обстоятельство. В лемме 2.3 устанавливается лишь факт существования универсального множества требуемой мощности, но не дается эффективного (т. е. приемлемого с точки зрения трудоемкости) способа его построения. Очевидно, что степень эффективности предлагаемого метода в случае его применения непосредственно для синтеза схем (а не только в целях получения оценок функций Шеннона, для чего он, собственно, предназначен) зависит от возможности эффективного решения данной задачи. Вместе с тем, предлагаемый метод во всех случаях дает гарантированные двусторонние оценки функции Шеннона.

Выражаю глубокую признательность О. Б. Лупанову за внимание,

проявленное к данной работе, и Н. П. Редькину за полезные замечания, способствовавшие улучшению изложения.

ЛИТЕРАТУРА

1. **Алексеев В. Е.** Об энтропии фрагментно-замкнутых классов графов // Комбинаторно-логические методы в прикладной математике. Горький: Изд-во Горьковского государственного университета им. Н. И. Лобачевского, 1986. С. 5–15.
2. **Вапник В. Н., Червоненкис А. Я.** О равномерной сходимости частот появления событий к их вероятностям // Теория вероятностей и ее применения. 1971. Т. 16, вып. 2. С. 264–280.
3. **Вапник В. Н., Червоненкис А. Я.** Теория распознавания образов. М.: Наука, 1974.
4. **Карпова Н. А.** О некоторых свойствах функций Шеннона // Математические заметки. 1970. Т. 8, вып. 5. С. 663–674.
5. **Касим-Заде О. М.** О сложности схем в одном бесконечном базисе // Вестник Московского университета. Сер. 1. Математика. Механика. 1994. № 6. С. 40–44.
6. **Касим-Заде О. М.** О сложности реализации булевых функций схемами в одном бесконечном базисе // Дискрет. анализ и исслед. операций. 1995. Т. 2, № 1. С. 7–20.
7. **Касим-Заде О. М.** Общая верхняя оценка сложности схем в произвольном бесконечном полном базисе // Вестник Московского университета. Сер. 1. Математика. Механика. 1997. № 4. С. 59–61.
8. **Касим-Заде О. М.** Об одном методе получения оценок сложности схем над бесконечными базисами // Математические вопросы кибернетики. Вып. 11. М.: Наука. Физматлит, 2002. С. 247–254.
9. **Лупанов О. Б.** Об одном методе синтеза схем // Известия высших учебных заведений. Радиофизика. 1958. Т. 1, № 1. С. 120–140.
10. **Лупанов О. Б.** О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 26. М.: Наука, 1973. С. 109–140.
11. **Марков А. А.** Об инверсионной сложности систем функций // Докл. АН СССР. 1957. Т. 116, № 6. С. 917–919.
12. **Нечипорук Э. И.** О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Проблемы кибернетики. Вып. 8. М.: Физматгиз, 1962. С. 123–160.
13. **Нечипорук Э. И.** О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 11. М.: Наука, 1964. С. 149–162.
14. **Редькин Н. П.** О реализации систем конъюнкций контактными схемами // Проблемы кибернетики. Вып. 30. М.: Наука, 1975. С. 263–276.
15. **Яблонский С. В.** Введение в дискретную математику. М.: Наука, 1986.

16. Alon N. On the density of sets of vectors // Discrete Math. 1983. V. 46, N 2. P. 199–202.

17. Gilbert E. N. Lattice theoretic properties of frontal switching functions // J. Math. Phys. 1954. V. 33, N 1. P. 57– 67. (Имеется перевод: Гилберт Е. Н. Теоретико-структурные свойства замыкающих переключательных функций // Кибернетический сборник. Вып. 1. М.: ИЛ, 1960. С. 175–188).

18. Muller D. E. Complexity in electronic switching circuits // IRE Trans. on Electronic Computers. 1958. V. EC–5, N 1. P. 15–19.

19. Sauer N. On the density of families of sets // J. of Combinatorial Theory. Ser. A. 1972. V. 13, N 1. P. 145–147.

20. Shelah S. A combinatorial problem: stability and order for models and theories in infinite languages// Pacific J. of Math. 1972. V. 41, N 1. P. 247–261.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119992 Москва,
Россия.
E-mail: kasimz@mech.math.msu.su

Статья поступила
5 февраля 2004 г.