В.А. Коноводов, С.А. Ложкин

ОБ ОЦЕНКАХ ВЫСОКОЙ СТЕПЕНИ ТОЧНОСТИ ФУНКЦИИ ШЕННОНА ДЛЯ СЛОЖНОСТИ ФОРМУЛ В БАЗИСАХ С ПРЯМЫМИ И ИТЕРАТИВНЫМИ ПЕРЕМЕННЫМИ*

Введение

Рассматривается задача реализации булевых функций формулами с ограничением на операцию суперпозиции базисных функций. Все переменные делятся на два типа — прямые и итеративные [1], и суперпозиция возможна только по итеративным переменным. Кроме того, допускается подстановка констант вместо переменных функций, которая не влияет на сложность получаемых формул.

Формулы рассматриваются как одновыходные схемы из функциональных элементов (см., например, [2]) без ветвлений выходов внутренних элементов. В этом отношении указанное ограничение означает, что выход любого элемента может либо являться выходом схемы, либо подаваться на итеративный вход другого элемента. Сложность формулы определяется как суммарный вес используемых в ней элементов.

Разделение переменных на прямые и итеративные имеет смысл в тех случаях, когда в модели дискретной управляющей системы есть сигналы двух типов — входных прямых и управляющих итеративных. Схема реализует функцию, зависящую от переменных первого типа, по которым нельзя вести суперпозицию, а сигналы второго типа используются для передачи управления исполнения в зависимости от входного импульса.

В работе оценивается поведение функции Шеннона $L(n)$ для сложности реализаций функций, зависящих от n прямых переменных, формулами в базисах из элементах с прямыми и итеративными входами. Ранее было доказано [3], что в широком классе базисов порядок этой функции составляет $\frac{2^n}{\log n}$, а для ряда таких базисов были получены [4] оценки высокой степени точности, устанавливающие, что величина $2^n/L(n)$ с точностью до аддитивной константы представляет собой $c \cdot \log n$, где c — множитель, зависящий только от базиса.

В настоящей работе для ряда специальных симметричных базисов

*Работа выполнена при поддержке РФФИ (проект №18-01-00800-а) и Госбюджетной темы НИР №5.4 ВМК МГУ.

устанавливаются оценки величины $2^n/L(n)$ вида $c_1 \cdot \log n - c_2 \log\log n \pm \text{const}$, где константы $c_1, c_2 > 0$, и зависят только от базиса. Эти оценки обобщают на случай разделения переменных на прямые и итеративные аналогичный результат [5] для сложности формул в симметричных базисах без ограничения на суперпозицию.

Основные определения и формулировка результатов

Пусть $X = \{x_1, x_2, \ldots\}$ и $Y = \{y_1, y_2, \ldots\}$ — счетные множества булевых переменных, причем переменные из множества X будем называть *прямыми*, а переменные из множества Y — *итеративными*. Для произвольного множества переменных $Z \subseteq X \cup Y$ будем обозначать через $P_2(Z)$ множество всех функций алгебры логики (в дальнейшем — просто функций), зависящих от переменных из Z. Функции, не имеющие общих существенных [6] переменных, будем называть *независимыми*.

На множестве $P_2(X \cup Y)$, следуя [1,3,7], введём следующие операции суперпозиции:

1. переименование (с отождествлением) прямых переменных;
2. подстановка констант 0, 1 вместо переменных;
3. переименование (с отождествлением) итеративных переменных;
4. подстановка одной из двух независимых функций вместо итеративной переменной другой функции;
5. замена итеративных переменных прямыми.

Пусть A, $A \subseteq P_2(X \cup Y)$ — некоторое конечное множество базисных функций. Будем рассматривать одновыходные схемы из функциональных элементов (см., например, [2]) над базисом A с ограничением на соединения элементов между собой, соответствующим введённым операциям суперпозиции. Вход базисного функционального элемента будем называть *константным*, если вместо него в этот элемент подставлена константа 0 или 1. Правила соединения элементов в схемах ограничиваются следующим образом:

1. прямые входы любого элемента либо присоединяются к входам схемы, либо являются константными входами;
2. итеративные входы любого элемента либо присоединяются к выходам других элементов, либо присоединяются к входам схемы, либо являются константными входами;
3. неконстантным входам схемы сопоставлены некоторые переменные из множества X.

Под формулами будем понимать те одновыходные схемы, которые не содержат ветвлений выходов элементов. С точки зрения рекурсивного

определения формулы как символьной записи (см., например, [6]) указанные выше операции дают возможность проводить суперпозицию только по итеративным переменным базисных функций.

В настоящей работе рассматривается задача реализации функций от прямых переменных формулами описанного вида. Систему функций A, $A \subseteq P_2(X \cup Y)$, будем называть *полной*, если для любой функции f, $f \in P_2(X)$, существует формула, построенная в соответствии с введёнными выше ограничениями, реализующая функцию f. Множество всех функций из $P_2(X \cup Y)$, которые можно реализовать такими формулами в базисе A, будем обозначать через $[A]$. Критерий полноты произвольной системы функций был получен в работе [1].

Пусть $A = \{\varphi_1, \ldots, \varphi_b\}$ — конечный полный базис, $A \subseteq P_2(X \cup Y)$, и каждому базисному функциональному элементу $\mathscr{E}_i$, $i = 1, \ldots, b$, реализующему функцию φ_i, зависящую от k_i переменных, k_i' из которых прямые, а k_i'' — итеративные, $k_i = k_i' + k_i''$, поставлен в соответствие его вес $L_i \geqslant 0$. Под *сложностью* $L(\mathscr{F})$ формулы $\mathscr{F}$ в базисе A понимается сумма весов всех её элементов. Будем считать, что подстановка константы вместо входа любого элемента не меняет его сложности. Функцией Шеннона $L_A(n)$ для сложности формул в базисе A, как обычно, будем называть максимальное значение $L_A(f)$ среди всех функций f, $f \in P_2(\{x_1, \ldots, x_n\})$, где $L_A(f)$ — минимальная сложность формулы из рассматриваемого класса, реализующей функцию f. Аналогично можно определить функцию Шеннона $L_A^C(n)$ для сложности реализации функций от прямых переменных в классе схем над базисом A, $A \subseteq P_2(X \cup Y)$.

Приведенным весом элемента $\mathscr{E}_i$, $i = 1, \ldots, b$, такого, что $k_i > 1$, будем называть величину

$$\rho_i = \frac{L_i}{k_i - 1}.$$

Назовем *макроблоком* [3] в базисе A схему из функциональных элементов в этом базисе, состоящую из одного элемента $\mathscr{E}_j \in A$, $j \in \{1, \ldots, b\}$, такого, что $k_j'' > 1$, и m, $0 \leqslant m \leqslant k_j'' - 1$, элементов $\mathscr{E}_{i_1}, \ldots, \mathscr{E}_{i_m} \in A$, где $i_1, \ldots, i_m \in \{1, \ldots, b\}$, а $k_{i_1}'' = \ldots = k_{i_m}'' = 0$, выходы которых подаются на итеративные входы элемента $\mathscr{E}_j$. Отметим, что число макроблоков в конечном базисе конечно.

Прямыми входами макроблока будем считать входы элементов $\mathscr{E}_{i_1}, \ldots, \mathscr{E}_{i_m}$, а также все свободные (т. е. те, на которые не подаются выходы других элементов макроблока) входы элемента $\mathscr{E}_j$, кроме одного из итеративных, который будем считать единственным итеративным входом макроблока.

Таким образом, макроблок M имеет сложность $L_M = L_j + L_{i_1} + \ldots + L_{i_m}$, а число его входов равно $k_M = k_j' + k_{i_1} + \ldots + k_{i_m} + k_j'' - m = k_{i_1} + \ldots + k_{i_m} + k_j - m$. *Приведенным*

весом макроблока M назовем величину

$$\rho_M = \frac{L_M}{k_M - 1}.$$

Для базиса A, $A \subseteq P_2(X \cup Y)$, будем пользоваться следующими обозначениями: $A'' = A \cap P_2(X)$, $A' = A \setminus A''$, $\delta(A) = [A] \cap P_2(Y)$.

Приведенным весом ρ_A базиса A, $A \subseteq P_2(X \cup Y)$, назовем минимальный приведенный вес среди всех элементов из A' и всех макроблоков в этом базисе.

Пусть $\hat{A}'$ — множество тех элементов A', которые либо имеют приведенный вес, равный ρ_A, либо входят в макроблоки в этом базисе с приведенным весом ρ_A. Множество элементов из A'', входящих в макроблоки приведенного веса ρ_A будем обозначать $\hat{A}''$. И пусть $\check{A}' = A' \setminus \hat{A}'$, $\check{A}'' = A'' \setminus \hat{A}''$, $\hat{A} = \hat{A}' \cup \hat{A}''$.

Будем говорить, что множество базисных элементов $\hat{A}'$ является *симметричным*, если множество реализуемых ими функций состоит либо только из линейных функций, либо только из конъюнкций переменных, либо только из дизъюнкций переменных. В этом случае множество $\hat{A}''$ будем называть *согласованно симметричным*, если при добавлении к $\hat{A}'$ элементов из $\hat{A}''$ полученное множество элементов остается симметричным.

Теорема 1 ([5]). *Пусть A, $A \subseteq P_2(Y)$, — полный базис, все элементы которого имеют только итеративные входы, тогда*[1]

$$L_A(n) = \rho_A \frac{2^n}{\log n}\left(1 + \frac{\varkappa_A \log\log n \pm O(1)}{\log n}\right),$$

где $\varkappa_A \in \{0,1\}$ и $\varkappa_A = 1$ тогда и только тогда, когда $\hat{A}$ — симметричное множество.

Эта оценка является асимптотической оценкой высокой степени точности — она определяет с точностью до константы величину $2^n/L_A(n)$, которую можно интерпретировать как число бит информации (длина столбца значений булевой функции от n переменных равна 2^n) на единицу сложности при реализации функций в заданном классе формул.

Пусть M — класс монотонных [6] функций от переменных Y.

Теорема 2 ([7],[3]). *Для любой полной системы функций A, $A \subseteq P_2(X \cup Y)$, такой, что $\delta(A) \in \{M, P_2(Y)\}$, при $n \to \infty$ справедливо соотношение $L_A(n) \sim \rho_A \cdot \frac{2^n}{\log n}$. Для каждого δ, $\delta \notin \{B, M, P_2(Y)\}$, существует полный базис A такой, что $\delta(A) = \delta$ и при этом $L_A(n) = \Theta(2^n)$.*

Теорема 3 ([4],[8]). *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис, такой, что $\delta(A) \in \{M, P_2(Y)\}$. Пусть, далее, справедливо хотя бы одно из следующих утверждений:*[2]

[1] В настоящей работе все логарифмы рассматриваются по основанию 2.

[2] Здесь и далее $x_1 \oplus x_2 = x_1\overline{x_2} \vee \overline{x_1}x_2$.

1. $\delta(\hat{A}) \in \{M, P_2(Y)\}$;
2. *базис* $\hat{A}$ *является полным базисом;*
3. *множество* $[\hat{A}]$ *содержит функцию* f *вида* $f = (\varphi_1 \circ y_1) \diamond \ldots \diamond (\varphi_k \circ y_k) \diamond \varphi_0$, *где* $\varphi_0, \varphi_1, \ldots, \varphi_k \in P_2(X)$, $(\circ, \diamond) \in \{(\&, \vee), (\vee, \&), (\&, \oplus)\}$, *для которой найдутся такие индексы* $j_1, j_2 \in \{1, \ldots, k\}$, $j_1 \neq j_2$, *и наборы* α, β *значений прямых переменных, что* $\varphi_{j_1}(\alpha) = \overline{\varphi_{j_1}(\beta)} = \varphi_{j_2}(\beta) = \overline{\varphi_{j_2}(\alpha)} = 0$.

Тогда при растущем значении натурального аргумента n, $n \geqslant 2$, *справедливо соотношение*

$$L_A(n) = \rho_A \cdot \frac{2^n}{\log n} \left(1 \pm \frac{O(1)}{\log n}\right). \tag{1}$$

Для базиса A, $A \subseteq P_2(X \cup Y)$, для которого множество $\hat{A}'$ является симметричным, определим величину

$$\omega_A = \begin{cases} 1, & \text{если } \hat{A}'' = \varnothing \text{ или } \hat{A}'' \text{ является согласованно симметричным,} \\ 1/\max\limits_{\mathscr{E}_i \in \hat{A}''} k_i, & \text{иначе.} \end{cases}$$

В настоящей работе доказывается следующий результат.

Теорема 4. *Пусть* A, $A \subseteq P_2(X \cup Y)$, *— базис, для которого* $M \subseteq \delta(A)$, *а* $\hat{A}'$ *— симметричное множество, и выполнено одно из следующих условий:*

1. $\hat{A}'' = \varnothing$,
2. $\hat{A}''$ *является согласованно симметричным,*
3. *каждая функция из множества* $\hat{A}'$ *имеет вид* $y_1 \circ \ldots \circ y_q \circ x_{q+1} \circ \ldots \circ x_{k_1}$ *для некоторых* $q, k_1 \geqslant 2$, $\hat{A}''$ *содержит функцию вида* $g_1(x_1) \diamond g_2(x_2, \ldots, x_{k_2})$, *где* $k_2 \geqslant 2$, $k_2 = \max\limits_{\mathscr{E}_i \in \hat{A}''} k_i$, $(\circ, \diamond) \in \{(\&, \vee), (\vee, \&), (\oplus, \vee), (\oplus, \&)\}$, *а функции* g_1 *и* g_2 *существенно зависят от своих переменных.*

Тогда при растущем значении натурального аргумента n *справедливо соотношение*

$$L_A(n) = \rho_A \frac{2^n}{\log n} \left(1 + \frac{\omega_A \log\log n + O(1)}{\log n}\right). \tag{2}$$

Таким образом, для некоторых базисов A устанавливается поведение функции Шеннона $L_A(n)$ на уровне оценок высокой степени точности с ненулевой константой при $\frac{\log\log n}{\log n}$ в её асимптотическом разложении.

Нижняя оценка функции Шеннона

Для доказательства нижней оценки потребуется следующее утверждение.

Лемма 1 ([5]). *Если a, m, τ, α — действительные параметры такие, что*

$$a \geqslant 2, \quad m \geqslant 1, \quad \tau \geqslant 1, \quad \alpha \geqslant 0,$$

то выполняется неравенство

$$\max_{0 \leqslant y \leqslant m} \left(\frac{a y^{\tau}}{m-y} \right)^{m-y} y^{\alpha m} \leqslant \left(\beta t m^{\alpha} (\log t)^{-\alpha-\tau} \right)^{m},$$

где $\beta = \beta(\alpha, \tau)$, $t = a m^{\tau-1}$.

Для произвольной формулы $\mathscr{F}$ в базисе A, $A \subseteq P_2(X \cup Y)$, будем обозначать за $\check{L}(\mathscr{F})$ (соответственно, $\tilde{L}(\mathscr{F})$) сумму весов элементов из $\check{A}' \cup \check{A}''$ (соответственно, из $\check{A}' \cup \check{A}'' \cup \hat{A}''$), входящих в данную формулу.

Везде далее для произвольного i, $i \in \{1, \ldots, b\}$, и A_1, $A_1 \subseteq A$, будем использовать обозначение $\varphi_i \in A_1$, которое означает, что $\mathscr{E}_i \in A_1$.

Лемма 2. *Пусть $\mathscr{F}$ — формула в базисе A, $A \subseteq P_2(X \cup Y)$, тогда если приведенный вес ρ_A достигается на элементе из A', то*

$$R(\mathscr{F}) \leqslant \frac{1}{\rho_A} L(\mathscr{F}) - c_1 \tilde{L}(\mathscr{F}) + 1, \tag{3}$$

где c_1 — положительная константа, зависящая только от базиса; а если приведенный вес ρ_A достигается на макроблоке, отличном от элемента, то

$$R(\mathscr{F}) \leqslant \frac{1}{\rho_A} L(\mathscr{F}) - c_2 \check{L}(\mathscr{F}) + 1, \tag{4}$$

где c_2 — положительная константа, зависящая только от базиса.

Доказательство. Будем считать, что $|\hat{A}'| = 1$, в остальных случаях доказательство аналогично. Пусть формула $\mathscr{F}$ содержит n_i элементов $\mathscr{E}_i$ для всех i, $i = 1, \ldots, b$. Тогда сложность этой формулы $L(\mathscr{F}) = \sum\limits_{i=1}^{b} n_i L_i$, а ее ранг

$$R(\mathscr{F}) = \sum_{i=1}^{b} n_i (k_i - 1) + 1 = \sum_{i=1}^{b} \frac{n_i L_i}{\rho_i} + 1.$$

Пусть $\hat{A}' = \{\mathscr{E}_{j_1}\}$, а $\hat{A}''$ либо пусто (и тогда приведенный вес базиса достигается на одном элементе), либо $\hat{A}'' = \{\mathscr{E}_{j_2}\}$ (и тогда приведенный вес базиса достигается на макроблоке, состоящем из элемента $\mathscr{E}_{j_1}$ и $(k''_{j_1} - 1)$ элементов $\mathscr{E}_{j_2}$); случай, когда A'' состоит из нескольких элементов, рассматривается аналогично.

В первом случае для любого элемента $\mathscr{E}_j \in A''$ справедливо условие $\rho_A \leqslant \rho_j$. Действительно, предположим обратное, пусть для некоторого элемента $\mathscr{E}_j \in A''$ выполнено $\rho_j < \rho_A$, тогда составим макроблок M из

элемента $\mathscr{E}_{j_1}$ и $(k''_{j_1}-1)$ элементов $\mathscr{E}_j$. Нетрудно видеть, что $\rho_M = \frac{1}{k_{j_2}}\rho_{j_1} + \frac{k_{j_2}-1}{k_{j_2}}\rho_j < \rho_{j_1} = \rho_A$, что противоречит минимальности приведенного веса базиса. Таким образом,

$$R(\mathscr{F}) = \frac{1}{\rho_A} n_{j_1} L_{j_1} + \sum_{i\in\{1,\ldots b\}\setminus\{j_1\}} n_i L_i \left(\frac{1}{\rho_A} - \left(\frac{1}{\rho_A} - \frac{1}{\rho_i}\right)\right) + 1,$$

и неравенство (3) справедливо для $c_1 = \min\limits_{\mathscr{E}_i\in A\setminus\{\mathscr{E}_{j_1}\}} \left\{\frac{1}{\rho_A} - \frac{1}{\rho_i}\right\} > 0$.

Во втором случае построим формулу $\mathscr{G}$, представляющую собой цепь из $n' = \sum\limits_{\mathscr{E}_i\in A'} n_i$ макроблоков $M_1,\ldots,M_{n'}$, и состоящую из тех же самых элементов, что и формула $\mathscr{F}$. Элементы с прямыми входами в таком случае должны быть произвольно подсоединены к свободным итеративным входам такой формулы. При этом $L(\mathscr{F}) = L(\mathscr{G})$, $R(\mathscr{F}) = R(\mathscr{G})$. Рассмотрим формулу $\mathscr{G}$ как формулу в базисе из всех возможных макроблоков базиса A (каждый элемент такого базиса имеет соответствующий базису A вес и функционирует как один элемент). В таком базисе $\tilde{L}(\mathscr{G})$ представляет собой сумму весов всех неминимальных макроблоков из $M_1,\ldots,M_{n'}$, т. е. $\tilde{L}(\mathscr{G}) \geqslant \check{L}(\mathscr{F})$, поскольку каждый макроблок, содержащий элементы из $\check{A}$, не является минимальным. Получаем, согласно (3):

$$R(\mathscr{F}) = R(\mathscr{G}) \leqslant \frac{1}{\rho_A} L(\mathscr{G}) - c_2\tilde{L}(\mathscr{G}) + 1 \leqslant \frac{1}{\rho_A} L(\mathscr{F}) - c_2\check{L}(\mathscr{F}) + 1,$$

$c_2 = \min\limits_M \left\{\frac{1}{\rho_A} - \frac{1}{\rho_M}\right\} > 0$, где минимум берется по всем макроблокам M в базисе A. Лемма доказана.

Теорема 5. *Пусть A, $A \subseteq P_2(X\cup Y)$, — полный базис, для которого множество $\hat{A}'$ является симметричным. Тогда при достаточно больших n справедливо соотношение*

$$L_A(n) \geqslant \rho_A \frac{2^n}{\log n}\left(1 + \frac{\omega_A \log\log n - O(1)}{\log n}\right).$$

Доказательство. Если $\hat{A}'' = \varnothing$, то требуемая оценка следует из теоремы 1. Для доказательства достаточно рассмотреть базис A_1, получаемый из базиса A объявлением всех входов элементов итеративными. Как показано в доказательстве леммы 2, приведенный вес элементов из A'' в таком случае не больше, чем ρ_A, а сложность функции в базисе A_1 может только уменьшиться с переходом из базиса A.

Если множество $\hat{A}''$ является согласованно симметричным, то достаточно рассмотреть базис A_2, элементы которого составлены из всех макроблоков базиса A, при этом все их входы объявлены итеративными. Множество элементов минимального приведенного веса базиса A_2

является симметричным, поэтому требуемая оценка также следует из теоремы 1.

Далее рассматривается случай, когда $\hat{A}'' \neq \varnothing$. Сначала покажем, что найдется такая константа c_3, $c_3 > 0$, что при любых натуральных n и L число $\xi_A(L,n)$ попарно не эквивалентных формул в базисе A, реализующих функции от n переменных и имеющих сложность не большую, чем L, не превосходит

$$\left(\frac{c_3 n}{(\log n)^{w_A}}\right)^{L/\rho_A}. \tag{5}$$

Можно считать, что $\hat{A}'$ содержит все различные функции своего замыкания, зависящие от более, чем одной переменной, соответствующие им элементы имеют вес, равный сложности реализации соответствующих функций в базисе $\hat{A}'$. Заметим при этом, что множество $\hat{A}'$ остается симметричным. Поэтому будем предполагать, что в минимальных формулах в базисе A выход любого элемента из $\hat{A}'$ либо является выходом формулы, либо подается на вход элемента из $\check{A}'$.

Чтобы задать формулу $\mathscr{F}$ в базисе A, необходимо:

1. выбрать дерево $\mathscr{D}$ этой формулы без учета элементов из $\hat{A}''$, вершины которого помечены функциональными символами из $A \setminus \hat{A}''$;
2. добавить все возможные помеченные переменными из $\{x_1,\ldots,x_n\}$ элементы из $\hat{A}''$, и изолированные вершины-переменные $x_1,\ldots,x_n$;
3. провести ребра, соединяющие добавленные на предыдущем шаги вершины с вершинами дерева $\mathscr{D}$;
4. превратить полученную схему в формулу дублированием элементов из $\hat{A}''$, из которых исходит более одного ребра и удалением изолированных вершин.

Обозначим через U множество вершин, добавляемых на шаге 2, его мощность удовлетворяет соотношению

$$|U| \leqslant c_4 \cdot n^{1/\omega_A}. \tag{6}$$

Число t ребер, добавляемых на шаге 3, не превосходит $R(\mathscr{F})$. Обозначим через T множество упорядоченных пар вершин, на которых эти t ребер могут быть размещены.

Пусть V — множество таких вершин дерева $\mathscr{D}$, которые помечены элементом $\mathscr{E}_i$, $\mathscr{E}_i \in \check{A}' \cup \check{A}'' \cup \hat{A}'$ для которых число входящих ребер меньше, чем k_i (с учетом замечания про замыкание $\hat{A}'$). Заметим, что

$$|V| \leqslant c_5 \cdot \check{L}, \tag{7}$$

где $\check{L} = \check{L}(\mathscr{F})$, т. к. число элементов из $\hat{A}'$ в формуле $\mathscr{F}$ не больше, чем число элементов из $\check{A}'$.

Каждая пара $(u,v) \in T$ такова, что $u \in U$, $v \in V$. Поэтому, с учетом (6), (7),

$$|T| \leqslant c_6 \cdot \check{L} \cdot n^{1/\omega_A}. \tag{8}$$

Число способов выбора дерева $\mathscr{D}$ не превосходит c_7^L, а число способов проведения ребер на шаге 3 не превосходит $\mathrm{C}_{|T|}^t$, откуда, с учетом приведенных выше оценок и леммы 2, следует, что

$$\xi_A(L,n) \leqslant c_7^L \cdot \max_{0 \leqslant \check{L} \leqslant L} \left(\frac{c_8 \cdot \check{L} \cdot n^{1/\omega_A}}{\frac{1}{\rho_A} L - c_2 \check{L} + 1} \right)^{\frac{1}{\rho_A} L - c_2 \check{L} + 1}.$$

Применяя к последнему неравенству лемму 1 при $y = \frac{c_2 \check{L}}{\rho_A / \omega_A}$, $\tau = 1$, $\alpha = 0$, $a = n^{1/\omega_A}$, $m = \frac{L}{\rho_A / \omega_A}$, получим искомую оценку (5).

Теперь, записав мощностное неравенство

$$2^{2^n} \leqslant \left(\frac{c_3 n}{\log^{\omega_A} n} \right)^{\frac{L_A(n)}{\rho_A}},$$

получим, что при достаточно больших n справедливо соотношение

$$L_A(n) \geqslant \rho_A \frac{2^n}{\log n} \left(1 + \frac{\omega_A \log\log n - O(1)}{\log n} \right),$$

что и доказывает теорему.

Верхняя оценка функции Шеннона

Если D — разбиение конечного множества Y на непересекающиеся непустые подмножества $Y_1, \ldots, Y_d$, то величина

$$H(D) = -\sum_{i=1}^{d} \frac{|Y_i|}{|Y|} \log \frac{|Y_i|}{|Y|}$$

называется энтропией (см., например, [5]) разбиения D.

Пусть $\varphi(y_1, \ldots, y_N)$ — функция, существенно зависящая от всех своих переменных из множества $Y = \{y_1, \ldots, y_N\}$, а D — разбиение множества Y на компоненты $Y_1, \ldots, Y_d$. Разбиение D называется *селекторным* [5] для функции $\varphi(Y)$, если для каждого i, $i = 1, \ldots, d$, и для любой переменной y, $y \in Y_i$, найдутся константы $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_d \in \{0,1\}$, такие, что при подстановке их вместо переменных из $Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_d$ соответственно, выполняется равенство $\varphi = y \oplus \alpha_i$, $\alpha_i \in \{0,1\}$.

Лемма 3 ([4]). *Пусть A, $A \subseteq P_2(X \cup Y)$ — конечный полный базис функций, такой, что $\delta(A) \supseteq M$. Пусть, далее, для любого натурального числа N существует формула $\mathscr{F}^{(N)}$ в этом базисе, реализующая некоторую функцию φ, зависящую от N прямых переменных, со сложностью $L(\mathscr{F}^{(N)}) \leqslant \rho_A \cdot N + O(1)$, где функция φ имеет селекторное разбиение D своих переменных с энтропией, удовлетворяющей неравенству $H(D) \leqslant \alpha \log N + O(1)$, $\alpha \in [0,1]$.*

Тогда для любой функции f, $f \in P_2(\{x_1,\ldots,x_n\})$ существует формула $\mathscr{F}_f$ в базисе A, реализующая эту функцию, и такая, что

$$L(\mathscr{F}_f) \leqslant \rho_A \frac{2^n}{\log n}\left(1+\frac{\alpha \log\log n + O(1)}{\log n}\right).$$

Условие $\delta(A) \supseteq M$ необходимо для того, чтобы гарантировать существование в базисе A бесповторных по своим существенным переменным формул $\mathscr{F}_\vee$ и $\mathscr{F}_\&$, реализующих функции $y_1 \vee y_2$ и $y_1 y_2$ соответственно. Вместе с этими формулами, блок $\mathscr{F}^{(N)}$ используется для построения необходимой формулы $\mathscr{F}_f$, реализующей наперед заданную функцию f.

Теорема 6. *Пусть A, $A \subseteq P_2(X \cup Y)$, — базис, для которого $M \subseteq \delta(A)$, и пусть $\hat{A}' = \{y_1 \circ \ldots \circ y_{k_1}\}$, а $\hat{A}''$ содержит функцию вида $\psi_2(x_1,\ldots,x_{k_2}) = g_1(x_{i_1},\ldots,x_{i_{t_1}}) \diamond g_2(x_{j_1},\ldots,x_{j_{t_2}})$, где $t_1, t_2 \geqslant 1$, числа $i_1,\ldots,i_{t_1},j_1,\ldots,j_{t_2}$ попарно различны, и в объединении дают множество $\{1,\ldots,k_2\}$, $(\circ,\diamond) \in \{(\&,\vee),(\&,\vee),(\oplus,\vee),(\oplus,\&)\}$, а функции g_1 и g_2 существенно зависят от своих переменных. Тогда для любой функции f, $f \in P_2(\{x_1,\ldots,x_n\})$ существует формула $\mathscr{F}_f$ в базисе A, реализующая эту функцию, и такая, что*

$$L(\mathscr{F}_f) \leqslant \rho_A \frac{2^n}{\log n}\left(1+\frac{\alpha \log\log n + O(1)}{\log n}\right),$$

где $\alpha = 1$, если приведенный вес базиса A достигается только на элементе, реализующем функцию $y_1 \circ \ldots \circ y_{k_1}$, и $\alpha = \frac{\min\{t_1,t_2\}}{k_2}$ в случае, когда приведенный вес базиса A достигается на макроблоке, отличном от элемента.

Доказательство.

Рассмотрим сначала случай, когда приведенный вес базиса A достигается на макроблоке, отличном от элемента.

Для каждого N, $N \geqslant 1$, обозначая $p = \lfloor \frac{N}{k_2} \rfloor$, построим формулу

$$\mathscr{F}^{(N)} = \psi_2(x_1,\ldots,x_{k_2}) \circ \psi_2(x_{k_2+1},\ldots,x_{2k_2}) \circ \ldots \circ \psi_2(x_{(p-1)k_2+1},\ldots,x_{pk_2}) \circ \\ \circ x_{pk_2+1} \circ \ldots \circ x_N.$$

Обозначим за L_1 вес элемента, реализующего функцию $y_1 \circ \ldots \circ y_{k_1}$, а за L_2 — вес элемента, реализующего функцию ψ_2. Приведенный вес базиса A в рассматриваемом случае равен

$$\rho_A = \frac{L_1 + L_2(k_1-1)}{k_2(k_1-1)}.$$

В формулу $\mathscr{F}^{(N)}$ входит p элементов ψ_2 и $\lfloor \frac{p}{k_1-1} \rfloor + O(1)$ элементов базиса $\hat{A}'$. Тогда сложность формулы $\mathscr{F}^{(N)}$ удовлетворяет соотношению

$$L(\mathscr{F}^{(N)}) = pL_2 + \frac{p}{k_1-1}L_1 + O(1) = \frac{p(k_1-1)L_2 + pL_1}{k_1-1} + O(1) = \rho_A N + O(1).$$

Будем считать, что $t_1 \leqslant t_2$, противоположный случай рассматривается аналогично. Также без ограничения общности можно предполагать, что $\psi_2(x_1,\ldots,x_{k_2}) = g_1(x_1,\ldots,x_{t_1}) \diamond g_2(x_{t_1+1},\ldots,x_{k_2})$. Рассмотрим следующее разбиение D множества переменных реализуемой формулой $\mathscr{F}^{(N)}$ функции:

$$D: \bigcup_{i=0}^{p-1}\bigcup_{j=1}^{t_1}\{x_{ik_2+j}\}\cup$$

$$\cup \bigcup_{j=t_1+1}^{k_2}\{x_i, x_{k_2+i},\ldots,x_{(p-1)k_2+i}\}\cup\{x_{pk_2+1}\}\cup\{x_{pk_2+2}\}\cup\ldots\cup\{x_N\}.$$

Оно состоит из $t_1\cdot p + N - pk_2$ компонент мощности 1 и $t_2 = k_2 - t_1$ компонент мощности p, и, как нетрудно видеть, при всех возможных указанных в условии теоремы операциях $(\circ,\diamond)$ является селекторным для функции, которую реализует формула $\mathscr{F}^{(N)}$. Его энтропия имеет вид

$$H(D) = (p+k_2)t_1\frac{1}{N}\log N + t_2\frac{p}{N}\log\frac{N}{p} = \frac{t_1}{k_2}\log N + O(1),$$

что с учетом сделанных замечаний и леммы 3 доказывает теорему.

Доказательство с $\alpha = 1$ для случая, когда приведенный вес базиса A достигается только на элементе, реализующем функцию $y_1\circ\ldots\circ y_{k_1}$, аналогично. Отличие состоит в том, что в качестве формулы $\mathscr{F}^{(N)}$ необходимо взять формулу $x_1\circ\ldots\circ x_N$ и тривиальное разбиение $D = \{\{x_1\},\ldots,\{x_n\}\}$ множества переменных реализуемой этой формулой функции, энтропия которого равна $\log N$.

Нетрудно видеть, что если множество $\hat{A}''$ пусто, то приведенная в теореме оценка остается справедливой при $\alpha = 1$. Также заметим, что доказательство оценки для случая, когда $\hat{A}'$ состоит из функций вида $y_1\circ\ldots\circ y_q\circ x_{q+1}\circ\ldots\circ x_{k_1}$, где $2\leqslant q\leqslant k_1$, аналогично.

Теоремы 5 и 6 доказывают теорему 4.

Отметим особенность влияния на оценки высокой степени точности разделения входов элементов на прямые и итеративные на примере базиса A, в котором $\hat{A}' = \{y_1y_2\}$. Если $\hat{A}'' = \{x_1x_2\}$, то константа в оценке (2) при повторном логарифме равна 1, если же $\hat{A}'' = \{x_1\vee x_2\}$, то она равна $\frac{1}{2}$, а если $\hat{A}'' = \{x_1\oplus x_2\}$, то эти константы определяют верхнюю и нижнюю оценку вида правой части (2) для функции Шеннона $L_A(n)$.

Литература

1. *Ложкин С. А.* О полноте и замкнутых классах функций алгебры логики с прямыми и итеративными переменными // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 1999. — № 3. — С. 35–41.

2. *Ложкин С. А.* Лекции по основам кибернетики: Учебное пособие. — М.: Изд. отдел ф-та ВМиК МГУ, 2004. — 256 с.

3. *Ложкин С. А., Коноводов В. А.* О сложности формул алгебры логики в некоторых полных базисах, состоящих из элементов с прямыми и итеративными входами // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 1. — С. 55–68.

4. *Ложкин С. А., Коноводов В. А.* Оценки высокой степени точности для сложности булевых формул в некоторых базисах из элементов с прямыми и итеративными входами // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 2. — С. 16–30.

5. *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.

6. *Яблонский С. В.* Введение в дискретную математику. — М.: Наука, 1986. — 384 с.

7. *Коноводов В. А.* Некоторые особенности задачи синтеза булевых формул в полных базисах с прямыми и итеративными входами // Учёные записки Казанского университета. Серия Физико-математические науки. — 2014. — Т. 156, № 3. — С. 76–83.

8. *Коноводов В. А.* Асимптотические оценки высокой степени точности для сложности булевых формул в некоторых базисах, состоящих из элементов с прямыми и итеративными входами // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г. — М.:МАКС Пресс, 2015. — С. 110-–113.