Дискретная математика

том 2 выпуск 2 * 1990

УДК 519.714,4+510.52

ФУНКЦИОНАЛЬНЫЕ ПРИБЛИЖЕНИЯ В ТЕОРИИ НИЖНИХ ОЦЕНОК СЛОЖНОСТИ СХЕМ

С. П. Юкна

Предлагается метод получения нижних оценок для сложности схем из функциональных элементов, основанный на построении сжимающих полуметрик в алгебрах реализуемых схемами объектов. Метод позволяет единым образом получать сверхполиномиальные нижние оценки для монотонных схем и некоторые новые оценки для других (в том числе немонотонных) схем. Приводятся нижняя оценка $\exp((\log_2 n)^2)$ для ограниченного класса схем в полном базисе $\{\&, \vee, ^-\}$ и оценка порядка $\exp(n^{1/4})$ для схем в некоторых трехзначных расширениях базиса $\{\&, \vee, ^-\}$.

§ 1. Введение

Рассматривается задача получения нижних оценок для сложности реализации индивидуальных булевых функций схемами из функциональных элементов. Предлагается общий метод — метод функциональных приближений, позволяющий получать нетривиальные (в ряде случаев сверхполиномиальные) нижние оценки при различных ограничениях на схемы. Метод представляет собой развитие некоторых идей работ [1—8] с точки зрения общей теории приближений.

Структура работы такова. В § 2 задача получения нижних оценок сложности сводится к построению согласованных с базисными операциями структур приближения на множестве реализуемых схемами объектов. В § 3 рассматривается схемная реализация подмножеств $X \subseteq P$ произвольной нижней полурешетки P и путем построения подходящей структуры приближения доказывается общая нижняя оценка для сложности реализации подмножеств $X \subseteq P$ схемами из функциональных элементов (СФЭ) в случае, когда на входы схем подаются атомы полурешетки P (теорема 3). В § 4 доказывается специальный вариант этой теоремы в случае, когда $P = A^n$ — полурешетка слов в произвольном конечном алфавите A. В § 5—7 демонстрируется, как, выбирая подходящий алфавит A, можно из этой общей оценки единым образом получать как все известные [2—5, 7—10] сверхполиномиальные нижние оценки для монотонных схем (этот случай соответствует двухбуквенному алфавиту $A = \{0, 1\}$), так и некоторые новые оценки для других (в том числе немонотонных) схем. В частности, приводятся нижняя оценка порядка $\exp((\log_2 n)^2)$ для СФЭ в полном базисе $\{\&, \vee, ^-\}$, вычисляющих достаточно много простых импликант реализуемых ими функций, и оценка порядка $\exp(n^{1/4})$ для СФЭ в некоторых трехзначных расширениях базиса $\{\&, \vee, ^-\}$. Там же сформулирован обозримый критерий применимости методов работ [2—5, 7]. Наконец, в приложении (§ 8) устанавливаются некоторые комбинаторные свойства фильтров в нижних полурешетках, нужные для доказательства основной теоремы 3.

Используемые далее без пояснений общеизвестные понятия, касающиеся теории булевых функций и схем, можно найти, например, в [11, 12]. Понятия, относящиеся к теории решеток, можно найти в [13, 14].

Работа докладывалась на заседании семинара по математическим вопросам кибернетики при МГУ (6 мая 1988 г.). Автор признателен участникам семинара за полезные обсуждения.

§ 2. Метод функциональных приближений

Нам будет удобно использовать теоретико-множественное определение схемы из функциональных элементов. Пусть даны некоторое множество объектов $\Omega \neq \varnothing$ (множество булевых функций, множество графов и т. п.), число $m \geqslant 1$ и некоторое семейство Б m-местных операций $f\colon \Omega^m \to \Omega$ (называемое далее базисом).

Схема из функциональных элементов со входом $H \subseteq \Omega$ (или *H-схема*) в базисе Б — это по определению множество объектов $S = \{a_1, \ldots, a_t\} \subseteq \Omega$, i-й объект a_i $(1 \leqslant i \leqslant t)$ в котором получается из предыдущих объектов $H \cup \{a_1, \ldots, a_{i-1}\}$ применением одной из базисных операций, т. е. $a_i = f(\tilde{a})$ для некоторых $f \in$ Б и $\tilde{a} \in (H \cup \{a_1, \ldots, a_{i-1}\})^m$. Число $t = |S|$ называется *размером* схемы S. (Если $S = \varnothing$, то полагаем $t = 0$.) Считается, что схема S реализует множество объектов $A \subseteq \Omega$, если $A \subseteq H \cup S$. В частности, S реализует объект $a \in \Omega$, если $a \in H \cup S$.

Пусть $L_{Б}(A, H)$ — минимальный возможный размер реализующей множество A H-схемы в базисе Б. Ясно, что

$$L_{Б}(A, H) = 0 \Leftrightarrow A \subseteq H.$$

Полуметрика на Ω — это неотрицательный функционал $\rho\colon \Omega^2 \to \mathbf{R}_+$ удовлетворяющий для любых $a, b, c \in \Omega$ условиям: $\rho(a, a) = 0$ и $\rho(a, b) \leqslant \rho(a, c) + \rho(c, b)$. Под полуметрикой на множестве $\mathcal{P}(\Omega)$ всех подмножеств множества Ω будем понимать произвольный функционал $\mu\colon \mathcal{P}(\Omega)^2 \to \mathbf{R}_+$, удовлетворяющий условиям:

1) $\mu(A, A) = 0$;
2) $\mu(A, C) \leqslant \mu(A \cup B, C) \leqslant \mu(A, C) + \mu(B, C)$ (аксиома выпуклости);
3) $\mu(A, B) \leqslant \mu(A, C) + \mu(C, B)$ (аксиома треугольника).

В частности, функционал сложности $L_{Б}(A, H)$ является полуметрикой на $\mathcal{P}(\Omega)$.

Доопределением полуметрики $\rho\colon \Omega^2 \to \mathbf{R}_+$ называется любая полуметрика μ на $\mathcal{P}(\Omega)$ такая, что $\mu(a, B) = \rho(a, B)$ для всех $a \in \Omega$ и $B \subseteq \Omega$, где, как обычно, $\rho(a, B) = \inf\{\rho(a, b) \mid b \in B\}$. (Здесь и далее мы будем иногда отождествлять одноэлементное множество $\{a\}$ с самим элементом a; в частности, записываем $\mu(a, B)$ вместо $\mu(\{a\}, B)$ и $A \cup a$ вместо $A \cup \{a\}$.) Для $A \subseteq \Omega$ полагаем $\rho(A, B) = \sup\{\rho(a, B) \mid a \in A\}$. Нетрудно видеть, что определенное таким образом расширение $\rho(A, B)$ полуметрики ρ до $\mathcal{P}(\Omega)$ является ее доопределением.

Определение. Функционал $\mu\colon \mathcal{P}(\Omega)^2 \to \mathbf{R}_+$ является *Б-сжимающим на подмножестве* $B \subseteq \Omega$ или *(Б, B)-сжимающим*, если для любых $f \in$ Б, $A \subseteq \Omega$ и $\tilde{a} \in A^m$ существует набор $\tilde{b} \in B^m$ такой, что

$$\mu(A \cup f(\tilde{a}), \quad B \cup f(\tilde{b})) \leqslant \mu(A, B).$$

Полуметрику $\rho\colon \Omega^2 \to \mathbf{R}_+$ назовем *(Б, B)-сжимающей*, если существует (Б, B)-сжимающее ее доопределение. Для $B \subseteq \Omega$ полагаем $Б(B) = \{f(\tilde{b}) \mid f \in Б, \tilde{b} \in B^m\}$.

Лемма 1. *Пусть* $\varnothing \neq H$, $B \subseteq \Omega$; ρ — *полуметрика на* Ω *и* $\delta = \rho(H \cup \text{Б}(B), B) > 0$. *Тогда для любого* (Б, B)-*сжимающего доопределения* μ *полуметрики* ρ *и любой* H-*схемы* S *в базисе* Б *выполнена оценка*

$$|S| \geqslant \delta^{-1}\mu(S, B) - 1.$$

Доказательство. Поведем его индукцией по $t = |S|$. Если $t = 0$, то $S = \varnothing$ и $\mu(\varnothing, B) \leqslant \rho(H, B) \leqslant \delta$. Пусть теперь $t \geqslant 1$. Тогда $S = S' \cup f(\tilde{a})$, где $f \in \text{Б}$, $\tilde{a} \in S'^m$ и S' — некоторая H-схема размера $\leqslant t - 1$. По индукционному предположению $\mu(S', B) \leqslant \delta t$. В силу сжимаемости μ существует набор $\tilde{b} \in B^m$ такой, что $\mu(S' \cup f(\tilde{a}), B \cup f(\tilde{b})) \leqslant \mu(S', B) \leqslant \delta t$. Отсюда с учетом аксиом треугольника и выпуклости заключаем:

$$\mu(S, B) \leqslant \mu(S' \cup f(\tilde{a}), \quad B \cup f(\tilde{b})) + \mu(B \cup f(\tilde{b}), B) \leqslant$$
$$\leqslant \delta t + \mu(B, B) + \rho(f(\tilde{b}), B) \leqslant \delta t + \delta,$$

что и дает требуемую оценку для $t = |S|$. Лемма доказана.

Общий метрический критерий сложности дает следующая

Теорема 1. *Пусть* $a \in \Omega$; $\varnothing \neq H$, $B \subseteq \Omega$ *и* ρ — *произвольная* (Б, B)-*сжимающая полуметрика на* Ω. *Тогда если*

$$\delta = \rho(H \cup \text{Б}(B), B) > 0,$$

то

$$L_{\text{Б}}(a, H) \geqslant \delta^{-1}\rho(a, B) - 1.$$

Доказательство. Пусть S — минимальная реализующая объект $a \in \Omega$ H-схема в базисе Б. Если $S = \varnothing$, то $a \in H$ и, стало быть, $\rho(a, B) \leqslant \delta$. Если же $S \neq \varnothing$, то $a \in S$. Поэтому $\mu(S, B) \geqslant \mu(a, B) = \rho(a, B)$ для любого (в том числе сжимающего) доопределения μ полуметрики ρ. По лемме 1

$$L_{\text{Б}}(a, B) = |S| \geqslant \delta^{-1}\mu(S, B) - 1 \geqslant \delta^{-1}\rho(a, B) - 1.$$

Теорема доказана.

Как строить сжимающие полуметрики? Можно поступать по аналогии с общей теорией приближений, т. е. определять $\rho(a, b)$ как меру точности приближения объекта $a \in \Omega$ объектом $b \in \Omega$ в той или иной «структуре приближений».

Структурой приближения на множестве Ω называется тройка $\sigma = (E, \oplus, \leqslant)$, где $E \subseteq \Omega$ — некоторое выделенное множество (называемое шкалой приближения); $\leqslant$ — предпорядок (т. е. транзитивное и рефлексивное отношение) на Ω; $(\Omega; \oplus)$ — аддитивная полугруппа с нулем $0 \in \Omega$, операция $\oplus$ которой монотонна относительно $\leqslant$, причем $0 \in E$ и $\forall a \in \Omega$ $(0 \leqslant a)$.

Каждая такая структура σ порождает следующую естественную меру $\rho_\sigma(a, b)$ точности приближения:

$$\rho_\sigma(a, b) = \inf\{t \geqslant 0 \mid \exists e \in E^{(t)}: \ a \leqslant b \oplus e\},$$

где $E^{(0)} \subseteq E^{(1)} \subseteq \ldots$ — последовательность линейных оболочек шкалы E в полугруппе $(\Omega; \oplus)$, т. е. $E^{(0)} = \{0\}$ и $E^{(t+1)} = \{a \oplus e \mid e \in E, \ a \in E^{(t)}\}$. Ясно, что ρ_σ является полуметрикой на Ω, причем $\rho_\sigma(a, b) = 0 \Leftrightarrow a \leqslant b$.

Через ρ^*_σ будем обозначать функционал ρ^*_σ: $\mathscr{P}(\Omega)^2 \to \{0, 1, \ldots\}$, задаваемый соотношением

$$\rho^*_\sigma(A, B) = \inf\{t \geqslant 0 \mid \exists e \in E^{(t)}: \ A \leqslant B \oplus e\},$$

где $B \oplus e = \{b \oplus e \mid b \in B\}$ и $A \leqslant B \Leftrightarrow \forall a \in A \exists b \in B$ $(a \leqslant b)$. Нетрудно видеть, что ρ^*_σ является полуметрикой на $\mathscr{P}(\Omega)$, причем $\rho^*_\sigma(A, B) \geqslant \rho_\sigma(A, B)$ для любых A, $B \subseteq \Omega$. Так как $\rho^*_\sigma(a, B) = \rho_\sigma(a, B)$, то отсюда следует, что ρ^*_σ является доопределением полуметрики ρ_σ.

Определение. Скажем, что структура $\sigma = (E, \oplus, \leqslant)$ *согласована* с базисом Б, если для всех $f \in \text{Б}$; $\tilde{a}$, $\tilde{b} \in \Omega^m$ и $e \in E^{(0)} \cup E^{(1)} \cup \ldots$

выполняются соотношения

$$\tilde{a} \leqslant \tilde{b} \Rightarrow f(\tilde{a}) \leqslant f(\tilde{b}),$$
$$f(\tilde{a} \oplus e) \leqslant f(\tilde{a}) \oplus e.$$

Здесь $\tilde{a} \oplus e = (a_1 \oplus e, \ \ldots, \ a_m \oplus e)$ и $\tilde{a} \leqslant \tilde{b} \Leftrightarrow \forall i = 1, \ \ldots, \ m$: $a_i \leqslant b_i$.

Лемма 2. *Если структура приближений* σ *согласована с базисом* Б, *то полуметрика* ρ_σ *является* (Б, B)*-сжимающей на любом* $B \subseteq \Omega$.

Доказательство. Так как функционал ρ_σ^* является доопределением полуметрики ρ_σ, то достаточно доказать его (Б, B)-сжимаемость. Пусть $f \in$ Б, $A \subseteq \Omega$, $\tilde{a} \in A^m$ и $t = \rho_\sigma^*(A, B)$. По определению ρ_σ^* существует объект $e \in E^{(t)}$ такой, что $A \leqslant B \oplus e$. Следовательно, имеется набор $\tilde{b} \in B^m$ такой, что $\tilde{a} \leqslant \tilde{b} \oplus e$. В силу согласованности σ с Б

$$A \cup f(\tilde{a}) \leqslant B \oplus e \cup f(\tilde{b} \oplus e) \leqslant (B \cup f(\tilde{b})) \oplus e,$$

т. е.

$$\rho_\sigma^*(A \cup f(\tilde{a}), \ B \cup f(\tilde{b})) \leqslant t = \rho_\sigma^*(A, \ B),$$

что и требовалось доказать.

Не всякая полуметрика является псевдометрикой, т. е., вообще говоря, $\rho(a, b) \neq \rho(b, a)$. Тем не менее любой паре (необязательно различных полуметрик ρ_0 и ρ_1 можно поставить в соответствие псевдометрику

$$[\rho_0, \rho_1](a, b) = \max\{\rho_0(a, b), \ \rho_1(b, a)\}.$$

Из теоремы 1 и леммы 2 вытекает следующая

Теорема 2. *Пусть* $a \in \Omega$; $\varnothing \neq H$, $B \subseteq \Omega$ *и* ρ_0, ρ_1*—полуметрики, порожденные согласованными с базисом* Б *структурами приближения. Тогда если*

$$\delta = [\rho_0, \rho_1] \ (H \cup \text{Б} \ (B), \ B) > 0,$$

то

$$L_\text{Б}(a, \ H) \geqslant \delta^{-1}[\rho_0, \ \rho_1](a, B) - 1.$$

В заключении данного параграфа отметим один очевидный (но весьма полезный для приложений) факт, позволяющий менять базис и тип реализуемых схемами объектов, сохраняя при этом сложность схем. С этой целью расширим несколько понятие гомоморфизма алгебр.

Пусть даны некоторые две алгебры $\langle \mathfrak{A}; F \rangle$ и $\langle \mathfrak{B}; G \rangle$ и отношение $Q \subseteq \mathfrak{A} \times \mathfrak{B}$. Скажем, что алгебра $\mathfrak{B}$ является *Q-образом* алгебры $\mathfrak{A}$, если для любой операции $f \in F$ найдется операция $g \in G$ такая, что для всех $\tilde{a} \in \mathfrak{A}^m$ и $\tilde{b} \in \mathfrak{B}^m$

$$\tilde{a} Q \tilde{b} \Rightarrow f(\tilde{a}) Q g(\tilde{b}).$$

Например, если ν: $\mathfrak{A} \to \mathfrak{B}$ есть гомоморфизм $\mathfrak{A}$ в $\mathfrak{B}$, то $\mathfrak{B}$ является Q-образом $\mathfrak{A}$ при $Q = \{(a, \ \nu(a)) \mid a \in \mathfrak{A}\}$. Для $H \subseteq \mathfrak{A}$ обозначим через $Q(H)$ «срез» отношения Q по H, т. е. полагаем $Q(H) = \{b \in \mathfrak{B} \mid \exists a \in H\colon aQb\}$. Индукцией по размеру схем легко доказывается следующая

Лемма 3. *Пусть* $a \in \mathfrak{A}$; $H \subseteq \mathfrak{A}$ *и* $Q \subseteq \mathfrak{A} \times \mathfrak{B}$. *Тогда для любого Q-образа* $\langle \mathfrak{B}; G \rangle$ *алгебры* $\langle \mathfrak{A}; F \rangle$ *выполнено соотношение*

$$L_F(a, \ H) \geqslant \inf\{L_G(b, \ Q(H)) \mid b \in Q(\{a\})\}.$$

§ 3. Основная теорема

Пусть $(P, \trianglelefteq)$—произвольная конечная нижняя полурешотка с нулем $0 \in P$. Элементы $x \in P$ будем называть точками, а множество точек $X \subseteq P$ — фигурами. Будем рассматривать сложность реализации фигур схемами в базисах, состоящих из так называемых $\exists$-операций на множестве всех фигур $\mathcal{P}(P)$. Для $x \in P$ и $Y \subseteq P$ записываем $x \trianglerighteq Y$, если $y \trianglelefteq x$ для некоторой $y \in Y$.

Определение. Операция $f\colon \mathcal{P}(P)^m \to \mathcal{P}(P)$ называется *$\exists$-операцией*, если существует система $\varnothing \neq \mathcal{I}_f \subseteq \mathcal{P}(\{1, \ldots, m\})$ такая, что для любых $x \in P$ и $\tilde{X} = (X_1, \ldots, X_m) \in \mathcal{P}(P)^m$ имеет место

$$x \trianglerighteq f(X) \Leftrightarrow (\exists \varnothing \neq I \in \mathcal{I}_f) \quad (\forall i \in I) \quad x \trianglelefteq X_i.$$

Примерами двухместных $\exists$-операций служат операция теоретико-множественного объединения $X \cup Y$ и следующая операция «сплетения» фигур: $X \odot Y = \{x \sqcup y \mid x \in X,\ y \in Y\}$, где $\sqcup$ — (частичная) операция взятия точной верхней грани в P. Для них $\mathcal{I}_\cup = \{\{1\}, \{2\}\}$ и $\mathcal{I}_\odot = \{\{1, 2\}\}$. Операция пересечения $X \cap Y$ не является $\exists$-операцией.

Пусть $\mathcal{H}$ — семейство «простейших» фигур, состоящее из пустой фигуры $\varnothing$ и всех одноточечных фигур $\{x\}$, где $x \in \{0\} \cup \mathrm{at}(P)$ и $\mathrm{at}(P)$ — множество всех атомов (т. е. минимальных, отличных от 0 точек) полурешетки P. В дальнейшем функционал сложности $L_Б(X, \mathcal{H})$ будем обозначать просто $L_Б(X)$.

Замечание. Если P — атомарная полурешетка, т. е. если каждая ее точка $x \neq 0$ является точной верхней гранью атомов, то все фигуры $X \subseteq P$ реализуемы $\mathcal{H}$-схемами в базисе $\{\odot, \cup\}$, причем

$$L_{\{\odot, \cup\}}(X) \leqslant |\mathrm{at}(P)|\,|X| + \log_2 |X|.$$

Главная цель настоящего параграфа — получить общую нижнюю оценку для $L_Б(X)$ через некоторые вероятностные характеристики распределения точек фигуры $X \subseteq P$ по отношению к некоторым подрешеткам полурешетки P.

Подмножество $M \subseteq P$ называем *правильной подрешеткой*, если $0 \in M$, $\mathrm{at}(P) \subseteq M$ и $(M, \trianglelefteq)$ образует нижнюю дистрибутивную полурешетку, каждый интервал $[0, x]$ $(x \in M)$ которой является полной решеткой. Пусть $\wedge$ и $\vee$ — операции взятия точной нижней и точной верхней грани в M. *Высота* $h(x)$ точки $x \in M$ определяется как длина самой длинной максимальной цепи в интервале $[0, x]$. Известно [13, 14], что в любой дистрибутивной полурешетке M для всех $x, y \in M$ (таких, что $x \vee y$ существует) выполняется равенство $h(x \vee y) = h(x) + h(y) - h(x \wedge y)$.

Мажорантой полурешетки M называется функция $\mu(r, k)$, определяемая соотношениями:

а) $\mu(r, 0) = \mu(1, k) = 1$ для всех $r \geqslant 1$ и $k \geqslant 0$;

б) $\mu(r+1, k) = \max\limits_{h(x)=k} \sum\limits_{y \trianglelefteq x} \mu(r, k - h(y))$.

Мажоранта характеризует «толщину» полурешетки M. В частности, $\mu(2, k)$ — это наибольшее число точек в интервалах $[0, x]$, где $h(x) = k$. *Дополнением* точки $x \in [0, y]$ в интервале $[0, y]$ называется точка $x^* \in [0, y]$ такая, что $x^* \vee x = y$ и $x^* \wedge x = 0$. Полурешетку M называем *полурешеткой со слабыми дополнениями*, если для любых $x, y \in M$ таких, что $h(x) = h(y)$, существуют дополнения точки $x \wedge y$ в интервалах $[0, x]$ и $[0, y]$. В частности, таковой является любая полурешетка с относительными дополнениями [13, 14].

Пусть теперь ξ — случайная точка, каким-то образом распределенная на M. Ее поведение на M описываем следующими двумя числовыми характеристиками:

$$\Lambda_\xi(s) = \max_{h(x)=s} \mathsf{P}[\xi \trianglerighteq x],$$

$$\Gamma_\xi(r, s) = \max \mathsf{P}[\neg(\xi \trianglerighteq X) \,\&\, (\xi \trianglerighteq \theta(X))],$$

где максимум берется по всем фигурам $X \subseteq M_s = \{x \in M \mid h(x) \leqslant s\}$ таким, что $|X| = r + 1$, а $\theta(X)$ — специальная точка, называемая *сцеплением* фигуры X и определяемая формулой

$$\theta(X)=\vee\{x\wedge y \mid x\neq y\in X\}.$$

Ясно, что $\Lambda_\xi(0)\geqslant\Lambda_\xi(1)\geqslant\ldots$, причем $\Lambda_\xi(0)=1$, поскольку $0\in M$. Скажем, что случайная точка ξ $(r, s)_a$*-разбросана* на M, если для всех $0\leqslant k\leqslant s-1$ выполняется неравенство

$$\Lambda_\xi(k)\geqslant\Lambda_\xi(k+1)\,\mu(r,\ k+1)\,(a+1)/\mu(r,\ k).$$

Теорема 3 (основная). *Пусть $X\subseteq P$ — произвольная фигура и* Б — *некоторый базис из m-местных $\exists$-операций, $m\geqslant 2$. Тогда для любой правильной подрешетки $M\subseteq P$ со слабыми дополнениями, любой $(r, s)_a$-разбросанной на M случайной точки ξ и любой случайной точки η из P таких, что $\Lambda_\xi(s)\ \Gamma_\eta(r, s)>0$, выполнено неравенство*

$$L_{\text{Б}}(X)\geqslant\min\left\{\frac{\mathsf{P}[\xi\trianglerighteq X]-a^{-1}}{2m\Lambda_\xi(v)\,\mu(r,\ v)},\ \frac{1-\mathsf{P}[\eta\trianglerighteq X]}{\Gamma_\eta(r,\ s)\,\mu(r+1,\ s)}\right\}-1,$$

где $v=[(s+1)/m]$ и μ — мажоранта полурешетки M.

Для доказательства теоремы нам понадобятся некоторые комбинаторные свойства фильтров. Фигуру $X\subseteq M$ называем *r-фильтром* $(r\geqslant 1)$ в M, если выполняются условия:

а) $X\ni x\trianglelefteq y\in M\Rightarrow y\in X$ (аксиома полуфильтра);

б) если $Y\subseteq X$, $|Y|=r+1$ и $\theta(Y)$ существует, то $\theta(Y)\in X$.

Наименьший r-фильтр в M, содержащий фигуру $X\subseteq M$, будем обозначать $X^{(r)}$. Таким образом, $X^{(1)}$ — это обычный фильтр, порожденный множеством X, причем

$$X^{(1)}\supseteq X^{(2)}\supseteq\ldots\supseteq X^{(t+1)}=X^{\triangledown},\ \text{где}\ t=|X|.$$

Важное свойство r-фильтров заключается в том, что они содержат сравнительно мало минимальных элементов. Точка $x\in X$ называется *гранью* фугуры $X\subseteq M$, если $\forall y\in X\ y\trianglelefteq x\Rightarrow y=x$. *Тенью* фигуры X в M называем фигуру $X^{\triangledown}=\{x\in M\mid x\trianglerighteq X\}$.

Лемма 4. *Пусть M — дистрибутивная нижняя полурешетка со слабыми дополнениями и μ — ее мажоранта. Тогда для любой фигуры $X\subseteq M$ и любых $k\geqslant 0$, $r\geqslant 1$ число граней высоты k в каждой из фигур $X^{(r)}$ и $X^{(r)}-X^{\triangledown}$ не превосходит $\mu(r,\ k)$.*

Доказательство этой леммы дается в приложении.

Доказательство теоремы 3. Применим описанный в § 2 метод в случае, когда $\Omega=\mathcal{P}(P)$ — множество всех фигур в полурешетке $(P,\ \trianglelefteq)$. Для фигур $X,\ Y\subseteq P$ полагаем

$$X\leqslant Y\Leftrightarrow\forall x\in X\colon\ x\trianglerighteq Y.$$

Наделим множество $\mathcal{P}(P)$ структурами $\sigma_0=(\mathcal{E}_0,\ \cup,\ \leqslant)$ и $\sigma_1=(\mathcal{E}_1,\ \cup,\ \leqslant)$, где $\mathcal{E}_0,\ \mathcal{E}_1\neq\varnothing$ — некоторые семейства фигур. Ясно, что такие структуры суть структуры приближения на $\mathcal{P}(P)$. Их согласованность с любым базисом из $\exists$-операций очевидна. Для применения теоремы 2 нам следует прежде всего подобрать семейства фигур $\mathcal{B}$, $\mathcal{E}_0$, $\mathcal{E}_1\subseteq\mathcal{P}(P)$ такими, чтобы для порождаемых этими структурами полуметрик ρ_0 и ρ_1 «базисный дефект» $\delta=[\rho_0,\ \rho_1](\mathcal{H}\cup\text{Б}(\mathcal{B}),\ \mathcal{B})$ был небольшим.

С этой целью возьмем в качестве $\mathcal{B}$ множество всех r-фильтров в полурешетке $(M_s,\ \trianglelefteq)$, где $M_s=\{x\in M\mid h(x)\leqslant s\}$. Для определения шкал приближения $\mathcal{E}_0$ и $\mathcal{E}_1$ свяжем с каждой $\exists$-операцией $f\in\text{Б}$ следующую операцию:

$$f[X_1,\ \ldots,\ X_m]=\bigcup_{I\in\mathcal{I}_f}\ \bigcap_{i\in I}X_i.$$

Ясно, что $f[\tilde{X}]\leqslant f(\tilde{X})$, хотя, вообще говоря, $f[\tilde{X}]\neq f(\tilde{X})$. Возьмем в качестве $\mathcal{E}_0$ и $\mathcal{E}_1$ множества, состоящие соответственно из фигур вида $f(\tilde{X})-f[\tilde{X}]^{\triangledown}$ и $f[\tilde{X}]^{(r)}-f(\tilde{X})^{\triangledown}$, где $f\in\text{Б}$, $\tilde{X}\in\mathcal{B}^m$ и $Y^{\triangledown}$ — тень фигуры $Y\subseteq P$ в P.

Нетрудно видеть, что при таком выборе множеств $\mathscr{B}$, $\mathscr{E}_0$ и $\mathscr{E}_1$ имеем $\delta=1$. Действительно, поскольку $\tilde{X}\in\mathscr{B}^m$ влечет $f[X]^{(r)}\in\mathscr{B}$, то $[\rho_0, \rho_1]\times\times(\text{Б}(\mathscr{B}), \mathscr{B})\leqslant 1$. Кроме того, поскольку $\mathrm{at}(M)\subseteq M_s$ и $\mathscr{B}$ содержит все главные фильтры $\{x\}^\nabla\cap M_s$, $x\in M_s$, то $[\rho_0, \rho_1](\mathscr{H}, \mathscr{B})=0$.

Итак, согласно теореме 2

$$L_{\text{Б}}(X)\geqslant[\rho_0, \rho_1](X, \mathscr{B})-1.$$

Возьмем фигуру $Y\in\mathscr{B}$, для которой $[\rho_0, \rho_1](X, Y)=[\rho_0, \rho_1](X, \mathscr{B})$. Пусть α и β — максимальные вероятности событий $\xi\trianglerighteq E$ и $\eta\trianglerighteq E$, где E пробегает соответственно $\mathscr{E}_0$ и $\mathscr{E}_1$.

Случай 1. $0\notin Y$. По определению полуметрики ρ_0 в семействе $\mathscr{E}_0$ найдется $t=\rho_0(X, Y)$ фигур $E_1, \ldots, E_t$ таких, что $X\leqslant Y\cup E_1\cup\ldots\cup E_t$, откуда

$$t\geqslant(\mathsf{P}[\xi\trianglerighteq X]-\mathsf{P}[\xi\trianglerighteq Y])\cdot\alpha^{-1}.$$

Оценим $\mathsf{P}[\xi\trianglerighteq Y]$. Согласно лемме 4 множество G всех граней r-фильтра Y содержит не более $\mu(r, k)$ точек высоты k $(0\leqslant k\leqslant s)$. Кроме того, $\forall x\in G$: $h(x)\geqslant 1$, так как $0\notin Y$. Учитывая $(r, s)_a$-разбросанность точки ξ и то, что $\mu(r, 0)=\Lambda_\xi(0)=1$, получаем

$$\mathsf{P}[\xi\trianglerighteq Y]=\mathsf{P}[\xi\trianglerighteq G]\leqslant\sum_{k=1}^{s}\Lambda_\xi(k)\,\mu(r, k)\leqslant\Lambda_\xi(0)\,\mu(r, 0)\sum_{k=1}^{s}(a+1)^{-k}<a^{-1}.$$

Оценим α. Возьмем $E\in\mathscr{E}_0$ такую, что $\alpha=\mathsf{P}[\xi\trianglerighteq E]$. Фигура E имеет вид $f(\tilde{X})-f[\tilde{X}]^\nabla$, где $f\in\text{Б}$ и $\tilde{X}=(X_1, \ldots, X_m)$ — набор r-фильтров в M_s. Пусть $\xi\trianglerighteq E$. Тогда по определению $\exists$-операции f найдется множество индексов $\varnothing\neq I\subseteq\{1, \ldots, m\}$ и для каждого $i\in I$ — грань x_i фигуры X_i такие, что $\forall i\in I$: $\xi\trianglerighteq x_i$. Так как M — правильная подрешетка, то существует $x=\sup_M\{x_i\mid i\in I\}$, причем $\xi\trianglerighteq x$, поскольку ξ принимает значения из M. Но тогда $h(x)\geqslant s+1$, так как в противном случае в силу того, что X_i суть полуфильтры в M_s, имело бы место $x\in\bigcap_{i\in I}X_i$, т. е. $\xi\trianglerighteq x\in f[\tilde{X}]^\nabla$, что невозможно. Следовательно, если $\xi\trianglerighteq E$, то ξ покрывает некоторую грань высоты, не меньшей чем $h(x)/|I|\geqslant[(s+1)/|I|]\geqslant v$, хотя бы одного из $|I|\leqslant m$ r-фильтров X_i, $i\in I$. Отсюда с учетом леммы 4 и $(r, s)_a$-разбросанности точки ξ имеем

$$\alpha=\mathsf{P}[\xi\trianglerighteq E]\leqslant\sum_{k=v}^{s}m\Lambda_\xi(k)\,\mu(r, k)<2m\Lambda_\xi(v)\,\mu(r, v).$$

Случай 2. $0\in Y$. По определению ρ_1 в семействе $\mathscr{E}_1$ найдется $t=\rho_1(Y, X)$ фигур $E_1, \ldots, E_t$ таких, что $Y\leqslant X\cup E_1\cup\ldots\cup E_t$. Поскольку $0\in Y$, то

$$t\geqslant(1-\mathsf{P}[\eta\trianglerighteq X])\,\beta^{-1}.$$

Оценим β. Вспомним, что каждая фигура E из $\mathscr{E}_1$ имеет вид $W^{(r)}-V^\nabla$, где $W\subseteq M_s$ и $W\leqslant V$. Поэтому $\mathsf{P}[\eta\trianglerighteq E]\leqslant\mathsf{P}[\eta\trianglerighteq W^{(r)}-W^\nabla]=\mathsf{P}[\eta\trianglerighteq G]$, где G — множество всех граней фигуры $W^{(r)}-W^\nabla$. По лемме 4 $|G|\leqslant\leqslant\sum_{k=0}^{s}\mu(r, k)\leqslant\mu(r+1, k)$. С другой стороны, по определению r-фильтра $W^{(r)}$ каждая точка $x\in G$ является сцеплением $\theta(Z)$ некоторой фигуры $Z\subseteq M_s$, $|Z|=r+1$. Поэтому

$$\beta=\mathsf{P}[\eta\trianglerighteq E]\leqslant\mathsf{P}[\eta\trianglerighteq G]\leqslant|G|\,\Gamma_\eta(r, s)\leqslant\Gamma_\eta(r, s)\,\mu(r+1, s).$$

Таким образом, независимо от того, содержит или нет фигура Y нуль полурешетки P, расстояние $[\rho_0, \rho_1](X, Y)$ оценивается снизу минимумом указанных в формулировке теоремы выражений. Теорема доказана.

§ 4. Вычисления в полурешетках слов

Пусть A — некоторый конечный алфавит букв, $|A| \geqslant 2$. Зафиксируем произвольную букву $* \in A$ и рассмотрим нижнюю дистрибутивную полурешетку $(A^n, \trianglelefteq)$ с нулем $(*, \ldots, *)$, где

$$x \trianglelefteq y \Leftrightarrow \forall i = 1, \ldots, n: \; x_i \in \{*, y_i\}.$$

Атомы этой полурешетки суть слова вида $(*, \ldots, *, a, *, \ldots, *)$, где $a \in A - \{*\}$. *Весом* $\|x\|$ слова $x \in A^n$ считаем число отличных от $*$ букв в x. Ясно, что тогда $h(x) = \|x\|$ является функцией высоты в $(A^n, \trianglelefteq)$, а функция $\mu(r, k) = r^k$ — ее мажорантой.

Для $k \geqslant 0$ и $X \subseteq A^n$ обозначим через $\lambda_k(X)$ наибольшее число граней фигуры X в полурешетке $(A^n, \trianglelefteq)$, имеющих не менее k общих отличных от $*$ букв. Тогда $\lambda_0(X) \geqslant \lambda_1(X) \geqslant \ldots \geqslant \lambda_n(X) = 1$, причем $\lambda_0(X)$ — число всех граней фигуры X. Пусть $\Delta_{i, j}(X) = \lambda_i(X)/\lambda_j(X)$. Фигуру $X \subseteq A^n$ называем (r, s)-*редкой*, если $\Delta_{k, k+1}(X) \geqslant 3r$ для всех $k = 0, 1, \ldots, s-1$.

Случайное слово η, принимающее значения из A^n, будем называть *локально независимым*, если для любых двух слов $x, y \in A^n$ при условии, что $\eta \trianglerighteq x \wedge y$, события $\eta \trianglerighteq x$ и $\eta \trianglerighteq y$ независимы.

С каждой фигурой $X \subseteq A^n$ связываем следующие две ее комбинаторные характеристики:

$$\Phi(X, r, s) = \max \Delta_{0, v}(Y) \, r^{-v},$$

где $v = [(s+1)/2]$ и максимум берется по всем (r, s)-редким фигурам $Y \subseteq A^n$ таким, что $Y \leqslant X$; и

$$\Psi(X, r, s, \eta) = (1 - \mathsf{P}[\eta \trianglerighteq X]) (r+1)^{-s} (1 - q_\eta(s))^{-(r+1)},$$

где

$$q_\eta(s) = \min \{\mathsf{P}[\eta \trianglerighteq x] \mid x \in A^n, \; \|x\| = s\}.$$

Легко видеть, что для любой фигуры $X \subseteq A^n$ имеет место

$$L_{\{\odot, \cup\}}(X) \leqslant n|X| + \log_2 |X|.$$

Нижнюю оценку дает следующая

Теорема 4. *Если $r, s \geqslant 1$, $X \subseteq A^n$ и η — случайное локально-независимое слово в A^n, то*

$$L_{\{\odot, \cup\}}(X) \geqslant \frac{1}{8} \min \{\Phi(X, r, s) \Psi(X, r, s, \eta)\} - 1.$$

Доказательство. Применим теорему 3 в случае, когда $P = M = (A^n, \trianglelefteq)$. Возьмем (r, s)-редкую фигуру $Y \leqslant X$, при которой выражение $\Phi(X, r, s)$ достигает своего максимума. Пусть ξ — случайная величина, независимо и с одинаковой вероятностью $\lambda_0(Y)^{-1}$ принимающая значения из множества G всех граней фигуры Y. Так как $Y \leqslant X$, то $\mathsf{P}[\xi \trianglerighteq X] = \mathsf{P}[\xi \trianglerighteq G] = 1$. Кроме того, ξ является $(r, s)_2$-разбросанной, поскольку $\Lambda_\xi(i) = \Delta_{0, i}(Y)$ и $\Delta_{i, j}(Y) = \Lambda_\xi(i)/\Lambda_\xi(j)$. Так как $\mu(r, k) = r^k$, то в силу теоремы 3 остается оценить $\Gamma_\eta(r, s)$.

Возьмем фигуру $W \subseteq \{x \in A^n \mid \|x\| \leqslant s\}$ такую, что $|W| = r+1$ и $\Gamma_\eta(r, s) = \mathsf{P}[\neg(\eta \trianglerighteq W) \& (\eta \trianglerighteq \theta(W))]$. В силу локальной независимости η

$$\Gamma_\eta(r, s) \leqslant \mathsf{P}[\neg(\eta \trianglerighteq W) \mid \eta \trianglerighteq \theta(W)] = \prod_{x \in W} \mathsf{P}[\neg(\eta \trianglerighteq x) \mid \eta \trianglerighteq \theta(W)] \leqslant (1 - q_\eta(s))^{r+1}.$$

Теорема доказана.

Сформулируем вариант теоремы 4 в случае, когда случайное слово η распределено по биномиальному закону.

Теорема 4'. *Пусть $* \in B \subseteq A$, $|B| \geqslant 2$, $X_n \subseteq B^n$ — последовательность фигур в алфавите B, $R(X_n) = \min \{\|x\| \mid x \in X_n\}$ и $0 \leqslant \varepsilon = \varepsilon_n < (|B| - 1)^{-1}$,* *Тогда при $n \to \infty$ выполнена оценка*

$$L_{\{\odot, \cup\}}(X_n) \geqslant \frac{1}{8} \min\{\Phi(X_n, r, s), \psi(X_n, r, s, \varepsilon)\} - 1,$$

где

$$\psi = (1 - \lambda_0(X_n)\,\varepsilon^{R(X_n)}) \exp\{(r+1)\,\varepsilon^s - s\ln(r+1)\}.$$

Доказательство. Пусть η — случайное слово из B^n, в котором каждая отличная от $*$ буква появляется независимо и с одинаковой вероятностью ε. Тогда η локально независимо, причем $q_\eta(s) = \varepsilon^s$. Поэтому $\Psi(X_n, r, s, \eta) \geqslant \psi(X_n, n, s, \varepsilon)$, что вместе с теоремой 4 и дает требуемый результат. Теорема доказана.

Опираясь на полученные результаты, можно единым образом и достаточно просто получать нетривиальные нижние оценки в различных классах СФЭ. В следующих трех параграфах продемонстрируем это на трех классах схем: СФЭ в базисе $\{\&, \vee, 0, 1\}$, СФЭ в полном базисе $\{\&, \vee, {}^-\}$ при некоторых дополнительных ограничениях на способ их функционирования и СФЭ в некоторых трехзначных расширениях базиса $\{\&, \vee, {}^-\}$.

§ 5. Монотонные схемы

В этом случае берем алфавит $A = \{0, 1\}$ и 0 в качестве выделенной буквы, т. е. полагаем $* = 0$. Тогда $\trianglelefteq$ — это обычное отношение $\leqslant$ частичного порядка на $\{0, 1\}^n$.

Пусть $\mathbf{B}_n^+$ — множество всех монотонных булевых функций от n переменных. С каждой $f \in \mathbf{B}_n^+$ можно связать фигуру $X_f \subseteq A^n$, состоящую из всех нижних единиц функции f. Иными словами, X_f — это множество всех граней фигуры $f^{-1}(1)$ в решетке $(A^n, \leqslant)$. В частности, для констант 0, 1 и переменной x_i имеем: $X_0 = \varnothing$, $X_1 = \{(0, \ldots, 0)\}$ и $X_{x_i} = \{(0, \ldots, 1, 0, \ldots, 0)\}$ с единицей на i-м месте.

Пусть $L^+(f)$ — сложность реализации монотонной функции f СФЭ в базисе $\{\&, \vee, 0, 1\}$. Поскольку алгебра фигур $\langle \mathcal{P}(A^n); \odot, \cup \rangle$ является, как нетрудно видеть, Q-образом алгебры монотонных функций $\langle \mathbf{B}_n^+; \&, \vee \rangle$ при $Q = \{(f, X_f) \mid f \in \mathbf{B}_n^+\}$, то из леммы 3 вытекает следующее вспомогательное

Предложение 1. $\forall f \in \mathbf{B}_n^+$: $L^+(f) = L_{\{\odot, \cup\}}(X_f)$.

С учетом этого факта из теоремы 4 при подходящих $r, s \geqslant 1$ и $0 \leqslant \varepsilon < (|A| - 1)^{-1} = 1$ можно вывести все известные [2—5, 7, 9] сверхполиномиальные нижние оценки для L^+.

Возьмем, например, монотонную функцию $f_{n,s}$ от $n = m^2$ переменных $\{x_{ij} \mid 1 \leqslant i, j \leqslant m\}$, соответствующую множеству тех графов на m вершинах, которые содержат полный подграф не менее чем на s вершинах:

$$f_{n,s} = \bigvee_{|I| = s} \mathop{\&}_{i, j \in I} x_{ij}.$$

Пусть $X \subseteq \{0, 1\}^n$ — множество нижних единиц функции $f_{n,s}$. Тогда $R(X) = s^2$ и фигура X является (r, k)-редкой для всех $r \leqslant [m/3]$ и $k \leqslant s$, поскольку

$$\lambda_k(X) = \binom{m-k}{s-k}, \quad \Delta_{k, k+i}(X) \geqslant \left(\frac{m-k}{s-k}\right)^i.$$

Возьмем $s = \left[\frac{1}{4}(m/\ln m)^{2/3}\right]$, $k = [\sqrt{s}]$, $r = [4k\ln m]$ и $\varepsilon = m^{-2/s}$. Тогда

$$\lambda_0(X) \cdot \varepsilon^{R(X)} = \binom{m}{s} m^{-2s} \leqslant m^{-s}, \quad (r+1) \cdot \varepsilon^k - k\ln(r+1) \gtrsim m^{1/3 - o(1)}.$$

Поэтому, подставляя эти значения параметров r, k и ε в выражения $\Phi(X, r, k)$ и $\psi(X, r, k, \varepsilon)$, после несложных преобразований получаем следующую оценку:

$$L^+(f_{n,s}) = L_{\{\odot, \cup\}}(X) \geqslant \exp(n^{1/6 - o(1)}),$$

где $f \gg \exp(g)$ служит сокращением для

$$(\exists C > 1)(\forall m)(\exists n \geqslant m) f(n) \geqslant C^{g(n)}.$$

Совершенно аналогично из теоремы 4 вытекают все остальные оценки работ [2—5, 7, 9], в том числе и приводимая в [3] рекордная для L^+ нижняя оценка, рост которой достигает $\exp(n^{1/3-o(1)})$. Это обстоятельство позволяет сформулировать следующий критерий применимости методов работ [2—5, 7, 9].

Для последовательности монотонных булевых функций f_n ($n=1, 2, \ldots$) через $G_n(k)$ обозначим соотношение $\lambda_n(0)/\lambda_n(k)$, где $\lambda_n(k)$ — наибольшее число нижних единиц функции f_n, имеющих не менее $k \geqslant 0$ общих единичных координат.

Критерий. *Если существует последовательность локально-независимых случайных наборов* $\tilde{\alpha}_n$ *из* $\{0, 1\}^n$ ($n=1, 2, \ldots$) *такая, что*

$$\mathsf{P}[f_n(\tilde{\alpha}_n)=0] \gtrsim \mathrm{const} > 0,$$

$$\mathsf{P}[\|\tilde{\alpha}_n\| \geqslant s] \gtrsim r^{-1} \ln G_n(s)$$

для некоторых $r(n)$, $s(n)$ *таких, что* $\ln r \lesssim s^{-1} \ln G_n(s)$, *то*

$$L^+(f_n) \gtrsim G_n(s)\, r^{-s}.$$

Другими словами, методы работ [2—5, 7, 9] применимы к тем функциям $f \in \mathbf{B}_n^+$, которые одновременно содержат достаточно много «сильно разбросанных» по вершинам куба $\{0, 1\}^n$ нижних единиц веса $\ll n/2$ и достаточно много верхних нулей веса $\gg n/2$.

§ 6. Схемы в полном базисе

Будем рассматривать «регулярные» СФЭ в базисе $\{\&, \vee, {}^-\}$, т. е. СФЭ, все отрицания в которых подсоединены непосредственно к входам схемы. (Путем несложных преобразований всякую СФЭ в базисе $\{\&, \vee, {}^-\}$ можно привести к регулярному виду с не более чем двухкратным увеличением сложности схем.)

Всякая СФЭ S в базисе $\{\&, \vee, {}^-\}$ реализует не только булеву функцию f_S, но и некоторую ее дизъюнктивную нормальную форму (ДНФ) D_S, получающуюся из соответствующей формулы раскрытием скобок с последующим удалением тождественно нулевых конъюнкций. Поэтому путем наложения ограничений на вид реализуемых ДНФ можно выделять те или иные классы схем.

Пусть $PI(f)$ — множество всех простых импликант функции f, т. е. ее сокращенная ДНФ. Импликанта $K \in PI(f)$ называется *ядровой*, если существует набор $\tilde{\alpha} \in f^{-1}(1)$ такой, что $K(\tilde{\alpha})=1$ и $W(\tilde{\alpha})=0$ для любой другой $W \in PI(f)$, $W \neq K$. Пусть Я(f) — множество всех ядровых импликант функции f. Для действительного числа $\delta \in [0, 1]$ через $\mathscr{D}_\delta(f)$ будем обозначать множество всех ДНФ D функции f таких, что

$$|D \cap \text{Я}(f)| \geqslant \delta\, |\text{Я}(f)|.$$

Определение. Схема S в базисе $\{\&, \vee, {}^-\}$ называется *δ-схемой*, если $D_S \in \mathscr{D}_\delta(f_S)$.

Ясно, что всякая СФЭ в базисе $\{\&, \vee, {}^-\}$ является δ-схемой при некотором $\delta \in [0, 1]$. Частным случаем 1-схем являются рассматриваемые в [15] «схемы с минимально достаточными конъюнкциями» (min-схемы). Это такие схемы S, для которых $D_S \subseteq PI(f_S)$; ясно, что тогда $D_S \cap \text{Я}(f_S) = \text{Я}(f_S)$.

Пусть $L_\delta(f)$ — сложность реализации функции f в классе δ-схем. Поведение этого функционала рассматривалось многими авторами. Так, в [15] построена последовательность $f_n \in \mathbf{B}_n^+$ ($n=1, 2, \ldots$) такая, что $L_1(f_n) \leqslant 2n$, но $L_{\min}(f_n) \geqslant \exp(n^{1/4})$. Это значит, что уже при $\delta = 1$ δ-схемы существенно сильнее, чем min-схемы. Следующий важный шаг был сделан А. Е. Андреевым и А. А. Разборовым в работах [2—5], где получены сверхполиномиальные нижние оценки для $L^+(f)$. Эти оценки прямо переносятся и для $L_1(f)$, поскольку $L_1(f) = L^+(f)$ для любой монотонной f. Это следует из того, что, как нетрудно видеть, любая реализующая монотонную функцию минимальная 1-схема не содержит нулевых цепей (каждый вход $\bar{x}_i$ можно заменить на константу 0).

Однако известно [5, 9, 16, 17], что наличие нулевых цепей ведет к почти экспоненциальному уменьшению сложности схем. Поэтому представляет интерес задача получения нижних оценок для $L_\delta(f)$ при $\delta < 1$ и, в частности, для сложности реализации немонотонных ДНФ схемами в полном базисе. Теорема 4 позволяет получать некоторые результаты в этом направлении.

Рассмотрим алфавит $A = \{*, 0, 1\}$. Каждой элементарной конъюнкции от n переменных можно поставить в соответствие слово в A^n. Например, $x_1\bar{x}_3x_4 \leftrightarrow (1, *, 0, 1, *, \ldots, *)$. При этом ДНФ превращаются в фигуры $D \subseteq A^n$ нижней полурешетки $(A^n, \trianglelefteq)$. При этом ДНФ D реализует f, если $f^{-1}(1) = D^\nabla \cap \{0, 1\}^n$. Рассматривая отношение $Q = \{(f, D) | D$ реализует $f\}$, из леммы 3 получаем следующее вспомогательное

Предложение 2. *Для произвольной булевой функции f и любого $\delta \in [0, 1]$ справедлива оценка*

$$L_\delta(f) \geqslant \min_{D \in \mathcal{D}_\delta(f)} L_{\{\odot, \cup\}}(D).$$

Пример 1. Пусть $d \geqslant 2$ и Π—множество всех полиномов $p(t)$ степени не выше $d-1$ над полем Галуа $GF(m)$ порядка m (m—степень простого числа). Зафиксируем произвольный элемент $e \neq 0$ поля $GF(m)$ и с каждым полиномом $p \in \Pi$ свяжем следующие две элементарные конъюнкции:

$$K_p^+ = \& \, x_{i,\, p(i)} \quad \text{и} \quad K_p^- = \& \, \bar{x}_{i,\, p(i) \oplus e}, \quad \text{где} \quad i \in GF(m).$$

Пусть $f = f_{n,d}$—булева функция от $n = m^2$ переменных, реализуемая следующей ДНФ:

$$D^0 = \bigvee_{p \in \Pi} K_p^+ \,\&\, K_p^-.$$

Ясно, что f немонотонная, причем конъюнкции $K_p^+ \& K_p^-$ суть ядровые импликанты f. Так как ДНФ D^0 тупиковая, то отсюда получаем, что $D^0 = Я(f)$.

Следствие 1. *Пусть $d = \left[\frac{1}{4}\log_2 n\right]$ и $n^{\varkappa - 1/4} \leqslant \delta(n) \leqslant 1$ для некоторой константы $\varkappa > 0$. Тогда*

$$L_\delta(f_{n,d}) \geqslant \delta \exp((\log_2 n)^2).$$

Доказательство. Возьмем произвольную ДНФ $D \in \mathcal{D}_\delta(f_{n,d})$. Пусть $Y = D \cap D^0$. Тогда $Y \leqslant D$, причем для всех $k = 0, \ldots, d-1$

$$\delta m^{d-k} \leqslant \lambda_k(Y) \leqslant m^{d-k}.$$

Следовательно, фигура Y является (r, s)-редкой для любых $s \leqslant d-2$ и $r \leqslant [\delta m/3]$, причем $\Delta_{0,k}(Y) \geqslant \delta m^k$. С другой стороны, нетрудно видеть, что для любой ДНФ D, реализующей $f_{n,d}$,

$$D \leqslant \bigvee_{p_1, p_2 \in \Pi} K_{p_1}^+ \& K_{p_2}^-,$$

откуда $\lambda_0(D)\, \varepsilon^{R(D)} \leqslant m^{2d} \varepsilon^{2m}$. Поэтому, полагая $r = [\delta\sqrt{m}]$, $s = d-2$ и $\varepsilon = ((\ln r)^2/r)^{1/s}$, из теоремы 4 с учетом предложения 2 после несложных преобразований получаем требуемую нижнюю оценку для $L_\delta(f_{n,d})$. Следствие доказано.

Для сравнения приведем очевидную верхнюю оценку

$$\forall\delta \in [0, 1]: \ L_\delta(f_{n,d}) \leqslant \exp((\log_2 n)^2).$$

Отсюда, в частности, следует, что для сколь угодно близкой к нулю константы $\delta \in (0, 1]$ сложность реализации функции $f_{n,d}$ в классе δ-схем (в базисе $\{\&, \vee, {}^-\}$) совпадает по порядку с длиной кратчайшей ее ДНФ.

§ 7. Схемы в трехзначных базисах

Пусть $\mathcal{F}^{(n)}$ — семейство всех функций f: $A^n \to A$, где $A = \{0, 1, 2\}$. Для $F \subseteq \mathcal{F}^{(1)}$ через HF будем обозначать семейство всех функций $f \in \mathcal{F}^{(n)}$ таких, что $f(x_1, \ldots, x_n) = \nu(x_i)$ для некоторых $1 \leqslant i \leqslant n$ и $\nu \in F$. Для буквы $* \in A$ через F_* обозначаем множество всех одноместных функций ν: $A \to \{0, 1\}$ таких, что либо $\nu \equiv 1$, либо $\nu(*) \neq 1$. В частности, множество F_* содержит все три константы 0, 1, 2 и функции $J_a(x)$ $(a \in A)$ такие, что

$$J_*(x) \equiv 1 \quad \text{и} \quad J_a(x) = 1 \Leftrightarrow x = a \quad \text{для} \quad a \neq *.$$

Пусть $x \otimes y = xy \pmod 2$ и $x \vee y = \max(x, y)$.

Зафиксируем букву $* \in A$ и рассмотрим полурешетку $(A^n, \trianglelefteq)$. Пусть $\mathcal{T}_*^{(n)} \subset \mathcal{F}^{(n)}$ — семейство таких функций f: $A^n \to \{0, 1\}$, что $f^{-1}(1) \ni \tilde{x} \trianglelefteq \tilde{y} \Rightarrow$ $\Rightarrow f(\tilde{y}) = 1$. Из представления

$$f(\tilde{x}) = \bigvee_{\tilde{\alpha} \in A^n} J_{\alpha_1}(x_1) \otimes \ldots \otimes J_{\alpha_n}(x_n) \otimes f(\tilde{\alpha})$$

следует, что все функции из $\mathcal{T}_*^{(n)}$ реализуемы схемами в базисе $\{\otimes, \vee\}$ со входом HF_*. Функционал сложности $L_{\{\otimes, \vee\}}(f, HF_*)$ будем обозначать просто $L^*(f)$. При получении нижних оценок для этого функционала можно использовать теорему 4.

Прежде всего с каждой функцией f: $A^n \to A$ свяжем множество слов $X_f^* \subseteq A^n$, состоящее из всех граней фигуры $f^{-1}(1)$ в полурешетке $(A^n, \trianglelefteq)$. Например, для $f(\tilde{x}) = (x_1 \vee x_2) \otimes x_3$ при $* = 0$ имеем $X_f^* = \{(1, 0, 1, 0, \ldots, 0),$ $(0, 1, 1, 0, \ldots, 0)\}$, а при $* = 2$ имеем $X_f^* = \{(1, 0, 1, 2, \ldots, 2), (0, 1, 1, 2, \ldots, 2), (1, 1, 1, 2, \ldots, 2)\}$.

Рассмотрим отношение $Q = \{(f, X_f^*) \mid f \in \mathcal{T}_*^{(n)}\}$. Нетрудно убедиться, что тогда алгебра фигур $\langle \mathcal{P}(A^n); \odot, \cup \rangle$ является Q-образом алгебры функций $\langle \mathcal{T}_*^{(n)}; \otimes, \vee \rangle$. Кроме того, для любой функции $f \in HF_*$ имеем, что либо $X_f^* = \varnothing$ (если $f^{-1}(1) = \varnothing$), либо $X_f^* = \{(*, \ldots, *)\}$ (если $f \equiv 1$), либо X_f^* состоит из одного или двух слов веса 1. Поэтому из леммы 3 вытекает следующее вспомогательное

Предложение 3. *Если* $f \in \mathcal{T}_*^{(n)}$, *то*

$$L^*(f) \geqslant L_{\{\odot, \cup\}}(X_f^*) - 2n.$$

Пример 2. Для иллюстрации рассмотрим следующий трехзначный аналог определяемой в примере 1 булевой функции. Пусть $a \in A$, $a \neq *$. Определим функцию $f_{n,d}^*$: $A^n \to \{0, 1\}$ от $n = m^2$ переменных $x_{i,j}$ $(1 \leqslant i, j \leqslant m)$ следующим образом:

$$f_{n,d}^* = \bigvee_{p \in \Pi} \bigotimes_{i \in GF(m)} J_a(x_{i, p(i)}),$$

где Π — множество всех полиномов степени не выше $d-1$ над полем $GF(m)$. Ясно, что $f_{n,d}^*$ входит в $\mathcal{T}_*^{(n)}$, причем

$$L^*(f_{n,d}^*) \leqslant m^{d+1}.$$

С другой стороны, согласно предложению 3 имеем

$$L^*(f_{n,d}^*) \geqslant L_{\{\odot, \cup\}}(X) - 2n,$$

где $X = X^*_{f_{n,d}}$. Поскольку $\lambda_i(X) = m^{d-i}$, то фигура X является (r, s)-редкой для любого $r \leqslant [m/3]$. Кроме того, поскольку $X \subseteq \{*, a\}^n$, то в теореме 4 в качестве ε можно брать любое число $\varepsilon \in [0, 1)$. Поэтому, полагая $r = [s \ln m]$, $s = d-2$ и $\varepsilon = m^{-2s/m}$, находим, что $\Phi(X, r, s) \gtrsim m^{s/2}(s \ln m)^{-s/2}$ и $\psi(X, r, s, \varepsilon) \gtrsim m^{Cs(1-s/m)}$, $C > 0$. Из теоремы 4 вытекает

Следствие 2. *Если* $d \leqslant (m/\ln m)^{1/2}$, *то*

$$m^{Cd} \leqslant L^*(f^*_{n,d}) \leqslant m^{d+1}, \qquad C > 0.$$

В частности, при $d = [\sqrt{m}/\ln m]$ получаем точный порядок логарифма

$$\log_2 L^*(f^*_{n,d}) \asymp n^{1/4}.$$

Замечание. Первая экспоненциальная нижняя оценка для схем в трехзначных базисах была получена ранее Г. А. Ткачевым в [18], где рассматриваются СФЭ в базисе $\{\otimes, \wedge\}$, $x \wedge y = \min(x, y)$. В наших терминах—это схемы в базисе $\{\otimes, \wedge\}$ со входом HI, где I состоит из единственной функции $\mathrm{id}(x) = x$. В [18] рассматривается функция $g_n\colon A^n \to \{0, 1\}$ такая, что

$$g_n(\tilde{x}) = 1 \Leftrightarrow \tilde{x} \in \{1, 2\}^n \quad \text{и} \quad |\{i\colon x_i = 1\}| \geqslant n/2,$$

и для нее доказывается справедливость оценки

$$L_{\{\otimes, \wedge\}}(g_n, HI) \gtrsim 2^n n^{-1/2}.$$

Для сравнения отметим, что эта функция просто реализуется уже в классе HF_*-схем в базисе $\{\otimes, \vee\}$ при $* = 0$; точнее,

$$L^0(g_n) = O(n^{5,3}).$$

Это вытекает из представления

$$g_n(\tilde{x}) = \bigotimes_{i=1}^{n} (J_1(x_i) \vee J_2(x_i)) \otimes MAJ_n(J_1(x_1), \ldots, J_1(x_n)),$$

где MAJ_n—монотонная булевая функция «большинства», сложность которой в классе булевых формул в базисе $\{\&, \vee\}$ не превосходит $O(n^{5,3})$ [19]. Более того, известно, что при $* = 0$ HF_*-схемы в базисе $\{\otimes, \vee\}$ не слабее HI-схем в базисе $\{\otimes, \wedge\}$ для всех функций $f_n\colon A^n \to \{0, 1\}$. А именно, в работе [8] доказано, что для любой такой функции f_n имеет место соотношение

$$L^0(f_n) \leqslant (2n+6) L_{\{\otimes, \wedge\}}(f_n, HI).$$

§ 8. Приложение: комбинаторные свойства r-фильтров

Докажем одно свойство r-фильтров, из которого прямо вытекает лемма 4. Пусть $(M, \trianglelefteq)$—нижняя полурешетка с нулем $0 \in M$, с функцией высоты h и мажорантой $\mu(r, k)$. Для фигуры $X \subseteq M$ через $\dim(X)$ и $\mathrm{Dim}(X)$ обозначаем соответственно наименьшую и наибольшую высоту ее точек. Для $x \trianglelefteq y$ записываем $x \triangleleft y$, если $x \neq y$.

Определение. Фигуру $X \subseteq M$ называем *r-простой* $(r \geqslant 1)$, если $\dim(X) = \mathrm{Dim}(X)$ и не существуют $x \in X$ и $Y \subseteq X$ такие, что $|Y| = r+1$ и $x \trianglerighteq \theta(Y)$.

Предложение 4. *Пусть* $X \subseteq M$, $k \geqslant 0$ *и* F, G —*множества всех граней высоты* k *фигур* $X^{(r)}$ *и* $X^{(r)}—X^{\nabla}$ *соответственно. Тогда обе фигуры* F *и* G *являются r-простыми.*

Доказательство. Простота фигуры F следует прямо из определения r-фильтра $X^{(r)}$. Убедимся в r-простоте фигуры G.

Предположим, что G не является r-простой. Поскольку $\dim(G) = \mathrm{Dim}(G) = k$, то тогда существуют точка $x \in G$ и фигура $Y \subseteq G$ такие, что $|Y|=r+1$ и $x \triangleright \theta(Y)$. Но тогда $\theta(Y) \in X^{(r)}$, поскольку $Y \subseteq G \subseteq X^{(r)}$. С другой стороны, сцепление $\theta(Y)$ не принадлежит X^{∇}, так как в противном случае имели бы $x \triangleright \theta(Y) \trianglerighteq X$, что противоречит тому, что $x \notin X^{\nabla}$. Стало быть, получаем, что $x \triangleright \theta(Y)$ и $\theta(Y) \in X^{(r)}-X^{\nabla}$, а это противоречит тому, что x есть грань фигуры $X^{(r)}-X^{\nabla}$. Предложение доказано.

В силу предложения 4 лемма 4 вытекает из следующей леммы.

Лемма 5. *Пусть M — дистрибутивная нижняя полурешетка со слабыми дополнениями. Тогда для любой r-простой фигуры $X \subseteq M$ имеет место*

$$|X| \leqslant \mu(r, \dim(X)).$$

Доказательство поведем индукцией по $r \geqslant 1$. Если фигура X 1-простая, то, очевидно, $|X|=1=\mu(1, \dim(X))$.

Пусть теперь $r \geqslant 2$, $k=\dim(X)$, и утверждение леммы доказано для всех $r' \leqslant r-1$. Зафиксируем произвольную точку $x_0 \in X$ и рассмотрим фигуру

$$Z=\{x \wedge x_0 \mid x \in X-\{x_0\}\}.$$

Так как M — полурешетка со слабыми дополнениями и $h(x)=k$ для всех $x \in X$, то каждая точка $y=x \wedge x_0 \in Z$ имеет хотя бы одно свое дополнение в интервале $[0, x]$. Кроме того, в силу дистрибутивности M это дополнение единственное; обозначим его $\partial_y(x)$. Сказанное выше позволяет связать с каждой точкой $y \in Z$ фигуру

$$X_y=\{\partial_y(x) \mid x \in X, \quad x \wedge x_0=y\}.$$

Поскольку $x_1 \neq x_2$ влечет за собой $\partial_y(x_1) \neq \partial_y(x_2)$, то

$$|X|=\sum_{y \in Z} |X_y|.$$

Кроме того, поскольку $h(\partial_y(x))=h(x)-h(y)$, то

$$\forall y \in Z\colon \ \dim(X_y)=\operatorname{Dim}(X_y)=k-h(y).$$

Поэтому, если справедливо утверждение:

(*) *для всех $y \in Z$ фигура X_y является $(r-1)$-простой*, то согласно индуктивному предположению получаем

$$|X| \leqslant \textstyle\sum_{y \in Z} \mu(r-1, \ k-h(y)) \leqslant \mu(r, \ k),$$

что и требуется доказать. Докажем утверждение (*).

Допустим противное, т. е. что существуют $x' \in X_y$ и $Y' \subseteq X_y$ такие, что $|Y'|=r$ и $x' \triangleright \theta(Y')$. Рассмотрим фигуру

$$Y=\{x_0\} \cup \{y' \vee y \mid y' \in Y'\}.$$

Ясно, что $Y \subseteq X$, причем $|Y|=r+1$, поскольку $y_1' \neq y_2' \in Y$ влечет за собой $y_1' \vee y \neq y_2' \vee y$. Кроме того, используя дистрибутивность полурешетки M, получаем, что $\theta(Y)=y \vee \theta(Y')$.

Возьмем теперь точку $x \in X$, для которой $\partial_y(x)=x'$. Поскольку $x' \triangleright \theta(Y')$ и $a \trianglelefteq b \Rightarrow a \vee c \trianglelefteq b \vee c$ в любой дистрибутивной полурешетке (см., например, [13, с. 65]), то возможны лишь два случая:

$$y \vee x'=\theta(Y) \quad \text{или} \quad y \vee x' \triangleright \theta(Y).$$

Поскольку $y \vee x'=x \in X$, то второй случай невозможен в силу r-простоты фигуры X. В первом же случае имеем $y \vee \theta(Y')=x$. Однако в силу того, что $y \wedge \partial_y(x)=0$ для всех $x \in X$, имеем $y \wedge \theta(Y')=0$. Стало быть, в этом случае сцепление $\theta(Y')$ является дополнением точки y в интервале $[0, x]$, т. е. $\theta(Y')=\partial_y(x)=x'$. Полученное противоречие с тем, что $x' \triangleright \theta(Y')$ завершает доказательство утверждения (*) и тем самым леммы 5. Лемма доказана.

СПИСОК ЛИТЕРАТУРЫ

1. Храпченко В. М. Об одном методе получения нижних оценок сложности П-схем // Мат. заметки.— 1971.— Т. 10, № 1.— С. 83—92.
2. Андреев А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // ДАН СССР.— 1985.— Т. 282, №5.— С. 1033—1037.
3. Андреев А. Е. Об одном методе получения эффективных нижних оценок монотонной сложности // Алгебра и логика.— 1987.— Т. 26, № 1.— С. 3—21.
4. Разборов А. А. Нижние оценки монотонной сложности некоторых булевых функций // ДАН СССР.— 1985.— Т. 281, № 4. С. 798—801.
5. Разборов А. А. Нижние оценки монотонной сложности логического перманента // Мат. заметки.— 1985.— Т. 37, № 6.— С. 887—900.
6. Разборов А. А. Нижние оценки размера схем ограниченной глубины в базисе, содержащем функцию логического сложения // Мат. заметки.— 1987.— Т. 41, №4.— С. 598—607.
7. Alon N., Boppana R. B. The monotone circuit complexity of Boolean functions // Combinatorica.— 1987.— V. 7, № 1.— P. 1—22.
6. Юкна С. П. Метод функциональных приближений для получения нижних оценок сложности схем.— Препринт № 6/ИМК АН ЛитССР.— Вильнюс, 1988.
9. Tardos E. The gap between monotone and non-monotone circuit complexity is exponential // Combinatorica.— 1987.— V. 7, № 4.— P. 141—142.
10. Угольников А. Б. О сложности реализации булевых функций схемами в базисе из медианы и импликации // Вестн. МГУ, Сер. 1, Математика, механика.— 1987.— № 4. — С. 76—78.
11. Лупанов О. Б. Асимптотические оценки сложности управляющих систем.— М.: Изд-во МГУ, 1984.
12. Нигматуллин Р. Г. Сложность булевых функций.— Казань: Изд-во КГУ, 1983.
13. Айгнер М. Комбинаторная теория.— М.: Мир, 1982.
14. Гретцер Г. Общая теория решеток.— М.: Мир, 1982.
15. Окольнишникова Е. А. О влиянии одного типа ограничений на сложность схем из функциональных элементов // Дискретный анализ. Вып. 36.— Новосибирск, 1981.— С. 46—58.
16. Jukna S. P. Entropy of contact circuits and lower bounds of their complexity // Theoretical Comput. Sci.— 1988.— V. 57, № 1.— P. 113—129.
17. Юкна С. П. Об одном энтропийном методе получения нижних оценок сложности булевых функций // ДАН СССР.— 1988.— Т. 298, № 3.— С. 556—559.
18. Ткачев Г. А. О сложности реализации одной последовательности функций k-значной логики // Вестн. МГУ. Сер. 15, Вычисл. математика и кибернетика.—1977.— № 1.— С. 45—57.
19. Valiant L. G. Short montone formulae for the majority function // Journal of Algorithms.— 1984.— V. 5.— P. 363—366.

Статья поступила 21.02.89