**Московский государственный университет
имени М. В. Ломоносова**

Факультет вычислительной математики и кибернетики

С. А. Ложкин

Лекции по основам кибернетики

Вариант 2016 г. (гр. 418), глава 6

Москва 2016

Оглавление

Введение

Курс «Основы кибернетики» (ранее «Элементы кибернетики»), создателем и основным лектором которого был чл.-корр. РАН С. В. Яблонский, читается на факультете ВМиК МГУ с первых лет его существования. В настоящее время он читается в 6–8 семестрах и является обязательным для всех бакалавров (интегрированных магистров) направления 01400 — «Прикладная математика и информатика». При этом объем и, в некоторой степени, программа курса «Основы кибернетики» варьируются в зависимости от профиля. Данный вариант курса ориентирован на студентов, кафедры математической кибернетики (318, 418 группы), которые изучают его в 6 и 7 семестрах.

Курс «Основы кибернетики» посвящен изложению теории дискретных управляющих систем, которая представляет собой часть дискретной математики и математической кибернетики. В ней разрабатываются и изучаются дискретные математические модели, описывающие функционирование и структуру сложных систем преобразования информации (интегральных схем, программ и т. п.). В основе этих моделей лежат различные способы задания функционирования управляющих систем с помощью дискретных функций и их структурная реализация в тех или иных классах графов (классах схем). При исследовании управляющих систем ставятся и решаются две основные задачи: задача анализа и задача синтеза.

Задача анализа состоит в нахождении функционирования данной схемы, а задача синтеза — в построении схемы,

имеющей (реализующей) заданное функционирование. Каждая из этих задач может рассматриваться либо как индивидуальная задача, и тогда ее решением является конкретное функционирование (схема), либо как массовая задача, и тогда ее решением должен быть алгоритм нахождения функционирования (схемы). Задача синтеза имеет, как правило, множество решений, из которых выбирают решение, оптимальное по какому-либо критерию. Чаще всего в качестве такого критерия выступает сложность схемы, понимаемая как сумма сложностей составляющих ее элементов или задержка схемы, понимаемая как максимальная сумма задержек для последовательно соединенных элементов схемы.

С содержательной точки зрения различные критерии оптимальности отражают различные параметры моделируемых электронных схем или программ. Так, например, сложность может характеризовать стоимость, размеры или потребляемую мощность СБИС, а также время выполнения программы на одном процессоре. При этом задержка схемы характеризует время срабатывания СБИС или время выполнения программы на параллельных процессорах и т. п.

Если задача синтеза решена в одной модели, можно пытаться перенести это решение в другие модели с помощью структурного моделирования. Кроме того, полученное решение можно «улучшить» с помощью эквивалентных преобразований. С другой стороны, если задача синтеза решена для одних функций, можно пытаться «разбить» (декомпозировать) новую функцию на уже рассмотренные и построить из синтезированных для них схем схему для новой функции с помощью операции суперпозиции.

Указанные выше задачи рассматриваются в лекциях для всех основных классов схем (дизъюнктивные нормальные формы, формулы и схемы из функциональных элементов, контактные схемы), а также для некоторых модификаций

этих классов.

Первая глава посвящена различным вопросам представления функций алгебры логики с помощью таблиц и дизъюнктивных нормальных форм (минимизация дизъюнктивных нормальных форм).

Вторая глава содержит описание структуры и функционирования схем из основных классов управляющих систем, а также из некоторых классов, представляющих собой их обобщения или модификации. В ней устанавливаются верхние оценки числа схем различных типов, рассматриваются особенности применения операции суперпозиции в различных классах схем и некоторые вопросы их структурного моделирования.

В третьей главе подробно рассматривается задача синтеза управляющих систем. В ней приводится целый спектр методов синтеза схем (от простейших до асимптотически оптимальных), устанавливаются нижние мощностные оценки функций Шеннона и оценки сложности ряда конкретных функций, доказывается минимальность некоторых схем.

В четвертой главе изучаются эквивалентные преобразования схем на основе тождеств во всех основных классах управляющих систем. Для каждого из них приводится система «основных» тождеств, доказывается полнота этой системы и изучаются вопросы ее избыточности.

В пятой главе представлены некоторые вопросы надежности и контроля схем: построение тестов для таблиц; синтез самокорректирующихся контактных схем и схем из функциональных элементов (СФЭ) в некоторых базисах; синтез надёжных СФЭ из ненадёжных функциональных элементов.

В шестой главе излагаются основные вопросы, связанные с задачей синтеза схем для функций из специальных классов.

Заметим, что 2 и 3 главы программы 318 группы 2016 г. соответствуют, в основном, 2 главе программы 320–328 групп

за 2016 г., а 4 глава программы 418 группы — 3 главе программы 320–328 групп.

Глава 6

Синтез схем для функций алгебры логики из специальных классов

§1 Инвариантные классы С. В. Яблонского, их структурные и метрические свойства, теорема о числе инвариантных классов

Для множества ФАЛ Q, $Q \subseteq P_2$, и натурального n через $Q(n)$ будем обозначать множество $Q \cap P_2(n)$. При этом, как само множество Q, так и связанную с ним последовательность $Q(1), Q(2), \ldots$ будем называть *классом ФАЛ*. Для класса ФАЛ Q и $n = 1, 2, \ldots$ введём последовательность

$$\sigma_Q(n) = \frac{\log |Q(n)|}{2^n},$$

для которой, очевидно, $0 \leqslant \sigma_Q(n) \leqslant 1$.

Рассмотрим теперь следующие операции над ФАЛ:

1) добавление и изъятие фиктивных БП (переход к равной ФАЛ);

2) переименование БП без отождествления (переход к конгруэнтной ФАЛ);

3) подстановка констант 0, 1 вместо БП (переход к подфункции).

Если функция g получена из функции f применением операций 1–3, то говорят, что g является *квазиподфункцией*

ФАЛ f, а f — *квазинадфункцией* ФАЛ g. Для множества функций F через $F^{\urcorner}$ и $F_{\lrcorner}$ будем обозначать множества всех квазинадфункций и квазиподфункций для функций из F соответственно.

Множество ФАЛ Q, $Q \subseteq P_2$, называется *инвариантным классом ФАЛ*, если оно замкнуто относительно трёх указанных операций. Множества $\{0\}$, $\{1\}$, $\{0,1\}$ называются *тривиальными инвариантными классами*. Если инвариантный класс Q не является тривиальным, то $Q \supseteq \{0,1\}$, поскольку Q содержит неконстантую функцию, из которой при помощи операции 3 можно получить обе константы. Отметим, что если класс Q замкнут по суперпозиции и $\{0,1\} \subseteq Q$, то класс Q является инвариантным. Примерами инвариантных классов могут, следовательно, служить классы M и $\widehat{L}$ всех монотонных и всех линейных ФАЛ соответственно. При этом класс самодвойственных функций, а также классы T_0 и T_1 — классы сохранения констант 0 и 1 соответственно, — не являются инвариантными (они не замкнуты относительно операции 3). Класс всех симметрических ФАЛ также не является инвариантным, так как он не замкнут относительно операции 1. При этом инвариантным является класс $\widehat{S}$ — класс *квазисимметрических* ФАЛ, то есть функций, симметрических по всем своим существенным переменным.

Лемма 1.1. *Пусть Q — инвариантный класс ФАЛ. Тогда существует предел*

$$\sigma_Q = \lim_{n\to\infty} \sigma_Q(n) = \lim_{n\to\infty} \frac{\log |Q(n)|}{2^n},$$

где число σ_Q удовлетворяет неравенствам $0 \leqslant \sigma_Q \leqslant 1$.

Доказательство. Из определения последовтельности $\sigma_Q(n)$ следует, что для каждого n выполнено $0 \leqslant \sigma_Q(n) \leqslant 1$, то есть последовательность $\sigma_Q(n)$ ограничена. Покажем, что

она монотонно не возрастает, откуда будет следовать её сходимость. В силу инвариантности класса Q, всякую функцию f из множества $Q(n+1)$ можно представить в виде

$$f(x_1,\dots,x_{n+1}) = \overline{x}_{n+1}f_0(x_1,\dots,x_n) \vee x_{n+1}f_1(x_1,\dots,x_n),$$

где $f_\sigma(x_1,\dots,x_n) = f(x_1,\dots,x_n,\sigma)$, $\sigma \in B$, и обе ФАЛ f_0, f_1 принадлежат множеству $Q(n)$. Отсюда сразу вытекает неравенство

$$|Q(n+1)| \leqslant |Q(n)|^2,$$

из которого, в свою очередь, следует, что

$$\sigma_Q(n+1) = \frac{\log|Q(n+1)|}{2^{n+1}} \leqslant \frac{\log|Q(n)|}{2^n} = \sigma_Q(n).$$

Сходимость последовательности $\sigma_Q(n)$, $n = 1,2,\dots$, доказана, а принадлежность её предела σ_Q действительному отрезку $[0,1]$ следует из того, что ему принадлежат все члены данной последовательности.

Лемма доказана. □

Замечание. Предел σ_Q будем называть *мощностной* характеристикой класса Q.

Инвариантный класс Q с характеристикой $\sigma_Q = 0$ называется *нулевым*. Покажем, что существует только один инвариантный класс Q с характеристикой $\sigma_Q = 1$ — это класс P_2. Действительно, если инвариантный класс Q не совпадает с P_2, то для некоторого m будет выполнено неравенство $|Q(m)| < |P_2(m)|$, которое равносильно неравенству $\sigma_Q(m) < 1$. Из последнего неравенства в силу монотонного невозрастания последовательности $\sigma_Q(n)$, $n = 1,2,\dots$, и её сходимости к пределу σ_Q следует, что $\sigma_Q \leqslant \sigma_Q(m) < 1$.

Найдём значение характеристик инвариантных классов M, $\widehat{L}$ и $\widehat{S}$. Известно [36], что

$$\log|M(n)| \sim C_n^{\lceil n/2\rceil} \sim \frac{2^n}{\sqrt{2\pi n}},$$

откуда следует, что $\sigma_M = 0$. Для класса линейных функций, очевидно, при любом n выполняется равенство $|\widehat{L}(n)| = 2^{n+1}$ и, значит, $\sigma_L = 0$. Всякую функцию из множества $\widehat{S}(n)$ можно получить так: сначала выбираем k её существенных БП, а затем не более чем 2^{k+1} способами определяем значение этой функции на каждом слое куба B^k (в пределах одного слоя значение функции одно и то же). Отсюда следует, что

$$|\widehat{S}(n)| \leqslant \sum_{k=0}^{n} C_n^k \cdot 2^{k+1} = 2 \cdot 3^n,$$

и поэтому $\sigma_{\widehat{S}} = 0$. Таким образом, все три класса M, $\widehat{L}$, $\widehat{S}$ являются нулевыми.

Примером ненулевого инвариантного класса, отличного от P_2, является класс Q, состоящий из всех ФАЛ вида $f(x_{i_1}, \ldots, x_{i_r})(x_{i_1} \oplus \cdots \oplus x_{i_r} \oplus \sigma)$, где $1 \leqslant i_1 < \cdots < i_r$ и $\sigma \in B$. Действительно, класс Q замкнут относительно операций 1–3. При этом любая ФАЛ из $Q(n)$ однозначно определяется множеством X её существенных БП, $X \subseteq X(n)$, и своими значениями на множестве тех наборов единичного куба от БП X, которые имеют либо чётное, если $\sigma = 1$, либо нечётное, если $\sigma = 0$, число единиц. Таким образом,

$$2 \cdot 2^{2^{n-1}} \leqslant |Q(n)| \leqslant \sum_{r=0}^{n} 2 \cdot C_n^r \cdot 2^{2^{r-1}} \leqslant 2^{2^{n-1}+n+1}$$

и, следовательно, $\sigma_Q = \frac{1}{2}$.

Выше было установлено, что существует единственный инвариантный класс с характеристикой 1. Можно доказать, что при при любом σ, $0 \leqslant \sigma < 1$ существует континуум инвариантных классов с характеристикой σ. Докажем это в частном случае $\sigma = 0$.

Лемма 1.2. *Существует континуум различных инвариантных классов с характеристикой* 0.

Доказательство. Отметим, что число различных инвариантных классов не может быть больше континуума, поскольку множество P_2 счётно.

Рассмотрим симметрические функции $s_m^{\{0,m\}}$, определяемые при $m > 1$ следующим образом:

$$s_m^{\{0,m\}}(x_1, \ldots, x_m) = x_1 \cdot \ldots \cdot x_m \vee \overline{x}_1 \cdot \ldots \cdot \overline{x}_m.$$

Заметим, что $s^{\{0,m'\}} \notin \{s^{\{0,m''\}}\}_{\lrcorner}$ при $m' \neq m''$, и, следовательно, для различных множеств J, $J \subseteq \mathbb{N}\backslash\{1\}$, соответствующие им множества функций $Q_J = \{ s_m^{\{0,m\}} \mid m \in J \}_{\lrcorner}$ будут различны. Очевидно, что каждое из указанных множеств является инвариантным классом, содержащимся в классе $\widehat{S}$, и, следовательно, имеет характеристику 0. Классов Q_J будет столько же, сколько подмножеств имеет множество $\mathbb{N} \setminus \{1\}$, то есть континуум.

Лемма доказана. □

Множество F называется *базовым множеством* инвариантного класса Q, если $F_{\lrcorner} = Q$. Базовое множество класса Q называется *базой*, если любое его собственное подмножество уже не является базовым множеством для Q. Существуют инвариантные классы, не имеющие базы. Например, класс, состоящий из констант 0, 1 и всех монотонных элементарных дизъюнкций (функций вида $x_{i_1} \vee \cdots \vee x_{i_s}$), имеет счётное базовое множество, но не имеет базы.

Для задания всякого инвариантного класса достаточно задать, таким образом, его базовое множество. Существует и другой способ задания инвариантных классов. Пусть Q — нетривиальный отличный от P_2 инвариантный класс. Функция $g \in P_2$ называется *порождающим элементом* класса Q тогда и только тогда, когда $g \notin Q$, а все собственные подфункции[1] g принадлежат Q. Из определения сле-

[1]Под собственной подфункцией функции g понимается её произвольная подфункция, не совпадающая с g.

дует, что порождающий элемент нетривиального инвариантного класса является существенной функцией и что никакие два различных порождающих элемента не являются квазиподфункциями друг друга. Приведём примеры порождающих элементов. Класс M монотонных ФАЛ имеет единственный с точностью до конгруэнтности порождающий элемент — функцию $\overline{x}_1$. Для инвариантного класса Q его *порождающим множеством* называется всякое максимальное по включению множество попарно не конгруэнтных порождающих элементов Q. Так, порождающее множество класса, состоящего из констант и монотонных элементарных дизъюнкций, суть $\{\overline{x}_1, x_1x_2\}$.

Лемма 1.3. *Пусть Q — нетривиальный отличный от P_2 инвариантный класс, а G — его порождающее множество. Тогда $Q = P_2 \setminus (G^{\urcorner})$.*

Доказательство. Индукцией по n, $n = 1, 2, \ldots$, докажем, что если f — существенная ФАЛ от n БП и $f \notin Q$, то $G \cap (\{f\}_{\lrcorner}) \neq \varnothing$. Заметим, что данное утверждение верно, если любая собственная подФАЛ ФАЛ f прининадлежит Q. Действительно, в указанном случае ФАЛ f является порождающим элементом Q и в G имеется конгруэнтная ей ФАЛ. Это верно, в частности, для случая $n = 1$, который составляет базис рассматриваемой индукции.

Пусть сформулированное утверждение верно для всех n, $n \in [1, k)$, где $k \geqslant 2$, и пусть f — существенная ФАЛ из $P_2(k) \setminus Q(k)$, которая (см. разобранный выше случай) имеет собственную подФАЛ f', $f' \notin Q$. Тогда, по индуктивному предположению $G \cap (\{f'\}_{\lrcorner}) \neq \varnothing$ и, следовательно, $G \cap (\{f\}_{\lrcorner}) \neq \varnothing$, так как первое из этих множеств содержится во втором.

Лемма доказана. □

Следствие. *Пусть множество G состоит из ФАЛ, не являющихся квазиподфункциями друг друга. Тогда $P_2 \setminus (G^{\urcorner})$ —*

инвариантный класс с порождающим множеством G.

§2 Задача синтеза схем для ФАЛ из специальных классов, связанные с ней понятия и мощностные нижние оценки. Примеры решения этой задачи на основе модификации асимптотически наилучших методов синтеза

Аналогично классу ФАЛ последовательность

$$Q(1), \ldots, Q(n), \ldots,$$

где $Q(n) \subseteq P_2^m(n)$ и $m = m_Q(n)$ называется *классом операторов*. Будем предполагать, что ни одно из множеств $Q(n)$, $n = 1, 2, \ldots$, рассматриваемого класса ФАЛ или операторов Q не является пустым и, как правило, $|Q(n)| \geqslant 3$.

Пусть заданы класс ФАЛ или операторов Q, класс схем $\mathcal{U}$ и функционал сложности $\mathcal{L}$. Тогда *функцией Шеннона для класса ФАЛ или операторов Q при их реализации в классе схем $\mathcal{U}$ относительно функционала сложности $\mathcal{L}$* называется функция натурального аргумента

$$\mathcal{L}(Q(n)) = \max_{f \in Q(n)} \mathcal{L}(f),$$

где $\mathcal{L}(f)$ — минимальная $\mathcal{L}$–сложность схем из $\mathcal{U}$, реализующих (систему) ФАЛ f. Для класса ФАЛ или операторов Q введём функцию

$$\mathcal{J}\big(Q(n)\big) = \frac{\log |Q(n)|}{\log\log |Q(n)|},$$

где $n = 1, 2, \ldots$.

Класс ФАЛ (операторов) Q называется:

1) *невырожденным*, если $n + m_Q(n) = o\big(\mathcal{J}\big(Q(n)\big)\big)$;

2) *строго невырожденным* классом ФАЛ, если $\log n = o\big(\log|Q(n)|\big)$;

3) *ненулевым классом ФАЛ*, если $\underline{\lim}_{n\to\infty}\sigma_Q(n) > 0$.

На основе стандартного мощностного метода получения нижних оценок можно установить справедливость следующего утверждения.

Лемма 2.1. *Если Q — невырожденный класс ФАЛ (операторов), то*

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \gtrsim \rho_{\text{Б}}\cdot\mathcal{J}\big(Q(n)\big), \qquad L^{\text{ИКС}}\big(Q(n)\big) \gtrsim \frac{1}{2}\cdot\mathcal{J}\big(Q(n)\big),$$

а если Q — строго невырожденный класс ФАЛ, то

$$L^{\text{K}}\big(Q(n)\big) \gtrsim \mathcal{J}\big(Q(n)\big).$$

Следствие. *Для всякого ненулевого класса ФАЛ Q выполнены асимптотические неравенства*

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \gtrsim \rho_{\text{Б}}\cdot\sigma_Q(n)\frac{2^n}{n},$$
$$L^{\text{ИКС}}\big(Q(n)\big) \gtrsim \frac{1}{2}\cdot\sigma_Q(n)\frac{2^n}{n},$$
$$L^{\text{K}}\big(Q(n)\big) \gtrsim \sigma_Q(n)\frac{2^n}{n}.$$

Класс ФАЛ (операторов) Q называется *стандартным относительно функционала сложности $\mathcal{L}$ класса схем $\mathfrak{U}_{\text{Б}}^{\text{C}}$*, если выполнено асимптотическое неравенство

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \lesssim \rho_{\text{Б}}\cdot\mathcal{J}\big(Q(n)\big) + O\big(n+m(n)\big).$$

Аналогично вводится определения стандартного класса операторов относительно других классов схем и функционалов их сложности, если соответствующая функция Шеннона имеет порядок роста $2^n/n$. Отметим, что при этом для

невырожденного стандартного класса ФАЛ Q имеет место асимптотическое равенство

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \sim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big).$$

Для $n = 1, 2, \ldots$ и $r = r(n) \geqslant 1$ рассмотрим множество ФАЛ $P_2(n, t)$, которое включает в себя все ФАЛ из $P_2(n)$, обращающиеся в 0 на наборах с номерами $t, t+1, \ldots, 2^n - 1$, и мощность которого равна, очевидно, 2^t. Для любой функции $r = r(n) \geqslant 1$ рассмотрим класс ФАЛ Q, определённый равенствами $Q(n) = P_2(n, r(n))$, $n = 1, 2, \ldots$.

Лемма 2.2. *Для любой функции $r = r(n) \geqslant 1$ соответствующий класс $Q(n) = P_2(n, r(n))$ является стандартным относительно функционала сложности $\mathcal{L}$ схем класса $\mathcal{U}_{\text{Б}}^{\text{C}}$, то есть*

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \lesssim \rho_{\text{Б}} \frac{r}{\log r} + O(n).$$

Доказательство. Будем считать, для удобства, что при лексикографической ν–нумерации наборов куба B^n от БП $X(n)$, $n = 1, 2, \ldots$, БП x_i «старше» БП x_j, если $i > j$. Полученные при этом предположении оценки сложности будут справедливы, очевидно, и для «обычного» порядка «старшинства» БП.

Рассмотрим сначала случай, когда $r > 2^{n-1}$. Выберем из множества $P_2(n, r)$ произвольную ФАЛ f и построим для неё СФЭ Σ_f с помощью асимптотически наилучшего метода синтеза (см. [13, гл. 4, §8]). Напомним, что при этом ФАЛ f (см. доказательство теоремы 8.1) разлагается по БП $x'' = (x_{q+1}, \ldots, x_n)$ следующим образом:

$$f(x',\, x'') = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') f_{\sigma''}(x'),$$

где $x' = (x_1, \ldots, x_q)$, и что для реализации каждой ФАЛ $f_{\sigma''}(x')$ в СФЭ Σ_f используется одна формула $\mathcal{F}_t$. Из принадлежности ФАЛ f классу $P_2(n, r)$ следует, что при $\nu(\sigma'') > \lceil r/2^q \rceil$ функция $f_{\sigma''}(x')$ тождественно равна нулю, и, таким образом, из схемы Σ_f можно удалить подсхемы, реализующие все указанные подфункции. Для сложности полученной при этом СФЭ $\widetilde{\Sigma}_f$ будет выполняться неравенство

$$\mathcal{L}\big(\widetilde{\Sigma}_f\big) \leqslant \mathcal{L}_j \left\lceil \frac{r}{2^q} \right\rceil t + O\big(2^{n-m} + p \cdot 2^s + p \cdot 2^{\frac{s}{2}+m}\big),$$

из которого при значениях параметров

$$m = q = \lceil 2 \log n \rceil, \quad s = 2 \left\lceil \frac{n - 3 \log n}{2} \right\rceil$$

следует, что

$$\mathcal{L}\big(\widetilde{\Sigma}_f\big) \lesssim \rho_{\text{Б}} \frac{r}{\log r}. \tag{2.1}$$

Пусть теперь $r \leqslant 2^{n-1}$. В этом случае найдём число k такое, что

$$k < n, \qquad 2^{k-1} < r \leqslant 2^k$$

и, следовательно,

$$f(x_1, \ldots, x_n) = \overline{x}_{k+1} \cdot \ldots \cdot \overline{x}_n \cdot f'(x_1, \ldots, x_k). \tag{2.2}$$

Заметим, что функция f' принадлежит классу $P_2(k, r)$, где $r > 2^{k-1}$, и для неё по предыдущему случаю можно построить СФЭ $\widetilde{\Sigma}_{f'}$, удовлетворяющую (2.1). Искомая СФЭ $\widetilde{\Sigma}_f$ строится на основе (2.2) так, что

$$\mathcal{L}\big(\widetilde{\Sigma}_f\big) \leqslant \mathcal{L}\big(\widetilde{\Sigma}_{f'}\big) + O(n) \lesssim \rho_{\text{Б}} \frac{r}{\log r} + O(n).$$

Лемма доказана. □

Следствие. *Если* $n = o\big(\frac{r}{\log r}\big)$, *то* $Q(n) = P_2(n, r(n))$ — *стандартный невырожденный класс ФАЛ, для которого выполнено асимптотическое равенство*

$$\mathcal{L}^{\mathrm{C}}_{\mathrm{Б}}\big(Q(n)\big) \sim \rho_{\mathrm{Б}} \frac{r}{\log r}.$$

Замечание. Аналогично доказывается стандартность класса $Q(n) = P_2(n, r(n))$ относительно функционала «обычной» сложности и классов схем $\mathcal{U}^{\mathrm{ИКС}}, \mathcal{U}^{\mathrm{К}}$.

§3 Принцип локального кодирования О. Б. Лупанова и примеры его применения

Рассмотрим достаточно общий подход к решению задачи синтеза СФЭ для ФАЛ из специальных классов, предложенный в работе [17] О. Б. Лупанова и названный им принципом локального кодирования.

Основаная идея этого подхода состоит в том, чтобы с помощью определённого «кодирования» свести задачу синтеза СФЭ для ФАЛ или операторов из заданного класса Q к аналогичной задаче синтеза для класса произвольных или близких к ним операторов соответствующей размерности. В [17] был предложен ряд условий, налагаемых как на класс Q, так и на его кодирование, при выполнении которых получаемые указанным способом схемы могли оказаться асимптотически наилучшими как для самых «плохих» ФАЛ (систем ФАЛ) из $Q(n)$, так и для почти всех ФАЛ (систем ФАЛ) из $Q(n)$, $n = 1, 2, \ldots$. Следующее утверждение и его доказательство дают пример решения задачи синтеза СФЭ для ФАЛ из инвариантного класса Q с помощью принципа локального кодирования.

Лемма 3.1. *Для всякого инвариантного класса* Q *и* $n =$

$1, 2, \ldots$

$$L^{\mathrm{C}}\big(Q(n)\big) \sim \sigma_Q \frac{2^n}{n} \qquad \textit{при } \sigma_Q > 0, \tag{3.1}$$

$$L^{\mathrm{C}}\big(Q(n)\big) = o\Big(\sigma_Q \frac{2^n}{n}\Big) \qquad \textit{при } \sigma_Q = 0. \tag{3.2}$$

Доказательство. Рассмотрим сначала случай $\sigma_Q > 0$. В этом случае в соответствии с введёнными в §1, §2 обозначениями и в силу леммы 1.1 получим

$$\mathcal{J}\big(Q(n)\big) = \frac{\log|Q(n)|}{\log\log|Q(n)|} = \frac{\sigma_Q(n)\cdot 2^n}{\log(\sigma_Q(n)\cdot 2^n)} \sim \sigma_Q \frac{2^n}{n},$$

откуда по лемме 2.1 следует нижняя оценка (3.1).

Перейдём к получению верхней оценки (3.1). Для этого возьмём произвольное натуральное n и натуральное q, $q \leqslant n$, а затем обычным образом разобьём набор БП $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$. Выберем из множества $Q(n)$ произвольную ФАЛ f и для каждого набора σ'', $\sigma'' \in B^{n-q}(x'')$, положим как обычно, $f_{\sigma''}(x') = f(x', \sigma'')$, причём в данном случае $f_{\sigma''}(x') \in Q(q)$ в силу инвариантности класса Q.

Положим $\lambda = \lceil \log|Q(q)| \rceil$ и пусть Π' — произвольное инъективное отображение (кодирование) ФАЛ множества $Q(q)$ двоичными наборами куба B^λ от БП $y = (y_1, \ldots, y_\lambda)$, то есть $\Pi'\colon Q(q) \mapsto B^\lambda(y)$, которое существует, так как $2^\lambda \geqslant |Q(q)|$. Заметим, что ФАЛ $f_{\sigma''}(x')$ однозначно определяется своим «кодом» $\pi_{\sigma''} = \Pi'(f_{\sigma''}(x'))$ и поэтому существует ФАЛ $h(x', y)$, $h \in P_2(q+\lambda)$, такая что

$$f(\sigma', \sigma'') = h(\sigma', \pi_{\sigma''})$$

при любых σ' и σ'' из $B^q(x')$ и $B^{n-q}(x'')$ соответственно.

Пусть $\mathcal{O} = (\mathcal{O}_1, \ldots, \mathcal{O}_\lambda) \in P_2^\lambda(n-q)$ — система ФАЛ, которая сопоставляет произвольному набору σ'', $\sigma'' \in B^{n-q}$, набор («код») $\pi_{\sigma''}$ и пусть СФЭ $\Sigma_{\mathcal{O}}$ из $\mathcal{U}^{\mathrm{C}}$, построенная асимптотически наилучшим методом, реализует эту систему ФАЛ

со сложностью

$$L\big(\Sigma_{\mathcal{O}}\big) \leqslant \lambda\frac{2^{n-q}}{n-q} + o\Big(\frac{2^{n-q}}{n-q}\Big).$$

Искомая СФЭ Σ_f реализует ФАЛ f в соответствии с представлением

$$f(x', x'') = h(x', \mathcal{O}(x''))$$

и содержит в качестве подсхемы СФЭ $\Sigma_{\mathcal{O}}(x'', y)$, а также построенную асимптотически наилучшим методом СФЭ Σ_h, которая реализует ФАЛ $h(x', y)$.

Полагая $q = \lceil \log n \rceil$, и учитывая, что

$$\lambda \leqslant \sigma_Q(q)2^q + 1 \lesssim \sigma_Q 2^q,$$

получим верхнюю оценку

$$L\big(\Sigma_f\big) \lesssim \sigma_Q 2^q \frac{2^{n-q}}{n-q} \lesssim \sigma_Q \frac{2^n}{n}.$$

В случае $\sigma_Q > 0$ отсюда, с учётом нижней оценки, вытекает (3.1).

В случае $\sigma_Q = 0$ искомая СФЭ Σ_f строится аналогично, но так как при этом полседовательность $\sigma_Q(q)$ стремится к нулю, то

$$L\big(\Sigma_f\big) = o\Big(\frac{2^n}{n}\Big),$$

что доказывает (3.2).

Лемма доказана. □

Как уже говорилось, при доказательстве верхней оценки леммы 3.1 мы фактически использовали приём, называемый *принципом локального кодирования*, предложенный О. Б. Лупановым, который состоит в следующем. Пусть Q —

класс операторов, и пусть для каждого натурального n определено кодирование $\Pi = \Pi_n$, ставящее в соответствие произвольному оператору $F = F_n$, $F \in Q(n)$, двоичный набор («код») $\pi = \pi(F)$ длины $d = d(n)$, в котором выделены «куски» π_i, $i \in [1, t]$, составленные из подряд идущих разрядов кода π и имеющие длину не больше, чем $\lambda = \lambda(n)$. Пусть указанное кодирование обладает свойством «локальности»: для вычисления значения оператора F на произвольном фиксированном наборе σ достаточно знать лишь один кусок кода $\pi_{i(\sigma)}$, задаваемый своими «координатами» (например, позицией его первого разряда в коде и длиной, или номером куска, если куски кода не пересекаются и имеют одинаковую длину, и т. п.).

Пусть, далее, оператор кодирования $A^{(1)} = A_n^{(1)}$ по набору σ вычисляет координаты куска кода $\pi_{i(\sigma)}$, а оператор декодирования $A^{(2)} = A_n^{(2)}$ по куску $\pi_{i(\sigma)}$ и, возможно, набору σ, вычисляет $F(\sigma)$. Искомая схема $\Sigma = \Sigma_n$, реализующая оператор F и построенная на основе локального кодирования Π, состоит из подсхем $A^{(1)}$, $A^{(2)}$ и «основного» блока $O = O_n$, который по координатам куска $\pi_{i(\sigma)}$ выдаёт сам этот кусок.

Если при этом сложность указанных выше операторов $A_n^{(1)}$, $A_n^{(2)}$ и O_n удовлетворяет соотношениям

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(A_n^{(1)}\big) = o\big(\mathcal{J}\big(Q(n)\big)\big), \qquad \mathcal{L}_{\text{Б}}^{\text{C}}\big(A_n^{(2)}\big) = o\big(\mathcal{J}\big(Q(n)\big)\big), \quad (3.3)$$

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(O_n\big) \lesssim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big), \quad (3.4)$$

то искомая СФЭ Σ_n может быть выбрана так, что

$$\mathcal{L}\big(\Sigma_n\big) \lesssim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big).$$

Отсюда вытекает, что

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \lesssim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big),$$

и, следовательно, в силу леммы 2.1 в случае невырожденности класса Q выполняется асимптотическое равенство

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \sim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big),$$

которое означает стандартность класса Q относительно функционала сложности $\mathcal{L}$ класса схем $\mathcal{U}_{\text{Б}}^{\text{C}}$.

Заметим, что в случае асимптотической неизбыточности кодирования $\Pi = \Pi_n$, когда

$$d(n) \sim \log |Q(n)|,$$

при построении схемы, которая реализует оператор O_n со сложностью, удовлетворяющей (3.4), достаточно, как правило, использовать асимптотически наилучший метод синтеза СФЭ для произвольных систем ФАЛ подходящей размерности или некоторые его модификации (см., например, лемму 2.2).

Заметим также, что соотношение (3.3) означает возможность существенно более простой по сравнению с оператором O_n реализации операторов $A_n^{(1)}$ и $A_n^{(2)}$ в классе $\mathcal{U}_{\text{Б}}^{\text{C}}$.

Покажем, что описанный в доказательстве леммы 3.1 асимптотически наилучший метод синтеза СФЭ над базисом Б является примером применения принципа локального кодирования.

Действительно, в обозначениях данного доказательства, локальное кодирование Π сопоставляет произвольной ФАЛ f, $f \in Q(n)$, код π длины $d = \lambda \cdot 2^{n-q}$, разбитый на 2^{n-q} непересекающихся кусков длины λ и вида $\pi_{\sigma''}$, где $\sigma'' \in B^{n-q}$. При этом оператор кодирования $A^{(1)}$ представляет собой оператор выбора поднабора x'' из набора x, оператор O совпадает с оператором $\mathcal{O}$, а оператор $A^{(2)}$ — с ФАЛ h.

Рассмотрим ещё два класса операторов и с помощью принципа локального кодирования докажем (при некоторых условиях) их стандартность. Обозначим через S класс всех

симметрических ФАЛ, а под (n, m)-оператором будем понимать систему ФАЛ $F = (f_1, \ldots, f_m)$ из $P_2^m(n)$.

Лемма 3.2. *Если натуральная последовательность $m = m(n)$, $n = 1, 2, \ldots$, такова, что*

$$\log n = o(m) \quad и \quad \log m = o(n), \tag{3.5}$$

то класс операторов Q, для которого $Q(n) = S^m(n)$, является невырожденным и стандартным относительно функционала сложности L СФЭ из $\mathfrak{U}^{\mathrm{C}}$ классом операторов.

Доказательство. Для рассматриваемого класса операторов Q при любых натуральных n и m выполняется равенство $|Q(n)| = 2^{m(n+1)}$, из которого следует, что

$$\mathcal{J}\big((Q(n)\big) = \frac{m(n+1)}{\log m + \log(n+1)}. \tag{3.6}$$

Из (3.6), в свою очередь, вытекает, что последовательности

$$\frac{m}{\mathcal{J}\big(Q(n)\big)} = \frac{\log m + \log(n+1)}{n+1} \leqslant \frac{\log m}{n} + o(1),$$
$$\frac{n}{\mathcal{J}\big(Q(n)\big)} \leqslant \frac{\log m + \log(n+1)}{m} \leqslant \frac{\log n}{m} + o(1)$$

в силу (3.5) стремятся к 0 при n стремящемся к бесконечности и, следовательно, $m + n = o(\mathcal{J}(Q(n))$, то есть $Q(n)$ — невырожденный класс операторов. Отсюда по лемме 2.1 с учётом (3.5) получаем нижнюю оценку

$$L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \mathcal{J}\big(Q(n)\big) \sim \frac{m \cdot n}{\log n}. \tag{3.7}$$

Для получения аналогичной вехней оценки рассмотрим кодирование $\Pi = \Pi_n$, которое оператору F, $F \in Q(n)$, сопоставляет набор $\pi(F) = \pi$ длины $d = m(n+1)$ и вида $\pi =$

$(F(0,\dots,0), F(0,\dots,0,1), F(0,\dots,0,1,1), \dots, F(1,\dots,1))$, разбитый на $(n+1)$ непересекающихся кусков длины $\lambda = m$. При этом «координатами» i-го, $i \in [0,n]$, куска кода $\pi_i = F((0,\dots,0,\underbrace{1,\dots,1}_{i}))$ будем считать набор $\nu_t^{-1}(i)$, где $t = \lceil \log(n+1) \rceil$.

Следовательно, оператор декодирования $A_n^{(2)}$ является тождественным оператором, а оператор кодирования $A_n^{(1)}$ представляет собой счётчик числа единиц, который набор $\alpha = (\alpha_1, \dots, \alpha_n) \in B^n$ переводит в набор β, $\beta \in B^t$, такой, что $\nu(\beta) = \alpha_1 + \dots + \alpha_n$, и имеет сложность [3]

$$L^{\mathrm{C}}\big(A_n^{(1)}\big) \leqslant 9n.$$

Заметим, что основной оператор O_n может быть при этом выбран из множества $P_2^m(t, n+1)$, а его сложность в силу леммы 2.2 удовлетворяет неравенству

$$L^{\mathrm{C}}\big(O_n\big) \lesssim \frac{t \cdot m}{\log t} + O(n).$$

Таким образом, СФЭ Σ, реализующая оператор F и построенная на основе описанного выше локального кодирования, имеет сложность

$$L(\Sigma) \lesssim \frac{m \cdot n}{\log n} + O(n),$$

которая асимптотически совпадает с нижней оценкой (3.7).

Лемма доказана. □

Лемма 3.3. *Для постоянной последовательности $m = m(n)$, $m(n) \geqslant 2$, $n = 1, 2, \dots$, класс операторов Q, для которого множество $Q(n)$ состоит из всех (n,m)-операторов $F = (f_1, \dots, f_m)$ таких, что $f_i(\beta) = f_1(\alpha)$ при любом i, $i \in [2,m]$, любом α, $\alpha \in B^n$, и $\nu(\beta) - \nu(\alpha) \equiv i - 1 \,(\mathrm{mod}\, 2^n)$, является стандартным относительно функционала сложности схем из $\mathfrak{U}^{\mathrm{C}}$ классом.*

Доказательство. Так как $|Q(n)| = 2^{2^n}$ и, следовательно, $\mathcal{J}(Q(n)) = 2^n/n$, то $n = o(\mathcal{J}(Q(n)))$ и Q — невырожденный класс операторов, а из леммы 2.1 непосредственно вытекает необходимая нижняя оценка

$$L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \frac{2^n}{n}.$$

Для получения аналогичной верхней оценки возьмём произвольное натуральное n и натуральное q, $q \leqslant n$, а затем обычным образом разобьём набор БП $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$. Выберем из $Q(n)$ произвольный оператор $F = (f_1, \ldots, f_m)$ и положим $f = f_1$.

Рассмотрим кодирование $\Pi = \Pi_n$, которое сопоставляет оператору $F = F_n$ набор π длины $d = 2^n + (m-1)$, получающийся удлинением столбца значений $\tilde{\alpha}_f$ ФАЛ f первыми $(m-1)$ разрядами этого же столбца. Выделим в этом наборе 2^{n-q} кусков $\pi_{\sigma''}$, $\sigma'' \in B^{n-q}$, длины $\lambda = 2^q + (m-1)$, где кусок $\pi_{\sigma''}$ получается удлинением той части столбца $\tilde{\alpha}_f$, которая соответствует ФАЛ $f(x', \sigma'')$, на $(m-1)$ следующий за ней разряд.

Легко видеть, что построенное кодирование обладает свойством локальности и что координатами куска кода $\pi_{\sigma''}$ можно считать индексирующий его набор σ'', $\sigma'' \in B^{n-q}$. При этом оператор кодирования $A_n^{(1)}$ является оператором выбора поднабора x'' из набора x, а оператор декодирования $A_n^{(2)}$ и основной оператор O_n принадлежат множествам $P_2^m(q+\lambda)$ и $P_2^\lambda(n-q)$ соответственно. При $q = \left\lceil \frac{1}{2}\log n \right\rceil$ для сложности указанных операторов будут выполняться соотношения

$$L^{\mathrm{C}}\big(A_n^{(1)}\big) = 0, \qquad L^{\mathrm{C}}\big(A_n^{(2)}\big) \lesssim m \cdot \frac{2^{q+\lambda}}{q+\lambda} = o\Big(\frac{2^n}{n}\Big),$$

$$L^{\mathrm{C}}\big(O_n\big) \lesssim \big(2^q + (m-1)\big) \cdot \frac{2^{n-q}}{n-q} \sim \frac{2^n}{n},$$

из которых следует, что

$$L^{\mathrm{C}}(F_n) \lesssim \frac{2^n}{n}.$$

Лемма доказана. □

§4 Синтез схем для не всюду определённых функций

В заключение главы 6 рассмотрим задачу синтеза схем для не всюду определённых функций, которая близка к задаче синтеза схем для ФАЛ из специальных классов.

Отображение $f\colon B^n \overset{f}{\mapsto} [0,2]$ будем называть *не всюду определённой* ФАЛ от n БП, а множество $f^{-1}(\{0,1\})$ будем считать её *областью определённости* и обозначать через $\delta(f)$. При этом *доопределением* указанной функции f считается любая ФАЛ из $P_2(n)$, совпадающая с f на множестве $\delta(f)$, а под сложностью $L^{\mathrm{C}}(f)$ реализации функции f в классе $\mathfrak{U}^{\mathrm{C}}$ понимается наименьшая из соответствующих сложностей её доопределений.

Обозначим через $\widehat{P}_2(n)$ множество всех не всюду определённых ФАЛ от БП $X(n) = \{x_1, \ldots, x_n\}$ и для любого t, $t \in [0, 2^n]$, введём его подкласс $\widehat{P}_2(n,t)$, состоящий из всех тех функций f, $f \in \widehat{P}_2(n)$, для которых $|\delta(f)| = t$.

Функция Шеннона для этого класса определяется стандартным образом:

$$L^{\mathrm{C}}\bigl(\widehat{P}_2(n,t)\bigr) = \max_{f \in \widehat{P}_2(n,t)} L^{\mathrm{C}}(f),$$

причём считается, как обычно, что $t = t(n)$, $n = 1, 2, \ldots$.

Лемма 4.1. *Если* $n \log n = o(t(n))$, *то*

$$L^{\mathrm{C}}\bigl(\widehat{P}_2(n, t(n))\bigr) \gtrsim \frac{t(n)}{\log t(n)}. \tag{4.1}$$

Доказательство. Для $n = 1, 2, \ldots$ рассмотрим множество

$$\check{P}_2(n,t) = \{f \in \widehat{P}_2(n,t) \mid \delta(f) = [0,t)\},$$

для каждой из 2^t его функций выберем одно доопределение с минимальной сложностью, и множество этих доопределений обозначим через $Q(n) = Q$. Так как различные функции из $\check{P}_2(n,t)$ не могут иметь общих доопределений, то

$$|\check{P}_2(n,t)| = |Q| = 2^t, \qquad \jmath(Q) = \frac{t}{\log t}.$$

Из последнего равенства и условий леммы следует, что $n = o\big(\jmath(|Q(n)|)\big)$, то есть класс ФАЛ $Q(1), \ldots, Q(n)$, является невырожденным. Из этой невырожденности, леммы 2.1 и очевидных соотношений

$$L^{\mathrm{C}}\big(Q(n)\big) = L^{\mathrm{C}}\big(\check{P}_2(n,t)\big) \leqslant L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big)$$

вытекает оценка (4.1).

Лемма доказана. □

Рассмотрим, далее, несколько утверждений, позволяющих установить для исследуемой функции Шеннона верхнюю оценку вида правой части (4.1) при последовательно ослабляемых ограничениях на рост функции $t = t(n)$.

Лемма 4.2. *Если $t = t(n) \sim n$, то*

$$L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big) \lesssim \frac{t(n)}{\log t(n)}. \tag{4.2}$$

Доказательство. Для произвольного натурального n и натурального q, $1 \leqslant q < n$, разобъём, как обычно, набор БП $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$. Выберем натуральный параметр μ, $\mu \leqslant 2^q$, и для любого s, $s \leqslant 2^q$, построим такое множество наборов $\mathfrak{A}_s$ куба B^s, которое «протыкает» (см. [13]) все грани ранга не больше чем μ,

этого куба и состоит не более, чем из $s \cdot 2^{\mu}$ наборов. Для каждого отрезка I куба B^q от БП x' рассмотрим множество G_I, состоящее из тех равных 0 вне I ФАЛ $P_2(x')$, «проекции» столбцов значений которых на I принадлежат множеству $\mathfrak{A}_s$, где $s = |I|$.

Определим множество ФАЛ G как объединение множеств G_I по всем отрезкам куба $B^q(x')$ и заметим, что

$$|G| \leqslant 2^{\mu+3q}, \qquad L^{\mathrm{C}}\big(\overrightarrow{G}\big) \leqslant 2^{\mu+4q}. \tag{4.3}$$

Заметим также, что любая ФАЛ $\widehat{g}$ из $\widehat{P}_2(q, t')$, где $t' \leqslant \mu$, равная 0 вне отрезка I куба B^q от БП x', имеет в G_I доопределение.

Возьмём произвольную функцию f, $f \in \widehat{P}_2(n, t)$, и разложим её по БП x'':

$$f(x', x'') = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') f_{\sigma''}(x'), \tag{4.4}$$

где при любом σ'', $\sigma'' \in B^{n-q}$, функция $f_{\sigma''}(x')$ принадлежит множеству $\widehat{P}_2(x', t_{\sigma''})$, причём $\Sigma_{\sigma''} t_{\sigma''} = t$.

Для каждого набора σ'', $\sigma'' \in B^{n-q}$, положим $p_{\sigma''} = \lceil t_{\sigma''}/\mu \rceil$ и розобьём куб B^q от БП x' на последовательные отрезки $I_1, \ldots, I_{p_{\sigma''}}$ так, чтобы при любом i, $i \in [1, p_{\sigma''}]$, та часть столбца значений функции $f_{\sigma''}(x')$, которая связана с отрезком I_i содержала μ (соответственно не больше, чем μ) булевских значений, если $i < p_{\sigma''}$ (соответственно $i = p_{\sigma''}$). Пусть, далее, функция $f^{(i)}_{\sigma''}(x')$, $i = 1, 2, \ldots, p_{\sigma''}$, совпадает с функцией $f_{\sigma''}$ на отрезке I_i и равна 0 вне его, а ФАЛ $g^{(i)}_{\sigma''}$ из G_{I_i} является её доопределением. Отсюда следует, что функция $f_{\sigma''}$ может быть представлена в виде

$$f_{\sigma''} = f^{(1)}_{\sigma''} \vee \cdots \vee f^{(p_{\sigma''})}_{\sigma''} \tag{4.5}$$

и поэтому её доопределением является ФАЛ

$$g_{\sigma''} = g^{(1)}_{\sigma''} \vee \cdots \vee g^{(p_{\sigma''})}_{\sigma''}. \tag{4.6}$$

Из (4.3)–(4.6) следует, что ФАЛ $g(x)$ вида

$$g(x) = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''} \left(\bigvee_{i=1}^{p_{\sigma''}} g_{\sigma''}^{(i)}(x') \right), \tag{4.7}$$

где $g_{\sigma''}^{(i)} \in G$ при любых σ'', $\sigma'' \in B^{n-q}$, и i, $i \in [1, p_{\sigma''}]$, является доопределением ФАЛ f и что на основе (4.7) можно построить СФЭ Σ, которая реализует ФАЛ g со сложностью

$$L(\Sigma) \leqslant 2^{4q+\mu} + t/\mu + O(2^{n-q}).$$

Из последнего неравенства при

$$q = \lceil n - \log t + 2 \log n \rceil, \qquad \mu = \lceil \log t - 4q - 2 \log n \rceil$$

получаем требуемую оценку

$$L^{\mathrm{C}}(g) \lesssim \frac{t}{\log t}.$$

Лемма доказана. □

Замечание. Из леммы 4.2 вытекает что, при построении оптимальной схемы для не всюду определённой функции f, $f \in \widehat{P}_2(n,t)$, в общем случае невыгодно доопределять её нулями на множестве $B^n \setminus \delta(f)$. Действительно, полагая $t = \lceil 2^n/3 \rceil$ и доопределяя функции из $\widehat{P}_2(n,t)$ нулями, получим множество $Q(n)$ всюду определённых функций, для которого

$$\log |Q(n)| \sim \log C_{2^n}^{\lceil 2^n/3 \rceil} \sim 2^n \left(\frac{\log 3}{3} + \frac{2}{3} \log \frac{3}{2} \right) = 2^n \cdot \log \frac{3}{\sqrt[3]{4}} > 2^n \cdot \frac{2}{3}.$$

В силу леммы 2.1 отсюда следует, что

$$L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \frac{2}{3} \cdot \frac{2^n}{n},$$

в то время как

$$L^{\mathrm{C}}\big(\widehat{P}_2(n, \lceil 2^n/3 \rceil)\big) \sim \frac{1}{3} \cdot 2^n.$$

Введём некоторые понятия и рассмотрим связанные с ними конструкции, позволяющие ослабить условия леммы 4.2.

Пусть n и s, $s \leqslant n$, — натуральные числа, а A — произвольное множество наборов куба B^n и $|A| \leqslant 2^s$. Будем говорить, что (n, s)– оператор ψ, $\psi \in P_2^s(n)$, является *оператором разделения* или, иначе, *оператором хэширования* для A, если $\psi(\alpha) \neq \psi(\beta)$ для любых различных наборов α и β из A. Обозначим через Λ класс линейных ФАЛ с нулевым свободным членом и будем выбирать нужные нам операторы разделения из множества $\Lambda^s(n)$.

Лемма 4.3. *Для любого множества A, $A \subseteq B^n$, и любого s, $s \leqslant n$, существует оператор ψ, $\psi \in \Lambda^s(n)$, разделяющий некоторое множество A', $A' \subseteq A$, такое, что*

$$|A'| \geqslant t - \frac{t(t-1)}{2^{s+1}},$$

где $t = |A|$.

Доказательство. Рассмотрим множество $\Lambda^s(n)$ как вероятностное пространство, в котором вероятность выбора любого из 2^{ns} операторов равна 2^{-ns}. В этой модели для любых различных наборов α и β из B^n вероятность того, что случайный оператор из $\Lambda^s(n)$ их не разделит, равна 2^{-s}. Действительно, для наборов $\alpha = (\alpha_1, \ldots, \alpha_n) \neq \beta = (\beta_1, \ldots, \beta_n)$ число не разделяющих их линейных ФАЛ вида $\gamma_1 x_1 \oplus \cdots \oplus \gamma_n x_n$ равно числу тех наборов $\gamma = (\gamma_1, \ldots, \gamma_n)$ из B^n, для которых $\gamma_1(\alpha_1 \oplus \beta_1) \oplus \cdots \oplus \gamma_n(\alpha_n \oplus \beta_n) = 0$, то есть равно 2^{n-1}, а значит число тех операторов из $\Lambda^s(n)$, которое не разделяют α и β, равно $2^{s(n-1)}$.

Отсюда следует, что математическое ожидание числа не разделённых случайным оператором из $\Lambda^s(n)$ неупорядоченных пар различных наборов из A равна $t(t-1)/2^{s+1}$. Это означает, что найдётся такой оператор ψ, $\psi \in \Lambda^s(n)$, для которого множество R, состоящее из не разделённых

им пар наборов указанного вида имеет мощность r, где $r \leqslant t(t-1)/2$.

Индукцией по r легко показать, что мощность минимального по включению подмножества A'' множества A, которое «протыкает» все пары из R, то есть имеет с каждой из них непустое пересечение, не больше, чем r. Действительно, при $r = 1$ это очевидно, а при увеличении числа r на 1 мощность множества A'' увеличивается не больше, чем на 1. Таким образом, множество $A' = A \setminus A''$ разделяется оператором ψ и имеет требуемую мощность.

Лемма доказана. □

Следствие. *Если в условиях леммы* $s \geqslant \lfloor 2 \log t \rfloor$, *то* $A' = A$, *так как*

$$|A'| \geqslant t - \frac{t(t-1)}{2^{s+1}} > t - 1.$$

Лемма 4.4. *Если* $2^{n/3} \leqslant t \leqslant 2^n/n^5$, *то*

$$L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big) \lesssim \frac{t}{\log t}.$$

Доказательство. Положим $s = \lfloor \log t + 2 \log n + \log \log t \rfloor$ и заметим, что в силу условий леммы выполняются соотношения

$$s \leqslant n, \qquad s \sim \log t, \qquad nt \log t = o(2^s). \tag{4.8}$$

Возьмём произвольную фунцию f, $f \in \widehat{P}_2(n,t)$, и пусть $A = \delta(f)$, $|A| = t$. Построим по лемме 4.3 для множества A, $A \subset B^n$, оператор ψ, который отображает куб B^n от БП $x = (x_1, \ldots, x_n)$ в куб B^s от БП $y = (y_1, \ldots, y_s)$ и разделяет подмножество A', $A' \subseteq A$, такое, что

$$|A'| = t' \geqslant t - \frac{t(t-1)}{2^{s+1}}.$$

Заметим, что при этом в силу (4.8) $t' \sim t$, $s \sim \log t'$, и следовательно, для множества $\widehat{P}_2(s,t')$, которому принадлежит

функция $\widetilde{f}'(y)$ такая, что $\delta(\widetilde{f}') = \psi(A')$ и $\widetilde{f}'(\psi(\alpha)) = f(\alpha)$ при любом α, $\alpha \in A'$, выполнены условия леммы 4.2. Найдём по этому утверждению такое доопределение $\widetilde{g}'(y)$ ФАЛ $\widetilde{f}'(y)$, для которого

$$L^{\mathrm{C}}(\widetilde{g}') \lesssim \frac{t'}{\log t'} \sim \frac{t}{\log t}. \tag{4.9}$$

Легко видеть, что ФАЛ вида

$$g(x) = \widetilde{g}'(\psi(x)) \cdot \overline{\chi}''(x) \vee g''(x), \tag{4.10}$$

где χ'' – характеристическая ФАЛ множества $A'' = A \setminus A'$, а g'' — ФАЛ, совпадающая с f на A'' и равная 0 вне его, является доопределением ФАЛ f. Заметим, что реализация ФАЛ χ'' и g'' по их совершенным ДНФ даёт следующую суммарную оценку их сложности

$$L^{\mathrm{C}}(\chi'') + L^{\mathrm{C}}(g'') = O(nt^2/2^s),$$

а известная оптимальная реализация линейной ФАЛ — оценку

$$L^{\mathrm{C}}(\psi) \leqslant 4ns,$$

из которых в силу (4.8) вытекает оценка

$$L^{\mathrm{C}}(\chi'') + L^{\mathrm{C}}(g'') + L^{\mathrm{C}}(\psi) = o(t/\log t). \tag{4.11}$$

Таким образом, реализуя ФАЛ $g(x)$ в соответствии с (4.10) и учитывая (4.9), (4.11), получим

$$L^{\mathrm{C}}(f) \lesssim \frac{t}{\log t}.$$

Лемма доказана. □

Лемма 4.5. *Если* $t \leqslant 2^{n/3}$ *и* $n \log^2 n = o(t)$, *то*

$$L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big) \lesssim \frac{t}{\log t}.$$

Доказательство этого утверждения представляет собой упрощённый вариант доказательства леммы 4.4, при котором $s = \lfloor 2 \log t \rfloor$ и, следовательно, $A' = A$, то есть вариант, не требующий реализации ФАЛ χ'', g''.

Суммируя доказанные утверждения, получаем следующий основной результат.

Теорема 4.1. *Если* $n \log^2 n = o(t)$, *то*

$$L^{\mathrm{C}}\bigl(\widehat{P}_2(n,t)\bigr) \sim \frac{t}{\log t}.$$

Замечание. Оценка теоремы верна и при более слабом условии $n \log n = o(t)$ [35].

Литература

[1] *Алексеев В. Б.* Введение в теорию сложности алгоритмов. М.: Издательский отдел ф-та ВМиК МГУ, 2002.

[2] *Алексеев В. Б., Вороненко А. А., Ложкин С. А., Романов Д. С., Сапоженко А. А., Селезнева С. Н.* Задачи по курсу «Основы кибернетики». Издательский отдел ф-та ВМиК МГУ, 2002.

[3] *Алексеев В. Б., Ложкин С. А.* Элементы теории графов, схем и автоматов. М.: Издательский отдел ф-та ВМиК МГУ, 2000.

[4] *Боровков А. А.* Курс теории вероятностей. М.: Наука, 1976.

[5] *Гаврилов Г. П., Сапоженко А. А.* Задачи и упражнения по дискретной математике. 3-е изд., перераб. М.: ФИЗМАТЛИТ, 2004.

[6] Дискретная математика и математические вопросы кибернетики, под редакцией *С. В. Яблонского* и *О. Б. Лупанова*. Т. 1. М.: Наука, 1974.

[7] *Евдокимов А. А.* О максимальной длине цепи в единичном n-мерном кубе // Матем. заметки. 1969. 6. №3. С. 309–319.

[8] *Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И.* Лекции по теории графов. М.: Наука, 1977.

[9] *Журавлев Ю. И.* Локальные алгоритмы вычисления информации // Кибернетика. №1. 1965. С. 12–19.

[10] *Журавлев Ю. И.* Теоретико-множественные методы в алгебре логики // Проблемы кибернетики. Вып. 8. М.: Физматгиз, 1962. С. 5-44.

[11] *Кузьмин В. А.* Оценки сложности реализации функций алгебры логики простейшими видами бинарных программ // Сб. «Методы дискретного анализа в теории кодов и схем». Новосибирск, 1976. Вып. 29. С. 11–39

[12] *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.

[13] *Ложкин С. А.* Лекции по основам кибернетики: Учеб. пособие. М: Издательский отдел Факультета ВМиК МГУ им. М. В. Ломоносова, 2004. 256 С.

[14] *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.

[15] *Лупанов О. Б.* О сложности реализации функций алгебры логики релейно-контактными схемами // Проблемы кибернетики. Вып. 11. М.: Наука, 1964. С. 25–48.

[16] *Лупанов О. Б.* О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. Вып. 3. М.: Физматгиз, 1960. С. 61–80.

[17] *Лупанов О. Б.* Об одном подходе к синтезу управляющих систем — принципе локального кодирования.

// Проблемы кибернетики. Вып. 14. М.: Наука, 1965. С. 31–110.

[18] *Мурога С.* Системы проектирования сверхбольших интегральных схем. М.: Мир, 1985.

[19] *Нечипорук Э. И.* О топологических принципах самокорректирования // Проблемы кибернетики. Вып. 21. М.: Наука, 1969. С. 5–102.

[20] *Нигматуллин Р. Г.* Сложность булевых функций. М.: Наука, 1991.

[21] *Поваров Г. Н.* Метод синтеза вычислительных и управляющих контактных схем // Автоматика и телемеханика. 1957. Т. 18. №2. С. 145–162.

[22] *Сапоженко А. А.* Дизъюнктивные нормальные формы. М.: Изд-во МГУ, 1975.

[23] *Сапоженко А. А.* Некоторые вопросы сложности алгоритмов. Издательский отдел ф-та ВМиК МГУ, 2001.

[24] *Сапоженко А. А., Ложкин С. А.* Методы логического проектирования и оценки сложности схем на дополняющих МОП-транзисторах // Микроэлектроника. 1983. Т. 12. №1. С. 42–47.

[25] *Фихтенгольц Г. М.* Основы математического анализа, том 1. М.: Наука, 1968.

[26] *Фихтенгольц Г. М.* Основы математического анализа, том 2. М.: Наука, 1964.

[27] *Чегис И. А., Яблонский С. В.* Логические способы контроля работы электрических схем // Труды МИ АН СССР. Т. 51. М.: Изд-во АН СССР, 1958. С. 270–360.

[28] *Яблонский С. В.* Введение в дискретную математику. 2-е изд., перераб. и доп. М.: Наука, 1986.

[29] *Яблонский С. В.* Надежность управляющих систем. М.: Изд-во МГУ, 1991.

[30] *Яблонский С. В.* Некоторые вопросы надежности и контроля управляющих систем // Математические вопросы кибернетики. Вып. 1. М.: Наука, 1988. С. 5–25.

[31] *Яблонский С. В.* Элементы математической кибернетики. М.: Высшая школа, 2007.

[32] *Cardot C.* Quelques resultats sur l'application de l'algèbre de Boole à la synthèse des circuits a relais // Ann. Telecommunications. 1952. V.7. №2. P. 75–84.

[33] *Shannon C. E.* The syntesis of two-terminal switching circuits // Bell Syst. Techn. J. 1949. V. 28. №1. P. 59–98 (Русский перевод: *Шеннон К.* Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 59–101).

[34] *Wegener I.* Branching programs and binary decision diagrams. SIAM Publishers, 2000.

[35] *Андреев А. Е.* О сложности реализации частичных булевых функций схемами из функциональных элементов. Дискретная математика, т. 1 (1989), №4. С. 36-45.

[36] *Клейтмен Д.* О проблеме Дедекинда: число булевых монотонных функций. Кибернетический сб. Новая серия, вып. 7. М.: Мир, 1970. С. 43-52.