Московский государственный университет имени М. В. Ломоносова

На правах рукописи

УДК 519.714

Коноводов Владимир Александрович

Методы синтеза и оценки сложности схем с некоторыми структурными ограничениями

Специальность 01.01.09 — дискретная математика и математическая кибернетика

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
д. ф.-м. н., профессор
Ложкин С. А.

Москва – 2015

Содержание

Введение

Общая характеристика работы

Вопросы исследования сложности реализации булевых функций в различных классах схем, которым посвящена диссертация, относятся к теории синтеза управляющих систем, активно изучаемой в математической кибернетике и дискретной математике.

Основная задача данной теории — задача синтеза, — заключается в построении схемы из заданного класса, имеющей предопределенное функционирование. При этом, как правило, это функционирование задается при помощи системы булевых функций, которую схема должна реализовывать в смысле своей семантики. Чаще всего такая задача имеет не единственное решение, поэтому из всех решений требуется найти оптимальное (или близкое к нему) в смысле некоторого функционала сложности.

Задача массового синтеза, которая впервые была рассмотрена в работах Шеннона, состоит в построении оптимального метода или алгоритма синтеза схем из определенного класса для произвольной функции (или системы функций). В этом направлении вводится понятие функции Шеннона от натурального аргумента n как сложности самой «трудной» функции от n переменных, и исследуется поведение этой функции для различных классов схем. Задача индивидуального синтеза состоит в нахождении оптимальной схемы для конкретной функции или последовательности функций.

В диссертации в качестве управляющих систем рассматривается модель схем из функциональных элементов в некоторых конечных базисах и, как частный случай, модель булевых формул. Под сложностью схемы, если это специально не оговорено, понимается число входящих в нее элементов.

Первый результат о поведении функции Шеннона для сложности схем в конечных полных базисах был получен Мюллером в [5] с использованием метода Шеннона [6]. Было показано, что порядок роста указанной функции при стремлении натурального аргумента n к бесконечности равен $2^n/n$.

Затем О. Б. Лупановым [41] был предложен оптимальный метод синтеза схем в произвольных полных конечных базисах. Им же был получен первый результат об асимптотическом поведении функции Шеннона для сложности формул в таких базисах. А именно, была установлена асимптотика функции Шеннона вида

$$\rho \cdot \frac{2^n}{n},$$

для сложности схем из функциональных элементов, и асимптотика для случая булевых формул [42] вида[1]

$$\rho \cdot \frac{2^n}{\log n},$$

где ρ — константа, зависящая от базиса, и одинаковая для случая формул и схем в одном базисе.

В дальнейшем в работах С. А. Ложкина [31] уточнялись оценки остаточного члена асимптотического разложения для некоторых функций Шеннона и устанавливались асимптотические оценки высокой степени точности, в которых указывалась асимптотика второго члена этого разложения. Такие оценки были получены для сложности некоторых основных классов схем.

При решении задач синтеза часто требуется учитывать различного рода ограничения на структуру и параметры управляющих систем. Постановка задач в

[1]Здесь и далее все логарифмы двоичные

такой форме связана, с одной стороны, с тем, что модели с ограничениями часто более точно описывают реальные вычисления, а структурные особенности схем, которые необходимо учитывать, имеют реальную физическую интерпретацию, — это может быть задержка времени срабатывания схемы, объем используемой памяти, возможность размещения схемы на плоскости (т. е. планарность её графа) и др. С другой стороны, в моделях с ограничениями могут возникать новые эффекты, позволяющие более полно исследовать решаемые проблемы. В частности, получение оценок высокой степени точности позволяет обнаруживать «тонкие» эффекты влияния различных структурных ограничений на поведение соответствующей функции Шеннона, когда при заданных ограничениях асимптотика этой функции не меняется, но поведение остаточного члена становится другим.

О. Б. Лупановым одним из первых были исследованы некоторые классы схем из функциональных элементов с ограничениями.

В работе [43] была получена асимптотика функции Шеннона, связанной со сложностью схем, в которых выход любого элемента может быть подсоединен не более чем к заданному числу входов других элементов. Число присоединенных к элементу входов других элементов схемы называется ветвлением выхода. Ограничение этой величины означает ограничение на число использований функций на выходах функциональных элементов схемы как промежуточного результата вычислений. В указанной работе схемы с ограничением на ветвление выходов элементов назывались формулами с частичной памятью. Они занимают промежуточное положение между схемами с произвольным ветвлением и формулами, являющимися схемами без ветвлений. В этой работе было показано, что при допущении ветвлений хотя бы у одного базисного элемента функция Шеннона сложности соответствующих схем имеет такой же порядок роста, как и для схем без ограничений, однако, асимптотика может быть значительно выше.

В работе [44] рассматривались формулы ограниченной глубины в стандартном базисе $\{\vee, \&, \neg\}$. Глубина формулы в этой работе определялась индуктивно. Формулы глубины 0 составляли символы переменных и их отрицаний, а формулы глубины d, $d \geqslant 1$, делились на два типа по внешней операции. Формулы глубины $(d+1)$ с внешней дизъюнкцией представляли собой дизъюнкцию формул глубины d с внешней конъюнкцией. Формулы глубины $(d+1)$ с внешней конъюнкцией определялись двойственным образом. Установлено, что функция Шеннона для сложности формул, имеющих глубину не большую, чем d, и реализующих функции от n переменных, при всех $d \geqslant 3$ асимптотически ведет себя как $2^n / \log n$. При этом для $d = 2$ сложность самой трудной функции в этом классе составляет $3 \cdot n \cdot 2^{n-2} - 1$.

Аналогичный результат для СФЭ был получен в работе [45].

Влияние таким образом определенной глубины формул на их сложность было исследовано в работе [46], где был построен пример последовательности функций, которая в классах формул с большей глубиной реализуется существенно более простыми формулами.

В настоящей работе глубина формулы в смысле [44] называется глубиной альтернирования данной формулы. Следует отметить, что в работе [32] величина $(d-1)$ называлась альтернированием формулы.

Другой тип ограничения, связанный с числом регистров, т. е. ячеек памяти, необходимых для осуществляемых схемой вычислений, был рассмотрен в работах Н. А. Карповой [13, 14]. В [14] изучались схемы с 1 регистром — линейные суперпозиции, и возможность реализации ими булевых функций. Было показано существование функции от трех переменных, которая не может быть представлена линейной суперпозицией в базисе из всех двухместных функций. При переходе к схемам с двумя регистрами такой эффект не имеет места. В [13] получено, что функция Шеннона для класса схем с t регистрами в базисе из всех

p-местных функций при фиксированных $t \geqslant 3$ и $p \geqslant 2$ асимптотически ведет себя как

$$\frac{2^n}{(p-1)\log n}.$$

В работах Н. А. Карповой схемы с t регистрами назывались схемами толщины t.

Задача синтеза управляющих систем с ограничениями активно изучалась и в классе контактных схем. В этой модели реализация булевых функций осуществляется в терминах проводимости контактов, которой управляют внешние булевы переменные. Сложностью таких схем называется число контактов в них. Шенноном [6] был установлен порядок роста соответствующей функции Шеннона, а О. Б. Лупанов в [47] разработал асимптотически оптимальный метод синтеза контактных схем и показал, что функция Шеннона для их сложности асимптотически ведёт себя как $2^n/n$.

Одной из первых моделей контактных схем с ограничениями была модель, в которой степени вершин схемы ограничены некоторой константой. Такие схемы рассматривались в работе А. Д. Коршунова [23], где был описан асимптотически оптимальный метод их синтеза. В работе Х. А. Мадатяна [48] получены асимптотические оценки сложности реализации булевых функций с помощью контатных схем ограниченной ширины.

А. Е. Шиганов [55, 56] рассматривал контактные схемы и итеративные контактные схемы с различными типами ограничений на смежные контакты. В работе [56] были разработаны методы синтеза ориентированных контактных схем с ограничением на полустепени исхода вершин, и установлена асимптотика первого остаточного члена асимптотического разложения функции Шеннона, зависящая от параметров ограничений.

Другой моделью, изучаемой в математической кибернетике, являются вычисляющие программы. Класс бинарных программ был введён в работе В. А. Кузьмина [25], в которой рассматривались два основных типа команд — вычислительные команды, записывающие в заданную ячейку памяти результат применения заданной двуместной логической функции к содержимому некоторых других ячеек памяти, и переадресующие команды, которые осуществляют условный или безусловный переход на команду с заданным номером. Асимптотику вида

$$\frac{2^n}{3n}$$

для сложности таких программ получил О. М. Касим-Заде в [15]. В [25] показано, что программы, состоящие только из вычислительных команд, эквивалентны классу схем из функциональных элементов, поэтому для соответствующей функции Шеннона справедлива асимптотика $2^n/n$. В [25] также указано, что бинарные программы, где все ячейки памяти в вычислительных командах, в которые происходит запись результата вычисления, различны, эквивалентны одному из специальных видов контактных схем, и установлена асимптотика $2^{n-1}/n$ функции Шеннона для такого класса программ. Класс бинарных программ, состоящих только из переадресующих команд, был впервые предложен Ли в [4]. Такие программы также называются BDD (Binary Decision Diagrams), и имеют огромное значение в прикладных задачах. Подходы к созданию алгоритмов для синтеза и верификации схем, основанных на представлении булевых функций специальными упорядоченными BDD, были исследованы в работе Брайанта [1]. Наряду с обычными BDD рассматриваются также различные их модификации, имеющие приложения в теории квантовых вычислений. В работе Ф. М. Аблаева [7] рассматривались синтаксические квантовые ветвящиеся программы, вычисляющие булевы функции с большой надежностью.

Асимптотику $2^n/n$ функции Шеннона для сложности двоичных решающих диаграмм установил В. А. Кузьмин в [25]. Такие программы представимы в виде контактных схем из ориентированных контактов без циклов с одним истоком, являющимся входом схемы, и двумя стоками, являющимися её выходами. При этом выходы помечены символами 0 и 1, а из каждой невыходной вершины исходит ровно два контакта, один из которых помечен символом переменной, а другой — символом её отрицания. Для некоторых классов BDD С. А. Ложкиным [35] и А. Е. Шигановым [57, 58] были получены асимптотические оценки высокой степени точности для соответствующих функций Шеннона.

Ещё одно обобщение бинарных программ было введено С. В. Грибком в работе [11]. Вычисляющая программа представлялась в виде набора подпрограмм, каждой из которых соответствовало отдельное множество ячеек памяти, и была введена команда вызова подпрограммы. Исследована задача синтеза для таких классов программ со специальными весовыми характеристиками и получены асимптотические оценки для соответствующих функций Шеннона. Кроме того, для некоторых классов были установлены оценки высокой степени точности, в которых асимптотика второго члена разложения зависела от весовых характеристик — параметров ограничений.

Отметим следующую связь между вычислительными программами и схемами с регистрами. Если под шириной вычисляющей программы понимать минимальное число ячеек памяти, необходимых для хранения её внутренних переменных, то вычисляющие программы ширины t представляют собой схемы с t регистрами, определенные в указанных выше работах Н. А. Карповой.

Другим направлением задачи синтеза является исследование реализации булевых функций в схемах с ограничениями на типы соединяемых элементов и номера присоединяемых входов. При этом предполагается, что базисные элементы имеют входы двух видов — прямые и итеративные. Прямые входы могут являться только входами схемы, а на итеративные входы должны подаваться выходы других элементов. Возможность итеративных входов являться входами схемы может оговариваться отдельно. Впервые задача синтеза в такой модели была предложена и рассмотрена С. А. Ложкиным в работах [37, 38]. В [37] был установлен критерий полноты относительно всех функций прямых переменных при наличии в базисе элементов, реализующих функции-константы, и описаны некоторые особенности решетки вложения замкнутых классов функций с прямыми и итеративными переменными. В [38] было исследовано поведение функции Шеннона на уровне асимптотических оценок высокой степени точности для класса всех схем из функциональных элементов над произвольным полным базисом с прямыми и итеративными переменными и некоторых его подклассов. Эта функция имеет «стандартный» порядок роста $2^n/n$. В [38] указано также, что функция Шеннона для формул в таких базисах имеет порядок роста не более, чем 2^n, и не менее, чем $2^n/\log n$.

К этому направлению задачи синтеза относится также задача реализации функций алгебры логики α-формулами, которые определяются индуктивно следующим образом. Пусть X — некоторое множество переменных. Если φ — α-формула или символ переменной из множества X, а f — функция из некоторого множества A, то выражение вида $f(\varphi, x_{i_1}, \ldots, x_{i_s})$, где $x_{i_1}, \ldots, x_{i_s} \in X$, является α-формулой над множеством функций A. Нетрудно видеть, что α-формулы над множеством A можно рассматривать как формулы в базисе A', состоящем из констант и функций множества A, в каждой из которых первая переменная является итеративной. Формулы такого вида были введены в работе М. М. Глухова [10] и рассматривались над множествами функций k-значных логик, $k \geqslant 2$. В [10] было показано существование при $k \geqslant 7$ конечных α-полных систем, т. е. таких систем, что любую функцию k-значной логики можно реализовать α-формулой над этой системой. А. Л. Чернышовым в работе [54] был доказан критерий α-полноты функций многозначной логики и показано отсутствие конечных α-полных систем в случае булевых функций. Оценки функции Шеннона для глубины α-формул были получены в работах Д. В. Трущина [50, 51].

Модель схем из функциональных элементов в базисах с прямыми и итеративными переменными обладает рядом сходств с другими моделями, использующими память. Так, в случае базиса, в котором каждый элемент имеет не более одного итеративного входа, соответствующие схемы представимы как схемы с одним регистром памяти. Другой базис, приводящий к связи с моделью вычисляющих программ, — базис, состоящий из функции $\mu_1 = x_1 y_1 \vee \bar{x}_1 y_2$, в которой переменные y_1 и y_2 итеративные, а x_1 — прямая. Класс схем в этом базисе, в которых итеративные входы функции μ_1 могут быть константными, изоморфно соответствует классу бинарных адресующих программ.

При достаточно сильных ограничениях возникает вопрос о возможности реализации всех функций алгебры логики в рассматриваемом классе схем. Например, схемы в базисах, в которых каждый элемент имеет не более одного итеративного входа, не всегда обладают указанной функциональной полнотой. Формулы с глубиной альтернирования 1 не позволяют реализовывать, например, линейные функции более, чем одной переменной.

В ряде работ задача синтеза управляющих систем решалась для специальных классов функций, в частности для функций, связанных с языками. В [39] оценки высокой степени точности установлены для сложности реализации функций из таких классов схемами из функциональных элементов с ограниченной глубиной ветвления и ориентированными контактными схемами, в [17] — для сложности реализации таких функций в специальном классе схем из функционально-проводящих элементов.

Основные определения и формулировка полученных результатов

Пусть $X = \{x_1, \ldots, x_n, \ldots\}$ — счетный алфавит булевых переменных, каждая из которых может принимать значения из множества $B = \{0, 1\}$. Пусть, далее, B^n, $n = 1, 2, \ldots,$ — единичный n-мерный куб, то есть множество всех упорядоченных наборов длины n из элементов B; а $P_2(n)$ – множество всех функций $f = f(x_1, \ldots, x_n) \ : \ B^n \xrightarrow{f} B$. Элементы m-й декартовой степени множества $P_2(n)$, т. е. множества $(P_2(n))^m = P_2^m(n)$, будем, как обычно, считать системами функций и записывать их в виде вектора $(f_1, \ldots, f_m)$, где $f_i \in P_2(n)$ при любом i, $i \in [1, m]$.

Будем рассматривать схемы из функциональных элементов (в дальнейшем будем называть их просто схемы) и формулы в различных полных базисах, состоящих из функциональных элементов (далее — элементов). Базис Б$_0$, состоящий из элементов $\&$, $\vee$ и $\neg$ веса 1, которые реализуют функции алгебры логики $x_1 \cdot x_2$, $x_1 \vee x_2$ и $\bar{x}_1$ соответственно, будем называть *стандартным*. Под формулами будем понимать те одновыходные схемы, в которых выход любого элемента либо поступает на вход ровно одного (другого) элемента, либо является выходом схемы. Полнота базиса означает возможность реализации всех функций алгебры логики схемами в этом базисе. Каждый элемент базиса $\mathcal{E}$, если не оговорено иное, имеет вес $\rho(\mathcal{E}) = 1$.

Под *сложностью* $\mathcal{L}(\Sigma)$ схемы Σ понимается, как обычно, сумма весов её элементов. При этом, если веса всех элементов равны 1, то сложность схемы совпадает с числом элементов в ней, и для указанной величины будет использоваться обозначение $L(\Sigma)$, а для соответствующей функции Шеннона — обозначение $L(n)$. В случае существования элементов неединичного веса функция Шеннона будет обозначена как $\mathcal{L}(n)$.

Рангом формулы $\mathcal{F}$ будем называть число переменных, встречающихся в её записи, т. е. число листьев в соответствующем ей дереве.

Определим понятие глубины альтернирования схемы в стандартном базисе Б$_0$. Формулу C, которая состоит из r, $r \geqslant 1$, элементов $\mathcal{E}^{(1)}, \ldots, \mathcal{E}^{(r)}$, и в которой выход элемента $\mathcal{E}^{(i)}$, $i = 1, \ldots, r-1$, является входом элемента $\mathcal{E}^{(i+1)}$, будем называть *нетривиальной цепью*, а число r – её *длиной* или *глубиной*. Если при этом последовательность $\varphi^{(1)}, \ldots, \varphi^{(r)}$, где $\varphi^{(i)}$, $\varphi^{(i)} \in Б_0$, – тип базисного элемента $\mathcal{E}^{(i)}$, $i = 1, \ldots, r$, имеет вид $\varphi_1, \ldots, \varphi_1, \varphi_2, \ldots, \varphi_2, \ldots, \varphi_a, \ldots, \varphi_a$, где $\varphi_j \neq \varphi_{j+1}$ при всех j, $j = 1, \ldots, a-1$, а число c равно 1 в случае $\varphi_1 = \neg$ и равно 0 в остальных случаях, то разность $(a-c)$ будем называть *глубиной альтернирования* указанной цепи C. Формулу, которая состоит из единственной вершины, являющейся как её входом, так и её выходом, будем считать тривиальной цепью, а глубину и глубину альтернирования такой цепи положим равными 0.

Для схемы Σ её *глубина* $D(\Sigma)$ (*глубина альтернирования* $A(\Sigma)$) определяется как максимальная глубина (соответственно глубина альтернирования) цепей, являющихся подсхемами Σ.

Таким образом, схема Σ имеет глубину альтернирования a в том и только том случае, когда максимальное число изменений типов элементов в последовательностях, которые являются цепями схемы Σ и не содержат отрицаний, присоединённых к её входам, равно $(a-1)$. Так, любая элементарная конъюнкция или дизъюнкция переменных и их отрицаний имеет глубину альтернирования 1, а любая отличная от них дизъюнктивная нормальная форма (ДНФ) и конъюнктивная нормальная форма (КНФ) имеют глубину альтернирования 2.

Для любого a, $a \geqslant 2$, определим сложность $L^{(a)}(f)$ функции f как минимальную из сложностей тех реализующих её формул, глубина альтернирования которых не больше, чем a. Введем далее функцию Шеннона $L^{(a)}(n)$ как максимальную из сложностей $L^{(a)}(f)$, где максимум берется по всем функциям f от булевых переменных $x_1, \ldots, x_n$.

При любом a, $a \geqslant 3$, из результатов О. Б. Лупанова [44] следуют оценки[2]

$$\frac{2^n}{\log n}\left(1 - O\left(\frac{1}{\log n}\right)\right) \leqslant L^{(a)}(n) \leqslant L^{(3)}(n) \leqslant \frac{2^n}{\log n}\left(1 + \frac{2\log\log n + O(1)}{\log n}\right),$$

[2]Для числовых функций $g(n)$ и $h(n)$ натурального аргумента n запись $h(n) = O(g(n))$ означает, как обычно, что отношение $|h(n)/g(n)|$ ограничено сверху. Эта запись равносильна записи $g(n) = \Omega(h(n))$. Запись $h(n) = \Theta(g(n))$ означает, что $h(n) = O(g(n))$ и $g(n) = O(h(n))$.

которые устанавливают поведение функции Шеннона $L^{(a)}(n)$ с относительной погрешностью вида $O\left(\frac{\log\log n}{\log n}\right)$. Положим $\log^{[a]} x = \underbrace{\log\ldots\log}_{a \text{ раз}} x$, если указанный повторный логарифм определен и неотрицателен, и $\log^{[a]} x = 0$ в остальных случаях. При этом будем считать, что $\log^{[0]} x = 1$ при любом x.

В настоящей работе при $a \geqslant 3$ указанные выше оценки величины $L^{(a)}(n)$ уточняются и устанавливается её поведение с относительной погрешностью вида $O\left(\frac{1}{\log n}\right)$.

Теорема 1 ([26]). *Для любого натурального числа* a, $a \geqslant 3$, *при растущем значении натурального аргумента* n, $n \geqslant 2$, *выполняется соотношение*

$$L^{(a)}(n) = \frac{2^n}{\log n}\left(1 + \frac{\log^{[a-1]} n \pm O(1)}{\log n}\right).$$

Далее приведем результаты, связанные с реализацией функций из специального класса, связанного с конечными грамматиками, формулами глубины альтернирования 3.

В работе [2] введено понятие грамматики с конечным числом состояний. Модифицируем это понятие следующим образом. Пусть грамматика Γ задается множеством внутренних состояний $S_1, \ldots, S_p$ и множеством грамматических правил. Каждое грамматическое правило определяется упорядоченной парой (σ, k), $\sigma \in \{0, 1\}$, $1 \leqslant k \leqslant p$. Если такое правило (σ, k) сопоставляется состоянию S_i, $1 \leqslant i \leqslant p$, то это означает, что, когда грамматика находится в состоянии S_i, может быть произведен символ σ, причем грамматика переходит в состояние S_k. Выделим в Γ два произвольных (возможно, совпадающих) состояния S_i и S_j, $1 \leqslant i, j \leqslant p$. Грамматика Γ, отправляясь от состояния S_i, пробегает в соответствии с грамматическими правилами последовательность состояний $S_{i_1}, \ldots, S_{i_t}$, где $1 \leqslant i_1, \ldots, i_t \leqslant p$, $i_1 = i$, $i_t = j$, и переходит в состояние S_j, при этом она производит слово, состоящее из цепочки символов в том порядке, в котором они выбирались при последовательных переходах. Пусть T_{ij} — множество таких слов. *Языком* грамматики Γ без выделенного начального состояния будем называть язык

$$T_\Gamma = \bigcup_{1 \leqslant i,j \leqslant p} T_{ij}.$$

Пусть $T_\Gamma(s)$, $s \geqslant 1$, — множество слов языка T_Γ, длина которых равна s. Тогда, как следует из работы [2], мощность $T_\Gamma(s)$ либо ограничена, либо с ростом s растет линейно, либо экспоненциально. В последнем случае существует такая константа $\sigma_\Gamma \in (0, 1]$, что при $s \to \infty$ справедливо [17] соотношение

$$|T_\Gamma(s)| = 2^{\sigma_\Gamma \cdot s + O(1)}. \tag{1}$$

Величину σ_Γ будем называть *мощностной константой* грамматики Γ.

Пусть $Q_\Gamma(n)$ — класс булевых функций от n, $n \geqslant 1$, переменных, множество столбцов значений которых совпадает с $T_\Gamma(2^n)$. Положим

$$Q_\Gamma = \bigcup_{n \geqslant 1} Q_\Gamma(n).$$

Как обычно, функция Шеннона для сложности формул с глубиной альтернирования не более 3, реализующих функции из класса Q_Γ, определяется как

$$L_\Gamma(n) = \max_{f \in Q_\Gamma(n)} L^{(3)}(f).$$

Теорема 2 ([27]). *Пусть Γ — грамматика с конечным числом состояний, для которой мощность множества $T_\Gamma(s)$ растет экспоненциально с ростом s, а σ_Γ, $\sigma_\Gamma \in (0, 1]$, — её мощностная константа. Тогда при растущем значении натурального аргумента n, $n \geqslant 2$, справедливо соотношение*

$$L_\Gamma(n) = \sigma_\Gamma \cdot \frac{2^n}{\log n} \left(1 + \frac{\log\log n \pm O(1)}{\log n}\right).$$

Эта теорема устанавливает поведение функции Шеннона $L_\Gamma(n)$ с относительной погрешностью $O\left(\frac{1}{\log n}\right)$, и, тем самым, приведённая в ней оценка является оценкой высокой степени точности.

В качестве примера рассмотрим грамматику Γ_0 с двумя состояниями S_1 и S_2, в которой состоянию S_1 приписаны правила $(0,1)$, $(1,2)$, а состоянию S_2 — правило $(0,1)$. Схематично она изображена на рис. 1.

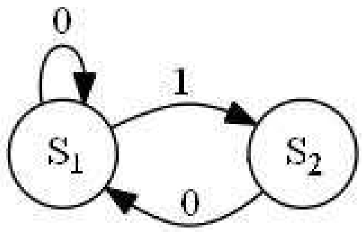

Рисунок 1: Грамматика Γ_0.

Этой грамматике соответствует класс Q_{Γ_0} всех булевых функций, столбцы значений которых не содержат двух подряд идущих единиц. По индукции легко доказать, что $|T_{\Gamma_0}(n)| = F_{n+2}$ для всех n, $n = 1, 2, \ldots$, где F_n — n-ое число Фибоначчи. Так как (см., например, [9])

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right),$$

то для данной грамматики мощностная константа $\sigma_{\Gamma_0} = \log\dfrac{1+\sqrt{5}}{2}$, поэтому, согласно теореме 2, справедлива следующая оценка функции Шеннона для сложности формул глубины альтернирования не большей, чем 3, реализующих функции из класса Q_{Γ_0} :

$$L_{\Gamma_0}(n) = \left(\log(1+\sqrt{5}) - 1\right) \cdot \frac{2^n}{\log n}\left(1 + \frac{\log\log n \pm O(1)}{\log n}\right).$$

Далее приведем определения и результаты, связанные со схемами ограниченной ширины.

Будем говорить, что схема Σ является *схемой с t регистрами*, если все её функциональные элементы занумерованы числами $1, 2, \ldots, L$, где $L = L(\Sigma)$, и каждому из них приписан регистр из множества $R = \{r_1, \ldots, r_t\}$ так, что для произвольного элемента $\mathcal{E}$ схемы Σ выполняются условия:

1. номер $\mathcal{E}$ больше номера любого элемента, выход которого подается на один из его входов;
2. если на вход элемента $\mathcal{E}$ с номером j, $j \in [2, L]$, подается выход элемента $\mathcal{E}'$ с номером i, $i \in [1, j-1]$, и приписанным ему регистром r, $r \in R$, то другим элементам с номерами из интервала (i, j) регистр r не приписан.

Кроме того, будем считать, что значения входных переменных схемы записаны в отдельных входных регистрах $r_{x_1}, \ldots, r_{x_n}$, не лежащих во множестве R. При этом предполагается, что функциональный элемент с номером j, $j = 1, \ldots, L$, указанной схемы «срабатывает» в момент времени j, выбирая значение каждого своего входа либо из регистра, приписанного выходу соответствующего элемента Σ, либо из некоторого входного регистра, и занося вычисленное значение своей базисной функции в приписанный ему регистр.

Входные регистры, таким образом, не используются схемой в процессе описанного вычисления для записи результатов. Регистры из множества R, наоборот, служат ячейками памяти для вычисления, производимого схемой. Формальное определение вычисления дано в работе [13].

Для схемы Σ с t, $t \in \{1, 2, \ldots\}$, регистрами число t будем называть её *шириной*. Для произвольной функции алгебры логики f и для любого t, $t \in \{1, 2, \ldots\}$, определим сложность $L_{\text{Б}}^{\{t\}}(f)$ функции f как минимальную из сложностей тех реализующих её схем в базисе Б, ширина которых не превосходит t, причем в случае стандартного базиса $\{\&, \vee, \neg\}$ индекс Б_0 будем опускать.

Пусть $L_{\text{Б}}^{\{t\}}(n)$ — функция Шеннона для класса схем в базисе Б, ширина которых не превосходит t. Как следует из работы [13], при любом натуральном t, $t \geqslant 3$, функция $L_{\text{Б}}^{\{t\}}(n)$ асимптотически равна $c_{\text{Б}} \frac{2^n}{\log n}$, где $c_{\text{Б}}$ — константа, зависящая от базиса. В частности, в случае стандартного базиса[3] $L^{\{t\}}(n) \sim \frac{2^n}{\log n}$ для $t \geqslant 3$.

Заметим, что формула с глубиной альтернирования a с помощью тождеств коммутативности и ассоциативности [32] может быть преобразована в формулу, которая при подходящей нумерации вершин и приписывании им регистров становится схемой с a регистрами. Это дает возможность установить справедливость следующего утверждения.

Утверждение. *Для любого натурального* t, $t \geqslant 3$, *при растущем значении натурального аргумента* n, $n \geqslant 2$, *выполняется соотношение*

$$\frac{2^n}{\log n}\left(1 - O\left(\frac{1}{\log n}\right)\right) \leqslant L^{\{t\}}(n) \leqslant \frac{2^n}{\log n}\left(1 + \frac{\log^{[t-1]} n + O(1)}{\log n}\right).$$

В настоящей работе рассмотрены некоторые индивидуальные оценки сложности функций в классе схем с малым числом регистров.

Функция

$$s_n(x_1, \ldots, x_n) = \bigvee_{1 \leqslant i < j \leqslant n} x_i x_j.$$

называется *монотонной симметрической функцией с порогом 2*. В работе [12] доказано, что сложность реализации этой функции в классе схем из функциональных элементов в базисе $\{\&, \vee\}$ без ограничений асимптотически равна $2n$. Кроме того, в [24] установлено, что в классе π-схем (а, следовательно, и в классе формул в стандартном базисе, у которых отрицания стоят только над переменными и не учитываются при подсчете сложности) сложность этой функции равна

$$\lfloor \log n \rfloor \cdot 2^{\lfloor \log n \rfloor} + (\lfloor \log n \rfloor + 2) \cdot \left(n - 2^{\lfloor \log n \rfloor}\right),$$

[3] Асимптотическое равенство $f(n) \sim g(n)$ неотрицательных функций $f(n)$ и $g(n)$ натурального аргумента n означает, что $f(n) = (1 + o(1))g(n)$; асимптотическое неравенство $f(n) \gtrsim g(n)$ означает, что $f(n) \geqslant (1 - o(1))g(n)$.

что асимптотически равно $n \log n$. В [40] этот результат был обобщён для случая π-схем, в которых контакты различных переменных могут иметь различные веса.

Линейной функцией порядка n, $n \geqslant 2$, будем называть функцию $l_n = x_1 \oplus \ldots \oplus x_n$, где символом $\oplus$ обозначается сумма по модулю 2. Известно [49], что сложность её реализации в классе схем в стандартном базисе $Б_0$ без ограничений равна $4n-4$. Из результатов В. М. Храпченко [53] и С. В. Яблонского [60] следует, что сложность этой функции в классе π-схем (а, следовательно, и в классе формул в $Б_0$, у которых отрицания стоят только над переменными) равна $\Theta(n^2)$. Реализовать линейную функцию порядка n при $n \geqslant 2$ схемой ширины 1 в базисе $Б_0$ невозможно. Следующая теорема, в частности, показывает, что в классе схем с двумя регистрами данная функция допускает оптимальную реализацию.

Теорема 3 ([19]). *Для любого натурального n, $n \geqslant 2$, справедливы следующие соотношения:*

$$L^{\{2\}}(l_n) = L^{\{2\}}(\bar{l}_n) = 4n - 4;$$

$$L^{\{3\}}(s_n) \leqslant 3n - 5.$$

При $n \to \infty$ справедлива оценка:

$$L^{\{2\}}(s_n) \lesssim n \log n.$$

Следует отметить, что, как следует из работы [40], каждая минимальная формула для функции s_n имеет глубину альтернирования 3 и сложность, асимптотически равную $n \log n$, и, следовательно, может быть представлена схемой с 3 регистрами. Приведенная теорема устанавливает возможность реализации этой функции схемой линейной сложности с тремя регистрами, а также схемой с двумя регистрами со сложностью, асимптотически минимальной для случая формул — $n \log n$.

Для любого множества G, $G \subseteq P_2(n)$, будем использовать обозначение $\overrightarrow{G}$ для системы, составленной из функций множества G, упорядоченных в соответствии с лексикографическим порядком их столбцов значений.

Будем говорить, что схема с t, $t \geqslant 1$, регистрами реализует систему из m, $m > 1$, функций F, $F \subseteq (P_2(n))^m$, если в схеме выделены m элементов $\mathcal{E}_1, \ldots, \mathcal{E}_m$, являющихся выходными, и имеются m дополнительных выходных регистров $r'_1, \ldots, r'_m$ ($r'_i \notin R$ при всех i, $i = 1, \ldots, m$) таких, что после срабатывания $\mathcal{E}_i$ ($i = 1, \ldots, m$) в регистр r'_i записывается значение из регистра, приписанного элементу $\mathcal{E}_i$. Кроме того, значения в выходных регистрах не могут подаваться на входы элементов схемы.

Сложностью системы функций F будем, как обычно, называть минимальную сложность схем с $|F|$ выходами, реализующих систему F. Соответствующую сложность в классе схем с t регистрами в стандартном базисе будем обозначать $L^{\{t\}}(F)$.

Система функций

$$\overrightarrow{Q}_n = \{\bar{x}_1 \cdots \bar{x}_{n-1}\bar{x}_n,\ \bar{x}_1 \cdots \bar{x}_{n-1}x_n,\ \ldots,\ x_1 \cdots x_{n-1}x_n\}, \tag{2}$$

состоящая из всех элементарных конъюнкций ранга n от n переменных, называется *дешифратором* порядка n. Известно [8], что его сложность в классе схем из функциональных элементов в стандартном базисе без ограничений асимптотически равна 2^n. В диссертации доказывается следующая теорема.

Теорема 4 ([19]). *При $n \to \infty$ справедливы следующие оценки:*

$$L^{\{3\}}(\overrightarrow{Q}_n) \sim 2^n,$$

$$L^{\{2\}}(\overrightarrow{Q}_n) = \Theta(2^n).$$

Введем дополнительно счетный алфавит $Y = \{y_1, \ldots, y_n, \ldots\}$ булевых переменных, которые будем называть *итеративными*. В контексте схем и формул в базисах, содержащих переменные из множества Y, переменные из множества X будем называть *прямыми* переменными.

Для каждого множества переменных Z обозначим через $P_2(Z)$ множество всех функций, зависящих от переменных из Z. В частности, $P_2(\{x_1, \ldots, x_n\}) = P_2(n)$. Функции, не имеющие общих существенных переменных, будем называть *независимыми*.

На множестве $P_2(X \cup Y)$, согласно [37], определим следующие операции суперпозиции:

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

Пусть $A \subset P_2(X \cup Y)$ — некоторое конечное множество базисных функций. В соответствии с введенными операциями суперпозиции будем рассматривать одновыходные схемы над базисом A, в которых:

1. прямые входы любого элемента либо присоединяются к входам схемы, либо являются константными входами (вход называется константным, если вместо него в базисный элемент подставлена константа 0 или 1);
2. итеративные входы любого элемента либо присоединяются к выходам других элементов, либо присоединяются к входам схемы, либо являются константными входами;

3. неконстантным входам схемы сопоставлены некоторые переменные из множества X.

Отметим, что с точки зрения рекурсивного определения формулы как символьной записи [59], указанные выше операции 1–6 дают возможность проводить суперпозицию только по итеративным переменным базисных функций.

Систему функций A будем называть *полной*, если для любой функции f, $f \in P_2(X)$, существует формула над A указанного вида, реализующая функцию f. Везде далее, если не указано обратное, рассматриваются только конечные полные системы функций. Функцией Шеннона $\mathcal{L}_A(n)$ для сложности формул в базисе A, как обычно, называется максимальное значение $\mathcal{L}_A(f)$ среди всех функций f, $f \in P_2(n)$, где $\mathcal{L}_A(f)$ — минимальная сложность формулы из рассматриваемого класса, реализующей функцию f.

Пусть $A \subseteq P_2(X \cup Y)$. Множество тех функций, которые можно получить из функций системы A в результате применения операций суперпозиции с номерами из множества T', $T' \subseteq T = \{1, 2, 3, 4, 5, 6\}$, обозначим через $[A]_{T'}$, и пусть $[A]_T = [A]$.

В работе [37] вводится множество $\delta(A) = \left[[A]_{\{2\}} \cap P_2(Y)\right]_{\{3,4,6\}}$, которое будем называть *итеративным замыканием* базиса A. Заметим, что множество $\delta(A)$ является «обычным» замкнутым классом [59] в $P_2(Y)$, содержащим все константы, и поэтому совпадает с одним из классов системы

$$\Delta = \{B, I, O, D, K, L, M, P_2(Y)\}, \tag{3}$$

где $B = \{0, 1\}$, $I = Y \cup B$, $O = I \cup \{\bar{y} \ : \ y \in Y\}$, класс D (класс K) содержит константы и дизъюнкции (соответственно, конъюнкции) переменных Y, а классы L и M состоят из линейных и монотонных функций от переменных Y соответственно. Структура включений классов системы Δ изображена на рис. 2.

В настоящей работе доказано, что для оператора δ справедливо более наглядное представление:

Теорема 5 ([18]). *Для любой системы функций* A, $A \subseteq P_2(X \cup Y)$, *справедливо равенство*

$$\delta(A) = [A] \cap P_2(Y).$$

Таким образом, $\delta(A)$ определяет все те функции от итеративных переменных, которые можно получить из базисных функций рассматриваемыми операциями суперпозиции. Введение оператора δ позволяет классифицировать все системы функций от прямых и итеративных переменных по их итеративным замыканиям. Эта классификация имеет прямое отношение к исследованию сложности формул в соответствующих базисах.

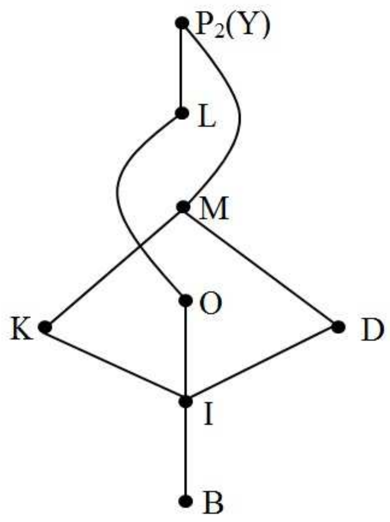

Рисунок 2: Структура включений классов системы Δ

Рассмотрим произвольный базис $A = \{\mathcal{E}_1, \ldots, \mathcal{E}_b\}$, $A \subseteq P_2(X \cup Y)$. Будем считать, что каждый элемент $\mathcal{E}_i$, $i = 1, \ldots, b$, имеет вес $\rho(\mathcal{E}_i) = L_i$, $L_i > 0$, и k_i входов, при этом k_i' из них прямые, а $k_i'' = k_i - k_i'$ итеративны. Кроме того, везде далее будем предполагать, что функция, реализуемая элементом $\mathcal{E}_i$, $i = 1, \ldots, b$, существенно зависит от всех своих k_i входных переменных.

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

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

Без ограничения общности будем считать, что $k''_i = 0$ для всех i, $b' < i \leqslant b$, где $1 \leqslant b' \leqslant b$, при этом базис A разбивается на два множества

$$A' = \{\mathcal{E}_1, \ldots, \mathcal{E}_{b'}\}, \quad A'' = \{\mathcal{E}_{b'+1}, \ldots, \mathcal{E}_b\},$$

во втором из которых (возможно, пустом) все входы каждого элемента прямые.

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

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

Таким образом, макроблок M имеет сложность $\mathcal{L}_M = L_j + L_{i_1} + \ldots + L_{i_m}$, а число его входов равно $k_M = k'_j + k_{i_1} + \ldots + k_{i_m} + k''_j - m = k_{i_1} + \ldots + k_{i_m} + k_j - m$. *Приведенным весом* макроблока M назовем величину

$$\rho_M = \frac{\mathcal{L}_M}{k_M - 1}.$$

Макроблок M указанного вида назовем *каноническим,* если $m = k''_j - 1$ и $i_1 = \ldots = i_m$ во введённых выше обозначениях. Макроблок назовем *минимальным* в базисе A, если он имеет минимальный приведенный вес среди всех макроблоков в этом базисе.

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

Следующая теорема устанавливает асимптотику функции Шеннона для сложности формул в базисах, итеративное замыкание которых содержит класс монотонных функций. Для таких базисов функция Шеннона имеет «стандартный» для формул порядок роста $2^n/\log n$. В остальных семействах базисов в классификации по их итеративным замыканиям существуют примеры, для которых эта функция имеет «граничный» порядок роста 2^n.

Теорема 6 ([18, 28]). *Для любой системы функций A, $A \subseteq P_2(X \cup Y)$, такой, что $\delta(A) \in \{M, P_2(Y)\}$, при $n \to \infty$ справедливо соотношение*

$$\mathcal{L}_A(n) \sim \rho_A \cdot \frac{2^n}{\log n}.$$

Для каждого δ, $\delta \in \{I, O, D, K, L\}$, существует базис A такой, что $\delta(A) = \delta$ и при этом

$$\mathcal{L}_A(n) = \Theta\left(2^n\right).$$

В некоторых базисах A, таких, что $\delta(A) = D$ и $\mathcal{L}_A(n) = \Theta(2^n)$, самой сложной функцией является линейная функция $l_n = x_1 \oplus \ldots \oplus x_n$, однако, как показывает следующий результат, при переходе от базиса к базису сложность функции l_n может кардинально изменяться в рамках одного и того же семейства.

Теорема 7 ([18]). *В базисе* [4] $A_1 = \{(x_1 \oplus x_2)y_1, (x_1 \sim x_2)y_1, y_1 \vee y_2\}$ *сложность линейной функции l_n удовлетворяет соотношению*

$$L_{A_1}(l_n) = \Theta(2^{n/2}),$$

а в базисах $A_2 = \{(x_1 \oplus x_2)y_1, y_1 \vee y_2\}$ и $A_3 = \{(x_1 \sim x_2)y_1, y_1 \vee y_2\}$ — соотношению

$$c_1 \cdot 2^{n/2} \leqslant L_{A_i}(l_n) \leqslant c_2 \cdot 3^{n/2}, \quad i = 1, 2,$$

где c_1, c_2 — некоторые положительные константы.

Итеративное замыкание каждого из указанных в теореме базисов образует класс D.

[4] Здесь и далее $x' \sim x'' = x' \oplus x'' \oplus 1$.

В работе [33] рассматривались так называемые обобщённые ДНФ, а из полученных в ней результатов следует, в частности, что

$$L_{A_2}(n) = \Omega\left(\frac{2^n}{n^{1/4}}\right).$$

В теореме 6 получена асимптотика функции Шеннона для случая тех базисов A, для которых $\delta(A) \supseteq M$. Для некоторых классов таких базисов в следующих теоремах установлены асимптотические оценки высокой степени точности. Для каждого базиса A, $A \subseteq P_2(X \cup Y)$, обозначим через $\hat{A}$ множество тех элементов базиса A из множества A', которые либо имеют приведенный вес, равный ρ_A, либо входят в макроблоки этого базиса с приведенным весом ρ_A.

Теорема 8 ([22, 29]). *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис, такой, что $\delta(A) \supseteq M$. Пусть, далее, справедливо хотя бы одно из следующих утверждений:*

1. *$\delta(\hat{A}) \supseteq M$;*
2. *базис $\hat{A}$ является полным базисом;*
3. *$\delta(\hat{A}) \in \{L, D, K\}$, множество $[\hat{A}]_{\{1,3,4\}}$ содержит функцию f вида*

$$f = (\varphi_1 \circ y_1) \diamond \ldots \diamond (\varphi_k \circ y_k) \diamond \varphi_0,$$

где $\varphi_0, \varphi_1, \ldots, \varphi_k \in P_2(X)$, $(\circ, \diamond) \in \{(\&, \vee), (\vee, \&), (\&, \oplus)\}$, для которой найдутся такие индексы $j_1, j_2 \in \{1, \ldots, k\}$, $j_1 \neq j_2$, и наборы α, β значений прямых переменных, что

$$\varphi_{j_1}(\alpha) = \overline{\varphi_{j_1}(\beta)} = \varphi_{j_2}(\beta) = \overline{\varphi_{j_2}(\alpha)} = 0.$$

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

$$\mathcal{L}_A(n) = \rho_A \cdot \frac{2^n}{\log n}\left(1 \pm \frac{O(1)}{\log n}\right). \tag{4}$$

Следует отметить, что в случае 3 система $\hat{A}$ не обязательно является полной. Примером неполной системы $\hat{A}$, удовлетворяющей условиям пункта 3 теоремы, может служить базис

$$\hat{A} = \{x_1 y_1 \vee x_2 y_2\},$$

для которого $\delta(\hat{A}) = D$.

Теорема 8 остается справедливой, если в пункте 3 заменить множество $[\hat{A}]_{\{1,3,4\}}$ множеством $\hat{A}$. Однако, класс базисов при этом сужается. Например, каждый базис A, для которого

$$\hat{A} = \{y_1 \vee y_2, x_1 y_1\},$$

удовлетворяет условию этой теоремы, так как множество $[\hat{A}]_{\{1,3,4\}}$ содержит функцию $x_1 y_1 \vee x_2 y_2$, но при этом $x_1 y_1 \vee x_2 y_2 \notin \hat{A}$.

Другое поведение остаточного члена в оценках высокой степени точности для функции Шеннона сложности формул рассматриваемого класса демонстрирует следующая теорема. Итеративное замыкание приведённых в ней базисов равно $P_2(Y)$.

Теорема 9 ([22]). *Пусть*

$$Б_1 = \{y_1 \cdot \ldots \cdot y_{k_1}, x_1 \vee \ldots \vee x_{k_2}, \bar{y}_1\};$$

$$Б_2 = \{y_1 \vee \ldots \vee y_{k_1}, x_1 \cdot \ldots \cdot x_{k_2}, \bar{y}_1\};$$

где $k_1, k_2 \geqslant 2$. *Тогда для* $i = 1, 2$ *имеют место следующие неравенства:*

$$\rho_{Б_i} \frac{2^n}{\log n} \left(1 + \frac{\frac{1}{k_2} \log\log n \pm O(1)}{\log n}\right) \leqslant \mathcal{L}_{Б_i}(n) \leqslant \rho_{Б_i} \frac{2^n}{\log n} \left(1 + \frac{\log\log n \pm O(1)}{\log n}\right).$$

Если при этом минимальный приведенный вес базиса $Б_i$, $i \in \{1, 2\}$, *достигается на макроблоке, отличном от элемента, то справедливо соотношение:*

$$\mathcal{L}_{Б_i}(n) = \rho_{Б_i} \frac{2^n}{\log n} \left(1 + \frac{\frac{1}{k_2} \log\log n \pm O(1)}{\log n}\right).$$

Заметим, что для формул в «обычных» базисах оценка высокой степени точности для соответствующей функции Шеннона получена в [31] и имеет вид:

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

где ρ_A — минимальный приведенный вес элементов из A, а константа $\varkappa_A \in \{0, 1\}$ и зависит только от функций, реализуемых элементами с минимальным приведенным весом.

Результаты работы докладывались на следующих конференциях.

- XVI Международная конференция «Проблемы теоретической кибернетики» (Нижний Новгород, 2011),
- VIII Молодежная научная школа по дискретной математике и ее приложениям (Москва, 2011),
- IX Молодежная научная школа по дискретной математике и ее приложениям (Москва, 2013),
- XVII Международная конференция «Проблемы теоретической кибернетики» (Казань, 2014),
- IX Международная конференция «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, 2015).

Результаты диссертации изложены в 10 печатных изданиях [18–22, 26–30], из которых [18, 26–29] — в журналах из перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук.

Перечислим основные положения диссертации, выносимые на защиту.

1. Получены оценки высокой степени точности функции Шеннона для сложности формул в базисе $\{\&, \vee, \neg\}$ с ограниченной глубиной альтернирования.

2. Получена оценка высокой степени точности функции Шеннона для сложности реализации формулами глубины альтернирования 3 функций из классов, связанных с конечными грамматиками.

3. Получена асимптотика функции Шеннона для сложности формул в базисах из элементов с прямыми и итеративными входами, итеративное замыкание которых содержит класс монотонных функций. Выделен широкий класс базисов с прямыми и итеративными переменными, в котором для этой функции получены асимптотические оценки высокой степени точности.

4. Выявлены новые особенности задачи синтеза формул в базисах из элементов с прямыми и итеративными входами. Для каждого семейства базисов в их классификации по итеративным замыканиям, в котором поведение функции Шеннона не является «стандартным», приведены примеры базисов, где эта функция имеет «граничный» порядок роста 2^n.

Глава 1

Синтез формул с ограниченной глубиной альтернирования и схем из функциональных элементов ограниченной ширины

1.1 Формулы с ограниченной глубиной альтернирования

Вначале приведем некоторые вспомогательные утверждения и дадим определения, необходимые для доказательства основного результата данного раздела.

1.1.1 Вспомогательные определения и утверждения

Для обозначения характеристической функции множества наборов δ, $\delta \subseteq B^n$, от переменных $x_1, \ldots, x_n$, т. е. функции, равной 1 на множестве δ и равной 0 вне его, будем использовать запись χ_δ. Заметим, что характеристическая функция множества $B^n \setminus \{\alpha\}$, где $\alpha = (\alpha_1, \ldots, \alpha_n) \in B^n$, является элементарной дизъюнкцией ранга n от n переменных $x_1, \ldots, x_n$ и имеет вид $J_\alpha(x_1, \ldots, x_n) = x_1^{\overline{\alpha}_1} \vee \ldots \vee x_n^{\overline{\alpha}_n}$. Если D – разбиение конечного множества Y на непересекающиеся непустые подмножества $Y_1, \ldots, Y_d$, то величина

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

называется энтропией [31] разбиения D.

Пусть $\varphi(y_1, \ldots, y_N)$ – функция, существенно зависящая от всех своих переменных из множества $Y = \{y_1, \ldots, y_N\}$, а D – разбиение множества Y на компоненты $Y_1, \ldots, Y_d$. Разбиение D называется *селекторным* [31] для функции $\varphi(Y)$, если для каждого i, $i = 1, \ldots, d$, и для любой переменной y, $y \in Y_i$, найдутся константы $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_d$, такие, что при подстановке их вместо переменных из $Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_d$ соответственно, выполняется равенство $\varphi = y \oplus \alpha_i$, $\alpha_i \in \{0, 1\}$.

Множество функций G, $G \subseteq P_2(m)$, называется [32] *φ-универсальным множеством порядка m*, если любая функция g, $g \in P_2(m)$, может быть представлена в виде $g = \varphi(g_1, \ldots, g_N)$, где $g_i \in G$ для всех i, $i = 1, \ldots, N$. Справедливо следующее утверждение.

Лемма 1 ([31]). *Пусть D – селекторное разбиение множества переменных Y, $Y = \{y_1, \ldots, y_N\}$, функции $\varphi(Y)$ на d компонент. Тогда для любого натурального s, где $s > \log N$ и $N(s - H(D)) \geqslant 2^m$, можно построить φ-универсальное множество G порядка m, такое, что $|G| \leqslant 2^{s+2}$. При этом существует схема из функциональных элементов Σ в базисе $Б_0$, реализующая систему функций $\overrightarrow{G}$, такая, что $L(\Sigma) \leqslant |G| + O(d \cdot 2^{\frac{s}{2}+m})$.*

Множество наборов δ, $\delta \subseteq B^q$, будем называть *m-регулярным множеством наборов* [32] куба B^q, если $m < q$, $|\delta| = 2^m$, и все префиксы длины m наборов из δ различны. Пусть $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ – разбиение куба B^q на m-регулярные подмножества. Будем говорить, что разбиение Δ *моделирует* функции из множества G, $G \subseteq P_2(m)$, с помощью булевых переменных или их отрицаний тогда и только тогда, когда для любой функции g, $g \in G$, и для каждого i,

$i = 1, \ldots, 2^{q-m}$, существует переменная x_j, где $1 \leqslant j \leqslant q$, и константа σ, $\sigma \in B$, такие, что $g \equiv x_j^\sigma$ на компоненте δ_i. При этом компонента δ_i считается «хорошей» компонентой, если для каждой такой функции g указанное свойство выполняется при $\sigma = 1$. В противном случае соответствующую компоненту будем называть «плохой».

Лемма 2 ([32]). *Пусть $G \subseteq P_2(m)$ и $q \geqslant m + |G|$. Тогда существует разбиение Δ куба B^q на m-регулярные подмножества $\delta_1, \ldots, \delta_{2^{q-m}}$, моделирующее функции из G с помощью булевых переменных или их отрицаний.*

Далее буквой e здесь обозначается основание натурального логарифма, e_i – некоторые абсолютные константы.

Лемма 3 ([34]). *Для любого множества G_1, $G_1 \subseteq P_2(m)$, и любого q, $q \geqslant m + 3|G_1|$, существует разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q на m-регулярные подмножества, моделирующее все функции из G_1 с помощью булевых переменных или их отрицаний, и такое, что доля «плохих» компонент в нём не превосходит $(e_1)^{q-m}$, где $e_1 < 1$.*

Лемма 4. *Пусть $G \subseteq P_2(m)$, а схема Σ в базисе $Б_0$ реализует систему $\overrightarrow{G}$. Тогда существует m-регулярное разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q, где $q = m + L(\Sigma)$, моделирующее все функции из G с помощью булевых переменных или их отрицаний, такое, что характеристическая функция каждой компоненты может быть представлена в виде КНФ, сложность которой не превосходит $e_2 \cdot L(\Sigma)$.*

Доказательство. Введем произвольную монотонную нумерацию вершин схемы Σ числами отрезка $[1, q]$, где $q = m + L(\Sigma)$, при которой различные вершины имеют различные номера, номер начальной вершины любой дуги Σ меньше номера её конечной вершины, а входы $x_1, \ldots, x_m$ пронумерованы числами

$1, \ldots, m$ соответственно. Сопоставим вершине с номером i, $i \in [m+1, q]$, которая связана с k_i-входовым базисным элементом φ_i, $\varphi_i \in$ Б$_0$, переменную x_i и формулу

$$R_i = \left(x_i \sim \varphi_i(x_{j_1^{(i)}}, \ldots, x_{j_{k_i}^{(i)}}) \right),$$

где $j_1^{(i)}, \ldots, j_{k_i}^{(i)}$ – номера начальных вершин тех дуг Σ, которые входят в данную вершину.

Рассмотрим множество G', $G' \supseteq G$, состоящее из всех различных и отличных от переменных $x_1, \ldots, x_m$ функций, которые реализуются в вершинах схемы Σ. Построим по лемме 2 разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q, на компонентах которого моделируются функции из G', и заметим, что для характеристической функции χ_1 компоненты δ_1 выполняется равенство

$$\chi_1 = R_{m+1} \cdot \ldots \cdot R_q. \tag{1.1}$$

Действительно, пусть в вершине с номером i, $i \in [m+1, q]$, схемы Σ реализуется функция f_i, $f_i \in G'$. Индукцией по i, $i = m+1, \ldots, q$, нетрудно показать, что единственным решением уравнения

$$R_{m+1} \cdot \ldots \cdot R_i \equiv 1$$

относительно переменных $x_{m+1}, \ldots, x_i$ являются функции $f_{m+1}, \ldots, f_i$ соответственно. Следовательно, правая часть (1.1) обращается в 1 на наборе $(\alpha_1, \ldots, \alpha_q)$ значений переменных $x_1, \ldots, x_q$ тогда и только тогда, когда для каждого i, $i = m+1, \ldots, q$, выполняется равенство $\alpha_i = f_i(\alpha_1, \ldots, \alpha_m)$, т. е. тогда и только тогда, когда $\chi_1(\alpha_1, \ldots, \alpha_q) = 1$.

Искомая КНФ $\mathfrak{B}_1$ для функции χ_1 получается заменой в правой части (1.1) каждой формулы R_i, $i \in [m+1, q]$, её совершенной КНФ. Искомые КНФ для характеристических функций других компонент Δ получаются из $\mathfrak{B}_1$ в результате инвертирования некоторых переменных.

Лемма доказана. $\square$

Аналогично на основе леммы 3 можно доказать следующее утверждение.

Лемма 5. *Пусть $G \subseteq P_2(m)$, а схема из функциональных элементов Σ в базисе $Б_0$ реализует систему $\overrightarrow{G}$. Тогда существует m-регулярное разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q, где $q = m + 3L(\Sigma)$, моделирующее все функции из G с помощью булевых переменных или их отрицаний, такое, что доля «плохих» компонент в нём не превосходит $(e_3)^{q-m}$, где $e_3 < 1$, а характеристическая функция каждой компоненты может быть представлена в виде КНФ, сложность которой не превосходит $e_4 \cdot L(\Sigma)$.*

Лемма 6. *Пусть $\Delta = (Y_1, \ldots, Y_d)$ – разбиение множества Y, в котором первые k, $k \leqslant d$, компонент имеют мощность t, и пусть для каждого i, $i \in [1, k]$, $\delta_i = (X_1^i, \ldots, X_p^i)$ – разбиение множества Y_i, причем для каждого j, $j = 1, \ldots, p$, выполняются равенства*

$$|X_j^1| = |X_j^2| = \ldots = |X_j^k|.$$

Тогда для разбиения

$$D = (X_1, \ldots, X_p, Y_{k+1}, \ldots, Y_d)$$

множества Y, где

$$X_j = \bigcup_{i=1}^{k} X_j^i$$

при любом j, $j = 1, \ldots, p$, выполняется равенство

$$H(D) = H(\Delta) + \frac{tk}{|Y|}(H(\delta_i) - \log k). \tag{1.2}$$

Доказательство. По определению,

$$H(\delta_i) = -\sum_{j=1}^{p} \frac{|X_j^i|}{t} \log \frac{|X_j^i|}{t},$$

$$H(\Delta) = -\sum_{i=1}^{d} \frac{|Y_i|}{|Y|} \log \frac{|Y_i|}{|Y|} = -\frac{tk}{|Y|} \log \frac{t}{|Y|} - \sum_{i=k+1}^{d} \frac{|Y_i|}{|Y|} \log \frac{|Y_i|}{|Y|}.$$

Следовательно,

$$\begin{aligned}
H(D) &= -\sum_{j=1}^{p}\frac{|X_j|}{|Y|}\log\frac{|X_j|}{|Y|} - \sum_{i=k+1}^{d}\frac{|Y_i|}{|Y|}\log\frac{|Y_i|}{|Y|} = \\
&= -\frac{t}{|Y|}\sum_{j=1}^{p}\frac{|X_j|}{t}\log\frac{|X_j|}{t} - \frac{t}{|Y|}\log\frac{t}{|Y|}\sum_{j=1}^{p}\frac{|X_j|}{t} - \sum_{i=k+1}^{d}\frac{|Y_i|}{|Y|}\log\frac{|Y_i|}{|Y|} = \\
&= -\frac{tk}{|Y|}\sum_{j=1}^{p}\frac{|X_j^i|}{t}\left(\log\frac{|X_j^i|}{t} + \log k\right) - \frac{tk}{|Y|}\log\frac{t}{|Y|} - \sum_{i=k+1}^{d}\frac{|Y_i|}{|Y|}\log\frac{|Y_i|}{|Y|} = \\
&= \frac{tk}{|Y|}(H(\delta_i) - \log k) + H(\Delta).
\end{aligned}$$

Лемма доказана. □

Для любого натурального a определим величину W_a как наименьшее натуральное число x, при котором $\log^{[a]} x > 1$, т. е. $W_a = \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{a\ \text{раз}} + 1$. При этом положим $W_0 = 2$.

Лемма 7. *При любых натуральных a и x, где $x \geqslant W_{a+1}$, справедливо неравенство*

$$\max_{2\leqslant k\leqslant \frac{x}{W_a}} \frac{x^k}{k^k k!}\left(\frac{\log^{[a+1]} x}{\log^{[a]}\left(\frac{x}{k}\right)}\right)^x \leqslant (e_5)^x.$$

Доказательство. Полагая $\beta = \frac{x}{k}$ и учитывая то, что $k! > \left(\frac{k}{e}\right)^k$, получим

$$\frac{x^k}{k^k k!}\left(\frac{\log^{[a+1]} x}{\log^{[a]}\left(\frac{x}{k}\right)}\right)^x \leqslant \frac{x^k e^k}{k^{2k}}\left(\frac{\log^{[a+1]} x}{\log^{[a]}\left(\frac{x}{k}\right)}\right)^x = \beta^{\frac{x}{\beta}} e^{\frac{x}{\beta}}\left(\frac{x}{\beta}\right)^{-\frac{x}{\beta}}\left(\frac{\log^{[a+1]} x}{\log^{[a]}\beta}\right)^x.$$

Поделив на x натуральный логарифм последнего выражения, легко убедиться в том, что для доказательства леммы достаточно показать справедливость неравенства

$$\frac{2}{\beta}\ln\beta + \frac{1}{\beta} - \frac{1}{\beta}\ln x + \ln\log^{[a+1]} x - \ln\log^{[a]}\beta \leqslant \ln e_5. \tag{1.3}$$

Найдем максимум левой части (1.3) как функции от β. Если он достигается при $\beta = \beta'$, то из необходимого условия достижения максимума вытекает, что

$$-2\ln\beta' + 1 + \ln x - \frac{\beta'}{\left(\log^{[a]}\beta'\right)\left(\log^{[a-1]}\beta'\right)\ldots(\log\beta')\ln^a 2} = 0,$$

то есть

$$1 + \ln x = 2 \ln \beta' + \frac{\beta'}{\left(\log^{[a]} \beta'\right)\left(\log^{[a-1]} \beta'\right) \ldots (\log \beta') \ln^a 2} < 3\beta',$$

и, следовательно, $\beta' > \frac{1+\ln x}{3}$. Учитывая то, что

$$\frac{2}{\beta} \ln \beta \leqslant \frac{2}{e} < 1, \ \frac{1}{\beta} \leqslant 1, \ -\frac{1}{\beta} \ln x < 0,$$

а также то, что функция $\left(-\ln \log^{[a]} \beta\right)$ не возрастает, получаем, что максимум выражения в левой части (1.3) не больше чем

$$2 + \ln \log^{[a+1]} x - \ln \log^{[a]} \left(\frac{1+\ln x}{3}\right) \leqslant 3,$$

то есть неравенство (1.3) справедливо при $e_5 = e^3$.

Лемма доказана. $\square$

1.1.2 Верхняя оценка функции Шеннона

Запись $A^a_\&$ (соответственно $A^a_\vee$), $a \geqslant 1$, будем использовать для обозначения класса всех формул с глубиной альтернирования, не превосходящей a, и таких, что любая цепь максимальной длины заканчивается элементом $\&$ (соответственно $\vee$). Пусть, далее, $\mathcal{U}^\Phi$ – множество формул в базисе $\text{Б}_0 = \{\&, \vee, \neg\}$, а $\mathcal{U}^{\Phi,a}(L, n)$ – множество формул $\mathcal{F}$ из $\mathcal{U}^\Phi$, реализующих функции от n переменных, для которых $A(\mathcal{F}) \leqslant a$, $L(\mathcal{F}) \leqslant L$.

Сначала рассмотрим формулы специального вида из классов $A^a_\&$, $A^a_\vee$ и оценим энтропию некоторых селекторных разбиений переменных для реализуемых ими функций.

Лемма 8. *При любых натуральных a и N, где $a \geqslant 1$, $N \geqslant W_a$, существуют формулы $\mathcal{F}^a_\&(y_1, \ldots, y_N)$ и $\mathcal{F}^a_\vee(y_1, \ldots, y_N)$ сложности $N - 1$, принадлежащие классам $A^a_\&$ и $A^a_\vee$ соответственно, каждая из которых реализует функцию, имеющую селекторное разбиение D множества своих булевых переменных с энтропией $H(D) \leqslant \log^{[a]} N + C_a$, где C_a – число, зависящее только от a.*

Доказательство. Докажем существование искомых формул индукцией по a.

Если $a = 1$, то в качестве искомых формул возьмем формулы

$$\mathcal{F}_{\vee}^{1}(y_1, \ldots, y_N) = y_1 \vee \ldots \vee y_N, \ \mathcal{F}_{\&}^{1}(y_1, \ldots, y_N) = y_1 \cdot \ldots \cdot y_N,$$

а в качестве искомого разбиения D – тривиальное разбиение $(\{y_1\}, \ldots, \{y_N\})$.

Предположим, что лемма верна для значения глубины альтернирования, равного a, и построим искомую формулу $\mathcal{F}_{\vee}^{a+1}$. Представим число N в виде $N = p \cdot r + q$, где $p = \lceil \log N \rceil$ и $0 \leqslant q < p$. Положим

$$\begin{aligned}\mathcal{F}_{\vee}^{a+1}(y_1, \ldots, y_N) =& \mathcal{F}_{\&}^{a}(y_1, \ldots, y_{p-1}) \cdot y_p \vee \mathcal{F}_{\&}^{a}(y_{p+1}, \ldots, y_{2p-1}) \cdot y_{2p} \vee \ldots \vee \\ & \vee \mathcal{F}_{\&}^{a}(y_{p(r-1)+1}, \ldots, y_{pr-1}) \cdot y_{pr} \vee y_{pr+1} \cdot \ldots \cdot y_N,\end{aligned}$$

где $\mathcal{F}_{\&}^{a}$ – формула, построенная на предыдущем шаге индукции.

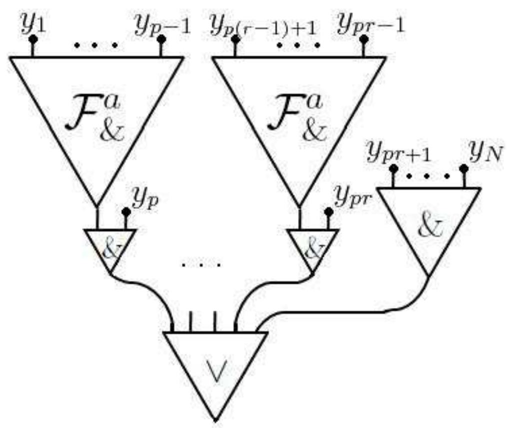

Рисунок 1.1: Дерево формулы $\mathcal{F}_{\vee}^{a+1}$

Заметим, что формула $\mathcal{F}_{\vee}^{a+1}$ (рис. 1.1) имеет сложность $(N-1)$, и рассмотрим разбиение

$$\Delta = \{Y_1, \ldots, Y_r, Y_{r+1}, \ldots, Y_{2r}, Y_{2r+1}, \ldots, Y_{N-pr+2r}\}$$

множества переменных $Y = \{y_1, \ldots, y_N\}$ такое, что

$$Y_i = \{y_{p(i-1)+1}, \ldots, y_{pi-1}\}, \quad Y_{r+i} = \{y_{pi}\}$$

для всех i, $i = 1, \ldots, r$, и

$$Y_i = \{y_{pr-2r+i}\}$$

для всех i, $i = 2r+1, \ldots, N - pr + 2r$.

Энтропия этого разбиения удовлетворяет соотношениям

$$H(\Delta) = \frac{r}{N}\log N + \frac{r(p-1)}{N}\log\frac{N}{p-1} + \frac{q}{N}\log N \leqslant$$
$$\leqslant \frac{r}{N}\log N + \frac{r(p-1)}{N}\log\frac{N}{p-1} + 1.$$

Пусть δ_i – разбиение множества переменных Y_i, $i = 1, \ldots, r$, которое совпадает с селекторным разбиением переменных функции, реализуемой формулой $\mathcal{F}^a_\&(y_{p(i-1)+1}, \ldots, y_{pi-1})$, построенным на предыдущем шаге индукции, и для которого $H(\delta_i) \leqslant \log^{[a]}(p-1) + C_a$. Тогда искомое разбиение D переменных функции, реализуемой формулой $\mathcal{F}^{a+1}_\vee(y_1, \ldots, y_N)$, строится по лемме 6, и, как нетрудно проверить, также является селекторным, а его энтропия, согласно (1.2), удовлетворяет соотношению:

$$H(D) = H(\Delta) + \frac{r(p-1)}{N}(H(\delta_i) - \log r) \leqslant$$
$$\leqslant \log^{[a]}(p-1) + C_a + 1 \leqslant \log^{[a+1]} N + C_{a+1}.$$

Остается заметить, что в качестве формулы $\mathcal{F}^{a+1}_\&$ достаточно взять формулу, двойственную к формуле $\mathcal{F}^{a+1}_\vee$.

Лемма доказана. $\square$

Теорема 10. *При любом a, $a \geqslant 3$, для любой функции f, $f \in P_2(n)$, существует формула $\mathcal{F}_f \in \mathcal{U}^{\Phi,a}$, реализующая эту функцию, такая, что*

$$L(\mathcal{F}_f) \leqslant \frac{2^n}{\log n}\left(1 + \frac{\log^{[a-1]} n + O(1)}{\log n}\right).$$

Доказательство. Пусть натуральные параметры m, q, t таковы, что

$$1 \leqslant m < q \text{ и } q + t \leqslant n,$$

и пусть $x' = (x_1, \ldots, x_q)$, $x'' = (x_{q+1}, \ldots, x_n)$, $\hat{x}' = (x_1, \ldots, x_m)$, $\check{x}' = (x_{m+1}, \ldots, x_q)$, $\hat{x}'' = (x_{q+1}, \ldots, x_{q+t})$, $\check{x}'' = (x_{q+t+1}, \ldots, x_n)$.

Пусть, далее, натуральные параметры s и N удовлетворяют неравенствам

$$s > \log N \text{ и } N(s - H(D)) \geqslant 2^m,$$

где D – селекторное разбиение переменных функции $\varphi(y_1, \ldots, y_N)$, реализуемой формулой $\mathcal{F}$ из класса $A_\vee^{a-2}$, построенной по лемме 8, которое состоит из d компонент и имеет энтропию $H(D) \leqslant \log^{[a-2]} N + C_a$.

Построим по лемме 1 φ-универсальное множество G', $G' \subseteq P_2(m)$, порядка m, такое, что $|G'| \leqslant 2^{s+2}$, и реализующую его схему Σ' сложности

$$L(\Sigma') \leqslant |G'| + O(d \cdot 2^{\frac{s}{2}+m}).$$

Положим $q = m + 3L(\Sigma')$, и в предположении, что $q < n$, по лемме 5 построим разбиение $\Delta' = (\delta'_1, \ldots, \delta'_{2^{q-m}})$ куба B^q на m-регулярные компоненты, в котором доля «плохих» компонент не превосходит e_3^{q-m}, где $e_3 < 1$, моделирующее функции из множества G' при помощи булевых переменных группы $\check{x}'$ или их отрицаний.

Заметим, что при любом i, $i \in [1, 2^{q-m}]$, любая функция $g(x')$ совпадает на множестве δ'_i в силу его m-регулярности с одной из функций от переменных $\hat{x}'$ и, следовательно, в силу φ-универсальности множества G' совпадает на δ'_i с суперпозицией вида $\varphi(g^{(1)}, \ldots, g^{(N)})$, внутренние функции которой принадлежат G'. Из построения разбиения Δ' следует, что указанная суперпозиция, в свою очередь, совпадает на δ'_i с формулой $\varphi(x_{j_1}^{\tau_1}, \ldots, x_{j_N}^{\tau_N})$, переменные которой берутся из набора $\check{x}'$ так, что $x_{j_v}^{\tau_v}$ моделирует на δ'_i функцию $g^{(v)}$ при всех v, $v \in [1, N]$. Таким образом, на множестве δ'_i выполняется равенство

$$g(x') = \mathcal{F}(x_{j_1}^{\tau_1}, \ldots, x_{j_N}^{\tau_N}), \tag{1.4}$$

причем $\tau_1 = \ldots = \tau_N = 1$, если δ'_i — «хорошая» компонента разбиения Δ'.

Пусть G'' – множество всех элементарных дизъюнкций ранга t от переменных $\hat{x}''$, а Σ'' – реализующая систему $\overrightarrow{G}''$ схема, для которой [32] $L(\Sigma'') \leqslant 2^{t+1}$.

В предположении, что $t + 2^{t+1} \leqslant n - q$, по лемме 4 построим разбиение $\Delta'' = (\delta''_1, \ldots, \delta''_{2^{n-q-t}})$ куба B^{n-q} на t-регулярные подмножества, моделирующее функции из множества G'' при помощи булевых переменных группы $\check{x}''$ или их отрицаний. Заметим, что при любом j, $j \in [1, 2^{n-q-t}]$, и любом σ'', $\sigma'' \in \delta''_j$, дизъюнкция $J_{\sigma''}(x'')$ в силу t-регулярности множества наборов δ''_j совпадает на нём с одной из функций множества G'' и, следовательно, совпадает на δ''_j с переменной или её отрицанием вида $x_{u_{\sigma''}}^{\gamma_{\sigma''}}$, где $u_{\sigma''} \in [q+t+1, n]$ и $\gamma_{\sigma''} \in \{0,1\}$.

Рассмотрим конъюнктивное разложение функции $f(x', x'')$ по переменным группы x'' и его последующую модификацию на основе разбиений Δ' и Δ'' вида

$$f(x', x'') = \mathop{\&}_{\sigma'' \in B^{n-q}} (J_{\sigma''}(x'') \vee f(x', \sigma'')) =$$
$$= \bigvee_{i=1}^{2^{q-m}} \bigvee_{j=1}^{2^{n-q-t}} \chi_{\delta'_i}(x') \chi_{\delta''_j}(x'') \mathop{\&}_{\sigma'' \in \delta''_j} \left(x_{u_{\sigma''}}^{\gamma_{\sigma''}} \vee g_{\sigma'',i}(x') \right),$$

где для каждого i, $i \in [1, 2^{q-m}]$, функция $g_{\sigma'',i}(x')$ реализуется формулой $\Phi_{\sigma'',i}(x')$, имеющей вид правой части (1.4) и построенной для функции $f(x', \sigma'')$. Искомой формулой является формула

$$\mathcal{F}_f = \bigvee_{i=1}^{2^{q-m}} \bigvee_{j=1}^{2^{n-q-t}} \mathfrak{B}_{\mathfrak{i}}(x') \mathfrak{B}_{\mathfrak{j}}(x'') \mathop{\&}_{\sigma'' \in \delta''_j} \left(x_{u_{\sigma''}}^{\gamma_{\sigma''}} \vee \Phi_{\sigma'',i}(x') \right),$$

где $\mathfrak{B}_{\mathfrak{i}}(x')$, $i \in [1, 2^{q-m}]$, и $\mathfrak{B}_{\mathfrak{j}}(x'')$, $j \in [1, 2^{n-q-t}]$, – КНФ, построенные по леммам 4 и 5 для функций $\chi_{\delta'_i}$ и $\chi_{\delta''_j}$ соответственно. Нетрудно видеть, что $A(\mathcal{F}_f) \leqslant a$.

Выберем значения параметров, удовлетворяющие всем введенным ограничениям, и оценим сложность построенной формулы $\mathcal{F}_f$. Положим

$$m = \lceil 2 \log \log n \rceil, \ \ s = \lceil \log n - 5 \rceil,$$

и пусть N – минимальное натуральное число, удовлетворяющее неравенству

$$N \geqslant \frac{2^m}{s - \log^{[a-2]} N - C_a},$$

которое, очевидно, асимптотически равно $2^m/s$, т. е. имеет порядок роста $\log n$, и для которого, поэтому, при достаточно больших n выполняется неравенство $s > \log N$. Заметим, что при этом

$$q = m + 3L(\Sigma') \leqslant m + 3 \cdot 2^{s+2} + O\left(d \cdot 2^{\frac{s}{2}+m}\right) \lesssim \frac{3}{4}n,$$

и положим

$$t = \lceil \log(n-q) \rceil - 2.$$

При выбранных значениях параметров выполнены все ограничения, и сложность формулы $\mathcal{F}_f$ удовлетворяет требованиям теоремы, т. е.

$$L(\mathcal{F}_f) \leqslant \frac{2^n}{\log n}\left(1 + \frac{\log^{[a-1]} n + O(1)}{\log n}\right),$$

так как

1. сложность реализации всех КНФ не превосходит
$$2^{n-m-t}(e_2 \cdot L(\Sigma') + e_4 \cdot L(\Sigma'')) = O\left(\frac{2^n}{\log^2 n}\right);$$

2. основная сложность формулы $\mathcal{F}_f$ – сложность реализации всех подформул вида $\left(x_{u_{\sigma''}}^{\gamma_{\sigma''}} \vee \Phi_{\sigma'',i}(x')\right)$ на «хороших» компонентах, – не превосходит величины
$$2^{n-m} \cdot (N+1) \leqslant \frac{2^n}{s - H(D)} + 2^{n-m},$$
где $H(D) \leqslant \log^{[a-1]} n + O(1)$;

3. сложность всех аналогичных подформул для «плохих» компонент не больше, чем
$$2^{n-m} \cdot e_3^{q-m} \cdot 2N = O\left(\frac{2^n}{\log^2 n}\right).$$

Теорема доказана. □

1.1.3 Нижняя мощностная оценка функции Шеннона

Перейдём теперь к получению нижней оценки для функции Шеннона в классе формул с ограниченной глубиной альтернирования. Обозначим число попарно неэквивалентных формул во множестве $\mathcal{U}$ через $\|\mathcal{U}\|$.

В этом параграфе обозначение $c^{[a]}$ или $c_i = c_i^{[a]}$ используется для записи констант, зависящих только от a.

Лемма 9. *Для любого натурального a при любых натуральных значениях n и L, таких, что*[1] $\log^*(L+1) \geqslant a$ *и* $\log^{[a-1]}(L+1) \leqslant n$, *справедлива оценка*

$$\|\mathcal{U}^{\Phi,a}(L,n)\| \leqslant \left(\frac{c^{[a]}n}{\log^{[a-1]}(L+1)}\right)^{L+1}.$$

Доказательство. При $a = 1$ утверждение леммы, очевидно, справедливо. Предположим, что оно выполняется при глубине альтернирования $(a-1)$, где $a \geqslant 2$, т. е.

$$\|\mathcal{U}^{\Phi,a-1}(L,n)\| \leqslant \left(\frac{c^{[a-1]}n}{\log^{[a-2]}(L+1)}\right)^{L+1},$$

если $L+1 \geqslant W_{a-2}$, и докажем его справедливость при значении глубины альтернирования, равном a.

Пусть $L \geqslant W_{a-1} - 1$, $\mathcal{F} \in \mathcal{U}^{\Phi,a}(L,n)$ и $A(\mathcal{F}) = a$. Из определения глубины альтернирования следует, что рассматриваемая формула $\mathcal{F}$ представляет собой либо формулу первого типа, которая имеет вид $\mathcal{F} = \overline{\mathcal{F}'}$, где $A(\mathcal{F}') = a-1$, либо формулу второго типа, которая имеет вид $\mathcal{F} = \mathcal{F}_1 \circ \ldots \circ \mathcal{F}_k$, где $k \geqslant 2$, $\circ \in \{\&, \vee\}$ и $\mathcal{F}_1, \ldots, \mathcal{F}_k \in \mathcal{U}^{\Phi,a-1}$, причем ни одна из формул $\mathcal{F}_1, \ldots, \mathcal{F}_k$ не является формулой вида $\mathcal{F}' \circ \mathcal{F}''$, хотя бы одна из них отлична от символа переменной или её отрицания, и хотя бы одна имеет глубину альтернирования $(a-1)$.

[1]Обозначение $\log^* x$ используется для итерационного логарифма, т. е. функции, равной 0, при $x \leqslant 1$, и $\log^*(\log x) + 1$ при $x > 1$.

Заметим, что число рассматриваемых попарно не эквивалентных формул $\mathcal{F}$ первого типа не больше, чем

$$\|\mathcal{U}^{\Phi,a-1}(L-1,n)\| \leqslant \left(\frac{c^{[a-1]}n}{\log^{[a-2]} L}\right)^{L}.$$

Докажем, что число рассматриваемых формул $\mathcal{F}$ второго типа не больше, чем

$$\left(\frac{c_0 n}{\log^{[a-1]}(L+1)}\right)^{L+1}.$$

Для $i = 1, \ldots, k$ положим $L(\mathcal{F}_i) = L_i$, и пусть

$$L_1 + \ldots + L_k = \widehat{L} = L - k + 1. \tag{1.5}$$

Заметим, что число различных упорядоченных наборов $\mathcal{L} = (L_1, \ldots, L_k)$, являющихся решениями уравнения (1.5), равно $\mathrm{C}_{\widehat{L}-1}^{k-1}$.

При оценке числа попарно не эквивалентных формул $\mathcal{F}$ второго типа выделим три случая.

Случай 1. Набор $\mathcal{L}$ принадлежит множеству $\widetilde{\mathcal{L}}_k$, состоящему из таких неупорядоченных наборов $(L_1, \ldots, L_k)$, для которых выполнено (1.5) и, кроме того, $L_1, \ldots, L_k \geqslant W_{a-2} - 1$. Пусть при этом набор $\mathcal{L} = (L_1, \ldots, L_k)$ состоит из s попарно различных чисел $l_1, \ldots, l_s$, где $l_1 < l_2 < \ldots < l_s$, встречающихся в нём с кратностями $t_1, \ldots, t_s$ соответственно, и пусть $t(\mathcal{L}) = (t_1, \ldots, t_s)$. Число способов выбрать t_i, $i = 1, \ldots, s$, главных подформул сложности l_i формулы $\mathcal{F}$ есть

$$\mathrm{C}^{\,t_i}_{\|\mathcal{U}^{\Phi,a-1}(l_i,n)\|} \leqslant \left(\frac{3}{t_i}\right)^{t_i} \left(\frac{c^{[a-1]}n}{\log^{[a-2]}(l_i+1)}\right)^{t_i(l_i+1)},$$

так как справедливо неравенство $\mathrm{C}_a^b \leqslant \left(\frac{3a}{b}\right)^b$. Таким образом, при фиксированных $k, L_1, \ldots, L_k$ формулу описанного вида можно выбрать не более, чем

$$\frac{3^{t_1+\ldots+t_s}}{t_1^{t_1} \ldots t_s^{t_s}} \cdot \frac{(c^{[a-1]}n)^{L+1}}{(\log^{[a-2]}(L_1+1))^{(L_1+1)} \cdots (\log^{[a-2]}(L_k+1))^{(L_k+1)}} \tag{1.6}$$

способами. Величину (1.6) обозначим $M_1(L,k,L_1,\dots,L_k,t_1,\dots,t_s)$. Из выпуклости функции действительного переменного $f(x)=x\ln(\log^{[a-2]}x)$ следует, что

$$M_1(L,k,L_1,\dots,L_k,t_1,\dots,t_s)\leqslant\frac{3^{t_1+\ldots+t_s}}{t_1^{t_1}\ldots t_s^{t_s}}\frac{(c^{[a-1]}n)^{L+1}}{\left(\log^{[a-2]}\left(\frac{L+1}{k}\right)\right)^{L+1}}.$$

Выражение в правой части последнего неравенства обозначим за $M_2(L,k,t_1,\dots,t_s)$.

Таким образом, число попарно не эквивалентных формул рассматриваемого вида не больше, чем

$$\sum_{2\leqslant k\leqslant\frac{L+1}{W_{a-2}}}\ \sum_{\substack{1\leqslant s\leqslant k,\\ t_1+\ldots+t_s=k}}\ \sum_{\substack{\mathcal{L}=(L_1,\dots,L_k)\in\widetilde{\mathcal{L}}_k:\\ t(\mathcal{L})=(t_1,\dots,t_s)}} M_1(L,k,L_1,\dots,L_k,t_1,\dots,t_s). \tag{1.7}$$

Заметим, что число различных упорядоченных наборов, получаемых перестановками элементов из $\mathcal{L}$ равно полиномиальному коэффициенту [52] $\frac{k!}{t_1!\cdot\ldots\cdot t_s!}$. С учетом этого, выражение (1.7) не превосходит

$$\sum_{2\leqslant k\leqslant\frac{L+1}{W_{a-2}}}\ \sum_{\substack{1\leqslant s\leqslant k,\\ t_1+\ldots+t_s=k}}\xi(t_1,\dots,t_s)\frac{t_1!\cdot\ldots\cdot t_s!}{k!}M_2(L,k,t_1,\dots,t_s), \tag{1.8}$$

где $\xi(t_1,\dots,t_s)$ – количество упорядоченных наборов $\mathcal{L}$, для которых выполнено (1.5) и таких, что $t(\mathcal{L})=(t_1,\dots,t_s)$. Так как

$$\frac{t_1!\cdot\ldots\cdot t_s!}{k!}M_2(L,k,t_1,\dots,t_s)\leqslant\frac{(3c^{[a-1]}n)^{L+1}}{k!\left(\log^{[a-2]}\left(\frac{L+1}{k}\right)\right)^{L+1}},$$

и, кроме того,

$$\sum_{\substack{1\leqslant s\leqslant k,\\ t_1+\ldots+t_s=k}}\xi(t_1,\dots,t_s)=\mathrm{C}_{\hat{L}-1}^{k-1}\leqslant\left(\frac{3L}{k}\right)^k,$$

то выражение (1.8) можно ограничить сверху величиной

$$L\cdot\max_{2\leqslant k\leqslant\frac{L+1}{W_{a-2}}}\frac{(9c^{[a-1]}n)^{L+1}(L+1)^k}{k!k^k\left(\log^{[a-2]}\left(\frac{L+1}{k}\right)\right)^{L+1}}\leqslant\left(\frac{c_1n}{\log^{[a-1]}(L+1)}\right)^{L+1},$$

где последнее неравенство справедливо в силу леммы 7.

Случай 2. Оценим число попарно не эквивалентных формул второго типа, для которых $L_i < W_{a-2} - 1$ при всех i, $i = 1, \ldots, k$. Тогда

$$L + 1 = (L_1 + 1) + \ldots + (L_k + 1) < k \cdot W_{a-2},$$

т. е. $\frac{L+1}{k} < W_{a-2}$. Заметим, что при любом допустимом L и любой глубине альтернирования a справедлива тривиальная оценка $\|\mathcal{U}^{\Phi,a}(L,n)\| \leqslant (e_7 \cdot n)^L$, следовательно, аналогично первому случаю получаем, что число формул такого вида не больше, чем

$$\max_{\frac{L+1}{W_{a-2}} < k \leqslant L+1} \frac{(L+1)^k (c_2 n)^{L+1}}{k^k k!}. \tag{1.9}$$

Заметим также, что

$$\frac{(L+1)^k}{k^k k!} < \frac{(W_{a-2})^k}{k!} < \frac{(eW_{a-2})^k}{k^k} < \frac{(eW_{a-2})^k}{\left(\frac{L+1}{W_{a-2}}\right)^{\left(\frac{L+1}{W_{a-2}}\right)}} < \frac{(c_3)^{L+1}}{(\log(L+1))^{L+1}}.$$

Поэтому выражение (1.9) не больше, чем

$$\left(\frac{c_4 n}{\log(L+1)}\right)^{L+1} \leqslant \left(\frac{c_4 n}{\log^{[a-1]}(L+1)}\right)^{L+1}.$$

Легко видеть, что указанный результат будет справедлив и в том случае, когда $L_i < \gamma$, при всех i, $i = 1, \ldots, k$, где γ – некоторая константа.

Случай 3. Оценим число попарно не эквивалентных формул второго типа, для которых $L_1, \ldots, L_q < W_{a-2} - 1$, $L_{q+1}, \ldots, L_k \geqslant W_{a-2} - 1$, где $q \in [1, k-1]$. Пусть $L' = L_1 + \ldots + L_q$, $L'' = L_{q+1} + \ldots + L_k$.

Если $L'' + k - q < W_{a-1}$, то, как и в случае 2 при $\gamma = W_{a-1}$, количество попарно не эквивалентных формул такого вида не превосходит $\left(\frac{c_4 n}{\log^{[a-1]}(L+1)}\right)^{L+1}$. Поэтому далее будем считать, что $L'' + k - q \geqslant W_{a-1}$. Каждая формула $\mathcal{F}$ указанного типа может быть представлена как $\mathcal{F} = \mathcal{F}' \circ \mathcal{F}''$, где $\mathcal{F}' = \mathcal{F}_1 \circ \ldots \circ \mathcal{F}_q$, $\mathcal{F}'' = \mathcal{F}_{q+1} \circ \ldots \circ \mathcal{F}_k$, а $\circ \in \{\&, \vee\}$. Число попарно не эквивалентных формул $\mathcal{F}$ такого вида, как показано в случаях 1 и 2, не превосходит

$$\left(\frac{c_5 n}{\log(L'+q)}\right)^{L'+q} \cdot \left(\frac{c_6 n}{\log^{[a-1]}(L''+k-q)}\right)^{L''+k-q} \leqslant \left(\frac{c_7 n}{\log^{[a-1]}(L+1)}\right)^{L+1}.$$

Лемма доказана. $\square$

Из леммы 9, учитывая, что для всех $a \geqslant 3$: $\|\mathcal{U}^{\Phi,a}(L^{(a)}(n), n)\| = 2^{2^n}$ и $L^{(a)}(n) \sim \frac{2^n}{\log n}$, следует нижняя оценка функции Шеннона $L^{(a)}(n)$:

Теорема 11. *Для всех a, $a \geqslant 3$, при достаточно больших n*

$$L^{(a)}(n) \geqslant \frac{2^n}{\log n}\left(1 + \frac{\log^{[a-1]} n - O(1)}{\log n}\right).$$

Из теорем 10 и 11 следует сформулированный во введении результат:

Теорема 1. *Для любого натурального числа a, $a \geqslant 3$, при растущем значении натурального аргумента n, $n \geqslant 2$, выполняется соотношение*

$$L^{(a)}(n) = \frac{2^n}{\log n}\left(1 + \frac{\log^{[a-1]} n \pm O(1)}{\log n}\right).$$

1.2 Реализация функций из некоторых классов, связанных с конечными грамматиками, формулами глубины альтернирования 3

В этом разделе исследуется сложность реализации булевых функций, связанных с конечными грамматиками, в классе формул с глубиной альтернирования 3. Для соответствующей функции Шеннона докажем асимптотические оценки высокой степени точности.

Теорема 2. *Пусть* Γ *— грамматика с конечным числом состояний, для которой мощность множества* $T_\Gamma(s)$ *растет экспоненциально с ростом* s, *а* σ_Γ, $\sigma_\Gamma \in (0,1]$, *— её мощностная константа. Тогда при растущем значении натурального аргумента* n, $n \geqslant 2$, *справедливо соотношение*

$$L_\Gamma(n) = \sigma_\Gamma \cdot \frac{2^n}{\log n}\left(1 + \frac{\log\log n \pm O(1)}{\log n}\right).$$

Доказательство. Зафиксируем произвольную грамматику Γ с конечным числом состояний, для которой мощность множества слов T_Γ длины s растет экспоненциально с ростом s, и пусть σ_Γ, $\sigma_\Gamma \in (0,1]$, — мощностная константа этой грамматики. Рассмотрим произвольную функцию f, $f \in Q_\Gamma(n)$. Для построения формулы $\mathcal{F}$, которая имеет глубину альтернирования 3 и реализует эту функцию со сложностью

$$L(\mathcal{F}) \leqslant \sigma_\Gamma \cdot \frac{2^n}{\log n}\left(1 + \frac{\log\log n + O(1)}{\log n}\right), \tag{1.10}$$

воспользуемся методом, предложенным в [44], с некоторыми модификациями.

Разобьем набор переменных $(x_1, \ldots, x_n)$ на группы

$$\tilde{x} = (x_1, \ldots, x_a),$$

$$\tilde{y} = (x_{a+1}, \ldots, x_{a+b}),$$

$$\tilde{z} = (x_{a+b+1}, \ldots, x_{a+b+c}),$$

$$\tilde{u} = (x_{a+b+c+1}, \ldots, x_{a+b+c+d}),$$

где $n = a + b + c + d$. Кроме того, будем считать, что $c = m + 3 \cdot 2^{m+1}$ для некоторого натурального m, и обозначим

$$\tilde{z}' = (x_{a+b+1}, \ldots, x_{a+b+m}),$$
$$\tilde{z}'' = (x_{a+b+m+1}, \ldots, x_{a+b+c}).$$

Пусть H' — множество всех элементарных конъюнкций ранга m от переменных $\tilde{z}'$, а Σ' — реализующая систему $\overrightarrow{H}'$ схема, для которой $L(\Sigma') \leqslant 2^{m+1}$ [32]. По лемме 5 построим разбиение $\Delta' = (\delta'_1, \ldots, \delta'_{2^{c-m}})$ куба B^c на m-регулярные подмножества, в котором доля «плохих» компонент не превосходит $(e_2)^{c-m}$, $e_2 < 1$, и которое моделирует функции из множества H' при помощи булевых переменных группы $\tilde{z}''$ или их отрицаний. Заметим, что при любом i, $1 \leqslant i \leqslant 2^{c-m}$, и любом $\tilde{\alpha}$, $\tilde{\alpha} \in \delta'_i$, конъюнкция $K_{\tilde{\alpha}}(\tilde{z})$ в силу m-регулярности множества наборов δ'_i совпадает на этом множестве с одной из функций множества H' и, следовательно, совпадает с переменной или её отрицанием вида $x_{v_{\tilde{\alpha}}}^{\gamma_{\tilde{\alpha}}}$, где $\gamma_{\tilde{\alpha}} \in B$ и $a + b + c + m + 1 \leqslant v_{\tilde{\alpha}} \leqslant a + b + c$.

Функцию $f_{i,\tilde{\sigma},\tilde{\rho}}(\tilde{z}, \tilde{u})$, где $\tilde{\sigma} \in B^a$, $\tilde{\rho} \in B^b$, $1 \leqslant i \leqslant 2^{c-m}$, совпадающую с функцией $f(\tilde{\sigma}, \tilde{\rho}, \tilde{z}, \tilde{u})$ на наборах значений переменных, у которых значения группы $\tilde{z}$ принадлежат i-й компоненте разбиения Δ', и равную 0 на остальных наборах, зададим булевой матрицей M размера $2^d \times 2^m$. Строки этой матрицы соответствуют наборам значений переменных группы $\tilde{u}$, а столбцы — наборам компоненты δ'_i. Разобьем строки матрицы M на N полос, каждая из которых содержит по s строк (последняя может содержать менее s строк). Очевидно, что

$$1 \leqslant N \leqslant \frac{2^d}{s} + 1.$$

Столбцы матрицы, соответствующей функции $f_{i,\tilde{\sigma},\tilde{\rho},k}$, совпадающей на k-й полосе ($1 \leqslant k \leqslant N$) с $f_{i,\tilde{\sigma},\tilde{\rho}}$ и равной 0 вне её, разбиваются на группы совпадающих между собой столбцов. Пусть $f_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}$ — функция, совпадающая с $f_{i,\tilde{\sigma},\tilde{\rho},k}$ на группе $I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}$ столбцов, равных $\tilde{\tau}$ в k-й полосе, и принимающая значение

0 в остальных случаях. Заметим, что $\tilde{\tau}$ принимает не более $2^{\sigma_\Gamma \cdot s+O(1)}$ различных значений. Функция $f_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}$ может быть представлена в виде произведения функции $f^{(1)}_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}$, равной 1 на столбцах из $I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}$ и 0 на остальных столбцах, и функции $f^{(2)}_{k,\tilde{\tau}}$, в матрице которой все столбцы равны $\tilde{\tau}$ в k-й полосе и нулю вне этой полосы. Первая из этих функций может быть задана следующим образом:

$$f^{(1)}_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}(\tilde{z}) = \chi_{\delta'_i}(\tilde{z}) \cdot \bigvee_{\tilde{\alpha}\in I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}} K_{\tilde{\alpha}}(\tilde{z}) = \chi_{\delta'_i}(\tilde{z}) \cdot \bigvee_{\tilde{\alpha}\in I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}} x^{\gamma_{\tilde{\alpha}}}_{v_{\tilde{\alpha}}}, \tag{1.11}$$

где дизъюнкция берется по всем наборам $\tilde{\alpha}$ компоненты δ'_i, соответствующим столбцам из I.

Заметим, что суммарное (для всех $\tilde{\tau}$) число дизъюнктируемых переменных и отрицаний переменных равно числу наборов в компоненте δ'_i, т. е. 2^m.

Рассмотрим разложение функции f по переменным групп $\tilde{x}, \tilde{y}$ и его последующую модификацию на основе разбиения Δ' вида

$$\begin{aligned} f(\tilde{x},\tilde{y},\tilde{z},\tilde{u}) &= \bigvee_{\tilde{\sigma}\in B^a} \bigvee_{\tilde{\rho}\in B^b} K_{\tilde{\sigma}}(\tilde{x}) K_{\tilde{\rho}}(\tilde{y}) f(\tilde{\sigma},\tilde{\rho},\tilde{x},\tilde{y}) = \\ &= \bigvee_{i=1}^{2^{c-m}} \bigvee_{\tilde{\sigma}\in B^a} \bigvee_{\tilde{\rho}\in B^b} \bigvee_{k=1}^{N} \bigvee_{\tilde{\tau}} K_{\tilde{\sigma}}(\tilde{x}) K_{\tilde{\rho}}(\tilde{y}) \chi_{\delta'_i}(\tilde{z}) f^{(2)}_{k,\tilde{\tau}}(\tilde{u}) \left(\bigvee_{\tilde{\alpha}\in I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}} K_{\tilde{\alpha}}(\tilde{z}) \right). \end{aligned} \tag{1.12}$$

С учетом (1.11) и того, что

$$\bigvee_{\tilde{\rho}\in B^b} K_{\tilde{\rho}}(\tilde{y}) \left(\bigvee_{\tilde{\alpha}\in I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}} K_{\tilde{\alpha}}(\tilde{z}) \right) = \bigwedge_{\tilde{\rho}\in B^b} \left(J_{\tilde{\rho}}(\tilde{y}) \vee \bigvee_{\tilde{\alpha}\in I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}} K_{\tilde{\alpha}}(\tilde{z}) \right),$$

преобразуем представление (1.12) и получим следующую формулу для функции f:

$$\mathcal{F}_1 = \bigvee_{i=1}^{2^{c-m}} \bigvee_{\tilde{\sigma}\in B^a} \bigvee_{k=1}^{N} \bigvee_{\tilde{\tau}} K_{\tilde{\sigma}}(\tilde{x}) \mathfrak{B}'_i(\tilde{z}) F^{(2)}_{k,\tilde{\tau}}(\tilde{u}) \left(\bigwedge_{\tilde{\rho}\in B^b} \left(J_{\tilde{\rho}}(\tilde{y}) \vee \bigvee_{\tilde{\alpha}\in I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}} x^{\gamma_{\tilde{\alpha}}}_{v_{\tilde{\alpha}}} \right) \right),$$

где формула $F^{(2)}_{k,\tilde{\tau}}(\tilde{u})$ — совершенная КНФ функции $f^{(2)}_{k,\tilde{\tau}}(\tilde{u})$, а формула $\mathfrak{B}'_i(\tilde{z})$ — КНФ, построенная по лемме 5 для функции $\chi_{\delta'_i}(\tilde{z})$. Нетрудно видеть, что глубина альтернирования формулы $\mathcal{F}_1$ равна 3.

Положим $b = t + 2^{t+1}$ для некоторого натурального параметра t. Произведем дополнительно разбиение переменных группы $\tilde{y}$ на $\tilde{y}' = (x_{a+1}, \ldots, x_{a+t})$ и $\tilde{y}'' = (x_{a+t+1}, \ldots, x_{a+b})$.

Пусть H'' — множество всех элементарных дизъюнкций ранга t от переменных $\tilde{y}'$. Сложность реализации системы $\overrightarrow{H}''$ в классе схем из функциональных элементов не превосходит 2^{t+1} [32]. По лемме 4 построим разбиение $\Delta'' = (\delta''_1, \ldots, \delta''_{2^{b-t}})$ куба B^b на t-регулярные подмножества, моделирующее функции из множества H'' с помощью переменных из $\tilde{y}''$ или их отрицаний. При любом j, $1 \leqslant j \leqslant 2^{b-t}$, и любом $\tilde{\rho}$, $\tilde{\rho} \in \delta''_j$, дизъюнкция $J_{\tilde{\rho}}(\tilde{y})$ в силу t-регулярности множества наборов δ''_j совпадает на этом множестве с одной из функций множества H'' и, следовательно, с одной из переменных $\tilde{y}''$ или её отрицанием вида $x^{\beta_{\tilde{\rho}}}_{w_{\tilde{\rho}}}$, где $a + t + 1 \leqslant w_{\tilde{\rho}} \leqslant a + b$ и $\beta_{\tilde{\rho}} \in B$. Тогда, модифицируя формулу $\mathcal{F}_1$, представим функцию f в виде формулы

$$\mathcal{F} = \bigvee_{i=1}^{2^{c-m}} \bigvee_{j=1}^{2^{b-t}} \bigvee_{\tilde{\sigma}\in B^a} \bigvee_{k=1}^{N} \bigvee_{\tilde{\tau}} K_{\tilde{\sigma}}(\tilde{x})\mathfrak{B}'_i(\tilde{z})\mathfrak{B}''_j(\tilde{y})F^{(2)}_{k,\tilde{\tau}}(\tilde{u}) \left(\bigwedge_{\tilde{\rho}\in B^b} \left(x^{\beta_{\tilde{\rho}}}_{w_{\tilde{\rho}}} \vee \bigvee_{\tilde{\alpha}\in I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}} x^{\gamma_{\tilde{\alpha}}}_{v_{\tilde{\alpha}}} \right) \right),$$

где $\mathfrak{B}''_j(\tilde{y})$, $1 \leqslant j \leqslant 2^{b-t}$, — КНФ, построенная по лемме 1 для функции $\chi_{\delta''_j}(\tilde{y})$. При этом $A(\mathcal{F}) = 3$.

Выберем значения параметров, удовлетворяющие всем введенным ограничениям, и оценим сложность построенной формулы $\mathcal{F}$. Положим

$$m = \lfloor \log n \rfloor - 5,$$

$$t = \lfloor \log n \rfloor - 3,$$

$$d = \lfloor 2 \log\log n \rfloor,$$

$$s = \left\lfloor \frac{1}{\sigma_\Gamma} (\log n - \log\log n) \right\rfloor.$$

При таких значениях параметров сложность формулы $\mathcal{F}$ удовлетворяет неравенству (1.10), так как

1) каждый множитель вида $K_{\tilde{\sigma}}(\tilde{x})\mathfrak{B}'_i(\tilde{z})\mathfrak{B}''_j(\tilde{y})F^{(2)}_{k,\tilde{\tau}}(\tilde{u})$ имеет сложность $O\left(a+2^m+d2^d+2^t\right)=O(n)$, а суммарная сложность множителей такого вида есть

$$O\left(2^{c-m}\cdot 2^{b-t}\cdot 2^a\cdot\frac{2^d}{s}\cdot 2^s\cdot n\right)=O\left(\frac{2^{n-m-t+s}}{s}\cdot n\right)=O\left(\frac{2^n}{\log^2 n}\right);$$

2) число букв вида $x^{\beta_{\tilde{\rho}}}_{w_{\tilde{\rho}}}$ есть

$$O\left(2^{c-m}\cdot 2^{b-t}\cdot 2^a\cdot\frac{2^d}{s}\cdot 2^s\cdot 2^t\right)=O\left(\frac{2^n}{\log^2 n}\right);$$

3) основная сложность формулы $\mathcal{F}$ — сложность реализации всех подформул вида $\bigvee\limits_{\tilde{\alpha}\in I_{i,\tilde{\sigma},\tilde{\rho},k,\tilde{\tau}}} x^{\gamma_{\tilde{\alpha}}}_{v_{\tilde{\alpha}}}$ на «хороших» компонентах разбиения Δ', — не превосходит величины

$$2^{c-m}\cdot 2^{b-t}\cdot 2^a\cdot\left(\frac{2^d}{s}+1\right)\cdot 2^t\cdot 2^m=\frac{2^n}{s}+2^{n-d}=\frac{\sigma_\Gamma\cdot 2^n}{\lfloor\log n-\log\log n\rfloor}+O\left(\frac{2^n}{\log^2 n}\right);$$

4) сложность аналогичных подформул для «плохих» компонент не более

$$\frac{2^{n+1}}{s}\cdot(e_2)^{c-m}=O\left(\frac{2^n}{\log^2 n}\right).$$

Таким образом, верхняя оценка теоремы 2 доказана.

Для доказательства нижней оценки воспользуемся леммой 9 и равенством (1). В силу неравенства

$$\|\mathcal{U}^{\Phi,a}(L_\Gamma(n),n)\|\geqslant|Q_\Gamma(n)|=2^{\sigma_\Gamma\cdot 2^n+O(1)}$$

получаем, что при достаточно больших n

$$L_\Gamma(n)\geqslant\sigma_\Gamma\cdot\frac{2^n}{\log n}\left(1+\frac{\log\log n-O(1)}{\log n}\right).$$

Теорема 2 доказана. $\square$

1.3 Схемы с ограниченной памятью

Во введении было определено понятие схем ограниченной ширины — это схемы из функциональных элементов с ограничением на число одновременно запоминаемых результатов вычисления. Схемы ширины 1 во многих базисах не обладают полнотой в том смысле, что не каждую функцию можно реализовать в классе таких схем. Однако, при переходе к ограничению числа регистров до двух, возникает больше свободы при построении схем. Например, в стандартном базисе Б$_0$ можно реализовать любую функцию алгебры логики схемой, ширина которой не превосходит 2. Для этого достаточно построить совершенную ДНФ заданной функции и воспользоваться тем, что любая элементарная конъюнкция может быть представлена в виде $\bar{x}_{i_1}\ldots\bar{x}_{i_k}x_{j_1}\ldots x_{j_n} = \overline{(x_{i_1}\vee\ldots\vee x_{i_k})}x_{j_1}\ldots x_{j_n}$, что позволяет реализовать её в виде линейной суперпозиции.

Отметим связь формул с ограниченной глубиной альтернирования со схемами ограниченной ширины. Рассмотрим формулу $\mathcal{F}$ в базисе Б$_0$, реализующую некоторую функцию f, глубина альтернирования $A(\mathcal{F})$ которой равна a, $a \geqslant 1$. Покажем, что существует схема Σ в стандартном базисе, реализующая функцию f со сложностью не большей, чем $L(\mathcal{F})$, и имеющая ширину не большую, чем a. Действительно, если $a = 1$, то $\mathcal{F}$ – элементарная конъюнкция или элементарная дизъюнкция, и может быть реализована с той же сложностью схемой с одним регистром. Пусть $a > 1$, тогда формула $\mathcal{F}$ либо имеет вид $\overline{\mathcal{F}_1}$, где $A(\mathcal{F}_1) \leqslant a-1$, либо имеет вид $\mathcal{F} = \mathcal{F}_1\circ\ldots\circ\mathcal{F}_k$, где $\circ \in \{\&, \vee\}$, $k \geqslant 2$, и ни одна из формул $\mathcal{F}_i$ не представима в виде $\mathcal{F}'\circ\mathcal{F}''$, $i = 1,\ldots,k$, и хотя бы одна из них отлична от переменной и отрицания переменной. Тогда, если каждую главную подформулу заменить соответствующей схемой с $(a-1)$ регистрами, а внешнюю операцию $\circ$ выполнять на отдельном регистре r_a, то можно получить схему с a регистрами, вычисляющую функцию, реализуемую формулой $\mathcal{F}$.

Таким образом, сложностная функция Шеннона для класса схем ширины t не превосходит функции Шеннона для класса формул глубины альтернирования t. Из этого, с учетом тривиальной мощностной нижней оценки, вытекает справедливость следующих оценок для функции Шеннона сложности схем с t регистрами:

Утверждение. *Для любого натурального t, $t \geqslant 3$, при растущем значении натурального аргумента n, $n \geqslant 2$, выполняется соотношение*

$$\frac{2^n}{\log n}\left(1 - O\left(\frac{1}{\log n}\right)\right) \leqslant L^{\{t\}}(n) \leqslant \frac{2^n}{\log n}\left(1 + \frac{\log^{[t-1]} n + O(1)}{\log n}\right).$$

В этом параграфе будут рассмотрены некоторые свойства схем ширины 2 и 3 в стандартном базисе. Также будет показано существование формул, имеющих глубину альтернирования a, $a \geqslant 2$, и являющихся минимальными для реализуемых ими функций, для которых существуют эквивалентные им схемы ширины строго меньшей, чем a, и имеющие сложность, не превосходящую сложности исходных формул.

Покажем, что линейная функция $l_n = x_1 \oplus \ldots \oplus x_n$ и её отрицание $\bar{l}_n = x_1 \oplus \ldots \oplus x_n \oplus 1$ в классе схем ширины 2 в стандартном базисе допускает оптимальную реализацию.

Лемма 10. *Для любого натурального n, $n \geqslant 2$, справедливо соотношение:*

$$L^{\{2\}}(l_n) = L^{\{2\}}(\bar{l}_n) = 4n - 4.$$

Нижняя оценка следует из нижней оценки в классе схем без ограничений [49]. Верхняя оценка доказывается построением искомых оптимальных схем. На рис. 1.2 приведен сумматор порядка 2 с распределением регистров и нумерацией вершин. Используя суперпозицию таких блоков (и аналогичных для $\bar{l}_n$), естественным образом строятся схемы для линейных функций с указанной сложностью.

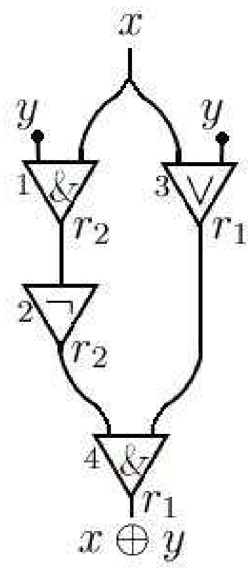

Рисунок 1.2: Основной блок для l_n.

Рассмотрим теперь монотонную симметрическую функцию с порогом 2:

$$s_n(x_1, \ldots, x_n) = \bigvee_{1 \leqslant i < j \leqslant n} x_i x_j.$$

Лемма 11. *При $n \to \infty$ справедлива следующая оценка*

$$L^{\{2\}}(s_n) \lesssim n \log n.$$

Как следует из работы [24], существует формула в базисе $\{\&, \vee\}$ вида

$$\mathcal{F}(x_1, \ldots, x_n) = \bigvee_{i=1}^{t} \left(\bigvee_{x' \in X_i'} x' \right) \left(\bigvee_{x'' \in X_i''} x'' \right), \tag{1.13}$$

реализующая функцию s_n, и имеющая сложность, асимптотически равную $n \log n$. В этой формуле X_i' и X_i'' – некоторые непустые непересекающиеся подмножества множества переменных $\{x_1, \ldots, x_n\}$.

Функция $y \vee J_1(x) J_2(x)$, где $J_1(x) = x_{i_1} \vee x_{i_2} \vee \ldots \vee x_{i_k}$, $J_2(x) = x_{j_1} \vee x_{j_2} \vee \ldots \vee x_{j_l}$ – дизъюнкции некоторых переменных из $\{x_1, \ldots, x_n\}$, может быть реализована схемой ширины 2. Действительно, так как $y \vee J_1(x) J_2(x) = (y \vee J_1(x))(y \vee J_2(x))$, то схема, показанная на рис. 1.3, её реализует.

С использованием t таких блоков строится искомая схема Σ ширины 2 по формуле $\mathcal{F}$. При этом $L(\Sigma) \leqslant L(\mathcal{F}) + t$, а $t \leqslant n$, поэтому утверждение доказано.

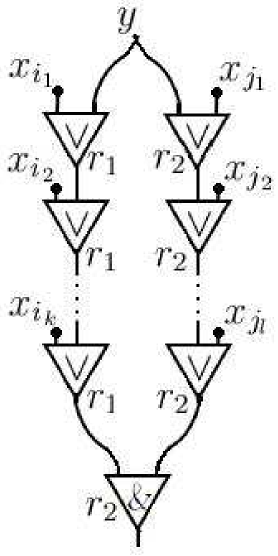

Рисунок 1.3: Блок ширины 2 для функции s_n.

Следует отметить, что формула (1.13) имеет глубину альтернирования, равную 3, но при этом реализуемая ею функция s_n допускает вычисление схемой с двумя регистрами, имеющей сложность не большую, чем сложность исходной формулы.

Лемма 12. *Для любого натурального* n, $n \geqslant 2$, *справедлива оценка:*

$$L^{\{3\}}(s_n) \leqslant 3n - 5.$$

Доказательство. Для доказательства построим схему с тремя регистрами r_1, r_2, r_3, реализующую функцию s_n. Рассмотрим вычисление, реализуемое схемой.

Пусть $n > 2$, $i \in \{1, \ldots, n-1\}$, и в регистрах r_1 и r_2 записаны значения функций s_i и $(x_1 \vee \ldots \vee x_{i-1})$ соответственно. Тогда сначала вычислим значение $(x_1 \vee \ldots \vee x_{i-1} \vee x_i)$, записав его в r_2, затем вычислим $(x_1 \vee \ldots \vee x_i)x_{i+1}$, поместив в r_3, и затем запишем в r_1 дизъюнкцию результатов на r_1 и r_3, получив тем самым s_{i+1}. Заметим, что теперь в r_1 и r_2 находятся значения выражений s_{i+1} и $(x_1 \vee \ldots \vee x_i)$. Таким образом, за три шага вычисления, потратив три функциональных элемента, можно осуществить переход от s_i к s_{i+1}.

С учётом сказанного и того, что функция $s_2 = x_1 x_2$ реализуется схемой ширины 1, получаем, что для функции s_n достаточно $3(n-2)+1 = 3n-5$ функциональных элементов. При $n = 2$ оценка остается справедливой. $\square$

Заметим, что конструкция, предложенная в работе [12], не может быть использована для построения линейной по сложности схемы константной ширины.

Леммы 10–12 доказывают следующий результат.

Теорема 3. *Для любого натурального n, $n \geqslant 2$, справедливы следующие соотношения:*

$$L^{\{2\}}(l_n) = L^{\{2\}}(\bar{l}_n) = 4n - 4;$$

$$L^{\{3\}}(s_n) \leqslant 3n - 5.$$

При $n \to \infty$ справедлива оценка:

$$L^{\{2\}}(s_n) \lesssim n \log n.$$

Рассмотрим систему (2) функций Q_n, состоящую из всех элементарных конъюнкций ранга n от n переменных. Как уже было сказано, его сложность в классе схем из функциональных элементов в стандартном базисе без ограничений асимптотически равна 2^n. Однако, асимптотически оптимальная схема для него, строящаяся [8] из двух дешифраторов порядка $n/2$, требует для вычислений растущее с ростом n число регистров. Докажем оценки сложности дешифратора в классе схем ширины 2 и 3.

Теорема 4. *При $n \to \infty$ справедливы следующие оценки:*

$$L^{\{3\}}(\overrightarrow{Q}_n) \sim 2^n,$$

$$L^{\{2\}}(\overrightarrow{Q}_n) = \Theta(2^n).$$

Доказательство. В силу того, что любая схема, реализующая дешифратор, имеет 2^n выходов, достаточно доказать только верхние оценки.

Пусть натуральные параметры m и q таковы, что

$$1 \leqslant m < q < n,$$

и пусть $x' = (x_1, \ldots, x_q)$, а $x'' = (x_{q+1}, \ldots, x_n)$. Пусть $G = Q_m \cup \{0\}$, а $q = m + 3L(G)$, где $L(G)$ – сложность реализации системы G в классе схем без ограничений. Построим по лемме 5 разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q на m-регулярные компоненты, в котором доля «плохих» компонент не превосходит e_3^{q-m}, где $e_3 < 1$, моделирующее все функции из множества G при помощи булевых переменных группы $(x_{m+1}, \ldots, x_q)$ или их отрицаний.

Заметим, что при любом i, $i = 1, \ldots, 2^{q-m}$, каждая элементарная конъюнкция $K_{\sigma'}(x') = x_1^{\sigma_1} \ldots x_q^{\sigma_q}$ совпадает на множестве δ_i либо с элементарной конъюнкцией ранга m, либо с функцией 0, а, следовательно, по построению Δ, совпадает с некоторой переменной $x_{\sigma',i}$ из группы $(x_{m+1}, \ldots, x_q)$ или её отрицанием.

Таким образом, любая элементарная конъюнкция $K_\sigma(x)$ представима в виде:

$$K_\sigma(x) = K_{\sigma'}(x') \cdot K_{\sigma''}(x'') = \chi_i(x') \cdot x_{\sigma',i} \cdot K_{\sigma''}(x''), \tag{1.14}$$

где i – номер компоненты разбиения Δ, в которой содержится набор σ, обращающий данную конъюнкцию в единицу. Используем данное представление для реализации дешифратора в схемах с двумя и тремя регистрами.

1. Схемы ширины 3. Для каждого i, $i = 1, \ldots, 2^{q-m}$, будем строить следующую подсхему. Первые по нумерации в этой подсхеме элементы будут вычислять характеристическую функцию $\chi_i(x')$ в соответствии с КНФ, построенной по лемме 5. Для этого необходимы два регистра. Пусть результат этого вычисления записан в регистр r_1. Далее последовательно производятся следующие вычисления: в регистре r_2 вычисляется очередная элементарная конъюнкция $K_{\sigma''}(x'')$, находится результат произведения значений на

регистрах r_1 и r_2, записывается в r_2, затем этот результат последовательно домножается на переменные типа $x_{\sigma',i}$ или их отрицания с помощью регистра r_3, как это показано на рис. 1.4.

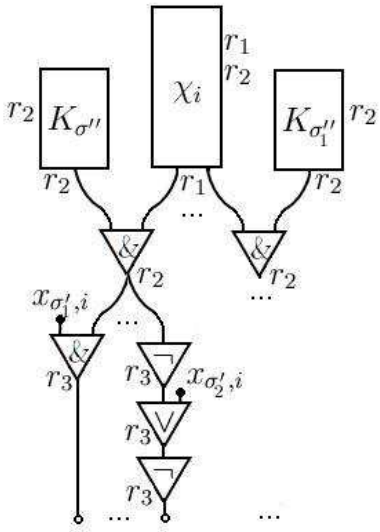

Рисунок 1.4: Подсхема для реализации Q_n.

Оценим сложность схемы. В каждом блоке сложность характеристической функции, согласно лемме 5, не превосходит $c \cdot L(G) \leqslant c' \cdot 2^m$, где c и c' – некоторые положительные константы. Кроме того, каждая конъюнкция типа $K_{\sigma''}(x'')$ от $(n-q)$ переменных реализуется схемой сложности $(n-q)$. Блок имеет 2^{n-q+m} выходов, поэтому сложность последних домножений, с учетом того, что доля «плохих» компонент не более, чем e_3^{q-m}, $e_3 < 1$, равна $2^{n-q+m}\left((1-e_3^{q-m}) + 3 \cdot e_3^{q-m}\right)$. Таким образом, сложность всей схемы, построенной из 2^{q-m} таких блоков, равна

$$2^{q-m}\left(c'2^m + (n-q)2^{n-q} + 2^{n-q+m}\left((1-e_3^{q-m}) + 3 \cdot e_3^{q-m}\right)\right) \sim 2^n,$$

при $n - q = \lfloor \log n \rfloor$.

2. Схемы ширины 2. В этом случае разрешено использовать только два регистра, поэтому использование конструкции, предложенной в предыдущем пункте, невозможно. Будем использовать аналогичное разложение (1.14),

но новый блок схемы будет реализовывать все элементарные конъюнкции $K_\sigma(x)$, имеющие общую компоненту разбиения Δ (содержащую набор, обращающий их в единицу) и общую импликанту ранга $n-q$ от переменных группы x'' (рис. 1.5).

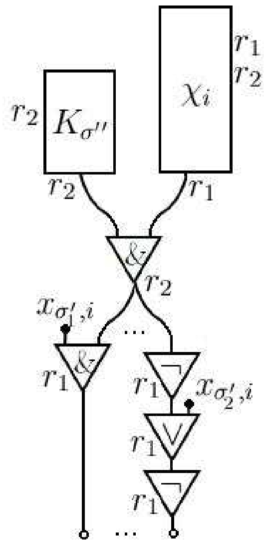

Рисунок 1.5: Подсхема для реализации Q_n.

Число таких блоков во всей схеме равно $2^{q-m}2^{n-q} = 2^{n-m}$, сложность каждого блока составляют: реализация $\chi_i(x')$ по КНФ со сложностью не большей, чем $c''2^m$, где $c'' = \mathrm{const}$, реализация $K_{\sigma''}$ со сложностью $n-q$, и реализация моделирования переменными. Аналогично предыдущему пункту, имеем следующую оценку сложности для всей схемы:

$$2^{n-m}\left(c''2^m + (n-q)\right) + 2^n\big((e_3)^{q-m} + 3\cdot(1-(e_3)^{q-m})\big) = O(2^n),$$

при $n-q = \lfloor \log n \rfloor$.

$\square$

Глава 2

Синтез формул в базисах с прямыми и итеративными переменными

2.1 Некоторые особенности задачи и порядок функции Шеннона

Рассмотрим различные базисы, состоящие из элементов с прямыми и итеративными переменными, и реализацию булевых функций формулами в них. Сначала будет доказано удобное представление оператора итеративного замыкания δ, определенного во введении. Этот оператор позволяет классифицировать все базисы из элементов с прямыми и итеративными входами. Эта классификация, в частности, используется в критерии полноты [37]. Будет рассмотрено поведение функции Шеннона сложности формул в различных базисах из всех семейств указанной классификации.

Далее за μ_n обозначается мультиплексорная функция порядка n, $n \geqslant 1$, определяемая равенством

$$\mu_n(x_1, \ldots, x_n, z_0, \ldots, z_{2^n-1}) = \bigvee_{\sigma_1,\ldots,\sigma_n \in B} x_1^{\sigma_1} \ldots x_n^{\sigma_n} z_{\nu(\sigma_1,\ldots,\sigma_n)},$$

где $\nu(\sigma_1, \ldots, \sigma_n)$ — число, двоичная запись которого совпадает с набором $(\sigma_1, \ldots, \sigma_n) \in B^n$, $z_i \in X \cup Y$ для всех i, $i = 0, \ldots, 2^n - 1$; а $x^\sigma = x \sim \sigma$,

$\sigma \in B$. Переменные $z_0, \ldots, z_{2^n-1}$ этой функции будем называть *информационными*.

Пусть A, $A \subseteq P_2(X \cup Y)$, — произвольное, не обязательно полное, конечное множество функций. Очевидно, $\delta(A) \subseteq [A] \cap P_2(Y)$. Покажем, что справедливо и обратное включение:

Теорема 5. *Для любой системы функций A, $A \subseteq P_2(X \cup Y)$, справедливо равенство*

$$\delta(A) = [A] \cap P_2(Y).$$

Доказательство. Заметим, что множество $[A] \cap P_2(Y)$ является «обычным» замкнутым классом [59] в $P_2(Y)$, содержащим константы, поэтому $[A] \cap P_2(Y) \in \Delta$, где Δ — множество, определенное соотношением (3).

Предположим, что найдутся два различных класса δ_1, $\delta_2 \in \Delta$, таких, что $\delta(A) = \delta_1$, $[A] \cap P_2(Y) = \delta_2$ и при этом $\delta_1 \subset \delta_2$.

Для каждого δ, $\delta \in \Delta$, обозначим, согласно [37],

$$R(\delta) = \{f \in P_2(X \cup Y) \,:\, [\{f\}]_{\{2\}} \cap P_2(Y) \subseteq \delta\}.$$

Заметим, что если функция $f \in R(\delta)$ зависит от n прямых переменных, то при подстановки вместо них любых констант получится функция из δ. Это означает, что функция f может быть представлена в виде

$$f = \mu_n(x_1, \ldots, x_n, g_1, \ldots, g_{2^n}), \tag{2.1}$$

где $g_i \in \delta$ для всех $i = 1, \ldots, 2^n$.

Из такого определения следует, что $A \subseteq R(\delta(A)) = R(\delta_1)$. Действительно, так как $\delta(A) = \left[[A]_{\{2\}} \cap P_2(Y)\right]_{\{3,4,6\}}$, то для произвольной функции $g \in A$ справедливо включение $[\{g\}]_{\{2\}} \cap P_2(Y) \subseteq \delta(A)$, а это и означает, что $g \in R(\delta(A))$.

Далее, $\delta_2 = [A] \cap P_2(Y) \subseteq [R(\delta_1)] \cap P_2(Y) = R(\delta_1) \cap P_2(Y)$, так как $R(\delta_1)$ - замкнутый класс. Получаем, что

$$\delta_2 \subseteq R(\delta_1) \cap P_2(Y), \quad \delta_1 \subset \delta_2. \tag{2.2}$$

Пользуясь тем, что для любых классов δ', δ'' системы Δ из условия $\delta' \subset \delta''$ следует включение $R(\delta') \subset R(\delta'')$, покажем невозможность выполнения (2.2), что и докажет утверждение. Рассмотрим все случаи.

1. Если $\delta(A) = \delta_1 = B$, то $A \subseteq P_2(X)$, откуда $\delta_2 = B = \delta_1$, что противоречит определению классов δ_1 и δ_2.

2. Если $\delta(A) = \delta_1 = I$, то для $\delta_2 \in \{D, K, O\}$ (а, следовательно, и для $\delta_2 \in \{M, L, P_2(Y)\}$) выполнение (2.2) невозможно, так как во множестве $R(I) \cap P_2(Y)$, согласно (2.1), отсутствуют дизъюнкции и конъюнкции двух и более итеративных переменных, а также отрицания итеративных переменных.

3. Если $\delta(A) = \delta_1 = O$, то для $\delta_2 = L$, (а, следовательно, для $\delta_2 = P_2(Y)$) выполнение (2.2)также невозможно, так как множество $R(O) \cap P_2(Y)$ не содержит линейных функции от двух и более итеративных переменных, как следует из (2.1).

4. Если $\delta(A) = \delta_1 = D$, то для $\delta_2 = M$ (а, следовательно, и для $\delta_2 = P_2(Y)$) выполнение (2.2) невозможно, так как $R(D) \cap P_2(Y)$ не содержит конъюнкцию итеративных переменных. Случай $\delta_1 = K$ аналогичен.

5. Если же $\delta(A) = \delta_1 \in \{M, L\}$, то $\delta_2 = P_2(Y)$, но $R(\delta_1)$ не содержит все функции итеративных переменных, поэтому (2.2) также не выполняется.

Полученные противоречия доказывают теорему 5. $\square$

Рассмотрим далее поведение функции Шеннона в некоторых базисах, являющихся представителями систем, итеративное замыкание которых принадлежит различным множествам семейства Δ. Далее всюду в этой главе рассматриваются только полные системы функций.

Пусть A, $A \subseteq P_2(X \cup Y)$, — система базисных функций, и $\delta(A) = \delta$. Как уже было указано, $\delta \in \Delta \setminus \{B\}$, в случае $\delta = B$ базис A не является полным.

Если $\delta = P_2(Y)$, то соответствующая функция Шеннона имеет порядок роста [42] $\frac{2^n}{\log n}$. В разделе 2.2 будет доказана асимптотика этой функции в более общем случае, когда $\delta \supseteq M$.

Рассмотрим системы функций A, $A \subseteq P_2(X \cup Y)$, такие, что $\delta(A) = D$.

Множество номеров существенных итеративных переменных функции f обозначим через $J(f)$. Из (2.1) следует, что любую функцию f, $f \in R(D)$, можно представить в виде:

$$f = \bigvee_{j \in J(f)} y_j \varphi_j \vee \varphi_0, \tag{2.3}$$

где $\varphi_j \in P_2(X)$ при всех j, $j \in J(f) \cup \{0\}$.

Пусть $D^{(1)}$ (соответственно, $D^{(0)}$) — множество тех функций f, $f \in R(D)$, для которых все коэффициенты φ_j, $j \in J(f)$, при переменных в разложении (2.3) являются монотонными (соответственно, антимонотонными) функциями.

Лемма 13. *Пусть полные системы системы функций A' и A'' таковы, что*

$$A' = \{\bar{x}_1 y_1, f'_1, \ldots, f'_k, y_1 \vee y_2\},$$

где $f'_1, \ldots, f'_k \in D^{(1)}$, $k \geqslant 1$, и

$$A'' = \{x_1 y_1, f''_1, \ldots, f''_k, y_1 \vee y_2\},$$

где $f''_1, \ldots, f''_k \in D^{(0)}$, $k \geqslant 1$, тогда

$$L_{A'}(n) = \Theta(2^n),\ L_{A''}(n) = \Theta(2^n).$$

Доказательство. Заметим, что $\delta(A') = \delta(A'') = D$.

Рассмотрим минимальную по сложности формулу $\mathcal{F}$ для линейной функции l_n в базисе A' (случай базиса A'' рассматривается аналогично). Пусть каждая функция f'_i, $i = 1, \ldots, k$, представима в виде разложения (2.3) следующим образом: $f'_i = \bigvee_{j \in J(f_i)} y_j \varphi_j^{(i)} \vee \varphi_0^{(i)}$. В символьной записи $\mathcal{F}$, принимая символы функций $\varphi_j^{(i)}$ ($i = 1, \ldots, k$; $j = 1, \ldots, |J(f_i)|$) за отдельные переменные, раскроем скобки, используя дистрибутивность конъюнкции относительно дизъюнкции. При этом не изменится число символов дизъюнкции, входящих в формулу. В результате получится ДНФ, конъюнкции которой состоят из отрицаний прямых переменных, а также из символов функций $\varphi_j^{(i)}$. Если хотя бы одна из таких конъюнкций обращается в единицу на более, чем одном наборе, то, так как все функции $\varphi_j^{(i)}$ монотонны, такая конъюнкция обратится в единицу на двух соседних наборах, что противоречит реализации этой ДНФ линейной функции. Таким образом, каждая конъюнкция покрывает не более одного набора, а это означает, что их число не менее, чем 2^{n-1}. С учетом того, что при раскрытии скобок число дизъюнкций не изменилось, а множества $J(f_1), \ldots, J(f_k)$ конечны и не зависят от n, имеем, что число элементов $y_1 \vee y_2$ в формуле $\mathcal{F}$ есть $\Omega(2^n)$, что, с учетом верхней оценки из [38], доказывает лемму.

$\square$

Доказанное утверждение означает существование в семействе систем функций с итеративным замыканием, равным D, базисов, поведение функции Шеннона для сложности формул в которых не является «стандартным» $2^n/\log n$, а достигает порядка 2^n. Кроме того, из доказательства леммы 13 следует, что для базисов $\{\mu_k\}$, $\{h'_k\}$ и $\{h''_k\}$, где

$$\mu_k = \mu_k(x_1, \ldots, x_k, y_0, \ldots, y_{2^k-1}) = \bigvee_{\sigma_1, \ldots, \sigma_k \in \{0,1\}} x_1^{\sigma_1} \cdots x_k^{\sigma_k} \cdot y_{\nu(\sigma_1, \ldots, \sigma_k)}, \tag{2.4}$$

$$h'_k = (\bar{x}_1 \vee \ldots \vee \bar{x}_k) \cdot y_1 \vee x_1 \cdots x_k \cdot y_2 = \mu_k(x_1, \ldots, x_k, y_1, y_1, \ldots, y_1, y_2),$$

$$h''_k = \bar{x}_1 \cdots \bar{x}_k \cdot y_1 \vee (x_1 \vee \ldots \vee x_k) \cdot y_2 = \mu_k(x_1, \ldots, x_k, y_1, y_2, \ldots, y_2, y_2),$$

при любых натуральных k, $k \geqslant 1$, справедливо следующее утверждение.

Лемма 14. *Для любого фиксированного натурального числа* k

$$L_{\{\mu_k\}}(n) = \Theta(2^n), \quad L_{\{h'_k\}}(n) = \Theta(2^n), \quad L_{\{h''_k\}}(n) = \Theta(2^n).$$

Отметим, что

$$\delta(\{\mu_k\}) = \delta(\{h'_k\}) = \delta(\{h''_k\}) = I,$$

для всех k, $k \geqslant 1$.

Пусть $k \geqslant 1$. Для каждого набора $(\tau_0, \ldots, \tau_{2^k-1}) \in B^{2^k-1}$ введем обозначение

$$\mu_k^{(\tau_0,\ldots,\tau_{2^k-1})}(x_1, \ldots, x_k, z_0, \ldots, z_{2^k-1}) = \bigvee_{\sigma_1,\ldots,\sigma_k \in B} x_1^{\sigma_1} \ldots x_k^{\sigma_k} z_{\nu(\sigma_1,\ldots,\sigma_k)}^{\tau_{\nu(\sigma_1,\ldots,\sigma_k)}}.$$

При этом $\mu_k^{(1,\ldots,1)} \equiv \mu_k$. Положим

$$A_\mu^k = \left\{ \mu_k^{(\tau_0,\ldots,\tau_{2^k-1})}(x_1, \ldots, x_k, y_0, \ldots, y_{2^k-1}) \,\middle|\, (\tau_0, \ldots, \tau_{2^k-1}) \in B^{2^k-1} \right\}.$$

При всех k, $k \geqslant 1$, система A_μ^k полна, и $\delta(A_\mu^k) = O$.

Лемма 15. *Пусть* k, $k \geqslant 1$, *— фиксированное натуральное число. Тогда для любой системы функций* A, $A \subseteq A_\mu^k$, *справедливо соотношение:*

$$L_A(l_n) = \Omega(2^n).$$

Доказательство. Пусть $\mathcal{F}$ — произвольная формула в базисе A_μ^k, реализующая функцию от прямых переменных. Построим эквивалентную ей формулу $\mathcal{F}'$ в базисе $\{\mu_k, \bar{y}_1\}$, у которой все отрицания стоят только над переменными, и при этом $L(\mathcal{F}') \leqslant c \cdot L(\mathcal{F})$ для некоторой константы c.

Для построения формулы $\mathcal{F}'$ указанного вида будем последовательно применять, пока это возможно, следующее преобразование.

Пусть в дереве формулы $\mathcal{F}$ существует элемент $\mathcal{E}$, реализующий функцию $\mu_k^{(\tau_0,\ldots,\tau_{2^k-1})}$, где $(\tau_0, \ldots, \tau_{2^k-1}) \neq (1, \ldots, 1)$. Заменим его на элемент $\mathcal{E}'$, реализующий функцию μ_k, с сохранением порядка входов. Кроме того, для каждого i, $i \in \{0, \ldots, 2^k - 1\}$, такого, что $\tau_i = 0$, произведем следующую замену:

1. если i-й вход элемента $\mathcal{E}$ был константным, то подадим на i-й вход элемента $\mathcal{E}'$ противоположную константу;

2. если на i-й вход элемента $\mathcal{E}$ подавалась переменная $x \in X$, то добавим в формулу элемент отрицания, на вход которого подается переменная x, а его выход подается на i-й вход $\mathcal{E}'$.

3. если на i-й вход элемента $\mathcal{E}$ подавался выход элемента $\mathcal{E}''$, реализующего функцию $\mu_k^{(\tau'_0,\ldots,\tau'_{2^k-1})}$, $(\tau'_0,\ldots,\tau'_{2^k-1}) \in B^{2^k-1}$, то заменим элемент $\mathcal{E}''$ на элемент, реализующий функцию $\mu_k^{(\bar{\tau}'_0,\ldots,\bar{\tau}'_{2^k-1})}$.

Проводя, пока это возможно, такое преобразование для формулы $\mathcal{F}$ «снизу вверх», получим искомую формулу $\mathcal{F}'$. Заметим, что число добавленных таким образом отрицаний не превосходит ранга формулы $\mathcal{F}$, и потому $L(\mathcal{F}') \leqslant c{\cdot}L(\mathcal{F})$.

Для каждой функции f, $f \in P_2(X)$, обозначим через $L_k(f)$ минимальную сложность реализации функции f в классе формул в базисе $\{\mu_k, \bar{y}_1\}$, у которых отрицания стоят только над переменными. Из доказательства леммы 13 следует, что $L_k(l_n) = \Omega(2^n)$ для всех k, $k \geqslant 1$. Действительно, расписав каждую функцию μ_k в виде (2.4) в формуле $\mathcal{F}_{l_n}$, реализующую линейную функцию, и раскрыв скобки в полученной формуле, получим ДНФ, число слагаемых в которой по порядку равно числу элементов μ_k в формуле $\mathcal{F}_{l_n}$, а ДНФ линейной функции имеет, как это уже указывалось, длину 2^{n-1}.

Из приведенных выше рассуждений следует, что

$$L_A(l_n) \geqslant L_{A_\mu^k}(l_n) \geqslant \frac{1}{c}L_k(l_n) = \Omega(2^n),$$

что и доказывает лемму. □

Далее докажем, что в базисах

$$A_1 = \{(x_1 \oplus x_2)y_1, (x_1 \sim x_2)y_1, y_1 \vee y_2\},$$

$$A_2 = \{(x_1 \oplus x_2)y_1, y_1 \vee y_2\},$$

$$A_3 = \{(x_1 \sim x_2)y_1, y_1 \vee y_2\}$$

семейства $\{A : \delta(A) = D\}$ сложность линейной функции сильно изменяется по сравнению с базисами, рассмотренными в лемме 13.

Лемма 16. *Справедливы соотношения*

$$L_{A_1}(l_n) = O\left(2^{n/2}\right),$$

$$L_{A_i}(l_n) = O\left(3^{n/2}\right), \quad i = 2, 3.$$

Доказательство. Доказательство основано на следующих рекуррентных разложениях, справедливых при любых n, $n \geqslant 3$:

$$l_n(x_1, \ldots, x_n) = (x_1 \oplus x_2)\bar{l}_{n-2}(x_3, \ldots, x_n) \vee (x_1 \sim x_2)l_{n-2}(x_3, \ldots, x_n),$$

$$l_n(x_1, \ldots, x_n) = (x_1 \oplus x_2)\bar{l}_{n-2}(x_3, \ldots, x_n) \vee$$
$$\vee\, \bar{x}_1\bar{x}_2 l_{n-2}(x_3, \ldots, x_n) \vee x_1 x_2 l_{n-2}(x_3, \ldots, x_n),$$

$$l_n(x_1, \ldots, x_n) = (x_1 \sim x_2)l_{n-2}(x_3, \ldots, x_n) \vee$$
$$\vee\, x_1\bar{x}_2\bar{l}_{n-2}(x_3, \ldots, x_n) \vee \bar{x}_1 x_2 l_{n-2}(x_3, \ldots, x_n),$$

аналогичных разложениях для отрицания линейной функции, и на том, что $x_1 = x_1 \oplus 0 = x_1 \sim 1$, а $\bar{x}_1 = x_1 \oplus 1 = x_1 \sim 0$. □

Доказанная лемма, в частности, означает, что утверждение леммы 13 не допускает прямого обобщения относительно сложности линейной функции на случай произвольного базиса из $D^{(0)} \cup D^{(1)}$, а именно, если $A \subseteq D^{(0)} \cup D^{(1)}$, то в классе формул над A необязательно самой сложной является линейная функция. Действительно, пусть

$$A' = \{(x_1 \vee x_2)y_1, (\bar{x}_1 \vee \bar{x}_2)y_1, y_1 \vee y_2\},$$

тогда $A \subseteq D^{(0)} \cap D^{(1)}$, и, как следует из леммы 16,

$$L_{A'}(l_n) = O\left(3^{n/2}\right) = o\left(\frac{2^n}{\log n}\right),$$

так как

$$(x_1 \oplus x_2)y_1 = (x_1 \vee x_2)(\bar{x}_1 \vee \bar{x}_2)y_1.$$

Далее докажем нижние оценки сложности линейной функции в базисах A_1, A_2, A_3.

Лемма 17. *Существует такая положительная константа c_1, что для любых натуральных n справедливы соотношения:*

$$L_{A_i}(l_n) \geqslant c_1 \cdot 2^{n/2}, \quad i = 1, 2, 3.$$

Доказательство. Рассмотрим конъюнкцию K некоторого числа функций вида $(x_1 \oplus x_2)$, $(x_1 \sim x_2)$, взятых от произвольных переменных из множества $\{x_1, \ldots, x_m\}$. Будем предполагать, что конъюнкция K зависит от всех переменных их этого множества существенно.

Построим неориентированный граф G_1, $G_1 = (V, E)$, в котором $V = \{v_1, \ldots, v_m\}$ — множество вершин. Будем считать, что каждая вершина v_i, $v_i \in V$, взаимно однозначно поставлена в соответствие переменной x_i, где $i = 1, \ldots, m$. Для каждой функции вида $(x_i \oplus x_j)$, участвующей в конъюнкции K, построим ребро (v_i, v_j) в графе G_1. Все такие ребра и будут образовывать множество E.

Пусть граф G_2 получается из графа G_1 отождествлением всех пар вершин v_i, v_j, для которых функция $(x_i \sim x_j)$ участвует в конъюнкции K.

Рассмотрим правильную (см., например, [59]) раскраску вершин графа G_2 в два цвета 0 и 1. Из построения графа следует, что набор цветов вершин $\alpha = (\alpha_1, \ldots, \alpha_m)$, по которому вершина v_i красится в цвет $\alpha_i \in B$, $i = 1, \ldots, m$, при правильной раскраске обращает конъюнкцию K в единицу. И наоборот, если $K(\alpha) = 1$, то набор α образует правильную раскраску графа G_2 в два цвета.

Заметим, что каждую компоненту связности графа можно покрасить правильно не более, чем двумя способами, так как указав цвет одной вершины (0 или 1), цвета остальных вершин этой компоненты определяются однозначно, при условии, что правильная раскраска возможна. Таким образом, если граф G_2 имеет t компонент связности, то число способов раскрасить этот граф правильно в два цвета есть 2^t.

Далее, поскольку каждая вершина графа G_1 либо отождествлена, либо смежна с некоторой другой вершиной, что справедливо в силу существенной зависимости конъюнкции K от всех переменных, для t справедлива оценка $t \leqslant m/2$. Это означает, что конъюнкция K обращается в единицу на не более, чем $2^{m/2}$ наборах значений своих существенных переменных.

Заметим, что эта оценка не изменится, если в конъюнкцию K дополнительно будут входить сомножители вида x_i, $\bar{x}_i$, $i \notin \{1, \ldots, m\}$.

Аналогично доказательству леммы 13, рассмотрим минимальную по сложности формулу $\mathcal{F}$ в базисе A_1 для линейной функции l_n, и раскроем скобки в её символьной записи, пользуясь только тождеством дистрибутивности конъюнкции относительно дизъюнкции и тождествами подстановки констант. В результате получим формулу $\mathcal{F}' = K_1 \vee \ldots \vee K_p$, в которой каждая конъюнкция K_i, $i = 1, \ldots, p$, имеет вид

$$K_i = x_{u_1}^{\sigma_1} \ldots x_{u_r}^{\sigma_r} \varphi_1(x_{v_1'}, x_{v_1''}) \ldots \varphi_s(x_{v_s'}, x_{v_s'}),$$

где $1 \leqslant u_1, \ldots, u_r, v_1', v_1'', \ldots, v_s', v_s'' \leqslant n$, $\sigma_1, \ldots, \sigma_r \in B$, а $\varphi_j(x', x'')$ является при каждом j, $j = 1, \ldots, s$, либо функцией $x' \oplus x''$, либо функцией $x' \sim x''$.

В силу тождеств $x'(x' \sim x'') = x'x''$, $\bar{x}'(x' \sim x'') = \bar{x}'\bar{x}''$, $x'(x' \oplus x'') = x'\bar{x}''$, $\bar{x}'(x' \oplus x'') = \bar{x}'x''$, будем считать, что $\{u_1, \ldots, u_r\} \cap \{v_1', v_1'', \ldots, v_s', v_s''\} = \varnothing$.

Заметим, что $\{u_1, \ldots, u_r\} \cup \{v_1', v_1'', \ldots, v_s', v_s''\} = \{1, \ldots, n\}$, в силу реализации формулой $\mathcal{F}'$ линейной функции, а потому каждая из конъюнкций $K_1, \ldots, K_p$ обращается в единицу на не более, чем $2^{n/2}$ наборах. Следовательно, так как функция l_n равна единице на 2^{n-1} наборах, справедлива оценка $p \geqslant 2^{n/2-1}$.

По построению, формула $\mathcal{F}$ содержит столько же элементов дизъюнкции, сколько и формула $\mathcal{F}'$, то есть $p - 1 = \Omega(2^{n/2})$, что и доказывает оценку в случае базиса A_1. Так как $A_2 \subset A_1$ и $A_3 \subset A_1$, то данная оценка верна и для базисов A_2, A_3.

$\square$

Заметим, что аналогичные леммам 13, 16 и 17 результаты можно получить и для случая систем A таких, что $\delta(A) = K$.

Леммы 16 и 17 доказывают следующую теорему.

Теорема 7. *В базисе* $A_1 = \{(x_1 \oplus x_2)y_1, (x_1 \sim x_2)y_1, y_1 \vee y_2\}$ *сложность линейной функции* l_n *удовлетворяет соотношению*

$$L_{A_1}(l_n) = \Theta(2^{n/2}),$$

а в базисах $A_2 = \{(x_1 \oplus x_2)y_1, y_1 \vee y_2\}$ *и* $A_3 = \{(x_1 \sim x_2)y_1, y_1 \vee y_2\}$ *— соотношению*

$$c_1 \cdot 2^{n/2} \leqslant L_{A_i}(l_n) \leqslant c_2 \cdot 3^{n/2}, \quad i = 1, 2,$$

где c_1, c_2 *— некоторые положительные константы.*

Далее рассмотрим системы функций A, $A \subseteq P_2(X \cup Y)$, такие, что $\delta(A) = L$.

Лемма 18. *Для системы функций* $A_4 = \{x_1 y_1,\ y_1 \oplus y_2\}$ *выполняется соотношение*

$$L_{A_4}(n) = \Theta(2^n).$$

Доказательство. Рассмотрим произвольную формулу в базисе A_4, реализующую некоторую функцию f. Если в данной формуле раскрыть скобки и привести подобные, то получится полином Жегалкина [59] для функции f, который единственен с точностью до перестановки слагаемых в нем. При этом число функциональных символов $\oplus$ может только уменьшиться, так как все умножения в базисе — это умножения на булевскую переменную.

Для функции $d_n = x_1 \vee \ldots \vee x_n$ полином Жегалкина представляет собой сумму $2^n - 1$ монотонных элементарных конъюнкций, поэтому в любой формуле над базисом A_4, реализующей функцию d_n, содержится не менее $2^n - 2$ функциональных элементов $y_1 \oplus y_2$, значит, и сложность всей формулы не менее, чем 2^n. $\square$

Пусть базисная система функций A такова, что $\delta(A) = L$, а любая функция f системы A имеет вид

$$f = \bigoplus_{j \in J(f)} K_j y_j \oplus \sigma,$$

где $\sigma \in B$, и каждая K_j, $j \in J(f)$, представляет собой монотонную конъюнкцию прямых переменных. Как следует из доказательства леммы 18, сложность функции d_n в этом базисе есть $\Omega(2^n)$.

Рассмотрим систему функций $A_5 = \{x_1 y_1, \bar{x}_1 y_1, y_1 \oplus y_2\}$. Заметим, что в отличие от предыдущего базиса, функция d_n имеет в A_5 линейную сложность, так как справедливо соотношение

$$d_n = d_{n-1} \bar{x}_n \oplus x_n.$$

При аналогичном рассматриваемому в доказательстве леммы 18 раскрытию скобок в формуле над таким базисом возникает полиномиальная нормальная форма (ПНФ) — сумма по модулю два элементарных конъюнкций. Из результатов работ [3, 16] следует, что функция Шеннона для длины ПНФ (т. е. для числа элементарных конъюнкций в ней) имеет порядок роста $2^n/n$. Это говорит о неэффективности применения нижней оценки числа элементов сложения для оценки снизу функции Шеннона $L_{A_5}(n)$.

2.2 Сложность формул в базисах, итеративное замыкание которых содержит все монотонные функции

В этом разделе рассматриваются формулы в базисах A, $A \subseteq P_2(X \cup Y)$, таких, что $\delta(A) \in \{P_2(Y), M\}$. Сначала изучаются некоторые свойства макроблоков, определенных во введении, затем доказывается асимптотика функции Шеннона сложности формул в указанных базисах.

Далее предполагается, что каждый базис A разбивается на два множества

$$A' = \{\mathcal{E}_1, \dots, \mathcal{E}_{b'}\}, \quad A'' = \{\mathcal{E}_{b'+1}, \dots, \mathcal{E}_b\},$$

где $1 \leqslant b' \leqslant b$, при этом в A'' все входы каждого элемента прямые (в случае отсутствия таких элементов $A'' = \varnothing$).

Лемма 19. *Для любого базиса* A, $A \subseteq P_2(X \cup Y)$, *существует канонический макроблок, являющийся в нем минимальным.*

Доказательство. Пусть M — произвольный минимальный макроблок в базисе A, который состоит из элементов $\mathcal{E}_j, \mathcal{E}_{i_1}, \dots, \mathcal{E}_{i_m}$, где $j \in \{1, \dots, b'\}$, $m \in \{0, \dots, k''_j - 1\}$, $i_1, \dots, i_m \in \{b'+1, \dots, b\}$. Сначала докажем, что найдется такой индекс p, $p \in \{i_1, \dots, i_m\}$, что макроблок M', полученный из макроблока M заменой всех элементов $\mathcal{E}_{i_1}, \dots, \mathcal{E}_{i_m}$ на элемент $\mathcal{E}_p$, имеет приведенный вес $\rho_{M'} = \rho_M$. Для этого достаточно доказать справедливость неравенства

$$\rho_M = \frac{L_j + L_{i_1} + \ldots + L_{i_m}}{k_{i_1} + \ldots + k_{i_m} + k_j - m - 1} \geqslant \frac{L_j + mL_p}{k_j - 1 + m(k_p - 1)} = \rho_{M'}.$$

для некоторого p, $p \in \{i_1, \dots, i_m\}$. Предположим противное, пусть для всех p, $p \in \{i_1, \dots, i_m\}$, выполняется:

$$\rho_M < \rho_{M'},$$

что эквивалентно

$$L_j m(k_p - 1) + (k_j - 1 + m(k_p - 1)) \sum_{t=1}^{m} L_{i_t} < L_p m(k_j - 1) + (L_j + mL_p) \sum_{t=1}^{m} (k_{i_t} - 1).$$

Просуммировав последнее неравенство для всех $p \in \{i_1, \ldots, i_m\}$, получим противоречие, что доказывает существование определенного выше макроблока M'.

Заметим далее, что если рассмотреть функцию

$$r(m) = \frac{L_j + mL_p}{k_j - 1 + m(k_p - 1)},$$

задающую приведенный вес макроблока M', как функцию действительного аргумента m на отрезке $[0, k''_j - 1]$, то такая функция будет непрерывной, ограниченной и монотонной на этом отрезке, а это означает, что её минимум достигается на одном из концов этого отрезка. При $m \in \{0, k''_j - 1\}$ соответствующий макроблок M'', который отличается от M' количеством m элементов с прямыми входами, имеет приведенный вес $\rho_{M''} \leqslant \rho_{M'} \leqslant \rho_M$, и при этом является каноническим. $\square$

Следует отметить, что минимальный макроблок может не быть каноническим. Действительно, рассмотрим базис, состоящий из трех элементов:

$$\mathcal{E}_1: \quad \varphi_1 = \varphi_1(y_1, y_2, y_3),\ L_1 = 3,\ \rho_1 = 3/2;$$

$$\mathcal{E}_2: \quad \varphi_2 = \varphi_2(x_1, x_2),\ L_2 = 1/6,\ \rho_2 = 1/6;$$

$$\mathcal{E}_3: \quad \varphi_3 = \varphi_3(x_1, x_2, x_3),\ L_3 = 1,\ \rho_3 = 1/2.$$

Приведенный вес базиса, равный $5/6$, достигается, в частности, на канонических макроблоках, соответствующих формулам

$$\varphi_1(\varphi_2(x_1, x_2), \varphi_2(x_3, x_4), y_1),$$

$$\varphi_1(\varphi_3(x_1, x_2, x_3), \varphi_3(x_4, x_5, x_6), y_1),$$

а так же на макроблоках, не являющихся каноническими, но также являющихся минимальными:

$$\varphi_1(\varphi_2(x_1, x_2), \varphi_3(x_3, x_4, x_5), y_1),$$

$$\varphi_1(\varphi_3(x_1, x_2, x_3), \varphi_2(x_4, x_5), y_1).$$

Будем говорить, что канонический макроблок *порожден* парой базисных элементов $(\mathcal{E}', \mathcal{E}'') \in A' \times A''$, если этот макроблок состоит из элемента $\mathcal{E}'$ с k

итеративными входами и $(k-1)$ элементов $\mathcal{E}''$, выходы которых подаются на итеративные входы элемента $\mathcal{E}'$.

Следующая лемма доказывает еще одно свойство минимальных канонических макроблоков.

Лемма 20. *Пусть A, $A \subseteq P_2(X \cup Y)$, — базис из элементов с прямыми и итеративными входами. Тогда если его приведенный вес ρ_A достигается на двух различных канонических макроблоках M_1 и M_2, порожденных парами базисных элементов $(\mathcal{E}_1, \mathcal{E}_3)$ и $(\mathcal{E}_2, \mathcal{E}_4)$ соответственно, где $\mathcal{E}_1, \mathcal{E}_2 \in A'$, $\mathcal{E}_3, \mathcal{E}_4 \in A''$, то канонические макроблоки M_3 и M_4, порожденные парами базисных элементов $(\mathcal{E}_1, \mathcal{E}_4)$ и $(\mathcal{E}_2, \mathcal{E}_3)$ соответственно, также являются минимальными.*

Доказательство. В соответствии с обозначениями, определенными во введении, пусть

$$\begin{aligned}
&a = k_1'' - 1, \quad b = k_2'' - 1,\\
&c = k_1' + (k_1'' - 1)k_3, \quad d = k_2' + (k_2'' - 1)k_4,\\
&e = k_1' + (k_1'' - 1)k_4, \quad f = k_2' + (k_2'' - 1)k_3.
\end{aligned}$$

Заметим, что $\frac{d-f}{b} = \frac{e-c}{a}$, то есть $ad - af = be - bc$.

По определению, $\rho_{M_1} = (L_1 + aL_3)/c$, $\rho_{M_2} = (L_2 + bL_4)/d$. Из условия равенства $\rho_{M_1} = \rho_{M_2}$ следует, что

$$L_3 = \frac{L_2c + L_4bc - L_1d}{ad}. \tag{2.5}$$

Так как макроблоки M_1 и M_2 являются минимальными, то $\rho_{M_1} \leqslant \rho_{M_4}$ и $\rho_{M_2} \leqslant \rho_{M_3}$. По определению это означает, что

$$\frac{L_1 + aL_3}{c} \leqslant \frac{L_2 + L_3b}{f} \quad \text{и} \quad \frac{L_2 + L_4b}{d} \leqslant \frac{L_1 + L_4a}{e}$$

соответственно. Второе из этих неравенств влечет

$$L_1d - L_2e \geqslant L_4(be - ad), \tag{2.6}$$

а первое, с учетом (2.5), можно переписать в виде

$$L_1 f - L_2 c \leqslant \frac{L_2 c + L_4 bc - L_1 d}{ad}(bc - af).$$

Преобразуем последнее неравенство:

$$(L_1 f - L_2 c)ad \leqslant L_2(cbc - caf) + L_4(bc - af)bc - L_1(dbc - daf),$$

что эквивалентно

$$L_1 dbc - L_2(af - bc - ad)c \leqslant L_4(bc - af)bc.$$

Далее, так как $af - bc - ad = -be$, то $L_1 dbc - L_2 bec \leqslant L_4(bc - af)bc = L_4(be - ad)bc$, т. е.

$$L_1 d - L_2 e \leqslant L_4(be - ad),$$

что, в силу (2.6), обращает все приведенные неравенства в равенство, и, в частности, $\rho_{M_1} = \rho_{M_4} = \rho_{M_2} = \rho_{M_3} = \rho_A$. □

Далее докажем следующую теорему.

Теорема 12. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис функций, такой, что $\delta(A) \in \{P_2(Y), M\}$. Тогда при $n \to \infty$ справедливо соотношение*

$$\mathcal{L}_A(n) \sim \rho_A \frac{2^n}{\log n}.$$

Нижнюю оценку в теореме докажем при помощи мощностного метода. Пусть $\mathcal{U}_A(\mathcal{L}, n)$ — множество формул в базисе A, реализующих функции от n прямых переменных и имеющих сложность не более $\mathcal{L}$.

Лемма 21. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис функций, такой, что $\delta(A) \in \{P_2(Y), M\}$. Тогда*

$$\mathcal{L}_A(n) \geqslant \rho_A \frac{2^n}{\log n}\left(1 - O\left(\frac{1}{\log n}\right)\right).$$

Доказательство. Рассмотрим произвольную формулу $\mathcal{F}$ в базисе A, реализующую функцию от n прямых переменных $\tilde{x}_n = (x_1, \ldots, x_n)$. Пусть эта формула содержит n_i элементов $\mathcal{E}_i$ для всех $i = 1, \ldots, b$. Тогда ранг этой формулы

$$R(\mathcal{F}) = \sum_{i=1}^{b} n_i(k_i - 1) + 1,$$

а её сложность

$$\mathcal{L}(\mathcal{F}) = \sum_{i=1}^{b} n_i L_i.$$

Покажем сначала, что

$$\mathcal{L}(\mathcal{F}) \geqslant \rho_A R(\mathcal{F}) - O(1) \tag{2.7}$$

при больших значениях $R(\mathcal{F})$. Рассмотрим два случая.

1. Среди элементов с минимальным приведенным весом есть элементы, имеющие хотя бы один итеративный вход. Пусть $\mathcal{E}_j$ — один из таких элементов, $j \in \{1, \ldots, b\}$. Тогда

$$\begin{aligned}\mathcal{L}(\mathcal{F}) &= \sum_{i \in \{1,\ldots,b\} \setminus \{j\}} n_i L_i + n_j L_j = \\ &= \sum_{i \in \{1,\ldots,b\} \setminus \{j\}} n_i L_i - \frac{L_i}{k_j - 1} \left(R(\mathcal{F}) - \sum_{i \in \{1,\ldots,b\} \setminus \{j\}} n_i(k_i - 1) - 1 \right) = \\ &= \sum_{i \in \{1,\ldots,b\} \setminus \{j\}} n_i(L_i - \rho_j(k_i - 1)) + \rho_j R(\mathcal{F}) - \rho_j \geqslant \rho_j \cdot R(\mathcal{F}) - O(1),\end{aligned}$$

   так как для всех $i = 1, \ldots, b$ справедливо неравенство $(L_i - \rho_j(k_i - 1)) \geqslant 0$, в силу минимальности приведенного веса элемента $\mathcal{E}_j$.

   Заметим, что оценка $\mathcal{L}(\mathcal{F}) = \rho_j \cdot R(\mathcal{F})$ достигается на формуле, целиком состоящей из элементов $\mathcal{E}_j$.

2. Все элементы минимального приведенного веса имеют только прямые входы. Формула $\mathcal{F}$ представима в виде

$$\mathcal{F}(\tilde{x}_n) = \mathcal{F}' \left(\tilde{x}_n, \varphi_{j_1}(\tilde{x}_n), \ldots, \varphi_{j_p}(\tilde{x}_n) \right),$$

где $\mathcal{F}'$ — формула, реализующая функцию из $P_2(X \cup Y)$ в базисе A', а $j_1, \ldots, j_p \in \{b'+1, \ldots, b\}$. Построим формулу $\mathcal{G}$, представляющую собой цепь из $n' = \sum_{i=1}^{b'} n_i$ макроблоков $M_1, \ldots, M_{n'}$, и состоящую из тех же самых элементов, что и формула $\mathcal{F}$. Элементы с прямыми входами в таком случае должны быть произвольно подсоединены к свободным итеративным входам такой формулы. Заметим, что $\mathcal{L}(\mathcal{F}) = \mathcal{L}(\mathcal{G})$ и $R(\mathcal{F}) = R(\mathcal{G})$. Рассмотрим формулу $\mathcal{G}$ как формулу в базисе из макроблоков $M_1, \ldots, M_{n'}$, тогда, аналогично случаю 1, сложность такой формулы не менее, чем $\rho_M R(\mathcal{G}) - O(1)$, где M — макроблок из $M_1, \ldots, M_{n'}$ с наименьшим приведенным весом. Таким образом, в силу леммы 19, в этом случае оценка (2.7) также справедлива, и достигается на формуле, целиком состоящей из минимальных канонических для базиса A макроблоков.

Число попарно не эквивалентных формул ранга R в базисе A, реализующих функции от n прямых переменных, не превосходит $(cn)^R$, где c — некоторая константа, поэтому, в силу (2.7),

$$\|\mathcal{U}_A(\mathcal{L}, n)\| \leqslant (cn)^{\frac{1}{\rho_A}\mathcal{L}}.$$

Так как $\|\mathcal{U}_A(\mathcal{L}_A(n), n)\| \geqslant 2^{2^n}$, то при достаточно больших n справедливо утверждение леммы. $\square$

Далее докажем верхнюю оценку в теореме 12.

Формулу $\mathcal{F}$, в записи которой переменная z, $z \in X \cup Y$, встречается только один раз, будем называть *бесповторной по переменной* z.

Из [32] и леммы о немонотонной функции (см., например, [59]) следует, что для любого базиса A, $A \subseteq P_2(X \cup Y)$, такого, что $\delta(A) \in \{P_2(Y), M\}$, существуют бесповторные по своим существенным переменным формулы $\mathcal{F}_\&$, $\mathcal{F}_\vee$, $\mathcal{F}_\neg$, реализующие функции $y_1 \cdot y_2$, $y_1 \vee y_2$, $\bar{x}_1$ соответственно.

Лемма 22 ([32]). *Существует бесповторная по информационным переменным формула $\mathcal{F}_{\mu_n}$ в базисе $\{y_1 \cdot y_2, y_1 \vee y_2, \bar{x}_1\}$, реализующая мультиплексорную функцию $\mu_n(x_1, \ldots, x_n, y_0, \ldots, y_{2^n-1})$ порядка n со сложностью $O(2^n)$.*

Для дальнейших рассуждений приведем следующий упрощенный вариант леммы 1.

Лемма 23 ([32]). *Для любых натуральных чисел s, m, N, удовлетворяющим условию*

$$s \cdot N \geqslant 2^m,$$

и для любой функции $\varphi(z_1, \ldots, z_N)$ существует φ-универсальное множество G порядка m такое, что

$$|G| \leqslant N \cdot 2^s.$$

Лемма 24. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис функций, такой, что $\delta(A) \in \{P_2(Y), M\}$. Тогда для любой функции f, $f \in P_2(n)$, существует формула $\mathcal{F}_f$ в этом базисе, реализующая эту функцию, и такая, что*

$$\mathcal{L}(\mathcal{F}_f) \lesssim \rho_A \frac{2^n}{\log n}.$$

Доказательство. Пусть M — минимальный канонический макроблок в базисе A. В случае, когда минимальный приведенный вес элементов базиса достигается на некотором элементе $\mathcal{E}_j$, $j \in \{1, \ldots, b'\}$, имеющем хотя бы один итеративный вход, положим $M = \mathcal{E}_j$.

Пусть, далее, натуральные параметры m, q, s, N и p таковы, что

$$1 \leqslant m < q < n, \quad s \cdot N \geqslant 2^m, \quad p \cdot (k_M - 1) + 1 = N,$$

где k_M — число входов M, и пусть $x' = (x_1, \ldots, x_q)$, $x'' = (x_{q+1}, \ldots, x_n)$.

Рассмотрим произвольную формулу $\mathcal{F}_1$, состоящую из p блоков M. Как обычно, выходы любого блока могут подсоединяться только к итеративным входам других блоков. Считая все входы этой формулы прямыми, обозначим реализуемую формулой $\mathcal{F}_1$ функцию как φ. Заметим, что

$$\mathcal{L}(\mathcal{F}_1) = \rho_A \cdot N.$$

Рассмотрим функцию $d(y_1, \ldots, y_N) = y_1 \vee \ldots \vee y_N$, эта функция, как было указано выше, реализуема бесповторной по всем своим переменным формулой в базисе A сложности $O(N)$. Построим по лемме 23 φ-универсальное множество G_1 порядка m и d-универсальное множество G_2 порядка m так, что функции из этих множеств зависят от одних и тех же переменных $(x_1, \ldots, x_m)$, и при этом

$$|G_1 \cup G_2| \leqslant 2 \cdot N \cdot 2^s.$$

Положим $q = m + 3|G|$, где $G = G_1 \cup G_2$, и построим по лемме 3 разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q на m-регулярные компоненты, в котором доля «плохих» компонент не превосходит e_1^{q-m}, $e_1 < 1$, и которое моделирует все функции из множества G с помощью переменных или их отрицаний.

Заметим, что при любом i, $i \in \{1, \ldots, 2^{q-m}\}$, любая функция $g \in P_2(x')$ совпадает на множестве δ_i в силу его m-регулярности с одной из функций от переменных $(x_1, \ldots, x_m)$, и, поэтому, с одной стороны, в силу φ-универсальности множества G_1 функция g совпадает на δ_i с суперпозицией вида $\varphi(g_1^{(1)}, \ldots, g_1^{(N)})$, внутренние функции которой принадлежат G_1, а с другой стороны, в силу d-универсальности множества G_2, функция g на δ_i может быть представлена в виде дизъюнкции $g_2^{(1)} \vee \ldots \vee g_2^{(N)}$ функций из G_2. Из свойств разбиения Δ следует, что на «хороших» компонентах δ_i указанная функция g совпадает с формулой $\varphi(x_{j_1}, \ldots, x_{j_N})$, где каждая переменная x_{j_v} моделирует на δ_i функцию $g_1^{(v)}$ при всех v, $v \in \{1, \ldots, N\}$. Кроме того, на «плохих» компонентах δ_i функция g представима в виде $x_{t_1}^{\sigma_1} \vee \ldots \vee x_{t_N}^{\sigma_N}$, где каждая функция $g_2^{(v)}$ моделируется на δ_i при помощи $x_{t_v}^{\sigma_v}$ при всех v, $v \in \{1, \ldots, N\}$.

Таким образом, на «хороших» компонентах разбиения Δ указанная функция $g \in P_2(x')$ реализуется формулой

$$\mathcal{F}_1(x_{j_1}, \ldots, x_{j_N}), \tag{2.8}$$

а на «плохих» компонентах этого разбиения она допускает реализацию формулой

$$x_{t_1}^{\sigma_1} \vee \ldots \vee x_{t_N}^{\sigma_N}, \tag{2.9}$$

которая имеет сложность $O(N)$ в силу линейной сложности функции d в базисе A и возможности реализовать прямое отрицание $\bar{x}_1$ в этом базисе.

Рассмотрим дизъюнктивное разложение функции $f(x', x'')$ по переменным группы x'' и его последующую модификацию на основе разбиения Δ:

$$f(x', x'') = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') f(x', \sigma'') = \bigvee_{i=1}^{2^{q-m}} \chi_i(x') \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') f(x', \sigma''), \tag{2.10}$$

где $\sigma'' = (\sigma_{q+1}, \ldots, \sigma_n)$, $K_{\sigma''}(x'') = x_{q+1}^{\sigma_{q+1}} \ldots x_n^{\sigma_n}$, а $\chi_i(x')$ — характеристическая функция компоненты δ_i, $i \in \{1, \ldots, 2^{q-m}\}$, то есть функция, равная 1 только на наборах множества δ_i.

Согласно этому разложению, построим формулу

$$\mathcal{F}'_f = \bigvee_{i=1}^{2^{q-m}} \mathfrak{A}_i(x') \cdot \mathcal{F}_{\mu_{n-q}}\left(x'', \Phi_0^{(i)}(x'), \ldots, \Phi_{2^{n-q}-1}^{(i)}(x')\right), \tag{2.11}$$

где для каждого i, $i \in \{1, \ldots, 2^{q-m}\}$, формула $\mathfrak{A}_i(x')$ — совершенная ДНФ, реализующая функцию $\chi_i(x')$, а формула $\Phi_j^{(i)}(x')$, $j \in \{0, \ldots, 2^{n-q} - 1\}$, реализует функцию $f(x', \sigma'')$ при $\nu(\sigma'') = j$ и имеет вид (2.8) в случае, когда компонента δ_i «хорошая», и (2.9) иначе.

Искомая формула $\mathcal{F}_f$ получается из формулы $\mathcal{F}'_f$ заменой элементов $y_1 \cdot y_2$, $y_1 \vee y_2$, $\bar{x}_1$ соответствующими им бесповторными формулами $\mathcal{F}_{\&}$, $\mathcal{F}_{\vee}$, $\mathcal{F}_{\neg}$. Заметим, что при этом итеративное отрицание не потребуется, так как в формуле $\mathcal{F}'_f$ все отрицания стоят над переменными.

Выберем значения параметров, удовлетворяющие всем условиям, и оценим сложность построенной формулы $\mathcal{F}_f$. Положим

$$m = \lceil 2 \log \log n \rceil, \quad s = \lceil \log n - 3 \log \log n \rceil,$$

и пусть N — минимальное натуральное число, удовлетворяющее введенным ограничениям. Заметим, что при этом

$$q = m + 3|G| \leqslant m + 6N \cdot 2^s = O\left(\frac{n}{\log^2 n}\right).$$

Сложность реализации всех ДНФ $\mathfrak{A}_i(x')$ не превосходит

$$O(2^q \cdot q) = O\left(\frac{2^n}{\log^2 n}\right),$$

так как каждая функция $\chi_i(x')$ обращается в единицу на 2^m наборах. Сложность реализации формулы $\mathcal{F}_{\mu_{n-q}}$ не превосходит, согласно лемме 22,

$$O(2^{n-q}) = O\left(\frac{2^n}{\log^2 n}\right).$$

Основная сложность формулы $\mathcal{F}_f$ — сложность реализации всех подформул вида $\Phi_j^{(i)}(x')$ на «хороших» компонентах разбиения Δ, — не превосходит величины

$$\rho_A \cdot N \cdot 2^{q-m} \cdot 2^{n-q} \sim \rho_A \cdot \frac{2^n}{\log n}.$$

Сложность всех аналогичных подформул для «плохих» компонент не больше, чем

$$O(N) \cdot 2^{n-m} \cdot (e_1)^{q-m} = O\left(\frac{2^n}{\log^2 n}\right).$$

Таким образом, $\mathcal{L}(\mathcal{F}_f) \sim \rho_A \cdot \frac{2^n}{\log n}$, что доказывает лемму. $\square$

Леммы 21 и 24 доказывают теорему 12, которая вместе с леммами 13, 14, 15, 18 доказывает результат об особенностях функции Шеннона для сложности формул в базисах из элементов с прямыми и итеративными входами, сформулированный во введении:

Теорема 6. *Для любой системы функций* A, $A \subseteq P_2(X \cup Y)$, *такой, что* $\delta(A) \in \{M, P_2(Y)\}$, *при* $n \to \infty$ *справедливо соотношение*

$$\mathcal{L}_A(n) \sim \rho_A \cdot \frac{2^n}{\log n}.$$

Для каждого δ, $\delta \in \{I, O, D, K, L\}$, *существует базис* A *такой, что* $\delta(A) = \delta$ *и при этом*

$$\mathcal{L}_A(n) = \Theta\left(2^n\right).$$

2.3 Асимптотические оценки высокой степени точности для некоторых базисов

В этом разделе продолжается исследование формул в специальных базисах A, $A \subseteq P_2(X \cup Y)$, таких, что $\delta(A) \in \{P_2(Y), M\}$, и приводится доказательство теорем 8 и 9, сформулированных во введении и содержащих оценки высокой степени точности функции Шеннона для сложности таких формул.

Разбиение D конечного множества называется *геометрическим* [31] *разбиением кратности* q *и высоты* h, если оно для каждого i, $i = 0, 1, \ldots, h-1$, содержит q компонент мощности 2^i и, возможно, включает в себя еще одну дополнительную компоненту. Известно [31], что энтропия такого разбиения удовлетворяет неравенству

$$H(D) \leqslant \log q + 5. \tag{2.12}$$

Пусть разбиение Δ получается в результате применения разбиения D' к одной из компонент Z_i разбиения $D = \{Z_1, \ldots, Z_d\}$, $i \in \{1, \ldots, d\}$. Тогда, по определению энтропии нетрудно показать, что

$$H(\Delta) = H(D) + \frac{|Z_i|}{|Z|} H(D'), \tag{2.13}$$

где $Z = Z_1 \cup \ldots \cup Z_d$.

Для любой формулы $\mathcal{F}$ будем называть её приведенным весом отношение $\frac{\mathcal{L}(\mathcal{F})}{R(\mathcal{F})-1}$.

Пусть $\mathcal{G}$ — формула, реализующая функцию из $P_2(X \cup Y)$. Будем говорить, что формула $\mathcal{F}$ является *надстройкой* над формулой $\mathcal{G}$, если $\mathcal{F}$ получена из $\mathcal{G}$ добавлением в неё некоторых элементов из A'' и присоединением их выходов к итеративным входам формулы $\mathcal{G}$.

Докажем следующее утверждение.

Лемма 25. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис функций, такой, что $\delta(\hat{A}) \in \{P_2(Y), M\}$. Тогда для любого натурального N, $N \geqslant 1$, найдется* *формула $\mathcal{F}^{(N)}$ в базисе A, реализующая функцию от $N + O(1)$ переменных, имеющую селекторное разбиение D этих переменных с энтропией $H(D) = O(1)$, и для которой справедливо соотношение*

$$R(\mathcal{F}^{(N)}) \leqslant \frac{1}{\rho_A}\mathcal{L}(\mathcal{F}^{(N)}) + 1. \tag{2.14}$$

Доказательство. Так как $M \subseteq \delta(\hat{A})$, то существуют бесповторные формулы $\mathcal{F}_1$ и $\mathcal{F}_2$ над $\hat{A}$, такие, что подстановками констант из них можно получить функции y_1y_2 и $y_1 \vee y_2$ соответственно.

Рассмотрим формулу $\mathcal{F}_1$ и построим формулу $\mathcal{F}_1''$ в виде цепи из всех элементов формулы $\mathcal{F}_1$, соединенных через один из итеративных входов. Так как $\hat{A} \subseteq A'$, то каждый такой элемент имеет хотя бы один итеративный вход. Заметим, что число итеративных входов в формуле $\mathcal{F}_1''$ совпадает с числом итеративных входов $\mathcal{F}_1$. Дополним каждый элемент построенной таким образом линейной суперпозиции, имеющий приведенный вес больший, чем ρ_A, до соответствующего ему минимального канонического макроблока элементами $\mathcal{E}_{i_1}^{(1)}, \ldots, \mathcal{E}_{i_p}^{(1)} \in A''$, взятыми от различных в совокупности прямых переменных, где $b' < i_1, \ldots, i_p \leqslant b$, а число $p+1$ равно числу «свободных» итеративных входов дополняемых до макроблоков элементов $\hat{A}$, участвующих в формуле $\mathcal{F}_1''$. Таким образом, приведенный вес формулы $\mathcal{F}_1''$ равен ρ_A.

Присоединим элементы $\mathcal{E}_{i_2}^{(1)}, \ldots, \mathcal{E}_{i_p}^{(1)}$ к произвольным итеративным входам формулы $\mathcal{F}_1$, кроме входов y_1 и y_2, построив таким образом формулу $\mathcal{F}_1'$, являющуюся надстройкой формулы $\mathcal{F}$. При этом при подстановке вместо любого из входов y_1 или y_2 выхода элемента $\mathcal{E}_{i_1}^{(1)}$ приведенный вес такой формулы будет совпадать с ρ_A, так как в этом случае её сложность и ранг будут равны сложности и рангу формулы $\mathcal{F}_1''$ соответственно.

Аналогичной надстройкой над формулой $\mathcal{F}_2$ при помощи элементов $\mathcal{E}_{i_2}^{(2)}, \ldots, \mathcal{E}_{i_q}^{(2)}$, выходы которых подсоединены к произвольным итеративным входам формулы $\mathcal{F}_2$, кроме входов y_1 и y_2, построим формулу $\mathcal{F}_2'$, и пусть $\mathcal{E}_{i_1}^{(2)}$

— элемент, аналогичный элементу $\mathcal{E}_{i_1}^{(1)}$ для случая формулы $\mathcal{F}_1$, а именно, при подстановке его вместо одного из итеративных входов формулы $\mathcal{F}_2'$ получается формула, имеющая приведенный вес ρ_A.

Следует отметить, что в том случае, когда множество $\hat{A}$ состоит только из элементов A' с минимальным приведенным весом, формулы $\mathcal{F}_1'$ и $\mathcal{F}_2'$ совпадают с формулами $\mathcal{F}_1$ и $\mathcal{F}_2$ соответственно.

Будем считать, что формулы $\mathcal{F}_1'$ и $\mathcal{F}_2'$ реализуют функции, существенно зависящие от p_1 и p_2 переменных соответственно. Пусть, без ограничения общности,

$$\mathcal{F}_1'(\tilde{\alpha}, y_1, y_2) = y_1 y_2,$$

$$\mathcal{F}_2'(\tilde{\beta}, y_1, y_2) = y_1 \vee y_2,$$

где $\tilde{\alpha} \in B^{p_1-2}$, $\tilde{\beta} \in B^{p_2-2}$. Пусть, далее, Ψ — формула над A вида

$$\mathcal{F}_2'\left(\tilde{z}^{(1)}, \mathcal{F}_1'(\tilde{z}^{(2)}, y_1, y_3), \mathcal{F}_1'(\tilde{z}^{(3)}, y_2, y_4)\right),$$

где $\tilde{z}^{(1)}$, $\tilde{z}^{(2)}$, $\tilde{z}^{(3)}$ — наборы из различных в совокупности переменных из $X \cup Y$ длины $(p_2 - 2)$, $(p_1 - 1)$ и $(p_1 - 1)$ соответственно. Функцию, реализуемую формулой Ψ, обозначим через $\psi(\tilde{z}, y_1, y_2, y_3, y_4)$, где набор $\tilde{z}$ содержит p_2+2p_1-4 переменных.

Нетрудно видеть, что $\psi(\tilde{\beta}, \tilde{\alpha}, \tilde{\alpha}, y_1, y_2, y_3, y_4) = y_1 y_3 \vee y_2 y_4$, и что функция ψ имеет нетривиальное селекторное разбиение множества своих переменных, содержащее переменные y_3 и y_4 в одной из своих компонент.

Все дальнейшие формулы в доказательстве этой леммы будем строить так, чтобы каждая переменная входила в каждую формулу не более одного раза.

Построим формулу Ψ' добавлением к формуле Ψ двух элементов $\mathcal{E}_{i_1}^{(1)}$ и присоединением их выходов ко входам, соответствующим итеративным переменным y_1 и y_2. Заметим, что при добавлении к формуле Ψ' элемента $\mathcal{E}_{i_1}^{(2)}$ и подсоединении его выхода ко входу y_3 или y_4 приведенный вес полученной формулы будет равен ρ_A. В случае, когда множество $\hat{A}$ состоит только из элементов A' с минимальным приведенным весом, положим $\Psi' = \Psi$.

Пусть $\psi'(\tilde{z}, y_3, y_4)$ — функция, реализуемая формулой Ψ', где $\tilde{z}$ — набор переменных из $X \cup Y$ длины $(r-1)$. Она, так же, как и функция ψ, имеет нетривиальное селекторное разбиение множества своих переменных, содержащее переменные y_3 и y_4 в одной из своих компонент. Это, в частности, означает, что если $\mathcal{G}$ — произвольная формула над A, реализующая функцию от v переменных из $X \cup Y$, а формула $\mathcal{G}'$ получена присоединением двух формул $\mathcal{G}(z'_1, \dots, z'_v)$ и $\mathcal{G}(z''_1, \dots, z''_v)$ ко входам y_3 и y_4 формулы Ψ', то разбиение, содержащее компоненты $\{z'_i, z''_i\}$ для всех $i = 1, \dots, v$, и по одной компоненте на каждую из остальных переменных формулы Ψ', является селекторным для реализуемой формулой $\mathcal{G}'$ функции.

Построим для каждого t, $t = 1, 2, \dots$, формулу $\mathcal{G}^{(t)}$ в базисе A из s_t формул Ψ', соединенных между собой через итеративные входы y_3, y_4 в h_t-ярусное двоичное дерево, содержащее полное $(h_t - 1)$-ярусное поддерево, $s_t = \lceil (t-1)/r \rceil$, $h_t = \lceil \log(s_t + 1) \rceil$. Для каждого $t = 1, 2, \dots$ формула $\mathcal{G}^{(t)}$ реализует функцию, существенно зависящую от не менее, чем t переменных.

Пусть $\mathcal{F}^{(t)}$ — формула, получаемая надстройкой над формулой $\mathcal{G}^{(t)}$ при помощи присоединения s_t элементов вида $\mathcal{E}^{(2)}_{i_1}$ к произвольным итеративным входам формулы $\mathcal{G}^{(t)}$. Таким образом, приведенный вес формулы $\mathcal{F}^{(t)}$ равен ρ_A. Функцию, реализуемую этой формулой, обозначим через φ_t.

Пусть для каждого i, $i = 1, \dots, h_t - 1$, $Z^{(i)}_j$ — множество тех переменных функции φ_t, которые связаны с j-ми входами подформул Ψ' на i-ом ярусе, $j = 1, \dots, r-1$. Множество всех остальных переменных функции φ_t обозначим Z_{h_t}. Разбиение

$$\hat{D} = \{Z^{(i)}_j \,|\, i = 1, \dots, h_t - 1,\ j = 1, \dots, r-1\} \cup Z_{h_t}$$

множества переменных функции φ_t является геометрическим разбиением кратности $r-1$ и высоты $h_t - 1$, так как для каждого $i = 0, \dots, h_t - 2$ оно содержит $r-1$ компонент мощности 2^i и еще одну компоненту Z_{h_t}.

В множество Z_{h_t} входят прямые переменные подформул Ψ' h_t-го уровня формулы $\mathcal{F}^{(t)}$, а также прямые переменные присоединенных при переходе от формулы $\mathcal{G}^{(t)}$ к формуле $\mathcal{F}^{(t)}$ элементов вида $\mathcal{E}^{(2)}_{i_1}$. У этого множества аналогичным образом существует разбиение D' на не более, чем $r+q$ подмножеств, где q — число входов элемента $\mathcal{E}^{(2)}_{i_1}$. Величина $r+q$ зависит только от базиса, а, следовательно, энтропия $H(D') = O(1)$.

Подразбиением компоненты Z_{h_t} при помощи D' построим из $\hat{D}$ разбиение D, энтропия которого, согласно (2.13) и (2.12), ограничена константой, и которое, как нетрудно видеть, также является селекторным.

Для завершения доказательства остается заметить, что для любого натурального числа N число t можно выбрать так, что формула $\mathcal{F}^{(t)}$ реализует функцию, зависящую от $N+O(1)$ переменных. $\square$

Лемма 26. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис функций, такой, что множество $\hat{A}$ является полным. Тогда для любого натурального N, $N \geqslant 1$, найдется формула $\mathcal{F}^{(N)}$ в базисе A, реализующая функцию от $N+O(1)$ переменных, имеющую селекторное разбиение D этих переменных с энтропией $H(D) = O(1)$, и для которой справедливо соотношение (2.14).*

Доказательство. Как показано в [37], если $\hat{A}$ — полная система функций, то существует бесповторная формула $\mathcal{F}$ над $\hat{A}$, которая при подстановке констант в неё реализует функцию вида $x_1^\sigma y_1 \oplus x_2^\sigma y_2$ ($x_1^\sigma y_1 \vee x_2^\sigma y_2$, $(x_1^\sigma \vee y_1) \cdot (x_2^\sigma \vee y_2)$), $\sigma \in B$, в случае $\delta(A) = L$ (соответственно, $\delta(A) = D$, $\delta(A) = K$), и либо функцию $\mu_1(x_1, y_1, y_2)$, либо функцию $g(x_1, x_2, y_1, y_2)$, удовлетворяющую условию $g(x_1, \bar{x}_1, y_1, y_2) = \mu_1(x_1, y_1, y_2)$, в остальных случаях. Каждая такая функция имеет селекторное разбиение, содержащее в одной из своих компонент обе переменные y_1, y_2.

Как следует из доказательства леммы 25, существует надстройка Ψ' формулы $\mathcal{F}$ в базисе A, реализующая функцию от двух итеративных переменных y_1,

y_2, и элемент $\mathcal{E} \in A''$ такой, что приведенный вес формулы Ψ' при присоединении к одному из её входов y_1 или y_2 элемента $\mathcal{E}$ равен ρ_A. Реализуемая этой надстройкой функция имеет нетривиальное селекторное разбиение множества своих переменных, содержащее переменные y_1 и y_2 в одной из своих компонент.

Для доказательства леммы необходимо повторить ход рассуждений и построения, проведенные в лемме 25, для формулы Ψ', полагая в этом доказательстве $\mathcal{E}_{i_2}^{(2)} = \mathcal{E}$. □

Лемма 27. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис функций, такой, что $\delta(\hat{A}) \in \{L, D, K\}$, и множество $[\hat{A}]_{\{1,3,4\}}$ содержит функцию вида*

$$f = (\varphi_1 \circ y_1) \diamond \ldots \diamond (\varphi_k \circ y_k) \diamond \varphi_0,$$

где $\varphi_0, \varphi_1, \ldots, \varphi_k \in P_2(X)$, $(\circ, \diamond) \in \{(\&, \vee), (\vee, \&), (\&, \oplus)\}$, для которой найдутся такие индексы $j_1, j_2 \in \{1, \ldots, k\}$, $j_1 \neq j_2$, и наборы α, β значений прямых переменных, что

$$\varphi_{j_1}(\alpha) = \overline{\varphi_{j_1}(\beta)} = \varphi_{j_2}(\beta) = \overline{\varphi_{j_2}(\alpha)} = 0.$$

Тогда для любого натурального N, $N \geqslant 1$, найдется формула $\mathcal{F}^{(N)}$ в базисе A, реализующая функцию от $N + O(1)$ переменных, имеющую селекторное разбиение D этих переменных с энтропией $H(D) = O(1)$, и для которой справедливо соотношение (2.14).

Доказательство. Доказательство этой леммы аналогично доказательству леммы 26, так как:

1. для функции f существует селекторное разбиение множества её переменных, содержащее переменные y_{j_1} и y_{j_2} в одной из своих компонент;

2. операции 1, 3 и 4 для формул с минимальным приведенным весом дают формулу минимального приведенного веса.

$\square$

Лемма 28. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис функций, такой, что $\delta(A) \supseteq M$, и справедливо хотя бы одно из следующих утверждений:*

1. $\delta(\hat{A}) \supseteq M$;

2. *базис $\hat{A}$ является полным базисом;*

3. $\delta(\hat{A}) \in \{L, D, K\}$, *а множество $[\hat{A}]_{\{1,3,4\}}$ содержит функцию f вида*

$$f = (\varphi_1 \circ y_1) \diamond \ldots \diamond (\varphi_k \circ y_k) \diamond \varphi_0,$$

где $\varphi_0, \varphi_1, \ldots, \varphi_k \in P_2(X)$, $(\circ, \diamond) \in \{(\&, \vee), (\vee, \&), (\&, \oplus)\}$, для которой найдутся такие индексы $j_1, j_2 \in \{1, \ldots, k\}$, $j_1 \neq j_2$, и наборы α, β значений прямых переменных, что

$$\varphi_{j_1}(\alpha) = \overline{\varphi_{j_1}(\beta)} = \varphi_{j_2}(\beta) = \overline{\varphi_{j_2}(\alpha)} = 0.$$

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

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

Доказательство. Согласно леммам 25–27, для $N = 1, 2, \ldots$ существует формула $\mathcal{F}^{(N)}$ в базисе A, которая реализует функцию от N переменных, имеющую селекторное разбиение D этих переменных с энтропией $H(D) = O(1)$, при этом справедливо соотношение

$$\mathcal{L}(\mathcal{F}^{(N)}) = \rho_A \cdot N + O(1). \tag{2.15}$$

Как было указано, для функций $y_1 y_2$, $y_1 \vee y_2$ существуют реализующие их формулы $\mathcal{F}_\&$ и $\mathcal{F}_\vee$ в базисе A соответственно, бесповторные по своим существенным переменным. Рассмотрим бесповторную формулу

$$\Psi' = \mathcal{F}_\vee \left(\mathcal{F}_\&(y_1, y_3), \mathcal{F}_\&(y_2, y_4)\right),$$

реализующую функцию $y_1 y_3 \vee y_2 y_4$. Напомним, что для этой функции существует нетривиальное селекторное разбиение её переменных на подмножества $\{y_3, y_4\}$, $\{y_1\}$ и $\{y_2\}$.

Аналогично формулам вида $\mathcal{G}^{(t)}$ из доказательства леммы 25 для каждого $t = 1, 2, \ldots$ построим формулу $\hat{\mathcal{F}}^{(t)}$ из s'_t формул Ψ', соединив их между собой через два итеративных входа y_3, y_4 в h'_t-ярусное двоичное дерево, содержащее полное $(h'_t - 1)$-ярусное поддерево, где $s'_t = \lceil (t-1)/2 \rceil$, $h'_t = \lceil \log(s'_t + 1) \rceil$. Аналогично лемме 25, для реализуемой формулой $\hat{\mathcal{F}}^{(t)}$ функции существует селекторное разбиение D' её переменных с энтропией $H(D') = O(1)$. Для сложности построенной формулы справедливо равенство

$$\mathcal{L}(\hat{\mathcal{F}}^{(t)}) = O(t). \tag{2.16}$$

Введем натуральные параметры m, q, s, N такие, что

$$1 \leqslant m < q < n,$$

и пусть $x' = (x_1, \ldots, x_q)$, $x'' = (x_{q+1}, \ldots, x_n)$. Пусть, далее, φ — функция, реализуемая формулой $\mathcal{F}^{(N)}$, а φ' — функция, реализуемая формулой $\hat{\mathcal{F}}^{(N)}$. Считая, что

$$N(s - \max\{H(D), H(D')\}) \geqslant 2^m,$$

построим по лемме 1 φ-универсальное множество G_1 порядка m и φ'-универсальное множество G_2 порядка m так, что функции из этих множеств зависят от одних и тех же переменных $(x_1, \ldots, x_m)$, и при этом $|G| \leqslant 2^{s+3}$, где $G = G_1 \cup G_2$.

Положим $q = m + 3|G|$, где $G = G_1 \cup G_2$, и построим по лемме 3 разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q на m-регулярные компоненты, в котором доля «плохих» компонент не превосходит e_1^{q-m}, $e_1 < 1$, и которое моделирует все функции из множества G с помощью переменных или их отрицаний.

Повторяя рассуждения из доказательства леммы 24, получим, что на «хороших» компонентах разбиения Δ любая функция $g \in P_2(x')$ реализуется формулой вида

$$\mathcal{F}^{(N)}(x_{j_1}, \ldots, x_{j_N}), \tag{2.17}$$

сложность которой удовлетворяет соотношению (2.15), а на «плохих» компонентах этого разбиения функция g допускает реализацию формулой вида

$$\hat{\mathcal{F}}^{(N)}(x_{t_1}^{\sigma_1}, \ldots, x_{t_N}^{\sigma_N}), \tag{2.18}$$

которая имеет сложность $O(N)$ в силу (2.16) и возможности реализации прямого отрицания в базисе A.

Рассмотрим разложение (2.10) функции $f(x', x'')$ по переменным группы x'' на основе разбиения Δ. Согласно этому разложению построим формулу (2.11) $\mathcal{F}'_f$, в которой, как и в доказательстве леммы 24, формула $\mathfrak{A}_i(x')$ — совершенная ДНФ, реализующая функцию $\chi_i(x')$ для каждого i, $i \in \{1, \ldots, 2^{q-m}\}$, а формула $\Phi_j^{(i)}(x')$, $j \in \{0, \ldots, 2^{n-q} - 1\}$, реализует функцию $f(x', \sigma'')$ при $\nu(\sigma'') = j$ и имеет вид (2.17) в случае, когда компонента δ_i «хорошая» и (2.18) иначе.

Искомая формула $\mathcal{F}_f$ получается из формулы $\mathcal{F}'_f$ заменой элементов $y_1 \cdot y_2$, $y_1 \vee y_2$, $\bar{x}_1$ соответствующими им бесповторными формулами $\mathcal{F}_{\&}$, $\mathcal{F}_{\vee}$, $\mathcal{F}_{\neg}$.

Положим

$$m = \lceil 2 \log \log n \rceil, \quad s = \lceil \log n - 7 \rceil,$$

и пусть N — минимальное натуральное число, удовлетворяющее всем введенным ограничениям. При этом

$$q = m + 3|G| \leqslant m + 3 \cdot 2^{s+3} \lesssim \frac{n}{2}.$$

Так же как и в конструкции леммы 24, основная сложность формулы $\mathcal{F}_f$ заключается в реализации подформул для остаточных функций $f(x', \sigma'')$ на «хороших» компонентах разбиения Δ. Указанная сложность не превосходит величины

$$\rho_A \cdot N \cdot 2^{q-m} \cdot 2^{n-m} \leqslant \rho_A \cdot \frac{2^n}{s - \max\{H(D), H(D')\}} = \rho_A \frac{2^n}{\log n} \left(1 + O\left(\frac{1}{\log n}\right)\right).$$

Таким образом,

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

что и доказывает лемму. □

Леммы 21 и 28 устанавливают асимптотические оценки высокой степени точности функции Шеннона для сложности формул в рассматриваемой модели:

Теорема 8. *Пусть A, $A \subseteq P_2(X \cup Y)$, — конечный полный базис, такой, что $\delta(A) \supseteq M$. Пусть, далее, справедливо хотя бы одно из следующих утверждений:*

1. $\delta(\hat{A}) \supseteq M$*;*

2. *базис $\hat{A}$ является полным базисом;*

3. $\delta(\hat{A}) \in \{L, D, K\}$*, множество $[\hat{A}]_{\{1,3,4\}}$ содержит функцию f вида*

$$f = (\varphi_1 \circ y_1) \diamond \ldots \diamond (\varphi_k \circ y_k) \diamond \varphi_0,$$

где $\varphi_0, \varphi_1, \ldots, \varphi_k \in P_2(X)$, $(\circ, \diamond) \in \{(\&, \vee), (\vee, \&), (\&, \oplus)\}$, для которой найдутся такие индексы $j_1, j_2 \in \{1, \ldots, k\}$, $j_1 \neq j_2$, и наборы α, β значений прямых переменных, что

$$\varphi_{j_1}(\alpha) = \overline{\varphi_{j_1}(\beta)} = \varphi_{j_2}(\beta) = \overline{\varphi_{j_2}(\alpha)} = 0.$$

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

$$\mathcal{L}_A(n) = \rho_A \cdot \frac{2^n}{\log n} \left(1 \pm \frac{O(1)}{\log n}\right). \qquad (2.19)$$

Далее докажем оценки функции Шеннона высокой степени точности с другим поведением остаточного члена для случая специальных базисов, являющихся итеративными модификациями стандартного базиса:

Теорема 9. *Пусть*

$$Б_1 = \{y_1 \cdot \ldots \cdot y_{k_1}, x_1 \vee \ldots \vee x_{k_2}, \bar{y}_1\};$$

$$Б_2 = \{y_1 \vee \ldots \vee y_{k_1}, x_1 \cdot \ldots \cdot x_{k_2}, \bar{y}_1\};$$

где $k_1, k_2 \geqslant 2$. *Тогда для* $i = 1, 2$ *имеют место следующие неравенства:*

$$\rho_{Б_i} \frac{2^n}{\log n} \left(1 + \frac{\frac{1}{k_2} \log\log n \pm O(1)}{\log n}\right) \leqslant \mathcal{L}_{Б_i}(n) \leqslant \rho_{Б_i} \frac{2^n}{\log n} \left(1 + \frac{\log\log n \pm O(1)}{\log n}\right).$$

Если при этом минимальный приведенный вес базиса $Б_i$, $i \in \{1, 2\}$, *достигается на макроблоке, отличном от элемента, то справедливо соотношение:*

$$\mathcal{L}_{Б_i}(n) = \rho_{Б_i} \frac{2^n}{\log n} \left(1 + \frac{\frac{1}{k_2} \log\log n \pm O(1)}{\log n}\right).$$

Для доказательства нижней оценки потребуется следующее утверждение.

Лемма 29 ([36]). *Если* a, m, τ, α — *действительные параметры такие, что*

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

то выполняется неравенство

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

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

Лемма 30. *Найдется такая константа* c, $c > 0$, *что при любых натуральных* n *и* $\mathcal{L}$ *число попарно не эквивалентных формул в базисе* $Б_1$, *реализующих функции от* n *переменных и имеющих сложность не большую, чем* $\mathcal{L}$, *не превосходит*

$$\left(\frac{cn}{\sqrt[k_2]{\log n}}\right)^{\mathcal{L}/\rho_{Б_1}}.$$

Доказательство. Обозначим за L_1 вес элемента, реализующего функцию $y_1 \cdot \ldots \cdot y_{k_1}$, за L_2 — вес элемента $x_1 \vee \ldots \vee x_{k_2}$, за L_3 — вес элемента $\bar{y}_1$. Рассмотрим произвольную формулу $\mathcal{F}$ в базисе Б$_1$, имеющую сложность $\mathcal{L}$ и содержащую

l_1 элементов конъюнкции, l_2 элементов дизъюнкции и l_3 элементов отрицания. Сложность этой формулы равна $\mathcal{L}(\mathcal{F}) = L_1 l_1 + L_2 l_2 + L_3 l_3 = \mathcal{L}$, а её ранг — $R(\mathcal{F}) = l_1(k_1 - 1) + l_2(k_2 - 1) + 1$.

Пусть $\mathcal{F}'$ — формула, полученная из $\mathcal{F}$ удалением всех элементов отрицания. Тогда $R(\mathcal{F}') = R(\mathcal{F})$, а $\mathcal{L}(\mathcal{F}') = \mathcal{L}(\mathcal{F}) - L_3 l_3$. При этом для формулы $\mathcal{F}'$ справедливо соотношение (2.7): $\mathcal{L}(\mathcal{F}') \geqslant \rho_{Б_1} R(\mathcal{F}') - O(1)$. Следовательно, $\mathcal{L}(\mathcal{F}) \geqslant \rho_{Б_1} R(\mathcal{F}) + L_3 l_3 - O(1)$. Таким образом, найдется такая константа c_1, $c_1 > 0$, что

$$R(\mathcal{F}) \leqslant \frac{1}{\rho_{Б_1}}(\mathcal{L} - L_3 l_3 + c_1). \tag{2.20}$$

Разобьем все входы формулы $\mathcal{F}$, подающиеся на элементы, реализующие конъюнкцию, и выходы элементов, реализующих дизъюнкции, на не более, чем $(l_3{+}1)$ групп, каждая из которых связана через цепь конъюнкций либо с выходом $\mathcal{F}$, либо с некоторым элементом отрицания. Число способов выбора дерева формулы $\mathcal{F}$ и расположения элементов в его узлах не превосходит $c_2^{\mathcal{L}}$, где $c_2 = \mathrm{const}$, $c_2 > 0$. Такой выбор однозначно определяет указанное разбиение. Пусть количество групп в разбиении есть m, $m \leqslant l_3 + 1$, а в каждой i-ой группе в точности t_i листьев и s_i выходов элементов дизъюнкции. Тогда число входов формулы, соответствующее i-ой группе, равно $t_i + k_2 s_i$. Положим $s = s_1 + \ldots + s_m$, $t = t_1 + \ldots + t_m$, и заметим, что $R(\mathcal{F}) = t + k_2 s$.

Количество способов пометки листьев формулы символами булевых переменных из $\{x_1, \ldots, x_n\}$ не превосходит величины

$$\max_{t_i, s_i} \left\{ \mathrm{C}_n^{t_1} \cdot \mathrm{C}_{\mathrm{C}_n^{k_2}}^{s_1} \cdots \mathrm{C}_n^{t_m} \cdot \mathrm{C}_{\mathrm{C}_n^{k_2}}^{s_m} \right\} \leqslant \max_{t_i, s_i} \frac{(c_3 n)^{t_1 + \ldots + t_m + k_2 s_1 + k_2 s_m}}{t_1^{t_1} \cdots t_m^{t_m} \cdot s_1^{s_1} \cdots s_m^{s_m}}, \tag{2.21}$$

так как $\mathrm{C}_{\mathrm{C}_n^{k_2}} \leqslant \left(\frac{c_3 n^{k_2}}{s}\right)^s$, где $c_3 = \mathrm{const}, c_3 > 0$. Из выпуклости функции $x \ln x$ действительного переменного x следует, что

$$t_1^{t_1} \cdots t_m^{t_m} \cdot s_1^{s_1} \cdots s_m^{s_m} \geqslant \left(\frac{t+s}{2m}\right)^{t+s},$$

поэтому выражение (2.21) не больше, чем

$$\frac{(c_3 n)^{R(\mathcal{F})}}{\left(\frac{t+s}{2m}\right)^{t+s}}.$$

Заметим, что $t+s = R(\mathcal{F}) - (k_2-1)s = R(\mathcal{F}) - (k_2-1)l_2 = l_1(k_1-1)+1$.

Покажем, что найдется константа c_4, $c_4 > 0$, такая, что

$$\left(\frac{l_3}{l_1(k_1-1)+1}\right)^{R(\mathcal{F})-(k_2-1)l_2} \leqslant \left(\frac{c_4 l_3}{\mathcal{L} - L_3 l_3}\right)^{\frac{R(\mathcal{F})}{k_2}}. \tag{2.22}$$

Предварительно заметим, что $\mathcal{L} - L_3 l_3 = L_1 l_1 + L_2 l_2 \leqslant c_5 l_1$, (так как $l_2 \leqslant (k_1-1)l_1+1$), где $c_5 = \text{const}$, $c_5 > 0$, а также, что $l_3 \leqslant c_6 l_1$, считая, что два подряд идущих отрицания не встречаются в рассматриваемых формулах, $c_6 = \text{const}$, $c_6 > 0$. Тогда, обозначая для краткости $R = R(\mathcal{F})$,

$$\begin{aligned} l_3^{R-(k_2-1)l_2} \cdot (\mathcal{L} - L_3 l_3)^{\frac{R}{k_2}} &\leqslant (l_3)^{\frac{R}{k_2}} \cdot (l_3)^{\frac{R(k_2-1)}{k_2}-(k_2-1)l_2} \cdot (c_5 l_1)^{\frac{R}{k_2}} \leqslant \\ &\leqslant (c_5 l_3)^{\frac{R}{k_2}} (c_6 l_1)^{\frac{R(k_2-1)}{k_2}-(k_2-1)l_2} \cdot (l_1)^{\frac{R}{k_2}} \leqslant \\ &\leqslant (c_5 c_6^{k_2-1} l_3)^{\frac{R}{k_2}} \cdot (l_1(k_1-1)+1)^{R-(k_2-1)l_2}, \end{aligned}$$

что доказывает неравенство (2.22).

Таким образом, так как $m \leqslant l_3 + 1$,

$$\begin{aligned} \frac{(c_3 n)^{R(\mathcal{F})}(2m)^{t+s}}{(t+s)^{t+s}} &\leqslant (c_7 n)^{R(\mathcal{F})} \cdot \left(\frac{l_3}{l_1(k_1-1)+1}\right)^{R(\mathcal{F})-(k_2-1)l_2} \leqslant \\ &\leqslant (c_7 n)^{R(\mathcal{F})} \cdot \left(\frac{c_4 l_3}{\mathcal{L} - L_3 l_3}\right)^{\frac{R(\mathcal{F})}{k_2}} \leqslant \\ &\leqslant \left(\frac{c_8 l_3 n^{k_2}}{\mathcal{L} - L_3 l_3}\right)^{\frac{R(\mathcal{F})}{k_2}} \leqslant \left(\frac{c_8 l_3 n^{k_2}}{\mathcal{L} - L_3 l_3}\right)^{\frac{1}{k_2 \rho_{Б_1}}(\mathcal{L} - L_3 l_3 + c_1)}, \end{aligned}$$

где c_7, c_8 — положительные константы, а последнее неравенство справедливо в силу (2.20). Воспользуемся леммой 29 при $y = \frac{L_3 l_3 - c_1}{\rho_{Б_1} k_2}$, $\tau = 1$, $\alpha = 0$, $a = n^{k_2}$, $m = \frac{\mathcal{L}}{\rho_{Б_1} k_2}$. Тогда число попарно не эквивалентных формул в рассматриваемом базисе, сложность которых не превосходит $\mathcal{L}$, и которые реализуют функции от n переменных, может быть оценено сверху как

$$\left(\frac{c_9 n^{k_2}}{\log n^{k_2}}\right)^{\frac{\mathcal{L}}{\rho_{Б_1} k_2}} \leqslant \left(\frac{cn}{\sqrt[k_2]{\log n}}\right)^{\frac{\mathcal{L}}{\rho_{Б_1}}}.$$

Здесь c_9 и c — положительные константы. Лемма доказана. $\square$

Записав мощностное неравенство

$$2^{2^n} \leqslant \left(\frac{cn}{\sqrt[k_2]{\log n}}\right)^{\frac{\mathcal{L}_{\text{Б}_1}(n)}{\rho_{\text{Б}_1}}},$$

получим, что при достаточно больших n справедливо соотношение

$$\mathcal{L}_{\text{Б}_1}(n) \geqslant \rho_{\text{Б}_1} \frac{2^n}{\log n}\left(1 + \frac{\frac{1}{k_2}\log\log n - O(1)}{\log n}\right).$$

Лемма 31. *Для любой функции f, $f \in P_2(n)$, существует формула $\mathcal{F}_f$ в базисе $Б_1$, реализующая эту функцию, и такая, что*

$$\mathcal{L}(\mathcal{F}_f) \leqslant \rho_{Б_1} \frac{2^n}{\log n}\left(1 + \frac{\alpha \log\log n + O(1)}{\log n}\right), \tag{2.23}$$

где $\alpha = 1$, если приведенный вес базиса $Б_1$ достигается только на элементе, реализующем функцию $y_1 \cdot \ldots \cdot y_{k_1}$, и $\alpha = \frac{1}{k_2}$ в случае, когда приведенный вес базиса достигается на макроблоке, отличном от элемента.

Доказательство. Рассмотрим сначала случай, когда приведенный вес базиса Б_1 достигается на макроблоке, отличном от элемента. Воспользуемся методом, приведенным в доказательстве леммы 28. Как следует из этого доказательства, для построения искомой формулы $\mathcal{F}_f$ достаточно для каждого натурального N построить формулу $\mathcal{F}^{(N)}$ в базисе Б_1, реализующую функцию φ от N прямых переменных со сложностью

$$\mathcal{L}(\mathcal{F}^{(N)}) = \rho_{\text{Б}_1} N + O(1),$$

где функция φ имеет селекторное разбиение D своих переменных с энтропией, удовлетворяющей неравенству

$$H(D) \leqslant \frac{1}{k_2}\log N + O(1).$$

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

$$\mathcal{F}^{(N)} = (x_1 \vee \ldots \vee x_{k_2})(x_{k_2+1} \vee \ldots \vee x_{2k_2}) \cdot \ldots \cdot (x_{(p-1)k_2+1} \vee \ldots \vee x_{pk_2}) x_{pk_2+1} \ldots x_N.$$

Нетрудно видеть, что разбиение D, состоящее из множеств

$$
\begin{aligned}
&\{x_1\}, \{x_{k_2+1}\}, \ldots, \{x_{(p-1)k_2+1}\},\\
&\{x_2,\, x_{k_2+2}, \ldots, x_{(p-1)k_2+2}\},\\
&\ldots\\
&\{x_{k_2},\, x_{2k_2}, \ldots, x_{pk_2}\},\\
&\{x_{pk_2+1}\}, \{x_{pk_2+2}\}, \ldots, \{x_N\};
\end{aligned}
$$

является селекторным разбиением множества переменных реализуемой формулой $\mathcal{F}^{(N)}$ функции. Энтропия этого разбиения имеет вид

$$H(D) = (p+k_2)\frac{1}{N}\log N + (k_2-1)\frac{p}{N}\log\frac{N}{p} = \frac{1}{k_2}\log N + O(1).$$

Так как приведенный вес базиса достигается на макроблоках, то соответствующий минимальный макроблок состоит из элемента, реализующего конъюнкцию, и (k_1-1) элементов дизъюнкции, поэтому

$$\rho_{\text{Б}_1} = \frac{L_1 + L_2(k_1-1)}{k_2(k_1-1)}.$$

В формулу $\mathcal{F}^{(N)}$ входит p элементов дизъюнкции и $\lfloor\frac{p}{k_1-1}\rfloor + O(1)$ элементов конъюнкции. Тогда, сохраняя обозначения леммы 30, сложность формулы $\mathcal{F}^{(N)}$ удовлетворяет соотношению

$$\mathcal{L}(\mathcal{F}^{(N)}) = pL_2 + \frac{p}{k_1-1}L_1 + O(1) = \frac{p(k_1-1)L_2 + pL_1}{k_1-1} + O(1) = \rho_{\text{Б}_1}N + O(1).$$

Будем использовать для произвольной функции f, $f \in P_2(n)$, то же разложение, что и в лемме 28, моделируя дизъюнкции на «плохих» компонентах разбиения и дизъюнкции вне формул вида $\mathcal{F}^{(N)}$ при помощи конъюнкций и отрицаний. Основная сложность получаемой формулы при выборе тех же значений параметров останется по-прежнему в реализации подформул для функции φ на «хороших» компонентах и будет составлять $\rho_{\text{Б}_1}\cdot\frac{2^n}{s-H(D)}$, где s — параметр из доказательства леммы 28. В результате будем иметь оценку (2.23) при $\alpha = \frac{1}{k_2}$.

Доказательство этой оценки с $\alpha = 1$ для случая, когда приведенный вес базиса Б$_1$ достигается только на элементе, реализующем функцию $y_1 \cdot \ldots \cdot y_{k_1}$, аналогично. Отличие состоит в том, что в качестве формулы $\mathcal{F}^{(N)}$ необходимо взять формулу $x_1 \ldots x_N$ и тривиальное разбиение $D = \{\{x_1\}, \ldots, \{x_n\}\}$ множества переменных реализуемой этой формулой функции, энтропия которого равна $\log N$. Эта оценка верна и в первом случае.

Лемма доказана. $\square$

Заметим, что леммы 30 и 31 остаются справедливыми и для случая базиса Б$_2$. Эти леммы доказывают теорему 9.

Заключение

Полученные в диссертации результаты относятся к теории синтеза управляющих систем с ограничениями. В качестве модели управляющих систем рассмотрены булевы схемы и формулы в конечных полных базисах, для которых изучены несколько видов ограничений на их структуру и на способы их построения. Под сложностью в данных моделях понимается число элементов или сумма их весов, а основная изучаемая характеристика при массовом синтезе — функция Шеннона для этой сложности.

Первая глава посвящена формулам с ограниченной глубиной альтернирования и схемам ограниченной ширины. Установлены оценки высокой степени точности для функции Шеннона сложности формул с глубиной альтернирования, не большей заданного числа a, $a \geqslant 3$, этот результат улучшает оценки, полученные в работах О. Б. Лупанова. Кроме того, в теории оценок высокой степени точности этот результат является первым, в котором параметр структурного ограничения модели не меняет асимптотику соответствующей функции Шеннона, но влияет на кратность логарифма во втором остаточном члене её разложения. В первой главе также изучены примеры применения полученного результата в задаче синтеза схем ограниченной ширины и в задаче реализации формулами глубины альтернирования 3 булевых функций из классов, связанных с конечными грамматиками, где также установлены оценки высокой степени точности. Кроме того, изучены некоторые особенности схем с малой шириной, и получены результаты по индивидуальной сложности линейной функции, монотонной симметрической функции с порогом 2, а также конъюнктивного дешифратора в схемах ширины 2 и 3.

Вторая глава посвящена формулам в базисах с прямыми и итеративными входами. Получено более компактное представление оператора итеративного замыкания, введенного С. А. Ложкиным для классификации полных базисов такого вида. В работах С. А. Ложкина также была найдена асимптотика функции Шеннона для схем из функциональных элементов в такой модели, её порядок роста является «стандартным» — $2^n/n$, а для случая формул указывалось, что порядок роста соответствующей функции Шеннона не более, чем 2^n, и не менее, чем $2^n/\log n$, где n — число входных переменных реализуемой функции. В диссертации для двух семейств базисов в этой классификации, а именно, для базисов, итеративное замыкание которых содержит класс монотонных функций, установлена асимптотика функции Шеннона, имеющей в этих базисах «стандартный» для формул порядок роста $2^n/\log n$. Указан способ определения константы в этой асимптотике и изучены свойства макроблоков, необходимые для определения приведенного веса базиса в рассматриваемой модели. Кроме того, в семействе таких базисов выделен достаточно широкий подкласс, в котором получены оценки высокой степени точности для соответствующей функции Шеннона, при этом найдено два типа поведения второго члена асимптотического разложения в таких оценках. Для остальных семейств базисов в упомянутой классификации по итеративным замыканиям приведены примеры базисов с порядком роста функции Шеннона, равным 2^n. Отдельно во второй главе показано существование булевых функций, которые могут быть самыми сложными по порядку роста в классе формул над одним базисом, и кардинально меняющих сложность при небольших изменениях базиса, оставляющих его в том же семействе указанной классификации. Таким образом, выявлены новые особенности задачи синтеза формул в базисах с прямыми и итеративными входами, показывающие существенную сложность этой задачи по сравнению с аналогичной задачей синтеза схем из функциональных элементов.

Литература

1. Bryant R. E. Graph-based algorithms for Boolean function manipulation // IEEE Trans. Comput. — 1986. — Vol. 35, no. 8. — P. 677–691.
2. Chomsky N., Miller G. A. Finite state languages // Information and Control — 1958. — Vol. 1. — P. 91–112.
3. Cooper J. N., Ellis R. B., Kahng A. B. Asymmetric binary covering codes // Journal of Combinatorial Theory, Series A. — 2002. — Vol. 100, no. 2. — P. 232–249.
4. Lee C. Y. Representation of switching circuits by binary-decision programs //Bell Labs Technical Journal. — 1959. — Vol. 38, no. 4. — P. 958–999.
5. Muller D. E. Complexity in electronic switching circuits //Electronic Computers, IRE Transactions on — 1956. — Vol. 5, no. 1. — P. 15–19.
6. Shannon C. E. The synthesis of two-terminal switching circuits //Bell System Technical Journal. — 1949. — Vol. 28, no. 1. — P. 59–98.
7. Аблаев Ф. М. К вопросу о сложности классического моделирования квантовых ветвящихся программ // Учёные записки Казанского государственного университета. Серия Физико-математические науки. — 2009. — Т. 151, № 2. — С. 7–15.
8. Алексеев В. Б., Ложкин С. А. Элементы теории графов, схем и автоматов. — М.: Издательский отдел факультета вычислительной математики и кибернетики МГУ им. М. В. Ломоносова, 2000. — 58 с.

9. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по курсу дискретной математики. — М.: ФИЗМАТЛИТ, 2005. — 416 с.

10. Глухов М. М. Об α-замкнутых классах и α-полных системах функций k-значной логики // Дискретная математика. — 1989. — Т. 1, вып. 1. — С. 16-21.

11. Грибок С. В. Оценка высокой степени точности для сложности обобщенных бинарных программ // Проблемы теоретической кибернетики. Материалы XIII международной конференции (Казань, 27–31 мая 2002 г.), Часть I. — М.: Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2002. — С. 47.

12. Гринчук М. И. О монотонной сложности пороговых функций // Дискретный анализ. — Вып. 52. — Новосибирск: ИМ СО АН СССР, 1992. — С. 41–48.

13. Карпова Н. А. О вычислениях с ограниченной памятью // Математические вопросы кибернетики. — Вып. 2. — М.: Наука, 1989. — С. 131–144.

14. Карпова Н. А. О сложности представлений функций алгебры логики линейными суперпозициями // Дискретный анализ. — Вып. 43. — Новосибирск: ИМ СО АН СССР, 1986. — С. 40–46.

15. Касим-Заде О. М. О сложности реализации функций в одном классе алгоритмов// Материалы IX межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 16–19 декабря 1998 г.). — М.: Издательство механико-математического факультета МГУ, 1999. — С. 25–30.

16. Кириченко К. Д. Верхняя оценка сложности полиномиальных нормальных форм булевых функций // Дискретная математика. — 2005. — Т. 17, вып. 3. — С. 80–88.

17. Кондратов А. В. Асимптотические оценки высокой степени точности для сложности реализации функций, связанных с автоматными языками, в неко-

торых классах схем // Математические вопросы кибернетики. — Вып. 13. — М.: Наука, 2004. — С. 279–288.

18. Коноводов В. А. Некоторые особенности задачи синтеза булевых формул в полных базисах с прямыми и итеративными входами // Учёные записки Казанского университета. Серия Физико-математические науки. — 2014. — Т. 156, № 3. — С. 76–83.
19. Коноводов В. А. О синтезе схем ограниченной ширины // Материалы VIII молодежной научной школы по дискретной математике и ее приложениям (г. Москва, 24—29 октября 2011 г.). — М.: Издательство механико-математического факультета МГУ им. М. В. Ломоносова, 2011. — Ч. 1. — С. 37—41.
20. Коноводов В. А. О сложности булевых формул в базисах из элементов с прямыми и итеративными входами // Материалы IX молодежной научной школы по дискретной математике и ее приложениям (г. Москва, 16—21 сентября 2013 г.). — М.: Издательство ИПМ РАН, 2013. — С. 57–60.
21. Коноводов В. А. Некоторые особенности задачи синтеза булевых формул в полных базисах с прямыми и итеративными переменными // Проблемы теоретической кибернетики. Материалы XVII международной конференции (Казань, 16–20 июня 2014 г.). — Казань: Отечество, 2014. — С. 138—140.
22. Коноводов В. А. Асимптотические оценки высокой степени точности для сложности булевых формул в некоторых базисах, состоящих из элементов с прямыми и итеративными входами // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г.— М.:МАКС Пресс, 2015. — С. 110-–113.
23. Коршунов А. Д. Об асимптотических оценках сложности контактных схем заданной степени // Дискретный анализ. — Вып. 5. — Новосибирск: ИМ СО АН СССР, 1965. — С. 35–63.

24. Кричевский Р. Е. Минимальная схема из замыкающих контактов для одной булевой функции от n аргументов // Дискретный анализ. — Вып. 5. — Новосибирск: ИМ СО АН СССР, 1965. — С. 89–92.
25. Кузьмин В. А. Оценка сложности реализации функций алгебры логики простейшими видами бинарных программ // Дискретный анализ. — Вып. 29. — Новосибирск: ИМ СО АН СССР, 1976. — С. 11–39.
26. Ложкин С. А., Коноводов В. А. О синтезе и сложности формул с ограниченной глубиной альтернирования // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2012. — № 2. — С. 28–36.
27. Ложкин С. А., Коноводов В. А. О сложности реализации булевых функций из некоторых классов, связанных с конечными грамматиками, формулами глубины альтернирования 3 // Вестник Московского университета. Серия 1. Математика. Механика. — 2014. — № 3. — С. 14–19.
28. Ложкин С. А., Коноводов В. А. О сложности формул алгебры логики в некоторых полных базисах, состоящих из элементов с прямыми и итеративными входами // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 1. — С. 55–68.
29. Ложкин С. А., Коноводов В. А. Оценки высокой степени точности для сложности булевых формул в некоторых базисах из элементов с прямыми и итеративными входами // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 2. — С. 16–30.
30. Ложкин С. А., Коноводов В. А. О синтезе и сложности формул с ограниченной глубиной альтернирования // Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Издательство Нижегородского университета, 2011. — С. 281–284.

31. 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.
32. Ложкин С. А. Лекции по основам кибернетики: Учебное пособие. — М.: Изд. отдел ф-та ВМиК МГУ, 2004. — 256 с
33. Ложкин С. А. Реализация функций алгебры логики схемами из функциональных элементов с задержками // Диссертация на соискание ученой степени кандидата физико-математических наук. — МГУ им. М. В. Ломоносова, 1979.
34. Ложкин С. А. О синтезе формул, сложность и глубина которых не превосходят асимптотически наилучшие оценки высокой степени точности // Вестник Московского университета. Серия 1. Математика. Механика. — 2007. —№ 3. — С. 19–25.
35. Ложкин С. А. О сложности реализации произвольных булевых функций в некоторых классах BDD // Труды Международной школы-семинара «Дискретная математика и математическая кибернетика» (Ратмино, 31 мая — 1 июня 2001 г.). — М.: МАКС Пресс ИПМ РАН, 2001. — С. 18–19.
36. Ложкин С. А. Асимптотические оценки высокой степени точности для сложности управляющих систем // Диссертация на соискание ученой степени доктора физико-математических наук. МГУ им. М. В. Ломоносова, 1998.
37. Ложкин С. А. О полноте и замкнутых классах функций алгебры логики с прямыми и итеративными переменными // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 1999. — № 3. — С. 35–41.
38. Ложкин С. А. О сложности реализации функций алгебры логики схемами и формулами, построенными из функциональных элементов с прямыми и итеративными переменными // Труды III Международной конференции «Дис-

кретные модели в теории управляющих систем» (Красновидово, 1998 г.). — М.: Диалог-МГУ, 1998. — С. 72–73.

39. Ложкин С. А. Асимптотические оценки высокой степени точности для сложности функций, связанных с автоматными языками // Проблемы теоретической кибернетики. Тезисы докладов XII международной конференции (Нижний Новгород, 17–22 мая 1999 г.), Часть II. — М.: Издательство механико-математического факультета МГУ, 1999. — С. 138.

40. Ложкин С. А. О минимальных π-схемах для монотонных симметрических функций с порогом 2 // Дискретная математика. — 2005. — Т. 17, вып. 4. — С. 108–110.

41. Лупанов О. Б. Об одном методе синтеза схем // Известия вузов. Радиофизика. — 1958. — Т. 1, № 1. — С. 120–140.

42. Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики — 1960. — Вып. 3. — С. 61–80.

43. Лупанов О. Б. Об одном классе схем из функциональных элементов (формулы с частичной памятью) // Проблемы кибернетики — 1962. — Вып. 7. — С. 61–114.

44. Лупанов О. Б. О реализации функций алгебры логики формулами из конечных классов (формулами ограниченной глубины) в базисе $\&$, $\vee$, $\neg$. // Проблемы кибернетики — 1961. — Вып. 6. — С. 5–14.

45. Лупанов О. Б. О реализации функций алгебры логики схемами из функциональных элементов «ограниченной глубины» в базисе $\&$, $\vee$, $\neg$ // Сборник работ по математической кибернетике — 1977. — Вып. 2. — С. 3–8.

46. Лупанов О. Б. О влиянии глубины формул на их сложность // Кибернетика — 1970. — Вып. 2. — С. 46–49.

47. Лупанов О. Б. О синтезе контактных схем // Доклады АН СССР — 1958. — Т. 119, № 1. — С. 23–26.

48. Мадатян Х. А. Синтез контактных схем ограниченной ширины // Проблемы кибернетики — 1965. — Вып. 14. — С. 301–307.

49. Редькин Н. П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики — 1970. — Вып. 23. — С. 83–102.

50. Трущин Д. В. О глубине α-пополнений систем булевых функций // Вестник Московского университета. Серия 1. Математика. Механика. — 2009. —№ 2. — С. 72–75.

51. Трущин Д. В. О сложности реализации функци многозначной логики формулами специального вида // Материалы XI Международного семинара «Дискретная математика и ее приложения»(Москва, 18–23 июня 2012 г.). — М.: Издательство механико-математического факультета МГУ. — С. 174–176.

52. Холл М. Комбинаторика. — М.: Мир, 1970. — 424 с.

53. Храпченко В. М. О сложности реализации линейной функции в классе П-схем // Математические заметки — 1971. — Т. 9, № 1. — С. 21–23.

54. Чернышов А. Л. Условия α-полноты систем функций многозначной логики // Дискретная математика. — 1992. — Т. 4, вып. 4. — С. 117–130.

55. Шиганов А. Е. О синтезе ориентированных контактных схем с некоторыми ограничениями на смежные контакты // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2009. — № 3. — С. 46–52.

56. Шиганов А. Е. Некоторые особенности задачи синтеза булевых формул в полных базисах с прямыми и итеративными входами // Учёные записки Ка-

занского государственного университета. Серия Физико-математические науки. — 2009. — Т. 151, № 2. — С. 164–172.

57. Шиганов А. Е. Синтез схем контактного типа с ограничением на смежные контакты // Диссертация на соискание ученой степени кандидата физико-математических наук. — МГУ им. М. В. Ломоносова, 2010.

58. Шиганов А. Е. Некоторые оценки сложности двоичных решающих диаграмм // Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Издательство Нижегородского университета, 2011. — С. 568–570.

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

60. Яблонский. С. В. Реализация линейной функции в классе π-схем // Доклады АН СССР — 1954. — Т. 94, № 5. — С. 805–806.