На правах рукописи

Коноводов Владимир Александрович

Методы синтеза и оценки сложности схем с некоторыми структурными ограничениями

Специальность 01.01.09 — дискретная математика и математическая кибернетика

Автореферат

диссертации на соискание учёной степени

кандидата физико-математических наук

Москва — 2015

Работа выполнена на кафедре математической кибернетики факультета вычислительной математики и кибернетики федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М. В. Ломоносова».

Научный руководитель:	**Ложкин Сергей Андреевич**, доктор физико-математических наук, профессор кафедры математической кибернетики факультета вычислительной математики и кибернетики федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М. В. Ломоносова»
Официальные оппоненты:	**Аблаев Фарид Мансурович,** доктор физико-математических наук, профессор, член-корреспондент Академии Наук Республики Татарстан, заведующий кафедрой теоретической кибернетики Казанского федерального университета
	Шиганов Александр Евгеньевич, кандидат физико-математических наук, ведущий инженер по разработке программного обеспечения в филиале компании «Ментор Графикс Девелопмент Сервисез Лимитед» (Ирландия)
Ведущая организация:	«Федеральный исследовательский центр «Информатика и управление» Российской Академии Наук

Защита состоится 25 сентября 2015 г. в 11 час. 00 мин. на заседании диссертационного совета 501.001.44 при Московском государственном университете имени М. В. Ломоносова по адресу: 119991, г. Москва, ГСП-1, Ленинские горы, д. 1, стр. 52, 2-й учебный корпус, аудитория 685.

С диссертацией можно ознакомиться в Научной библиотеке Московского государственного университета имени М. В. Ломоносова по адресу: 119192, г. Москва, Ломоносовский проспект, д. 27 — а также на официальном сайте факультета ВМК МГУ http://cmc.msu.ru в разделе «Диссертации».

Автореферат разослан «____» ____________ 2015 года.

Ученый секретарь
диссертационного совета 501.001.44,
доктор физико-математических наук, доцент О. В. Шестаков

Общая характеристика работы

Актуальность темы диссертации. 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 [1] с использованием метода Шеннона[2]. Было показано, что порядок роста указанной функции при стремлении натурального аргумента n к бесконечности равен $2^n/n$.

Затем О. Б. Лупановым [3] 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

[1] Muller D. E. Complexity in electronic switching circuits // Electronic Computers, IRE Transactions on. 1956. Vol. 5. no. 1. P. 15–19.

[2] Shannon C. E. The synthesis of two-terminal switching circuits // Bell System Technical Journal, 1949. Vol. 28, no. 1. P. 59–98.

[3] Лупанов О. Б. Об одном методе синтеза схем // Известия вузов. Радиофизика. — 1958. — Т. 1. — № 1. — С. 120–140.

случая булевых формул вида $\rho \cdot \frac{2^n}{\log n}$ (здесь и далее все логарифмы двоичные), где ρ — константа, зависящая от базиса, и одинаковая для случая формул и схем в одном базисе.

В дальнейшем в работах С. А. Ложкина [4] 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 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 ее 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. Им 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[5]. Также О. Б. Лупанов [6,7] рассматривал формулы и схемы ограниченной глубины в стандартном базисе $\{\vee, \&, \neg\}$, у которых отрицания стояли только над переменными. Под глубиной схемы понимается уменьшенное на единицу максимальное число изменений типов элементов в последовательностях, которые являются цепями этой схемы без учета отрицаний, присоединённых к её входам. В диссертации эта величина называется *глубиной альтернирования* схемы. Установлено, что функция Шеннона для сложности формул, имеющих

[4]Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. — 1996. — Вып. 6. — С. 189–214.

[5]Лупанов О. Б. Об одном классе схем из функциональных элементов (формулы с частичной памятью) // Проблемы кибернетики. — 1962. — Вып. 7. — С. 61–114.

[6]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.

[7]Лупанов О. Б. О влиянии глубины формул на их сложность // Кибернетика. — 1970. — № 2. — С. 46–49.

глубину альтернирования не большую, чем d, и реализующих функции от n переменных, при всех $d \geqslant 3$ асимптотически ведет себя так же, как и в случае без ограничений — $2^n / \log n$. Аналогичный результат был получен и для схем из функциональных элементов[8].

Другой тип ограничения, связанный с числом регистров, т. е. ячеек памяти, необходимых для осуществляемых схемой вычислений, был рассмотрен в работах Н. А. Карповой [9,10], которая, в частности, показала, 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 диссертации схемы с t регистрами называются схемами *ширины* 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. К. Шенноном [11] был установлен порядок роста соответствующей функции Шеннона, а О. Б. Лупанов [12] 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. А. Д. Коршунов описал[13] асимптотически оптимальный метод их синтеза, а Х. А. Мадатян получил[14] асимптотические оценки сложности реализации булевых функций с помощью контатных схем ограниченной ширины. А. Е. Шигановым [15,16] рассматривались контактные схемы и итеративные контактные схемы с различными типами ограничений на смежные контакты. В частности, были раз-

[8] 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.

[9] Карпова Н. А. О вычислениях с ограниченной памятью // Математические вопросы кибернетики. — 1989. — Вып. 2. — С. 131-144.

[10] Карпова Н. А. О сложности представлений функций алгебры логики линейными суперпозициями // Дискретный анализ. — 1986. — Вып. 43. — С. 40–46.

[11] Shannon C. E. The synthesis of two-terminal switching circuits // Bell System Technical Journal, 1949. Vol. 28, no. 1. P. 59–98.

[12] Лупанов О. Б. О синтезе некоторых классов управляющих систем. // Проблемы кибернетики. — 1963. — Вып. 10. — С. 63–97.

[13] Коршунов А. Д. Об асимптотических оценках сложности контактных схем заданной степени // Дискретный анализ. — 1965. — Вып. 5. — С. 35–63.

[14] Мадатян Х. А. Синтез контактных схем ограниченной ширины // Проблемы кибернетики. — 1965. — Вып. 14. — С. 301–307.

[15] Шиганов А. Е. О синтезе ориентированных контактных схем с некоторыми ограничениями на смежные контакты // Вестник Московского ун-та. Сер. 15. Выч. мат-ка и кибернетика. — 2009. — № 3. — С. 46–52.

[16] Шиганов А. Е. О сложности ориентированных контактных схем с ограниченной полустепенью исхода // Учён. зап. Казан. гос. ун-та. Сер. Физ.-матем. науки. — 2009. — Т. 151. — № 2. — С. 164–172.

работаны 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. А. Кузьминым[17], который рассматривал два основных типа команд — вычислительные и переадресующие команды, и получил асимптотику функции Шеннона сложности таких программ из некоторых классов. Асимптотику вида $2^n/(3n)$ для сложности бинарных программ общего вида получил О. М. Касим-Заде[18]. Класс бинарных программ, состоящих только из переадресующих команд, был впервые предложен Ли[19], такие программы также называются BDD (Binary Decision Diagrams), и имеют огромное значение в прикладных задачах[20,21]. Асимптотику $2^n/n$ функции Шеннона для сложности двоичных решающих диаграмм установил В. А. Кузьмин[17]. Для некоторых классов BDD С. А. Ложкиным[22], А. Е. Шигановым[23] и С. В. Грибком [24] были получены асимптотические оценки высокой степени точности для соответствующих функций Шеннона.

Отметим, что если под шириной вычисляющей программы понимать минимальное число ячеек памяти, необходимых для хранения ее внутренних переменных, то вычисляющие программы ширины t представляют собой схемы с t регистрами.

Другим направлением задачи синтеза является исследование реализации булевых функций в схемах с ограничениями на типы соединяемых элементов и

[17] Кузьмин В. А. Оценка сложности реализации функций алгебры логики простейшими видами бинарных программ // Дискретный анализ. — 1976. — Вып. 29. — С. 11–39.

[18] Касим-Заде О. М. О сложности реализации функций в одном классе алгоритмов // Материалы IX межгосударственной школы-семинара «Синтез и сложность управляющих систем». Изд. мех.-мат. ф-та МГУ. — 1999. — С. 25–30.

[19] Lee C. Y. Representation of switching circuits by binary-decision programs // Bell Labs Tech. J., 1959. Vol. 38, no. 4. P. 958–999.

[20] Bryant R. E. Graph-based algorithms for Boolean function manipulation // IEEE Transactions on Computers. 1986. Vol. 35, no. 8. P. 677–691.

[21] 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.

[22] Ложкин С. А. О сложности реализации произвольных булевых функций в некоторых классах BDD // Труды международной школы-семинара «Дискретная математика и математическая кибернетика». М.: МАКС Пресс, 2001. С. 18–19.

[23] 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.

[24] Грибок С. В. Оценка высокой степени точности для сложности обобщенных бинарных программ // Проблемы теоретической кибернетики. Тезисы докладов XIII Международной конференции (Казань, 27–31 мая 2002 г.), Часть I. — 2002. — С. 47.

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. Впервые задача синтеза в такой модели была предложена и рассмотрена С. А. Ложкиным[25,26]. Им 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. При этом все базисы специальным образом классифицировались для определения их полноты. Для оператора, с помощью которого проводилась эта классификация, в настоящей диссертации получено более наглядное представление. Это представление определяет результат применения этого оператора к некоторому базису A как множество тех функций, зависящих только от итеративных переменных, которые можно получить рассматриваемыми суперпозициями функций из A. В диссертации указанный оператор назван оператором *итеративного замыкания*.

Также С. А. Ложкиным 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» для схем порядок роста $2^n/n$. Известно также[26], 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, т. е. формулами, в которых каждая подформула содержит не более одной нетривиальной главной подформулы. Эту задачу впервые рассматривал М. М. Глухов[27], он показал 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[28] был доказан критерий α-полноты функций многозначной логики и показано от-

[25] 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.

[26] 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 «Дискретные модели в теории управляющих систем» (Красновидово, 1998 г.) Диалог-МГУ, Москва. — 1998. — С. 72–73.

[27] 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.

[28] Чернышов А. Л. Условия α-полноты систем функций многозначной логики // Дискретная математика. — 1992. — Т. 4. — Вып. 4. — С. 117–130.

сутствие конечных α-полных систем в случае булевых функций. Д. В. Трущин получил оценки функции Шеннона для глубины α-формул[29]. Следует отметить, 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.

Модель схем из функциональных элементов в базисах с прямыми и итеративными переменными обладает рядом и других сходств с 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 $\mu_1 = x_1y_1 \vee \bar{x}_1y_2$, 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.

Цель работы — исследование поведения функций Шеннона для сложности схем и формул в моделях со структурными ограничениями, получение оценок высокой степени точности для этих функций и изучение степени влияния этих ограничений на сложность булевых функций.

Основные результаты работы:

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.

[29] Трущин Д. В. О глубине α-пополнений систем булевых функций // Вестник Московского университета. Серия 1. Математика. Механика. — 2009. — Вып. 2. — С. 72–75.

Научная новизна. Все результаты диссертации являются новыми.

Методы исследования. В работе используются методы дискретной математики и математической кибернетики, теории управляющих систем, комбинаторики и теории графов. Кроме того, в диссертации используются методы синтеза схем и формул, направленные на получение асимптотических оценок высокой степени точности.

Теоретическая и практическая значимость. Диссертация носит теоретический характер. Результаты диссертации могут найти применение при практическом синтезе интегральных схем.

Апробация работы. 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).

Также результаты обсуждались на научных семинарах кафедры математической кибернетики факультета ВМК МГУ и кафедры дискретной математики механико-математического факультета МГУ.

Личный вклад. Все результаты получены автором самостоятельно.

Публикации. Результаты диссертации изложены в 10 печатных изданиях [1–10], из которых [1–5] — в журналах из перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук. В работах [1, 2, 4–6] Коноводову В. А. принадлежат все результаты, а Ложкину С. А. — постановка задачи.

Структура и объем работы. Диссертация состоит из введения, двух глав, заключения и списка литературы. Общий объем диссертации составляет 109 страниц. Принята сквозная нумерация лемм и теорем. Список литературы содержит **60** наименований.

Содержание работы

Введение диссертации состоит из обзора исследований, связанных с темой работы, определения основных понятий, используемых в диссертации, а также краткого изложения полученных результатов, сформулированных в виде теорем 1–9. Вводятся определения рассматриваемых моделей, являющихся модификациями булевых формул и схем из функциональных элементов при помощи различного рода структурных ограничений.

Под сложностью $\mathcal{L}(\Sigma)$ схемы Σ понимается сумма весов её элементов. Функция Шеннона натурального аргумента n для сложности схем в некоторой модели определяется как сложность самой сложной функции от n переменных в этой модели, где под сложностью функции понимается сложность минимальной реализующей её схемы в модели. При этом, если веса всех элементов равны 1, то сложность схемы совпадает с числом элементов в ней, и для указанной величины используется обозначение $L(\Sigma)$, а для соответствующей функции Шеннона — обозначение $L(n)$. В случае существования элементов неединичного веса функция Шеннона обозначается как $\mathcal{L}(n)$.

Вводится модифицированное понятие грамматики с конечным числом состояний[30]. 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, отправлясь 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 называется язык $T_\Gamma = \bigcup\limits_{1 \leqslant i,j \leqslant p} T_{ij}$.

Пусть $T_\Gamma(s)$, $s \geqslant 1$, — множество слов языка T_Γ, длина которых равна s. Н. Хомский и Дж. Миллер показали[30], что 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 соотношение $|T_\Gamma(s)| = 2^{\sigma_\Gamma \cdot s + O(1)}$. Величина σ_Γ называется *мощностной константой* грамматики Γ. Класс булевых функций от n, $n \geqslant 1$, переменных, множество столбцов значений которых совпадает с $T_\Gamma(2^n)$, обозначается как $Q_\Gamma(n)$.

[30] Chomsky N., Miller G. A. Finite state languages // Information and Control. 1958. Vol. 1. P. 91–112

Далее определяется понятие *схемы ограниченной ширины*. 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 номер $\mathcal{E}$ больше номера любого элемента, выход которого подается на один из его входов; и 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, считается, 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. Для схемы Σ с t, $t \in \{1, 2, \ldots\}$, регистрами число t называется её шириной.

Схема с t, $t \geqslant 1$, регистрами реализует систему из m, $m > 1$, функций F, 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.

Пусть $X = \{x_1, x_2, \ldots\}$ и $Y = \{y_1, y_2, \ldots\}$ — счетные множества булевых переменных, переменные из множества X (из Y) называются *прямыми* (соответственно, *итеративными*). Для каждого множества переменных Z через $P_2(Z)$ обозначается множество всех функций алгебры логики, зависящих от переменных из Z.

На множестве $P_2(X \cup Y)$, определяются 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 функций, не имеющих общих существенных переменных, вместо итеративной переменной другой функции,

5. замена итеративных переменных прямыми переменными,

6. отождествление итеративных переменных.

Пусть $A \subseteq P_2(X \cup Y)$ — некоторое конечное множество базисных функций. В соответствии с введенными операциями суперпозиции в диссертации рассматриваются одновыходные схемы из функциональных элементов и формулы над базисом A, в которых 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); итеративные входы любого элемента либо присоединяются к выходам других элементов, либо присоединяются к входам схемы, либо являются константными входами; неконстантным входам схемы сопоставлены некоторые переменные из множества X.

Система функций A, $A \subseteq P_2(X \cup Y)$, называется *полной*, если для любой функции f, $f \in P_2(X)$, существует формула над A указанного вида, реализующая функцию f.

Далее вводятся некоторые понятия, необходимые для формулировки результата о поведении функции Шеннона в таких базисах. *Приведенным весом* элемента с k входами (прямыми и итеративными), имеющего вес L, называется величина $L/(k-1)$. *Макроблоком* в базисе A, $A \subseteq P_2(X \cup Y)$, называется схема из функциональных элементов в этом базисе, состоящая из элемента $\mathcal{E}$, имеющего более одного итеративного входа, и элементов, имеющих только прямые входы, выходы которых подаются на итеративные входы элемента $\mathcal{E}$, причем количество элементов с прямыми входами на единицу меньше числа итеративных входов элемента $\mathcal{E}$. Итеративным входом макроблока считается его свободный (т. е. тот, на который не подаются выходы других элементов макроблока) входов элемента $\mathcal{E}$, остальные входы макроблока считаются прямыми. *Приведенным весом* макроблока указанного вида называется величина, равная отношению суммарной сложности макроблока к числу его прямых входов.

Приведенным весом ρ_A базиса A называется минимальный приведенный вес среди всех элементов с хотя бы одним итеративным входом и всех макроблоков в этом базисе.

Для рассматриваемых в диссертации моделей с ограничениями используются следующие обозначения:

- Для любого a, $a \geqslant 2$, функция Шеннона для сложности формул, глубина альтернирования которых не больше чем a, обозначается как $L^{(a)}(n)$.

- Функция Шеннона для сложности формул с глубиной альтернирования не более 3, реализующих функции из класса $Q_\Gamma = \bigcup\limits_{n \geqslant 1} Q_\Gamma(n)$, обозначается как $L_\Gamma(n)$.

- Сложность $L^{\{t\}}(f)$ функции алгебры логики f в классе схем в базисе $\{\&, \vee, \neg\}$, ширина которых не превосходит t, определяется как минимальная сложность схемы из этого класса, реализующей функцию f. За $L_{\text{Б}}^{\{t\}}(n)$ обозначается соответствующая функция Шеннона. Сложностью системы функций F называется минимальная сложность схем с $|F|$ выходами, реализующих систему F. Соответствующая сложность в классе схем с t регистрами в стандартном базисе обозначается $L^{\{t\}}(F)$.

- Если A — базис, состоящий из элементов с прямыми и итеративными входами, то $\mathcal{L}_A(n)$ — функция Шеннона для сложности формул в этом базисе, определенной как сумма весов элементов этих формул.

Кроме того, во **введении** определяются следующие обозначения для отдельных функций и систем:

- $s_n(x_1, \dots, x_n) = \bigvee\limits_{1 \leqslant i < j \leqslant n} x_i x_j$. — монотонная симметрическая функция с порогом 2.

- $l_n = x_1 \oplus \ldots \oplus x_n$, $n \geqslant 2$, —линейная функция порядка n, здесь символом $\oplus$ обозначается сумма по модулю 2.

- Система функций $\overrightarrow{Q}_n = \{\bar{x}_1 \cdots \bar{x}_{n-1}\bar{x}_n,\ \bar{x}_1 \cdots \bar{x}_{n-1}x_n,\ \dots,\ x_1 \cdots x_{n-1}x_n\}$, состоящая из всех элементарных конъюнкций ранга n от n переменных, называется *дешифратором* порядка n.

Первая глава посвящена формулам с ограниченной глубиной альтернирования и схемам ограниченной ширины.

Для функции Шеннона $L^{(a)}(n)$ сложности формул с ограниченной глубиной альтернирования устанавливаются следующие оценки высокой степени точности, имеющие относительную погрешность вида $O\left(\frac{1}{\log n}\right)$:

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

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

где $\log^{[a]} x = \underbrace{\log \ldots \log}_{a \text{ раз}} x$, если указанный повторный логарифм определен и неотрицателен, и $\log^{[a]} x = 0$ в остальных случаях.

В следующей теореме получена оценка высокой степени точности для величины $L_{\Gamma}(n)$.

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*

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

Далее приводятся результаты, связанные с задачей индивидуального синтеза схем ограниченной ширины.

М. И. Гринчук доказал[31], что сложность реализации функции s_n в классе схем из функциональных элементов в базисе $\{\&, \vee\}$ без ограничений асимптотически равна $2n$. Кроме того, Р. Е. Кричевским установлено[32], что в классе π-схем (а, следовательно, и в классе формул в стандартном базисе, у которых отрицания стоят только над переменными) сложность этой функции равна $\lfloor \log n \rfloor \cdot 2^{\lfloor \log n \rfloor} + (\lfloor \log n \rfloor + 2) \cdot \left(n - 2^{\lfloor \log n \rfloor}\right) \sim n \log n$. С. А. Ложкиным этот результат был обобщён[33] для случая π-схем, в которых контакты различных переменных могут иметь различные веса.

Н. П. Редькин показал[34], что сложность реализации линейной функции l_n, $n \geqslant 2$, в классе схем из функциональных элементов без ограничений равна $4n - 4$. Из результатов В. М. Храпченко[35] и С. В. Яблонского[36] следует, что сложность этой функции в классе π-схем (а, следовательно, и в классе формул в $\{\&, \vee, \neg\}$, 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 $\{\&, \vee, \neg\}$ невозможно. Следующая теорема, в частности, показывает, что в классе схем с двумя регистрами данная функция допускает оптимальную реализацию.

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

$$L^{\{2\}}(l_n) = L^{\{2\}}(\bar{l}_n) = 4n - 4;$$
$$L^{\{3\}}(s_n) \leqslant 3n - 5.$$

---

[31] Гринчук М. И. О монотонной сложности пороговых функций // Дискретный анализ. — 1992. — Вып. 52. — С. 41–48.

[32] Кричевский Р. Е. Минимальная схема из замыкающих контактов для одной булевой функции от n аргументов // Дискретный анализ. — 1965. — Вып. 5. — С. 89–92.

[33] Ложкин С. А. О минимальных π-схемах для монотонных симметрических функций с порогом 2 // Дискретная математика. — 2005. — Вып. 17. — № 4. — С. 108–110.

[34] Редькин Н. П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. — 1970. — Вып. 23. — С. 83–102.

[35] Храпченко В. М. О сложности реализации линейной функции в классе П-схем // Математические заметки. — 1971. — Т. 9. — № 1. — С. 21–23.

[36] Яблонский С. В. Реализация линейной функции в классе π-схем // Доклады АН СССР. — 1954. — Т. 94. — № 5. — С. 805–806.

При $n \to \infty$ справедлива оценка:

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

Следует отметить, что, как следует из результатов С. А. Ложкина[33], 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 — $n \log n$.

Далее приводится результат о сложности реализации дешифратора в схемах ширины 2 и 3.

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

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

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

Отметим, что сложность дешифратора в классе схем из функциональных элементов в стандартном базисе без ограничений асимптотически равна 2^n.

Вторая глава посвящена формулам в базисах из элементов с прямыми и итеративными входами.

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 С. А. Ложкина[25] введено обозначение $\delta(A) = \left[[A]_{\{2\}} \cap P_2(Y)\right]_{\{3,4,6\}}$. В диссертации это множество называется итеративным замыканием множества A. Множество $\delta(A)$ является «обычным» замкнутым классом в $P_2(Y)$, содержащим все константы, и поэтому совпадает с одним из классов системы $\Delta = \{B, I, O, D, K, L, M, P_2(Y)\}$, 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. В первой теореме **второй главы** для оператора δ приводится более наглядное представление:

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

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

Множество $\delta(A)$ 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. Следующая теорема **второй главы** показывает, что эта классификация имеет прямое отношение к исследованию сложности формул в соответствующих базисах.

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

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

В некоторых базисах A, таких, что $\delta(A) = D$ и $L_A(n) = \Theta(2^n)$, 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. *В базисе $A_1 = \{(x_1 \oplus x_2)y_1, (x_1 \oplus x_2 \oplus 1)y_1, y_1 \vee y_2\}$ 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 $A_3 = \{(x_1 \oplus x_2 \oplus 1)y_1, y_1 \vee y_2\}$ — 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.

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, $A \subseteq P_2(X \cup Y)$, через $\hat{A}$ обозначается множество тех элементов базиса A с итеративными входами, которые либо имеют приведенный вес, равный ρ_A, либо входят в макроблоки этого базиса с приведенным весом ρ_A.

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*

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

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

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:*

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

В **заключении** приведены основные результаты работы.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

1. 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.
2. 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.
3. Коноводов В. А. Некоторые особенности задачи синтеза булевых формул в полных базисах с прямыми и итеративными входами // Ученые записки Казанского университета. Серия Физико-математические науки. — 2014. — Т. 156, № 3. — С. 76–83.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.

9. 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.
10. 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.