ФГБОУ ВПО Московский государственный университет

имени М.В. Ломоносова

На правах рукописи

КИБКАЛО Мария Александровна

Автоматная сложность булевых функций из классов Поста

Специальность 05.13.17 – теоретические основы информатики

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата физико-математических наук

Москва – 2013

Работа выполнена на кафедре математической теории интеллектуальных систем механико-математического факультета ФГБОУ ВПО «Московский государственный университет имени М.В. Ломоносова».

Научный руководитель: доктор физико-математических наук, профессор Бабин Дмитрий Николаевич

Официальные оппоненты: доктор физико-математических наук, профессор Чечкин Александр Витальевич ФГВОУ ВПО «Военная академия Ракетных войск стратегического назначения имени Петра Великого»

кандидат физико-математических наук, ведущий инженер Зайцев Денис Владимирович ООО «ЭЛ ЭС АЙ Интернешнел Ресерч»

Ведущая организация: ФГБОУ ВПО «Российский государственный гуманитарный университет»

Защита диссертации состоится 25 декабря 2013 года в 16 час. 45 мин. на заседании диссертационного совета Д 501.002.16, созданного на базе ФГБОУ ВПО «Московский государственный университет имени М.В. Ломоносова», по адресу: 119991, Москва, ГСП-1, Ленинские горы, д.1, ФГБОУ ВПО МГУ имени М.В. Ломоносова, механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВПО «Московский государственный университет имени М.В. Ломоносова» (Москва, Ломоносовский проспект, д.27, сектор А, 8 этаж).

Автореферат разослан 25 ноября 2013 г.

Ученый секретарь диссертационного совета
Д.501.002.16, созданного на базе ФГБОУ ВПО МГУ,
доктор физико-математических наук,
профессор А.А.Корнев

.

Общая характеристика задачи

Актуальность темы. Теоретическое осмысление вопросов программирования привело к необходимости учитывать сложность используемых для разработки программ методов и объектов. Наиболее употребительными методами решения прикладных задач оказались линейные методы распознавания, фильтрации, кодирования, предсказания поведения объектов и.т.д. Линейные методы быстро решают традиционные задачи, суммируя вклады отдельных признаков, но при этом качественная часть работы по подбору удачных признаков перекладывается на инженеров и прикладных математиков, что надолго затягивает решение новых задач.

Неудовлетворенность исследователей линейными методами привела к широкому использованию термина «нелинейные». При этом нелинейными часто называют либо пороговые методы, либо булевы функции, в полиноме которых присутствуют два-три члена второй степени. Широкому использованию произвольных нелинейных методов препятствует их высокая сложность. При их реализации приходится выполнять экспоненциально растущее от входных данных число операций.

При реализации вычислений в процессорах естественным образом происходит переход от математики непрерывной к математике булевой. За два десятилетия процессоры прошли путь из 16-битных к 32-битным, а затем – к 64-битным. Поскольку передача данных по каналам связи происходит последовательно, актуален вопрос о последовательном вычислении булевых функций по мере появления значений их переменных, то есть о вычислении булевых функций автоматами или двоичными диаграммами решений (binary decision diagram). Эта задача была поставлена еще в 1955 году Олегом Борисовичем Лупановым[1].

За последнее десятилетие по сложности двоичных диаграмм решений появилось большое число работ. Одна из основных причин в том, что сложность реализации функций в небольших устройствах, как правило, приводит к коммерческому успеху. Тем не менее, оценка автоматной сложности классов Поста[2] оставалась вне поля зрения исследователей. Этот пробел заполняет настоящая работа.

[1] Лупанов О.Б. О возможностях синтеза схем из разнообразных элементов. Докл. АН СССР. Т. 103, № 4, 1955, с. 561-563

[2] Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б. Функции алгебры логики и классы Поста. Наука, Москва, 1966

Понятие конечного автомата окончательно сформировалось в результате исследования дискретных преобразователей информации[3,4,5,6,7,8] и оценки их сложности (например, времени работы, числа операций для построения автомата или числа состояний автомата)[9,10,11,12,]. В настоящей работе под сложностью автомата понимается число его состояний.

Конечные автоматы могут использоваться для представления булевых (k-значных) функций. В этом случае наборы, на которых функция равна 1, рассматриваются как слова языка. Сложность функции определяется как сложность представляющего указанный язык минимального автомата. При этом естественным образом определяется функция Шеннона для класса функций.

Для представления функций часто используются упрощенные модели конечных автоматов – двоичные диаграммы решений (Binary Decision Diagrams – BDD), впервые примененные Брайантом[13]. Обзор свойств и особенностей различных видов BDD дан в диссертации Грёпля[14]. Такой способ отличается от представления функций конечными автоматами лишь несущественными деталями[15,16].

В диссертации рассматриваются как булевы и k-значные функции (т.е. языки из слов постоянной длины), так и языки из слов переменной длины. Для представления функций и языков используется формализм конечных автоматов. OBDD, представляющие такие функции, имеют ту же асимптотику сложности, что и аналогичные автоматы.

Сложности автоматов и диаграмм решений, представляющих булевы функции, посвящена обширная литература. Рассматривались конкретные функции (сумматоры, умножители, пороговые функции, мультиплексоры,

---

[3] Shannon C.E. A Mathematical Theory of Communication, Bell System Technical Journal, Volume 27, 1948, pp. 379-423, 623-656

[4] Клини С.К.. Представление событий в нервных сетях и конечных автоматах. В Шеннон К.Э., Маккарти Дж. (ред.), Автоматы, Издательство иностранной литературы, Москва, 1956, с. 15-67

[5] Мур Э.Ф., Умозрительные эксперименты с последовательностными машинами. В Шеннон К.Э., Маккарти Дж. (ред.), Автоматы, Издательство иностранной литературы, Москва, 1956, с.179-210

[6] Минский М. Вычисления и автоматы, Мир, Москва, 1971

[7] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. Наука, Москва, 1985

[8] Гилл А. Введение в теорию конечных автоматов. Мир, Москва, 1966

[9] Хопкрофт Дж., Мотвани Р., Ульман Дж. Введение в теорию автоматов, языков и вычислений, Издательский дом «Вильямс», Москва, 2002

[10] Yu S., Chapter 2. Regular Languages, In: Rozenberg G., Salomaa A. (eds.) Handbook of Formal Languages, Springer-Verlag, 1998, pp. 41-110

[11] Wegener I. The Complexity of Boolean Aunctions. John Wiley & Sons Ltd. and B.G. Teubner, Stuttgart, 1987

[12] Wegener I. The Complexity of Boolean Aunctions. John Wiley & Sons Ltd. and B.G. Teubner, Stuttgart, 1987

[13] Bryant R.E. Graph Based Algorithms for Boolean Functions Manipulation, IEEE Transactions on Computers, Volume C-35, Number 8, 1986, pp. 677-692

[14] Gröpl C. Binary Decision Diagrams for Random Boolean Functions; Dissertation, Humboldt Universität zu Berlin, 1999

[15] Wegener I. Branching Programs and Binary Decision Diagrams. Theory and Applications, SIAM Monographs on Discrete Mathematics and Applications, Philadelphia, PA, 2000

[16] Champarnaud J.-M., Duchamp G., Finite Automata and Boolean Functions. *Proceedings* of SCI'2001 (Systemics, Cybernetics and Informatics), XIV, Orlando, FL, 2001, pp. 126-131

функции бита скрытого веса и др.)[17,18,19,20]. Наибольший интерес исследователей вызвала функция прямого доступа к памяти (мультиплексор). Эта функция реализована во многих электронных схемах и замечательна тем, что при прямом порядке переменных имеет максимальную автоматную сложность $O\left(\frac{2^n}{n}\right)$ [21], а при обратном – сложность $O(n^2)$ [22,23].

Автоматная сложность класса всех булевых функций была впервые рассмотрена А.Д. Кузьминым[24]. Он получил для нее оценку функции Шеннона и отметил, что ее график имеет пилообразный вид:

$$\frac{2^n}{n} \lesssim \mathbb{S}(P_2, n) \lesssim 2 \cdot \frac{2^n}{n}$$

Позже результаты Кузьмина были повторены и уточнены[25,26,27]. Хип и Мерсер[28] получили формулу для максимальной сложности ROBDD

$$\mathbb{S}_{ROBDD}(P_2, n) = 2^{n-p} + 2^{2^p} - 3$$

и отметили осцилляции графика функции Шеннона. Шампорно и Пен[29] получили (в терминах конечных автоматов) ту же оценку функции Шеннона для P_2 и привели формулу

$$\mathbb{S}(P_2, n) = 2^{n-p} - p - 2 + \sum_{i=0}^{p} 2^{2^i},$$

---

[17] Hosaka K., Takenaga Y., Yajima S. On the Size of Ordered Binary Decision Diagrams Representing Threshold Functions, Proceedings of ISAAC'1994 (International Symposium on Algorithms and Computation), Springer-Verlag, 1994, pp. 87-93

[18] Sawitzki D. Lower Bounds on the OBDD Size of Graphs of Some Popular Functions. In: Vojtáš P., Bieliková M., Charron-Bost B., Sýkora O. (eds.): SOFSEM 2005, Lecture Notes in Computer Science 3381, Springer Verlag, 2005, pp. 298–309

[19] Bollig B. The Optimal Read-Once Branching Program Complexity for the Direct Storage Access Function. Information Processing Letters, Volume 106, Issue 4, 2008, pp. 171–174

[20] Bollig B., Range N., Wegener I. Exact OBDD Bounds for Some Fundamental Functions. Theory of Computing Systems, Volume 47, Number 2, 2010, pp. 593–609

[21] Michon J.-F., Yunès J.-B., Valarcher P. On Maximal QROBDD of Boolean Functions. Theoretical Informatics and Applications, Volume 39, Issue 4, 2005, pp. 677-686

[22] Wegener I. Branching Programs and Binary Decision Diagrams. Theory and Applications, SIAM Monographs on Discrete Mathematics and Applications, Philadelphia, PA, 2000

[23] Bollig B., Löbbing M., Sauerhoff M., Wegener I. On the Complexity of the Hidden Weighted Bit Function for Various BDD Models. Theoretical Informatics and Applications, Volume 33, 1999, pp. 103-115

[24] Кузьмин А.Д. Реализация функций алгебры логики автоматами, нормальными алгорифмами и машинами Тьюринга. Проблемы кибернетики, Выпуск 13, Наука, Москва, 1955, с. 75-96

[25] Lee C.Y. Representation of Switching Circuits by Binary Decision Programs. Bell System Technical Journal, Volume 38, 1959, pp. 985-999

[26] Liaw H.-T., Lin C.-S. On the OBDD-Representation of General Boolean Functions. IEEE Transactions on Computers, Volume 41, Number 6, 1992, pp. 661-664

[27] Breitbart Y., Hunt III H., Rosenkrantz D. On the Size of Binary Decision Diagrams Representing Boolean Functions, Theoretical Computer Science, Volume 145, Issue 1-2, 1995, pp. 45-69

[28] Heap M.A., Mercer M.R. Least Upper Bounds on OBDD Sizes, IEEE Transactions on Computers, Volume 43, Issue 6, 1994, pp. 764-767

[29] Champarnaud J.-M., Pin J.-E. A Maxmin Problem on Finite Automata. Discrete Applied Mathematics, Volume 23, Issue 1, 1989, pp. 91-96

где величина p определяется через обращение функции $n(x) = 2^x + x$ или сравнение величин 2^{n-q} и 2^{2^q}. Более детально функция Шеннона класса P_2 была исследована Грёплем[30,31,32]. Он описал поведение ее графика вблизи особых точек вида $n = 2^p + p$ (вершин «зубцов» графика) и привел асимптотические оценки и точные формулы максимальной сложности QROBDD и ROBDD. Для нахождения параметра p, входящего в состав формул, используется функция $L(n) = n + \log n$ и ее оценки или сравнение величин 2^{n-q} и 2^{2^q}. В работе Мишона, Юнеса и Валаршера[33] введено понятие сложной функции из P_2 (имеющей QROBDD максимальной сложности), приведена диаграмма решений сложной функции и рассмотрены некоторые свойства и метрические характеристики сложных функций.

Сложность упорядоченных N-арных диаграмм решений для M-значных функций, рассматривалась Дворжаком[34]. В работе Грубера и Хольцера[35] исследовалась средняя сложность детерминированных и недетерминированных автоматов, представляющих конечные языки. Сложность классов конечных языков длины, равной мощности входного алфавита, рассматривалась в статье Бржозовски и Константинидиса[36].

Значимых результатов для автоматной сложности других классов Поста, в частности, для замкнутых классов монотонных функций до сих пор не получено.

Цель работы. В диссертации исследуется сложность автоматов, представляющих булевы функции из замкнутых классов Поста. Рассматривается также сложность автоматов, представляющих конечные языки.

Методы исследования. В диссертации используются методы дискретной математики, теории автоматов и теории синтеза и сложности управляющих систем.

[30] Gröpl C., Prömel H.J., A. Srivastav. Size and Structure of Random Ordered Binary Decision Diagrams (Extended Abstract). In: Krob D., Meinel C., Morvan M. eds., STACS 98, Lecture Notes in Computer Science 1373, Springer-Verlag, 1998, pp. 238-248

[31] Gröpl C. Binary Decision Diagrams for Random Boolean Functions; Dissertation, Humboldt Universität zu Berlin, 1999

[32] Gröpl C., Prömel H.J. and Srivastav A. On the Evolution of the Worst-Case OBDD Size, Information Processing Letters, Volume 77, Issue 1, 2001, pp. 1–7

[33] Michon J.-F., Yunès J.-B., Valarcher P. On Maximal QROBDD of Boolean Functions. Theoretical Informatics and Applications, Volume 39, Issue 4, 2005, pp. 677-686

[34] Dvorak V. Bounds on the Sizes of Decision Diagrams. Journal of Universal Computer Science, Volume 3, Issue 1, 1997, pp. 2-22

[35] Gruber H., Holzer M. On the Average State and Transition Complexity of Finite Languages, Theoretical Computer Science, Volume 387, Issue 2, 2007, pp. 167-176

[36] Brzozowski J., Konstantinidis S. State-Complexity Hierarchies of Uniform Languages of Alphabet-Size Length, Theoretical Computer Science, Volume 410, 2009, pp. 3223-3235

Научная новизна.

- Предложен ряд методов синтеза сложных автоматов, представляющих булевы функции и конечные языки.
- Построены автоматы максимальной или асимптотически максимальной сложности, представляющие функции из классов Поста C_j, A_j, D_j, F_j^{∞} для всех j F_k^2, $k = 2{,}3{,}6{,}7$. Получены точные формулы и/или асимптотика функции Шеннона для классов Поста. Согласно полученным результатам классы решетки Поста разбиваются на 3 группы в соответствии с асимптотическим поведением функции Шеннона.
- Для оставшихся классов Поста построены функции, автоматная сложность которых по прядку совпадает с асимптотикой функции Шеннона.
- Построены автоматы максимальной сложности, представляющие конечные языки длины n и длины не больше n. Получены точные формулы и асимптотика функции Шеннона для классов таких языков.
- Рассмотрена также связь автоматной сложности классов Поста со сложностью классов в других моделях и показано, что автоматная сложность является независимой характеристикой класса и не сводится к другим мерам сложности.

Работа имеет теоретический характер. Ее результаты могут быть полезны специалистам-исследователям Московского государственного университета им. М. В. Ломоносова, Института прикладной математики им. М. В. Келдыша РАН, Вычислительного центра им. А. А. Дородницына РАН, Института математики им. С. Л. Соболева СО РАН, Нижегородского государственного университета им. М. В. Лобачевского, Новосибирского государственного университета, Санкт-Петербургского государственного университета.

Практическая значимость.

Полученные в настоящей работе оценки показывают, что сложность программной реализации произвольной булевой функции от 50 переменных автоматами потребует 17 терабайт памяти, или микросхему, состоящую из $17 \cdot 10^{12}$ логических элементов. Если при этом функция монотонна, то потребуется в худшем случае автомат с тремя терабайтами памяти, или микросхема из $2.5\text{x}10^{12}$ логических элементов. Это обстоятельство означает, что время широкого использования произвольных булевых функций в задачах кодирования и распознавания еще не наступило. В настоящем проще и дешевле применять методы, близкие к линейным. Вместе с тем, когда память в 1000 терабайт станет доступна, эти подходы станут реализуемы на практике.

Из утверждения 3.24 главы 3 следует, что вычислять булевы функций лучше параллельно. При этом одновременное вычисление M булевых функций увеличит память всего в $\log M$ раз, а не в M раз, как это может показаться. Дело в том, что автоматы сложных булевых функций ведут себя одинаково, отличаясь лишь на небольшом заключительном участке диаграммы.

Наконец, при кодировании или распознавании с помощью конкретных булевых функции, следует проверять не только сложность полиномов используемых функций, но и находить автоматную сложность этих функций, которая может оказаться значительно меньше сложности полиномов.

С учетом представленных выше соображений результаты, представленные в диссертации, имеют важное прикладное значение.

Апробация работы. Результаты диссертации докладывались на семинарах механико-математического факультета МГУ им. М.В. Ломоносова: на семинаре «Теория автоматов» под руководством д.ф.-м.н., профессора В.Б. Кудрявцева, на семинаре «Приложения дискретных функций» под руководством д.ф.-м.н., профессора Д.Н. Бабина, а также на следующих конференциях:

1. Международная конференция «Современные проблемы математики, механики и их приложений», посвященная 70-летию ректора МГУ академика В.А. Садовничего, секция «Интеллектуальные системы и компьютерные науки», 30 марта - 2 апреля 2009 г.
2. XVI Международная конференция студентов, аспирантов и молодых ученых «Ломоносов», 13-18 апреля 2009 г.
3. X международный научный семинар «Дискретная математика и ее приложения», 1-6 февраля 2010 г.
4. Научная конференция «Ломоносовские чтения», 16-25 апреля 2010 г.
5. Международный молодежный научный форум «ЛОМОНОСОВ-2011», 11-15 апреля 2011 г.
6. Научная конференция «Ломоносовские чтения», 11-25 ноября 2011 г.
7. X Международная конференция «Интеллектуальные системы и компьютерные науки», 5-10 декабря 2011 г.
8. XI международный семинар «Дискретная математика и ее приложения», посвященный 80-летию со дня рождения академика О.Б. Лупанова, 18-23 июня 2012 г.
9. Международный молодежный научный форум «ЛОМОНОСОВ-2013», 8-13 апреля 2013 г.

Результаты, выносимые на защиту.

1. Методы и алгоритмы синтеза оптимальных автоматов, представляющих почти все булевы функции.
2. Методы и алгоритмы синтеза оптимальных автоматов, представляющих булевы функции асимптотически максимальной сложности из всех классов Поста.
3. Точные формулы и асимптотики функции Шеннона для классов Поста.
4. Сравнение функций Шеннона автоматной сложности классов Поста с функциями Шеннона этих же классов для других моделей управляющих систем.
5. Несводимость автоматной сложности булевых функций к другим мерам сложности булевых функций.

Публикации. Основное содержание диссертации опубликовано в 9 работах автора, список которых приведен в конце автореферата [1–9].

Структура работы. Диссертация состоит из введения, четырех глав, заключения, трех приложений и списка литературы, содержащего 61 наименований. Общий объем диссертации 139 страниц.

Краткое содержание работы.

Пусть A, B и Q − конечные алфавиты, $|A| = N \geq 2$, $|B| = M \geq 2$. Не ограничивая общности, можем считать, что $A = \{0,1, \dots N-1\}$, $B = \{0,1, \dots M-1\}$. Конечный алфавит мощности 2 будем обозначать через $E = \{0,1\}$. Наборы из n элементов алфавита A можно рассматривать как слова длины n в алфавите A. Обозначим через A^* множество всех непустых слов конечной длины в алфавите A.

Конечным языком L в алфавите A назовем любое непустое конечное подмножество $L \subseteq A^*$. Множество языков в алфавите A обозначим через $\mathcal{L}(A)$.

***M*-коллекцией языков** $\mathcal{C}$ из множества $\mathcal{K} \subseteq \mathcal{L}(A)$ назовем семейство попарно не пересекающихся языков $\{L_1, \dots L_{M-1}\} \subseteq \mathcal{K}$. Множество M-коллекций языков из $\mathcal{K}$ обозначим через $\mathcal{C}_M\ (\mathcal{K})$. Для M-коллекции $\mathcal{C}$ языков из $\mathcal{K}$ будем считать, что

$$L_0 = \mathcal{K} \setminus \bigcup_{i=1}^{M-1} L_i$$

Определим детерминированный конечный автомат (ДКА) и инициальный конечный автомат (ИКА) согласно[37]. **Конечным автоматом** назовем набор

$$V = (A, B, Q, \varphi, \psi),$$

где $\varphi: Q \times A \to Q$ – функция переходов, $\psi: Q \times A \to B$ – функция выходов. **Инициальным конечным автоматом** (ИКА) V_{q_0} назовем конечный автомат V с выделенным начальным состоянием q_0: $V_{q_0} = (A, B, Q, \varphi, \psi, q_0)$.

ИКА $V_{q_0} = (A, B, Q, \varphi, \psi, q_0)$ **представляет язык** $L \subseteq A^*$ с помощью подмножества выходных символов $B' \subseteq B$, если $\bar{\alpha} \in L \Leftrightarrow \psi(q_0, \bar{\alpha}) \in B'$. В этом случае говорим также, что язык L **представим** в автомате V_{q_0} с помощью B'. Обозначим представимость языка L в автомате V_{q_0} через $V_{q_0} \sim L$. Не ограничивая общности, считаем, что $B' = B \backslash \{0\}$.

ИКА $V_{q_0} = (A, B, Q, \varphi, \psi, q_0)$ **представляет *M*-коллекцию языков** $\mathcal{C} \subseteq \mathcal{L}(A)$, если $\forall\, \bar{\alpha} \in L_i$, $i = 0, \dots M-1$ выполнено $\psi(q_0, \bar{\alpha}) = i$. В этом случае говорим также, что коллекция $\mathcal{C}$ **представима** в автомате V_{q_0}. Представимость коллекции $\mathcal{C}$ в автомате V_{q_0} обозначим через $V_{q_0} \sim \mathcal{C}$.

Обозначим через $A^n = \{\bar{\alpha} \in A^* \,|\, |\bar{\alpha}| = n\}$ множество слов длины n и через $A^{\leq n} = \{\bar{\alpha} \in A^* \,|\, |\bar{\alpha}| \leq n\}$ – множество слов длины не более n в алфавите A. Положим $\mathcal{L}_n(A) = \{L \in \mathcal{L}(A) | L \subseteq A^n\}$ и $\mathcal{L}_n^{\leq}(A) = \{L \in \mathcal{L}(A) | L \subseteq A^{\leq n}\}$. Для множества языков $\mathcal{K} \subseteq \mathcal{L}(A)$ обозначим $\mathcal{K}(n) = \mathcal{K} \cap \mathcal{L}_n(A)$ и $\mathcal{K}^{\leq}(n) = \mathcal{K} \cap \mathcal{L}_n^{\leq}(A)$.

Сложностью $\mathbb{S}(V_q)$ автомата V_q назовем $|Q|$ – число состояний в автомате V_q. **Сложностью языка** $L \in \mathcal{L}(A)$ назовем величину

$$\mathbb{S}(L) = \min_{V_q \sim L} \mathbb{S}(V_q)$$

Сложностью *M*-коллекции $\mathcal{C} \subseteq \mathcal{L}(A)$ назовем величину

$$\mathbb{S}(\mathcal{C}) = \min_{V_q \sim \mathcal{C}} \mathbb{S}(V_q)$$

Функциями Шеннона множества $\mathcal{K} \subseteq \mathcal{L}(A)$ назовем величины

$$\mathbb{S}(\mathcal{K}, n) = \max_{L \in \mathcal{K}(n)} \mathbb{S}(L), \qquad \mathbb{S}^{\leq}(\mathcal{K}, n) = \max_{L \in \mathcal{K}^{\leq}(n)} \mathbb{S}(L),$$

$$\mathbb{S}_{N,M}(\mathcal{K}, n) = \max_{\mathcal{C} \in \mathcal{C}_M(\mathcal{K}(n))} \mathbb{S}(\mathcal{C}), \qquad \mathbb{S}_{N,M}^{\leq}(\mathcal{K}, n) = \max_{\mathcal{C} \in \mathcal{C}_M(\mathcal{K}^{\leq}(n))} \mathbb{S}(\mathcal{C}).$$

Множество A^n можно рассматривать как n-мерный N-значный куб $A^n = A \times \ldots \times A$. Через E^n будем обозначать n-мерный двоичный куб. Через $P_{N,M}^n$

[37] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. Наука, Москва, 1985

обозначим множество M-значных функций, определенных на A^n, $P^n_{N,M} = \{f | f: A^n \to B\}$ и положим $P_{N,M} = \bigcup_{n \geq 0} P^n_{N,M}$. Через P^n_2 обозначим множество всех булевых функций от n переменных и положим $P_2 = \bigcup_{n \geq 0} P^n_2$. Если $\mathcal{K} \subseteq P_{N,M}$ ($\mathcal{K} \subseteq P_2$), положим $\mathcal{K}(n) = \mathcal{K} \cap P^n_{N,M}$ ($\mathcal{K} \cap P^n_2$).

Существует взаимно-однозначное соответствие между языками из $\mathcal{L}_n(E)$ и функциями из P^n_2, определяемое условием $\bar{\alpha} \in L \Leftrightarrow f(\bar{\alpha}) = 1$. Будем говорить, что в этом случае язык L соответствует функции f, $L \sim f$. Будем считать, что автомат V_{q_0}, представляющий язык $L \in \mathcal{L}_n(E)$, представляет и соответствующую ему функцию $f \in P^n_2$ – $V_{q_0} \sim f$.

Назовем **сложностью** $\mathbb{S}(f)$ **булевой функции** f сложность $\mathbb{S}(L)$ языка L, $L \sim f$. **Функцией Шеннона** множества булевых функций $\mathcal{K} \subseteq P^n_2$ назовем величину $\mathbb{S}(\mathcal{K}, n) = \max\limits_{L \sim f, f \in \mathcal{K}(n)} \mathbb{S}(L)$. Аналогично определяется взаимно-однозначное соответствие между M-коллекциями из $\mathcal{C}_M\big(\mathcal{L}_n(A)\big)$ и функциями из $P^n_{N,M}$: $\bar{\alpha} \in L_i \Leftrightarrow f(\bar{\alpha}) = i$, $i = 0, \dots M-1$. В этом случае коллекция $\mathcal{C}$ соответствует функции f, $\mathcal{C} \sim f$. Будем считать, что автомат V_{q_0}, представляющий коллекцию $\mathcal{C} \in \mathcal{C}_M\big(\mathcal{L}_n(A)\big)$, представляет и соответствующую ей функцию $f \in P^n_{N,M}$ – $V_{q_0} \sim f$.

Назовем **сложностью** $\mathbb{S}(f)$ **функции** $f \in P^n_{N,M}$ сложность $\mathbb{S}(\mathcal{C})$ M-коллекции $\mathcal{C}$, $\mathcal{C} \sim f$. **Функцией Шеннона** множества функций $\mathcal{K} \subseteq P^n_{N,M}$ назовем величину $\mathbb{S}_{N,M}(\mathcal{K}, n) = \max\limits_{\mathcal{C} \sim f, f \in \mathcal{K}(n)} \mathbb{S}(\mathcal{C})$.

В **Главе 1** рассматриваются методы построения сложных автоматов, представляющих конечные языки, коллекции языков и функции. Общий подход к синтезу автоматов заключается в построении диаграммы автомата путем объединения прямого и обратного деревьев. Выбор деревьев и способов их объединения позволяет получить автоматы для языков и функций из различных классов.

Разработан оригинальный метод синтеза сложных автоматов, представляющих монотонные функции. Для этого используется специальное отображение единичного куба в множество монотонных булевых функций, названное монотонным вложением.

Найден простой способ вычисления параметра p (высоты обратного дерева), входящего в состав формул сложности построенных автоматов. При этом не требуется сравнение величин вида 2^{n-q} и 2^{2^q} или обращение функций вида $n(x) = 2^x + x$. В **Приложении А** приведены формулы вычисления высоты обратного дерева для построенных сложных автоматов.

В **Главе 2** предложенные методы используются для оценки автоматной сложности замкнутых классов булевых функций. Приведем обозначения замкнутых классов, введенных Постом[38,39], и их описания:

- $C_i,\ i = 1, \dots 4$ – все булевы функции, все функции сохраняющие 0 и/или 1.
- $A_i,\ i = 1, \dots 4$ – все монотонные функции, все монотонные функции сохраняющие 0 и/или 1.
- $D_i,\ i = 1,2,3$ – все самодвойственные α-функции, все монотонные самодвойственные функции, все самодвойственные функции.
- $F_1^\mu,\ \mu = 2, \dots \infty$ – все α-функции, удовлетворяющие условию $\langle \alpha^\mu \rangle$
- $F_2^\mu,\ \mu = 2, \dots \infty$ – все монотонные α-функции, удовлетворяющие условию $\langle \alpha^\mu \rangle$
- $F_3^\mu,\ \mu = 2, \dots \infty$ – все монотонные функции, удовлетворяющие условию $\langle \alpha^\mu \rangle$.
- $F_4^\mu,\ \mu = 2, \dots \infty$ – все функции, удовлетворяющие условию $\langle \alpha^\mu \rangle$.
- $F_5^\mu,\ \mu = 2, \dots \infty$ – все α-функции, удовлетворяющие условию $\langle \mathrm{A}^\mu \rangle$.
- $F_6^\mu,\ \mu = 2, \dots \infty$ – все монотонные α-функции, удовлетворяющие условию $\langle \mathrm{A}^\mu \rangle$.
- $F_7^\mu,\ \mu = 2, \dots \infty$ – все монотонные функции, удовлетворяющие условию $\langle \mathrm{A}^\mu \rangle$
- $F_8^\mu,\ \mu = 2, \dots \infty$ – все функции, удовлетворяющие условию $\langle \mathrm{A}^\mu \rangle$.
- $L_i,\ i = 1, \dots 5$ – классы линейных функций.
- $S_i,\ i = 1,3,5,6$ – классы логических сумм.
- $P_i,\ i = 1,3,5,6$ – классы логических произведений.
- $O_i,\ i = 1, \dots 9$ – классы констант и/или переменных.

Вышеперечисленные классы образуют решетку Поста[40].

Для классов $C_1, C_2, C_3, C_4, D_1, D_3, F_1^\infty, F_4^\infty, F_5^\infty, F_8^\infty$получены точные значения и асимптотика функции Шеннона, а также построены автоматы,

[38] Post E. Two-valued Iterative Systems. Princeton University Press, 1941

[39] Post E. Introduction to a General Theory of Elementary Propositions, American Journal of Mathematics, Volume 43, Number 1, 1921, pp. 163-185

[40] Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б. Функции алгебры логики и классы Поста. Наука, Москва, 1966

представляющие самые сложные функции в классах. Показано, что классы F_j^2, $j = 1,4,5,8$, существенно сложнее в автоматном смысле, чем соответствующие классы F_j^∞.Считаем далее, что $p, n \in \mathbb{N}$, положим $\tilde{n}(p) = 2^p + p$.

Теорема 2.1. $\forall p \geq 1, n \in [\tilde{n}(p), \tilde{n}(p+1))$ и $\mathcal{K} \in \{C_1, C_2, C_3, C_4\}$ существует такая функция $f_n \in \mathcal{K}(n)$, что

$$\mathbb{S}(\mathcal{K}, n) = \mathbb{S}(f_n) = 2^{n-p} - p - 2 + \sum_{i=0}^{p} 2^{2^i}.$$

Теорема 2.2. $\forall p \geq 1$, $n \in [\tilde{n}(p), \tilde{n}(p+1))$ и класса $\mathcal{K} \in \{D_1, D_3\}$ существует такая функция $f_{n,s} \in \mathcal{K}(n)$, что

$$\mathbb{S}(\mathcal{K}, n) = \mathbb{S}\left(f_{n,s}\right) = 2^{n-p} - p - 2 - u(p) + \sum_{i=0}^{p} 2^{2^i},$$

где $u(p) = \begin{cases} 2^{2^{p-1}-1} & \text{при } n = \tilde{n}(p) \\ 0 & \text{иначе} \end{cases}$.

Теорема 2.3. При $n \to \infty$ и $\mathcal{K} \in \{C_1, C_2, C_3, C_4, D_1, D_3\}$

$$\frac{2^n}{n} \lesssim \mathbb{S}(\mathcal{K}, n) \lesssim 2 \cdot \frac{2^n}{n},$$

и при $p \longrightarrow \infty$, $n \in [\tilde{n}(p), \tilde{n}(p+1))$, $n \sim \alpha \cdot 2^p$, $\alpha \in (1,2]$ выполнено

$$\mathbb{S}(\mathcal{K}, n) \sim \alpha \cdot \frac{2^n}{n}$$

Теорема 2.4. $\forall p \geq 2$ и $\mathcal{K} \in \{F_j^\infty,\ j = 1,4,5,8\}$ существует такая функция $f_{n,\infty} \in \mathcal{K}(n)$, что при $n \in (\tilde{n}(p) + 1, \tilde{n}(p+1) + 1)$

$$\mathbb{S}(\mathcal{K}, n) = \mathbb{S}\left(f_{n,\infty}\right) = \frac{3}{4} \cdot 2^{n-p} - p - u(j) + \sum_{i=0}^{p} 2^{2^i},$$

и при $n = \tilde{n}(p) + 1$

$$\mathbb{S}(\mathcal{K}, n) = \mathbb{S}\left(f_{n,\infty}\right) = 2^{n-p} - p - 1 - u(j) + \sum_{i=0}^{p} 2^{2^i},$$

где $u(j) = \begin{cases} 1 & \text{при } j = 1,4 \\ 2 & \text{при } j = 5,8 \end{cases}$.

Теорема 2.5. При $n \to \infty$ и $\mathcal{K} \in \{F_j^{\infty},\ j = 1,4,5,8\}$

$$\frac{3}{4} \cdot \frac{2^n}{n} \lesssim \mathbb{S}(\mathcal{K}, n) \lesssim \frac{3}{2} \cdot \frac{2^n}{n},$$

и при $p \longrightarrow \infty$, $n \sim \alpha \cdot 2^p$, $\alpha \in (1,2]$, $n \in [\tilde{n}(p) + 1, \tilde{n}(p+1) + 1)$ выполнено

$$\mathbb{S}(\mathcal{K}, n) \sim \frac{3\alpha}{4} \cdot \frac{2^n}{n}$$

Теорема 2.6. $\forall p \geq 1$ и $\mathcal{K} \in \{F_j^2,\ j = 1,4,5,8\}$ существует такая функция $f_{n,2} \in \mathcal{K}(n)$, что при $n \in (\tilde{n}(p) + 1, \tilde{n}(p+1) + 1)$

$$\mathbb{S}(\mathcal{K}, n) \geq \mathbb{S}(f_{n,2}) = \frac{3}{4} \cdot 2^{n-p} - p - u(j) + 2^{2^p - 1} + \sum_{i=0}^{p} 2^{2^i},$$

где $u(j) = \begin{cases} 1 & \text{при } j = 1,4 \\ 2 & \text{при } j = 5,8 \end{cases}$, и при $n = \tilde{n}(p) + 1$

$$\mathbb{S}(\mathcal{K}, n) \geq \mathbb{S}(f_{n,2}) = 2^{n-p} - p - 1 + \sum_{i=0}^{p} 2^{2^i}$$

Следствие 2.1. При $p \to \infty$, $n = 2^p + p + 1 + i$, $i \in \mathbb{N}$ выполнено $\mathbb{S}(F_j^2, n) \gtrsim d_i \cdot \mathbb{S}(F_j^{\infty}, n)$ для некоторого $d_i > 1$ и $j = 1,4,5,8$.

Следствие 2.2. При $n \to \infty$ и $\mathcal{K} \in \{F_j^{\mu}, \mu \geq 2, j = 1,4,5,8\}$ выполнено

$$\frac{3}{4} \cdot \frac{2^n}{n} \lesssim \mathbb{S}(\mathcal{K}, n) \lesssim 2 \cdot \frac{2^n}{n}$$

Для классов $A_1, A_2, A_3, A_4, D_2, F_2^2, F_3^2, F_6^2, F_7^2, F_2^{\infty}, F_3^{\infty}, F_6^{\infty}, F_7^{\infty}$ получены асимптотические оценки функции Шеннона и построены автоматы, представляющие сложные функции. Показано, что числовая ось, представляющая аргумент функции Шеннона (число переменных), распадается на последовательность пар интервалов, на бóльших из которых функция Шеннона асимптотически равна сложности построенных функций, а на меньших превосходит ее не более, чем вдвое.

Положим $\hat{n}(p) = \binom{p}{\lfloor p/2 \rfloor} + p$, $\check{n}(p) = \binom{p}{\lfloor p/2 + 1 \rfloor} + p$, $c = \sqrt{2/\pi}$.

Теорема 2.7. При $p \to \infty$, $n \in (\hat{n}(p-1), \hat{n}(p) + p \bmod 2]$ и $\mathcal{K} \in \{A_1, A_2, A_3, A_4\}$ существует такая функция $g_n \in \mathcal{K}(n)$, что

$$\mathbb{S}(g_n) \gtrsim 2^{n-p+1}$$

Для функции g_n выполнено

$$\mathbb{S}(\mathcal{K}, n) \lesssim 2 \cdot \mathbb{S}(g_n)$$

и при $n \sim \alpha \binom{p}{\lfloor p/2 \rfloor}$, $\alpha \in \left(\frac{1}{2}, 1\right]$, $n \in (\hat{n}(p-1), \hat{n}(p)]$ имеет место асимптотическая оценка

$$\mathbb{S}(\mathcal{K}, n) \sim \mathbb{S}(g_n) \sim \frac{2\alpha c}{\sqrt{\log n}} \cdot \frac{2^n}{n}$$

Теорема 2.8. При $p \to \infty$, $n \in (\check{n}(p-1), \check{n}(p)]$ и $\mathcal{K} \in \left\{F_j^2, j = 2{,}3{,}6{,}7\right\}$ существует такая функция $g_{n,2} \in \mathcal{K}(n)$, что

$$\mathbb{S}(g_{n,2}) \gtrsim 2^{n-p+1}$$

Для функции $g_{n,2}$ выполнено

$$\mathbb{S}(\mathcal{K}, n) \lesssim 2 \cdot \mathbb{S}(g_{n,2})$$

и при $n \sim \alpha \binom{p}{\lfloor p/2 \rfloor}$, $\alpha \in \left(\frac{1}{2}, 1\right]$, $n \in (\check{n}(p-1), \check{n}(p)]$ имеет место асимптотическая оценка

$$\mathbb{S}(\mathcal{K}, n) \sim \mathbb{S}(g_{n,2}) \sim \frac{2\alpha c}{\sqrt{\log n}} \cdot \frac{2^n}{n}$$

Теорема 2.9. При $p \to \infty$, $n \in (\check{n}(p-1) + 1, \check{n}(p) + 1]$ существует такая функция $g_{n,s} \in D_2(n)$, что

$$\mathbb{S}(g_{n,s}) \gtrsim 2^{n-p+1}$$

Для функции $g_{n,s}$ выполнено

$$\mathbb{S}(D_2, n) \lesssim 2 \cdot \mathbb{S}(g_{n,s})$$

и при $n \sim \alpha \binom{p}{\lfloor p/2 \rfloor}$, $\alpha \in \left(\frac{1}{2}, 1\right]$, $n \in (\check{n}(p-1) + 1, \check{n}(p) + 1]$ имеет место асимптотическая оценка

$$\mathbb{S}(D_2, n) \sim \mathbb{S}(g_{n,s}) \sim \frac{2\alpha c}{\sqrt{\log n}} \cdot \frac{2^n}{n}$$

Теорема 2.10. При $p \to \infty$, $n \in (\hat{n}(p-1) + 1, \hat{n}(p) + 1 + p \bmod 2]$ и $\mathcal{K} \in \left\{F_j^\infty, j = 2{,}3{,}6{,}7\right\}$ существует такая функция $g_{n,\infty} \in \mathcal{K}(n)$, что

$$\mathbb{S}(g_{n,\infty}) \gtrsim \frac{3}{4} \cdot 2^{n-p+1}$$

Для функции $g_{n,\infty}$ выполнено

$$\mathbb{S}(\mathcal{K}, n) \lesssim 2 \cdot \mathbb{S}(g_{n,\infty})$$

и при $n \sim \alpha \binom{p}{\lfloor p/2 \rfloor}$, $\alpha \in \left(\frac{1}{2}, 1\right]$, $n \in (\hat{n}(p-1)+1, \hat{n}(p)+1]$ имеет место асимптотическая оценка

$$\mathbb{S}(\mathcal{K}, n) \sim \mathbb{S}(g_{n,\infty}) \sim \frac{3\alpha c}{2\sqrt{\log n}} \cdot \frac{2^n}{n}$$

Следствие 2.3. При $p \to \infty$ и $\mathcal{K} \in \left\{F_j^{\mu}, \mu \geq 3, j = 2,3,6,7\right\}$ выполнено

$$\frac{3c}{4\sqrt{\log n}} \cdot \frac{2^n}{n} \lesssim \mathbb{S}(\mathcal{K}, n) \lesssim \frac{2c}{\sqrt{\log n}} \cdot \frac{2^n}{n}$$

Далее рассматривается автоматная сложность классов Поста F_j^{μ}, $\mu \geq 3$. Для нетривиальных подмножеств $F_j^{\mu} \backslash F_j^{\mu+1}$ этих классов получены нижние асимптотические оценки функции Шеннона и построены автоматы, представляющие сложные функции. Сложность построенных функций из классов F_j^{μ} по порядку совпадает с функцией Шеннона для объемлющих классов (C_1 и A_1). Вопрос о точных асимптотических оценках функции Шеннона для этих классов остается открытым. Считаем далее, что $\mu \in \mathbb{N}$.

Теорема 2.11. $\forall \mu \geq 3$, $p > \log(\mu - 1)$ и $\mathcal{K} \in \{F_j^{\mu} \backslash F_j^{\mu+1},\ j = 1,4,5,8\}$ существует такая функция $f_{n,\mu} \in \mathcal{K}(n)$, что

при $n \in (\tilde{n}(p) + \mu - 1, \tilde{n}(p+1) + \mu)$:

$$\mathbb{S}(f_{n,\mu}, n) = \frac{\mu+1}{2^{\mu}} \cdot 2^{n-p} - p - 3 + (\mu - 1) \cdot \left(2^{2^{p}-1} + u(j)\right) + \sum_{i=0}^{p} 2^{2^i},$$

и при $n = \tilde{n}(p) + \mu - 1$:

$$\mathbb{S}(f_{n,\mu}, n) = \frac{\mu}{2^{\mu-1}} \cdot 2^{n-p} - p - 2 + (\mu - 1) \cdot u(j) + \sum_{i=0}^{p} 2^{2^i},$$

где $u(j) = \begin{cases} 2 & \text{при } j = 1,4 \\ 1 & \text{при } j = 5,8 \end{cases}.$

При $p \to \infty$, $n \sim \alpha \cdot 2^p$, $\alpha \in [1,2]$, $n \in (\tilde{n}(p) + \mu - 1, \tilde{n}(p+1) + \mu)$ выполнено

$$\mathbb{S}(\mathcal{K}, n) \gtrsim \mathbb{S}(f_{n,\mu}, n) \gtrsim \alpha \cdot \frac{\mu+1}{2^{\mu}} \cdot \frac{2^n}{n},$$

при $n = \tilde{n}(p) + \mu - 1$ выполнено

$$\mathbb{S}(\mathcal{K},n) \gtrsim \mathbb{S}(f_{n,\mu},n) \gtrsim \frac{\mu}{2^{\mu-1}}\cdot\frac{2^n}{n}$$

Теорема 2.12.
$\forall\mu \geq 2,\, p > \max(\log(\mu+1-\lfloor\log(\mu+2)\rfloor), \log\lfloor\log(\mu+2)\rfloor+1)$,
$n \in [\tilde{n}(p)+\mu+1-\lfloor\log(\mu+2)\rfloor, \tilde{n}(p+1)+\mu+1-\lfloor\log(\mu+2)\rfloor + p \bmod 2)$ и $\mathcal{K} \in \{F_j^{\mu}\backslash F_j^{\mu+1},\ i = 1{,}4{,}5{,}8\}$ существует такая функция $\hat{f}_{n,\mu} \in \mathcal{K}(n)$, что

$$\mathbb{S}(\hat{f}_{n,\mu},n) = \frac{(\mu+2)(\mu+3)+2}{2^{\mu+3}}\cdot 2^{n-p} - p + u(\mu,j) + \sum_{i=0}^{p} 2^{2^i},$$

где $u(\mu,j) = \begin{cases}\mu-2 & \text{при } j = 1{,}4\\ -2 & \text{при } j = 5{,}8\end{cases}.$

При $p \to \infty$, $n \sim \alpha\cdot 2^p$, $\alpha \in [1,2]$,
$n \in [\tilde{n}(p)+\mu+1-\lfloor\log(\mu+2)\rfloor, \tilde{n}(p+1)+\mu+1-\lfloor\log(\mu+2)\rfloor + p \bmod 2)$
выполнено

$$\mathbb{S}(\mathcal{K},n) \gtrsim \mathbb{S}(\hat{f}_{n,\mu},n) \gtrsim \alpha\cdot\frac{(\mu+2)(\mu+3)+2}{2^{\mu+3}}\cdot\frac{2^n}{n}$$

Теорема 2.13. При $p \to \infty$, $\mu \geq 2$ и $\mathcal{K} \in \{F_j^{\mu}\backslash F_j^{\mu+1},\ j = 2{,}3{,}6{,}7\}$ существует такая функция $g_{n,\mu} \in \mathcal{K}(n)$, что при $n \sim \alpha\binom{p}{\lfloor p/2\rfloor}$, $\alpha \in \left[\frac{1}{2},1\right]$ и $n \in (\check{n}(p-1)+\mu-2, \check{n}(p)+\mu-2]$ имеет место асимптотическая оценка

$$\mathbb{S}(\mathcal{K},n) \gtrsim \mathbb{S}(g_{n,\mu},n) \gtrsim \frac{\mu}{2^{\mu-1}}\cdot\frac{2\alpha c}{\sqrt{\log n}}\cdot\frac{2^n}{n}, \qquad c = \sqrt{2/\pi}.$$

Теорема 2.14. При $p \to \infty$, $\mu \geq 2$, $n \sim \alpha\binom{p}{\lfloor p/2\rfloor}$, $\alpha \in \left[\frac{1}{2},1\right]$ и
$n \in (\hat{n}(p-1)+\mu+1-\lceil\log(\mu+2)\rceil, \hat{n}(p)+\mu+1-\lceil\log(\mu+2)\rceil]$ и
$\mathcal{K} \in \{F_j^{\mu}\backslash F_j^{\mu+1},\ j = 2{,}3{,}6{,}7\}$ существует такая функция $\hat{g}_{n,\mu} \in \mathcal{K}(n)$, что

$$\mathbb{S}(\mathcal{K},n) \gtrsim \mathbb{S}(\hat{g}_{n,\mu},n) \gtrsim \frac{(\mu+2)(\mu+3)+2}{2^{\mu+3}}\cdot\frac{2\alpha c}{\sqrt{\log n}}\cdot\frac{2^n}{n}, \qquad c = \sqrt{2/\pi}.$$

Приведенные выше утверждения суммирует **Теорема 2.15**, опирающаяся на известные оценки сложности[41].

Теорема 2.15. Для следующих классов достижимы точные значения автоматной сложности:

[41] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. Наука, Москва, 1985

- $\mathbb{S}(L_i, n) = 2n$, i=1,2,3,4,5.
- $\mathbb{S}(S_i, n) = 2n$, i=1,3,5,6.
- $\mathbb{S}\big(P_i(n)\big) = n + 1$, i=1,3,5,6.
- $\mathbb{S}\big(O_i(n)\big) = n + 1$, i=1,2,4,5,6,7,8,9.
- $\mathbb{S}\big(O_3(n)\big) = 1$.

Таким образом, имеет место разбиение решетки классов Поста на три пояса в соответствии с асимптотикой автоматной сложности. На **Рис. 1** изображена решетка Поста с поясами, обозначенными черным, серым и белым цветами.

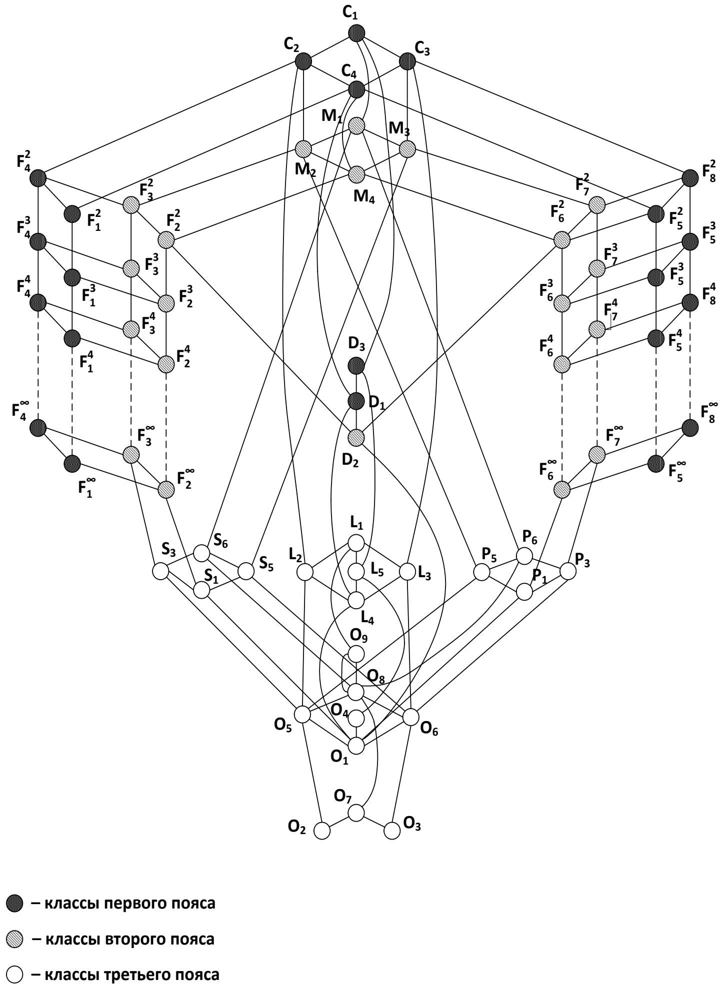

Рис. 1. Разбиение решетки классов Поста в соответствии с асимптотикой автоматной сложности

Пусть $\widetilde{m} = \{m_i\}$ – строго возрастающая последовательность, $m_i \to \infty$. Если $\mathcal{K}$ – один из классов первого пояса $C_1, C_2, C_3, C_4, D_1, D_3, F_1^\infty, F_4^\infty, F_5^\infty, F_8^\infty$, $F_1^\mu, F_4^\mu, F_5^\mu, F_8^\mu$ или его подмножество, положим $\widetilde{\mathbb{S}}(\mathcal{K}, n) = \frac{2^n}{n}$. Если $\mathcal{K}$ – один из классов второго пояса $A_1, A_2, A_3, A_4, D_2, F_2^2, F_3^2, F_6^2, F_7^2, F_2^\infty, F_3^\infty F_6^\infty, F_7^\infty, F_2^\mu, F_3^\mu$, F_6^μ, F_7^μ или его подмножество, положим $\widetilde{\mathbb{S}}(\mathcal{K}, n) = \frac{\sqrt{2/\pi}}{\sqrt{\log n}} \cdot \frac{2^n}{n}$. Если $\mathcal{K}$ – один из классов третьего пояса, $\widetilde{\mathbb{S}}(\mathcal{K}, n) = n$.

Назовем **константой автоматной сложности** последовательности функций $\{f_i\}$, $f_i \in \mathcal{K}(m_i)$ и представляющих их автоматов $\{V_{q,i}\}$, где $\mathcal{K}$ – класс Поста, величины

$$\mathbb{A}(f_i, \widetilde{m}) = \lim_{i\to\infty} \frac{\mathbb{S}(f_i)}{\widetilde{\mathbb{S}}(\mathcal{K}, m_i)} \text{ и } \mathbb{A}(V_{q,i}, \widetilde{m}) = \lim_{i\to\infty} \frac{\mathbb{S}(V_{q,i})}{\widetilde{\mathbb{S}}(\mathcal{K}, m_i)}$$

(если пределы существуют). Назовем **константой автоматной сложности** для $\mathcal{K}$ и $\widetilde{m}$, где $\mathcal{K}$ – класс Поста или его подмножество, величину

$$\mathbb{A}(\mathcal{K}, \widetilde{m}) = \lim_{i\to\infty} \frac{\mathbb{S}(\mathcal{K}, m_i)}{\widetilde{\mathbb{S}}(\mathcal{K}, m_i)}$$

(если предел существует).

В **Главе 3** рассматриваются более сложные языки. Получены точные значения и асимптотика функции Шеннона для классов конечных языков $\mathcal{L}_n(A)$ и $\mathcal{L}_n^{\leq}(A)$. Построены автоматы, представляющие самые сложные коллекции языков. Такие автоматы моделируют процесс выбора одного из M возможных решений при N альтернативах на каждом шаге.

Считаем далее, что $M, N \in \mathbb{N}$, $M, N \geq 2$, $|A| = N$, $p, n \in \mathbb{N}$, положим $\tilde{n}_{N,M}(p) = N^p \cdot \log_N M + p$, $\ddot{n}_{N,M}(p) = \log_N \left(M^{\cdot \frac{N^{p+1}-N}{N-1}} - M^{\cdot \frac{N^p - N}{N-1}} \right) + p$.

Теорема 3.1. $\forall p \geq 1$, $n \in \left[\tilde{n}_{N,M}(p), \tilde{n}_{N,M}(p+1)\right)$ существует такая M-коллекция языков $\mathcal{C}_{N,M,n} \in \mathcal{C}_M(\mathcal{L}_n(A))$, что

$$\mathbb{S}_{N,M}(\mathcal{L}(A), n) = \mathbb{S}(\mathcal{C}_{N,M,n}) = \mathbb{S}(f_{N,M,n}) == \frac{N^{n-p} - 1}{N - 1} - p - M + 1 + \sum_{i=0}^{p} M^{N^i}.$$

Теорема 3.2. При $p \to \infty$ для функции Шеннона $\mathbb{S}_{N,M}$ верно

$$\frac{\log_N M}{N-1} \cdot \frac{N^n}{n} \lesssim \mathbb{S}_{N,M}(\mathcal{L}(A), n) \lesssim \frac{N \cdot \log_N M}{N-1} \cdot \frac{N^n}{n},$$

и при $n \sim \alpha \cdot N^p \cdot \log_N M$, $\alpha \in (1, N]$, $n \in \left(\tilde{n}_{N,M}(p), \tilde{n}_{N,M}(p+1)\right]$ выполнено

$$\mathbb{S}_{N,M}(\mathcal{L}(A), n) \sim \frac{\alpha \cdot \log_N M}{N-1} \cdot \frac{N^n}{n}$$

Теорема 3.3. $\forall p \geq 1$, $n \in \left(\ddot{n}_{N,M}(p-1), \ddot{n}_{N,M}(p)\right]$ существует такая M-коллекция языков $\ddot{\mathcal{C}}_{N,M,n} \in \mathcal{C}_M(\mathcal{L}_n^{\leq}(A))$, что

$$\mathbb{S}^{\lesssim}_{N,M}(\mathcal{L}(A), n) = \mathbb{S}\left(\ddot{\mathcal{C}}_{N,M,n}\right) = \frac{N^{n-p+1} - 1}{N - 1} + M^{\frac{N^p - N}{N-1}}$$

Теорема 3.4. При $p \to \infty$ для функции Шеннона $\mathbb{S}^{\lesssim}_{N,M}$ верно

$$\frac{N \cdot \log_N M}{(N-1)^2} \cdot \frac{N^n}{n} \lesssim \mathbb{S}^{\lesssim}_{N,M}(\mathcal{L}(A), n) \lesssim \frac{N^2 \cdot \log_N M}{(N-1)^2} \cdot \frac{N^n}{n}$$

и при $n \sim \frac{\alpha \log_N M}{N-1} N^p$, $\alpha \in [1, N]$, $n \in \left(\ddot{n}_{N,M}(p-1), \ddot{n}_{N,M}(p)\right]$ выполнено

$$\mathbb{S}^{\lesssim}_{N,M}(\mathcal{L}(A), n) \sim \frac{\alpha\, N \cdot \log_N M}{(N-1)^2} \cdot \frac{N^n}{n}$$

В **Главе 4** рассматриваются другие меры сложности булевых функций и их классов, а также их соотношение с автоматной сложностью.

Покрывающим автоматом U_p для ИКА V_q, представляющего конечный язык $L \subseteq A^*$, назовем автомат, представляющий (не обязательно конечный) язык $\tilde{L} \subseteq A^*$, $\tilde{L} \cap A^l = L$, где $l = \max\limits_{\bar{\alpha} \in L} |\bar{\alpha}|$[42].

Покрывающим автоматом U_p для ИКА V_q, представляющего M-коллекцию языков $\mathcal{C} \subseteq \mathcal{L}(A)$, назовем автомат, представляющий M-коллекцию (не обязательно конечных) попарно не пересекающихся языков $\tilde{\mathcal{C}} = \{\tilde{L}_1, \dots \tilde{L}_{M-1}\}$, $\tilde{L} \subseteq A^*$, $\tilde{L}_i \cap A^l = L_i$, где l – максимальная длина слова в языках $L_1, \dots L_{M-1}$. Обозначим через $U_p \succ V_q$ то, что автомат U_p является покрывающим для ИКА V_q. $\bar{\alpha} \in L_i, i = 1, \dots M$.

Сложностью покрытия автомата V_q назовем величину $\mathbb{S}^{\succ}\left(V_q\right) = \min\limits_{U_p \succ V_q} \mathbb{S}\left(U_p\right)$. Сложностью покрытия языка $L \in \mathcal{L}(A)$ назовем величину $\mathbb{S}^{\succ}(L) = \min\limits_{V_q \sim L} \mathbb{S}^{\succ}\left(V_q\right)$. Сложностью покрытия M-коллекции $\mathcal{C} \subseteq \mathcal{L}(A)$ назовем величину $\mathbb{S}^{\succ}(\mathcal{C}) = \min\limits_{V_q \sim \mathcal{C}} \mathbb{S}^{\succ}\left(V_q\right)$. Сложностью покрытия $\mathbb{S}^{\succ}(f)$ функции f из P_2^n или $P_{N,M}^n$ считаем сложность покрытия соответствующего языка или коллекции.

[42] Câmpeanu C., Sântean N., S., Yu S. Minimal Cover Automata for Finite Languages, In: Champarnaud J.-M., Maurel D., Ziadi D. eds., WIA'98, Lecture Notes in Computer Science 1660, Springer-Verlag, 1999, pp. 43-56

Было показано[43,44,45,46], что для некоторых языков можно построить покрывающие автоматы значительно меньшей сложности, чем автоматы, представляющие эти языки. Однако, для сложных функций из теорем **Главы 2** и сложных коллекций из теорем **Главы 3** это не так:

Теорема 4.1. Для функции
$f \in \{f_n, f_{n,s}, f_{n,2}, f_{n,\infty}, g_n, g_{n,s}, g_{n,2}, g_{n,\infty}\}$ выполнено

$$\mathbb{S}^{\succ}(f) = \mathbb{S}(f)$$

Теорема 4.2. Для коллекции $\mathcal{C} \in \{\mathcal{C}_{N,M,n}, \ddot{\mathcal{C}}_{N,M,n}\}$ выполнено

$$\mathbb{S}^{\succ}(\mathcal{C}) = \mathbb{S}(\mathcal{C})$$

То есть, построение покрывающих автоматов для этих функций и коллекций не приводит к уменьшению сложности.

Булеву функцию от n переменных можно представить в виде **полинома Жегалкина[47]**, причем существует взаимно-однозначное соответствие между булевыми функциями и полиномами Жегалкина:

$$f(x_1, \dots x_n) = \bigoplus_{\bar{\alpha} \in E^n} b_{\bar{\alpha}} x_1^{\alpha_1} \dots x_n^{\alpha_n}, \quad b_{\bar{\alpha}} \in E$$

Сложность полинома Жегалкина $\mathbb{S}^{\oplus}(f)$ функции f определяется как число ненулевых коэффициентов $b_{\bar{\alpha}}$. Сложности реализации булевых функций полиномами Жегалкина и конечными автоматами не связаны друг с другом. Так, для функции f_0, равной единице лишь на наборе 0^n выполнено $\mathbb{S}^{\oplus}(f_0) = 2^n$ и $\mathbb{S}(f_0) = n + 1$. В свою очередь, сложность полиномов Жегалкина для булевых функций, представляемых сложными автоматами может кардинально отличаться.

Теорема 4.3. При $p \to \infty$ существуют функции f_n' и f_n'' для которых $\mathbb{S}(f_n') = \mathbb{S}(f_n'') \sim \frac{2^{n+1}}{n}$, $\mathbb{S}^{\oplus}(f_n') \sim n$ и $\mathbb{S}^{\oplus}(f_n') \sim 2^n$. $\mathbb{S}^{\succ}(f) = \mathbb{S}(f)$

Автоматная сложность классов Поста коррелирует с некоторыми другими мерами сложности. Например, классы Поста распадаются относительно логарифма мощности класса на те же 3 пояса. Для классов $\mathcal{K}$ первого пояса

---

[43] Champarnaud J.-M., Michon J.-F. Automata and Binary Decision Diagrams, In: Champarnaud J.-M., Maurel D., Ziadi D. eds., WIA'98, Lecture Notes in Computer Science 1660, Springer-Verlag, 1999, pp. 178-182

[44] Champarnaud J.-M., Duchamp G., Finite Automata and Boolean Functions. *Proceedings* of SCI'2001 (Systemics, Cybernetics and Informatics), XIV, Orlando, FL, 2001, pp. 126-131

[45] Champarnaud J.-M., Pin J.-E. A Maxmin Problem on Finite Automata. Discrete Applied Mathematics, Volume 23, Issue 1, 1989, pp. 91-96

[46] Körner H. A Time and Space Efficient Algorithm for Minimizing Cover Automata for Finite Languages, International Journal of Foundations of Computer Science, Volume 14, Issue 6, 2003, pp. 1071–1086

[47] Яблонский С.В. Введение в дискретную математику. Наука, Москва, 1966

выполнено $\log|\mathcal{K}| = O(2^n)$[48,49,50,51]. Для классов $\mathcal{K}$ второго пояса выполнено $\log|\mathcal{K}| \asymp O\left(\frac{2^n}{\sqrt{n}}\right)$[52,53,54,55]. Для классов $\mathcal{K}$ третьего пояса $\log|\mathcal{K}| = O(n)$.

Функция Шеннона для сложности схем из функциональных элементов для классов первого пояса имеет порядок $O\left(\frac{2^n}{n}\right)$, для классов второго пояса – $O\left(\frac{2^n}{n^{3/2}}\right)$[56,57,58], для классов третьего пояса – $O(n)$.

Однако, порядок сложности и константные множители для конкретных классов Поста для мощности класса, сложности схем и автоматной сложности не совпадают. Важным отличием автоматной сложности является также пилообразное поведение графика функции Шеннона, не характерное для других мер сложности булевых функций.

В последнем параграфе приведены формулировки основных результатов в терминах QROBDD и ROBDD.

Заключение

1. С учетом научной актуальности и практической значимости вопроса о сложности автоматного вычисления булевых функций удалось найти не только оценки, но и получать точные значения автоматной сложности некоторых классов булевых функций, а также разработать алгоритм построения самой автоматно сложной булевой функции от данного числа переменных, чего не удавалось сделать для сложности схем из функциональных элементов.

2. Для классов $A_1, A_2, A_3, A_4, D_2, F_2^2, F_3^2, F_6^2, F_7^2, F_2^\infty, F_3^\infty, F_6^\infty, F_7^\infty$ получены асимптотические оценки функции Шеннона и построены автоматы,

48 Яблонский С.В. Введение в дискретную математику. Наука, Москва, 1966

49 Коршунов А.Д. Число k-неразделенных семейств подмножеств n-элементного множества (k-неразделенных булевых функций). Часть 1. Случай четных n и $k = 2$. Дискретный анализ и исследование операций, Серия 1, Том 10, № 4, 2003, с. 31-69

50 Коршунов А.Д. Число k-неразделенных семейств подмножеств n-элементного множества (k-неразделенных булевых функций). Часть II. Случай нечетных n и $k = 2$. Дискретный анализ и исследование операций, Серия 1, Том 12, № 1, 2005, с. 12-70

51 Коршунов А.Д. Число k-неразделенных семейств подмножеств n-элементного множества (k-неразделенных булевых функций). Часть III. Случай $k \geq 3$ и произвольных n. Дискретный анализ и исследование операций, Серия 1, Том 12, № 3, 2005, с. 60-73

52 Коршунов А.Д. О мощности и структуре некоторых замкнутых классов Поста (семейств подмножеств конечного множества), Модели и методы оптимизации, Наука, Новосибирск, 1988, с. 159-204

53 Коршунов А.Д. О числе и строении монотонных булевых функций. В: Лупанов О.Б. (ред.) Дискретная математика и ее приложения: Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. Часть 1, МГУ им. М.В. Ломоносова, Механико-математический факультет, Москва, 2001, с. 34-58

54 Сапоженко А.А. О числе антицепей в многослойных ранжированных множествах, Дискретная математика, 1989, Том 1, Выпуск 2, с. 110-128

55 Емеличев А.В., Сапоженко А.А. О числе монотонных самодвойственных функций. Материалы Второго Всесоюзного семинара по дискретной математике и ее приложениям. Издательство МГУ, Москва, 1988, с. 140-141

56 Лупанов О.Б. Об одном методе синтеза схем. Известия вузов. Радиофизика, 1, 1958, с. 120-140

57 Угольников А.Б. О реализации функций из замкнутых классов схемами из функциональных элементов. Математические вопросы кибернетики, Выпуск 1, Москва, Наука, 1988, с. 89-113

58 Угольников А.Б. О реализации монотонных функций схемами из функциональных элементов. Проблемы кибернетики, Выпуск 32, Москва, Наука, 1976, с. 167-185

представляющие сложные функции. Показано, что числовая ось, представляющая аргумент функции Шеннона (число переменных), распадается на последовательность пар интервалов, на бóльших из которых функция Шеннона асимптотически равна сложности построенных функций, а на меньших превосходит ее не более, чем вдвое. Разработан оригинальный метод синтеза сложных автоматов, представляющих монотонные функции, для чего используется специальное отображение единичного куба в множество монотонных булевых функций.

3. В ходе исследования автоматной сложности классов Поста F_j^{μ}, $\mu \geq 3$, для нетривиальных подмножеств $F_j^{\mu} \backslash F_j^{\mu+1}$ этих классов получены нижние асимптотические оценки функции Шеннона и построены автоматы, представляющие сложные функции.

4. Получены точные значения и асимптотика функции Шеннона для классов конечных языков $\mathcal{L}_n(A)$ и $\mathcal{L}_n^{\leq}(A)$. Построены автоматы, представляющие самые сложные коллекции языков. Такие автоматы моделируют процесс выбора одного из M возможных решений при N альтернативах на каждом шаге. Найден простой способ вычисления параметра p (высоты обратного дерева), входящего в состав формул сложности построенных автоматов. При этом не требуется сравнение величин вида 2^{n-q} и 2^{2^q} или обращение функций вида $n(x) = 2^x + x$.

5. Практическая и инновационная ценность результатов работы заключается в том, что последние являются основой для оценки практической пригодности новых информационных технологий и создания новых поколений быстрых автоматизированных информационных систем и программных комплексов, а также микропроцессоров. Указанные информационные технологии и системы могут быть использованы для решения в реальном времени задач кодирования, распознавания, криптографии, мониторинга и прогнозирования.

Благодарности. Автор выражает глубокую благодарность академику, профессору В.Б. Кудрявцеву и д.ф.-м.н., профессору Д.Н. Бабину за постановку задач, постоянную поддержку и внимание к работе.

Работы автора по теме диссертации

Основное содержание диссертации опубликовано в следующих работах автора:

1. Кибкало М.А. О сложности представления коллекции языков в конечных автоматах, Интеллектуальные системы, Том 13, Выпуск 1-4, 2010, сс. 347-360

2. Кибкало М.А. Об автоматной сложности некоторых классов булевых функций, Интеллектуальные системы, Том 14, Выпуск 1-4, 2010, сс. 319-322.

3. Кибкало М.А. Об автоматной сложности классов Поста булевых функций, Интеллектуальные системы, Том 15, Выпуск 1-4, 2011, сс. 379-400.

4. Кибкало М.А. Представление коллекций языков в конечных автоматах. Труды Международной конференции «Современные проблемы математики, механики и их приложений», посвященная 70-летию ректора МГУ академика В.А. Садовничего, секция «Интеллектуальные системы и компьютерные науки», 2009, сс. 358-359.

5. Кибкало М.А. О сложности представления коллекций языков в конечных автоматах. Материалы докладов XVI Международной конференции студентов, аспирантов и молодых ученых «Ломоносов», секция «Математика и механика», 2009, сс. 32-33.

6. Кибкало М.А. Представление коллекций языков автоматами. Материалы X международного семинара «Дискретная математика и ее приложения», Секция «Теория интеллектуальных систем и автоматов», 2010, сс. 361 – 363.

7. Кибкало М.А. Автоматная сложность классов Поста. Материалы Международного молодежного научного форума «ЛОМОНОСОВ-2011», секция «Математика и механика», подсекция «Математика», 2011.

8. Кибкало М.А. Оценки автоматной сложности классов булевых функций. Материалы X Международной конференции «Интеллектуальные системы и компьютерные науки», 2011.

9. Кибкало М.А. Об автоматной сложности некоторых классов Поста булевых функций. Материалы XI международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О.Б. Лупанова, Секция «Теория интеллектуальных систем и автоматов», 2012, сс. 343-346.