МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи
УДК 519.7

Кочергин Вадим Васильевич

О СЛОЖНОСТИ АДДИТИВНЫХ ВЫЧИСЛЕНИЙ

01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

Москва 2008

Работа выполнена на кафедре дискретной математики Механико-математического факультета Московского государственного университета имени М. В. Ломоносова.

Официальные оппоненты: доктор физико-математических наук, профессор Глухов Михаил Михайлович

доктор физико-математических наук, профессор Шевченко Валерий Николаевич

доктор физико-математических наук, профессор Шоломов Лев Абрамович

Ведущая организация: Институт математики им. С. Л. Соболева Сибирского отделения РАН

Защита диссертации состоится 17 октября 2008 г. в 16 часов 45 минут на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М. В. Ломоносова по адресу: Российская Федерация, 119991, ГСП-1, Москва, Ленинские горы, МГУ имени М. В. Ломоносова, Механико-математический факультет, аудитория 14–08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ имени М. В. Ломоносова (Главное здание, 14 этаж).

Автореферат разослан 17 сентября 2008 г.

Ученый секретарь
диссертационного совета
Д.501.001.84 при МГУ
доктор физико-математических наук,
профессор А. О. Иванов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Данная работа относится к одной из центральных областей дискретной математики и математической кибернетики — теории синтеза и сложности управляющих систем, получающей постановки задач и находящей многообразные применения в информатике и вычислительной технике.

Проблему синтеза управляющих систем кратко можно сформулировать следующим образом. Задан запас элементов (базис), реализующих некоторые функции. Заданы правила построения из элементов более сложных объектов — схем, а также задан способ нахождения по схеме реализуемой (вычисляемой) ею функции; схема определяет строение, а функция — поведение управляющей системы или модели вычислений. Задача состоит в построении для каждой рассматриваемой функции схемы, которая реализует эту функцию, причем обычно важно не просто построить схему, но и добиться, чтобы она была в каком-то определенном смысле наилучшей. Качество схемы обычно выражается с помощью какой-либо из мер сложности, среди которых рассматриваются, в частности[1]), число элементов, стоимость, занимаемые объем или площадь, глубина, задержка, мощность и др.

Если базис является конечным, то существует тривиальный переборный алгоритм решения этой задачи. Однако реально воспользоваться им чаще всего невозможно, так как с ростом числа элементов в схемах количество схем растет очень быстро и применение тривиального метода становится практически неосуществимым. На самом деле большая трудоемкость решения задачи синтеза в общем виде присуща всем алгоритмам, предназначенным для ее решения, — к этому выводу одним из первых пришел С. В. Яблонский[2]). С тех пор эта точка зрения стала общепринятой,

---

[1]) См., например: Лупанов О. Б. *Асимптотические оценки сложности управляющих систем.* — М.: Изд-во Московского университета, 1984; Коршунов А. Д. Об оценках сложности схем из объемных функциональных элементов // *Проблемы кибернетики, вып.* 19. — М.: Наука, 1967. — С. 275–284; Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // *Проблемы кибернетики, вып.* 19. — М.: Наука, 1967. — С. 285–292; McColl W. F., Paterson M. S. The depth of all Boolean functions // *SIAM J. Comput.* — 1977. — V. 6, № 2. — P. 373–380; Лупанов О. Б. О схемах из функциональных элементов с задержками // *Проблемы кибернетики, вып.* 23. — М.: Наука, 1970. — С. 43–81; Вайнцвайг М. Н. О мощности схем из функциональных элементов // *Доклады АН СССР.* — 1961. — Т. 139, № 2. — С. 320–323; Касим-Заде О. М. Об одной мере сложности схем из функциональных элементов // *Проблемы кибернетики, вып.* 38. — М.: Наука, 1981. — С. 117–179.

[2]) Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контакт-

получив много косвенных подтверждений своей справедливости. В силу этого обычно рассматривают некоторые ослабления рассматриваемой задачи. Одно из таких ослаблений заключается в приближенном решении задачи, т. е. в построении не обязательно минимальных, а «достаточно экономных» схем. Но и эта задача при поиске «достаточно точного» решения, вообще говоря, остается очень трудной. Поэтому часто рассматривают задачу построения асимптотически оптимальных схем. Постановка этой задачи, скажем, для классического случая вычисления булевых функций такова. Каждой схеме S ставится в соответствие неотрицательное число $L(S)$ — сложность схемы S, например, число элементов схемы. Считается, что схема тем лучше, чем меньше величина $L(S)$. Через $L(f)$ обозначается сложность схемы из заданного класса, которая реализует f и имеет минимальную сложность. Вводится функция $L(n) = \max L(f)$, где максимум берется по всем рассматриваемым функциям от n переменных. Требуется найти метод синтеза схем, позволяющий для любой рассматриваемой функции f от n переменных стоить схему, которая реализует f и имеет сложность, не превосходящую или мало превосходящую величину $L(n)$. Такой подход был предложен К. Шенноном[3]) в 1949 г. при исследовании контактных схем и может быть перенесен на другие классы управляющих систем. Функцию $L(n)$ принято называть *функцией Шеннона*.

Фундаментальные основы асимптотической теории синтеза и сложности управляющих систем были заложены О. Б. Лупановым. Им были предложены асимптотически оптимальные методы синтеза и получены асимптотически точные оценки сложности для важнейших классов управляющих систем — вентильных схем глубины 2, контактно-вентильных схем, схем из функциональных элементов, контактных схем, схем из функциональных элементов без ветвления выходов (формул) и с ограниченным ветвлением (формул с частичной памятью), формул ограниченной глубины, параллельно-последовательных контактных схем, релейно-контактных схем и др. При изучении этих модельных классов управляющих систем О. Б. Лупановым были выявлены новые эффекты и закономерности, в числе которых было явление, названное эффектом Шеннона: при реализации в большинстве исследованных им классов управляющих систем почти все функции имеют почти одинаковую сложность, асимптотически равную сложности наиболее сложных функций.

К асимптотической теории синтеза и сложности управляющих систем

ных схем // *Проблемы кибернетики, вып.* 2. — М.: Физматгиз, 1959. — С. 75–121.

[3]) Shannon C. E. The synthesis of two-terminal switching circuits // *Bell Syst. Techn. J.* — 1949. — V. 28, № 1. — P. 59–98.

относятся и вопросы, исследуемые в данной работе. При этом часть изучаемых вопросов следует отнести к области построения универсальных методов синтеза (расчитанных на реализацию произвольных функций), а другую — к области синтеза схем для конкретных (индивидуальных) функций (последовательностей функций).

Рассматриваемые в работе вычислительные схемы относятся к одному из важнейших модельных классов управляющих систем — классу схем из функциональных элементов. При этом изучаемые схемы обладают также многими свойствами, присущими вентильным схемам — классу наиболее простых управляющих систем, несущему большую «топологическую» нагрузку и удобному для разработки общих методов синтеза, которые, как правило, в той или иной степени могут быть промоделированы в других классах управляющих систем.

В работе изучаются различные обобщения хорошо известной задачи о сложности возведения в степень, т. е. задачи о нахождении величины $l(x^n)$ — минимального числа операций умножения, достаточного для вычисления по переменной x величины x^n. Эту задачу (а также ее обобщения) обычно рассматривают в аддитивной постановке — это известная задача об аддитивных цепочках, которая формулируется следующим образом[4]). *Аддитивной цепочкой* для натурального числа n называется всякая последовательность целых чисел

$$a_0 = 1, a_1, \ldots, a_m = n,$$

удовлетворяющая следующему свойству: для каждого k, $1 \leq k \leq m$, найдется два целых числа (не обязательно различных) i и j, $0 \leq i, j \leq k-1$, таких, что $a_k = a_i + a_j$. Минимальная длина m аддитивной цепочки для n называется *аддитивной сложностью* числа n и обозначается $l(n)$. Очевидно, что величины $l(n)$ и $l(x^n)$ совпадают.

Считается, что задачу определения величины $l(n)$ поставил в 1894 г. Х. Деллак, хотя, по-видимому, еще в древней Индии был известен «бинарный» метод возведения в степень. В 1937 г. А. Шольц для этой задачи ввел понятие аддитивной цепочки.

В 1939 А. Брауэром[5]) для величины $l(n)$ при $n \to \infty$ была установлена

---

[4]) Кнут Д. Е. *Искусство программирования, т.* 2. 3-*е издание.* — М.: Издательский дом «Вильямс», 2000.

[5]) Brauer A. On addition chains // *Bull. Amer. Math. Soc.* — 1939. — V. 45. — P. 736–739.

асимптотическая формула[6])

$$l(n) \sim \log n,$$

причем им была получена верхняя оценка

$$l(n) \leq \log n + \frac{\log n}{\log\log n} + O\left(\frac{\log n \log\log\log n}{(\log\log n)^2}\right).$$

В 1960 г. П. Эрдёш[7]) показал, что для почти всех n справедливо асимптотическое равенство

$$l(n) = \log n + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right),$$

при этом стоит отметить разную природу слагаемых в правой части этого равенства — слагаемое $\log n$ связано с величиной числа n и должно присутствовать для любого значения n, а «мощностное» слагаемое (отношение логарифма количества чисел, не превосходящих n, к повторному логарифму) зависит от «строения» числа n и присутствует для «почти всех» n.

После этого исследовались (как правило, на языке аддитивных цепочек) различные вопросы, связанные с задачей о наискорейшем возведении в степень[8]).

Теперь перейдем к обобщениям задачи об аддитивной сложности натурального числа (или задачи о наискорейшем возведении в степень). Эти обобщения, по-существу, являются основными объектами исследования данной работы.

Пусть $A = (a_{ij})$ — целочисленная матрица размера $p \times q$ с неотрицательными коэффициентами без нулевых строк.

Аддитивной цепочкой для матрицы A называется[9]) последователь-

---

[6]) Здесь и далее $\log x$ означает $\log_2 x$, а запись $f(n) \sim g(n)$ означает, что при $n \to \infty$ отношение $f(n)/g(n)$ стремится к 1.

[7]) Erdos P. Remarks on number theory, III: On addition chains // *Acta Arith.* — 1960. — V. 6. — P. 77–81.

[8]) См., например, обзоры: Subbarao M. V. Addition chains — some results and problems // *Number Theory and Applications. Editor R. A. Mollin. NATO Advanced Science Institutes Series: Series C.* — Kluwer Academic Publisher Group, 1989. — V. 265. — P. 555–574; Bos J., Coster M. Addition chain heuristics // *Proceedings of Crypto'89.* — Springer-Verlag, 1990. — V. 435. — P. 400–407; Gordon D. M. A survey of fast exponentiation methods // *Journal of Algorithms.* — 1998. — V. 27. — P. 129–146.

[9]) Knuth D. E., Papadimitriou C. H. Duality in addition chains // *Bulletin of the European association for Theoretical Computer Science.* — 1981. — V. 13. — P. 2–4.

ность q-мерных векторов (наборов) вида

$$\mathbf{v}_1 = (1, 0, \ldots, 0), \mathbf{v}_2 = (0, 1, \ldots, 0), \ldots, \mathbf{v}_q = (0, 0, \ldots, 1),$$
$$\mathbf{v}_{q+1}, \mathbf{v}_{q+2}, \ldots, \mathbf{v}_{q+r},$$

начинающаяся с q единичных векторов и удовлетворяющая условиям:

1) для каждого k, $q+1 \le k \le q+r$, найдется два натуральных числа (не обязательно различных) i и j, $1 \le i \le k-1$, $1 \le j \le k-1$, таких, что $\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$ (сложение векторов покомпонентное);

2) $\{(a_{11}, a_{12}, \ldots a_{1q}), (a_{21}, a_{22}, \ldots a_{2q}), \ldots, (a_{p1}, a_{p2}, \ldots a_{pq})\} \subseteq$
$$\subseteq \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{q+r}\}.$$

Число r называется длиной цепочки. Минимальная длина аддитивной цепочки для матрицы A называется *аддитивной сложностью* (*вычисления, порождения, реализации*) *матрицы* A и обозначается через $l(A)$.

Задача об аддитивной сложности матриц по-существу совпадает с известной[10]) задачей о сложности вычисления систем одночленов (систем коммутативных мономов) — величина $l(A)$ численно равна минимально возможному числу операций умножения, достаточному для (схемного) вычисления по переменным $x_1, x_2, \ldots, x_q$ задаваемой матрицей A системы одночленов

$$f_1 = x_1^{a_{11}} x_2^{a_{12}} \ldots x_q^{a_{1q}}, \quad f_2 = x_1^{a_{21}} x_2^{a_{22}} \ldots x_q^{a_{2q}}, \quad \ldots, \quad f_p = x_1^{a_{p1}} x_2^{a_{p2}} \ldots x_q^{a_{pq}},$$

(при этом допускается многократное использование промежуточных результатов).

Пусть теперь $A = (a_{ij})$ — произвольная (не обязательно с неотрицательными элементами и без нулевых строк) целочисленная матрица. Определим еще две меры сложности порождения таких матриц.

Через $l_2(A)$ обозначим минимальную длину обобщенных аддитивных цепочек для матрицы A, в которых помимо операции сложения ($\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$) разрешена и операция вычитания ($\mathbf{v}_k = \mathbf{v}_i - \mathbf{v}_j$). Величина $l_2(A)$ численно равна минимально возможному числу операций умножения и деления, достаточному для (схемного) вычисления по переменным $x_1, x_2, \ldots, x_q$ задаваемой матрицей A системы функций $f_i = x_1^{a_{i1}} x_2^{a_{i2}} \ldots x_q^{a_{iq}}$,

---

[10]) См., например: Pippenger N. On evaluation of powers and monomials // *SIAM J. Comput.* — 1980. — V. 9, N 2. — P. 230–250; Vassiliev N. N. Complexity of monomial evaluations and duality // *Computer algebra in scientific computing — CASC'99* (*Munich*). — Berlin: Springer, 1999. — P. 479–484; Bernstein D. J. Pippenger's exponentiation algorithm // `Available at: http://cr.yp.to/papers/pippenger.pdf.` — 2002.

$i = 1, 2, \ldots, p$, а также минимально возможному числу операций сложения и вычитания, достаточному для (схемного) вычисления по переменным $x_1, x_2, \ldots, x_q$ задаваемой матрицей A системы целочисленных линейных форм $g_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{iq}x_q$, $i = 1, 2, \ldots, p$. В таком виде задача о нахождении величины $l_2(A)$ поставлена, например, А. Ф. Сидоренко[11]).

Эта мера сложности тесно связана с быстрыми вычислениями на эллиптических кривых[12]) и имеет два малоотличающихся друг от друга варианта — не допускающий[13]) операции вида $\mathbf{v}_k = -\mathbf{v}_i - \mathbf{v}_j$ и допускающий[14]) такие операции.

Через $l_F(A)$ обозначим минимальную длину таких аддитивных цепочек для матрицы A, в которых используется только операции сложения ($\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$), но которые начинаются не с q начальных единичных векторов, а с $2q$ векторов — помимо векторов $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_q$ разрешается использовать противоположные к ним векторы $-\mathbf{v}_1, -\mathbf{v}_2, \ldots, -\mathbf{v}_q$. Величина $l_F(A)$ численно равна минимально возможному числу операций умножения, достаточному для (схемного) вычисления по образующим $x_1, x_2, \ldots, x_q$ свободной абелевой группы и обратным к ним элементам $x_1^{-1}, x_2^{-1}, \ldots, x_q^{-1}$ задаваемой матрицей A системы $f_i = x_1^{a_{i1}} x_2^{a_{i2}} \ldots x_q^{a_{iq}}$, $i = 1, 2, \ldots, p$, элементов этой группы. Впервые, по-видимому, такая мера сложности исследовалась Ф. Штрассеном[15]) (причем не только для коммутативного случая).

Величины $l(A)$, $l_2(A)$ и $l_F(A)$ можно интерпретировать как минимально возможную сложность (число элементов) схемы из функциональных элементов[16]), на входы которой подаются переменные $x_1, x_2, \ldots, x_q$ (а также

---

[11]) Сидоренко А. Ф. Сложность аддитивных вычислений семейств целочисленных линейных форм // *Записки научных семинаров ЛОМИ.* — Л.: Наука, 1981. — Т. 105. — С. 53–61.

[12]) Morain F., Olivos J. Speeding up the computation on an eliptic curve using addition-subsraction chains // *Informatique Théorique et Applications.* — 1990. — V. 24. — P. 531–544.

[13]) См., например: Volger H. Some results on addition/subtraction chains // *Information Processing Letters.* — 1985. — V. 20. — P. 155–160; Goundar R. R., Shiota K., Toyonaga M. New strategy for doubling-free short addition-subtraction chain // *International Journal of Applied Mathematics.* — 2007. — V. 2, № 3.

[14]) См., например: Kunihiro N., Yamamoto H. Window and extended window methods for addition chain and addition-subtraction chain // *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences.* — 1998. — V. E81-A, № 1. — P. 72–81; Kweon K., Hong S.-M., Oh S.-Y., Yoon H. Finding shorter addition/subtraction-chains // *CCCT'05* (*International Conference on Computing, Communications and Control Technologies*). — http://hdl.handle.net/10203/447

[15]) Strassen V. Berechnungen in partiellen Algebren endlichen Typs // *Computing.* — 1973. — V. 11. — P. 181–196.

[16]) См., например: Лупанов О. Б. О синтезе некоторых классов управляющих си-

обратные к ним величины $x_1^{-1}, x_2^{-1}, \ldots, x_q^{-1}$, если речь идет о мере сложности l_F), на выходах схемы вычисляются функции $f_1, f_2, \ldots, f_p$, задаваемые матрицей A, а сама схема состоит из двухвходовых элементов, реализующих произведение (произведение или частное, если речь идет о мере сложности l_2) функций, подаваемых на входы элемента.

В 1963 г. Р. Беллман[17]), а затем в 1964 г. Е. Страус[18]) сформулировали задачу о сложности вычисления одночлена от q переменных (в наших обозначениях — случай $p = 1$, мера сложности — l), т. е. нахождения величины $l(x_1^{a_1} x_2^{a_2} \ldots x_q^{a_q})$.

В 1969 г. Д. Кнут[19]) поставил задачу о сложности вычисления p степеней одной переменной (в наших обозначениях — случай $q = 1$, мера сложности — l), т. е. нахождения величины $l(x^{a_1}, x^{a_2}, \ldots, x^{a_p})$.

Е. Страус показал, что для любого фиксированного q при $\sum a_i \to \infty$ справедлива асимптотическая формула

$$l(x_1^{a_1} x_2^{a_2} \ldots x_q^{a_q}) \sim \log(\max a_i).$$

А. Яо[20]) установил аналогичную формулу для любого фиксированного p при $\sum a_i \to \infty$:

$$l(x^{a_1}, x^{a_2}, \ldots, x^{a_p}) \sim \log(\max a_i).$$

В 1981 г. независимо А. Ф. Сидоренко, Дж. Оливосом[21]), а также Д. Кнутом и К. Пападимитриу было доказано, что в действительности задачи о сложности вычисления одночлена от m переменных и набора m степеней эквивалентны (и, следовательно, достаточно исследовать одну из них). На самом деле было установлено более сильное утверждение о двойственности относительно меры сложности l: сложность системы одночленов $\{f_1, f_2, \ldots, f_p\}$ от q переменных, заданной матрицей $A = (a_{ij})$ размера $p \times q$ и сложность двойственной системы одночленов $\{\widehat{f_1}, \widehat{f_2}, \ldots, \widehat{f_q}\}$ от p переменных, заданной транспонированной матрицей $A^T = (a_{ji})$ размера

стем // *Проблемы кибернетики, вып.* 10. — М.: Физматгиз, 1963. — С. 63–97; Сэвидж Д. Е. *Сложность вычислений.* — М.: Изд.-во «Факториал». — 1998.

[17]) Bellman R. E. Addition chains of vectors (Advanced problem 5125) // *Amer. Math. Monthly.* — 1963. — V. 70. — P. 765.

[18]) Straus E. G. Addition chains of vectors // *Amer. Math. Monthly.* — 1964. — V. 71. — P. 806–808.

[19]) Кнут Д. Е. *Искусство программирования для ЭВМ, т.* 2. 1-*е издание.* — М.: Мир, 1977. — Разд. 4.6.3, упр. 32.

[20]) Yao A. C.-C. On the evaluation of powers // *SIAM J. Comput.* — 1976. — V. 5. — P. 100–103.

[21]) Olivos J. On vectorial addition chains // *J. Algorithms.* — 1981. — V. 2, N 1. — P. 13–21.

$q \times p$, для любой матрицы A без нулевых строк и столбцов связаны соотношением

$$l(f_1, f_2, \ldots, f_p) + p = l(\widehat{f_1}, \widehat{f_2}, \ldots, \widehat{f_q}) + q,$$

т. е. для любой целочисленной матрицы A с неотрицательными элементами размера $p \times q$ без нулевых строк и столбцов выполняется равенство

$$l(A) + p = l\left(A^T\right) + q.$$

Похожее соотношение для двух матриц, получающихся друг из друга путем транспонирования, справедливо и для меры сложности l_2.

Также в 1981 г. установлено[22]), что задача распознавания по набору натуральных чисел $(n_1, n_2, \ldots, n_p, l)$ существования аддитивной цепочки, имеющей длину l и содержащей числа $n_1, n_2, \ldots, n_p$, является NP-полной. В связи с этим дополнительный вес приобретает асимптотическая постановка исходной задачи. Требуется найти метод построения для матрицы A аддитивной цепочки (соответствующего типа), длина которой в том или ином смысле близка к значению $l(A)$, $l_2(A)$ или $l_F(A)$ соответственно. Например, такой метод, чтобы отношение длины построенной цепочки для матрицы $A = (a_{ij})$ к значению соответствующей меры сложности матрицы стремилось к 1 при $\sum |a_{ij}| \to \infty$ для всех или «почти всех» матриц.

Существенным продвижением в этом направлении стала работа Н. Пиппенджера[23]). В ней исследовано асимптотическое поведение функции Шеннона, характеризующей сложность «самой сложной» матрицы среди матриц заданного размера с элементами, не превосходящими заданного значения $K - 1$, и определяемой при $K \geq 2$ равенством $L(p, q, K) = \max l(A)$, где максимум берется по всем целочисленным матрицам $A = (a_{ij})$ с неотрицательными элементами без нулевых строк размера $p \times q$, удовлетворяющим условиям $a_{ij} \leq K - 1$, $i = 1, \ldots, p$, $j = 1, \ldots, q$. С использованием своего технически весьма громоздкого и существенно опирающегося на результаты О. Б. Лупанова[24]) и Э. И. Нечипорука[25]) способа[26]) построения асимптотически оптимальных обобщенных вентильных схем,

---

[22]) Downey P., Leong B., Sethi R. Computing sequences with addition chains // *SIAM Journal on Computing.* — V. 10. — 1981. — P. 638–646.

[23]) Pippenger N. On evaluation of powers and monomials // *SIAM J. Comput.* — 1980. — V. 9, N 2. — P. 230–250.

[24]) Лупанов О. Б. О вентильных и контактно-вентильных схемах // *Доклады АН СССР.* — 1956. — Т. 111, № 6. — С. 1171–1174.

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

[26]) Pippenger N. The mimimum number of edges in graphs with prescribed paths // *Math. Systems Theory.* — 1979. — V. 12, № 4. — P. 325–346.

реализующих целочисленные матрицы с неотрицательными элементами, Пиппенджер показал, что при условии $pq \log K \to \infty$ имеет место асимптотическое равенство

$$L(p, q, K) = \min(p,\, q) \log K + \\ + \frac{pq \log K}{\log(pq \log K)} \left(1 + O\left(\left(\frac{\log\log(pq \log K)}{\log(pq \log K)}\right)^{1/2}\right)\right) + O(\max(p,\, q)).$$

Однако для конкретных (индивидуальных) матриц (последовательностей матриц) никаких нетривиальных асимптотически точных оценок сложности, кроме случая $p = 1$ при фиксированном q или $q = 1$ при фиксированном p, ни для одной из определенных здесь мер сложности известно, по-видимому, не было.

Цель работы. Целью диссертационной работы является исследование асимптотических закономерностей поведения величин $l(A)$, $l_2(A)$ и $l_F(A)$ при различных ограничениях на размеры и величину элементов целочисленных матриц A, построение асимптотически оптимальных методов вычисления систем одночленов, систем целочисленных линейных форм и систем элементов свободной абелевой группы, поиск и изучение новых эффектов и закономерностей в этой области.

Методы исследования. При решении рассматриваемых задач использовались методы дискретной математики и математической кибернетики.

Научная новизна. Все основные результаты диссертации являются новыми. Основные положения, выносимые на защиту, следующие:

- Для задачи о сложности вычисления одночлена от нескольких переменных (задача Беллмана) и для задачи о сложности вычисления набора степеней одной переменной (задача Кнута) при слабых ограничениях в области изменения параметров получены асимптотически точные решения.

- Установлена общая нижняя оценка сложности вычисления систем одночленов, систем целочисленных линейных форм и систем элементов свободных абелевых групп.

- Предложен метод получения верхних оценок сложности систем одночленов, основанный на использовании усиленной модели вычислений

с последующим сведением без асимптотического увеличения сложности к исходной модели. На основе этого метода получены асимптотически точные верхние оценки сложности: системы из двух одночленов от нескольких переменных, системы из нескольких одночленов от двух переменных; системы из трех одночленов от трех переменных.

- Для любых фиксированных (или слаборастущих) значениях p и q установлена асимптотика роста сложности вычисления системы из p целочисленных линейных форм от q переменных.

- Получены асимптотически точные верхние оценки сложности вычисления: системы из двух элементов свободной абелевой группы; системы из трех элементов свободной абелевой группы с двумя образующими.

- С использованием полученных оценок сложности вычисления наборов степеней установлена асимптотика роста сложности вычисления двоичных слов с заданным числом (или долей) единиц схемами конкатенации.

- Выявлены новые эффекты в задачах о сложности вычисления систем одночленов, систем целочисленных линейных форм и систем элементов свободных абелевых групп; в частности, установлены принципиальные различия в асимптотическом поведении трех исследуемых мер сложности.

Теоретическая и практическая ценность. Работа носит теоретический характер. Ее результаты могут быть использованы при исследовании различных вопросов теории сложности. Некоторые разделы диссертации могут быть использованы в специальных курсах для студентов и аспирантов, обучающихся по специальности математика.

Апробация работы. Научные результаты и положения диссертационной работы докладывались и обсуждались на следующих научных конференциях, семинарах и школах-семинарах: серии всесоюзных (затем международных) конференций «Проблемы теоретической кибернетики» — Волгоград (1990), Саратов (1993), Ульяновск (1996), Нижний Новгород (1999), Казань (2002), Пенза (2005), Казань (2008, пленарный доклад); серии международных семинаров «Дискретная математика и ее приложения» — Москва, МГУ (1993, 1995, 1998, 2004, 2007); серии всесоюзных (впоследствии международных) школ-семинаров «Синтез и сложность управляющих систем» — Ташкент (1990), Нижний Новгород (1992, 1994, 1996,

1998, 2000), Минск (1993, 1995, 1999), Санкт-Петербург (2006, пленарный доклад); серии международных конференций «Дискретные модели в теории управляющих систем» (1997, 1998, 2000, 2006); а также на совместном французско-российском семинаре «Combinatorial and algorithmical properties of discrete structures» (1999), на международной школе-семинаре «Сложность булевых функций» (Казань, 1999). Большинство из этих докладов нашли отражение в трудах, материалах, тезисах или аннотациях докладов соответствующих конференций и семинаров. Основные результаты диссертации многократно докладывались в МГУ имени М. В. Ломоносова на научно-исследовательских семинарах «Математические вопросы кибернетики» (руководители — С. В. Яблонский; О. Б. Лупанов; О. М. Касим-Заде), «Синтез управляющих систем» (руководители — О. Б. Лупанов; О. М. Касим-Заде), «Синтез управляющих систем и смежные вопросы» (руководители — О. Б. Лупанов и В. М. Храпченко) и других, а также на Ломоносовских чтениях в МГУ.

Публикации. Основное содержание диссертации опубликовано в 24 работах автора, список которых приведен в конце автореферата [1–24].

Структура и объем работы. Диссертационная работа состоит из введения, пяти глав и списка использованной литературы из 151 наименования. Полный объем работы составляет 344 страницы. Работа содержит 21 рисунок. Нумерация теорем, лемм, утверждений, следствий, замечаний и формул — двойная, состоящая из номера главы и собственно номера внутри данной главы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении дается общая характеристика работы и краткое содержание глав работы.

В **главе 1** исследуются задача о сложности вычисления одночлена от многих переменных (задача Беллмана) и задача о сложности вычисления системы степеней одной переменной (задача Кнута).

В **§ 1.1** сначала даются строгие определения уже обсуждавшимся выше трем обобщениям понятия аддитивной сложности натурального числа, с единых позиций вводятся три вычислительные модели и соответствующие им три меры аддитвной сложности целочисленных матриц (l, l_2 и l_F). Соответствующие этим вычислительным моделям и мерам сложности задачи, имеющие единую аддитивную природу, в силу ряда факторов получили условные названия «Вычисление системы одночленов», «Вычисление системы целочисленных линейных форм» и «Вычисление системы элементов свободной абелевой группы».

В асимптотической постановке они формулируются следующим образом. Пусть дана последовательность $\{A(n) = (a_{ij}(n))\}$ целочисленных матриц (для первой модели эти матрицы должны быть с неотрицательными элементами и без нулевых строк) размера $p(n) \times q(n)$, удовлетворяющая при $n \to \infty$ условию $\sum_{a_{ij} \in A(n)} |a_{ij}| \to \infty$. Задача состоит в нахождении при $n \to \infty$ асимптотики роста функционала сложности $l(A(n))$, $l_2(A(n))$ или $l_F(A(n))$ соответственно.

Далее изучаются простейшие свойства и соотношения введенных мер сложности, обсуждаются задачи Беллмана и Кнута, получившие усилиями Е. Страуса и А. Яо при фиксированном числе переменных (степеней) асимптотически точное решение. Вопрос об асимптотике роста сложности в случае растущего числа переменных (степеней) оставался открытым.

Из разных соображений, в том числе и основываясь на уже известных результатах, логично предположить, что на сложность вычисления одночлена от нескольких переменных (или системы из нескольких степеней одной переменной) так или иначе оказывают влияние следующие параметры — максимальное значение среди показателей степеней, общее число переменных (или степеней), а также параметр, связанный с общим числом объектов из рассматриваемого класса, и который для изучаемых задач естественно определить как произведение показателей степеней. Каждый из этих параметров, имеющих разную природу, при соответствующих условиях может быть определяющим. Изучению влияния каждого из этих параметров, а также нахождению асимптотики роста сложности в рассматриваемых задачах при слабых ограничениях на соотношения параметров посвящены следующие два параграфа.

В **§ 1.2** доказываются верхние оценки для задач Беллмана и Кнута. В силу двойственности этих задач достаточно исследовать одну из них. Ключевую роль при этом исследовании играет получение асимптотически наилучшей верхней оценки сложности вычисления одночлена в случае, когда доминирующей является «мощностная» составляющая.

В основе доказательства такой оценки лежит сведение задачи Беллмана к задаче реализации булевых матриц специального вида вентильными схемами — ориентированными графами без ориентированных циклов с двумя группами выделенных вершин, называемых соответственно входами и выходами схемы, такими что ориентированные пути от входа к входу, от выхода к выходу и от выхода к входу отсутствуют, а число путей от i-го входа к j-му выходу равно элементу матрицы, стоящему на пересечении i-й строки и j-го столбца. Вычисляемому одночлену сопоставляется булева матрица, столбцами которой являются двоичные записи показателей

степеней переменных, дополняемые нулями в старших разрядах для выравнивания высоты. С использованием вентильной конструкции[27]) автора (не вошедшей в данную работу), опирающейся в свою очередь на конструкции О. Б. Лупанова, Э. И. Нечипорука и Н. Пиппенджера и дающей асимптотически оптимальную оценку через «информационную площадь» матрицы, доказывается следующая

Теорема 1.1. *Пусть* $\tilde{n}(s) = \bigl(n_1(k), n_2(s), \ldots, n_{m(s)}(s)\bigr)$, $s = 1, 2, \ldots$, — *последовательность наборов натуральных чисел, удовлетворяющая условию* $\sum_{i=1}^{m(s)} n_i(s) \to \infty$. *Тогда*

$$l(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}) \le \frac{\log N}{\log\log N}\left(1 + O\left(\left(\frac{\log\log\log N}{\log\log N}\right)^{1/2}\right)\right) + \\ + O(m + \log\max n_i),$$

где $N = n_1 n_2 \ldots n_m$.

Это утверждение усиливает следующая теорема, доказанная автором совместно с С. Б. Гашковым[28]) (на защиту не выносится и включена в работу для полноты изложения):

Теорема 1.2. *Для любой последовательности наборов натуральных чисел* $\tilde{n}(s) = \bigl(n_1(s), n_2(s), \ldots, n_{m(s)}(s)\bigr)$, $s = 1, 2, \ldots$, *удовлетворяющей условию* $\sum_{i=1}^{m(s)} n_i(s) \to \infty$, *выполняется неравенство*

$$l(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}) \le \log\max n_i + \\ + \frac{\log N}{\log\log N}\left(1 + O\left(\left(\frac{\log\log\log N}{\log\log N}\right)^{1/2}\right)\right) + O(m),$$

где $N = n_1 n_2 \ldots n_m$.

Заключительная теорема этого параграфа устанавливает асимптотически точную верхнюю оценку при наиболее слабых ограничениях (при этом происходит огрубление оценок остаточных членов), а также дает хорошую верхнюю оценку в случае, когда число переменных в одночлене велико. Она формулируется отдельно для задач Беллмана и Кнута, поскольку в отличие от предыдущих теорем доказываемые оценки для этих задач уже отличаются.

---

[27]) Кочергин В. В. О сложности вычислений в конечных абелевых группах // *Математические вопросы кибернетики, вып.* 4. — М.: Наука, 1992. — С. 178–217.

[28]) Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // *Методы дискретного анализа в теории графов и сложности.* — Новосибирск, 1992. — Вып. 52. — С. 22–40.

Теорема 1.3. *Пусть функция $f(x)$ при $x \to \infty$ удовлетворяет условиям $f(x) \to \infty$, $\log f(x) = o(\log x)$. Тогда для любой последовательности наборов натуральных чисел $\tilde{n}(s) = \big(n_1(s), n_2(s), \ldots, n_{m(s)}(s)\big)$, $s = 1, 2, \ldots$, удовлетворяющей условию $\sum_{i=1}^{m(s)} n_i(s) \to \infty$, выполняются неравенства*

$$l(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}) \le \log(\max n_i)(1 + o(1)) + \frac{\log N}{\log\log N}(1 + o(1)) + \\ + \sum_{i=1}^{m} \left(\left\lceil \log_{(m/(f(m))^2)} n_i \right\rceil - \log_{(m/(f(m))^2)} n_i \right),$$

$$l(x^{n_1}, x^{n_2}, \ldots, x^{n_m}) \le \log(\max n_i)(1 + o(1)) + \frac{\log N}{\log\log N}(1 + o(1)) + \\ + \sum_{i=1}^{m} \left(\left\lceil \log_{(m/(f(m))^2)} n_i \right\rceil - \log_{(m/(f(m))^2)} n_i \right) - m,$$

где $N = n_1 n_2 \ldots n_m$.

В силу неравенства $\lceil x \rceil - x \le 1$ непосредственным следствием теоремы 1.3 являются асимптотические неравенства[29])

$$l(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}) \lesssim \log(\max n_i) + \frac{\log N}{\log\log N} + m,$$

$$l(x^{n_1}, x^{n_2}, \ldots, x^{n_m}) \lesssim \log(\max n_i) + \frac{\log N}{\log\log N}.$$

В **§ 1.3** доказываются нижние оценки для задач Беллмана и Кнута, причем в более сильной второй вычислительной модели, использующей не одну, а две операции. Нижние оценки для меры сложности l_2 автоматически являются нижними оценками для меры сложности l.

Для исследуемых задач получилось «объединить» в одном утверждении тривиальную нижнюю оценку вида $l(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}) \ge \log(\max n_i) + m - 1$ и нижнюю оценку, получающуюся из стандартных мощностных рассуждений[30]). Впервые «объединить» тривиальную и «мощностную» нижние оценки удалось, по-видимому, П. Эрдешу для задачи о длине аддитивной цепочки для числа n. Развитие эти методы получили в работе Н. Пиппенджера при оценке снизу сложности вычисления «самой сложной» системы

[29]) Здесь и далее запись $g(x) \lesssim h(x)$ означает неравенство $g(x) \le h(x)(1 + o(1))$.

[30]) Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // *Проблемы кибернетики, вып.* 14. — М.: Наука, 1965. — С. 31–110.

из p одночленов от q переменных. Здесь при доказательстве нижней оценки описанного вида использованы некоторые основные идеи упомянутых работ.

Для произвольного набора $\tilde{n} = (n_1, n_2, \ldots, n_m)$ различных натуральных чисел через σ обозначим перестановку, упорядочивающую набор $\tilde{n}$ по возрастанию: $n_{\sigma(1)} < n_{\sigma(2)} < \ldots < n_{\sigma(m)}$. Положим

$$\mathfrak{M}(\tilde{n}) = \big\{(k_1, k_2, \ldots, k_m) \mid \\ k_1 < k_2 < \ldots < k_m,\ k_i \in \mathbb{N},\ 1 \le k_i \le n_{\sigma(i)},\ i = 1, 2, \ldots, m\big\}.$$

Теорема 1.6. *Пусть последовательность наборов*

$$\tilde{n}(s) = \big(n_1(s), n_2(s), \ldots, n_{m(s)}(s)\big), \quad s = 1, 2, \ldots$$

различных натуральных чисел удовлетворяет условию $N(s) = \prod_{i=1}^{m(s)} n_i(s) \to \infty$ *при* $s \to \infty$. *Тогда существуют такие положительные константы* c, c_2 *и функции* $f(x)$ *и* $f_2(x)$, *стремящиеся к* 0 *при* $x \to \infty$, *что доли наборов* $(k_1, k_2, \ldots, k_m)$ *из* $\mathfrak{M}(\tilde{n}(s))$, *удовлетворяющих, соответственно, соотношениям*

$$\left| l\left(x^{k_1}, x^{k_2}, \ldots, x^{k_m}\right) - \left(\log \max n_i + \frac{\log N}{\log\log N}\right)\right| \le f(N)\frac{\log N}{\log\log N} + cm,$$

$$\left| l_2\left(x^{k_1}, x^{k_2}, \ldots, x^{k_m}\right) - \left(\log \max n_i + \frac{\log N}{\log\log N}\right)\right| \le f_2(N)\frac{\log N}{\log\log N} + c_2 m,$$

стремятся к единице при $s \to \infty$.

Утверждение теоремы 1.6 остается справедливым, если рассматривать доли наборов не из множества $\mathfrak{M}(\tilde{n}(s))$, а из множества $\mathfrak{N}(\tilde{n}(s))$, где $\mathfrak{N}(\tilde{n}) = \{(k_1, k_2, \ldots, k_m) \mid k_i \in \mathbb{N},\ 1 \le k_i \le n_i,\ i = 1, 2, \ldots, m\}$. Такой подход является более логичным при изучении задачи Беллмана. Отличия в подходах связаны с соображениями следущего толка — при вычислениях одночлены $x_1^{n_1}x_2^{n_2}$ и $x_1^{n_2}x_2^{n_1}$ естественно считать разными, а наборы степеней (x^{n_1}, x^{n_2}) и (x^{n_2}, x^{n_1}) — одинаковыми. Стоит отметить, что в изначальной формулировке теоремы 1.6 результат в некотором смысле является более тонким.

Содержательно утверждение теоремы 1.6 означает относительно, скажем, меры сложности l, что при выполнении условий теоремы и, кроме того, условия $m = o\left(\log\left(\max_i n_i\right) + \frac{\log N}{\log\log N}\right)$, для почти всех наборов из $\mathfrak{M}(\tilde{n})$ (или из $\mathfrak{N}(\tilde{n})$) справедливо асимптотическое равенство

$$l\left(x^{k_1}, x^{k_2}, \ldots, x^{k_m}\right) \sim \log\left(\max_i n_i\right) + \frac{\log N}{\log\log N},$$

из которого в силу теоремы 1.3 при тех же условиях следует для почти всех наборов и выполнение соотношения

$$l\left(x^{k_1}, x^{k_2}, \ldots, x^{k_m}\right) \sim \log\left(\max_i k_i\right) + \frac{\log K}{\log\log K},$$

где $K = k_1 k_2 \ldots k_m$.

При выполнении условия $m \geq \min\left(\log\left(\max n_i\right), \frac{\log N}{\log\log N}\right)$ утверждения теорем 1.3, 1.4 и 1.6 дают верхние и нижние асимптотические оценки для задач Беллмана и Кнута, отличающиеся на величину, не превосходящую m, причем при некоторых дополнительных ограничениях эти утверждения дают асимптотически совпадающие оценки. Простейшим примером асимптотического совпадения оценок является задача вычисления, скажем, одночлена $x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}$, где $n_i = o(m^2)$, $i = 1, 2, \ldots, m$, и все n_i различны. В этом случае указанные оценки устанавливают следующую асимптотику роста сложности: $l\left(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}\right) \sim 2m$.

В **§ 1.4** рассматривается применение оценок сложности, полученных при исследовании задачи Кнута, для получения асимптотически окончательного результата в одной задаче, которую также можно считать прямым обобщением классической задачи об аддитивных цепочках.

Конкатенацией слов $\tilde{\alpha}$ и $\tilde{\beta}$ конечной длины над произвольным алфавитом называется слово $\tilde{\alpha}\tilde{\beta}$, полученнное приписыванием к слову $\tilde{\alpha}$ справа слова $\tilde{\beta}$.

Последовательность S слов (наборов) $\tilde{\tau}_1$, $\tilde{\tau}_2$, $\ldots$, $\tilde{\tau}_r = \tilde{\alpha}$ из конечного алфавита $\mathfrak{A}$ называется *схемой конкатенации*[31]), реализующей (вычисляющей) слово (набор) $\tilde{\alpha}$, если для каждого i, $i = 1, 2, \ldots, r$, слово $\tilde{\tau}_i$ можно представить в виде $\tilde{\tau}_i = \tilde{\beta}_{i_1}\tilde{\beta}_{i_2}$, где для $j = 1, 2$ либо β_{i_j} — буква из алфавита $\mathfrak{A}$, либо $\beta_{i_j} = \tau_m$ для некоторого m, удовлетворяющего условию $m \leq i - 1$. *Сложностью* $l_c(S)$ схемы конкатенации S называется число r. Положим $l_c(\tilde{\alpha}) = \min l_c(S)$, где минимум берется по всем схемам конкатенации, реализующим слово $\tilde{\alpha}$ в алфавите $\mathfrak{A}$. Величина $l_c(\tilde{\alpha})$ называется *мультипликативной сложностью* слова (другие названия — аддитивная сложность[32]), длина цепочек слов[33])). В работе исследуются схемы конкатенации в двоичном алфавите, т. е. $\mathfrak{A} = \{0, 1\}$.

---

[31]) Мерекин Ю. В. Нижняя оценка сложности для схем конкатенации слов // *Дискретный анализ и исследование операций.* — 1996. — Т. 3, № 1. — С. 52–56.

[32]) См., например: Потапов В. Н. Аддитивная сложность слов с ограничениями на состав подслов // *Дискретный анализ и исследование операций. Сер.* 1. — 2004. — Т. 11, № 1. — С. 52–78; Мерекин Ю. В. Об аддитивной сложности частично коммутативных слов // *Дискретный анализ и исследование операций. Сер.* 1. — 2005. — Т. 12, № 4. — С. 40–50.

[33]) См., например: Althöfer I. Tight lower bounds on the length of word chains // *Inform.*

Обозначим через A_n^k множество всех двоичных наборов (слов) длины n, содержащих ровно k единиц. Положим

$$l_c(k,n) = \max_{\tilde{\alpha}\in A_n^k} l_c(\tilde{\alpha}), \quad k = 0,1,\ldots,n.$$

Доопределим выражение $\log C_n^k / \log\log C_n^k$ при $k = 0$ и $k = n$ нулем.

Теорема 1.7. *Пусть* $\{(k_m, n_m)\}, m = 1,2,\ldots,$ — *последовательность пар целых чисел, удовлетворяющая условиям:* $n_m \to \infty$ *при* $m \to \infty$, $0 \le k_m \le n_m$. *Тогда при* $m \to \infty$ *справедливо асимптотическое равенство*

$$l_c(k_m, n_m) \sim \log n_m + \frac{\log C_{n_m}^{k_m}}{\log\log C_{n_m}^{k_m}}.$$

При доказательстве верхней оценки этой теоремы в случае, когда $\log k = o(\log n)$ или $\log(n-k) = o(\log n)$ оказывается достаточно использовать верхнюю оценку для задачи Кнута. В случае, когда $\log k \sim \log(n-k) \sim \log n$ удается применить к этой задаче метод, разработанный Э. И. Нечипоруком для доказательства асимптотически точной верхней оценки сложности реализации класса булевых матриц с заданной долей единиц (заданной густоты) вентильными схемами глубины 2. В остальных случаях для получения асимптотически наилучшей верхней оценки предложен оригинальный метод.

В **§ 1.5** рассматривается одна задача о сложности вычислений в конечных группах, при исследовании которой важную роль играют оценки, полученные для задачи Беллмана.

Пусть G — конечная группа (групповую операцию будем называть умножением), а M_G — некоторое порождающее множество этой группы. Для каждого элемента g группы G определим его *сложность реализации над порождающим множеством* M_G, обозначаемую через $l(g; M_G)$, как минимальное число операций умножения, достаточное для вычисления элемента g с использованием элементов множества M_G (при этом все уже вычисленные элементы могут быть использованы многократно — и в

Process. Lett. — 1990. — V. 34, № 5. — P. 275–276; Berstel J., Brlek S. On the lenght of word chains // *Inform. Process. Lett.* — 1987. — V. 26, № 1. — P. 23–28; Red'kin N. P. Complexity of concatenation schemes for words from some classes // *Proceedings of two joint French-Russian seminars on combinatorial and algorithmical properties of discrete structures (April* 1998, *Moscow — February* 1999, *Nansy, France).* Project No 8/97. — French-Russian A. M. Liapunov Institute, 2001. — P. 107–114.

этом принципиальное отличие от других мер сложности вычислений элементов в группах[34])).

Сложность $L(G; M_G)$ конечной группы G над порождающим множеством M_G определяется так: $L(G; M_G) = \max_{g \in G} l(g; M_G)$.

Для произвольного класса $\mathfrak{K}_n$ групп порядка n сложность этого класса определяется равенством $L(\mathfrak{K}_n) = \max_{G \in \mathfrak{K}_n} \left(\max_{M_G} L(G; M_G) \right)$.

Для сложности абелевых групп при некоторых ограничениях установлена верхняя оценка, асимптотически совпадающая со стандартной «мощностной» нижней оценкой, справедливой для произвольной конечной группы. Кроме того, для класса $\mathfrak{A}_n$ всех абелевых групп порядка n установлена

Теорема 1.10. *При* $n \to \infty$

$$L(\mathfrak{A}_n) = \log n + \frac{\log n}{\log \log n} + o\left(\frac{\log n}{\log \log n} \right).$$

Глава 2 посвящена исследованию тех свойств мер сложности l, l_2 и l_F, которые из каких-либо соображений имеет смысл изучать одновременно для всех трех (или хотя бы для двух) вычислительных моделей.

В **§ 2.1** доказывается универсальная нижняя оценка, справедливая для всех трех изучаемых мер сложности целочисленных матриц. В ее основе лежат известные соображения об оценке сложности схемы через определитель матрицы, порождаемой вычисляемыми в вершинах схемы функциями. Впервые, по-видимому, рассуждения такого типа для нижних оценок сложности были использованы Ж. Моргенстерном[35]).

Пусть $A = (a_{ij})$ — произвольная матрица размера $p \times q$, а число k удовлетворяет неравенствам $1 \leq k \leq \min(p, q)$. Для наборов индексов $(i_1, i_2, \ldots, i_k)$ и $(j_1, j_2, \ldots, j_k)$, таких что $1 \leq i_1 < i_2 < \ldots < i_k \leq p$, $1 \leq j_1 < j_2 < \ldots < j_k \leq q$, обозначим через $A(i_1, i_2, \ldots, i_k;\ j_1, j_2, \ldots, j_k)$ квадратную матрицу порядка k, состоящую из элементов, находящихся на пересечении строк с номерами $i_1, i_2, \ldots, i_k$ и столбцов с номерами $j_1, j_2, \ldots, j_k$.

Положим

$$D(A) = \max_{k:\ 1 \leq k \leq \min(p,q)} \left(\max_{(i_1, \ldots, i_k;\ j_1, \ldots, j_k)} |\det A(i_1, i_2, \ldots, i_k;\ j_1, j_2, \ldots, j_k)| \right).$$

---

[34]) См., например: Глухов М. М., Зубов А. Ю. О длинах симметрических и знакопеременных групп подстановок в различных системах образующих // *Математические вопросы кибернетики, вып.* 8. — М.: Наука, 1999. — С. 5–32.

[35]) Morgenstern J. Note on a lower bound of the linear complexity of the fast Fourier transform // *J. Assoc. Comput. Mach.* — 1973. — V. 20. — P. 305–306.

Таким образом, $D(A)$ — это максимум абсолютных величин миноров матрицы A, где максимум берется по всем минорам.

Теорема 2.1. *Для любой ненулевой целочисленной матрицы A справедливы неравенства:*

$$l(A) \geq \log D(A), \quad l_2(A) \geq \log D(A), \quad l_F(A) \geq \log D(A)$$

(*в первом неравенстве подразумевается, что в матрице A нет нулевых строк и все ее элементы неотрицательны*).

Большинство доказываемых в данной работе нижних оценок сложности для индивидуальных последовательностей матриц во всех трех вычислительных моделях либо непосредственно следуют из теоремы 2.1, либо существенно ее используют.

В **§ 2.2** сначала обсуждается многократно открывавшийся и переоткрывавшийся (для разных задач, в разных терминах) так называемый «принцип двойственности»[36]), который применительно к изучаемым задачам формулируется следующим образом: для любой целочисленной матрицы A размера $p \times q$ с неотрицательными элементами без нулевых строк и столбцов справедливо равенство $l\left(A^T\right) - l(A) = p - q$; для любой целочисленной матрицы A размера $p \times q$ выполняются неравенства $-q \leq l_2\left(A^T\right) - l_2(A) \leq p$.

При этом, если во второй вычислительной модели в аддитивной постановке помимо операций $x + y$ и $x - y$ разрешить использование еще и операции $-x-y$, то для естественным образом определяемой меры сложности l_2' справедливо утверждение, аналогичное утверждению относительно меры сложности l: для любой целочисленной матрицы A размера $p \times q$ без нулевых строк и столбцов справедливо равенство $l_2'\left(A^T\right) - l_2'(A) = p - q$.

В отличие от мер сложности l и l_2, мера сложности l_F не обладает свойством двойственности. Действительно, сложность вычисления в третьей модели двух матриц размера, соответственно, 1×2 и 2×1, получающихся друг из друга транспонированием, может отличаться асимптотически в два раза:

$$l_F\left(\left(2^k, -2^k\right)\right) = k + 1, \quad l_F\left(\left(2^k, -2^k\right)^T\right) = 2k.$$

Прежде, чем переходить к исследованию асимптотического поведения величин $l(A)$, $l_2(A)$ и $l_F(A)$ в общем случае (для произвольных индивидуальных последовательностей матриц фиксированного или слаборастущего

[36]) Bernstein D. J. The transposition principle // `Available at: http://cr.yp.to/transposition.html.` — 2004.

размера), естественно изучить, как это было сделано для меры сложности l Н. Пиппенджером, асимптотическое поведение функций Шеннона для мер сложности l_2 и l_F.

При $K \geq 2$ положим $L_2(p, q, K) = \max l_2(A)$, $L_F(p, q, K) = \max l_F(A)$, где максимум берется по всем целочисленным матрицам $A = (a_{ij})$ размера $p \times q$, удовлетворяющим условиям $|a_{ij}| \leq K - 1$, $i = 1, \ldots, p$, $j = 1, \ldots, q$.

Доказательства двух следующих теорем существенно опираются на результат Н. Пиппенджера, но непосредственно из него не следуют. Более того, несмотря на общее сходство этих двух доказательств, есть и серьезные отличия, делающие попытку объединить их в одно неоправданной.

Теорема 2.2. *При условии* $pq \log K \to \infty$ *справедливо равенство*

$$L_2(p, q, K) = \min(p,\, q) \log K + \\ + \frac{pq \log(2K-1)}{\log(pq \log K)} \left(1 + O\left(\left(\frac{\log\log(pq \log K)}{\log(pq \log K)}\right)^{1/2}\right)\right) + O(\max(p,\, q));$$

Стоит отметить тот факт, что при доказательстве верхней оценки теоремы 2.2 предложен способ вычисления системы целочисленных линейных форм, дающий требуемую оценку числа операций и использующий только один раз операцию вычитания.

Теорема 2.3. *При условии* $pq \log K \to \infty$ *справедливы неравенства*

$$L_F(p, q, K) \leq \min(p,\, q+1) \log K + \\ + \frac{pq \log(2K-1)}{\log(pq \log K)} \left(1 + O\left(\left(\frac{\log\log(pq \log K)}{\log(pq \log K)}\right)^{1/2}\right)\right) + O(\max(p,\, q));$$

$$L_F(p, q, K) \geq \max\left(\min(p,\, q+1) \log K,\, \frac{pq \log(2K-1)}{\log(pq \log K)}\right) + O(\max(p,\, q)).$$

Таким образом для всех трех вычислительных моделей при слабых ограничениях установлена асимптотика роста соответствующих функций Шеннона, причем во всех трех случаях имеет место эффект Шеннона (при некоторых условиях). Однако можно ожидать (так часто бывает в различных задачах синтеза управляющих систем), что для некоторых достаточно широких классов матриц можно получать существенно лучшие оценки.

В этом направлении естественно исследовать классы матриц, для которых ограничение на величину элемента задается для каждого столбца (каждой строки) индивидуально. В качестве вычислительной модели используется первая модель — в данном случае это не очень принципиально.

Пусть $\mathcal{K} = (k_1, k_2, \ldots, k_q)$ — набор из q натуральных чисел, бóльших 1. Обозначим через $L(\mathcal{K}, p)$ наименьшее число операций умножения, достаточное для вычисления по переменным $x_1, x_2, \ldots, x_q$ любой системы одночленов $x_1^{r_{11}} x_2^{r_{12}} \ldots x_q^{r_{1q}}$, $x_1^{r_{21}} x_2^{r_{22}} \ldots x_q^{r_{2q}}, \ldots,$ $x_1^{r_{p1}} x_2^{r_{p2}} \ldots x_q^{r_{pq}}$, удовлетворяющей условиям $r_{ij} \le k_j - 1$, $i = 1, \ldots, p$, $j = 1, \ldots, q$.

Без ограничения общности можно считать, что $k_1 \ge k_2 \ge \ldots \ge k_q$ и выполнено естественное условие $p \le N_{\mathcal{K}}$, где $N_{\mathcal{K}} = k_1 k_2 \ldots k_m$ (т. е. число вычисляемых одночленов не превосходит общего числа одночленов соответствующего вида).

Теорема 2.4. *Пусть* $p \log N_{\mathcal{K}} \to \infty$. *Тогда*[37])

$$L(\mathcal{K}, p) \asymp \sum_{i=1}^{\min(p,q)} \log k_i + \frac{p \log N_{\mathcal{K}}}{\log(p \log N_{\mathcal{K}})} + p + q,$$

причем если выполняются условия

$$\sum_{i=1}^{\min(p,q)} \log k_i + p + q = o\left(\frac{p \log N_{\mathcal{K}}}{\log(p \log N_{\mathcal{K}})}\right), \quad q = o(\log N_{\mathcal{K}}),$$

то справедливо соотношение

$$L(\mathcal{K}, p) \sim \frac{p \log N_{\mathcal{K}}}{\log(p \log N_{\mathcal{K}})}.$$

Аналогичные оценки справедливы и в случае, когда на величины элементов матрицы ограничения накладываются по строкам, а не по столбцам.

В следующих трех главах изучается асимптотическое поведение величин $l(A)$, $l_2(A)$ и $l_F(A)$ для произвольных индивидуальных последовательностей матриц. При этой постановке имеет смысл в первую очередь рассматривать такое соотношение параметров, при котором вклад «мощностной» составляющей не является доминирующим. Этому условию удовлетворяет важный случай, когда размеры матриц фиксированы (или слабо растут). При этом отправной точкой, помимо тривиальных верхних оценок, получающихся из оценок соответствующих функций Шеннона, является универсальная для всех трех мер сложности оценка снизу через величину $\log D(A)$. Оказывается, что для каждой из трех вычислительных

[37]) Здесь и далее запись $f(x) \asymp g(x)$ означает одновременное выполнение соотношений $f(x) = O(g(x))$ и $g(x) = O(f(x))$

моделей ситуация при такой постановке сугубо индивидуальна. Для наиболее сильной второй вычислительной модели верхняя оценка асимптотически совпадает с универсальной нижней (при фиксированных или слаборастущих значениях размеров матриц), для первой модели верхняя оценка асимптотически совпадает с общей нижней только для матриц малой размерности, а для третьей модели уже для матриц размера 2×1 указанная нижняя оценка в некоторых случаях может быть улучшена асимптотически вдвое.

Глава 3 посвящена исследованию задачи о сложности вычисления систем одночленов.

В **§ 3.1** исследуется самый простой случай — вычисление системы из двух одночленов от двух переменных. Основным результатом этого параграфа является

Теорема 3.1. *Для произвольной последовательности целочисленных матриц* $A(n) = (a_{ij}(n))$ *размера* 2×2 *с неотрицательными элементами и без нулевых строк, удовлетворяющей при* $n \to \infty$ *условию* $\max_{a_{ij} \in A(n)} a_{ij}(n) \to \infty$, *справедливы оценки*

$$\log D(A(n)) \leq l\left(A(n)\right) \leq \log D(A(n)) + O\left(\frac{\log \max a_{ij}(n)}{\log \log \max a_{ij}(n)}\right).$$

Из теоремы 3.1 вытекает наличие для исследуемой задачи эффекта Шеннона, который в данном случае заключается в том, что почти все системы из двух одночленов от двух переменных с показателями степеней, не превосходящими n, имеют асимптотически максимальную сложность $2 \log n + o(\log n)$. При этом стоит подчеркнуть тот факт, что эффект Шеннона имеет место в задаче, для которой нижние оценки доказываются немощностным методом.

Уже в простейшем случае, когда матрицы имеют размер 2×2, при всей прозрачности основной идеи доказательства верхней оценки, само доказательство технически является довольно громоздким. Для того, чтобы упростить дальнейшие доказательства, выделив в них содержательную часть и проведя техническую работу один раз в общем случае, в **§ 3.1** вводится вспомогательная вычислительная модель, для которой, с одной стороны, доказывать верхние оценки существенно проще, и которая, с другой стороны, допускает при некоторых естественных условиях переход к вычислению в исследуемых моделях без асимптотического увеличения сложности.

В терминах схем из функциональных элементов умножения на примере первой вычислительной модели вводится понятие *обобщенной* схемы, в которой дополнительно разрешается использование одновходовых элементов, реализующих по подаваемой на вход элемента функции f ее степень f^r, где r — рациональное число, удовлетворяющее условию $0 \le r \le 2$ (значение r, вообще говоря, свое для каждого такого элемента). При таком усилении вычислительных возможностей также расширяется и класс вычисляемых матриц: обобщенными схемами можно вычислить любую матрицу с неотрицательными рациональными элементами.

Пусть $A = (a_{ij})$ — матрица размера $p \times q$ с неотрицательными рациональными элементами. Через $\lambda(A)$ обозначается минимально возможная сложность обобщенной схемы из функциональных элементов, реализующей систему функций $x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}}$, $x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}, \dots,$ $x_1^{a_{p1}} x_2^{a_{p2}} \dots x_q^{a_{pq}}$.

Ключевым свойством обобщенных схем является полная определенность со сложностью возведения в степень: при $0 \le \alpha < 1$ выполняется равенство $\lambda(x^\alpha) = 1$, а при $\alpha \ge 1$ — равенство $\lambda(x^\alpha) = \lceil \log \alpha \rceil$.

Способ доказательства верхних оценок, основанный на оценках сложности обобщенных схем заключается в следующем. Сначала для целочисленной матрицы A строится обобщенная схема нужной сложности (например, сложности $\log D(A) + O(1)$), причем эта обобщенная схема помимо ограничения на сложность должна обладать еще одним важным свойством — допускать разбиение на ограниченное (речь идет о вычислении последовательности матриц) или слаборастущее число подсхем, каждая из которых либо состоит из одного двухвходового функционального элемента, либо имеет один вход, один выход, и, соответственно, вычисляет некоторую степень подаваемой на вход подсхемы функции (подсхемы этих двух типов называются *простейшими*). После этого построенная обобщенная схема перестраивается без асимптотического увеличения сложности в обычную схему, вычисляющую ту же матрицу A. Возможность такого перестроения устанавливает

Теорема 3.2. *Пусть элементы последовательности целочисленных матриц $A(n) = (a_{ij}(n))$ размера $p(n) \times q(n)$ с неотрицательными элементами и без нулевых строк, $n = 1, 2, \dots$, удовлетворяющей при $n \to \infty$ условию $\max\limits_{a_{ij} \in A(n)} a_{ij}(n) \to \infty$, вычисляются обобщенными схемами $\widehat{S}(n)$, состоящими из $k(n)$ простейших подсхем, причем выполняются неравен-*

ства

$$k(n) \le \left(\log\log\log \max_{a_{ij} \in A(n)} a_{ij}(n) \right)^{1/2},$$

$$q(n) \le \frac{1}{8} \left(\log\log\log \max_{a_{ij} \in A(n)} a_{ij}(n) \right)^{1/2}.$$

Тогда справедливо соотношение

$$l\left(A(n)\right) \le \lambda\left(\widehat{S}(n)\right) + o\left(\frac{\log \max\limits_{a_{ij} \in A(n)} a_{ij}(n)}{\log\log\log \max\limits_{a_{ij} \in A(n)} a_{ij}(n)} \right).$$

Аналогичные утверждения справедливы также для второй и третьей вычислительной модели.

Далее описанным выше способом доказывается

Теорема 3.3. *Для произвольных последовательностей целочисленных матриц* $A(n) = (a_{ij}(n))$ *и* $B(n) = (b_{ij}(n))$ *размеров, соответственно,* $p(n) \times 2$ *и* $2 \times q(n)$ *с неотрицательными элементами и без нулевых строк, удовлетворяющих при* $n \to \infty$ *условиям*

$$p(n) = o\left(\left(\log\log\log \max_{a_{ij} \in A(n)} a_{ij}(n) \right)^{1/2} \right),$$

$$q(n) = o\left(\left(\log\log\log \max_{b_{ij} \in B(n)} b_{ij}(n) \right)^{1/2} \right),$$

справедливы оценки

$$\log D(A(n)) \le l\left(A(n)\right) \le \log D(A(n)) + o\left(\frac{\log \max a_{ij}(n)}{\log\log\log \max a_{ij}(n)} \right),$$

$$\log D(B(n)) \le l\left(B(n)\right) \le \log D(B(n)) + o\left(\frac{\log \max b_{ij}(n)}{\log\log\log \max b_{ij}(n)} \right).$$

В **§ 3.3** также путем сведения к реализации обобщенными схемами устанавливается асимптотическая формула для сложности вычисления системы из трех одночленов от трех переменных.

Теорема 3.4. *Для произвольной последовательности целочисленных матриц* $A(n) = (a_{ij}(n))$ *размера* 3×3 *с неотрицательными элементами и без нулевых строк, удовлетворяющей при* $n \to \infty$ *условию* $\max_{a_{ij} \in A(n)} a_{ij}(n) \to \infty$, *справедливы неравенства*

$$\log D(A(n)) \le l\left(x^{a_{11}} y^{a_{12}} z^{a_{13}}, x^{a_{21}} y^{a_{22}} z^{a_{23}}, x^{a_{31}} y^{a_{32}} z^{a_{33}}\right) \le \\ \le \log D(A(n)) + o\left(\log D(A(n))\right).$$

При доказательстве этой теоремы приходится исследовать большое число случаев, часть из которых довольно проста, однако для некоторых случаев требуется серьезный анализ.

Частичное разъяснение природы трудностей, возникающих при доказательстве верхней оценки теоремы 3.4 дают результаты из **§ 3.4**. Логично вытекающее из теорем 3.1, 3.3 и 3.4 предположение о том, что, возможно, при всех фиксированных значениях p и q для матриц размера $p \times q$ величина $l(A)$ асимптотически растет как $\log D(A)$ (косвенным доводом в пользу этого предположения является справедливость в аналогичных условиях формулы $l_2(A) \sim \log D(A)$ — об этом говорится подробнее в следующей главе), оказывается неверным уже для квадратных матриц порядка 4.

Обозначим через $A(t, n)$ квадратную матрицу порядка $2t$, $t \ge 2$, определяемую таким образом. Первой строкой матрицы $A(t, n)$ является набор длины $2t$, первая половина разрядов которого равна n, а вторая половина — 0. Остальные $2t - 1$ строк матрицы $A(t, n)$ получаются из первой строки последовательным циклическим сдвигом на один разряд вправо.

Теорема 3.5. *При условии* $t = o(\log n)$ *справедливо асимптотическое равенство*

$$l(A(t, n)) \sim 2t \log n.$$

Следствием этой теоремы является такое утверждение — при условии $t \le \log n / \log\log n$ выполняется соотношение

$$l(A(t, n)) \sim \frac{2t}{t+1} \log D(A(t, n)).$$

Таким образом, помимо прочего, приведен пример последовательности матриц размера $2t \times 2t$, для которой устанавливаемую теоремой 2.1 нижнюю оценку в рамках первой вычислительной модели можно усилить асимптотически в $2t/(t+1)$ раз.

Глава 4 посвящена исследованию задачи о сложности вычисления целочисленных линейных форм. Для этой задачи получен в некотором смысле (а именно, с точки зрения асимптотики) окончательный результат.

Теорема 4.1. *Пусть последовательность целочисленных матриц* $A(n) = \big(a_{ij}(n)\big)$ *размера* $p(n) \times q(n)$ *при* $n \to \infty$ *удовлетворяет условию*

$$\frac{p(n) + q(n)}{\left(\log\log D(A(n))\right)^{1/2}} \to 0.$$

Тогда

$$\log D(A(n)) \le l_2\left(A(n)\right) \le \log D(A(n)) + o\big(\log D(A(n))\big).$$

В формулировке этой теоремы можно указать более слабые ограничения (при этом более сложного вида), при которых справедлива верхняя оценка вида $\log D(A) + o\big(\log D(A)\big)$. Однако, наиболее принципиальным представляется содержащееся в теореме 4.1 утверждение о том, что для любых фиксированных (и даже слаборастущих) значениях размеров задающей систему функций матрицы верхняя оценка сложности вычисления этой системы асимптотически совпадает с нижней.

Из теорем 3.4 и 4.1 также следует, что при переходе от первой вычислительной модели ко второй, т. е. при добавлении возможности кроме основной операции использовать дополнительную (вычитание или деление в зависимости от интерпретации) сложность вычисления может значительно уменьшаться.

Глава 5 посвящена исследованию задачи о сложности вычисления систем элементов свободных абелевых групп. Мера сложности l_F значительно отличается по своим свойствам от мер сложности l и l_2. В частности, как уже отмечалось, применительно к ней не работают (или работают не в достаточной мере) соображения двойственности:

$$l_F\left(\left(2^k, -2^k\right)\right) = k + 1, \quad l_F\left(\left(2^k, -2^k\right)^T\right) = 2k.$$

Последнее равенство можно переписать так:

$$l_F\left(\left(2^k, -2^k\right)^T\right) = 2\log D(\left(\left(2^k, -2^k\right)^T\right),$$

что сразу дает пример нижней оценки, вдвое большей, чем дается теоремой 2.1 — для меры сложности l_2 при фиксированных размерах матриц

в силу теоремы 4.1 такого эффекта (с точки зрения асимптотики) быть не может, а для меры сложности l — такого эффекта не может быть для матриц малого размера.

В **§ 5.1** исследуются самые простые случаи — когда матрицы имеют размеры $1 \times q$, $p \times 1$ и $2 \times q$. И если в первом случае рост сложности вычисления в третьей модели устанавливается как простое следствие предыдущих результатов, то для последних двух типов матриц при изучении асимптотики роста обнаруживается новый эффект.

Для произвольной матрицы A размера $p \times q$ определим величину $T(A)$ равенством

$$T(A) = \max_{j\colon 1 \le j \le q} \left\{ \max\{a_{1j}, a_{2j}, \ldots, a_{pj}, 0\} \left| \min\{a_{1j}, a_{2j}, \ldots, a_{pj}, 0\} \right| \right\}.$$

Таким образом, $T(A)$ — это максимум абсолютных величин попарных произведений элементов матрицы A, где максимум берется по всем парам элементов, удовлетворяющим двум условиям — эти элементы должны находиться в одном столбце и иметь разные знаки (если таких пар нет, то $T(A) = 0$).

С использованием теоремы 2.1 в работе устанавливается справедливость для любой целочисленной матрицы A неравенства $l_F(A) \ge \log \max\{T(A), 1\}$. Величина $\log T(A)$, вообще говоря, может превосходить величину $\log D(A)$, но не более, чем в 2 раза.

Теорема 5.3. *Для произвольной последовательности целочисленных матриц $A(n) = (a_{ij}(n))$ размера $2 \times q(n)$, удовлетворяющей условию*

$$\frac{q(n)}{\log\log \max\limits_{i,\,j} |a_{ij}(n)|} \to 0$$

при $n \to \infty$, справедливо асимптотическое равенство

$$l_F(A(n)) \sim \log \max\{D(A(n)), T(A(n))\}.$$

Еще более нетривиальная ситуация возникает в изучаемом в **§ 5.2** случае матриц размера 3×2, для которого также установлена асимптотика роста величины l_F.

Пусть матрица $A = (a_{ij})$ имеет размеры 3×2. Под записью a_{st} при $s > 3$ или $t > 2$ будем понимать элемент a_{ij}, где i и j определяются из условий $1 \le i \le 3$, $i \equiv s \pmod 3$; $1 \le j \le 2$, $j \equiv t \pmod 2$.

Элемент a_{ij} матрицы A размера 3×2 называется *особым*, если выполняются следующие условия:

$$a_{ij} \neq 0, \quad a_{ij}a_{i+1,j} \leq 0, \quad a_{ij}a_{i+2,j} \leq 0, \quad |a_{i+1,j}| + |a_{i+2,j}| \neq 0.$$

Через $A(s,t)$ обозначим матрицу размера 2×2, в которой первой строкой является строка матрицы A, содержащая элемент a_{s1}, а второй — строка матрицы A, содержащая элемент a_{t1}.

Пусть a_{ij} — особый элемент матрицы A размера 3×2. Определим величину $r(a_{ij})$ следующим обазом:

1) если выполняются неравенства $\det A(i+1,i+2)\det A(i+2,i) \geq 0$ и $\det A(i+1,i+2)\det A(i,i+1) \geq 0$, то полагаем

$$r(a_{ij}) = |a_{ij}\det A(i+1,i+2)|\,;$$

2) если выполняется неравенство $\det A(i+1,i+2)\det A(i+2,i) < 0$, то полагаем

$$r(a_{ij}) = |a_{ij}\det A(i+1,i+2)|\,\frac{\max\{|a_{i1}|,|a_{i2}|,|a_{i+2,1}|,|a_{i+2,2}|\}}{D(A(i+2,i))};$$

3) если выполняется неравенство $\det A(i+1,i+2)\det A(i,i+1) < 0$, то полагаем

$$r(a_{ij}) = |a_{ij}\det A(i+1,i+2)|\,\frac{\max\{|a_{i1}|,|a_{i2}|,|a_{i+1,1}|,|a_{i+1,2}|\}}{D(A(i,i+1))}.$$

Для элементов a_{ij}, не являющихся особыми в целочисленной матрице A размера 3×2, положим $r(a_{ij}) = 0$. Далее, для матрицы A определим величину $R(A)$ равенством

$$R(A) = \max_{a_{ij} \in A} r(a_{ij}).$$

Теорема 5.4. *Для произвольной последовательности целочисленных матриц $A(n) = (a_{ij}(n))$ размера 3×2, удовлетворяющей при $n \to \infty$ условию*

$$\max_{a_{ij} \in A(n)} |a_{ij}(n)| \to 0,$$

справедливо асимптотическое равенство

$$l_F(A(n)) \sim \log \max\{D(A(n)), T(A(n)), R(A(n))\}.$$

Величина $R(A)$ в последнем соотношении может быть определяющей — например, для матрицы

$$A = \begin{pmatrix} -n & 0 \\ n & 0 \\ 0 & n \end{pmatrix}$$

выполняются равенства $D(A) = T(A) = n^2$, $R(A) = n^3$.

В **§ 5.3** для матриц $A(t, n)$, введенных в § 3.4, изучается сложность вычисления в третьей модели, причем асимптотика роста отличается от той, что была установлена для этой последовательности матриц в теореме 3.4 при вычислении в первой модели.

Теорема 5.5. *При условии* $t = o\left(\frac{\log n}{\log\log n}\right)$ *справедливы асимптотические равенства*

$$l_F(A(t, n)) \sim (t + 1)\log n \sim \log D(A).$$

Таким образом, переход от первой вычислительной модели к третьей, т. е. добавление не очень важной на первый взгляд возможности использования помимо переменных обратных к ним величин, может существенно менять ситуацию при вычислении системы одночленов.

Теорема 5.6. *При условии* $t = o(\log n)$ *справедливо асимптотическое равенство*

$$\frac{l(A(t, n))}{l_F(A(t, n))} \sim \frac{2t}{t + 1}.$$

Рассматриваемые в работе матрицы $A(t, n)$ вырождены — при размере $2t \times 2t$ они имеют ранг $t + 1$. Однако эти матрицы можно немного «подправить», увеличив на 1 диагональные элементы $a_{t+2,t+2}, a_{t+3,t+3}, \ldots, a_{2t,2t}$. Полученные матрицы $A'(t, n)$, с одной стороны, невырождены и удовлетворяют равенствам $D\left(A'(t, n)\right) = \det A'(t, n) = n^{t+1} = D(A(t, n))$, а с другой стороны, для них все оценки сложности сохраняются практически без изменений.

Появление данной работы было бы невозможно без Олега Борисовича Лупанова. Автор рассматривает эту работу как скромную дань памяти своего учителя.

СПИСОК ОСНОВНЫХ РАБОТ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ, ОПУБЛИКОВАННЫХ В ВЕДУЩИХ РЕЦЕНЗИРУЕМЫХ НАУЧНЫХ ЖУРНАЛАХ И ИЗДАНИЯХ (В СООТВЕТСТВИИ С ПЕРЕЧНЕМ ВАК)

1. Кочергин В. В. Об аддитивных вычислениях систем целочисленных линейных форм // *Вестник Московского университета. Сер.* 1. *Математика. Механика.* — 1993. — № 6. — С. 97–101.

2. Кочергин В. В. О вычислении наборов степеней // *Дискретная математика.* — Т. 6, вып. 2. — 1994. — С. 129–137.

3. Кочергин В. В. О сложности вычислений одночленов и наборов степеней // *Дискретный анализ.* — Новосибирск: Издательство Института математики СО РАН, 1994. — (Тр./РАН. Сиб. отделение. Ин-т математики; Т. 27) — С. 94–107.

4. Кочергин В. В. О сложности вычислений в конечных абелевых, нильпотентных и разрешимых группах // *Дискретная математика.* — Т. 5, вып. 1. — 1993. — С. 91–111.

5. Кочергин В. В. О сложности вычислений в конечных нильпотентных группах // *Дискретный анализ и исследование операций.* — 1996. — Т. 3, № 1. — С. 43–51.

6. Кочергин В. В. О сложности вычисления систем одночленов с ограничениями на степени переменных // *Дискретная математика.* — Т. 10, вып. 3. — 1998. — С. 27–34.

7. Кочергин В. В. О мультипликативной сложности двоичных слов с заданным числом единиц // *Математические вопросы кибернетики, вып.* 8. — М.: Наука, 1999. — С. 63–76.

8. Кочергин В. В. О сложности вычисления пары одночленов от двух переменных // *Дискретная математика.* — Т. 17, вып. 4. — 2005. — С. 116–142.

9. Кочергин В. В. Об асимптотике сложности аддитивных вычислений систем целочисленных линейных форм // *Дискретный анализ и исследование операций. Серия* 1. — 2006. — Т. 13, № 2. — С. 38–58.

10. Кочергин В. В. О сложности вычисления системы из трех одночленов от трех переменных // *Математические вопросы кибернетики, вып.* 15. — М.: Физматлит, 2006. — С. 79–155.

11. Кочергин В. В. О максимальной сложности совместного вычисления систем элементов свободной абелевой группы // *Вестник Московского университета. Сер.* 1. *Математика. Механика.* — 2007, № 3. — С. 14–19.

СПИСОК РАБОТ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ, ОПУБЛИКОВАННЫХ В ИЗДАНИЯХ, НЕ ВХОДЯЩИХ В ПЕРЕЧЕНЬ ВАК

12. Кочергин В. В. Об одном классе аддитивных цепочек // *Теоретические и прикладные аспекты математических исследований* (*сборник трудов конференции молодых ученых механико-математического ф-та МГУ*). — Москва: Изд-во Московского университета, 1994. — С. 9–13.

13. Кочергин В. В. О сложности некоторых мультипликативных вычислений // *Материалы* VII *межгосударственной школы-семинара "Синтез и сложность управляющих систем"* (*Минск*, 13–16/XI 1995). — Москва: Изд-во механико-математического факультета МГУ, 1996. — С. 16–18.

14. Kochergin V. V. Some generalizations of addition chains problem // *Proceedings of two joint French-Russian seminars on combinatorial and algorithmical properties of discrete structures* (*April* 1998, *Moscow — February* 1999, *Nansy, France*). Project No 8/97. — French-Russian A. M. Liapunov Institute, 2001. — P. 33–41.

15. Кочергин В. В. О сложности получения двоичных слов с заданным числом единиц схемами конкатенации // *Труды* III *Международной конференции "Дискретные модели в теории управляющих систем"* (22–27 *июня* 1998 *г.*). — Москва, Диалог–МГУ, 1998. — С. 58–62.

16. Кочергин В. В. О двух обобщениях задачи об аддитивных цепочках // *Труды* IV *Международной конференции "Дискретные модели в теории управляющих систем"* (19–25 *июня* 2000 *г.*). — Москва, "МАКС Пресс", 2000. — С. 55–59.

17. Кочергин В. В. О сложности вычисления системы одночленов специального вида // *Материалы* X *Межгосударственной школы-семинара "Синтез и сложность управляющих систем"* (*Минск*, 29 *ноября* – 3 *декабря* 1999 *г.*). – М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2000. — С. 12–14.

18. Кочергин В. В. О некоторых обобщениях задачи об аддитивных цепочках // *Дискретная математика и ее приложения. Сборник лекций.* — М.: Изд-во Центра прикладных исследований при механико-математическом факультете МГУ, 2001. — С. 59–83.

19. Кочергин В. В. О сложности вычисления систем одночленов от двух переменных // *Труды* VII *Международной конференции «Дискретные модели в теории управляющих систем»* (*Покровское,* 4–6 *марта* 2006 *г.*). — М.: МАКС Пресс, 2006. — С. 185–190.

20. Кочергин В. В. О сложности совместного вычисления двух эле-

ментов свободной абелевой группы // *Материалы* XVI *Международной школы-семинара «Синтез и сложность управляющих систем»* (*Санкт-Петербург,* 26–30 *июня* 2006 *г.*). — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 54–59.

21. Кочергин В. В. Об аддитивной сложности целочисленных матриц размера 3×2 // *Материалы* IX *Международного семинара «Дискретная математика и ее приложения», посвященного* 75*-летию со дня рождения академика О. Б. Лупанова* (*Москва,* 18–23 *июня* 2007 *г.*). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 99–102.

22. Кочергин В. В. О сложности вычисления систем одночленов и систем целочисленных линейных форм // *Дискретная математика и ее приложения. Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. Выпуск* III. — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 3–63.

23. Кочергин В. В. О сложности совместного вычисления трех элементов свободной абелевой группы с двумя образующими // *Дискретный анализ и исследование операций. Серия* 1. — 2008. — Т. 15, № 2. — С. 23–64.

24. Кочергин В. В. Замечание о сложности вычисления систем одночленов // *Проблемы теоретической кибернетики. Тезисы докладов* XIV *Международной конференции* (*Казань*, 2–7 *июня* 2008 *г.*). — Казань: Отечество, 2008. — С. 62.