МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи
УДК 519.714

Черухин Дмитрий Юрьевич

О СРАВНЕНИИ БАЗИСОВ ПРИ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ ФОРМУЛАМИ

01.01.09 математическая кибернетика

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

МОСКВА 2000

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

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

Научный руководитель — доктор физико-математических наук, член-корреспондент РАН, профессор О. Б. Лупанов.

Официальные оппоненты — доктор физико-математических наук, профессор В. Б. Алексеев;

— кандидат физико-математических наук, доцент В. А. Стеценко.

Ведущая организация — Институт математики Сибирского отделения РАН.

Защита диссертации состоится 16 июня 2000 г. в 16 час. 15 мин. на заседании диссертационного совета Д.053.05.05 при Московском государственном университете им. М. В. Ломоносова по адресу: 119899, ГСП, Москва, Воробьевы горы, МГУ, механико-математический факультет, аудитория 14–08.

С диссертацией можно ознакомиться в библиотеке механико-математического факультета МГУ (Главное здание, 14 этаж).

Автореферат разослан 16 мая 2000 г.

Ученый секретарь диссертационного совета Д.053.05.05 при МГУ,
доктор физико-математических наук,
профессор В. Н. Чубариков.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Тема диссертации относится к математической теории синтеза и сложности управляющих систем[1]. Предметом исследования в диссертации являются формулы в конечных полных булевых базисах[2]. В диссертации исследуется зависимость сложности реализации булевых функций формулами от базиса[3].

Как показал О. Б. Лупанов, сложность почти всех булевых функций в классе формул асимптотически не зависит от базиса[4]. В то же время, существуют последовательности функций, реализующиеся в одних базисах по порядку проще, чем в других. Первый пример такой последовательности привела Б. А. Субботовская[5]. Она показала, что последовательность линейных булевых функций $x_1 \oplus \ldots \oplus x_n$ реализуется в базисе $\{\&, \vee, \neg\}$ со сложностью, по порядку не меньшей, чем $n^{3/2}$. Очевидно, что эта же последовательность имеет линейную сложность в базисе $\{\&, \vee, \neg, \oplus\}$.

В связи с этим результатом Б. А. Субботовской, О. Б. Лупанов в начале 60-х годов поставил задачу сравнения базисов в следующем виде. Пусть $Б_1$ и $Б_2$ — произвольные базисы. Скажем, что базис $Б_1$ предшествует базису $Б_2$, если существуют такие константы C и D, что для любой булевой функции f выполнено неравенство $L_{Б_1}(f) \leqslant C \cdot L_{Б_2}(f) + D$ (здесь $L_Б(f)$ — сложность функции f в базисе $Б$, т. е. наименьшая из сложностей формул в базисе $Б$, реализующих функцию f; сложностью формулы называется

[1] Яблонский С. В. Основные понятия кибернетики // Проблемы кибернетики. Вып. 2. М.: Физматгиз, 1959. С. 7–38.

[2] Яблонский С. В. Введение в дискретную математику. М.: Наука, 1979. 272 с.

[3] Лупанов О. Б. О методах получения оценок сложности и вычисления индивидуальных функций // Дискретный анализ. Вып. 25. Новосибирск, ИМ СО АН СССР, 1974. С. 3–18.

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

[5] Субботовская Б. А. О реализации линейных функций формулами в базисе $\vee, \&, ^-$ // Докл. АН СССР. 1961. Т. 136, No 3. С. 553–555.

число вхождений в нее символов переменных). Отношение предшествования задает частичный порядок на множестве базисов и естественным образом определяет производные отношения: строгого предшествования, эквивалентности, несравнимости и непосредственного предшествования.

Отметим основные результаты предшественников, относящиеся к сравнению полных конечных булевых базисов. О. Б. Лупанов дал признак сравнения произвольных базисов и на его основании показал, что базис $Б_0 = \{\&, \vee, \neg\}$ является наибольшим, т. е. любой базис ему предшествует. Б. А. Субботовская построила пример неэквивалентных базисов; доказала критерий эквивалентности произвольного базиса базису $Б_0$[6]; дала неалгоритмический критерий сравнения произвольных базисов[7]; для некоторых базисов $Б$ (в том числе, неэквивалентных базису $Б_0$) доказала, что базис $Б \cup \{\oplus\}$ строго предшествует базису $Б$[8].

В. А. Стеценко классифицировал все S-функции (функции, ««слабоповторные»» в базисе $Б_0$) и дал необходимое условие того, что произвольный базис является предмаксимальным (т. е. непосредственно предшествует базису $Б_0$)[9]. Н. А. Перязев показал, что никакой ««немонолинейный»» базис не предшествует никакому ««монолинейному»» базису[10]; классифицировал все функции, ««слабоповторные»» в базисе, состоящем из всех двуместных функций[11];

---

[6]Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами // Докл. АН СССР. 1963. Т. 149, No 4. С. 784–787.

[7]Мучник Б. А. Об одном критерии сравнимости базисов при реализации функций алгебры логики формулами // Матем. заметки. 1967. Т. 1, No 5. С. 515–524.

[8]Мучник Б. А. Оценка сложности реализации линейной функции формулами в некоторых базисах // Кибернетика. 1970. No 4. С. 29–38.

[9]Стеценко В. А. О предплохих базисах в P_2 // Математические вопросы кибернетики. Вып. 4. М.: Наука, 1992. С. 139–177.

[10]Перязев Н. А. Сложность представлений булевых функций формулами в немонолинейных базисах. Иркутский университет. Серия: Дискретная математика и информатика. Вып. 2. Иркутск, 1995. 15 с.

[11]Перязев Н. А. Слабоповторные булевы функции в бинарном базисе. Иркутский университет. Серия: Дискретная математика и информатика. Вып. 4. Иркутск, 1998. 12 с.

Неисследованными оказались такие принципиальные вопросы, как алгоритмическая разрешимость задачи сравнения произвольных базисов, существование бесконечного множества попарно неэквивалентных и попарно несравнимых базисов, существование бесконечных строго возрастающих и строго убывающих цепей базисов, существование и структура предмаксимальных базисов и др.

Цель работы. Целью диссертации является доказательство алгоритмического критерия сравнения базисов и получение с его помощью качественных результатов о структуре отношения предшествования на множестве базисов.

Методы исследования. В диссертации использованы разработанные автором методы получения нижних оценок сложности индивидуальных последовательностей функций, основанные на идее ««забивания переменных»», впервые использованной Б. А. Субботовской[12].

Научная новизна. Результаты диссертации являются новыми. В диссертации получены следующие результаты:

1) доказана алгоритмическая разрешимость задачи сравнения базисов; дан алгоритмический критерий сравнения базисов;

2) доказано существование бесконечного множества попарно неэквивалентных базисов; доказано существование бесконечной строго убывающей цепи базисов; доказано отсутствие минимальных базисов; доказано отсутствие бесконечных строго возрастающих цепей базисов;

3) доказано существование предмаксимальных базисов; получена классификация с точностью до эквивалентности предмаксимальных базисов;

4) доказано существование несравнимых базисов; доказано существование бесконечного множества попарно несравнимых базисов; для каждого

[12]Субботовская Б. А. О реализации линейных функций формулами в базисе $\vee, \&, ^-$ // Докл. АН СССР. 1961. Т. 136, No 3. С. 553–555.

базиса доказано существование бесконечного множества попарно не эквивалентных базисов, непосредственно ему предшествующих.

Теоретическая и практическая ценность. Диссертация носит теоретический характер. Полученные результаты могут быть полезны специалистам по дискретной математике и математической кибернетике, работающим в МГУ, Институте прикладной математики РАН, НИИ Прикладной математики и кибернетики при Нижегородском гос. университете, Институте математики Сибирского отделения РАН.

Апробация. Результаты диссертации докладывались на XII-й Международной конференции ««Проблемы теоретической кибернетики»» (Н. Новгород, 1999), на I-й (Москва, 1997), II-й (Н. Новгород, 1998) и III-й (Новосибирск, 1999) Научных молодежных школах по дискретной математике и ее приложениям, XIX-й (1997), XX-й (1998) и XXI-й (1999) Конференциях молодых ученых механико-математического факультета МГУ, на семинаре ««Математические вопросы кибернетики»» в МГУ под руководством чл.-корр. РАН С. В. Яблонского (1998) и чл.-корр. РАН О. Б. Лупанова (1999), и на семинаре ««Синтез управляющих систем»» в МГУ под руководством чл.-корр. РАН О. Б. Лупанова (1998).

Публикация. Основные результаты диссертации опубликованы в работах [1–7].

Структура и объем диссертации. Диссертация изложена на 90 страницах, состоит из введения, четырех глав и списка литературы. Список литературы включает 21 источник.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении изложены: постановка задачи; история вопроса; результаты, полученные в диссертации; краткое содержание последующих глав и параграфов.

В первой главе введены и исследованы функции, для которых в последующих главах получена нижняя оценка сложности. Первая глава состоит из параграфов 1–3.

В §1 содержатся основные понятия, используемые в диссертации. Приведем некоторые из них. Базисом будем называть произвольную конечную полную систему булевых функций. Примерами базисов являются $Б_0 = \{\&, \vee, \neg\}$ и $P_2(n) = \{f : \{0,1\}^n \to \{0,1\}\}$. Определим по индукции множество *формул* (*в базисе Б*).

Базис индукции. Пусть f — n-местная функция, $f \in Б$. Тогда выражение $f(x_1, \dots, x_n)$ при $n \geqslant 1$ [символ f при $n = 0$] является формулой в $Б$.

Индуктивный переход. Пусть f — n-местная функция, $n \geqslant 1$, $f \in Б$, каждое из выражений $F_1, \dots, F_n$ является либо ранее построенной формулой в $Б$, либо переменной из множества $X = \{x_1, x_2, \dots\}$. Тогда выражение $f(F_1, \dots, F_n)$ является формулой в $Б$.

Подформулой формулы F называется часть формулы F, состоящая из подряд идущих символов и являющаяся формулой. *Сложностью формулы* F по переменной x_i (обозначение: $L_{x_i}(F)$) называется число вхождений в F переменной x_i. *Сложностью формулы* F (обозначение: $L(F)$) называется суммарное число вхождений в F символов переменных. *Сложностью функции* f *в базисе* $Б$ (обозначение: $L_Б(f)$) называется наименьшая из сложностей формул в базисе $Б$, реализующих функцию f. Обозначим через $V(f)$ множество существенных переменных функции f, положим $\mathrm{nes}(f) = |V(f)|$. Через $M_Б(f)$ обозначим отношение $L_Б(f)/\mathrm{nes}(f)$, если $\mathrm{nes}(f) \neq 0$.

Скажем, что базис $Б_1$ *предшествует* базису $Б_2$ (обозначение: $Б_1 \preccurlyeq Б_2$), если существуют такие числа C и D, что для любой булевой функции f выполнено $L_{Б_1}(f) \leqslant C L_{Б_2}(f) + D$. Базисы $Б_1$ и $Б_2$ *эквивалентны* (обозначение: $Б_1 \sim Б_2$), если $Б_1 \preccurlyeq Б_2$ и $Б_2 \preccurlyeq Б_1$. Базис $Б_1$ *строго предшествует* базису $Б_2$ (обозначение: $Б_1 \prec Б_2$), если $Б_1 \preccurlyeq Б_2$ и $Б_2 \not\preccurlyeq Б_1$. Базисы $Б_1$ и $Б_2$ *несравнимы*, если $Б_1 \not\preccurlyeq Б_2$ и $Б_2 \not\preccurlyeq Б_1$. Базис $Б_1$ *непосредственно предшествует* базису $Б_2$, если $Б_1 \prec Б_2$ и не существует такого базиса $Б'$, что выполнено $Б_1 \prec Б' \prec Б_2$. Базис $Б$ называется *предмаксимальным*, если $Б$ непосредственно предшествует базису $Б_0$.

Формула F называется *бесповторной*, если каждая переменная, существенная для функции, ею реализуемой, входит в формулу F ровно один раз. Скажем, что функция f *бесповторно выразима в базисе* $Б$, если существует бесповторная формула в базисе $Б$, реализующая функцию f. Функция f называется S*-функцией*, если f существенно зависит от всех своих переменных, f бесповторно не выразима в базисе $Б_0$, а любая функция, полученная из f подстановкой какой-либо константы вместо некоторой переменной, бесповторно выразима в $Б_0$.

Скажем, что функции f и g от n аргументов *обобщенно однотипны*, если существует такая перестановка $(i_1, \ldots, i_n)$ набора $(1, \ldots, n)$ и такие константы $c_0, c_1, \ldots, c_n$, что справедливо тождество:

$$f(x_1, \ldots, x_n) \equiv g(x_{i_1} \oplus c_1, \ldots, x_{i_n} \oplus c_n) \oplus c_0.$$

Отношение обобщенной однотипности является эквивалентностью.

Пусть f — функция n аргументов, $(i_1, \ldots, i_n)$ — перестановка набора $(1, \ldots, n)$, g — функция k аргументов и $0 \leqslant k \leqslant n$. Скажем, что множество переменных $\{x_{i_1}, \ldots, x_{i_k}\}$ функции f является g*-выделимым* (или *выделимым*) если существует такая функция h, что справедливо тождество:

$$f(x_1, \ldots, x_n) \equiv h(g(x_{i_1}, \ldots, x_{i_k}), x_{i_{k+1}}, \ldots, x_{i_n}).$$

Скажем, что функция f *разделима* если либо $\mathrm{nes}(f) < n$, либо существует такое выделимое множество Y переменных функции f, что $2 \leqslant |Y| \leqslant n-1$.

Обозначим через $[Б]$ множество всех функций, полученных из функций базиса $Б$ с помощью подстановки констант вместо некоторых переменных, удаления всех несущественных переменных, замены некоторых переменных их отрицаниями и (возможно) замены функции ее отрицанием. Базис $Б$ называется *нормальным*, если $[Б] = Б$. *Лексикографически минимальной* назовем функцию, набор значений которой лексикографически предшествует наборам значений всех других функций, обобщенно однотипных с ней. *Ядром базиса $Б$* (обозначение: $\mathrm{Ker}(Б)$) называется множество всех неразделимых лексикографически минимальных функций, входящих в множество $[Б]$. Например, $\mathrm{Ker}(Б_0) = \{0,\ x,\ xy\}$, $\mathrm{Ker}(P_2(2)) = \{0,\ x,\ xy,\ x \oplus y\}$. *Порядком базиса $Б$* (обозначение: $\mathrm{nes}(Б)$) называется наибольшее число существенных переменных у функций из базиса $Б$.

Подстановкой констант называется произвольное конечное множество пар $A = \{(x_{i_1}, c_1), \ldots, (x_{i_k}, c_k)\}$, где $x_{i_1}, \ldots, x_{i_k}$ — попарно различные переменные, $c_1, \ldots, c_k$ — константы из множества $\{0, 1\}$. Подстановку A также обозначим $\{x_{i_1} = c_1, \ldots, x_{i_k} = c_k\}$. Положим $V(A) = \{x_{i_1}, \ldots, x_{i_k}\}$, $|A| = k$. Пусть f — булева функция n аргументов, тогда через $f|_A$ обозначим функцию n аргументов, для которой выполнено тождество

$$f|_A(x_1, \ldots, x_n) \equiv f(x_1, \ldots, c_1, \ldots, c_k, \ldots, x_n),$$

где константы $c_1, \ldots, c_k$ стоят на местах переменных $x_{i_1}, \ldots, x_{i_k}$ соответственно. Функция $f|_A$ называется *подфункцией* функции f. Пусть F — формула, тогда через $F|_A$ обозначим формулу, полученную из F заменой всех вхождений переменных $x_{i_1}, \ldots, x_{i_k}$ на константы $c_1, \ldots, c_k$ соответственно.

В §2 дано определение степеней произвольной функции и доказаны их простейшие свойства. Пусть f — функция n аргументов, m — натуральное число. Индукцией по m определим *m-ю степень функции f*, которую будем обозначать $f^{(m)}$.

Базис индукции: $m = 1$. Положим $f^{(1)} = f$.

Индуктивный переход: $m \geqslant 2$ и функция $f^{(m-1)}$ уже определена. Если $n = 0$, то положим $f^{(m)} = f$. Если $n \geqslant 1$, то зададим функцию $f^{(m)}$ от n^m аргументов формулой

$$f(f^{(m-1)}(x_1, \dots , x_{n^{m-1}}), \dots , f^{(m-1)}(x_{n^{m-1}(n-1)+1}, \dots , x_{n^m})).$$

Функции $f^{(m)}$ рассматривала Б. А. Субботовская[13].

Пусть g — подфункция функции $f^{(m)}$, s — натуральное число, $s \leqslant m$. Множество переменных $V(g) \cap \{x_{n^s(i-1)+1}, \dots , x_{n^s i}\}$, $1 \leqslant i \leqslant n^{m-s}$, называется *$s$-множеством* (функции g); s-множество Z называется *регулярным*, если $|Z| = n^s$. Переменная x_j называется *s-регулярной переменной* функции g, если s-множество функции g, которому принадлежит переменная x_j, является регулярным. Количество s-регулярных переменных функции g обозначим через $R_s(g)$.

Лемма 1. Пусть f — функция n аргументов, $\mathrm{nes}(f) = n$, $n \geqslant 2$, m — натуральное число, $Y \subseteq V(f^{(m)})$ и

$$|Y| > (n-1)^m.$$

Тогда существует такая подфункция g функции $f^{(m)}$, что $V(g) \subseteq Y$ и функция, полученная из g удалением несущественных переменных, обобщенно однотипна с f.

Мерой устойчивости функции f (обозначение: $u(f)$) называется наименьшая из мощностей таких подстановок констант A, что $\mathrm{nes}(f|_A) = 0$.

Лемма 2. Для любой функции f и любого натурального числа m выполнено неравенство

$$u(f^{(m)}) \geqslant (u(f))^m.$$

[13] Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами // Докл. АН СССР. 1963. Т. 149, No 4. С. 784–787.

В §3 дано определение функции, p-универсальной для данного базиса $Б$ и, исходя из произвольной функции f, обладающей рядом свойств, связанных с базисом $Б$, построены p-универсальные функции для базиса $Б$ и любого числа p.

Скажем, что функция f *забивает* функцию g *подстановкой констант* A, если существует такая переменная x_i, что функции f, g и $f|_A$ существенно зависят от x_i, а функция $g|_A$ не зависит существенно от x_i.

Пусть $h_1, \dots , h_p$ — функции. Обозначим через $v(h_1, \dots , h_p)$ множество всевозможных наборов функций $(h_1|_B, \dots , h_p|_B)$, где B — подстановка констант и $V(B) = \bigcup\limits_{i=1}^{p} V(h_i)$. Скажем, что функции $h_1, \dots , h_p$ *независимы* (*в совокупности*), если

$$v(h_1, \dots , h_p) = v(h_1) \times \dots \times v(h_p).$$

Функция f называется *p-универсальной для базиса $Б$*, если $\mathrm{nes}(f) > 0$ и для любых функций $h_1, \dots , h_p$, бесповторно выразимых в $Б$, множества существенных переменных которых попарно не пересекаются и в объединении дают множество $V(f)$, выполнено хотя бы одно из двух:

1) либо функция f забивает какую-то из функций $h_1, \dots , h_p$ некоторой подстановкой констант;

2) либо функции f, $h_1, \dots , h_p$ независимы в совокупности.

Утверждение 1. Пусть $Б$ — произвольный базис. Если функция φ бесповторно не выразима в базисе $Б$, функция h бесповторно выразима в $Б$ и тождественно не равна константе, то

$$|v(\varphi, h)| \geqslant 3.$$

Лемма 3. Пусть $Б$ — произвольный базис, ψ — функция k аргументов, бесповторно не выразимая в $Б$, и $\mathrm{nes}(\psi) = k$. Тогда функция

$$\psi(x_1, \dots , x_k) \cdot x_{k+1} \vee x_{k+2}$$

является 1-универсальной для базиса $Б$.

Лемма 5. Пусть $Б$ — произвольный базис, φ — функция n аргументов, $\mathrm{nes}(\varphi) = n$, функция φ является 1-универсальной для базиса $Б$, $u = u(\varphi)$, $u \geqslant 2$, p — натуральное число и

$$m(p, \varphi) = \lfloor \log_{\left(\frac{n}{n-1}\right)} p \rfloor + \lfloor \log_u p \rfloor + 2.$$

Тогда функция $\varphi^{(m(p,\varphi))}$ является p-универсальной для базиса $Б$.

Во второй главе для каждой формулы введен класс ее μ_L^s-подформул; показано, что в подформулах из этого класса возможно производить ««забивание переменных»»; дана нижняя оценка мощности этого класса подформул исходя из свойств функции, реализуемой объемлющей формулой. Вторая глава состоит из параграфов 4–6.

В §4 дано определение приведенной формулы; показано что из любой формулы можно получить приведенную формулу, реализующую ту же функцию, не увеличивая сложность; введены класс ν-формул, его подклассы ν_L^s-формул и μ_L^s-формул, и исследованы их свойства.

Функция вида $x_{i_1} \oplus \ldots \oplus x_{i_k} \oplus c$ называется *линейной*. Обозначим через $\oplus_n$ функцию $x_1 \oplus \ldots \oplus x_n$. Базис $Б$ назовем *линейным*, если функция $\oplus_2$ бесповторно выразима в базисе $Б$. Скажем, что функция f *линейно зависит* от переменной x_i, если

$$f|_{\{x_i=0\}} \equiv f|_{\{x_i=1\}} \oplus 1.$$

Формула F называется *приведенной*, если выполнены условия:

a) либо F состоит из одного символа константы, либо ни одна подформула формулы F не реализует константу;

b) каждая функция, входящая в формулу F, существенно зависит от всех своих аргументов, и либо линейна, либо нелинейно зависит от всех своих аргументов;

c) ни одна подформула G формулы F не содержит вхождений переменных, несущественных для функции, реализуемой формулой G.

Утверждение 3. Пусть $Б$ — произвольный базис, F — формула в $Б$. Тогда существует приведенная формула F' в базисе $[Б]$, удовлетворяющая следующим свойствам: $F' \equiv F$; $\forall i\ L_{x_i}(F') \leqslant L_{x_i}(F)$.

Пусть $Б$ — произвольный базис, $p = \mathrm{nes}(Б)$. Скажем, что функция f *согласована* с базисом $Б$, если выполнены условия:

a) если базис $Б$ линеен, то функция f является p-универсальной для $Б$;

b) если базис $Б$ нелинеен, то $\mathrm{nes}(f) > 0$ и каждая существенная переменная функции f содержится в некотором $\oplus_p$-выделимом множестве переменных функции f.

Пусть F — формула вида $h(F_1, \ldots, F_n)$, где h — символ функции, $F_1, \ldots, F_n$ — формулы. Формула F называется *ν-формулой*, если не существует такой линейной функции Λ, что выполнено тождество

$$F \equiv \Lambda(F_1, \ldots, F_n).$$

Пусть f — функция, m, s — натуральные числа, $s \leqslant m$, g — подфункция функции $f^{(m)}$. Далее, пусть все переменные, входящие в F, существенны для функции g. Наконец, пусть L — целое неотрицательное число. Формула F называется *ν_L^s-формулой* (для функции g), если либо $L(F) \geqslant L$, либо хотя бы одна переменная, входящая в формулу F, не является s-регулярной для функции g.

Подформула F_i, $1 \leqslant i \leqslant n$, формулы F называется *ν_L^s-центральной*, если она не содержит подформул, являющихся ν_L^s-формулами. Формула F называется *μ_L^s-формулой*, если все формулы $F_1, \ldots, F_n$, за исключением, быть может, одной, являются ν_L^s-центральными. Переменная называется *ν_L^s-центральной* (для формулы F), если она входит хотя бы в одну ν_L^s-центральную подформулу формулы F.

Скажем, что функция f *забивает формулу* F *в базисе* $Б$ *подстановкой констант* A, если существует такая формула F' в базисе $Б$ и такая переменная z, что выполнены условия: $z \in V(f|_A)$; $F' \equiv F|_A$; $\forall i\ L_{x_i}(F') \leqslant L_{x_i}(F|_A)$; $L_z(F') < L_z(F|_A)$.

Лемма 8. Пусть $Б$ — нормальный базис, $p = \mathrm{nes}(Б)$, f — функция n аргументов, $\mathrm{nes}(f) = n$, f согласована с базисом $Б$, m, s — натуральные числа, $s \leqslant m$, g — подфункция функции $f^{(m)}$. Далее, пусть $L = np^2$, F — приведенная μ_L^s-формула в базисе $Б$, все переменные, входящие в F, существенны для g. Наконец, пусть Z — множество всех ν_L^s-центральных переменных формулы F и все переменные из множества Z являются s-регулярными для функции g. Тогда существует такая подстановка констант A, что $|A| \leqslant |Z| + np$, все переменные из множества $V(A)$ являются s-регулярными для g, и функция g забивает формулу F в базисе $Б$ подстановкой констант A.

В §5 введено понятие ранга функции и дана нижняя оценка количества ν-подформул данной формулы через ранг функции, ею реализуемой. *Рангом* функции f (обозначение: $r(f)$) называется наименьшее целое число r, для которого существует такая функция ψ и такие линейные функции $\Lambda_1, \ldots, \Lambda_r$, что выполнено тождество

$$f \equiv \psi(\Lambda_1, \ldots, \Lambda_r).$$

Лемма 9. Пусть k, n — неотрицательные целые числа, θ — функция $k + n$ аргументов, $\mathrm{nes}(\theta) = k + n$, φ — произвольная нелинейная функция двух аргументов и

$$g(x_1, \ldots, x_{2k+n}) \equiv \theta(\varphi(x_1, x_2), \ldots, \varphi(x_{2k-1}, x_{2k}), x_{2k+1}, \ldots, x_{2k+n}).$$

Тогда $r(g) \geqslant 2k$.

Лемма 10. Пусть f — нелинейная функция n аргументов, $\mathrm{nes}(f) = n$, m — натуральное число и g — подфункция функции $f^{(m)}$. Тогда

$$r(g) \geqslant \frac{2}{\mathrm{nes}(f)} R_1(g).$$

Пусть G — произвольная формула. Обозначим через $\nu(G)$ количество ν-формул среди подформул формулы G. Через $\mu_L^s(G)$ обозначим количество μ_L^s-формул среди подформул формулы G.

Лемма 11. Пусть формула G в базисе $Б$ реализует функцию g. Тогда

$$\nu(G) \geqslant \frac{1}{\mathrm{nes}(Б)}(r(g) - 1).$$

В §6, используя результаты §5, дана нижняя оценка количества μ_L^s-подформул данной формулы.

Пусть G — произвольная формула и P — произвольное подмножество множества подформул формулы G. Определим подмножество μP множества P следующим образом: пусть формула H, $H \in P$, имеет вид $H = h(H_1, \ldots, H_s)$, где h — символ функции и $H_1, \ldots, H_s$ — формулы; тогда H принадлежит множеству μP в том и только в том случае, когда никакая из формул $H_1, \ldots, H_s$, за исключением, быть может, одной, не содержит подформул, принадлежащих множеству P.

Лемма 12. Для любой формулы G и любого подмножества P множества подформул формулы G справедливо

$$|\mu P| \geqslant \frac{1}{2}|P|.$$

Лемма 13. Пусть $Б$ — произвольный базис, $p = \mathrm{nes}(Б)$, f — нелинейная функция n аргументов, $\mathrm{nes}(f) = n$; $m,\ s,\ L,\ k$ — натуральные числа, $s \leqslant m$, и

$$n^s \geqslant 2L^2 n^2 pk.$$

Далее, пусть g — подфункция функции $f^{(m)}$, G — формула в базисе $Б$, реализующая функцию g. Наконец, пусть каждая s-регулярная переменная функции g входит в формулу G не больше, чем k раз. Тогда

$$\mu_L^s(G) \geqslant \frac{1}{8L^2n^4p^2k} R_s(g).$$

В третьей главе, используя результаты первых двух глав, доказана нижняя оценка сложности для конкретных последовательностей функций. Третья глава состоит из параграфов 7 и 8. **В §7** доказана основная лемма, а **в §8**, используя результат основной леммы, доказаны теоремы 1 и 2, дающие нижнюю оценку.

Основная лемма. Пусть $Б$ — нормальный базис порядка p, f — функция n аргументов, $\operatorname{nes}(f) = n$, функция f нелинейна, согласована с базисом $Б$, $u = u(f)$ и $u \geqslant 2$. Далее, пусть m, s — натуральные числа, $s < m$ и

$$u^s \geqslant 99n^6p^6(M_Б(f^{(m)}))^2.$$

Тогда

$$M_Б(f^{(m-s)}) \leqslant M_Б(f^{(m)}) - \frac{1}{6n^s}.$$

Теорема 1. Пусть $Б$ — нормальный базис порядка p, f — функция n аргументов, $\operatorname{nes}(f) = n$, функция f нелинейна, согласована с базисом $Б$, $u = u(f)$ и $u \geqslant 2$. Тогда для любого натурального m, $m \geqslant n$, справедливо

$$M_Б(f^{(m)}) \geqslant C\left(\frac{m}{\log_n m}\right)^{\gamma},$$

где $C = \frac{1}{10n^3p^3\sqrt{u}}$, $\gamma = \frac{1}{1+2\log_u n}$.

Посредством $f(m) \succeq g(m)$ обозначим следующее условие: для некоторого числа C выполнено $\varlimsup\limits_{m\to\infty} g(m)/f(m) \leqslant C$; посредством $f(m) \asymp g(m)$ обозначим одновременную выполнимость условий $f(m) \succeq g(m)$ и $g(m) \succeq f(m)$.

Теорема 2. Пусть $Б_1$, $Б_2$ — произвольные базисы и пусть не все функции из базиса $Б_2$ бесповторно выразимы в $Б_1$. Тогда для любого числа ϵ, $\epsilon > 0$, существует такая функция f_ϵ, что

$$L_{Б_1}(f_\epsilon^{(m)}) \succeq N \cdot \sqrt[5+\epsilon]{\ln N}, \qquad \text{и} \qquad L_{Б_2}(f_\epsilon^{(m)}) \asymp N,$$

где $N = \mathrm{nes}(f_\epsilon^{(m)})$.

В четвертой главе, опираясь на нижнюю оценку, доказанную в третьей главе, получены результаты о сравнении базисов. Четвертая глава состоит из параграфов 9 и 10. **В §9** доказана основная теорема, дающая алгоритмический критерий сравнения произвольных базисов.

Основная теорема. Пусть $Б_1$ и $Б_2$ — произвольные базисы. Тогда равносильны следующие три условия[14]:

а) базис $Б_1$ предшествует базису $Б_2$,

б) все функции из базиса $Б_2$ бесповторно выразимы в $Б_1$,

в) $\mathrm{Ker}(Б_2) \subseteq \mathrm{Ker}(Б_1)$;

кроме того, равносильны условия г) и д):

г) базис $Б_1$ непосредственно предшествует базису $Б_2$,

д) $\mathrm{Ker}(Б_2) \subset \mathrm{Ker}(Б_1)$ и $|\,\mathrm{Ker}(Б_1) \setminus \mathrm{Ker}(Б_2)| = 1$.

В §10 из основной теоремы выведены теоремы 3–13, дающие качественные характеристики структуры отношения предшествования на множестве базисов.

Теорема 3. Для всякого натурального числа n, $n \geqslant 2$, базис $P_2(n+1)$ строго предшествует базису $P_2(n)$.

Теорема 4. Существует бесконечная последовательность базисов $Б_1$, $Б_2, \ldots$, в которой каждый базис $Б_{i+1}$, $i \in \mathbb{N}$, строго предшествует базису $Б_i$.

[14] импликация б) $\Rightarrow$ а) доказана О. Б. Лупановым, см. Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами // Докл. АН СССР. 1963. Т. 149, No 4. С. 784–787.

Теорема 5. Не существует такого базиса $Б^*$, который предшествует любому базису.

Теорема 6. Произвольный базис $Б$ является предмаксимальным тогда и только тогда, когда $Б$ эквивалентен базису вида $Б_0 \cup \{f\}$, где f — S-функция.

Теорема 7. а) Каждый предмаксимальный базис эквивалентен базису вида $Б_0 \cup \{f\}$, где f — одна из следующих функций:

$$\begin{gathered}
x_1 x_2 \cdot \ldots \cdot x_n \vee \bar{x}_1 \bar{x}_2 \cdot \ldots \cdot \bar{x}_n, \quad n \geqslant 2, \\
x_1(x_2 \vee \ldots \vee x_n) \vee x_2 \cdot \ldots \cdot x_n, \quad n \geqslant 3, \\
x_1(x_2 \vee x_3 \cdot \ldots \cdot x_n) \vee x_2 \bar{x}_3 \cdot \ldots \cdot \bar{x}_n, \quad n \geqslant 3, \\
x_1(x_2 \vee x_3) \vee x_3 x_4, \\
x_1(x_3 x_4 \vee x_5) \vee x_2(x_3 \vee x_4 x_5);
\end{gathered} \tag{1}$$

б) если f — функция из множества (1), то базис $Б_0 \cup \{f\}$ предмаксимален;

в) если f_1 и f_2 — различные функции их множества (1), то базисы $Б_0 \cup \{f_1\}$ и $Б_0 \cup \{f_2\}$ неэквивалентны.

Заметим, что множество (1) — это полная система различных представителей классов обобщенной однотипности S-функций. Множество (1) взято из работы В. А. Стеценко[15].

Теорема 8. Существует бесконечное множество попарно неэквивалентных предмаксимальных базисов.

Теорема 9. Существует бесконечное множество попарно несравнимых базисов.

Теорема 10. Каждый базис предшествует лишь конечному числу базисов с точностью до эквивалентности.

[15] Стеценко В. А. О предплохих базисах в P_2 // Математические вопросы кибернетики. Вып. 4. М.: Наука, 1992. С. 139–177.

Теорема 11. Не существует бесконечной последовательности базисов $Б_1,\ Б_2, \ldots$, в которой каждый базис $Б_i,\ i \in \mathbb{N}$, строго предшествует базису $Б_{i+1}$.

Теорема 12. Для произвольного базиса $Б$ существует бесконечное множество попарно неэквивалентных базисов, непосредственно предшествующих базису $Б$.

Теорема 13. Пусть $Б_1, \ldots, Б_n$ и $Б'_1, \ldots, Б'_m$ — две конечные последовательности базисов; $Б_1 = Б'_1$, $Б_n = Б'_m$; для любого $i,\ 1 \leqslant i \leqslant n-1$, базис $Б_{i+1}$ непосредственно предшествует базису $Б_i$, и для любого $j,\ 1 \leqslant j \leqslant m-1$, базис $Б'_{j+1}$ непосредственно предшествует базису $Б'_j$. Тогда $n = m$.

Пользуясь случаем, автор выражает благодарность научному руководителю чл.-корр. РАН О. Б. Лупанову за неоценимую поддержку на всех этапах подготовки диссертации.

РАБОТЫ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Черухин Д. Ю.** Об одной бесконечной цепочке улучшающихся булевых базисов. Препринт механико-математического факультета МГУ. 1997. No 7. 16 с.

2. **Черухин Д. Ю.** Об одной бесконечной последовательности улучшающихся булевых базисов // Дискретный анализ и исследование операций. 1997. Т. 4, No 4. С. 79–95.

3. **Черухин Д. Ю.** Алгоритм сравнения булевых базисов // Проблемы теоретической кибернетики. Тезисы докладов XII Международной конференции. Часть II. / Под ред. О. Б. Лупанова. М.: Изд-во механико-математического ф-та МГУ, 1999. С. 249.

4. **Черухин Д. Ю.** О предплохих булевых базисах // Дискретная математика. 1999. Т. 11, вып. 2. С. 118–160.

5. **Черухин Д. Ю.** О сравнении булевых базисов // Докл. РАН. 1999. Т. 367, No 6. С. 742–743.

6. **Черухин Д. Ю.** О булевых базисах, непосредственно предшествующих базису $\{\&, \ \vee, \ \neg\}$. // Докл. РАН. 1999. Т. 369, No 5. С. 605–606.

7. **Черухин Д. Ю.** Алгоритмический критерий сравнения булевых базисов // Математические вопросы кибернетики. Вып. 8. М.: Наука, 1999. С. 77–122.