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

Диссертация на соискание ученой степени
кандидата физико-математических наук

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

МОСКВА 2000

Typeset by $\mathcal{AMS}$-TEX

ОГЛАВЛЕНИЕ

Введение 3

Глава I. Свойства функций специального вида 10

§1. Основные понятия 10

§2. Степени функций 17

§3. Функции, p-универсальные для данного базиса 20

Глава II. Свойства формул специального вида 35

§4. Техника забивания μ_L^s-формул 35

§5. Ранг функции 50

§6. Оценка количества μ_L^s-подформул 56

Глава III. Нижние оценки сложности функций 63

§7. Основная лемма 63

§8. Оценка сложности степеней некоторых функций 71

Глава IV. Сравнение булевых базисов 78

§9. Критерий сравнения произвольных базисов 78

§10. Исследование структуры базисов 81

Литература 88

ВВЕДЕНИЕ

Результаты диссертации относятся к математической теории синтеза и сложности управляющих систем [20, 4]. Предметом исследования являются формулы в полных конечных булевых базисах [21, 2]. В диссертации изучается зависимость сложности булевых функций в классе формул от функционального базиса [3, 7].

О. Б. Лупанов показал [2, 4], что сложность почти всех булевых функций асимптотически не зависит от базиса. В то же время, существует последовательность булевых функций, сложность которой в одном базисе по порядку больше, нежели в другом базисе. Например, сложность последовательности линейных функций $x_1 \oplus \ldots \oplus x_n$ в базисе $\{\&, \vee, \neg, \oplus\}$ равна n. В то же время, как показала Б. А. Субботовская [11], сложность этой последовательности в базисе $\{\&, \vee, \neg\}$ по порядку не меньше, чем $n^{3/2}$.

В связи с результатом Б. А. Субботовской [11], О. Б. Лупанов предложил ввести следующее отношение предшествования на множестве базисов, характеризующее сложность отдельных последовательностей функций: базис $Б_1$ предшествует базису $Б_2$, если существуют такие действительные константы C и D, что для любой булевой функции f выполнено неравенство $L_{Б_1}(f) \leqslant CL_{Б_2}(f) + D$, где $L_Б(f)$ — сложность функции f в базисе $Б$. Отношение предшествования естественно порождает отношения эквивалентности, строгого предшествования, несравнимости и непосредственного предшествования на множестве базисов.

Отношение предшествования впервые было введено и исследовано в работе Б. А. Субботовской [12]. О. Б. Лупанов дал (см. [12]) следующий признак выполнимости отношения предшествования для произвольных базисов $Б_1$ и $Б_2$: если все функции из базиса $Б_2$ бесповторно выразимы [12] в базисе $Б_1$, то базис $Б_1$ предшествует базису $Б_2$. С помощью этого признака О. Б. Лупанов показал (см. [12]), что любой базис предшествует базису $Б_0$, $Б_0 = \{\&, \vee, \neg\}$, т. е. базис $Б_0$ является максимальным.

Б. А. Субботовская привела [12] пример базиса, строго предшествующего базису $Б_0$. Исходя из результатов работы [11], она показала, что базис $Б_0 \cup \{\oplus\}$ строго предшествует базису $Б_0$. Б. А. Субботовская дала [12] критерий эквивалентности произвольного базиса $Б$ базису $Б_0$. Она показала, что базис $Б$ эквивалентен базису $Б_0$ тогда и только тогда, когда все функции из базиса $Б$ бесповторно выразимы в базисе $Б_0$. Тем самым Б. А. Субботовская описала класс базисов, строго предшествующих базису $Б_0$.

Далее, Б. А. Мучник (Субботовская) для произвольных базисов $Б_1$ и $Б_2$ показала [5], что базис $Б_1$ предшествует базису $Б_2$ тогда и только тогда, когда сложность одной конкретной последовательности функций $f_1, f_2, \ldots$ (определяемой базисами $Б_1$ и $Б_2$) в базисе $Б_2$ по порядку не меньше ее сложности в базисе $Б_1$. Тем самым Б. А. Мучник свела задачу сравнения двух произвольных базисов к сравнению сложностей одной бесконечной последовательности булевых функций в этих базисах. Вопрос о существовании алгоритма сравнения произвольных базисов остался открытым.

Следующий результат также принадлежит Б. А. Мучник. Она рассмотрела [6] сложность линейных функций в ««нелинейных»» [6] базисах. Б. А. Мучник показала [6], что сложность линейной функции $x_1 \oplus \ldots \oplus x_n$ в произвольном ««нелинейном»» базисе по порядку не меньше, чем n^{1+c}, где c — действительная положительная константа, зависящая только от базиса. Тем самым было показано, что если $Б$ — произвольный ««нелинейный»» базис, а $Б'$ — произвольный ««линейный»» базис, то базис $Б'$ не предшествует базису $Б$, и базис $Б$ строго предшествует базису $Б \cup Б'$.

Примером ««нелинейного»» базиса является базис $Б_0 \cup \{xy \vee xz \vee yz\}$, примером линейного базиса — базис $Б_0 \cup \{\oplus\}$. В силу результатов работы [6], базис $Б_0 \cup \{\oplus, xy \vee xz \vee yz\}$ строго предшествует базису $Б_0 \cup \{xy \vee xz \vee yz\}$. Последний базис, в силу результатов работы [12], строго предшествует базису $Б_0$. Таким образом, используя результаты Б. А. Мучник [6, 12], можно построить последовательность из трех базисов, каждый следующий из которых строго предшествует предыдущему. Вопрос о существовании последовательности большей длины, удовлетворяющей этому условию, остался открытым.

Исследование задачи сравнения полных базисов продолжил В. А. Стеценко. Он рассмотрел [10] класс предмаксимальных базисов, т. е. базисов, непосредственно предшествующих максимальному базису $Б_0$. В. А. Стеценко показал, что каждый предмаксимальный базис эквивалентен базису вида $Б_0 \cup \{f\}$, где f — S-функция [10]. Он также полностью описал [10] множество S-функций. Тем самым В. А. Стеценко дал необходимое условие того, что данный базис является предмаксимальным. Вопрос о существовании предмаксимальных базисов остался открытым.

Ряд результатов получил Н. А. Перязев. В частности, он распространил [8] результат Б. А. Мучник [6] на класс ««монолинейных»» базисов [8], показав тем самым, что никакой ««немонолинейный»» базис не предшествует никакому ««монолинейному»» базису. Затем он получил [9] результат, аналогичный результату В. А. Стеценко [10], классифицировав все функции, ««слабоповторные»» [9] в базисе, состоящем из всех двуместных функций.

Отметим, что при перечислении результатов предшественников мы ограничились результатами о сравнении полных конечных булевых базисов.

В диссертации получены следующие результаты. Автор доказал [13, 14, 17], что существует бесконечная последовательность базисов, каждый следующий член которой строго предшествует предыдущему. Примером такой последовательности является последовательность $P_2(2), P_2(3), \ldots$, где $P_2(n)$ — множество всех n-местных булевых функций. Из данного результата следует, что не существует минимального базиса, т. е. такого базиса, который предшествует любому базису.

Далее, автор доказал [16, 17, 18] существование предмаксимальных базисов. Как было показано в [16], базис $Б$ предмаксимален тогда и только тогда, когда $Б$ эквивалентен базису вида $Б_0 \cup \{f\}$, где f — S-функция. Таким образом, необходимое условие, данное В. А. Стеценко, является также достаточным. На основании списка S-функций, данного В. А. Стеценко, автор классифицировал [16] все предмаксимальные базисы с точностью до эквивалентности. Автор также доказал [16] существование бесконечного множества попарно несравнимых булевых базисов. Примером такого множества является множество $\{Б_0 \cup \{f\} : f \in T\}$, где T — множество представителей всех классов S-функций по отношению обобщенной однотипности [10].

Наконец, автор доказал [17, 19] следующий критерий сравнения произвольных базисов $Б_1$ и $Б_2$: базис $Б_1$ предшествует базису $Б_2$ тогда и только тогда, когда все функции из базиса $Б_2$ бесповторно выразимы в базисе $Б_1$. Тем самым, достаточный признак сравнения базисов, данный О. Б. Лупановым (см. [12]), является также необходимым. Автор ввел понятие ядра базиса [19]. Ядро базиса является конечным множеством функций, эффективно вычислимым исходя из базиса. Автор доказал, что для произвольных базисов $Б_1$ и $Б_2$ справедлив следующий критерий: базис $Б_1$ предшествует базису $Б_2$ тогда и только тогда, когда ядро базиса $Б_2$ является подмножеством ядра базиса $Б_1$. Тем самым автор доказал [19] алгоритмическую разрешимость задачи сравнения произвольных базисов. Используя понятие ядра базиса, автор дал [19] следующий критерий непосредственного предшествования одного базиса другому: базис $Б_1$ непосредственно предшествует базису $Б_2$ тогда и только тогда, когда ядро базиса $Б_2$ является строгим подмножеством ядра базиса $Б_1$ и отличается от него ровно на одну функцию.

Критерии сравнения базисов, доказанные в [19], позволяют выявить некоторые факты о структуре отношения предшествования на множестве базисов. Например, можно показать, что каждый базис предшествует лишь конечному числу классов эквивалентности базисов. Таким образом, не существует бесконечной последовательности базисов, каждый член которой строго предшествует следующему. Далее, для каждого базиса существует бесконечное число попарно не эквивалентных базисов, непосредственно ему предшествующих. Наконец, если рассмотреть две произвольные цепи базисов, у которых совпадают начала и концы, и в которых каждый следующий член строго предшествует предыдущему, то длины этих цепей совпадут. Последний факт позволяет все базисы распределить по ярусам. На нулевом ярусе находится класс эквивалентности базиса $Б_0$, на первом ярусе — классы эквивалентности предмаксимальных базисов, на втором ярусе — классы эквивалентности базисов, непосредственно предшествующих предмаксимальным и т. д.

Основным результатом диссертации является критерий сравнения произвольных базисов (см. основную теорему в §9 главы IV). С помощью этого критерия доказаны все остальные вышеописанные результаты о сравнении базисов, полученные автором (см. теоремы 3–13 в §10 главы IV). Основная теорема опирается на нижние оценки сложности индивидуальных последовательностей функций в различных базисах (см. основную лемму в § 7 и теоремы 1, 2 в § 8 главы III). Результаты главы III, в свою очередь, опираются на результаты глав I и II. Результаты глав I и II носят вспомогательный характер.

Глава I посвящена построению и исследованию свойств последовательности функций, для которой в главе III будет доказана нижняя оценка сложности. В § 1 мы введем основные понятия и обозначения, используемые в диссертации. В § 2 для каждой функции f мы введем последовательность функций $f^{(m)}$ и докажем несколько ее свойств. В § 3 мы введем понятие p-универсальной функции для данного базиса $Б$ (здесь p — натуральный параметр) и построим p-универсальные функции для каждого базиса $Б$ и числа p. В частности мы докажем, что при некоторых условиях, накладываемых на функцию f, и числа m и p, функция $f^{(m)}$ является p-универсальной для данного базиса $Б$.

Глава II посвящена исследованию некоторых классов подформул заданной формулы, за счет которых возможно уменьшение сложности формулы при специально выбранной подстановке констант. В § 4 мы введем класс ν-формул и его подклассы μ_L^s-формул (L, s — параметры). Мы покажем, что при некотором условии, накладываемом на функцию f и μ_L^s-формулу F (связанном с p-универсальностью), существует подстановка констант A и переменная x_i такие, что функция $f|_A$ (полученная в результате действия подстановки констант A на функцию f) существенно зависит от x_i, а формула $F|_A$ (полученная в результате действия подстановки констант A на формулу F) допускает упрощение хотя бы на одно вхождение переменной x_i (другими словами, функция f забивает формулу F). В § 5 мы введем одни важный параметр функции ее ранг, и покажем связь ранга функции с количеством ν-подформул в произвольной формуле, реализующей данную функцию. В § 6, используя результаты § 5, мы оценим снизу количество μ_L^s-формул среди подформул данной формулы F.

Глава III посвящена получению нелинейных нижних оценок сложности эффективно заданных последовательностей функций. В § 7 мы докажем основную лемму, сводящую, при некоторых предположениях, сложность функции $f^{(m)}$ к сложности функции $f^{(m')}$ для некоторого $m' < m$. В § 8, опираясь на основную лемму, мы покажем, что при некотором условии, накладываемом на функцию f и базис $Б$ (связанном с p-универсальностью), последовательность $f^{(m)}$ имеет нелинейную сложность при реализации формулами в базисе $Б$.

Наконец, в главе IV мы докажем основную теорему (§9) и в качестве следствий из нее получим другие результаты о сравнении базисов (§10).

Пользуясь случаем, автор выражает глубокую благодарность своему научному руководителю чл.-корр. РАН О. Б. Лупанову за постановку задачи и всемерную поддержку в процессе ее решения.

ГЛАВА I. СВОЙСТВА ФУНКЦИЙ СПЕЦИАЛЬНОГО ВИДА

§1. Основные понятия.

Введем основные понятия и обозначения, используемые в диссертации. Произвольная функция $f : \{0,1\}^n \to \{0,1\}$ [константа 0 или 1 при $n = 0$] называется (*n-местной*) *булевой функцией* (иногда слово ««булева»» мы будем опускать). Множество всех булевых функций n аргументов обозначим $P_2(n)$. Булева функция однозначно определяется *набором* своих *значений*

$$(f(0,\dots,0,0),\ f(0,\dots,0,1),\dots,f(1,\dots,1,1)).$$

Зададим некоторые булевы функции наборами их значений. Отрицание ($\neg$) задается набором $(1,0)$, конъюнкция ($\&$) — набором $(0,0,0,1)$, дизъюнкция ($\vee$) — набором $(0,1,1,1)$, сумма по модулю два ($\oplus$) — набором $(0,1,1,0)$. Пусть f и g — булевы функции n аргументов, $(f_1,\dots,f_{2^n})$ и $(g_1,\dots,g_{2^n})$ соответственно — наборы их значений. Скажем, что функция f *лексикографически предшествует* функции g, если существует такое число k, $1 \leqslant k \leqslant 2^n$, что $f_i = g_i$ для всех i, $1 \leqslant i < k$, и $f_k < g_k$.

Обозначим через X счетное множество переменных $\{x_1, x_2, \dots\}$. Скажем, что функция f *существенно* зависит от переменной x_i, $1 \leqslant i \leqslant n$, если существуют такие константы $\sigma_1,\dots,\sigma_{i-1},\sigma_{i+1},\dots,\sigma_n$, что

$$f(\sigma_1,\dots,\sigma_{i-1},0,\sigma_{i+1},\dots,\sigma_n) \neq f(\sigma_1,\dots,\sigma_{i-1},1,\sigma_{i+1},\dots,\sigma_n).$$

Множество всех существенных переменных функции f обозначим $V(f)$. Положим $\mathrm{nes}(f) = |V(f)|$. Пусть $V(f) = \{x_{i_1}, x_{i_2},\dots,x_{i_k}\}$, $i_1 < i_2 < \dots < i_k$. Тогда через $\langle f\rangle$

обозначим булеву функцию k аргументов, принимающую на произвольном наборе $(\sigma_1, \dots, \sigma_k)$ значение

$$f(0, \dots, 0, \sigma_1, 0, \dots, 0, \sigma_2, 0, \ \dots \ , 0, \sigma_k, 0, \dots, 0),$$

где константы $\sigma_1, \dots, \sigma_k$ стоят в i_1-й, ..., i_k-й позициях соответственно.

Пусть M — произвольное множество булевых функций. Определим по индукции множество *формул над* M, а также множество *подформул* каждой формулы.

Базис индукции. Пусть f — n-местная функция, $f \in M$. Тогда выражение $f(x_1, \dots, x_n)$ при $n \geqslant 1$ [выражение f при $n = 0$] является формулой над M. Формула $f(x_1, \dots, x_n)$ [f] является единственной своей подформулой.

Индуктивный переход. Пусть f — n-местная функция, $n \geqslant 1$, $f \in M$, каждое из выражений $F_1, \dots, F_n$ является либо ранее построенной формулой над M, либо переменной из множества X. Тогда выражение $f(F_1, \dots, F_n)$ является формулой над M. Подформулами формулы $f(F_1, \dots, F_n)$ являются формула $f(F_1, \dots, F_n)$ и подформулы тех из выражений $F_1, \dots, F_n$, которые являются формулами.

Формулой будем называть формулу над множеством всех булевых функций. Пусть F, G — формулы. Посредством $F \circeq G$ будем обозначать графическое равенство формул F и G (т. е. совпадение их как выражений). Условимся, что запись вида $F \circeq f(F_1, \dots, F_n)$ также обозначает, что f является функцией, а каждое из выражений $F_1, \dots, F_n$ — либо формулой, либо переменной. Пусть каждое из выражений F_1, F_2 — либо формула, либо переменная. Тогда формулы $\neg(F_1)$, $\&(F_1, F_2)$, $\vee(F_1, F_2)$, $\oplus(F_1, F_2)$ также будем обозначать $\bar{F}_1$, $F_1 \& F_2$ (или $F_1 \cdot F_2$ или $F_1 F_2$), $F_1 \vee F_2$ и $F_1 \oplus F_2$ соответственно (считаем, что вначале выполняется операция $\&$, затем $\vee$ и, наконец, $\oplus$). Если $F \circeq f(x_1, \dots, x_n)$, то формулу F иногда будем обозначать символом f (опуская при этом стандартный набор переменных $(x_1, \ldots, x_n)$).

Если $F \circeq f(F_1, \ldots, F_n)$, то функцию f назовем *внешней функцией* формулы F, а выражения $F_1, \ldots, F_n$ назовем *субформулами* формулы F. Если $F \circeq c$, $c \in \{0, 1\}$, то внешней функцией формулы F назовем константу c. В этом случае формула F не имеет субформул. Пусть F — произвольная формула, $x_i \in X$, $Y \subseteq X$. Обозначим через $L_{x_i}(F)$ число вхождений в формулу F переменной x_i. Через $L_Y(F)$ обозначим суммарное число вхождений в формулу F всех переменных из множества Y. Положим $L(F) = L_X(F)$. Число $L(F)$ называется *сложностью* формулы F. Множество всех переменных, входящих в формулу F, обозначим $V(F)$.

Пусть x_j — переменная. Условимся, что множество подформул выражения x_j пусто. Положим $L_{x_i}(x_j) = 1$, если $i = j$, $L_{x_i}(x_j) = 0$, если $i \neq j$. Далее, $L_Y(x_j) = 1$, если $x_j \in Y$, $L_Y(x_j) = 0$, если $x_j \notin Y$. Наконец, $L(x_j) = 1$, $V(x_j) = \{x_j\}$.

Подстановкой констант называется произвольное конечное множество пар $\{(x_{i_1}, c_1), \ldots, (x_{i_n}, c_n)\}$, где $x_{i_1}, \ldots, x_{i_n}$ — попарно различные переменные, $c_1, \ldots, c_n$ — константы из множества $\{0, 1\}$ (подстановка может быть пустой). Подстановку констант $\{(x_{i_1}, c_1), \ldots, (x_{i_n}, c_n)\}$, где $i_1, \ldots, i_n$ попарно различны, также будем обозначать $\{x_{i_1} = c_1, \ldots, x_{i_n} = c_n\}$. Пусть $\{x_j = c\}$ — подстановка констант мощности 1, выражение F является либо формулой, либо переменной, и f — функция k аргументов. Обозначим через $F|_{\{x_j = c\}}$ выражение, полученное из F заменой каждого вхождения переменной x_j на константу c. Определим функцию $f|_{\{x_j = c\}}$ от k аргументов. Если $j > k$, то положим $f|_{\{x_j = c\}} = f$, а если $1 \leqslant j \leqslant k$, то значение функции $f|_{\{x_j = c\}}$ на произвольном наборе $(\sigma_1, \ldots, \sigma_k)$ положим равным

$$f(\sigma_1, \ldots, \sigma_{j-1}, c, \sigma_{j+1}, \ldots, \sigma_k).$$

Пусть теперь A — произвольная подстановка констант, $A = \{x_{i_1} = c_1, \ldots, x_{i_n} = c_n\}$. Положим

$$F|_A = (\ldots(F|_{\{x_{i_1}=c_1\}})\ldots)|_{\{x_{i_n}=c_n\}}, \qquad f|_A = (\ldots(f|_{\{x_{i_1}=c_1\}})\ldots)|_{\{x_{i_n}=c_n\}}$$

(если $A = \varnothing$, то $F|_A = F$, $f|_A = f$). Функция $f|_A$ называется *подфункцией* функции f. Если при этом $A \neq \varnothing$, то подфункция $f|_A$ называется *собственной.* Обозначим через $V(A)$ множество $\{x_{i_1}, \ldots, x_{i_n}\}$. Пусть $Y \subseteq X$. *Ограничением* подстановки констант A на множество Y называется подмножество множества A, состоящее из тех и только тех пар (x_j, c), для которых $x_j \in Y$.

Пусть F — формула сложности нуль. Тогда F не содержит переменных. Определим *значение* формулы F индукцией по числу вхождений функций в F.

Базис индукции: формула F содержит одно вхождение функции. В этом случае $F \overset{\circ}{=} c$, $c \in \{0, 1\}$. Значением формулы F является константа c.

Индуктивный переход: формула F содержит не меньше двух вхождений функций. Тогда $F \overset{\circ}{=} f(F_1, \ldots, F_n)$, где $F_1, \ldots, F_n$ — формулы сложности нуль и их значения уже определены. Пусть $c_1, \ldots, c_n$ — значения формул $F_1, \ldots, F_n$ соответственно. Значением формулы F является константа $f(c_1, \ldots, c_n)$.

Пусть F и G — произвольные формулы или переменные. Если A — подстановка констант и $V(A) \supseteq V(F)$, то формула $F|_A$ не содержит переменных и ее значение определено. Скажем, что выражения F и G *тождественно равны*, если для любой такой подстановки констант A, что $V(A) = V(F) \cup V(G)$, значения формул $F|_A$ и $G|_A$ равны. Тождественное равенство выражений F и G обозначим через $F \equiv G$. Пусть f — функция n аргументов. Скажем, что выражение F *реализует* функцию f, если выражения F и $f(x_1, \ldots, x_n)$ [f при $n = 0$] тождественно равны (функция, реализуемая выражением, определена, вообще говоря, не однозначно). Пусть g — функция k аргументов. Скажем, что функции f и g *тождественно равны*, если формулы $f(x_1, \ldots, x_n)$ [f при $n = 0$] и $g(x_1, \ldots, x_k)$ [g при $k = 0$] тождественно равны. Тождественное равенство функций f и g обозначим $f \equiv g$.

Пусть f — функция n аргументов, $\{1, \ldots, n\} = \{i_1, \ldots, i_n\}$, 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*, если существует такая функция h, что справедливо тождество:

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

В этом случае также скажем, что множество переменных $\{x_{i_1}, \ldots, x_{i_k}\}$ функции f *выделимо* [1]. Скажем, что функция f от n аргументов *разделима* (*разложима*) [1] если либо $\mathrm{nes}(f) < n$, либо существует выделимое множество переменных функции f, мощность которого не меньше двух и не больше, чем $n - 1$.

Пусть f и g — функции от n аргументов. Скажем, что функции f и g *обобщенно однотипны* [10], если существует такая перестановка $(i_1, \ldots, i_n)$ набора $(1, \ldots, n)$ (т. е. выполнено $\{i_1, \ldots, i_n\} = \{1, \ldots, n\}$) 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 $Б$ — конечное множество булевых функций. Множество $Б$ называется *базисом*, если любую булеву функцию можно реализовать формулой над $Б$. Примером базиса является $Б_0 = \{\&, \vee, \neg\}$. *Нормальным замыканием* базиса $Б$ называется множество всевозможных функций $\langle f|_A \rangle$, где $f \in Б$, A — подстановка констант. Нормальное замыкание базиса $Б$ обозначим через $[Б]$. Очевидно, что множество $[Б]$ является базисом. Базис $Б$ называется *нормальным*, если $[Б] = Б$. Очевидно, что $[[Б]] = [Б]$, т. е. базис $[Б]$ нормален. *Порядком базиса* $Б$ назовем наибольшее число аргументов у функций из базиса $Б$. Порядок базиса $Б$ обозначим через $\mathrm{nes}(Б)$.

Определим *ядро базиса* $Б$. Пусть f — произвольная неразложимая функция из множества $[Б]$. Обозначим через $\hat{f}$ ту функцию, обобщенно однотипную с функцией f, которая лексикографически предшествует всем другим функциям, обобщенно однотипным с f (функция $\hat{f}$ существует и единственна). Функцию $\hat{f}$ назовем лексикографически минимальной. Ядром базиса $Б$ называется множество всех таких функций $\hat{f}$, что f неразложима и $f \in [Б]$. Ядро базиса $Б$ обозначим $\mathrm{Ker}(Б)$.

Формулы над множеством $Б$ также будем называть формулами *в базисе* $Б$. Пусть f — произвольная булева функция. *Сложностью функции* f *в базисе* $Б$ называется наименьшая сложность, которую может иметь формула в базисе $Б$, реализующая функцию f. Сложность функции f в базисе $Б$ обозначим через $L_Б(f)$. Положим $M_Б(f) = \frac{L_Б(f)}{\mathrm{nes}(f)}$ (если $\mathrm{nes}(f) \neq 0$). Скажем, что базис $Б_1$ *предшествует* базису $Б_2$ [12] (обозначение: $Б_1 \preccurlyeq Б_2$), если существуют такие числа C и D, что для любой булевой функции f выполнено $L_{Б_1}(f) \leqslant CL_{Б_2}(f) + D$. 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 $Б_2 \not\preccurlyeq Б_1$. Наконец, 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* (см. [10]), если $Б$ непосредственно предшествует базису $Б_0$.

Пусть формула F реализует функцию f. Формула F называется *бесповторной*, если каждая переменная, существенная для функции f, входит в формулу F ровно один раз. Несложно показать, что если функции f и g реализуются формулой F, то $V(f) = V(g)$. Таким образом, определение бесповторной формулы корректно. Скажем, что функция f *бесповторно реализуется (выражается) через множество функций* M [*в базисе* $Б$], если существует бесповторная формула над множеством M [в базисе $Б$], которая реализует функцию f. Функция f называется S-функцией [10], если f существенно зависит от всех своих переменных, f бесповторно не выразима в базисе $Б_0$, а любая подфункция функции f, отличная от f, бесповторно выразима в $Б_0$.

В. А. Стеценко классифицировал [10] S-функции с точностью до отношения обобщенной однотипности. Он доказал [10], что любая S-функция обобщенно однотипна одной из следующих функций:

$$\begin{gathered}
x_1x_2\cdot\ldots\cdot x_n \vee \bar{x}_1\bar{x}_2\cdot\ldots\cdot\bar{x}_n, \quad n \geqslant 2,\\
x_1(x_2\vee\ldots\vee x_n)\vee x_2\cdot\ldots\cdot x_n, \quad n \geqslant 3,\\
x_1(x_2\vee x_3\cdot\ldots\cdot x_n)\vee x_2\bar{x}_3\cdot\ldots\cdot\bar{x}_n, \quad n \geqslant 3, \qquad (1)\\
x_1(x_2\vee x_3)\vee x_3x_4,\\
x_1(x_3x_4\vee x_5)\vee x_2(x_3\vee x_4x_5);
\end{gathered}$$

и функции из множества (1) попарно не обобщенно однотипны.

Все остальные понятия и обозначения будем вводить по мере необходимости.

§2. Степени функций и их 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 [12].

Пусть g — подфункция функции $f^{(m)}$, s — натуральное число, $s \leqslant m$. Множество переменных Z называется *s-множеством* функции g, если существует такое натуральное число i, $i \leqslant n^{m-s}$, что $Z = V(g) \cap \{x_{n^s(i-1)+1}, \dots, x_{n^s i}\}$. Множество Z, являющееся s-множеством функции g, 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 $R_s(g)$.

Пусть t — целое число, $0 \leqslant t \leqslant n^{m-s}$. Функция g называется *(s,t)-подфункцией* функции $f^{(m)}$, если каждое s-множество функции g либо имеет мощность 1, либо регулярно, причем количество s-множеств, имеющих мощность 1, равно t. Пусть $Y \subseteq V(g)$. Множество Y называется *s-специальным множеством* функции g, если для каждого s-множества Z функции g мощность пересечения $Y \cap Z$ равна 1.

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

$$|Y| > (n-1)^m. \tag{2}$$

Тогда существует такая подфункция g функции $f^{(m)}$, что $V(g) \subseteq Y$ и функция $\langle g \rangle$ обобщенно однотипна с f.

Доказательство. Проведем индукцию по m.

Базис индукции: $m = 1$. В этом случае из (2) следует, что $|Y| = n$, а значит, $Y = V(f^{(1)})$. Положив $g = f^{(1)}$, получим требуемое.

Индуктивный переход: $m \geqslant 2$, и для всех m', $m' < m$, лемма доказана.

Представим функцию $f^{(m)}$ в виде

$$f^{(m)} \equiv f(f_1, \dots, f_n),$$
$$\text{где} \quad f_i \equiv f^{(m-1)}(x_{n^{m-1}(i-1)+1}, \dots, x_{n^{m-1}i}), \quad 1 \leqslant i \leqslant n.$$

Обозначим

$$Y_i = Y \cap V(f_i), \;\; 1 \leqslant i \leqslant n.$$

Рассмотрим два случая: 1) для любого i, $1 \leqslant i \leqslant n$, множество Y_i непусто; 2) среди множеств Y_i, $1 \leqslant i \leqslant n$, хотя бы одно пусто.

Случай 1). Рассмотрим произвольное i, $1 \leqslant i \leqslant n$. Выберем число $w(i)$ так, чтобы $x_{w(i)} \in Y_i$. Существует подстановка констант A_i, $V(A_i) = V(f_i) \backslash \{x_{w(i)}\}$, и существует такая константа σ_i, что $f_i|_{A_i} \equiv x_{w(i)} \oplus \sigma_i$. Положим

$$A = \bigcup_{i=1}^{n} A_i, \qquad g = f|_A.$$

Тогда $g \equiv f(x_{w(1)} \oplus \sigma_1, \dots, x_{w(n)} \oplus \sigma_n)$, следовательно, $V(g) = \{x_{w(1)}, \dots, x_{w(n)}\} \subseteq Y$ и функция $\langle g \rangle$ обобщенно однотипна с f. Случай 1) рассмотрен.

Случай 2). Не ограничивая общность, будем считать, что $Y_1 = \varnothing$. Тогда, в силу (2), мощность хотя бы одного из множеств $Y_2, \dots, Y_n$ больше, чем $(n-1)^{m-1}$. Не ограничивая общность, будем считать, что $|Y_n| > (n-1)^{m-1}$. В силу существенной зависимости функции f от n-го аргумента, существует такая константа σ, что функция $f_n \oplus \sigma$ является подфункцией функции $f^{(m)}$. Функция $f^{(m-1)}$

может быть получена из f_n биективной заменой переменных. Кроме того, $Y_n \subseteq V(f_n)$ и $|Y_n| > (n-1)^{m-1}$. Поэтому, в силу предположения индукции для функции $f^{(m-1)}$, существует такая подфункция g' функции f_n, что $V(g') \subseteq Y_n$ и функция $\langle g' \rangle$ обобщенно однотипна с f. Пусть $g = g' \oplus \sigma$. Тогда функция g является подфункцией функции $f^{(m)}$, $V(g) \subseteq Y_n \subseteq Y$, и функция $\langle g \rangle$ обобщенно однотипна с f. Случай 2) рассмотрен.

Лемма 1 доказана.

Пусть f — произвольная функция. *Мерой устойчивости* функции f (обозначение: $u(f)$) называется наименьшая из мощностей таких подстановок констант A, для которых выполнено $V(f|_A) = \varnothing$.

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

$$u(f^{(m)}) \geqslant (u(f))^m. \tag{3}$$

Доказательство. Пусть n — число аргументов функции f. Если $n = 0$, то (3) выполнено. Пусть теперь $n \geqslant 1$. Проведем индукцию по m.

Базис индукции: $m = 1$. Имеем $u(f^{(1)}) = u(f) = (u(f))^1$, т. е. (3) выполнено.

Индуктивный переход: $m \geqslant 2$ и для всех m', $m' < m$, лемма доказана. Рассмотрим произвольную подстановку констант A, для которой выполнено

$$|A| < (u(f))^m. \tag{4}$$

Покажем, что функция $f^{(m)}|_A$ не равна тождественно константе. Тем самым, лемма будет доказана. Представим функцию $f^{(m)}$ в виде

$$f^{(m)} \equiv f(f_1, \ldots, f_n),$$
$$\text{где} \quad f_i \equiv f^{(m-1)}(x_{n^{m-1}(i-1)+1}, \ldots, x_{n^{m-1}i}), \quad 1 \leqslant i \leqslant n.$$

Для каждого i, $1 \leqslant i \leqslant n$, обозначим через A_i ограничение подстановки констант A на множество $V(f_i)$. Положим

$$I = \{i \mid 1 \leqslant i \leqslant n,\ V(f_i|_{A_i}) = \varnothing\}.$$

Рассмотрим произвольное i, $i \in I$. В силу соотношения $\langle f_i \rangle = f^{(m-1)}$ имеем $u(f_i) = u(f^{(m-1)})$. Отсюда, из условия $i \in I$ и предположения индукции следует

$$|A_i| \geqslant u(f_i) = u(f^{(m-1)}) \geqslant (u(f))^{m-1}.$$

Тогда, в силу (4), имеем

$$(u(f))^m > |A| \geqslant \sum_{i \in I} |A_i| \geqslant |I| \cdot (u(f))^{m-1}.$$

Отсюда видно, что $u(f) > 0$, а значит, $|I| < u(f)$. Таким образом, количество тех функций среди $f_1|_{A_1}, \ldots, f_n|_{A_n}$, которые тождественно равны константе, меньше, чем $u(f)$. Отсюда и из тождества $f|_A \equiv f(f_1|_{A_1}, \ldots, f_n|_{A_n})$ следует, что функция $f|_A$ не равна тождественно константе.

Лемма 2 доказана.

§3. Функции, p-универсальные для данного базиса.

Скажем, что функция f *забивает* функцию g *подстановкой констант* A, если существует такая переменная x_i, что $x_i \in V(f) \cap V(g)$, $x_i \in V(f|_A)$ и $x_i \notin V(g|_A)$.

Пусть $Y \subseteq X$ — множество переменных, $h_1, \ldots, h_p$ — функции. Обозначим через $v_Y(h_1, \ldots, h_p)$ множество всевозможных наборов функций $(h_1|_B, \ldots, h_p|_B)$, где B — подстановка констант, $V(B) = Y \cap \big(\bigcup_{i=1}^{p} V(h_i)\big)$. Если $Y = X$, то множество $v_Y(h_1, \ldots, h_p)$

обозначим также $v(h_1, \ldots, h_p)$. Скажем, что функции $h_1, \ldots, h_p$ *независимы (в совокупности) по множеству* Y, если

$$v_Y(h_1, \ldots, h_p) = v_Y(h_1) \times \ldots \times v_Y(h_p).$$

Если при этом $Y = X$, то скажем, что функции $h_1, \ldots, h_p$ *независимы (в совокупности)*.

Функция f, не равная тождественно константе, называется *p-универсальной для базиса $Б$*, если для любых функций $h_1, \ldots, h_p$, бесповторно выразимых в $Б$, таких, что множества $V(h_1), \ldots, V(h_p)$ попарно не пересекаются и $\bigcup\limits_{i=1}^{p} V(h_i) = V(f)$, выполнено хотя бы одно из двух:

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

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

Мы будем использовать следующие, несложно доказываемые, свойства бесповторной выразимости: если функция h бесповторно выразима в базисе $Б$, то любая подфункция функции h бесповторно выразима в $Б$ (здесь использовано то, что константы бесповторно выразимы в любом базисе), любая функция, обобщенно однотипная с h, бесповторно выразима в $Б$ (отрицание бесповторно выразимо в любом базисе), любая функция, полученная из h биективной заменой переменных, бесповторно выразима в $Б$. Заметим также, что если функция f является p-универсальной для базиса $Б$, то любая функция, обобщенно однотипная с f, и любая функция, полученная из f биективной заменой переменных, является p-универсальной для базиса $Б$.

Утверждение 1. Пусть $Б$ — произвольный базис. Если функция φ бесповторно не выразима в базисе $Б$, функция h бесповторно выразима в $Б$, и $V(h) \neq \varnothing$, то

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

Доказательство. Предположим противное, т. е. $|v(\varphi, h)| \leqslant 2$. Тогда возможны три случая:

1) функция φ тождественно равна константе;

2) функция h тождественно равна константе;

3) для некоторой константы c выполнено тождество $\varphi \equiv h \oplus c$.

Покажем, что ни один из этих случаев невозможен. Случай 1) невозможен в силу того, что константы бесповторно выразимы в любом базисе, а функция φ бесповторно не выразима в базисе $Б$. Случай 2) невозможен в силу условия $V(h) \neq \varnothing$. Наконец, случай 3) невозможен в силу того, что функция φ бесповторно не выразима в $Б$, а функция h бесповторно выразима в $Б$.

Утверждение 1 доказано.

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

$$\varphi(x_1, \ldots, x_{k+2}) \equiv \psi(x_1, \ldots, x_k) \cdot x_{k+1} \vee x_{k+2}, \tag{5}$$

является 1-универсальной для базиса $Б$.

Доказательство. Рассмотрим произвольную функцию h, бесповторно реализуемую в базисе $Б$, и такую, что $V(h) = \{x_1, \ldots, x_{k+2}\}$. Покажем, что либо φ забивает функцию h некоторой подстановкой констант, либо функции φ и h независимы. Тем самым лемма будет доказана. Положим $A_0 = \{x_{k+1} = 1,\ x_{k+2} = 0\}$. Тогда

$$\varphi|_{A_0} \equiv \psi. \tag{6}$$

Если $V(h|_{A_0}) \neq V(\psi)$, то функция φ забивает функцию h подстановкой констант A_0. Пусть теперь $V(h|_{A_0}) = V(\psi)$. По условию настоящей леммы, функция ψ бесповторно не реализуется в базисе $Б$, а значит, в силу (6), функция $\varphi|_{A_0}$ бесповторно не реализуется в базисе $Б$. В то же время, функция $h|_{A_0}$ бесповторно реализуется в $Б$

и $V(h|_{A_0}) = V(\psi) \neq \varnothing$. Отсюда, в силу утверждения 1, следует $|v(\varphi|_{A_0}, h|_{A_0})| \geqslant 3$. Кроме того, $v(\varphi|_{A_0}, h|_{A_0}) \subseteq v(\varphi, h)$. Поэтому, если $|v(\varphi|_{A_0}, h|_{A_0})| = 4$, то $|v(\varphi, h)| = 4$ и в этом случае функции φ, h независимы. Пусть теперь $|v(\varphi|_{A_0}, h|_{A_0})| = 3$. Тогда существует единственная пара функций (c, d), $(c, d) \in (v(\varphi|_{A_0}) \times v(h|_{A_0}))\backslash v(\varphi|_{A_0}, h|_{A_0})$ (функции c и d тождественно равны константам). Рассмотрим два случая: 1) $c \equiv 0$; 2) $c \equiv 1$.

Случай 1). Рассмотрим пару функций (c', d'), $(c', d') \in (v(\varphi|_{A_0}) \times v(h|_{A_0}))\backslash v(\varphi|_{A_0}, h|_{A_0})$, где $c' \equiv \bar{c}$, $d' \equiv \bar{d}$. Существует такая подстановка констант A_1, $V(A_1) = \{x_1, \dots, x_k\}$, что

$$\varphi|_{A_0 \cup A_1} = c' \equiv \bar{c}, \qquad h|_{A_0 \cup A_1} = d' \equiv \bar{d}. \tag{7}$$

Обозначим $B_1 = A_1 \cup \{x_{k+2} = 0\}$. Тогда

$$B_1 \cup \{x_{k+1} = 1\} = A_0 \cup A_1. \tag{8}$$

Используя (5), (6), (7) и условие случая 1), получим

$$\varphi|_{B_1} \equiv \psi|_{A_1} \cdot x_{k+1} \vee 0 \equiv \varphi|_{A_0 \cup A_1} \cdot x_{k+1} \equiv \bar{c} \cdot x_{k+1} \equiv 1 \cdot x_{k+1} \equiv x_{k+1},$$

т. е. функция $\varphi|_{B_1}$ существенно зависит от переменной x_{k+1}.

Если функция $h|_{B_1}$ существенно не зависит от x_{k+1}, то функция φ забивает функцию h подстановкой констант B_1. Пусть теперь $h|_{B_1}$ существенно зависит от x_{k+1}. Положим $D_1 = B_1 \cup \{x_{k+1} = 0\}$. Используя (8) и (7), получим

$$\varphi|_{D_1} \equiv \varphi|_{B_1 \cup \{x_{k+1}=0\}} \equiv \varphi|_{B_1 \cup \{x_{k+1}=1\}} \oplus 1 \equiv \varphi|_{A_0 \cup A_1} \oplus 1 \equiv c,$$
$$h|_{D_1} \equiv h|_{B_1 \cup \{x_{k+1}=0\}} \equiv h|_{B_1 \cup \{x_{k+1}=1\}} \oplus 1 \equiv h|_{A_0 \cup A_1} \oplus 1 \equiv d.$$

Итак, $(c, d) \in v(\varphi, h)$, следовательно, $|v(\varphi, h)| = 4$, а значит, функции φ, h независимы. Случай 1) рассмотрен.

Случай 2). Рассмотрим пару функций (c', d'), $(c', d') \in (v(\varphi|_{A_0}) \times v(h|_{A_0})) \backslash v(\varphi|_{A_0}, h|_{A_0})$, где $c' \equiv \bar{c}$, $d' \equiv \bar{d}$. Существует такая подстановка констант A_2, $V(A_2) = \{x_1, \ldots, x_k\}$, что

$$\varphi|_{A_0 \cup A_2} = c' \equiv \bar{c}, \qquad h|_{A_0 \cup A_2} = d' \equiv \bar{d}. \tag{9}$$

Обозначим $B_2 = A_2 \cup \{x_{k+1} = 1\}$. Тогда

$$B_2 \cup \{x_{k+2} = 0\} = A_0 \cup A_2. \tag{10}$$

Используя (5), (6), (9) и условие случая 2), получим

$$\varphi|_{B_2} \equiv \psi|_{A_2} \cdot 1 \vee x_{k+2} \equiv \varphi|_{A_0 \cup A_2} \vee x_{k+2} \equiv \bar{c} \vee x_{k+2} \equiv 0 \vee x_{k+2} \equiv x_{k+2},$$

т. е. функция $\varphi|_{B_2}$ существенно зависит от переменной x_{k+2}.

Если функция $h|_{B_2}$ существенно не зависит от x_{k+2}, то функция φ забивает функцию h подстановкой констант B_2. Пусть теперь $h|_{B_2}$ существенно зависит от x_{k+2}. Положим $D_2 = B_2 \cup \{x_{k+2} = 1\}$. Используя (10) и (9), получим

$$\varphi|_{D_2} \equiv \varphi|_{B_2 \cup \{x_{k+2}=1\}} \equiv \varphi|_{B_2 \cup \{x_{k+2}=0\}} \oplus 1 \equiv \varphi|_{A_0 \cup A_2} \oplus 1 \equiv c,$$
$$h|_{D_2} \equiv h|_{B_2 \cup \{x_{k+2}=1\}} \equiv h|_{B_2 \cup \{x_{k+2}=0\}} \oplus 1 \equiv h|_{A_0 \cup A_2} \oplus 1 \equiv d.$$

Итак, $(c, d) \in v(\varphi, h)$, следовательно, $|v(\varphi, h)| = 4$, а значит, функции φ, h независимы. Случай 2) рассмотрен.

Лемма 3 доказана.

Утверждение 2. Пусть $Б$ — произвольный базис, f — функция, 1-универсальная для базиса $Б$, и функция f является подфункцией функции g. Тогда функция g является 1-универсальной для базиса $Б$.

Доказательство. Рассмотрим произвольную функцию h, такую, что $V(h) = V(g)$ и h бесповторно выразима в базисе $Б$. Пусть A — такая подстановка констант, $V(A) = V(g) \backslash V(f)$, что $f = g|_A$. Если $V(h|_A) \neq V(g|_A)$, то функция g забивает функцию h

подстановкой констант A. Пусть теперь $V(h|_A) = V(g|_A)$. Тогда $V(h|_A) = V(f)$ и функция $h|_A$ бесповторно выразима в базисе $Б$. По определению 1-универсальности, либо функция f забивает функцию $h|_A$ некоторой подстановкой констант B, либо функции f, $h|_A$ независимы. В первом случае функция g забивает функцию h подстановкой констант $A \cup B'$ (где B' — ограничение подстановки B на множество $V(f)$). Во втором случае, в силу условия $\mathrm{nes}(f) > 0$ имеем $V(f) = V(h|_A) \neq \varnothing$, а значит, $|v(f, h|_A)| = |v(f) \times v(h|_A)| = 2 \cdot 2 = 4$. В то же время, $v(f, h|_A) = v(g|_A, h|_A) \subseteq v(g, h)$, поэтому $|v(g, h)| = 4$, а значит, функции g, h независимы. Таким образом, функция g является 1-универсальной для базиса $Б$.

Утверждение 2 доказано.

Лемма 4. Пусть $Б$ — произвольный базис, p, q — натуральные числа, r, t — целые неотрицательные числа, $f_1, \ldots, f_r$ — функции, p-универсальные для базиса $Б$, $y_1, \ldots, y_t$ — попарно различные переменные, θ — функция от $r + t$ аргументов, $\mathrm{nes}(\theta) = r + t$, множества $V(f_1), \ldots, V(f_r), \{y_1, \ldots, y_t\}$ попарно не пересекаются и

$$g \equiv \theta(f_1, \ldots, f_r,\ y_1, \ldots, y_t), \qquad Y = \bigcup_{j=1}^{r} V(f_j). \tag{11}$$

Далее, пусть $h_1, \ldots, h_q$ — функции, бесповторно реализуемые в базисе $Б$, множества $V(h_1), \ldots, V(h_q)$ попарно не пересекаются и $\bigcup_{i=1}^{q} V(h_i) = Y$. Наконец, пусть каждое из множеств $V(f_1), \ldots, V(f_r)$ содержится в объединении не более, чем p множеств среди $V(h_1), \ldots, V(h_q)$. Тогда выполнено хотя бы одно из двух:

(i) либо функция g забивает какую-то из функций $h_1, \ldots, h_q$ некоторой подстановкой констант A, $V(A) \subseteq Y$;

(ii) либо функции g, $h_1, \ldots, h_q$ независимы в совокупности по множеству Y.

Доказательство. Проведем индукцию по r.

Базис индукции: $r = 0$. В этом случае $Y = \varnothing$, следовательно, функции g, $h_1, \ldots, h_q$ независимы в совокупности по множеству Y, т. е. выполнено (ii).

Индуктивный переход: $r > 0$ и для всех r', $r' < r$, лемма доказана. Обозначим $\tilde{y} = (y_1, \ldots, y_t)$. Рассмотрим произвольные функции

$$g^* \in v_Y(g),\ c_1 \in v_Y(h_1), \ldots, c_q \in v_Y(h_q). \tag{12}$$

Заметим, что функции $c_1, \ldots, c_q$ тождественно равны константам, а функция g^* допускает представление в виде

$$g^* \equiv \theta(d_1, \ldots, d_r, \tilde{y}), \tag{13}$$

где функция d_i, $1 \leqslant i \leqslant r$, тождественно равна константе и $d_i \in v(f_i)$.

По условию леммы, множество $V(f_1)$ содержится в объединении не более, чем p множеств среди $V(h_1), \ldots, V(h_q)$. Поэтому существует натуральное число s, $s \leqslant p$, и такие попарно различные числа $w(1), \ldots, w(s)$ из множества $\{1, \ldots, q\}$, что каждое из множеств $V(h_{w(k)}) \cap V(f_1)$, $1 \leqslant k \leqslant s$, непусто и $V(f_1) \subseteq \bigcup\limits_{k=1}^{s} V(h_{w(k)})$. Положим $\chi_k = h_{w(k)}$, $1 \leqslant k \leqslant s$. Множество переменных $V(f_1)$ функции g выделимо, поэтому существует такая подстановка констант B_1, $V(B_1) = Y \setminus V(f_1)$, что функция $g|_{B_1}$ существенно зависит от всех переменных из множества $V(f_1)$. Рассмотрим произвольное k, $1 \leqslant k \leqslant s$. Если функция $\chi_k|_{B_1}$ существенно не зависит хотя бы от одной переменной из множества $V(\chi_k) \cap V(f_1)$, то функция g забивает функцию χ_k подстановкой констант B_1 и $V(B_1) = Y \setminus V(f_1) \subseteq Y$, т. е. выполнено (i).

В то же время $V(\chi_k|_{B_1}) \subseteq V(\chi_k) \cap V(f_1)$, поэтому остался нерассмотренным только случай, когда $V(\chi_k|_{B_1}) = V(\chi_k) \cap V(f_1)$. По условию настоящей леммы, функция f_1 является p-универсальной для базиса $Б$. Положим $\chi_{s+1} = \ldots = \chi_p = 0$. Каждая из функций $\chi_1|_{B_1}, \ldots, \chi_p|_{B_1}$ бесповторно выражается в базисе $Б$, множества $V(\chi_1|_{B_1}), \ldots, V(\chi_p|_{B_1})$ попарно не пересекаются и $\bigcup\limits_{k=1}^{p} V(\chi_k|_{B_1}) = V(f_1)$. Отсюда и из определения p-универсальности следует, что либо функция f_1 забивает какую-то из функций $\chi_k|_{B_1}$, $1 \leqslant k \leqslant p$, некоторой подстановкой констант, либо функции f_1, $\chi_1|_{B_1}, \ldots, \chi_p|_{B_1}$ независимы в совокупности. Вначале рассмотрим случай, когда функция f_1 забивает функцию $\chi_k|_{B_1}$, $1 \leqslant k \leqslant p$, подстановкой констант D_1. Тогда $k \leqslant s$. Пусть D_2 — ограничение подстановки D_1 на множество $V(f_1)$. Тогда функция g забивает функцию χ_k подстановкой констант $D_2 \cup B_1$ и $V(D_2 \cup B_1) = Y$, т. е. выполнено (i).

Теперь рассмотрим случай, когда функции f_1, $\chi_1|_{B_1}, \ldots, \chi_p|_{B_1}$ независимы. В этом случае функции f_1, $\chi_1|_{B_1}, \ldots, \chi_s|_{B_1}$ независимы. Ни одна из функций f_1, $\chi_1|_{B_1}, \ldots, \chi_s|_{B_1}$ не равна тождественно константе, поэтому

$$d_1 \in v(f_1), \qquad c_{w(k)} \in v(\chi_k|_{B_1}), \quad 1 \leqslant k \leqslant s.$$

Отсюда и из независимости функций f_1, $\chi_1|_{B_1}, \ldots, \chi_s|_{B_1}$, следует

$$(d_1,\ c_{w(1)}, \ldots, c_{w(s)}) \in v(f_1,\ \chi_1|_{B_1}, \ldots, \chi_s|_{B_1}).$$

Поэтому существует такая подстановка констант B_2, $V(B_2) = V(f_1)$, что

$$d_1 = f_1|_{B_2}, \qquad c_{w(k)} = \chi_k|_{B_1 \cup B_2}, \quad 1 \leqslant k \leqslant s. \tag{14}$$

Обозначим $Y_1 = Y \setminus V(f_1)$. Тогда из (14), с учетом (11) и (13), получим

$$g^* \in v_{Y_1}(g|_{B_2}), \qquad c_{w(k)} \in v_{Y_1}(\chi_k|_{B_2}), \quad 1 \leqslant k \leqslant s. \tag{15}$$

Заметим, что если $i \in \{1, \ldots, q\} \setminus \{w(1), \ldots, w(s)\}$, то $h_i = h_i|_{B_2}$, следовательно, ввиду (12), выполнено $c_i \in v_{Y_1}(h_i|_{B_2})$. Отсюда и из (15) следует

$$g^* \in v_{Y_1}(g|_{B_2}), \qquad c_i \in v_{Y_1}(h_i|_{B_2}), \quad 1 \leqslant i \leqslant q. \tag{16}$$

Обозначим $Y_2 = V(g|_{B_2}) \cap Y$. Рассмотрим произвольное i, $1 \leqslant i \leqslant q$. В силу (16), существует такая подстановка констант E_i, $V(E_i) = (Y_1 \backslash Y_2) \cap V(h_i)$, что

$$c_i \in v_{Y_2}(h_i|_{B_2 \cup E_i}). \tag{17}$$

Положим $B = B_2 \cup \big(\bigcup\limits_{i=1}^{q} E_i\big)$. Функция $g|_{B_2}$ существенно не зависит ни от одной переменной из множества $Y_1 \backslash Y_2$, поэтому $g|_B = g|_{B_2}$. Отсюда, из (16), (17) и определения подстановки B, следует

$$g^* \in v_{Y_2}(g|_B), \qquad c_i \in v_{Y_2}(h_i|_B), \quad 1 \leqslant i \leqslant q. \tag{18}$$

Рассмотрим произвольное i, $1 \leqslant i \leqslant q$. Функция $g|_B$ существенно зависит от всех переменных из множества Y_2. В то же время $V(h_i|_B) \subseteq V(h_i) \cap Y_2$. Поэтому, если $V(h_i|_B) \neq V(h_i) \cap Y_2$, то функция g забивает функцию h_i подстановкой констант B и $V(B) = Y \backslash Y_2 \subseteq Y$, т. е. выполнено (i).

Осталось рассмотреть случай, когда $V(h_i|_B) = V(h_i) \cap Y_2$. В этом случае

$$V(g|_B) \cap Y = Y_2 = \bigcup_{i=1}^{q} V(h_i|_B). \tag{19}$$

Заметим, что функцию $g|_B$ можно представить в виде

$$g|_B \equiv \theta'(f'_1, \dots, f'_{r'}, y'_1, \dots, y'_{t'}),$$

где $0 \leqslant r' \leqslant r$, $0 \leqslant t' \leqslant t$, $\{f'_1, \dots, f'_{r'}\} \subseteq \{f_2, \dots, f_r\}$, $\{y'_1, \dots, y'_{t'}\} \subseteq \{y_1, \dots, y_t\}$, все f'_j, $1 \leqslant j \leqslant r'$, попарно различны, все y'_j, $1 \leqslant j \leqslant t'$, попарно различны, θ' — функция $r' + t'$ аргументов и $\mathrm{nes}(\theta') = r' + t'$. Убедимся, что к числам p, q, r', t', функциям $f'_1, \dots, f'_{r'}$, $h_1|_B, \dots, h_q|_B$ и множеству Y_2 можно применить предположение индукции.

Функции $f'_1, \dots, f'_{r'}$ являются p-универсальными для базиса $Б$, множества $V(f'_1), \dots, V(f'_{r'})$, $\{y'_1, \dots, y'_{t'}\}$ попарно не пересекаются и, в силу (19), справедливо $\bigcup\limits_{j=1}^{r'} V(f'_j) = V(g|_B) \cap Y = Y_2$. Далее, функции $h_1|_B, \ldots, h_q|_B$ бесповторно выразимы в базисе $Б$, множества $V(h_1|_B), \ldots, V(h_q|_B)$ попарно не пересекаются и, в силу (19), $\bigcup\limits_{i=1}^{q} V(h_i|_B) = Y_2$. Кроме того, каждое из множеств $V(f'_j)$, $1 \leqslant j \leqslant r'$, целиком содержится в объединении не более, чем p множеств из $V(h_1|_B), \ldots, V(h_q|_B)$. Наконец, $r' < r$.

Из предположения индукции следует, что либо функция $g|_B$ забивает какую-то из функций $h_i|_B$, $1 \leqslant i \leqslant q$, некоторой подстановкой констант A', $V(A') \subseteq Y_2$, либо функции $g|_B$, $h_1|_B, \ldots, h_q|_B$ независимы в совокупности по множеству Y_2. Если для некоторого i, $1 \leqslant i \leqslant q$, функция $g|_B$ забивает функцию $h_i|_B$ подстановкой констант A', то функция g забивает функцию h_i подстановкой констант $A' \cup B$ и $V(A' \cup B) \subseteq Y$, т. е. в этом случае выполнено (i).

Наконец, рассмотрим случай, когда функции $g|_B$, $h_1|_B, \ldots, h_q|_B$ независимы по множеству Y_2. Тогда из (18) следует

$$(g^*,\ c_1, \ldots, c_q) \in v_{Y_2}(g|_B) \times v_{Y_2}(h_1|_B) \times \ldots \times v_{Y_2}(h_q|_B) =$$

(используем независимость функций $g|_B$, $h_1|_B, \ldots, h_q|_B$ по множеству Y_2)

$$= v_{Y_2}(g|_B,\ h_1|_B, \ldots, h_q|_B) \subseteq$$

(используем соотношение $V(B) = Y \backslash Y_2$)

$$\subseteq v_Y(g,\ h_1, \ldots, h_q).$$

Отсюда, в силу произвольности выбора $g^* \in v_Y(g)$, $c_1 \in v_Y(h_1), \ldots, c_q \in v_Y(h_q)$, получим

$$v_Y(g) \times v_Y(h_1) \times \ldots \times v_Y(h_q) \subseteq v_Y(g,\ h_1, \ldots, h_q).$$

Очевидно, что обратное включение также имеет место. Таким образом, функции g, $h_1, \ldots, h_q$ независимы по множеству Y, т. е. выполнено (ii). Индукция проведена.

Лемма 4 доказана.

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

$$m(p,\varphi) = \lfloor \log_{\left(\frac{n}{n-1}\right)} p \rfloor + \lfloor \log_u p \rfloor + 2. \tag{20}$$

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

Доказательство. Обозначим через f функцию $\varphi^{(m(p,\varphi))}$. Рассмотрим произвольные функции $h_1, \dots, h_p$, бесповторно реализуемые в базисе $Б$, такие, что множества $V(h_1), \dots, V(h_p)$ попарно не пересекаются и $\bigcup\limits_{i=1}^{p} V(h_i) = V(f)$. Покажем, что либо функция f забивает какую-то из функций $h_1, \dots, h_p$ некоторой подстановкой констант, либо функции f, $h_1, \dots, h_p$ независимы в совокупности. Тем самым лемма будет доказана.

Рассмотрим произвольные функции

$$c \in v(f), \qquad c_i \in v(h_i), \quad 1 \leqslant i \leqslant p. \tag{21}$$

Заметим, что эти функции тождественно равны константам. Положим

$$s = \lfloor \log_{\left(\frac{n}{n-1}\right)} p \rfloor + 1, \qquad r = \lfloor \log_u p \rfloor + 1.$$

Отсюда и из (20) следует, что

$$s + r = m(p,\varphi), \qquad \frac{n^s}{p} > (n-1)^s, \qquad p < u^r. \tag{22}$$

Представим функцию f в виде

$$f \equiv \varphi^{(r)}(f_1, \dots, f_{n^r}),$$
$$\text{где} \quad f_j \equiv \varphi^{(s)}(x_{n^s(j-1)+1}, \dots, x_{n^s j}), \quad 1 \leqslant j \leqslant n^r. \tag{23}$$

Рассмотрим произвольное j, $1 \leqslant j \leqslant n^r$. Обозначим $Y_j = V(f_j)$. Тогда $|Y_j| = n^s$, поэтому мощность хотя бы одного из множеств $Y_j \cap$

$V(h_i)$, $1 \leqslant i \leqslant p$, не меньше, чем $\frac{n^s}{p}$. Выберем число $w(j)$ так, чтобы выполнялось $|Y_j \cap V(h_{w(j)})| \geqslant \frac{n^s}{p}$. Тогда из второго соотношения в (22) следует $|Y_j \cap V(h_{w(j)})| > (n-1)^s$. Функция f_j может быть получена из функции $\varphi^{(s)}$ заменой переменных без отождествления, поэтому, в силу леммы 1 из § 2, существует такая подфункция g_j функции f_j, что $V(g_j) \subseteq Y_j \cap V(h_{w(j)})$ и функция $\langle g_j \rangle$ обобщенно однотипна с φ. Пусть B_j — такая подстановка констант, что $V(B_j) = Y_j \backslash V(g_j)$ и $g_j = f_j|_{B_j}$. Обозначим

$$Z = \bigcup_{j=1}^{n^r} V(g_j), \quad W = \{w(j) \mid 1 \leqslant j \leqslant n^r\}.$$

Рассмотрим произвольное i, $i \in \{1, \dots, p\} \backslash W$, для которого выполнено $V(h_i) \neq \varnothing$. Среди множеств $Y_j \cap V(h_i)$, $1 \leqslant j \leqslant n^r$, найдется непустое. Выберем число $t(i)$ так, чтобы выполнялось $Y_{t(i)} \cap V(h_i) \neq \varnothing$. Положим

$$T = \{t(i) \mid i \in \{1, \dots, p\} \backslash W,\ V(h_i) \neq \varnothing\},$$
$$B = \bigcup_{j \in \{1, \dots, n^r\} \backslash T} B_j, \qquad Y_T = \bigcup_{j \in T} Y_j.$$

В силу выбора подстановок B_j и представления (23), получим

$$V(f|_B) = Z \cup Y_T. \tag{24}$$

Рассмотрим теперь произвольное i, $1 \leqslant i \leqslant p$. Если $V(h_i) = \varnothing$, то ввиду (21), справедливо

$$c_i \in v(h_i) = v(h_i|_B), \qquad 1 \leqslant i \leqslant p,\ V(h_i) = \varnothing. \tag{25}$$

Пусть теперь $V(h_i) \neq \varnothing$. Если $i \in W$, то $Z \cap V(h_i) \neq \varnothing$, а если $i \notin W$, то $Y_T \cap V(h_i) \neq \varnothing$. В любом случае

$$(Z \cup Y_T) \cap V(h_i) \neq \varnothing. \tag{26}$$

Из выбора подстановки B и условия $V(h_i) \subseteq V(f)$ следует, что $V(h_i|_B) \subseteq (Z \cup Y_T) \cap V(h_i)$. Если $V(h_i|_B) \neq (Z \cup Y_T) \cap V(h_i)$, то, в силу (24), функция f забивает функцию h_i подстановкой констант B.

Осталось рассмотреть случай, когда $V(h_i|_B) = (Z \cup Y_T) \cap V(h_i)$. В этом случае, в силу (26), имеем $V(h_i|_B) \neq \varnothing$, а значит

$$c_i \in v(h_i|_B), \qquad 1 \leqslant i \leqslant p, \quad V(h_i) \neq \varnothing. \tag{27}$$

Объединяя (25) и (27), получим $c_i \in v(h_i|_B)$, $1 \leqslant i \leqslant p$. Отсюда и из условия, что множества $V(h_i)$, $1 \leqslant i \leqslant p$, попарно не пересекаются, следует, что существует такая подстановка констант D, $V(D) = Y_T$, что $c_i \in v(h_i|_{B\cup D})$, $1 \leqslant i \leqslant p$. Наконец, существует такая подстановка констант E, $V(E) = V(f)\backslash(V(f|_{B\cup D}) \cup B \cup D)$, что $c_i \in v(h_i|_{B\cup D\cup E})$, $1 \leqslant i \leqslant p$. Обозначим

$$A = B \cup D \cup E, \qquad Y = V(f|_A).$$

Тогда

$$c_i \in v(h_i|_A), \qquad 1 \leqslant i \leqslant p. \tag{28}$$

Рассмотрим произвольное i, $1 \leqslant i \leqslant p$. Из выбора подстановки констант A и вложения $V(h_i) \subseteq V(f)$ следует, что $V(h_i|_A) \subseteq V(h_i) \cap Y$. Если $V(h_i|_A) \neq V(h_i) \cap Y$, то функция f забивает функцию h_i подстановкой констант A. Осталось рассмотреть случай, когда $V(h_i|_A) = V(h_i) \cap Y$. В этом случае

$$\bigcup_{i=1}^{p} V(h_i|_A) = Y = V(f|_A). \tag{29}$$

Заметим, что функция $f|_A$ допускает представление в виде

$$f|_A \equiv \theta(g'_1, \ldots, g'_{r'}),$$

где r' — целое число, $r' \geqslant 0$, $\{g'_1, \ldots, g'_{r'}\} \subseteq \{g_1, \ldots, g_{n^r}\}$, все $g'_1, \ldots, g'_{r'}$ попарно различны, θ — функция r' аргументов и $\operatorname{nes}(\theta) = r'$. Убедимся, что к числам $p' = 1$, $q' = p$, r', $t' = 0$, функциям $f|_A$, $h_1|_A, \ldots, h_p|_A$ и множеству Y можно применить лемму 4.

Функции $\langle g'_j \rangle$, $1 \leqslant j \leqslant r'$, обобщенно однотипны с функцией φ. По условию настоящей леммы, функция φ является 1-универсальной для базиса $Б$. Следовательно, функции g'_j, $1 \leqslant j \leqslant r'$, являются 1-универсальными для базиса $Б$. Множества $V(g'_1), \ldots, V(g'_{r'})$ попарно не пересекаются и, в силу (29), $\bigcup\limits_{j=1}^{r'} V(g'_j) = V(f|_A) = Y$. Далее, функции $h_1|_A, \ldots, h_p|_A$ бесповторно выразимы в базисе $Б$, множества $V(h_1|_A), \ldots, V(h_p|_A)$ попарно не пересекаются и их объединение, в силу (29), совпадает с множеством Y. Наконец, каждое из множеств $V(g'_j)$ целиком содержится в одном из множеств $V(h_i)$, $1 \leqslant i \leqslant p$, а значит, и в одном из множеств $V(h_i|_A)$, $1 \leqslant i \leqslant p$.

Применив лемму 4, получим, что либо функция $f|_A$ забивает какую-то из функций $h_1|_A, \ldots, h_p|_A$ подстановкой констант A', $V(A') \subseteq Y$, либо функции $f|_A$, $h_1|_A, \ldots, h_p|_A$ независимы в совокупности по множеству Y. Если функция $f|_A$ забивает функцию $h_i|_A$ подстановкой констант A', то функция f забивает функцию h_i подстановкой $A \cup A'$. Рассмотрим теперь случай, когда функции $f|_A, h_1|_A, \ldots, h_p|_A$ независимы по множеству Y. Тогда, в силу (29), функции $f|_A, h_1|_A, \ldots, h_p|_A$ независимы. По определению независимости

$$v(f|_A) \times v(h_1|_A) \times \ldots \times v(h_p|_A) = v(f|_A, h_1|_A, \ldots, h_p|_A). \tag{30}$$

Рассмотрим подстановку констант $D' = \{(x_j, f_j|_D) \mid j \in T\}$. Из определения множества T, третьего соотношения в (22), и леммы 2 (из § 2) следует

$$|D'| = |T| \leqslant p < u^r = u(\varphi)^r \leqslant u(\varphi^{(r)}).$$

В то же время $V(D') \subseteq \{x_1, \dots, x_{n^r}\} = V(\varphi^{(r)})$, а значит, $V(\varphi^{(r)}|_{D'}) \neq \varnothing$. Отсюда и из представления (23) следует, что $V(f|_D) \neq \varnothing$, но тогда и $V(f|_A) \neq \varnothing$, поэтому $c \in v(f|_A)$. Объединив включение $c \in v(f|_A)$ с включениями (28), получим

$$(c, c_1, \dots, c_p) \in v(f|_A) \times v(h_1|_A) \times \ldots \times v(h_p|_A) =$$

(используем равенство (30))

$$= v(f|_A, h_1|_A, \dots, h_p|_A) \subseteq$$

(используем определение множества $v(f, h_1, \dots, h_p)$)

$$\subseteq v(f, h_1, \dots, h_p).$$

Отсюда, в силу произвольности выбора $c \in v(f)$, $c_i \in v(h_i)$, $1 \leqslant i \leqslant p$, следует

$$v(f) \times v(h_1) \times \ldots \times v(h_p) \subseteq v(f, h_1, \dots, h_p).$$

Обратное включение также выполнено, а значит, функции $f, h_1, \dots, h_p$ независимы.

Лемма 5 доказана.

ГЛАВА II. СВОЙСТВА ФОРМУЛ СПЕЦИАЛЬНОГО ВИДА

§4. Техника забивания μ_L^s-формул.

Пусть f — произвольная функция n аргументов, $Б$ — произвольный базис, x_i, $1 \leqslant i \leqslant n$, — переменная. Функция f называется *линейной*, если существуют такие константы $a_0, \ldots, a_n$, что

$$f \equiv a_1 x_1 \oplus \ldots \oplus a_n x_n \oplus a_0.$$

В противном случае функция f называется *нелинейной*. Введем функцию $\oplus_n$ от n аргументов, задав ее тождеством

$$\oplus_n \equiv x_1 \oplus \ldots \oplus x_n.$$

Базис $Б$ назовем *линейным*, если функция $\oplus_2$ бесповторно выразима в базисе $Б$. В противном случае базис $Б$ назовем *нелинейным*.

Скажем, что функция f *линейно зависит* от x_i, если

$$f|_{\{x_i=0\}} \equiv f|_{\{x_i=1\}} \oplus 1. \tag{31}$$

Скажем, что функция f *нелинейно зависит* от x_i, если $x_i \in V(f)$ и тождество (31) не выполнено.

Пусть F — произвольная формула. Формула F называется *приведенной*, если выполнены следующие условия:

a) либо $F \overline{\underline{\circ}}\, c$, $c \in \{0,1\}$, либо ни одна подформула формулы F не реализует константу;

b) внешняя функция каждой подформулы формулы 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:

(i) $F' \equiv F$;

(ii) $\forall i \; L_{x_i}(F') \leqslant L_{x_i}(F)$.

Доказательство. Проведем построение формулы F' в несколько этапов. Вначале для каждой подформулы G формулы F заменим все вхождения в G переменных, несущественных для функции ею реализуемой, одинаковыми константами. Полученную формулу обозначим через F_1. Затем рассмотрим все подформулы формулы F_1, реализующие константы. Среди них выделим максимальные по включению, и заменим их соответствующими константами. Полученную формулу обозначим через F_2. Если F_2 реализует константу, то $F_2 \mathrel{\overset{\circ}{=}} c$, где c — эта константа. В этом случае положим $F' = F_2$, и утверждение доказано. В противном случае продолжим построение.

Пусть G — произвольная подформула формулы F_2, отличная от константы, $G \mathrel{\overset{\circ}{=}} g(G_1, \ldots, G_n)$. Обозначим

$$A = \{(x_i, c_i) \mid x_i \in V(g),\; G_i \equiv c_i,\; c_i \in \{0,1\}\}, \qquad g' = \langle g|_A \rangle.$$

Пусть $V(g|_A) = \{j_1, \ldots, j_k\}$, $j_1 < \ldots < j_k$. Заменим подформулу G подформулой $G' = g'(G_{j_1}, \ldots, G_{j_k})$. При этом функция g' принадлежит базису $[Б]$ и существенно зависит от всех своих переменных. Кроме того, ни одна из субформул $G_{j_1}, \ldots, G_{j_k}$ не реализует константу. Заменим теперь каждую подформулу G формулы F_2 на соответствующую ей подформулу G'. Полученную формулу обозначим через F_3.

Формула F_3 не содержит подформул, реализующих константы, и внешняя функция каждой подформулы формулы F_3 существенно зависит от всех своих переменных. Рассмотрим произвольную подформулу H формулы F_3, внешняя функция которой нелинейна и линейно зависит хотя бы от одного своего аргумента. Если хотя бы одна такая подформула существует, то базис $[Б]$ линеен, а значит, существует такая константа σ, что функция Λ, $\Lambda(x_1, x_2) \equiv x_1 \oplus x_2 \oplus \sigma$, принадлежит базису $[Б]$. Пусть $H \mathrel{\overset{\circ}{=}} h(H_1, \ldots, H_m)$. Пусть также $x_{t_1}, \ldots, x_{t_s}$, $t_1 < \ldots < t_s$, — все переменные, от которых функция h зависит нелинейно, $x_{t_{s+1}}, \ldots, x_{t_m}$, $t_{s+1} < \ldots < t_m$, — все переменные, от которых функция h зависит линейно. Положим $B = \{x_{t_{s+1}} = \sigma, \ldots, x_{t_m} = \sigma\}$, $h' = \langle h|_B \rangle$. Тогда

$$h(x_1, \ldots, x_m) \equiv h'(x_{t_1}, \ldots, x_{t_s}) \oplus (x_{t_{s+1}} \oplus \sigma) \oplus \ldots \oplus (x_{t_m} \oplus \sigma).$$

Для каждого r, $s \leqslant r \leqslant m$, определим формулу H'_r, положив

$$H'_r = \Lambda(\ldots(\Lambda(h'(H_{t_1}, \ldots, H_{t_s}), H_{t_{s+1}}) \ldots), H_{t_r}).$$

Если ни одна из формул H'_r, $s \leqslant r \leqslant m-1$, не реализует константу, то положим $H' = H'_m$. В противном случае обозначим через w наибольшее из чисел r, $s \leqslant r \leqslant m-1$, для которых формула H'_r реализует константу. Пусть $H'_w \equiv \tau$, $\tau \in \{0, 1\}$. Обозначим

$$H^* = \Lambda(\ldots(\Lambda(H_{t_{w+1}}, H_{t_{w+2}}) \ldots), H_{t_m})$$

Заметим, что $\neg \in [Б]$. Положим $H' = \neg(\neg(H^*))$ при $\tau = \sigma$, $H' = \neg(H^*)$ при $\tau = \bar{\sigma}$.

Заменим теперь каждую из рассмотренных подформул H формулы F_3 на соответствующую ей подформулу H'. Полученную формулу примем за F'. Ни одна подформула формулы F' не содержит вхождений переменных, несущественных для функции, ею реализуемой (в силу выбора формулы F_1). Далее, внешняя функция f каждой подформулы формулы F' является либо функцией вида g' (если она линейна либо нелинейно зависит от всех своих аргументов), либо функцией вида h', либо одной из функций $\Lambda, \neg$. В любом случае, функция f существенно зависит от всех своих аргументов и либо линейна, либо нелинейно зависит от всех своих аргументов. Кроме того, $f \in [Б]$. Из построения подформул G' и H' следует, что формула F' не содержит подформул, реализующих константы. Итак, формула F' приведена, является формулой в базисе $[Б]$ и $F \equiv F_1 \equiv F_2 \equiv F_3 \equiv F'$. Наконец, заметим, что в процессе построения формулы F' не добавилось ни одного вхождения переменной, а значит, $\forall i\ L_{x_i}(F') \leqslant L_{x_i}(F)$. Свойства (i) и (ii) выполнены.

Утверждение 3 доказано.

Пусть F — формула, $F \overset{\circ}{=} f(F_1, \dots, F_n)$. Формула F называется *ν-формулой*, если не существует такой линейной функции Λ, что выполнено тождество

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

Скажем, что функция f *забивает формулу F в базисе $Б$ подстановкой констант A*, если существует формула F' в базисе $Б$ и существует такая переменная z, что выполнены следующие условия:

a) $z \in V(f|_A)$;

b) $F' \equiv F|_A$;

c) $\forall i\ L_{x_i}(F') \leqslant L_{x_i}(F|_A)$;

d) $L_z(F') < L_z(F|_A)$.

Лемма 6. Пусть $Б$ — нормальный линейный базис, $p = \mathrm{nes}(Б)$, f — функция n аргументов, $\mathrm{nes}(f) = n$, функция f является p-универсальной для $Б$, m — натуральное число и g — подфункция функции $f^{(m)}$. Далее, пусть H — приведенная ν-формула в базисе $Б$, $H \overset{\circ}{=} h(H_1, \dots, H_q)$, все переменные, входящие в H, существенны для g, $T = \bigcup_{i=1}^{q-1} V(H_i)$, и все переменные из множества T являются 1-регулярными для g. Наконец, пусть существуют такие переменные $z_1 \in V(H_1), \dots, z_q \in V(H_q)$, что $z_q \notin T$ и ни одна из переменных $z_1, \dots, z_{q-1}$ не входит в то 1-множество функции g, в котором содержится z_q. Тогда существует такая подстановка констант A, $V(A) \subseteq T$, что функция g забивает формулу H в базисе $Б$ подстановкой A.

Доказательство. Рассмотрим два случая: 1) существует переменная z, суммарное число вхождений которой в субформулы $H_1, \ldots, H_{q-1}$ не меньше двух; 2) суммарное число вхождений каждой переменной в субформулы $H_1, \ldots, H_{q-1}$ не больше одного.

Случай 1). В силу условия $z \in V(g)$, существует такая подстановка констант A, $V(A) = T \backslash \{z\}$, что $z \in V(g|_A)$. Пусть функция φ такова, что $H|_A \equiv \varphi(z, H_q|_A)$. В силу линейности и нормальности базиса $Б$, существует такая функция ψ, $\psi \in Б$, и такие константы σ_1, σ_2 и σ_3, что $\varphi(x_1, x_2) \equiv \psi(x_1 \oplus \sigma_1, x_2 \oplus \sigma_2) \oplus \sigma_3$. Положим $H' = \theta_{\sigma_3}(\psi(\theta_{\sigma_1}(z), \theta_{\sigma_2}(H_q)))$, где $\theta_0(F) \mathrel{\underline{\circ}} F$, $\theta_1(F) \mathrel{\underline{\circ}} \neg(F)$. Тогда, в силу условия случая 1), имеем $L_z(H') < L_z(H|_A)$. Ввиду этого, функция g забивает формулу H в базисе $Б$ подстановкой A. Случай 1) рассмотрен.

Случай 2). Положим $z = z_q$. Обозначим через Z то 1-множество функции g, которое содержит переменную z. Пусть $Z_1, \ldots, Z_r$ — все различные регулярные 1-множества функции g, не содержащие переменную z и пересекающиеся хотя бы с одним из множеств $V(H_1), \ldots, V(H_{q-1})$. Представим функцию g в виде

$$g \equiv \theta(f_1, \ldots, f_r, f^*, \tilde{y}),$$

где θ, $f_1, \ldots, f_r$, f^* — функции, причем функции $f_1, \ldots, f_r$ получены из f биективной заменой переменных, $V(f_1) = Z_1, \ldots, V(f_r) = Z_r$, $V(f^*) = Z$, $\tilde{y}$ — набор, составленный из всех различных переменных, существенных для функции g, и не входящих ни в одно из множеств $Z_1, \ldots, Z_r$, Z. Функция θ существенно зависит от всех своих аргументов. Существует подстановка констант B, $V(B) = Z \backslash \{z\}$, и такая константа σ, что $f^*|_B \equiv z \oplus \sigma$. Тогда

$$g|_B \equiv \theta(f_1, \ldots, f_r, z \oplus \sigma, \tilde{y}). \tag{32}$$

Положим

$$Y = \bigcup_{j=1}^{r} Z_j, \qquad Y_i = V(H_i|_B), \quad 1 \leqslant i \leqslant q-1, \qquad Y_q = Y \backslash (\bigcup_{i=1}^{q-1} Y_i).$$

Рассмотрим произвольное i, $1 \leqslant i \leqslant q-1$. Обозначим через h_i функцию, реализуемую формулой $H_i|_B$. Все переменные из множества Y_i существенны для функции $g|_B$. Поэтому, если какая-то переменная из множества Y_i несущественна для функции h_i, то функция g забивает формулу H в базисе $Б$ подстановкой констант B. Рассмотрим теперь случай, когда $V(h_i) = Y_i$, $1 \leqslant i \leqslant q-1$. Если $Y_q = \varnothing$, то положим $h_q = 0$, а если $Y_q \neq \varnothing$, то обозначим через h_q сумму по модулю два всех переменных из множества Y_q.

Убедимся, что к числам p, q, r, $t+1$ (где t равно длине набора $\tilde{y}$), функциям $g|_B$, $h_1, \ldots, h_q$ и множеству Y применима лемма 4 из § 3. В силу условия случая 2), каждое из выражений $H_1|_B, \ldots, H_{q-1}|_B$ — либо переменная, либо бесповторная формула в базисе $Б$. В любом случае функции $h_1, \ldots, h_{q-1}$ бесповторно выразимы в базисе $Б$. В силу линейности базиса $Б$, функция h_q также бесповторно выразима в $Б$. Из условия случая 2) и определения функции h_q следует, что множества $V(h_1), \ldots, V(h_q)$ попарно не пересекаются. Объединение множеств $V(h_1), \ldots, V(h_q)$ совпадает с множеством Y. По условию леммы, функция f является p-универсальной для базиса $Б$, поэтому каждая из функций $f_1, \ldots, f_s$ является p-универсальной для базиса $Б$. Наконец заметим, что в силу неравенства $q \leqslant p$, каждое из множеств $V(f_j)$, $1 \leqslant j \leqslant s$, содержится в объединении не более, чем p множеств среди $V(h_1), \ldots, V(h_q)$.

Применив лемму 4, получим, что либо функция $g|_B$ забивает какую-то из функций $h_1, \ldots, h_q$ некоторой подстановкой констант D, $V(D) \subseteq Y$, либо функции $g|_B, h_1, \ldots, h_q$ независимы в совокупности по множеству Y. Вначале рассмотрим случай, когда функция $g|_B$ забивает функцию h_i, $1 \leqslant i \leqslant q$, подстановкой констант D. В силу линейности функции h_q, никакая функция ее забивать не может, поэтому $i \leqslant q-1$. Обозначим через D' ограничение подстановки констант $D \cup B$ на множество $V(H_i)$. Тогда функция g забивает функцию, реализуемую выражением H_i, подстановкой констант D', а значит, функция g забивает формулу H в базисе $Б$ подстановкой констант D'.

Наконец, рассмотрим случай, когда функции $g|_B, h_1, \ldots, h_q$ независимы в совокупности по множеству Y. Тогда функции $g|_B, h_1, \ldots, h_{q-1}$ независимы в совокупности по множеству Y. По определению независимости,

$$v_Y(g|_B) \times v_Y(h_1) \times \ldots \times v_Y(h_{q-1}) = v_Y(g|_B, h_1, \ldots, h_{q-1}). \qquad (33)$$

Формула H является ν-формулой, следовательно, функция h нелинейна. В силу приведенности формулы H, функция h нелинейно зависит от переменной x_q. Поэтому существуют такие константы $c_1, \ldots, c_{q-1}$, что функция $h(c_1, \ldots, c_{q-1}, x_q)$ тождественно равна константе. По условию леммы, существует переменная z_i, $z_i \in V(H_i) \backslash Z$, $1 \leqslant i \leqslant q-1$. Тогда $z_i \in Y_i = V(h_i)$, а значит, $V(h_i) \neq \varnothing$. Поэтому существует функция c'_i, для которой выполнено

$$c'_i \in v(h_i) = v_Y(h_i), \qquad c'_i \equiv c_i, \qquad 1 \leqslant i \leqslant q-1. \qquad (34)$$

Функция θ существенно зависит от $(r+1)$-го аргумента, поэтому существуют такие константы $d_1, \ldots, d_r$, что функция $\theta(d_1, \ldots, d_r, z \oplus \sigma, \tilde{y})$ существенно зависит от переменной z. Пусть g' — такая функция, что

$$g' \in v_Y(g|_B), \qquad g' \equiv \theta(d_1, \ldots, d_r, z \oplus \sigma, \tilde{y}). \qquad (35)$$

Объединяя включения (34) и (35), получим

$$(g', c'_1, \ldots, c'_{q-1}) \in v_Y(g|_B) \times v_Y(h_1) \times \ldots \times v_Y(h_{q-1}) =$$

(используем равенство (33))

$$= v_Y(g|_B, h_1, \ldots, h_{q-1}).$$

Следовательно, существует такая подстановка констант E, $V(E) = Y$, что

$$g|_{B\cup E} \equiv g', \qquad h_1|_E \equiv c_1, \ldots, h_{q-1}|_E \equiv c_{q-1}.$$

В качестве A возьмем ограничение подстановки констант $B \cup E$ на множество T. Функция g' существенно зависит от переменной z, поэтому и функция $g|_A$ существенно зависит от z. Далее,

$$H|_A \equiv h(H_1|_{B\cup E}, \ldots, H_{q-1}|_{B\cup E}, H_q|_A) \equiv h(c_1, \ldots, c_{q-1}, H_q|_A).$$

Функция $h(c_1, \ldots, c_{q-1}, x_q)$ тождественно равна константе, а значит, формула $H|_A$ реализует константу. В то же время формула $H|_A$ содержит хотя бы одно вхождение переменной z. Таким образом, функция g забивает формулу H в базисе $Б$ подстановкой констант A.

Лемма 6 доказана.

Формула F называется *элементарной*, если $L(F) \geqslant 2$, и сложность любой подформулы формулы F, отличной от F, не больше единицы. Заметим, что каждая формула, сложность которой не меньше двух, содержит элементарную подформулу.

Лемма 7. Пусть $Б$ — нормальный нелинейный базис, $p = \mathrm{nes}(Б)$, f — функция n аргументов, $\mathrm{nes}(f) = n$, каждая переменная функции f входит в некоторое $\oplus_p$-выделимое множество переменных функции f, m — натуральное число и g — подфункция функции $f^{(m)}$. Далее, пусть H — приведенная ν-формула в базисе $Б$, $H \ \overline{\circ}\ h(H_1, \ldots, H_q)$, и все переменные, входящие в формулу H, существенны для функции g. Наконец, пусть $T = \bigcup\limits_{i=1}^{q-1} V(H_i)$, все переменные из множества T являются 1-регулярными для функции g и существует переменная z_q, $z_q \in V(H_q) \backslash T$. Тогда существует такая подстановка констант A, $V(A) \subseteq T$, что функция g забивает формулу H в базисе $Б$ подстановкой A.

Доказательство. Рассмотрим два случая: 1) сложность хотя бы одной из формул $H_1, \ldots, H_{q-1}$ не меньше двух; 2) сложность каждой из формул $H_1, \ldots, H_{q-1}$ меньше двух.

Случай 1). Пусть сложность формулы H_{i_0}, $1 \leqslant i_0 \leqslant q-1$, не меньше двух. Тогда существует элементарная подформула H' формулы H. Рассмотрим два случая: 1.1) формула H' бесповторна; 1.2) формула H' не бесповторна.

Случай 1.1). Пусть формула H' реализует функцию φ. Базис $Б$ нелинеен, поэтому функция φ не может быть линейной функцией, существенно зависящей от двух и более переменных. В то же время, в силу элементарности, $L(H') \geqslant 2$, поэтому $|V(H')| \geqslant 2$. В силу приведенности формулы H, формула H' не содержит вхождений переменных, несущественных для функции φ, поэтому $\mathrm{nes}(\varphi) \geqslant 2$, а значит функция φ нелинейна. Тогда существует переменная z, $z \in V(\varphi)$, и такая подстановка констант A, $V(A) = V(\varphi) \backslash \{z\}$, что функция $\varphi|_A$ тождественно равна константе.

В силу элементарности формулы H', имеем $L(H') \leqslant q$, а значит,

$$|A| \leqslant V(\varphi) - 1 = L(H') - 1 \leqslant q - 1 \leqslant p - 1. \tag{36}$$

Каждая переменная из множества $V(A)$ является 1-регулярной для функции g. Заметим, что каждая 1-регулярная переменная функции g входит в некоторое $\oplus_p$-выделимое множество переменных функции g. Поэтому для любой подстановки констант B мощности, не превосходящей $p-1$, определенной только на 1-регулярных переменных функции g, функция $g|_B$ существенно зависит от всех переменных из множества $V(g) \backslash V(B)$. Отсюда и из (36) следует, что $V(g|_A) = V(g) \backslash V(A)$, а тогда $z \in V(g|_A)$. В то же время, формула $H'|_A$ реализует константу и содержит вхождение переменной z. Таким образом, функция g забивает формулу H', а значит, и формулу H в базисе $Б$ подстановкой констант A. Кроме того, $V(A) \subseteq V(H') \subseteq V(H_{i_0}) \subseteq T$. Случай 1.1) рассмотрен.

Случай 1.2). Пусть переменная z входит в формулу H' не меньше двух раз. Переменная z существенна для функции g, поэтому существует такая подстановка констант A, $V(A) = V(H')\backslash\{z\}$, что функция $g|_A$ существенно зависит от z. Формула $H'|_A$ реализует функцию, существенно зависящую не более, чем от одной переменной, поэтому существует такая формула H'' в базисе $Б$, что $H'' \equiv H'|_A$ и $L(H'') \leqslant 1$. Отсюда следует, что функция g забивает формулу H', а значит, и формулу H в базисе $Б$ подстановкой констант A. Кроме того, $V(A) \subseteq V(H') \subseteq V(H_{i_0}) \subseteq T$. Случай 1) рассмотрен.

Случай 2). В этом случае, в силу приведенности формулы H, имеем $L(H_1) = \ldots = L(H_{q-1}) = 1$. Обозначим

$$H^* = h(H_1, \ldots, H_{q-1}, z_q).$$

Рассмотрим два случая: 2.1) существует такая подстановка констант B, $V(B) = T$, что формула $H^*|_B$ реализует константу; 2.2) ни для одной подстановки констант B, $V(B) = T$, формула $H^*|_B$ не реализует константу.

Случай 2.1). Положим $A = B$, $z = z_q$. Тогда формула $H|_A$ реализует константу. По условию леммы, $z \notin T$, поэтому формула $H|_A$ содержит вхождение переменной z. Наконец, подстановка констант A определена только на 1-регулярных переменных функции g, каждая 1-регулярная переменная функции g входит в некоторое $\oplus_p$-выделимое множество переменных и $|A| = |T| \leqslant q-1 \leqslant p-1$. Поэтому $V(g|_A) = V(g)\backslash V(A)$, а значит, $z \in V(g|_A)$. Таким образом, функция g забивает формулу H в базисе $Б$ подстановкой констант A. Случай 2.1) рассмотрен.

Случай 2.2). В этом случае для любой подстановки констант B, $V(B) = T$, имеем

$$H^*|_{B\cup\{z_q=0\}} \equiv H^*|_{B\cup\{z_q=1\}} \oplus 1,$$

а значит,

$$H^*|_{\{z_q=0\}} \equiv H^*|_{\{z_q=1\}} \oplus 1.$$

Тогда

$$H^* \equiv h(H_1, \dots, H_{q-1}, 0) \oplus z_q. \qquad (37)$$

Отсюда, подставляя вместо всех вхождений переменной z_q выражение H_q, получим

$$H \equiv h(H_1, \dots, H_{q-1}, 0) \oplus H_q. \qquad (38)$$

Функцию, реализуемую формулой $h(H_1, \dots, H_{q-1}, 0)$, обозначим через φ. Предположим, что функция φ линейна. Каждая из субформул $H_1, \dots, H_{q-1}$ содержит по одной переменной, поэтому существует такая линейная функция Λ, что

$$h(H_1, \dots, H_{q-1}, 0) \equiv \Lambda(H_1, \dots, H_{q-1}, 0). \qquad (39)$$

Пусть $\Lambda \equiv a_1x_1 \oplus \dots \oplus a_qx_q \oplus a_0$. Рассмотрим линейную функцию Λ' от q аргументов, задаваемую тождеством $\Lambda' \equiv a_1x_1 \oplus \dots \oplus a_{q-1}x_{q-1} \oplus x_q \oplus a_0$. Тогда из (38) и (39) следует $H \equiv \Lambda'(H_1, \dots, H_q)$, т. е. формула H не является ν-формулой, а это противоречит условию леммы.

Таким образом, функция φ нелинейна. Тогда существует переменная $z \in V(\varphi)$ и такая подстановка констант A, $V(A) = T\backslash\{z\}$, что функция $\varphi|_A$ тождественно равна константе. Мощность подстановки констант A не превосходит $p-1$, и каждая переменная из множества $V(A)$ входит в некоторое $\oplus_p$-выделимое множество переменных функции g, поэтому $V(g|_A) = V(g)\backslash V(A)$. Отсюда и из условия $z \notin T$

следует $z \in V(g|_A)$. Пусть σ — такая константа, что $\varphi|_A \equiv \sigma$. Положим $H' = \neg(\neg(H_q|_A))$ при $\sigma = 0$, $H' = \neg(H_q|_A)$ при $\sigma = 1$. В любом случае, $L_z(H') < L_z(H|_A)$. Отсюда видно, что функция g забивает формулу H в базисе $Б$ подстановкой A. Случай 2) рассмотрен.

Лемма 7 доказана.

Пусть $Б$ — произвольный базис, $p = \mathrm{nes}(Б)$. Скажем, что функция f *согласована* с базисом $Б$, если выполнены следующие 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 — функция, m, s — натуральные числа, $s \leqslant m$, g — подфункция функции $f^{(m)}$. Далее, пусть F — произвольная ν-формула, 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.

Пусть F является ν_L^s-формулой и $F \mathrel{\underline{\circ}} f(F_1, \ldots, F_n)$. Субформула F_i, $1 \leqslant i \leqslant n$, формулы F называется ν_L^s*-центральной*, если ни одна подформула выражения F_i не является ν_L^s-формулой. Формула F называется μ_L^s*-формулой*, если все ее субформулы, за исключением, быть может, одной, являются ν_L^s-центральными.

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

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, $s \leqslant m$, и g — подфункция функции $f^{(m)}$. Далее, пусть $L = np^2$, H — приведенная μ^s_L-формула в базисе $Б$ и все переменные, входящие в H, существенны для g. Наконец, пусть Z — множество всех переменных, входящих в ν^s_L-центральные субформулы формулы H, 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 H в базисе $Б$ подстановкой констант A.

Доказательство. Пусть $H \mathrel{\underline{\circ}} h(H_1, \dots, H_q)$. Формула H является μ^s_L-формулой, поэтому все субформулы $H_1, \dots, H_q$ кроме, быть может, одной, являются ν^s_L-центральными. Рассмотрим два случая: 1) каждая из субформул $H_1, \dots, H_q$ является ν^s_L-центральной; 2) среди субформул $H_1, \dots, H_q$ ровно одна не является ν^s_L-центральной.

Случай 1). В этом случае $Z = V(H)$. Рассмотрим два случая: 1.1) формула H бесповторна; 1.2) формула H не бесповторна.

Случай 1.1). Формула H является ν^s_L-формулой и все переменные, входящие в H, являются s-регулярными. Поэтому $L(H) \geqslant L = np^2$. Тогда существует такая субформула H_{i_0}, $1 \leqslant i_0 \leqslant q$, что $L(H_{i_0}) \geqslant \frac{np^2}{q} \geqslant np$. Не ограничивая общность, будем считать, что $i_0 = q$. Рассмотрим произвольное i, $1 \leqslant i \leqslant q-1$. В силу приведенности формулы H, множество $V(H_i)$ непусто. Выберем произвольным образом переменную z_i, $z_i \in V(H_i)$. Обозначим через Z_i то 1-множество функции g, которое содержит переменную z_i. Тогда

$$\Big|\bigcup_{i=1}^{q-1} Z_i\Big| \leqslant n(q-1) < np.$$

В то же время, $L(H_q) \geqslant np$, поэтому существует переменная z_q, $z_q \in V(H_q)$, не принадлежащая ни одному из множеств $Z_1, \dots, Z_{q-1}$.

Итак, ни одна из переменных $z_1, \dots, z_{q-1}$ не принадлежит тому 1-множеству функции g, которому принадлежит переменная z_q. Обозначим $T = \bigcup\limits_{i=1}^{q-1} V(H_i)$. В силу приведенности и бесповторности формулы H, переменная z_q входит в H ровно один раз, следовательно, $z_q \notin T$. Функция f согласована с базисом $Б$, поэтому, если $Б$ линеен, то функция f является p-универсальной для базиса $Б$. В этом случае, в силу леммы 6, существует такая подстановка констант A, $V(A) \subseteq T$, что функция g забивает формулу H в базисе $Б$ подстановкой констант A. Если же базис $Б$ нелинеен, то каждая существенная переменная функции f входит в некоторое $\oplus_p$-выделимое множество переменных функции f. В этом случае, в силу леммы 7, существует такая подстановка констант A, $V(A) \subseteq T$, что функция g забивает ею формулу H в базисе $Б$. В то же время, $|A| \leqslant |T| \leqslant |Z| + np$, и A определена только на s-регулярных переменных функции g. Случай 1.1) рассмотрен.

Случай 1.2). Пусть переменная z входит в формулу H не меньше двух раз. Обозначим через A такую подстановку констант, что $V(A) = V(H)\backslash\{z\}$ и $z \in V(g|_A)$. Существует такая формула H' в базисе $Б$, что $H' \equiv H$, $V(H') \subseteq \{z\}$ и $L(H') \leqslant 1$. Очевидно, функция g забивает формулу H в базисе $Б$ подстановкой констант A. В то же время, $|A| \leqslant |Z| + np$, и A определена только на s-регулярных переменных функции g. Случай 1) рассмотрен.

Случай 2). Не ограничивая общность, будем считать, что субформула H_q не является ν_L^s-центральной. Обозначим $T = Z$. Тогда каждая переменная из множества T является s-регулярной для функции g. Для каждого i, $1 \leqslant i \leqslant q-1$, обозначим через z_i произвольную переменную из множества $V(H_i)$, а через Z_i — то 1-множество переменных функции g, которое содержит переменную z_i. Рассмотрим два случая: 2.1) хотя бы одна переменная из множества $V(H_q)$ не является s-регулярной; 2.2) все переменные из множества $V(H_q)$ являются s-регулярными.

Случай 2.1). Обозначим через z_q произвольную переменную из множества $V(H_q)$, которая не является s-регулярной. Тогда z_q не входит ни в одно из множеств $Z_1, \ldots, Z_{q-1}$. В то же время, $z_q \notin T$. Если базис $Б$ линеен, то применяем лемму 6, а если базис $Б$ нелинеен, то применяем лемму 7. В любом случае получим, что существует такая подстановка констант A, $V(A) \subseteq T$, что функция g забивает ею формулу H в базисе $Б$. Кроме того, $|A| < |T| = |Z| < |Z| + np$, и подстановка A определена только на s-регулярных переменных функции g. Случай 2.1) рассмотрен.

Случай 2.2). В этом случае все переменные, входящие в формулу H, являются s-регулярными для функции g. Рассмотрим два случая: 2.2.1) $|V(H_q)\backslash T| \geqslant np$; 2.2.2) $|V(H_q)\backslash T| < np$.

Случай 2.2.1). В этом случае $\left|\bigcup\limits_{i=1}^{q-1} Z_i\right| < np$, поэтому существует переменная z_q, $z_q \in V(H_q)\backslash T$, не входящая ни в одно из множеств $Z_1, \ldots, Z_{q-1}$. Если базис $Б$ линеен, то применяем лемму 6, а если базис $Б$ нелинеен, то применяем лемму 7. В любом случае получим, что существует такая подстановка констант A, $V(A) \subseteq T$, что функция g забивает ею формулу H в базисе $Б$. Тогда $|A| < |T| = |Z| < |Z| + np$ и подстановка A определена только на s-регулярных переменных функции g. Случай 2.2.1) рассмотрен.

Случай 2.2.2). Субформула H_q не является ν_L^s-центральной, поэтому существует подформула формулы H_q, являющаяся ν_L^s-формулой. Пусть H^* — минимальная по включению формула среди всех подформул формулы H^*, являющихся ν_L^s-формулами. Тогда каждая субформула формулы H^* является ν_L^s-центральной. Применив к H^* рассуждения случая 1), получим, что существует такая подстановка констант A, $V(A) \subseteq V(H^*)$, что функция g забивает ею формулу H^* в базисе $Б$. Тогда g забивает формулу H в базисе $Б$ подстановкой A. В то же время выполнено $|A| \leqslant |V(H^*)| \leqslant |V(H_q)| \leqslant |T| + np = |Z| + np$. Случай 2) рассмотрен.

Лемма 8 доказана.

§5. Ранг функции.

Рангом функции f называется наименьшее целое число r, для которого существует функция ψ и существуют такие линейные функции $\Lambda_1, \ldots, \Lambda_r$, что выполнено тождество

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

Ранг функции f обозначим $r(f)$.

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

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

Тогда

$$r(g) \geqslant 2k.$$

Доказательство. Предположим противное, т. е. $r(g) < 2k$. Обозначим $r = r(g)$. В силу определения ранга, существует функция ψ и такие линейные функции $\Lambda_1, \ldots, \Lambda_r$, что $g \equiv \psi(\Lambda_1, \ldots, \Lambda_r)$. Рассмотрим матрицу M с r строками и $n+2k$ столбцами, на пересечении i-й строки j-го столбца которой стоит коэффициент линейной функции Λ_i при переменной x_j. Строки матрицы M линейно независимы (в противном случае, если бы какая-то линейная функция Λ_{i_0} линейно выражалась через остальные, то существовала бы такая функция ψ_1, что $g \equiv \psi_1(\Lambda_1, \ldots, \Lambda_{i_0-1}, \Lambda_{i_0+1}, \ldots, \Lambda_r)$ и, тем самым, мы бы имели $r(g) < r$). Таким образом, ранг матрицы M равен r. Поэтому в матрице M существует невырожденная подматрица M_1 размера $r \times r$. Пусть Z — множество переменных, соответствующих столбцам матрицы M_1. По нашему предположению, $|Z| < 2k$, поэтому в множестве $\{x_1, \ldots, x_{2k}\}$ существует переменная, не входящая в множество Z. Не ограничивая общность, будем считать, что $x_1 \notin Z$.

Рассмотрим переменную x_2. Она существенна хотя бы для одной из функций $\Lambda_1, \ldots, \Lambda_r$. Не ограничивая общность, будем считать, что она существенна для функции Λ_1. Обозначим через a_i, $2 \leqslant i \leqslant r$, коэффициент линейной функции Λ_i при переменной x_2. Положим $\Lambda'_1 = \Lambda_1$ и $\Lambda'_i = \Lambda_i \oplus a_i\Lambda_1$, $i = 2, \ldots, r$. Пусть $\psi'(x_1, x_2, \ldots, x_r) \equiv \psi(x_1, x_2 \oplus a_2x_1, \ldots, x_r \oplus a_rx_1)$. Тогда

$$g \equiv \psi'(\Lambda'_1, \ldots, \Lambda'_r), \tag{40}$$

причем $\Lambda'_1, \ldots, \Lambda'_r$ — линейные функции и ни одна из функций $\Lambda'_2, \ldots, \Lambda'_r$ существенно не зависит от переменной x_2.

Функция ψ' существенно зависит от переменной x_1, поэтому существуют такие константы $b_2, \ldots, b_r$, что функция $\psi'(x_1, b_2, \ldots, b_r)$ существенно зависит от x_1. Положим $b_1 = 0$ и рассмотрим систему линейных уравнений

$$\Lambda'_i(x_1, \ldots, x_{n+2k}) = b_i, \quad i = 1, \ldots, r. \tag{41}$$

Заметим, что матрица M' этой системы получается из матрицы M невырожденным линейным преобразованием строк, поэтому ранг матрицы M' равен r, а значит система (41) совместна. Более того, подматрица M'_1 матрицы M', образованная теми ее столбцами, которые соответствуют переменным из множества Z, невырождена, так как получается тем же невырожденным преобразованием строк из матрицы M_1. Следовательно, чтобы получить решение системы (41), достаточно произвольно выбрать значения всех переменных, не входящих в множество Z, а из системы найти значения переменных, входящих в множество Z.

Переменная x_1 не входит в множество Z. Ее значение положим равным той константе c_1, для которой функция $\varphi(c_1, x_2)$ не зависит от переменной x_2 (это всегда можно сделать, так как φ — нелинейная функция двух аргументов). Значения остальных переменных, не входящих в множество Z, положим равными нулю, и из системы (41) найдем значения переменных, входящих в множество Z. Полученное решение системы (41) обозначим через $\tilde{c} = (c_1, \dots, c_{n+2k})$. Из условия леммы, (40) и (41) следует цепочка тождеств

$$\theta(\varphi(c_1, x_2), \varphi(c_3, c_4), \dots, \varphi(c_{2k-1}, c_{2k}), c_{2k+1}, \dots, c_{n+2k}) \equiv$$
$$\equiv g(c_1, x_2, c_3, \dots, c_{n+2k}) \equiv$$
$$\equiv \psi'(\Lambda'_1(c_1, x_2, c_3, \dots, c_{n+2k}), \Lambda'_2(\tilde{c}), \dots, \Lambda'_r(\tilde{c})) \equiv$$
$$\equiv \psi'(x_2 \oplus c_2 \oplus b_1, b_2, \dots, b_r).$$

В то же время функция, выражаемая формулой

$$\theta(\varphi(c_1, x_2), \varphi(c_3, c_4), \dots, \varphi(c_{2k-1}, c_{2k}), c_{2k+1}, \dots, c_{n+2k}),$$

тождественно равна константе, а функция, выражаемая формулой

$$\psi'(x_2 \oplus c_2 \oplus b_1, b_2, \dots, b_r),$$

существенно зависит от переменной x_2. Противоречие.

Лемма 9 доказана.

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

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

Доказательство. Пусть $Z_1, \dots, Z_t$ — все регулярные 1-множества функции g, $\tilde{y}$ — набор, состоящий из всех существенных переменных функции g, не являющихся 1-регулярными. Представим функцию g в виде

$$g \equiv \theta(f_1, \ldots, f_t, \tilde{y}),$$

где функции $f_1, \ldots, f_t$ могут быть получены из f биективной заменой переменных, $V(f_1) = Z_1, \ldots, V(f_t) = Z_t$.

Функция f нелинейна, поэтому существует подфункция φ функции f, являющаяся нелинейной функцией двух аргументов. Таким образом, для любого i, $1 \leqslant i \leqslant t$, существуют переменные x_{j_i} и x_{k_i} и существует такая подстановка констант A_i, $V(A_i) = Z_i \setminus \{x_{j_i}, x_{k_i}\}$, что $f_i|_{A_i} \equiv \varphi(x_{j_i}, x_{k_i})$. Положим $A = \bigcup\limits_{i=1}^{t} A_i$. Тогда

$$g|_A \equiv \theta(\varphi(x_{j_1}, x_{k_1}), \ldots, \varphi(x_{j_t}, x_{k_t}), \tilde{y}).$$

По лемме 9 имеем $r(g|_A) \geqslant 2t$. Очевидно, что $r(g) \geqslant r(g|_A)$. Окончательно имеем

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

Лемма 10 доказана.

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

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

Доказательство. Вначале рассмотрим случай, когда формула G является ν-формулой. В этом случае индукцией по $\nu(G)$ докажем, что

$$\nu(G) \geqslant \frac{1}{\mathrm{nes}(Б)} r(g). \tag{42}$$

Базис индукции: $\nu(G) = 1$. Пусть $G \mathrel{\underline{\circ}} h(H_1, \ldots, H_t)$. При каждом i, $1 \leqslant i \leqslant t$, субформула H_i не содержит ν-формул и, следовательно, реализует линейную функцию, которую мы обозначим через Λ_i. Тогда $g \equiv h(\Lambda_1, \ldots, \Lambda_t)$, а значит, $r(g) \leqslant t$. Отсюда имеем

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

Индуктивный переход: для всех таких ν-формул G', что $\nu(G') < \nu(G)$, неравенство (42) доказано. Пусть $G \mathrel{\overline{\circ}} h(H_1, \dots, H_t)$.

Рассмотрим произвольное i, $1 \leqslant i \leqslant t$. Обозначим через $H_i^1, \dots, H_i^{k_i}$ все различные формулы, максимальные по включению в множестве подформул формулы H_i, являющихся ν-формулами (возможно, $k_i = 0$), а через $\tilde{x}_i$ — набор, состоящий из всех переменных, хотя бы одно вхождение которых содержится в субформуле H_i вне каждой из формул $H_i^1, \dots, H_i^{k_i}$. Пусть h_i — функция, реализуемая субформулой H_i, h_i^j, $j = 1, \dots, k_i$, — функция, реализуемая формулой H_i^j.

Если подформула H' выражения H_i не содержится ни в одной из формул $H_i^1, \dots, H_i^{k_i}$, то H' не является ν-формулой. В этом случае внешнюю функцию формулы H' можно заменить линейной функцией так, чтобы полученная формула реализовывала ту же функцию, что и формула H'. Поэтому существуют такие линейные функции Λ_i^1 и Λ_i^2, что

$$h_i \equiv \Lambda_i^1(h_i^1, \dots, h_i^{k_i}) \oplus \Lambda_i^2(\tilde{x}_i).$$

Отсюда следует

$$r(h_i) \leqslant \sum_{j=1}^{k_i} r(h_i^j) + 1. \tag{43}$$

Для любого j, $1 \leqslant j \leqslant k_i$, по предположению индукции для формулы H_i^j, имеем

$$\nu(H_i^j) \geqslant \frac{1}{\mathrm{nes}(Б)} r(h_i^j).$$

Отсюда и из (43) следует

$$\nu(H_i) = \sum_{j=1}^{k_i} \nu(H_i^j) \geqslant \frac{1}{\mathrm{nes}(Б)} \sum_{j=1}^{k_i} r(h_i^j) \geqslant \frac{1}{\mathrm{nes}(Б)} (r(h_i) - 1). \tag{44}$$

Далее, в силу тождества $g \equiv h(h_1, \dots, h_t)$, имеем

$$r(g) \leqslant \sum_{i=1}^{t} r(h_i),$$

откуда, с учетом (44) и неравенства $t \leqslant \mathrm{nes}(Б)$, заключаем

$$\nu(G) = \sum_{i=1}^{t} \nu(H_i) + 1 \geqslant \frac{1}{\mathrm{nes}(Б)} \sum_{i=1}^{t} (r(h_i) - 1) + 1 = \\ = \frac{1}{\mathrm{nes}(Б)} \sum_{i=1}^{t} r(h_i) + 1 - \frac{t}{\mathrm{nes}(Б)} \geqslant \frac{1}{\mathrm{nes}(Б)} r(g).$$

Индукция проведена и (42) справедливо.

Перейдем теперь к доказательству леммы.

Обозначим через $H^1, \ldots, H^k$ все различные формулы, максимальные по включению в множестве всех подформул формулы G, являющихся ν-формулами (возможно, $k = 0$), а через $\tilde{x}$ — набор, состоящий из всех переменных, хотя бы одно вхождение которых содержится в формуле G вне каждой из формул $H^1, \ldots, H^k$. Пусть h^j, $j = 1, \ldots, k$, — функция, реализуемая формулой H^j.

Если подформула H' формулы G не содержится ни в одной из формул $H^1, \ldots, H^k$, то H' не является ν-формулой. В этом случае внешнюю функцию формулы H' можно заменить линейной функцией так, чтобы полученная формула реализовывала ту же функцию, что и формула H'. Поэтому существуют такие линейные функции Λ^1 и Λ^2, что

$$g \equiv \Lambda^1(h^1, \ldots, h^k) \oplus \Lambda^2(\tilde{x}).$$

Отсюда следует

$$r(g) \leqslant \sum_{j=1}^{k} r(h^j) + 1. \tag{45}$$

Из (42) следует

$$\nu(H^j) \geqslant \frac{1}{\mathrm{nes}(Б)} r(h^j), \quad j = 1, \ldots, k.$$

Отсюда и из (45) окончательно получим

$$\nu(G) = \sum_{j=1}^{k} \nu(H^j) \geqslant \frac{1}{\mathrm{nes}(Б)} \sum_{j=1}^{k} r(h^j) \geqslant \frac{1}{\mathrm{nes}(Б)} (r(g) - 1).$$

Лемма 11 доказана.

§6. Оценка количества μ_L^s-подформул.

Пусть G — произвольная формула и P — произвольное подмножество множества подформул формулы G. Определим подмножество μP множества P следующим образом: формула H, $H \in P$, принадлежит множеству μP тогда и только тогда, когда никакая субформула формулы H, 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

$$|\mu P| \geqslant \frac{1}{2}|P|. \tag{46}$$

Доказательство. Если $|P| = 0$, то неравенство (46) выполнено. В случае, если $|P| \geqslant 1$, индукцией по $|P|$ докажем неравенство

$$|\mu P| \geqslant \frac{1}{2} + \frac{1}{2}|P|, \tag{47}$$

из которого следует (46).

Базис индукции: $|P| = 1$. Пусть H, $H \mathrel{\overline{\underline{\circ}}} h(H_1, \ldots, H_t)$, — та подформула формулы G, которая принадлежит множеству P. Ни одна из субформул $H_1, \ldots, H_t$ не содержит подформул, принадлежащих множеству P, поэтому $H \in \mu P$, следовательно

$$|\mu P| = 1 = \frac{1}{2} + \frac{1}{2} = \frac{1}{2} + \frac{1}{2}|P|.$$

Индуктивный переход: для всех таких G' и P', что $|P'| < |P|$, неравенство (47) доказано. Пусть $G \mathrel{\overline{\underline{\circ}}} h(G_1, \ldots, G_t)$ и, для определенности, субформулы $G_1, \ldots, G_k$ содержат подформулы, принадлежащие множеству P (и, следовательно, $G_1, \ldots, G_k$ являются формулами), а $G_{k+1}, \ldots, G_t$ таковых не содержат. Для каждого i, $1 \leqslant i \leqslant k$, обозначим через P_i пересечение множества P с множеством подформул формулы G_i. К формуле G_i, $i = 1, \ldots, k$, применимо предположение индукции, согласно которому имеем

$$|\mu P_i| \geqslant \frac{1}{2} + \frac{1}{2}|P_i|. \tag{48}$$

Рассмотрим три случая: 1) $G \in \mu P$; 2) $G \in P$ и $G \notin \mu P$; 3) $G \notin P$.

Случай 1). В этом случае $0 \leqslant k \leqslant 1$. Отсюда и из (48) имеем

$$|\mu P| = 1 + \sum_{i=1}^{k} |\mu P_i| \geqslant 1 + \frac{k}{2} + \frac{1}{2}\sum_{i=1}^{k} |P_i| \geqslant 1 + \frac{1}{2}\sum_{i=1}^{k} |P_i| =$$
$$= \frac{1}{2} + \frac{1}{2}\Big(1 + \sum_{i=1}^{k} |P_i|\Big) = \frac{1}{2} + \frac{1}{2}|P|.$$

Случай 2). В этом случае $k \geqslant 2$. С учетом (48), имеем

$$|\mu P| = \sum_{i=1}^{k} |\mu P_i| \geqslant \frac{k}{2} + \frac{1}{2}\sum_{i=1}^{k} |P_i| \geqslant 1 + \frac{1}{2}\sum_{i=1}^{k} |P_i| =$$
$$= \frac{1}{2} + \frac{1}{2}\Big(1 + \sum_{i=1}^{k} |P_i|\Big) = \frac{1}{2} + \frac{1}{2}|P|.$$

Случай 3). Мы доказываем (47) в предположении $|P| \geqslant 1$. Поэтому из условия $G \notin P$ следует, что хотя бы одна из субформул $G_1, \ldots, G_t$ содержит подформулу, принадлежащую множеству P, а значит, $k \geqslant 1$. Используя (48), имеем

$$|\mu P| = \sum_{i=1}^{k} |\mu P_i| \geqslant \frac{k}{2} + \frac{1}{2}\sum_{i=1}^{k} |P_i| \geqslant \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{k} |P_i| = \frac{1}{2} + \frac{1}{2}|P|.$$

Индукция проведена.

Лемма 12 доказана.

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

$$n^s \geqslant 2L^2 n^2 pk. \tag{49}$$

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

$$\mu_L^s(G) \geqslant \frac{1}{8L^2n^4p^2k} R_s(g). \tag{50}$$

Доказательство. Рассмотрим множество

$$W = \left\{t \mid t \in \mathbb{N},\, n^t \geqslant 2L^2n^2pk\right\}.$$

В силу (49), множество W непусто, поэтому существует $w = \min W$. Тогда

$$w \leqslant s, \qquad n^w \geqslant 2L^2n^2pk, \qquad n^{w-1} < 2L^2n^2pk. \tag{51}$$

Рассмотрим множество всех подформул формулы G, являющихся ν-формулами, но не являющихся ν_L^s-формулами. Обозначим через $H_1, \ldots, H_t$ все различные максимальные по включению формулы из этого множества. Пусть M — множество всех s-регулярных переменных функции g. Обозначим через $M_1, \ldots, M_r$ все различные регулярные $(w-1)$-множества функции g, являющиеся подмножествами множества M (заметим, что $w \geqslant 2$). Для любых переменных $y_1 \in M, \ldots, y_q \in M$ обозначим через $R(y_1, \ldots, y_q)$ количество тех формул среди $H_1, \ldots, H_t$, которые содержат не менее двух различных переменных из множества $\{y_1, \ldots, y_q\}$. Тогда

$$R(y_1, \ldots, y_q) \leqslant \sum_{1 \leqslant i,j \leqslant q} R(y_i, y_j). \tag{52}$$

Формула H_i, $1 \leqslant i \leqslant t$, является ν-формулой, но не является ν_L^s-формулой, поэтому H_i содержит только переменные из множества M и $L(H_i) \leqslant L$. Кроме того, каждая переменная из множества M входит не более, чем в k формул среди $H_1, \ldots, H_t$. Отсюда следует

$$\sum_{y \in M, z \in M} R(y,z) = \sum_{y \in M} \sum_{z \in M} R(y,z) \leqslant \sum_{y \in M} \sum_{i, y \in V(H_i)} |V(H_i)| \leqslant$$
$$\leqslant \sum_{y \in M} L \cdot |\{i \mid y \in V(H_i)\}| \leqslant \sum_{y \in M} Lk = |M|Lk. \tag{53}$$

Заметим, что $|M_1| = \ldots = |M_r|$. Используя (52) и (53), получим

$$\sum_{y_1 \in M_1, \ldots, y_r \in M_r} R(y_1, \ldots, y_r) \leqslant \sum_{y_1 \in M_1, \ldots, y_r \in M_r} \; \sum_{1 \leqslant i,j \leqslant r} R(y_i, y_j) =$$
$$= \sum_{1 \leqslant i,j \leqslant r} \; \sum_{y_1 \in M_1, \ldots, y_r \in M_r} R(y_i, y_j) =$$
$$= \sum_{1 \leqslant i,j \leqslant r} \; \sum_{y_i \in M_i, y_j \in M_j} R(y_i, y_j) \cdot |M_1|^{r-2} =$$
$$= \sum_{y \in M, z \in M} R(y, z) \cdot |M_1|^{r-2} \leqslant |M| Lk \cdot |M_1|^{r-2}. \quad (54)$$

Мощность множества $M_1 \times \ldots \times M_r$ равна $|M_1|^r$, поэтому из (54) следует, что среднее значение величины $R(y_1, \ldots, y_r)$ при $y_1 \in M_1, \ldots, y_r \in M_r$ не больше, чем $|M| Lk / |M_1|^2$. Тогда существуют такие переменные $y_1' \in M_1, \ldots, y_r' \in M_r$, что

$$R(y_1', \ldots, y_r') \leqslant \frac{|M| Lk}{|M_1|^2} =$$

(заметим, что $|M_1| = n^{w-1}$, $|M| = R_s(g)$)

$$= \frac{Lk}{n^{2w-2}} R_s(g). \quad (55)$$

Пусть $H_{d(1)}, \ldots, H_{d(l)}$ — все различные формулы из множества $\{H_1, \ldots, H_t\}$, каждая из которых содержит хотя бы две различные переменные из множества $\{y_1', \ldots, y_r'\}$. Тогда $l = R(y_1', \ldots, y_r')$. Обозначим через R' множество, состоящее из всех подформул формул $H_{d(1)}, \ldots, H_{d(l)}$, которые являются ν-формулами. Заметим, что для любой формулы F справедливо $\nu(F) \leqslant L(F) - 1$ (это несложно доказать индукцией по $L(F)$ использовав тот факт, что если F является ν-формулой, то хотя бы две субформулы формулы F имеют сложность, не меньшую единицы). Кроме того, сложность каждой из формул $H_{d(1)}, \ldots, H_{d(l)}$ меньше, чем L (ни одна из них не является ν_L^s-формулой). Отсюда и из (55) следует

$$|R'| = \sum_{j=1}^{l} \nu(H_{d(j)}) \leqslant \sum_{j=1}^{l} (L(H_{d(j)}) - 1) \leqslant$$
$$\leqslant L \cdot l = L \cdot R(y'_1, \ldots, y'_r) \leqslant \frac{kL^2}{n^{2w-2}} R_s(g). \quad (56)$$

Представим функцию g в виде

$$g \equiv f^{(m-w+1)}(g_1, \ldots, g_{n^{m-w+1}}),$$

где функция g_i, $1 \leqslant i \leqslant n^{m-w+1}$, получается заменой переменных из некоторой подфункции функции $f^{(w-1)}$, множества $V(g_1), \ldots, V(g_{n^{m-w+1}})$ являются $(w-1)$-множествами переменных функции g и попарно не пересекаются. Рассмотрим произвольное i, $1 \leqslant i \leqslant n^{m-w+1}$. Если множество $V(g_i)$ пусто, то положим $A_i = \varnothing$, Рассмотрим теперь произвольное i, для которого множество $V(g_i)$ непусто. Если множество $V(g_i)$ присутствует среди множеств $M_1, \ldots, M_r$, а именно, $V(g_i) = M_j$, то положим $z_i = y'_j$. Если множество $V(g_i)$ не присутствует среди множеств $M_1, \ldots, M_r$, то в качестве z_i возьмем произвольную переменную из множества $V(g_i)$. Переменная z_i существенна для функции g, поэтому существует такая подстановка констант A_i, $V(A_i) = V(g_i) \backslash \{z_i\}$, и такая константа σ_i, что $g_i|_{A_i} \equiv z_i \oplus \sigma_i$. Положим

$$A = \bigcup_{i=1}^{n^{m-w+1}} A_i.$$

Каждой подформуле H формулы G поставим в соответствие подформулу H' формулы $G|_A$, в которую переходит формула H при действии подстановки констант A. Если формула H не является ν-формулой, то и формула H' не является ν-формулой. Рассмотрим произвольную формулу H, которая является ν-формулой, не является ν_L^s-формулой и не принадлежит множеству R'. Тогда H содержит только s-регулярные переменные. Подстановка A определена, в частности, на всех s-регулярных переменных функции g, не вошедших в множество $\{y'_1, \ldots, y'_r\}$, поэтому $V(H') \subseteq \{y'_1, \ldots, y'_r\}$. Кроме того, $H \notin R'$, поэтому $V(H') \leqslant 1$. Пусть $H' \mathrel{\overline{\circ}} h(H_1, \ldots, H_q)$. Функции, реализуемые формулой H' и ее субформулами, существенно зависят не более, чем от одной, общей для них всех, переменной. Поэтому существует такая линейная функция Λ, что $\Lambda(H_1, \ldots, H_q) \equiv H'$, т. е. формула H' не является ν-формулой. Итак, если формула H' является ν-формулой, то формула H либо принадлежит множеству R', либо является ν_L^s-формулой для функции g. Отсюда следует

$$\nu_L^s(G) \geqslant \nu(G|_A) - |R'|. \tag{57}$$

Функция $g|_A$ существенно зависит от всех переменных z_i (для тех i, для которых z_i определена), и только от них. Обозначим через g' функцию, полученную из $g|_A$ заменой каждой переменной z_i на соответствующую переменную x_i и навешиванием отрицаний на те переменные x_i, для которых $\sigma_i = 1$. Функция g' является подфункцией функции $f^{(m-w+1)}$, причем, если переменная z_i является w-регулярной для функции g, то переменная x_i является 1-регулярной для функции g'. Каждая переменная из множества $\{y'_1, \ldots, y'_r\}$ является w-регулярной для функции g, поэтому

$$R_1(g') \geqslant r = \frac{R_s(g)}{n^{w-1}}. \tag{58}$$

В силу обобщенной однотипности функций $\langle g' \rangle$ и $\langle g|_A \rangle$ имеем

$$r(g') = r(g|_A). \tag{59}$$

Если $R_s(g) = 0$, то неравенство (50) справедливо. Рассмотрим теперь случай, когда $R_s(g) > 0$. В этом случае, в силу оценки (58), имеем $R_1(g') > 0$. Кроме того, по условию леммы, функция f нелинейна, поэтому функция g' нелинейна, а значит, функция $g|_A$ нелинейна. Тогда $r(g|_A) \geqslant 2$. Применив к функции $g|_A$ и формуле $G|_A$ лемму 11 и использовав неравенство $r(g|_A) \geqslant 2$, получим

$$\nu(G|_A) \geqslant \frac{1}{\mathrm{nes}(Б \cup \{0,1\})}(r(g|_A) - 1) = \frac{1}{\mathrm{nes}(Б)}(r(g|_A) - 1) \geqslant$$
$$\geqslant \frac{1}{2\,\mathrm{nes}(Б)} r(g|_A) = \frac{1}{2p} r(g|_A). \quad (60)$$

Применив к функции g' лемму 10 (в силу нелинейности функции f), получим

$$r(g') \geqslant \frac{2}{\mathrm{nes}(f)} R_1(g') = \frac{2}{n} R_1(g'). \quad (61)$$

Обозначим через P множество, состоящее из всех подформул формулы G, являющихся ν_L^s-формулами. Заметим, что множество μP состоит из всех подформул формулы G, являющихся μ_L^s-формулами. Применив лемму 12, получим

$$\mu_L^s(G) = |\mu P| \geqslant \frac{1}{2}|P| = \frac{1}{2}\nu_L^s(G). \quad (62)$$

Далее, из (60), (59), (61) и (58) следует

$$\nu(G|_A) \geqslant \frac{1}{2p} r(g|_A) = \frac{1}{2p} r(g') \geqslant \frac{1}{np} R_1(g') \geqslant \frac{1}{n^w p} R_s(g). \quad (63)$$

Наконец, из (62), (57), (63), (56), второго и третьего соотношений в (51), получим

$$\mu_L^s(G) \geqslant \frac{1}{2}\nu_L^s(G) \geqslant \frac{1}{2}(\nu(G|_A) - |R'|) \geqslant \frac{1}{2}\left(\frac{1}{n^w p} - \frac{L^2 k}{n^{2w-2}}\right) R_s(g) =$$
$$= \frac{n^{w-2} - L^2 pk}{2n^{2w-2} p} R_s(g) > \frac{2L^2 pk - L^2 pk}{8L^4 n^4 p^3 k^2} R_s(g) = \frac{1}{8L^2 n^4 p^2 k} R_s(g),$$

т. е. оценка (50) справедлива.

Лемма 13 доказана.

ГЛАВА III. НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ ФУНКЦИЙ

§7. Основная лемма.

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

$$u^s \geqslant 99 n^6 p^6 (M_Б(f^{(m)}))^2. \tag{64}$$

Тогда

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

Доказательство. Рассмотрим формулу F в базисе $Б$, реализующую функцию $f^{(m)}$ и имеющую сложность $L(F) = L_Б(f^{(m)})$. Обозначим $k = M_Б(f^{(m)})$. Тогда

$$L(F) = kn^m. \tag{65}$$

Пусть $W_1, \ldots, W_a$ — все различные s-множества функции $f^{(m)}$, каждое из которых содержит две переменные, входящие в формулу F различное число раз. Обозначим

$$T = \max\left\{0, \left\lceil \frac{n^{m-s} - 6a}{6n^s} \right\rceil \right\}. \tag{66}$$

Для каждого t, $t = 0, 1, \ldots, T$, построим подфункцию g_t функции $f^{(m)}$ и формулу G_t в базисе $Б$, реализующую функцию g_t так, чтобы выполнялись условия (67), (68) и (69).

$$\begin{gathered}\text{функция } g_t \text{ является } (s, v_t)\text{-подфункцией функции } f^{(m)}\\ \text{и } v_t \leqslant n^s t + a + \frac{1}{3} n^{m-s};\end{gathered} \tag{67}$$

$$\begin{gathered}\text{для любого } s\text{-специального множества } Y \text{ функции } g_t\\ \text{выполняется } L_Y(G_t) \leqslant kn^{m-s} - \frac{a}{n^s} - t;\end{gathered} \tag{68}$$

$$\begin{gathered}\text{каждая } s\text{-регулярная переменная входит в формулу } G_t\\ \text{не более, чем } 3k \text{ раз.}\end{gathered} \tag{69}$$

Построение будем вести индукцией по t.

Базис индукции (Построение g_0 и G_0). Обозначим через $W_{a+1},\dots,W_{a+b}$ все различные s-множества функции $f^{(m)}$, не входящие в список $W_1,\dots,W_a$, каждое из которых содержит переменную, входящую в формулу F больше, чем $3k$ раз. Тогда

$$L(F) \geqslant \sum_{i=a+1}^{a+b} L_{W_i}(F) \geqslant \sum_{i=a+1}^{a+b} 3kn^s = 3kn^s b.$$

Отсюда и из (65) следует

$$b \leqslant \frac{L(F)}{3kn^s} = \frac{kn^m}{3kn^s} = \frac{1}{3}n^{m-s}. \tag{70}$$

В множестве W_i, $1 \leqslant i \leqslant a+b$, выберем переменную y_i так, чтобы число ее вхождений в формулу F не превосходило числа вхождений в формулу F любой переменной из множества W_i. Обозначим через B такую подстановку констант, что $V(B) = \bigcup_{i=1}^{a+b}(W_i \backslash \{y_i\})$ и функция $f^{(m)}|_B$ существенно зависит от переменных $y_1,\dots,y_{a+b}$. Положим $g_0 = f^{(m)}|_B$. Тогда функция g_0 является (s,v_0)-подфункцией функции $f^{(m)}$, где $v_0 = a+b$. Используя (70), получим

$$v_0 = a+b \leqslant a + \frac{1}{3}n^{m-s} = n^s \cdot 0 + a + \frac{1}{3}n^{m-s}.$$

Таким образом, (67) выполнено.

Обозначим через G_0 формулу $F|_B$. Рассмотрим произвольное s-специальное множество Y функции g_0. Множество Y содержит, в частности, переменные $y_1,\dots,y_a$. Множество W_i, $1 \leqslant i \leqslant a$, содержит переменную, входящую в формулу F большее число раз, чем $L_{y_i}(F)$, поэтому

$$L_{W_i}(F) \geqslant n^s L_{y_i}(F) + 1, \qquad i = 1,\dots,a. \tag{71}$$

Обозначим через $W_{a+b+1},\dots,W_{n^{m-s}}$ все различные s-множества функции $f^{(m)}$, не вошедшие в список $W_1,\dots,W_{a+b}$. Пусть переменная y_i, $a+b+1 \leqslant i \leqslant n^{m-s}$, одновременно входит в множество Y и в множество W_i. Если $a+1 \leqslant i \leqslant n^{m-s}$, то все переменные из множества W_i входят в формулу F одинаковое число раз, поэтому

$$L_{W_i}(F) = n^s L_{y_i}(F), \qquad i = a+1, \ldots, n^{m-s}. \tag{72}$$

Просуммировав (71) и (72) по всем i, $i = 1, \ldots, n^{m-s}$, получим

$$L(F) = \sum_{i=1}^{n^{m-s}} L_{W_i}(F) \geqslant n^s \sum_{i=1}^{n^{m-s}} L_{y_i}(F) + a = n^s L_Y(F) + a.$$

Отсюда, с учетом (65), получим

$$L_Y(G_0) = L_Y(F) \leqslant \frac{1}{n^s}(L(F) - a) = \frac{1}{n^s}(kn^m - a) = kn^{m-s} - \frac{a}{n^s} - 0.$$

Таким образом, (68) выполнено.

Наконец, каждая s-регулярная переменная функции g_0 входит в одно из множеств $W_{a+b+1}, \ldots, W_{n^{m-s}}$, а все переменные из этих множеств входят в формулу F не больше, чем $3k$ раз. Поэтому каждая s-регулярная переменная функции g_0 входит в формулу G_0 не больше, чем $3k$ раз. Условие (69) также выполнено. Функция g_0 и формула G_0 построены.

Пусть функция g_t и формула G_t уже построены.

Индуктивный переход (Построение g_{t+1} и G_{t+1}). Согласно утверждению 3, существует такая приведенная формула G_t' в базисе *Б*, что $G_t' \equiv G_t$ и число вхождений каждой переменной в формулу G_t' не больше числа ее вхождений в формулу G_t. Положим

$$L = np^2, \qquad R = 97n^6p^6k^2. \tag{73}$$

Обозначим через μ_t множество, состоящее из всех подформул H формулы G_t', являющихся μ_L^s-формулами и удовлетворяющих условиям

(74) и (75):

$$\begin{gathered}\text{все переменные, входящие в } \nu_L^s\text{-центральные}\\ \text{субформулы формулы } H,\\ \text{являются } s\text{-регулярными для функции } g_t;\end{gathered} \tag{74}$$

$$\begin{gathered}\text{количество различных переменных,}\\ \text{входящих в } \nu_L^s\text{-центральные}\\ \text{субформулы формулы } H\text{, не превосходит } R.\end{gathered} \tag{75}$$

Обозначим через μ_t^* $[\mu_t^{**}]$ множество всех подформул формулы G_t', являющихся μ_L^s-формулами и не удовлетворяющих условию (74) [(75)] соответственно. Тогда

$$|\mu_t| \geqslant \mu_L^s(G_t') - |\mu_t^*| - |\mu_t^{**}|. \tag{76}$$

В силу (64) и (73), имеем

$$n^s \geqslant u^s \geqslant 99n^6p^6k^2 \geqslant 6n^4p^5k = 6L^2n^2pk \geqslant 2L^2n^2p\cdot\lfloor 3k\rfloor.$$

Поэтому условие (49) из леммы 13 § 6 выполнено. Кроме того, в силу условия (69), каждая s-регулярная переменная функции g_t входит в формулу G_t (а значит, и в формулу G_t') не более $3k$ раз (а значит, не более $\lfloor 3k\rfloor$ раз). Тогда из леммы 13 и определения L в (73) следует

$$\mu_L^s(G_t') \geqslant \frac{1}{8L^2n^4p^2\cdot\lfloor 3k\rfloor}R_s(g_t) \geqslant \frac{1}{24n^6p^6k}R_s(g_t). \tag{77}$$

Оценим $R_s(g_t)$. Согласно условию (67), функция g_t является (s, v_t)-подфункцией функции $f^{(m)}$, причем $v_t \leqslant n^st + a + \frac{1}{3}n^{m-s}$. Тогда

$$R_s(g_t) = n^s(n^{m-s} - v_t) \geqslant \frac{2}{3}n^m - n^s(n^st + a). \tag{78}$$

Заметим, что $T \geqslant t+1$ и $t \geqslant 0$, поэтому $T > 0$, а значит, в силу (66), имеем

$$n^st + a \leqslant n^s(T-1) + a \leqslant n^s\cdot\frac{n^{m-s} - 6a}{6n^s} + a = \frac{1}{6}n^{m-s}.$$

Отсюда, из (77) и (78) следует

$$\mu_L^s(G_t') \geqslant \frac{1}{24n^6p^6k} \cdot \left(\frac{2}{3}n^m - n^s(n^s t + a)\right) \geqslant$$
$$\geqslant \frac{1}{24n^6p^6k} \cdot \frac{1}{2}n^m = \frac{n^m}{48n^6p^6k}. \quad (79)$$

Заметим, что если H_1 и H_2 — различные подформулы формулы G_t', являющиеся μ_L^s-формулами, то ни одна ν_L^s-центральная подформула формулы H_1 не пересекается ни с одной ν_L^s-центральной подформулой формулы H_2. Поэтому количество формул в множестве μ_t^{**} не больше, чем $L(G_t')/R$, т. е.

$$|\mu_t^{**}| \leqslant \frac{L(G_t')}{R}, \quad (80)$$

а количество формул в множестве μ_t^* не больше, чем суммарное число вхождений в формулу G_t' всех переменных, не являющихся s-регулярными для функции g_t. Пусть Y' — произвольное s-специальное множество функции g_t. Тогда множество Y' содержит все существенные переменные функции g_t, не являющиеся s-регулярными. В силу приведенности, формула G_t' не содержит переменных, несущественных для функции g_t. Отсюда следует

$$|\mu_t^*| \leqslant L_{Y'}(G_t'). \quad (81)$$

В силу условия (68), для любого s-специального множества Y функции g_t справедливо

$$L_Y(G_t) \leqslant kn^{m-s} - a/n^s - t \leqslant kn^{m-s}, \quad (82)$$

поэтому

$$L(G_t) \leqslant n^s \cdot kn^{m-s} = kn^m.$$

Отсюда и из (80) следует

$$|\mu_t^{**}| \leqslant \frac{L(G_t')}{R} \leqslant \frac{L(G_t)}{R} \leqslant \frac{kn^m}{R}. \quad (83)$$

В то же время, из (81) и (82) следует

$$|\mu_t^*| \leqslant L_{Y'}(G_t') \leqslant L_{Y'}(G_t) \leqslant \frac{kn^m}{n^s}. \tag{84}$$

Наконец, заметим, что (в силу (64) и (73)) $R < u^s \leqslant n^s$. Собирая вместе оценки (76), (79), (84) и (83), получим

$$|\mu_t| \geqslant \frac{n^m}{48n^6p^6k} - \frac{kn^m}{n^s} - \frac{kn^m}{R} \geqslant \frac{n^m}{48n^6p^6k} - \frac{2kn^m}{R} = \frac{n^m(R - 96n^6p^6k^2)}{48n^6p^6kR} =$$

(применяем (73))

$$= \frac{n^m n^6 p^6 k^2}{48n^6p^6kR} > 0.$$

Таким образом, множество μ_t непусто.

Пусть формула H принадлежит множеству μ_t. Обозначим через Z множество всех переменных, входящих в ν_L^s-центральные субформулы формулы H. Тогда из условий (74) и (75) следует, что множество Z содержит только s-регулярные переменные функции g_t и $|Z| \leqslant R$. Применив к формуле H лемму 8 из § 4, получим, что существует такая подстановка констант A_t, для которой $|A_t| \leqslant |Z| + np$, все переменные из множества $V(A_t)$ являются s-регулярными для функции g_t, и функция g_t забивает формулу H в базисе $Б$ подстановкой констант A_t. С учетом определения числа R в (73) и неравенства (64), получим

$$|A_t| \leqslant |Z| + np \leqslant R + np \leqslant 98n^6p^6k^2 < 99n^6p^6k^2 \leqslant u^s. \tag{85}$$

Функция g_t забивает формулу H в базисе $Б$ подстановкой констант A_t, поэтому (см. определение в § 4) существует такая переменная z и формула H' в базисе $Б$, что $z \in V(g_t|_{A_t})$, $H' \equiv H|_{A_t}$, каждая переменная входит в формулу H' не большее число раз, нежели в формулу $H|_{A_t}$ и

$$L_z(H') \leqslant L_z(H|_{A_t}) - 1. \tag{86}$$

Обозначим через G_t^* формулу, полученную из $G_t'|_{A_t}$ заменой подформулы $H|_{A_t}$ на подформулу H'. Тогда формула G_t^* реализует функцию $g_t|_{A_t}$, каждая переменная входит в формулу G_t^* не большее число раз, чем в формулу $G_t|_{A_t}$ и, в силу (86), имеем

$$L_z(G_t^*) \leqslant L_z(G_t|_{A_t}) - 1. \tag{87}$$

Обозначим через $W_1^t, \ldots, W_{r_t}^t$ все различные регулярные s-множества функции g_t, пересекающиеся с множеством $V(A_t)$. Рассмотрим произвольное i, $1 \leqslant i \leqslant r_t$. Множество W_i^t является $f^{(s)}$-выделимым для функции g_t. В силу леммы 2 из § 2, устойчивость функции $f^{(s)}$ не меньше, чем u^s. Кроме того, в силу (85), мощность множества $W_i^t \cap V(A_t)$ меньше, чем u^s. Отсюда следует, что существует переменная из множества W_i^t, существенная для функции $g_t|_{A_t}$. Переменная z существенна для функции $g_t|_{A_t}$. Если $z \in W_i^t$, то положим $z_i = z$. Иначе в качестве z_i возьмем произвольную переменную из множества W_i^t, существенную для функции $g_t|_{A_t}$. Если переменная z входит в одно из множеств $W_1^t, \ldots, W_{r_t}^t$, то положим $W_0^t = \varnothing$. Иначе в качестве W_0^t возьмем то s-множество функции g_t (не обязательно регулярное), которое содержит переменную z.

Существует такая подстановка констант B_t, что

$$V(B_t) = \Big(\bigcup_{i=0}^{r_t} W_i^t\Big) \backslash \big(V(A_t) \cup \{z, z_1, \ldots, z_{r_t}\}\big),$$

и функция $g_t|_{A_t \cup B_t}$ существенно зависит от переменных $z, z_1, \ldots, z_{r_t}$. Положим $g_{t+1} = g_t|_{A_t \cup B_t}$. Каждое s-множество функции g_{t+1} либо состоит из одной переменной, входящей в множество $\{z, z_1, \ldots, z_{r_t}\}$, либо является s-множеством функции g_t. Поэтому каждое s-множество функции g_{t+1} имеет мощность, равную либо 1, либо n^s, т. е. функция g_{t+1} является (s, v_{t+1})-подфункцией функции $f^{(m)}$. Число v_{t+1}

допускает следующую оценку (мы пользуемся предположением индукции (67), оценкой $r_t \leqslant u^s - 1$, которая вытекает из (85), и очевидным неравенством $u \leqslant n$)

$$v_{t+1} \leqslant v_t + r_t + 1 \leqslant n^s t + a + \frac{1}{3}n^{m-s} + (u^s - 1) + 1 \leqslant n^s(t+1) + a + \frac{1}{3}n^{m-s}.$$

Таким образом, условие (67) проверено.

Положим $G_{t+1} = G_t^*|_{B_t}$. Тогда G_{t+1} — формула в базисе $Б$ и G_{t+1} реализует функцию g_{t+1}. Рассмотрим произвольное s-специальное множество Y функции g_{t+1}. Тогда Y является s-специальным множеством функции g_t и Y содержит переменную z. Использовав предположение индукции (68) и (87), получим

$$L_Y(G_{t+1}) = L_Y(G_t^*) \leqslant L_Y(G_t'|_{A_t}) - 1 \leqslant \\ \leqslant L_Y(G_t) - 1 \leqslant kn^{m-s} - \frac{a}{n^s} - (t+1),$$

т. е. (68) выполнено. Наконец заметим, что любая s-регулярная переменная функции g_{t+1} является s-регулярной переменной функции g_t, следовательно, число ее вхождений в формулу G_t не больше, чем $3k$. Число вхождений каждой переменной в формулу G_{t+1} не больше числа ее вхождений в формулу G_t. Отсюда вытекает (69).

Индукция проведена.

Продолжим доказательство леммы. Мы построили функцию g_T и формулу G_T, для которых выполнены условия (67), (68) и (69). Рассмотрим произвольное s-специальное множество Y функции g_T. Существует такая подстановка констант D, $V(D) = V(g_T)\backslash Y$, что функция $g_T|_D$ существенно зависит от всех переменных из множества Y. Функция $g_T|_D$ является (s, n^s)-подфункцией функции $f^{(m)}$, поэтому функция $f^{(m-s)}$ может быть получена из функции $g_T|_D$ с помощью замены переменных без отождествления и навешивания отрицаний на некоторые переменные. Отсюда следует

$$M_Б(f^{(m-s)}) = M_Б(g_T|_D) = \frac{1}{n^{m-s}} L_Б(g_T|_D) \leqslant \\ \leqslant \frac{1}{n^{m-s}} L(G_T|_D) = \frac{1}{n^{m-s}} L_Y(G_T) \leqslant$$

(применяем (68) и (66))

$$\leqslant \frac{1}{n^{m-s}}\left(kn^{m-s}-\frac{a}{n^s}-T\right)=k-\frac{a}{n^m}-\frac{1}{n^{m-s}}T\leqslant$$
$$\leqslant k-\frac{a}{n^m}-\frac{1}{n^{m-s}}\cdot\frac{n^{m-s}-6a}{6n^s}=$$

(используем обозначение $k = M_Б(f^{(m)})$)

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

Основная лемма доказана.

§8. Оценка сложности степеней некоторых функций.

Теорема 1. Пусть $Б$ — нормальный базис порядка p, f — функция n аргументов, $\mathrm{nes}(f) = n$, 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 $C = \frac{1}{10n^3p^3\sqrt{u}}$, $\gamma = \frac{1}{1+2\log_u n}$ (C и γ зависят только от f и $Б$).

Доказательство. Предположим противное, т. е. в условиях леммы выполняется неравенство

$$M_Б(f^{(m)})< C\left(\frac{m}{\log_n m}\right)^{\gamma}. \tag{88}$$

Положим

$$s_0=\min\left\{s\in\mathbb{N}\mid u^s\geqslant 99n^6p^6(M_Б(f^{(m)}))^2\right\}, \tag{89}$$
$$T=\max\{t\in\mathbb{N}\cup\{0\}\mid m-ts_0>0\}. \tag{90}$$

Применив T раз основную лемму, получим

$$M_Б(f^{(m-Ts_0)})\leqslant M_Б(f^{(m)})-T\cdot\frac{1}{6n^{s_0}}. \tag{91}$$

Из (89), (88) и определения C следует

$$u^{s_0-1} < 99n^6p^6(M_Б(f^{(m)}))^2 <$$
$$< 100n^6p^6\frac{1}{100n^6p^6u}\cdot\left(\frac{m}{\log_n m}\right)^{2\gamma} = \frac{1}{u}\left(\frac{m}{\log_n m}\right)^{2\gamma}.$$

Умножив обе части этого неравенства на u, затем возведя их в степень $\log_u n$, получим

$$n^{s_0} \leqslant \left(\frac{m}{\log_n m}\right)^{2\gamma\log_u n}. \tag{92}$$

Из $m \geqslant n$ следует, что $\log_n \log_n m \geqslant 0$, поэтому, прологарифмировав обе части неравенства (92) и раскрыв определение γ, получим

$$s_0 \leqslant 2\gamma\log_u n(\log_n m - \log_n\log_n m) \leqslant$$
$$\leqslant \frac{2\log_u n}{1+2\log_u n}\cdot\log_n m \leqslant \log_n m. \tag{93}$$

Из (90) следует, что $m-(T+1)s_0 \leqslant 0$, а значит

$$T \geqslant \frac{m}{s_0} - 1. \tag{94}$$

В силу выбора T имеем $m - Ts_0 > 0$, следовательно, $M_Б(f^{(m-Ts_0)}) \geqslant 1$. Использовав это, а также (91) и (94), получим

$$M_Б(f^{(m)}) \geqslant M_Б(f^{(m-Ts_0)}) + T\cdot\frac{1}{6n^{s_0}} \geqslant 1 + \left(\frac{m}{s_0}-1\right)\cdot\frac{1}{6n^{s_0}} \geqslant \frac{m}{6s_0n^{s_0}} \geqslant$$

(используем (92), (93), а также определения C и γ)

$$\geqslant \frac{m}{6\log_n m\cdot\left(\frac{m}{\log_n m}\right)^{2\gamma\log_u n}} = \frac{1}{6}\left(\frac{m}{\log_n m}\right)^{1-2\gamma\log_u n} =$$
$$= \frac{1}{6}\left(\frac{m}{\log_n m}\right)^{\gamma} \geqslant C\left(\frac{m}{\log_n m}\right)^{\gamma},$$

а это противоречит (88).

Теорема 1 доказана.

Утверждение 4. Пусть $Б$ — нормальный базис, g — функция, существенно зависящая от всех своих переменных, и m — натуральное число. Тогда

$$M_Б(g^{(m+1)}) \geqslant M_Б(g^{(m)}). \tag{95}$$

Доказательство. Рассмотрим произвольную формулу G в базисе $Б$, реализующую функцию $g^{(m+1)}$, и имеющую сложность $L(G) = L_Б(g^{(m+1)})$. В каждом 1-множестве функции $g^{(m+1)}$ выберем ту переменную, которая входит в формулу G наименьшее число раз. Возьмем такую подстановку констант B, что функция $g^{(m+1)}|_B$ существенно зависит от всех выбранных переменных и только от них. Тогда $L(G|_B) \leqslant \frac{1}{\mathrm{nes}(g)}L(G)$ и функция $g^{(m)}$ может быть получена из $g^{(m+1)}|_B$ с помощью перестановки переменных без отождествления и навешивания отрицаний на переменные. Поэтому

$$M_Б(g^{(m)}) \leqslant \frac{1}{\mathrm{nes}(g^{(m)})}L(G|_B) \leqslant \frac{1}{\mathrm{nes}(g^{(m+1)})}L(G) = M_Б(g^{(m+1)}).$$

Отсюда и следует (95).

Утверждение 4 доказано.

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

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

$$L_{Б_1}(f_\epsilon^{(m)}) \succeq N \cdot \sqrt[5+\epsilon]{\ln N} \tag{96}$$

и

$$L_{Б_2}(f_\epsilon^{(m)}) \asymp N, \tag{97}$$

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

Доказательство. Рассмотрим два случая: 1) базис $Б_2$ линеен, базис $Б_1$ нелинеен; 2) либо базис $Б_2$ нелинеен, либо базис $Б_1$ линеен.

Случай 1). Рассмотрим нормальный базис $Б = [Б_1]$. Пусть p — порядок базиса $Б$. Положим $t_\epsilon = \max\{\lceil 2^{4/\epsilon}\rceil, p\}$, $n = 2t_\epsilon$ и

$$f_\epsilon(x_1, \ldots, x_n) \equiv (x_1 \oplus \ldots \oplus x_{t_\epsilon}) \cdot (x_{t_\epsilon+1} \oplus \ldots \oplus x_{2t_\epsilon}).$$

В силу линейности базиса $Б_2$, функция f_ϵ бесповторно выразима в $Б_2$ (конъюнкция бесповторно выразима в любом базисе). Отсюда следует (97). Проверим, что для базиса $Б$ и функции f_ϵ выполняется условие теоремы 1. Очевидно, что функция f_ϵ нелинейна. Далее, базис $Б$ нелинеен, $\mathrm{nes}(f_\epsilon) > 0$ и, в силу неравенства $t_\epsilon \geqslant p$, каждая переменная функции f_ϵ содержится в некотором $\oplus_p$-выделимом множестве переменных функции f_ϵ. Поэтому (см. определение в § 4) функция f_ϵ согласована с базисом $Б$. Наконец, мера устойчивости u функции f_ϵ равна t_ϵ и $t_\epsilon \geqslant 2$.

Заметим, что

$$\log_u n = \frac{\log_2 n}{\log_2 u} = \frac{\log_2(2t_\epsilon)}{\log_2 t_\epsilon} = 1 + \frac{1}{\log_2 t_\epsilon} \leqslant 1 + \frac{1}{4/\epsilon} = 1 + \epsilon/4.$$

Применив теорему 1, получим

$$M_Б(f_\epsilon^{(m)}) \succeq \left(\frac{m}{\log_n m}\right)^{\frac{1}{1+2\log_u n}} \geqslant \sqrt[3+\epsilon/2]{\frac{m}{\log_n m}} \succeq \sqrt[3+\epsilon]{m} \asymp \sqrt[3+\epsilon]{\ln N}, \tag{98}$$

где $N = \mathrm{nes}(f_\epsilon^{(m)})$. Для любой функции g справедливо $L_{Б_1}(g) \geqslant L_{[Б_1]}(g) = L_Б(g)$, поэтому из (98) следует (96). Случай 1) рассмотрен.

Случай 2). Пусть функция θ, $\theta \in Б_2$, не выразима бесповторно в базисе $Б_1$. Если базис $Б_1$ линеен, то положим $Б = [Б_1]$. В этом случае функция θ бесповторно не выразима в базисе $Б$. Если базис $Б_1$ нелинеен, то положим $Б = [Б_1 \cup \{\oplus\}]$. Покажем, что и в этом случае функция θ не выразима бесповторно в базисе $Б$. Предположим противное, т. е. функция θ бесповторно выразима в базисе $Б$. Рассмотрим бесповторную приведенную формулу F в базисе $Б$, реализующую функцию θ. Если формула F не содержит вхождений функции $\oplus$, то F является формулой в базисе $[Б_1]$. В этом случае функция θ бесповторно выразима в базисе $Б_1$, что противоречит выбору функции θ.

Рассмотрим теперь случай, когда формула F содержит вхождение функции $\oplus$. Тогда формула F содержит подформулу H вида

$$H \mathrel{\overline{\underline{\circ}}} H_1 \oplus H_2.$$

Обозначим через W_0 множество всех переменных, входящих в формулу F вне подформулы H, положим $W_1 = V(H_1)$, $W_2 = V(H_2)$. В силу приведенности и бесповторности формулы F, множества W_0, W_1, W_2 попарно не пересекаются, состоят только из существенных переменных функции θ и, кроме того, множества W_1 и W_2 непусты. Пусть $y_1 \in W_1$, $y_2 \in W_2$. Существуют такие подстановки констант A_0, A_1, A_2, $V(A_0) = W_0$, $V(A_1) = W_1 \backslash \{y_1\}$, $V(A_2) = W_2 \backslash \{y_2\}$, что функции $\theta|_{A_0}$, $\theta|_{A_1}$, $\theta|_{A_2}$ существенно зависят от переменных y_1, y_1, y_2 соответственно.

Положим $A = A_0 \cup A_1 \cup A_2$. Тогда для некоторых констант σ_0, σ_1, σ_2 и σ выполняется

$$F|_A \equiv H|_{A_1 \cup A_2} \oplus \sigma_0 \equiv H_1|_{A_1} \oplus H_2|_{A_2} \oplus \sigma_0 \equiv y_1 \oplus \sigma_1 \oplus y_2 \oplus \sigma_2 \oplus \sigma_0 \equiv y_1 \oplus y_2 \oplus \sigma.$$

Следовательно, $\theta|_A \equiv y_1 \oplus y_2 \oplus \sigma$. В то же время $\theta \in Б_2$, поэтому функция $\oplus$ бесповторно выражается в базисе $Б_2$, а значит, базис $Б_2$ линеен. Тогда, в силу условия случая 2), базис $Б_1$ линеен, а мы рассматриваем ситуацию, когда базис $Б_1$ нелинеен. Противоречие.

Итак, в любом случае функция θ не выразима бесповторно в базисе $Б$. Положим $\psi = \langle \theta \rangle$. Пусть p — порядок базиса $Б$ и $k = \mathrm{nes}(\psi)$.

Положим $t_\epsilon = \max\{\lceil k^{4/\epsilon}\rceil, 2\}$. Для каждого i, $i = 1, \ldots, t_\epsilon^2$, обозначим

$$\psi_i = \psi(x_{(i-1)k+1}, \ldots, x_{ik}).$$

Наконец, положим

$$f_\epsilon(x_1, \ldots, x_{kt_\epsilon^2}) \equiv \psi_1 \cdot \ldots \cdot \psi_{t_\epsilon} \vee \psi_{t_\epsilon+1} \cdot \ldots \cdot \psi_{2t_\epsilon} \vee \ldots \vee \psi_{t_\epsilon(t_\epsilon-1)+1} \cdot \ldots \cdot \psi_{t_\epsilon^2}.$$

Функция ψ не выразима бесповторно в базисе $Б$. Тогда, в силу леммы 3 из § 3, функция φ, $\varphi(x_1, \ldots, x_{k+2}) \equiv \psi \cdot x_{k+1} \vee x_{k+2}$, является 1-универсальной для базиса $Б$. Заметим, что (в силу $t_\epsilon \geqslant 2$) функция f_ϵ содержит в качестве подфункции функцию вида $\varphi' = \psi \cdot y^{\tau_1} \vee z^{\tau_2}$, где y, z — различные переменные, не входящие в множество $V(\psi)$. Функция φ' может быть получена из функции φ заменой переменных без отождествления и навешиванием отрицаний на переменные, поэтому функция φ' является 1-универсальной для базиса $Б$. В то же время, φ' является подфункцией функции f_ϵ. Тогда, в силу утверждения 2 из § 3, функция f_ϵ является 1-универсальной для базиса $Б$.

Заметим, что мера устойчивости функции, реализуемой формулой

$$x_1 \cdot \ldots \cdot x_{t_\epsilon} \vee x_{t_\epsilon+1} \cdot \ldots \cdot x_{2t_\epsilon} \vee \ldots \vee x_{t_\epsilon(t_\epsilon-1)+1} \cdot \ldots \cdot x_{t_\epsilon^2}$$

равна t_ϵ, поэтому мера устойчивости функции f_ϵ не меньше, чем t_ϵ. В частности, $u(f_\epsilon) \geqslant 2$. Применим к функции f_ϵ, базису $Б$ и числу p лемму 5 из § 3. В силу леммы 5, существует такое число m_ϵ (зависящее от p и f_ϵ), что функция $f_\epsilon^{(m_\epsilon)}$ является p-универсальной для базиса $Б$. Обозначим $f = f_\epsilon^{(m_\epsilon)}$, $n = \mathrm{nes}(f)$, $u = u(f)$.

Проверим, что базис $Б$ и функция f удовлетворяют условиям теоремы 1. Базис $Б$ линеен, а функция f является p-универсальной для $Б$. Поэтому (см. определение в § 4) функция f согласована с базисом $Б$. Очевидно, что функция f нелинейна и, в силу леммы 2 из § 2, выполнено $u(f) \geqslant u(f_\epsilon) \geqslant 2$. Оценим $\log_u n$. Ранее мы отмечали, что $u(f_\epsilon) \geqslant t_\epsilon$. Поэтому, с учетом леммы 2, имеем

$$\log_u n = \frac{\log_k n}{\log_k u} \leqslant \frac{m_\epsilon \log_k \mathrm{nes}(f_\epsilon)}{m_\epsilon \log_k u(f_\epsilon)} \leqslant$$
$$\leqslant \frac{\log_k(kt_\epsilon^2)}{\log_k(t_\epsilon)} = 2 + \frac{1}{\log_k(t_\epsilon)} \leqslant 2 + \frac{1}{4/\epsilon} = 2 + \epsilon/4.$$

Применив теорему 1, получим

$$M_Б(f^{(m)}) \succeq \left(\frac{m}{\log_n m}\right)^{\frac{1}{1+2\log_u n}} \geqslant \sqrt[5+\epsilon/2]{\frac{m}{\log_n m}} \succeq \sqrt[5+\epsilon]{m} \asymp \sqrt[5+\epsilon]{\ln N}, \tag{99}$$

где $N = \mathrm{nes}(f^{(m)})$.

Заметим, что $f^{(m)} = f_\epsilon^{(m_\epsilon m)}$. Из утверждения 4 и (99) вытекает

$$M_Б(f_\epsilon^{(m)}) \geqslant M_Б(f_\epsilon^{(\lfloor m/m_\epsilon \rfloor \cdot m_\epsilon)}) =$$
$$= M_Б(f^{(\lfloor m/m_\epsilon \rfloor)}) \succeq \sqrt[5+\epsilon]{\ln N'} \asymp \sqrt[5+\epsilon]{\ln N}, \tag{100}$$

где $N' = \mathrm{nes}(f^{(\lfloor m/m_\epsilon \rfloor)}) = \mathrm{nes}(f_\epsilon^{(\lfloor m/m_\epsilon \rfloor \cdot m_\epsilon)})$ и $N = \mathrm{nes}(f_\epsilon^{(m)})$. Наконец, заметим, что $Б \supseteq [Б_1]$, поэтому для любой функции g справедливо

$$L_Б(g) \leqslant L_{[Б_1]}(g) \leqslant L_{Б_1}(g).$$

Отсюда и из (100) следует (96). Функция f_ϵ бесповторно выразима в $Б_2$ (конъюнкция и дизъюнкция бесповторно выразимы в любом базисе), поэтому (97) также выполнено. Случай 2) рассмотрен.

Теорема 2 доказана.

ГЛАВА IV. СРАВНЕНИЕ БУЛЕВЫХ БАЗИСОВ

§9. Критерий сравнения произвольных базисов.

Утверждение 5. Пусть f — функция, существенно зависящая от всех своих аргументов, $M(f)$ — множество всех функций, обобщенно однотипных с неразложимыми функциями вида $\langle g\rangle$, где g — подфункция функции f. Тогда функция f бесповторно выразима через множество $M(f)$.

Доказательство. Проведем индукцию по числу $\mathrm{nes}(f)$.

Базис индукции: $\mathrm{nes}(f) \leqslant 2$. В этом случае функция f неразложима, следовательно, $f \in M(f)$. Тогда функция f бесповторно выразима через $M(f)$.

Индуктивный переход: $\mathrm{nes}(f) \geqslant 3$ и для всех f', $\mathrm{nes}(f') < \mathrm{nes}(f)$, утверждение доказано. Если функция f неразложима, то $f \in M(f)$, следовательно, функция f бесповторно выразима через $M(f)$. Рассмотрим теперь случай, когда функция f разложима. Пусть $n = \mathrm{nes}(f)$. В этом случае существует такое выделимое множество переменных W функции f, что $2 \leqslant |W| \leqslant n-1$. Пусть $\{i_1, \ldots, i_n\} = \{1, \ldots, n\}$ и $W = \{x_{i_1}, \ldots, x_{i_k}\}$. Тогда существуют функции g и h, для которых выполнено тождество

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

Далее, существуют такие подстановки констант A, $V(A) = \{x_{i_2}, \ldots, x_{i_k}\}$, B, $V(B) = \{x_{i_{k+1}}, \ldots, x_{i_n}\}$, и константы c, d, что

$$f|_A \equiv g(x_{i_1} \oplus c, x_{i_{k+1}}, \ldots, x_{i_n}), \qquad f|_B \equiv h(x_{i_1}, \ldots, x_{i_k}) \oplus d.$$

Обозначим $f_1 = \langle f|_A\rangle$, $f_2 = \langle f|_B\rangle$. Тогда $\mathrm{nes}(f_1) < \mathrm{nes}(f)$ и $\mathrm{nes}(f_2) < \mathrm{nes}(f)$, поэтому к функциям f_1 и f_2 применимо предположение индукции. Применив его, получим, что f_i, $i = 1,\ 2$, бесповторно выразима через $M(f_i)$. Заметим, что $M(f_i) \subseteq M(f)$, $i = 1,\ 2$, поэтому функции f_1 и f_2 бесповторно выразимы через $M(f)$. Тогда функции g и h бесповторно выразимы через $M(f)$, а значит, f бесповторно выразима через $M(f)$.

Утверждение 5 доказано.

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

а) базис $Б_1$ предшествует базису $Б_2$ ($Б_1 \preccurlyeq Б_2$),

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

Доказательство. Импликация б) $\Rightarrow$ а) доказана О. Б. Лупановым (см. [12]). Импликация а) $\Rightarrow$ б) непосредственно следует из теоремы 2.

Импликация б) $\Rightarrow$ в). Пусть все функции из базиса $Б_2$ бесповторно выразимы в базисе $Б_1$. Рассмотрим произвольную функцию f, $f \in \mathrm{Ker}(Б_2)$. Покажем, что $f \in \mathrm{Ker}(Б_1)$. По построению ядра базиса, существует такая функция g, $g \in [Б_2]$, что функция g обобщенно однотипна с f. Функция g, в свою очередь, получена заменой переменных без отождествления из подфункции некоторой функции h, $h \in Б_2$. Функция h бесповторно выразима в $Б_1$, следовательно, g бесповторно выразима в $Б_1$, а значит, f бесповторно выразима в $Б_1$. Тогда f бесповторно выразима в базисе $[Б_1]$. Если функция f тождественно равна константе, то $f = 0$, следовательно, $f \in \mathrm{Ker}(Б_1)$. Пусть теперь f не равна тождественно константе.

Рассмотрим приведенную бесповторную формулу F в базисе $[Б_1]$, реализующую функцию f. В силу неразделимости функции f, формула F содержит не более одного вхождения функции, зависящей от двух и более переменных. Следовательно, формула F реализует функцию, обобщенно однотипную с некоторой функцией φ, $\varphi \in [Б_1]$, т. е. f обобщенно однотипна с φ. Тогда функция φ неразделима, поэтому некоторая функция, обобщенно однотипная с φ, принадлежит множеству $\mathrm{Ker}(Б_1)$. Следовательно, некоторая функция, обобщенно однотипная с f, принадлежит множеству $\mathrm{Ker}(Б_1)$, а значит, $f \in \mathrm{Ker}(Б_1)$. Импликация б) $\Rightarrow$ в) доказана.

Импликация в) $\Rightarrow$ б). Пусть $\mathrm{Ker}(Б_2) \subseteq \mathrm{Ker}(Б_1)$. Рассмотрим произвольную функцию f, $f \in Б_2$. Покажем, что f бесповторно выразима в базисе $Б_1$. Обозначим через M множество всех функций, обобщенно однотипных с неразложимыми функциями из базиса $[Б_2]$. Тогда $M(f) \subseteq M$ (см. утверждение 5). В силу утверждения 5, функция $\langle f \rangle$ бесповторно выразима через множество M. Отсюда следует, что $\langle f \rangle$ бесповторно выразима через множество $\mathrm{Ker}(Б_2) \cup \{\neg\}$, а значит, и через множество $\mathrm{Ker}(Б_1) \cup \{\neg\}$. Каждая функция из множества $\mathrm{Ker}(Б_1) \cup \{\neg\}$ бесповторно выражается в базисе $Б_1$. Следовательно, функция $\langle f \rangle$, а значит, и функция f бесповторно выразима в базисе $Б_1$. Импликация в) $\Rightarrow$ б) доказана.

Таким образом, равносильность условий а), б) и в) установлена. Докажем равносильность условий г) и д).

Импликация г) $\Rightarrow$ д). Пусть базис $Б_1$ непосредственно предшествует базису $Б_2$. Тогда $Б_1$ строго предшествует базису $Б_2$. Поэтому из ранее доказанного следует, что $\mathrm{Ker}(Б_2) \subset \mathrm{Ker}(Б_1)$. Покажем, что $|\mathrm{Ker}(Б_1) \setminus \mathrm{Ker}(Б_2)| = 1$. предположим противное, т. е. $|\mathrm{Ker}(Б_1) \setminus \mathrm{Ker}(Б_2)| \geqslant 2$. Среди всех функций из множества $\mathrm{Ker}(Б_1) \setminus \mathrm{Ker}(Б_2)$ выберем функцию, число аргументов которой минимально (произвольную из таких), и обозначим ее через f. Рассмотрим базис $Б' = Б_0 \cup \mathrm{Ker}(Б_2) \cup \{f\}$. Покажем, что $\mathrm{Ker}(Б') = \mathrm{Ker}(Б_2) \cup \{f\}$. Очевидно, что

$\operatorname{Ker}(Б_2) \cup \{f\} \subseteq \operatorname{Ker}(Б') \subseteq \operatorname{Ker}(Б_1)$. Рассмотрим произвольную функцию g, $g \in \operatorname{Ker}(Б')$. Покажем, что $g \in \operatorname{Ker}(Б_2) \cup \{f\}$.

Существует функция h, $h \in [Б']$, обобщенно однотипная с g. Функция h либо принадлежит множеству $[Б_0 \cup \operatorname{Ker}(Б_2)]$, либо является функцией вида $\langle f|_A \rangle$, где A — подстановка констант. Если $h \in [Б_0 \cup \operatorname{Ker}(Б_2)]$, то $g \in \operatorname{Ker}(Б_0 \cup \operatorname{Ker}(Б_2)) = \operatorname{Ker}(Б_2)$. Пусть теперь $h = \langle f|_A \rangle$. Если $f|_A \neq f$, то число аргументов у функции h (а значит, и у функции g) меньше, чем число аргументов у функции f. Поэтому (в силу выбора функции f) $g \notin \operatorname{Ker}(Б_1) \setminus \operatorname{Ker}(Б_2)$. В то же время, $g \in \operatorname{Ker}(Б_1)$, поэтому $g \in \operatorname{Ker}(Б_2)$. Наконец, в случае, если $f|_A = f$, имеем $h = f$, а значит, $g = f$.

Таким образом, $\operatorname{Ker}(Б') = \operatorname{Ker}(Б_2) \cup \{f\}$, следовательно, $\operatorname{Ker}(Б_2) \subset \operatorname{Ker}(Б') \subset \operatorname{Ker}(Б_1)$. Тогда, по ранее доказанному, $Б_1 \prec Б' \prec Б_2$, а это противоречит условию, что базис $Б_1$ непосредственно предшествует базису $Б_2$. Импликация г) $\Rightarrow$ д) доказана.

Импликация д) $\Rightarrow$ г). Пусть $\operatorname{Ker}(Б_2) \subset \operatorname{Ker}(Б_1)$ и $|\operatorname{Ker}(Б_1) \setminus \operatorname{Ker}(Б_2)| = 1$. Тогда базис $Б_1$ строго предшествует базису $Б_2$. Рассмотрим любой базис $Б$ такой, что $Б_1 \preccurlyeq Б \preccurlyeq Б_2$. Имеем $\operatorname{Ker}(Б_2) \subseteq \operatorname{Ker}(Б) \subseteq \operatorname{Ker}(Б_1)$. Поэтому, либо $\operatorname{Ker}(Б) = \operatorname{Ker}(Б_1)$, либо $\operatorname{Ker}(Б) = \operatorname{Ker}(Б_2)$, а значит, либо $Б \sim Б_1$, либо $Б \sim Б_2$. Следовательно, не существует такого базиса $Б'$, что $Б_1 \prec Б' \prec Б_2$. Таким образом, базис $Б_1$ непосредственно предшествует базису $Б_2$. Импликация д) $\Rightarrow$ г) доказана.

Основная теорема доказана.

§10. Исследование структуры базисов.

Утверждение 6. Всякая S-функция (см. определение в § 1) неразложима.

Доказательство. Пусть f — произвольная S-функция. Предположим противное: функция f разложима. По определению, f существенно зависит от всех своих аргументов. Согласно утверждению 5, f бесповторно реализуется через множество функций $M(f)$ (см. формулировку утверждения 5). Каждая функция из $M(f)$ представима в виде $\langle g \rangle$, где g обобщенно однотипна с некоторой подфункцией h функции f. Заметим, что $h \neq f$, поскольку функция $\langle f \rangle$ разложима, а функция $\langle h \rangle$ неразложима. Поэтому h — собственная подфункция функции f, а значит, h бесповторно выразима в базисе $Б_0$. Тогда и функция $\langle g \rangle$ бесповторно выразима в $Б_0$. Таким образом, все функции из множества $M(f)$ бесповторно выразимы в базисе $Б_0$, поэтому и функция f бесповторно выразима в $Б_0$. Последнее противоречит определению S-функции.

Утверждение 6 доказано.

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

Доказательство. В силу очевидного вложения $P_2(n) \subseteq [P_2(n+1)]$ имеем $\mathrm{Ker}(P_2(n)) \subseteq \mathrm{Ker}(P_2(n+1))$. С другой стороны, существует неразложимая функция от $(n+1)$ аргументов. Например, функция φ_{n+1}, где $\varphi_{n+1} = x_1 \cdot \ldots \cdot x_{n+1} \vee \bar{x}_1 \cdot \ldots \cdot \bar{x}_{n+1}$, принадлежит множеству (1) из § 1, следовательно, φ_{n+1} является S-функцией, а значит, согласно утверждению 6, φ_{n+1} неразложима. Тогда $\hat{\varphi}_{n+1} \in \mathrm{Ker}(P_2(n+1))$. Очевидно, что $\hat{\varphi}_{n+1} \notin \mathrm{Ker}(P_2(n))$. Следовательно, $\mathrm{Ker}(P_2(n)) \subset \mathrm{Ker}(P_2(n+1))$. Применив основную теорему, получим, что базис $P_2(n+1)$ строго предшествует базису $P_2(n)$.

Теорема 3 доказана.

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 $Б_i$.

Теорема 4 является непосредственным следствием теоремы 3.

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

Доказательство. Предположим противное: такой базис $Б^*$ существует. Обозначим через n наибольшее число аргументов у функций из базиса $Б^*$. Тогда $Б^* \subseteq [P_2(n)]$. Следовательно, базис $P_2(n)$ предшествует базису $Б^*$. По теореме 3, базис $P_2(n+1)$ строго предшествует базису $P_2(n)$, поэтому $P_2(n+1)$ строго предшествует базису $Б^*$. Противоречие.

Теорема 5 доказана.

Утверждение 7. Пусть f — произвольная S-функция Тогда

$$\mathrm{Ker}(Б_0 \cup \{f\}) = \mathrm{Ker}(Б_0) \cup \{\hat{f}\}.$$

Доказательство. Заметим, что f' также является S-функцией, поэтому, в силу утверждения 6, функция f' неразложима, а значит, $f' \in \mathrm{Ker}(Б_0 \cup \{f\})$. Очевидно, что $\mathrm{Ker}(Б_0) \subseteq \mathrm{Ker}(Б_0 \cup \{f\})$. Таким образом, $\mathrm{Ker}(Б_0) \cup \{f'\} \subseteq \mathrm{Ker}(Б_0 \cup \{f\})$.

Докажем обратное включение. Предположим противное, т. е. $\mathrm{Ker}(Б_0 \cup \{f\}) \nsubseteq \mathrm{Ker}(Б_0) \cup \{f'\}$. Тогда существует функция h, $h \in \mathrm{Ker}(Б_0 \cup \{f\}), h \notin \mathrm{Ker}(Б_0) \cup \{f'\}$. Функция h неразложима и лексикографически минимальна, поэтому из условия $h \notin \mathrm{Ker}(Б_0)$ следует, что h бесповторно не выразима в базисе $Б_0$. В то же время, h обобщенно однотипна с функцией вида $\langle g \rangle$, где g — подфункция функции f. Следовательно, g бесповторно не выразима в базисе $Б_0$. Из условия $h \neq f'$ следует, что $g \neq f$, поэтому g — собственная подфункция функции f, бесповторно не выразимая в базисе $Б_0$. Противоречие с определением S-функции.

Утверждение 7 доказано.

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

Доказательство. Пусть $Б$ — произвольный предмаксимальный базис. По основной теореме, $\mathrm{Ker}(Б) = \mathrm{Ker}(Б_0) \cup \{f\}$, где $f \notin \mathrm{Ker}(Б_0)$. Покажем, что f является S-функцией. Во-первых, f неразложима. Поэтому, если f бесповторно выражается в базисе $Б_0$, то f обобщенно однотипна с одной из функций 0, x, xy, а значит, $f \in \mathrm{Ker}(Б_0)$, что не так. Таким образом, f бесповторно не выражается в $Б_0$.

Далее, пусть h — подфункция функции f, отличная от f. Тогда h бесповторно выразима через множество $M(h)$ (см. формулировку утверждения 5). Предположим, что найдется функция φ из множества $M(h)$, бесповторно не выразимая в базисе $Б_0$. Тогда функция $\hat{\varphi}$ должна принадлежать ядру базиса $Б$. Но $\mathrm{nes}(\hat{\varphi}) \leqslant \mathrm{nes}(h) < \mathrm{nes}(f)$, а значит, $\hat{\varphi} \neq f$. Поэтому $\hat{\varphi} \notin \mathrm{Ker}(Б)$. Полученное противоречие говорит о том, что все функции из множества $M(h)$ бесповторно выразимы в базисе $Б_0$, а тогда и функция h бесповторно выразима в $Б_0$. Итак, мы показали, что f — S-функция.

Рассмотрим базис $Б' = Б_0 \cup \{f\}$. Используя утверждение 7, получим $\mathrm{Ker}(Б') = \mathrm{Ker}(Б_0) \cup \{f\} = \mathrm{Ker}(Б)$. В силу основной теоремы, базисы $Б$ и $Б'$ эквивалентны.

Докажем обратное утверждение. Рассмотрим базис $Б = Б_0 \cup \{f\}$, где f — S-функция. Тогда, по утверждению 7, $\mathrm{Ker}(Б) = \mathrm{Ker}(Б_0) \cup \{\hat{f}\}$. Функция $\hat{f}$ является S-функцией, поэтому $\hat{f} \notin Б_0$. Следовательно, в силу основной теоремы, $Б$ непосредственно предшествует базису $Б_0$, т. е. $Б$ является предмаксимальным базисом.

Теорема 6 доказана.

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

$$
\begin{gathered}
x_1 x_2 \cdot \ldots \cdot x_n \vee \bar{x}_1 \bar{x}_2 \cdot \ldots \cdot \bar{x}_n, \quad n \geqslant 2, \\
x_1(x_2 \vee \ldots \vee x_n) \vee x_2 \cdot \ldots \cdot x_n, \quad n \geqslant 3, \\
x_1(x_2 \vee x_3 \cdot \ldots \cdot x_n) \vee x_2 \bar{x}_3 \cdot \ldots \cdot \bar{x}_n, \quad n \geqslant 3, \\
x_1(x_2 \vee x_3) \vee x_3 x_4, \\
x_1(x_3 x_4 \vee x_5) \vee x_2(x_3 \vee x_4 x_5);
\end{gathered} \tag{101}
$$

б) если f — функция из множества (101), то базис $Б_0 \cup \{f\}$ предмаксимален;

в) если f_1 и f_2 — различные функции из множества (101), то базисы $Б_0 \cup \{f_1\}$ и $Б_0 \cup \{f_2\}$ неэквивалентны.

Доказательство. Заметим, что множество (101) совпадает с множеством (1), поэтому утверждения а) и б) следуют из теоремы 6. Докажем утверждение в). Пусть f_1 и f_2 — различные функции из множества (101). Тогда f_1 и f_2 не обобщенно однотипны, следовательно, $\hat{f}_1 \neq \hat{f}_2$. Применив утверждение 7, получим

$$
\mathrm{Ker}(Б_0 \cup \{f_1\}) = \mathrm{Ker}(Б_0) \cup \{\hat{f}_1\} \neq \mathrm{Ker}(Б_0) \cup \{\hat{f}_2\} = \mathrm{Ker}(Б_0 \cup \{f_2\}).
$$

Поэтому, в силу основной теоремы, базисы $Б_0 \cup \{f_1\}$ и $Б_0 \cup \{f_2\}$ неэквивалентны.

Теорема 7 доказана.

Теорема 8. Существует бесконечное множество попарно неэквивалентных предмаксимальных базисов.

Теорема 8 следует из теоремы 7 в силу бесконечности множества (101).

Теорема 9. Существует бесконечное множество попарно несравнимых базисов.

Очевидно, что если два предмаксимальных базиса неэквивалентны, то они несравнимы, поэтому теорема 9 следует из теоремы 8.

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

Доказательство. Пусть $Б$ — произвольный базис. Если базис $Б$ предшествует базису $Б'$, то, по основной теореме, $\mathrm{Ker}(Б') \subseteq \mathrm{Ker}(Б)$. Множество $\mathrm{Ker}(Б)$ конечно, поэтому число различных его подмножеств конечно. В силу основной теоремы, два базиса эквивалентны тогда и только тогда, когда их ядра совпадают, а значит, существует лишь конечное, с точностью до эквивалентности, число базисов, которым предшествует базис $Б$.

Теорема 10 доказана.

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 11 является следствием теоремы 10.

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

Доказательство. Рассмотрим множество $\mathrm{Ker}(Б)$. Оно конечно, следовательно, содержит лишь конечное число S-функций. Пусть T — подмножество множества (101), состоящее из всех тех функций, которые не обобщенно однотипны ни с одной функцией из множества $\mathrm{Ker}(Б)$. Тогда T — бесконечное множество. Рассмотрим произвольный базис вида $Б \cup \{f\}$, где $f \in T$. Очевидно, что $\mathrm{Ker}(Б \cup \{f\}) = \mathrm{Ker}(Б) \cup \mathrm{Ker}(Б_0 \cup \{f\})$. В то же время, в силу утверждения 7, $\mathrm{Ker}(Б_0 \cup \{f\}) = \mathrm{Ker}(Б_0) \cup \{\hat{f}\}$. Поэтому $\mathrm{Ker}(Б \cup \{f\}) = \mathrm{Ker}(Б) \cup \mathrm{Ker}(Б_0) \cup \{\hat{f}\} = \mathrm{Ker}(Б) \cup \{\hat{f}\}$. В силу выбора функции f, функция $\hat{f}$ не принадлежит ядру базиса $Б$, поэтому $|\,\mathrm{Ker}(Б \cup \{\hat{f}\}) \setminus \mathrm{Ker}(Б)| = 1$. Применив основную теорему, получим, что базис $Б \cup \{f\}$ непосредственно предшествует базису $Б$.

Теорема 12 доказана.

Теорема 13. Пусть $Б_1, \dots, Б_n$ и $Б'_1, \dots, Б'_m$ — 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 $n = m$.

Доказательство. В силу основной теоремы имеем $Б_1 \subset Б_2 \subset \ldots \subset Б_n$, $Б'_1 \subset Б'_2 \subset \ldots \subset Б'_m$; для любого i, $1 \leqslant i \leqslant n-1$, выполнено $|\operatorname{Ker}(Б_{i+1}) \setminus \operatorname{Ker}(Б_i)| = 1$ и для любого j, $1 \leqslant j \leqslant m-1$, выполнено $|\operatorname{Ker}(Б'_{j+1}) \setminus \operatorname{Ker}(Б'_j)| = 1$. Поэтому

$$n - 1 = |\operatorname{Ker}(Б_n) \setminus \operatorname{Ker}(Б_1)| = |\operatorname{Ker}(Б'_m) \setminus \operatorname{Ker}(Б'_1)| = m - 1,$$

следовательно, $n = m$.

Теорема 13 доказана.

ЛИТЕРАТУРА

1. **Кузнецов А. В.** О бесповторных контактных схемах и бесповторных суперпозициях функций алгебры логики // Труды МИАН СССР. 1958. Т. 51. С. 186–225.

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

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.** Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984. 138 с.

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

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

7. **Нигматуллин Р. Г.** Сложность булевых функций. М.: Наука, 1991. 240 с.

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

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

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

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

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

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

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

15. **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.

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

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

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

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

20. **Яблонский С. В.** Основные понятия кибернетики // Проблемы кибернетики. Вып. 2. М.: Физматгиз, 1959. С. 7–38.

21. **Яблонский С. В.** Введение в дискретную математику. М.: Наука, 1979. 272 с.