ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи

Балюк Александр Сергеевич

Сложность булевых функций в классах полиномиальных форм

01.01.09 — дискретная математика и
математическая кибернетика

Диссертация
на соискание ученой степени
кандидата физико-математических наук

Научные руководители:

доктор физико-математических наук С.Ф. Винокуров

доктор физико-математических наук, профессор Н.А. Перязев

Иркутск 2002

Оглавление

Введение

При проектировании современных вычислительных устройств важную роль играет аппарат дискретных функций. На современном этапе развития цифровой техники наиболее распространенным является кодирование сигнала двумя или тремя состояниями. Третье состояние чаще всего используется только на аппаратном уровне и лишь для указания того, что устройство еще не обработало входные данные или данные не готовы. Это связано с физическими ограничениями на скорость срабатывания устройств. Несмотря на то что скорость работы цифровых устройств постоянно повышается, существует некоторый физический предел этого роста. Поэтому в настоящее время ведутся разработки дискретных устройств с бóльшим числом состояний. Однако пока они носят экспериментальный характер.

До сих пор аппарат булевых функций является наиболее адекватным для проектирования цифровой, в том числе микропроцессорной техники. Постоянное стремление к повышению быстродействия систем, уменьшению их размера, потребляемой энергии и стоимости ставит задачи не только поиска новых технологий реализации цифровых устройств, но и более простой и эффективной реализации существующих. Это ведет к интенсивному исследованию и проектированию различных регулярных структур. Одними из наиболее распространенных являются программируемые логические матрицы (PGA и FPGA).

Теория булевых функций изначально была ориентирована на решение практических задач реализации цифровых устройств. Были созданы различные математические модели непосредственно отражающие аппаратную реализацию. Это оказало влияние и на терминологию. Так в теории булевых функций исследуются схемы из функциональных элементов, П-схемы, релейно-контактные схемы и другие структуры.

Одним из основных способов задания булевых функций является

формульное или, иначе, термальное представление. Одним из вопросов формульных представлений является вопрос о принципиальной возможности реализации тех или иных булевых функций формулами, использующими специально выбранные, базисные функции. Этот вопрос был решен Э. Постом [20, 44, 45].

И в теории, и в приложениях одним из наиболее интересных вопросов является вопрос о сложности представлений булевых функций с помощью тех или иных структур. Важными результатами в этом направлении, являются асимптотически точные оценки сложности реализаций булевых функций формулами и схемами из функциональных элементов, которые принадлежат О. Б. Лупанову [15, 16, 17, 18, 29]. Однако, несмотря на полученные экспоненциальные оценки, нахождение конкретных функций большой сложности, другими словами, нахождение эффективных нижних оценок, сопряжено с определенными трудностями [30, 31]. К настоящему времени построены лишь булевы функции, сложность которых в классе схем из функциональных элементов линейна [34], а в классе формул полиномиальна. Обзор результатов по этим вопросам можно найти в [21, 27, 28]. В более специализированных классах представлений удается получить более высокие эффективные нижние оценки сложности.

Одной из разновидностей представлений булевых функций является реализация их нормальными формами. Нормальные формы непосредственно реализуются на программируемых логических матрицах. Поэтому их исследование представляет определенный практический интерес.

Хорошо исследован вопрос о реализации булевых функций дизъюнктивными и конъюнктивными нормальными формами [25, 33, 42, 46, 26]. Однако здесь уже для хорошо известных и часто применяемых функций, например, для линейной, найдены высокие нижние оценки сложности, которые совпадают с верхними оценками [19]. Величина этих оценок накладывает определенные ограничения на возможности практической

реализации данных нормальных форм.

В этой связи более интересными представляются полиномиальные нормальные формы. Впервые полиномиальные нормальные формы были рассмотрены И. И. Жегалкиным при исследовании некоторых вопросов математической логики [9, 10]. Затем, в 50-х годах прошлого века, полиномиальные нормальные формы исследовались в связи с их применением в теории кодирования [43, 47]. Следующий всплеск интереса к полиномиальным нормальным формам произошел в конце прошлого века, после того как в цифровой технике стали активно применяться элементы типа «сложение по модулю 2» («EXOR») [11, 32, 40, 41].

Для сложности представлений булевых функций полиномиальными нормальными формами были найдены нижняя [37] и верхняя [13, 12] границы. Эти оценки отличаются на множитель $\log n$, поэтому вопрос об асимптотически точной оценке еще ждет своего решения. Также были построены эффективно заданные булевы функции, которые в классе полиномиальных нормальных форм имеют экспоненциальную сложность [58]. Однако, сложность построенных булевых функций значительно меньше теоретической верхней оценки. Поэтому стои́т также вопрос о поиске эффективно заданных сложных функций.

Для того чтобы провести более глубокие исследования, из всего класса полиномиальных нормальных форм выделяют некоторые подклассы, обладающие теми или иными свойствами. Эти подклассы образуют некоторую иерархию. Различные подходы к описанию подклассов приводят к различным иерархиям [35, 36, 39, 56]. В большинстве случаев между иерархиями нетрудно найти соответствие. Но одни классы удобнее описывать и исследовать на одном языке, другие — на другом.

В ряде работ был предложен и разработан операторный подход к исследованию булевых функций [1, 22]. Использование операторов позволило обобщить полиномиальные нормальные формы на полиномиальные формы по базисным функциям, а введение понятия пучка операторов и

применение аппарата линейной алгебры открыло возможность описывать произвольные классы полиномиальных форм по базисным функциям, в том числе классы полиномиальных нормальных форм [3, 4, 5, 6, 7, 38, 56].

В классах полиномиальных нормальных форм, исключая классы, порождаемые единственным операторным пучком, долгое время стоял вопрос о нахождении точных оценок сложности. Лишь в 1995 году появился первый результат такого рода [24]. В дальнейшем были получены точные оценки сложности для различных классов [2, 3, 54, 56, 59].

Методы, использованные для нахождения высоких нижних границ сложности, предполагают построение конкретных функций, на которых эта граница достигается. Встал вопрос об описании всех функций наибольшей сложности в различных классах полиномиальных форм. Этот вопрос был решен для всех классов, точные оценки сложности которых известны [52, 54, 56, 57, 59].

Данная диссертация является исследованием по полиномиальным операторным представлениям булевых функций, включая вопросы построения полиномиальных форм, их сложности и поиска наиболее сложных функций.

Диссертация состоит из введения, трех глав, разбитых на 10 параграфов, заключения и списка литературы.

В первой главе даются основные понятия определения принятые при изложении результатов (первый параграф), строится иерархия классов операторных пучков, которая более всего тяготеет к иерархии из [59] (второй параграф), а также делается обзор основных результатов по проблемам, рассматриваемым в диссертации, в том числе полученных автором (третий параграф). Обозначения, использованные для классов операторных пучков, в основном позаимствованы из [36].

Вторая глава посвящена нахождению функции Шеннона для некоторых классов полиномиальных форм и формул для вычисления коэф-

фициентов разложений.

В четвертом параграфе рассматривается вопрос нахождения коэффициентов полиномиальных форм. Известны эффективные методы их вычисления лишь для немногих классов [3]. В настоящей работе получены ранее неизвестные формулы вычисления коэффициентов в классе полиномиальных форм относительно обратимых пучков. Для пучков из свободно-кронекерова класса удалось явно выразить операторы обратного пучка.

В пятом параграфе исследуется функция Шеннона для классов полиномиальных форм. Выясняется, как отражаются отношения между классами пучков на поведение функции Шеннона для полиномиальных форм, как влияет на ее поведение выбор базисной функций. В частности показано, что функция Шеннона для классов полиномиальных форм не зависит от выбора базисной функции.

В шестом параграфе рассматривается проблема точных оценок сложности полиномиальных форм. Первые результаты по этой проблеме появились не так давно [2, 24]. В диссертации найдены точные значения функции Шеннона для некоторых классов полиномиальных форм.

Третья глава посвящена нахождению булевых функций, имеющих большую сложность в классах полиномиальных форм.

В седьмом параграфе диссертации найдена последовательность эффективно заданных функций, имеющих экспоненциальную сложность.

В восьмом параграфе доказывается ряд вспомогательных предложений, которые используются в дальнейшем изложении. Приведены некоторые свойства булевых функций, а также свойства сложности их представлений относительно различных операторных пучков.

В девятом параграфе для некоторых классов полиномиальных форм описаны все функции, имеющие в них наибольшую сложность.

В десятом параграфе описывается метод, позволяющий на основе результатов девятого параграфа найти функции наибольшей сложности в

полиномиальных формах, построенных по произвольной базисной функции, относительно достаточно широкого круга классов пучков.

В диссертации используются следующие утверждения: предложения, теоремы, леммы, следствия. Предложения носят вспомогательный характер, леммы используются для структурирования доказательств теорем. Нумерация теорем и предложений — сплошная, нумерация лемм — двойная: первым идет номер теоремы, вторым — порядковый номер леммы в теореме, следствия не нумеруются. В третьем параграфе формулируются несколько теорем, принадлежащих другим авторам. Такие теоремы нумеруются римскими числами. Формула нумеруются только в том случае, если на нее в тексте есть ссылка. Для формул используется двойная нумерация: первым идет номер главы, вторым — номер формулы в главе.

Начало и конец доказательства предложения, леммы или следствия будут обозначаться соответственно символами $\triangleright$ и $\triangleleft$, теоремы — $\blacktriangleright$ и $\blacktriangleleft$.

Терминология, используемая в диссертации, наиболее приближена к [23] и [56]. Там же можно найти все неопределенные в настоящей работе понятия и обозначения.

Глава 1. Классы полиномиальных форм

§ 1. Основные понятия и терминология

Следуя [8], наибольшее целое число, не превосходящее действительного числа a, будем обозначать $\lfloor a \rfloor$.

Символом $\mathbb{N}$ будем обозначать натуральный ряд $0, 1, 2, \ldots$.

Пусть $\sigma_i \in \{0, 1\}$, $i \in \{1, \ldots, n\}$, тогда выражение $\sigma_1, \sigma_2, \ldots, \sigma_n$ называется *двоичным набором* или просто *набором* и обозначается $\tilde{\sigma}$, а число n называется *длиной* этого набора. Если длина набора $\tilde{\sigma}$ явно не указана, она определяется по контексту. Множество всех наборов длины n будем обозначать через E^n. Очевидно, что количество наборов длины n равно 2^n. Набор $0, 0, \ldots, 0$ будет обозначаться через $\tilde{0}$, а набор $1, 1, \ldots, 1$ — через $\tilde{1}$. Размерность этих наборов всегда определяется по контексту. Существует единственный набор длины 0. Обозначим его $\varnothing$. Пусть $\tilde{\sigma} \in E^n$, $\tilde{\tau} \in E^m$, тогда под $\tilde{\sigma}, \tilde{\tau}$ будем понимать набор из E^{n+m}, построенный следующим образом:

$$\tilde{\sigma}, \tilde{\tau} = \sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m.$$

Введем в рассмотрение линейный порядок на E^n. Будем считать, что двоичные наборы $\tilde{\sigma}^1, \ldots, \tilde{\sigma}^m$, где $m = 2^n$, упорядочены по *натуральному порядку*, если для всех $s \in \{1, \ldots, m\}$ выполняется условие

$$s = 1 + \sum_{i=1}^{n} 2^{n-i} \cdot \sigma_i^s,$$

где $\tilde{\sigma}^s = \sigma_1^s, \ldots, \sigma_n^s$. Заметим, что двоичные наборы $\tilde{\sigma}^1, \ldots, \tilde{\sigma}^m$, $m = 2^n$, упорядоченные по натуральному порядку, представляют натуральные числа $0, \ldots, 2^n - 1$, записанные в двоичном исчислении. При натуральном порядке первым будет набор $\tilde{0}$, а последним — $\tilde{1}$. Двоичные наборы часто будут использоваться в качестве индексов. В этих случаях будем считать, что они упорядочены по натуральному порядку.

Булевой функцией или просто *функцией* называется отображение из $\{0,1\}^n$ в $\{0,1\}$. При этом n называется *размерностью* функции. Множество всех функций размерности n обозначается через F_n, множество всех функций — F. Если функция f имеет размерность n, то говорим, что функция f зависит от n *аргументов*. При отображении набора $\sigma_1, \ldots, \sigma_n$ функцией f будем считать, что i-й аргумент принимает значение σ_i, $i \in \{1, \ldots, n\}$.

Бывает удобно представлять функцию в векторном виде и в дальнейшем это представление часто используется.

Двоичный вектор $(\alpha_{\tilde{0}} \ldots \alpha_{\tilde{1}})_2$ *представляет функцию* $f \in F_n$, если $\alpha_{\tilde{\sigma}} = f(\tilde{\sigma})$, где наборы $\tilde{\sigma} \in E^n$ упорядочены по натуральному порядку. Заметим, что вектор, представляющий функцию размерности n, имеет длину 2^n.

Шестнадцатеричный вектор $(\Omega_1 \ldots \Omega_m)_{16}$ *представляет функцию* $f \in F_n$, если $n \geq 2$, $m = 2^{n-2}$ и

$$\Omega_i = 8 \cdot f(\tilde{\tau}^i, 0, 0) + 4 \cdot f(\tilde{\tau}^i, 0, 1) + 2 \cdot f(\tilde{\tau}^i, 1, 0) + 1 \cdot f(\tilde{\tau}^i, 1, 1),$$

где $\tilde{\tau}^1, \ldots, \tilde{\tau}^m$ — наборы из E^{n-2}, упорядоченные по натуральному порядку, и Ω_i записывается в шестнадцатеричном виде, $i \in \{1, \ldots, m\}$. В таблице 1 представлено соответствие между шестнадцатеричными цифрами, десятичными и двоичными числами.

hex	dec	bin	hex	dec	bin	hex	dec	bin	hex	dec	bin
0	0	0000	4	4	0100	8	8	1000	C	12	1100
1	1	0001	5	5	0101	9	9	1001	D	13	1101
2	2	0010	6	6	0110	A	10	1010	E	14	1110
3	3	0011	7	7	0111	B	11	1011	F	15	1111

Таблица 1

Следующие два вектора, двоичный и шестнадцатеричный, представляют одну и ту же функцию:

$$(11101000)_2, \qquad (E8)_{16}.$$

Широко используемым представлением в теории функций является представление термами.

Пусть $B \subseteq F$ и X — некоторое множество символов, называемых *переменными*. Индукцией определим понятие *терма над B от множества переменных X*:

1) переменная x из X есть терм;

2) если символом f обозначается функция размерности m, принадлежащая B, и $\Phi_1, \ldots, \Phi_m$ — термы, то $f(\Phi_1, \ldots, \Phi_m)$ есть терм.

Множество переменных, входящих в терм Φ, будет обозначаться $\chi(\Phi)$. Терм вида $f(x_1, \ldots, x_n)$, где $f \in B$ и $\{x_1, \ldots, x_n\} \subset X$, будем также называть функцией с именованными аргументами.

Для сокращения записи для некоторых функций в работе будут использованы специальные обозначения, которые представлены в таблице 2.

вектор	терм	название
$(0)_2$	0	тождественный ноль
$(1)_2$	1	тождественная единица
$(01)_2$	Φ	тождественная функция
$(10)_2$	$\overline{\Phi}$	отрицание
$(0001)_2$	$\Phi_1 \cdot \Phi_2$	конъюнкция
$(0111)_2$	$\Phi_1 \vee \Phi_2$	дизъюнкция
$(0110)_2$	$\Phi_1 \oplus \Phi_2$	сложение по модулю два

Таблица 2

Кроме того, будем опускать скобки, учитывая ассоциативность функций $\cdot$, $\vee$, $\oplus$, и используя приоритет этих функций. Приоритет функций в порядке убывания: $\cdot$, $\vee$, $\oplus$. Если $\alpha \in \{0, 1\}$, будем использовать обозначение:

$$\Phi^\alpha = \begin{cases} \overline{\Phi}, & \text{если } \alpha = 0; \\ \Phi, & \text{если } \alpha = 1. \end{cases}$$

Если $f \in F_0$, то вместо $f()$ будем писать f. Запись

$$\sum_{i \in I} \Phi_i$$

является сокращением для

$$\Phi_{i_1} \oplus \Phi_{i_2} \oplus \ldots \oplus \Phi_{i_m},$$

где $I = \{i_1, i_2, \ldots, i_m\}$ — некоторое конечное индексное множество.

В том случае, когда различные символы Φ и Ψ обозначают один и тот же терм, используем обозначение $\Phi \equiv \Psi$. Этот же символ используется и тогда, когда обозначения термов являются сложными выражениями, например $\Phi \equiv f(\Phi_1, \ldots, \Phi_n)$.

Выражение $x_1, \ldots, x_n$, где $x_i \in X$ при $i \in \{1, \ldots, n\}$, будем называть набором переменных и обозначать $\tilde{x}$, при этом n называется длиной набора переменных и чаще всего определяется по контексту.

Сопоставим набору переменных $x_1, \ldots, x_n$ один из наборов $\tilde{\sigma}$ множества E^n, при этом считаем, что задано *значение переменных* $\tilde{x}$, причем для переменной x_i задано значение σ_i, $i \in \{1, \ldots, n\}$. Определим *значение терма* Φ при заданных значениях переменных $x_1, \ldots, x_n$, где $\chi(\Phi) \subseteq \{x_1, \ldots, x_n\}$:
1) если Φ — переменная, то значение Φ совпадает со значением этой переменной;
2) если $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)$ и значения термов $\Phi_1, \ldots, \Phi_m$ есть $\tau_1, \ldots, \tau_m$ соответственно, то значение терма Φ есть $f(\tau_1, \ldots, \tau_m)$.

Пусть Φ и Ψ — термы. Если при любых значениях переменных из $\chi(\Phi) \cup \chi(\Psi)$ значения термов Φ и Ψ совпадают, то такие термы называются *эквивалентными*. Запись $\Phi = \Psi$ означает, что термы Φ и Ψ эквивалентны. Это отношение, очевидно, является отношением эквивалентности.

Пусть Φ — терм. Будем говорить, что *функция* $f \in F_n$ *представима термом* Φ, если существует упорядочение переменных $x_1, \ldots, x_n$ из множества $\chi(\Phi)$, такое что $\Phi = f(x_1, \ldots, x_n)$. *Многоместной* или n*-местной*

конъюнкцией называется функция, представимая термом $x_1 \cdot \ldots \cdot x_n$.

Остаточными функциями от функции f по i-му аргументу называются функции, размерности которых на единицу меньше размерности f. Обозначаются и определяются остаточные функции следующим образом:

$$f_i^{\sigma_i}(\tau_1, \ldots, \tau_{n-1}) = f(\tau_1, \ldots, \tau_{i-1}, \sigma_i, \tau_i, \ldots, \tau_{n-1})$$

для любого $\tilde{\tau} \in E^{n-1}$. Если $\sigma_i = 0$, то остаточная функция называется *нулевой остаточной*; если $\sigma_i = 1$, то — *единичной остаточной*.

Производной функцией от функции f по i-му аргументу называется функция, размерность которой на единицу меньше размерности f. Обозначается и определяется производная функция следующим образом:

$$f_i'(\tau_1, \ldots, \tau_{n-1}) = f_i^1(\tau_1, \ldots, \tau_{n-1}) \oplus f_i^0(\tau_1, \ldots, \tau_{n-1}),$$

для любого $\tilde{\tau} \in E^{n-1}$. Производную и остаточные функции будем также называть *обобщенно остаточными функциями*.

Понятие обобщенно остаточной функции индуктивно распространяется на множество аргументов $i_1, \ldots, i_s$, где $i_j \in \{1, \ldots, n-j+1\}$ при $1 \leq j \leq s \leq n$, следующим образом:

$$f_{i_1 \ldots i_s}^{\omega_1 \ldots \omega_s} = \begin{cases} \left(f_{i_1 \ldots i_{s-1}}^{\omega_1 \ldots \omega_{s-1}}\right)_{i_s}^1, & \text{если } \omega_s = 1; \\ \left(f_{i_1 \ldots i_{s-1}}^{\omega_1 \ldots \omega_{s-1}}\right)_{i_s}^0, & \text{если } \omega_s = 0; \\ \left(f_{i_1 \ldots i_{s-1}}^{\omega_1 \ldots \omega_{s-1}}\right)_{i_s}', & \text{если } \omega_s = \prime. \end{cases}$$

При этом s называется порядком обобщенно остаточной функции.

У функций с именованными аргументами при переходе к остаточным и производным будем сохранять именование аргументов:

$$f_{x_i}^{\omega_i}(x_1, \ldots, x_n) = f_i^{\omega_i}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n).$$

Непосредственно из определения следует, что

$$f_{x_{j_1} \ldots x_{j_m}}^{\omega_{j_1} \ldots \omega_{j_m}}(\tilde{x}) = f_{x_{i_1} \ldots x_{i_m}}^{\omega_{i_1} \ldots \omega_{i_m}}(\tilde{x})$$

для любой перестановки $j_1, \ldots, j_m$ индексов $i_1, \ldots, i_m$. Также легко проверить, что для любой функции $f \in F_n$

$$\big(f(x_1, \ldots, x_n)\big)'^{\ \ldots\ '}_{x_1 \ldots x_n} = \sum_{\tilde{\sigma}} f(\tilde{\sigma}).$$

Назовем i-й аргумент функции f *фиктивным*, если $f'_{x_i}(\tilde{x}) = 0$, и *существенным* в противном случае.

Функцию размерности n, не равную функции $f \in F_n$ ни на одном наборе из E^n, будем обозначать $\bar{f}$.

Функции g и f размерности n называются *однотипными*, если найдутся набор $\tilde{\sigma} \in E^n$ и перестановка $i_1, \ldots i_n$, такие что

$$g(x_{i_1}^{\sigma_1}, \ldots, x_{i_n}^{\sigma_n}) = f(x_1, \ldots, x_n).$$

Легко видеть, что отношение однотипности является отношением эквивалентности. Если M — некоторое множество функций, то $M^{\Diamond}$ — это множество однотипных им функций.

Функция $f \in F_n$ называется *симметрической*, если $f(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$ для любой перестановки $i_1, \ldots, i_n$.

Несколько обозначений для двоичных наборов и наборов переменных:

$$\overline{\tilde{\sigma}} = \bar{\sigma}_1, \ldots, \bar{\sigma}_n; \qquad \tilde{\sigma} \oplus \tilde{\tau} = \sigma_1 \oplus \tau_1, \ldots, \sigma_n \oplus \tau_n; \qquad \tilde{x}^{\tilde{\sigma}} = x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}.$$

Сквозь всю работу путеводной нитью проходят функции специального вида, которые впервые были использованы К. П. Шнорром [48] для получения высоких нижних оценок сложности в классе схем из функциональных элементов. Они определяются по индукции следующим образом:

$$\begin{gathered} p_0 = 0, \qquad q_0 = 1, \qquad r_0 = 1; \\ \begin{aligned} p_n(x_1, \ldots, x_n) &= x_n \cdot q_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot r_{n-1}(x_1, \ldots, x_{n-1}), \\ q_n(x_1, \ldots, x_n) &= x_n \cdot r_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}), \\ r_n(x_1, \ldots, x_n) &= x_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot q_{n-1}(x_1, \ldots, x_{n-1}). \end{aligned} \end{gathered} \tag{1.1}$$

Для удобства изложения введем множества, содержащие эти функции и их отрицания:

$$M_n = \{p_n, q_n, r_n\};$$
$$\overline{M}_n = \{p_n, q_n, r_n, \bar{p}_n, \bar{q}_n, \bar{r}_n\};$$
$$\widetilde{M}_n = \{p_n, q_n, r_n, \bar{p}_n\}.$$

Полиномиальной нормальной формой (пнф) называется терм вида

$$\sum_{i=1}^{m} \Psi_i, \tag{1.2}$$

где Ψ_i — *элементарные конъюнкции*, то есть выражения вида

$$x_{j_1}^{\sigma_1} \cdot x_{j_2}^{\sigma_2} \cdot \ldots \cdot x_{j_k}^{\sigma_k},$$

в которых все x_{j_s} различны, $\sigma_s \in \{0, 1\}$, $s \in \{1, \ldots, k\}$, $k \leq n$. Элементарной конъюнкцией при $k = 0$ будем считать константу 1. Под *сложностью* $L(\Phi)$ *полиномиальной нормальной формы* Φ понимают количество входящих в нее элементарных конъюнкций, то есть число m в (1.2).

Сложность $L_{\text{пнф}}(f)$ *функции* f *в классе полиномиальных нормальных форм* — это наименьшее число элементарных конъюнкций, необходимое для реализации ее в виде пнф:

$$L_{\text{пнф}}(f) = \min_{f(\tilde{x})=\Phi} L(\Phi),$$

здесь Φ — пробегает весь класс пнф.

Для оценок сложности представлений в теории булевых функций принято использовать *функцию Шеннона*, которая определяется как наибольшая сложность среди всех функций данной размерности в том или ином классе представлений. Отметим, что обычно функция Шеннона является целочисленной, хотя в некоторых работах используются функции Шеннона с рациональными и даже с действительными значениями.

Для класса полиномиальных нормальных форм функция Шеннона $L_{\text{пнф}}(n)$ определяется следующим образом:

$$L_{\text{пнф}}(n) = \max_{f \in F_n} L_{\text{пнф}}(f).$$

§ 2. Иерархия классов операторных пучков

Последовательность символов $\mathfrak{a}_1\mathfrak{a}_2\ldots\mathfrak{a}_n$, такая что $\mathfrak{a}_i \in \{\mathfrak{e},\mathfrak{p},\mathfrak{d}\}$ при $i \in \{1,2,\ldots,n\}$, называется *оператором* и обозначается $\mathfrak{a}$, ее члены называются *компонентами оператора*, а число n — *длиной* оператора. Пустая последовательность задает единственный оператор длины 0. Обозначим его $\emptyset$. Оператор $\mathfrak{a}$ длины n задает отображение из F_n в F_n по правилу $\mathfrak{a}f(\tilde{x}) = f_n(\tilde{x})$, где $f_n(\tilde{x})$ определяется по индукции следующим образом: $f_0(\tilde{x}) = f(\tilde{x})$,

$$f_i(\tilde{x}) = \begin{cases} f_{i-1}(\tilde{x}), & \text{если } \mathfrak{a}_i = \mathfrak{e}; \\ \hat{f}_{i-1}(\tilde{x}), & \text{если } \mathfrak{a}_i = \mathfrak{p}; \\ f_{i-1}(\tilde{x}) \oplus \hat{f}_{i-1}(\tilde{x}), & \text{если } \mathfrak{a}_i = \mathfrak{d}; \end{cases} \tag{1.3}$$

где $\hat{f}_{i-1}(\tilde{x}) = f_{i-1}(x_1,\ldots,x_{i-1},\bar{x}_i,x_{i+1},\ldots,x_n)$, $i \in \{1,\ldots,n\}$.

Множество, состоящее из 2^n операторов длины n называется *пучком операторов*, а число n называется *размерностью* этого пучка операторов. Пучки операторов будем также называть *операторными пучками* или просто *пучками*.

Упорядоченный набор $\left(\mathfrak{a}^{\tilde{0}},\ldots,\mathfrak{a}^{\tilde{1}}\right)$, содержащий все операторы из пучка A называется *нумерацией пучка*. Очевидно, что пучок однозначно определяется по своей нумерации. Если $\mathfrak{a}^{\tilde{\sigma}}$ — это оператор из какого-либо пучка, то запись $\mathfrak{a}_i^{\tilde{\sigma}}$ означает i-й компонент оператора $\mathfrak{a}^{\tilde{\sigma}}$.

Пучок операторов A размерности n называется *базисным*, если существует функция $g \in F_n$, такая что любую функцию $f \in F_n$ можно представить в виде линейной комбинации операторных образов функции g по операторам из A:

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}}\mathfrak{a}^{\tilde{\sigma}}g(\tilde{x}),$$

где $\alpha_{\tilde{\sigma}} \in \{0,1\}$ и $\left(\mathfrak{a}^{\tilde{0}},\ldots,\mathfrak{a}^{\tilde{1}}\right)$ — некоторая нумерация пучка A, то есть операторные образы функции g по операторам из A образуют базис линейного пространства всех функций размерности n. В [3] показано, что

если A — базисный пучок операторов размерности n, то для любой функции $g \in F_n$, удовлетворяющей свойству

$$\sum_{\tilde{\sigma}} g(\tilde{\sigma}) = 1,$$

ее операторные образы по операторам из A образуют базис всех функций размерности n. Такие функции будем называть *базисными*.

Пусть A — базисный пучок размерности n, $g \in F_n$ — базисная функция, тогда любая функция $f \in F_n$ может быть единственным образом с точностью до перестановки слагаемых представлена в виде *полиномиальной формы* Φ, построенной по A и g:

$$f(\tilde{x}) = \Phi, \qquad \Phi \equiv \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}), \tag{1.4}$$

где $\alpha_{\tilde{\sigma}} \in \{0, 1\}$ и $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — некоторая нумерация пучка A. Полиномиальная форма, построенная по базисному пучку и базисной функции одной и той же размерности, является *канонической* в том смысле, что каждая функция той же размерности представляется ею единственным образом с точностью до перестановки слагаемых. Отметим, что полиномиальная нормальная форма канонической не является. Под *сложностью* $L(\Phi)$ *полиномиальной формы* Φ будем понимать количество ненулевых слагаемых в ней, то есть число ненулевых коэффициентов $\alpha_{\tilde{\sigma}}$:

$$L(\Phi) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}}.$$

Отметим, что это определение согласуется с данным выше определением сложности полиномиальной нормальной формы. Поскольку произвольная функция $f \in F_n$ представляется в виде полиномиальной формы по A и g единственным образом, введем понятие сложности функции f. А именно, под *сложностью* $L^g_{\mathsf{A}}(f)$ *функции* f *относительно пучка* A *по функции* g понимаем сложность полиномиальной формы, построенной по A и g. В предыдущих обозначениях:

$$L^g_{\mathsf{A}}(f) = L(\Phi). \tag{1.5}$$

В дальнейшем будут введены различные классы базисных пучков. Теперь же определим функцию Шеннона для произвольного класса базисных пучков C. *Сложностью $L^g_C(f)$ функции f в классе базисных пучков C по базисной функции g* называется наименьшая сложность полиномиальной формы, реализующей функцию f:

$$L^g_C(f) = \min_{\mathsf{A}\in C} L^g_{\mathsf{A}}(f). \tag{1.6}$$

Отметим, что класс C может содержать пучки разных размерностей. В этом случае минимум берется только по тем пучкам, размерность которых совпадает с размерностью f. Кроме того размерности функций f и g также должны совпадать. *Функция Шеннона для класса базисных пучков C по базисной функции g* определяется обычным образом, как наибольшая сложность среди функций данной размерности:

$$L^g_C(n) = \max_{f\in F_n} L^g_C(f). \tag{1.7}$$

В дальнейшем, в качестве базисной функции g часто будет использоваться n-местная конъюнкция $x_1 \cdot x_2 \cdot \ldots \cdot x_n$. В этом случае вместо записи $L^g_{\mathsf{A}}(f)$ и $L^g_C(f)$ будем употреблять $L^{\&}_{\mathsf{A}}(f)$ и $L^{\&}_C(f)$ соответственно. Размерность конъюнкции однозначно определяется по функции f.

Пусть b, c — два покомпонентно неравных оператора длины n, то есть

$$\mathsf{b}_i \neq \mathsf{c}_i, \quad i \in \{1,\ldots,n\}.$$

Рассмотрим упорядоченный набор $\left(\mathfrak{a}^{\tilde{0}},\ldots,\mathfrak{a}^{\tilde{1}}\right)$, в котором компоненты операторов $\mathfrak{a}^{\tilde{\sigma}}$ определяются по формулам:

$$\mathfrak{a}^{\tilde{\sigma}}_i = \begin{cases} \mathsf{b}_i, & \text{если } \sigma_i = 0; \\ \mathsf{c}_i, & \text{если } \sigma_i = 1, \end{cases} \qquad i \in \{1,\ldots,n\}, \quad \tilde{\sigma} \in E^n. \tag{1.8}$$

Поскольку все $\mathfrak{a}^{\tilde{\sigma}}$ различны, $\left(\mathfrak{a}^{\tilde{0}},\ldots,\mathfrak{a}^{\tilde{1}}\right)$ является нумерацией некоторого пучка A размерности n. Будем называть такой пучок *двупорожденным*, а нумерацию $\left(\mathfrak{a}^{\tilde{0}},\ldots,\mathfrak{a}^{\tilde{1}}\right)$, удовлетворяющую (1.8), — *естественной*. Для двупорожденных пучков введем обозначение $\mathsf{A} = D(\mathsf{b},\mathsf{c})$, где

b и c — операторы, фигурирующие в (1.8). $D(\mathsf{a},\mathsf{b})$ является пучком размерности n. Из результатов работы [5] следует, что двупорожденные пучки являются базисными.

Пусть $\mathsf{A}=D(\mathsf{u},\mathsf{v})$ — двупорожденный операторный пучок размерности n с естественной нумерацией $\left(\mathsf{a}^{\tilde{0}},\ldots,\mathsf{a}^{\tilde{1}}\right)$, c — оператор длины n, удовлетворяющий условиям:

$$\mathsf{c}_i\neq\mathsf{u}_i,\quad \mathsf{c}_i\neq\mathsf{v}_i,\qquad i\in\{1,\ldots,n\},$$

$\tilde{\tau}$ — двоичный набор длины n. Тогда пучок B, определяемый своей нумерацией $\left(\mathsf{b}^{\tilde{0}},\ldots,\mathsf{b}^{\tilde{1}}\right)$ в которой

$$\mathsf{b}^{\tilde{\sigma}}=\begin{cases}\mathsf{a}^{\tilde{\sigma}}, & \text{если } \tilde{\sigma}\neq\tilde{\tau},\\ \mathsf{c}, & \text{если } \tilde{\sigma}=\tilde{\tau},\end{cases}\tag{1.9}$$

называется *расширением пучка* A *оператором* c, или просто *расширенным пучком*, а $\left(\mathsf{b}^{\tilde{0}},\ldots,\mathsf{b}^{\tilde{1}}\right)$ — его *естественной нумерацией*.

Пусть c — оператор длины n, тогда пучок A называется *однопорожденным*, или *порожденным оператором* a, если существует его нумерация $\left(\mathsf{a}^{\tilde{0}},\ldots,\mathsf{a}^{\tilde{1}}\right)$, компоненты операторов которой удовлетворяют условиям:

$$\mathsf{a}_i^{\tilde{\sigma}}=\mathsf{c}_i\quad\text{при}\quad\sigma_i=0,\qquad \mathsf{a}_i^{\tilde{\sigma}}\neq\mathsf{c}_i\quad\text{при}\quad\sigma_i=1,\qquad\tilde{\sigma}\in E^n,$$

при этом нумерация $\left(\mathsf{a}^{\tilde{0}},\ldots,\mathsf{a}^{\tilde{1}}\right)$ называется *естественной* нумерацией однопорожденного пучка A. В частности двупорожденные и расширенные пучки являются также и однопорожденными. Действительно, в качестве оператора c, порождающего однопорожденный пучок, нужно для случая двупорожденных пучков взять оператор b из (1.8), а для случая расширенных пучков — оператор $\mathsf{a}^{\overline{\tilde{\tau}}}$ из (1.9), при этом естественная нумерация в случае двупорожденных пучков сохраняется, а чтобы получить естественную нумерацию однопорожденного пучка из естественной нумерации расширенного, нужно верхний индекс оператора $\mathsf{b}^{\tilde{\sigma}}$ из (1.9) заменить на $\tilde{\sigma}\oplus\overline{\tilde{\tau}}$.

Существуют всего 3 базисных пучка размерности 1:

$$\{\mathfrak{e},\mathfrak{p}\};\quad \{\mathfrak{e},\mathfrak{d}\};\quad \{\mathfrak{p},\mathfrak{d}\}.$$

Их можно рассматривать и как двупорожденные, и как расширенные, и как однопорожденные. При этом любая нумерация этих пучков будет естественной.

Для операторов $\mathfrak{a}$ и $\mathfrak{b}$ длины n определим функционал «$\circ$» следующим образом:

$$\mathfrak{a}\circ\mathfrak{b}=\begin{cases}1, & \text{если } \mathfrak{a}_i\neq\mathfrak{b}_i \text{ для всех } i\in\{1,\ldots,n\};\\ 0, & \text{в противном случае.}\end{cases}$$

Для двух пучков A и B одинаковой размерности матрицу $M_{\mathsf{A}\times\mathsf{B}}$ будем называть *матрицей произведения этих пучков*:

$$M_{\mathsf{A}\times\mathsf{B}}=\begin{bmatrix}\mathfrak{a}^{\tilde{0}}\circ\mathfrak{b}^{\tilde{0}} & \cdots & \mathfrak{a}^{\tilde{0}}\circ\mathfrak{b}^{\tilde{1}}\\ \vdots & \ddots & \vdots\\ \mathfrak{a}^{\tilde{1}}\circ\mathfrak{b}^{\tilde{0}} & \cdots & \mathfrak{a}^{\tilde{1}}\circ\mathfrak{b}^{\tilde{1}}\end{bmatrix},$$

где $\left(\mathfrak{a}^{\tilde{0}},\ldots,\mathfrak{a}^{\tilde{1}}\right)$ и $\left(\mathfrak{b}^{\tilde{0}},\ldots,\mathfrak{b}^{\tilde{1}}\right)$ — некоторые нумерации пучков A и B соответственно. Легко видеть, что матрица произведения пучков определяется с точностью до перестановки строк и столбцов. Перестановке строк соответствует выбор другой нумерации пучка A, перестановке столбцов — нумерации пучка B.

Если $\mathsf{A}=\mathsf{B}$, тогда $M_{\mathsf{A}\times\mathsf{A}}$ будет называться *матрицей пучка* A и обозначаться M_{A}. Матрица пучка, как и матрица произведения пучков определяется с точностью до перестановки строк и столбцов.

В [3] показано, что пучок является базисным тогда и только тогда, когда его матрица невырожденная. Частным случаем невырожденных матриц являются диагональные и треугольные матрицы.

Пучок A называется *обратимым*, если существует пучок B той же размерности, такой что матрица $M_{\mathsf{A}\times\mathsf{B}}$ может быть приведена к диагональному виду перестановкой строк и столбцов. При этом пучок B называется *обратным* к пучку A.

Введем две операции, которые позволят нам получать из одних пучков другие.

Пусть A — пучок размерности n, $\mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}$ — 2^n пучков размерности m. Пусть $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — нумерация пучка A, $\left(\mathfrak{b}^{\tilde{0}}_{\tilde{\sigma}}, \ldots, \mathfrak{b}^{\tilde{1}}_{\tilde{\sigma}}\right)$ — нумерации пучков $\mathsf{B}_{\tilde{\sigma}}$, $\tilde{\sigma} \in E^n$. Тогда пучок C размерности $n+m$, определяемый своей нумерацией $\left(\mathfrak{c}^{\tilde{0}}, \ldots, \mathfrak{c}^{\tilde{1}}\right)$, операторы которой определяются по формулам:

$$\mathfrak{c}^{\tilde{\sigma},\tilde{\tau}} = \mathfrak{a}_1^{\tilde{\sigma}} \ldots \mathfrak{a}_n^{\tilde{\sigma}} \mathfrak{b}_1 \ldots \mathfrak{b}_m, \qquad \text{где } \mathfrak{b}_1 \ldots \mathfrak{b}_m = \mathfrak{b}_{\tilde{\delta}}^{\tilde{\tau}} \quad \tilde{\tau} \in E^m_{,} \quad \tilde{\sigma} \in E^n_{,} \tag{1.10}$$

называется *слиянием* пучков $\mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}$ по пучку A и обозначается:

$$\mathsf{C} = W(\mathsf{A} \mid \mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}).$$

При этом, если $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$, $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)_{\tilde{\sigma}}$ при $\tilde{\sigma} \in E^n$, — естественные нумерации соответствующих пучков, то нумерация $\left(\mathfrak{c}^{\tilde{0}}, \ldots, \mathfrak{c}^{\tilde{1}}\right)$, в которой $\mathfrak{c}^{\tilde{\sigma}}$ построены по формулам (1.10), также является естественной.

Пусть A — пучок размерности n и $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — его нумерация, а $i_1, \ldots, i_n$ — некоторая перестановка. Тогда пучок B размерности n, определяемый своей нумерацией $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$, где

$$\mathfrak{b}_{i_j}^{\tilde{\tau}} = \mathfrak{a}_j^{\tilde{\sigma}}, \qquad j \in \{1, \ldots, n\}, \quad \tilde{\tau} = \sigma_{i_1}, \ldots, \sigma_{i_n}, \quad \tilde{\sigma} \in E^n,$$

называется *перестановкой* пучка A и обозначается:

$$\mathsf{B} = I(\mathsf{A} \mid i_1, \ldots, i_n).$$

При этом, если $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — естественная нумерация пучка A, то нумерация $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$ является естественной для пучка B.

Пусть $\mathfrak{a}$ — оператор длины n. Класс, состоящий из двупорожденных пучков, для которых одним из порождающих является оператор $\mathfrak{a}$ называется $\mathfrak{a}$-*кронекеровым* и обозначается $K(\mathfrak{a})$:

$$K(\mathfrak{a}) = \{ D(\mathfrak{a}, \mathfrak{b}) \mid \mathfrak{b}_i \neq \mathfrak{a}_i, \ i \in \{1, \ldots, n\} \}.$$

Класс всех двупорожденных пучков называется *кронекеровым* и обо-

значается K:

$$K = \bigcup_{\mathfrak{a}} K(\mathfrak{a}).$$

Введем в рассмотрение еще один класс двупорожденных пучков. Пусть $\mathfrak{a}^0, \mathfrak{a}^1, \mathfrak{a}^2, \ldots$ — последовательность операторов длины $0, 1, 2, \ldots$ соответственно, все компоненты которых равны $\mathfrak{d}$. Тогда $\mathfrak{d}$-кронекеров класс пучков $K(\mathfrak{d} \ldots \mathfrak{d})$ определяется следующим образом:

$$K(\mathfrak{d} \ldots \mathfrak{d}) = \bigcup_{n \in \mathbb{N}} K(\mathfrak{a}_n).$$

Пусть $\mathfrak{a}$ — оператор длины n. Класс, состоящий из всех расширенных оператором $\mathfrak{a}$ пучков, называется $\mathfrak{a}$-*расширенным* и обозначается $E(\mathfrak{a})$.

Класс всех расширенных пучков называется *расширенным* и обозначается E:

$$E = \bigcup_{\mathfrak{a}} E(\mathfrak{a}).$$

Как и для случая двупорожденных пучков, определим $\mathfrak{d}$-*расширенный* класс пучков $E(\mathfrak{d} \ldots \mathfrak{d})$. Пусть $\mathfrak{a}^0, \mathfrak{a}^1, \mathfrak{a}^2, \ldots$ — последовательность операторов длины $0, 1, 2, \ldots$ соответственно, все компоненты которых равны $\mathfrak{d}$. Тогда $\mathfrak{d}$-расширенный класс пучков определяется следующим образом:

$$E(\mathfrak{d} \ldots \mathfrak{d}) = \bigcup_{n \in \mathbb{N}} E(\mathfrak{a}_n).$$

Пусть $\mathfrak{a}$ — оператор длины n. Класс, состоящий из всех однопорожденных пучков, порожденных оператором $\mathfrak{a}$, называется $\mathfrak{a}$-*обобщенным* и обозначается $G(\mathfrak{a})$.

Класс всех однопорожденных пучков называется *обобщенным* и обозначается G:

$$G = \bigcup_{\mathfrak{a}} G(\mathfrak{a}).$$

Свободно-кронекеров класс пучков FK определяется индуктивно по построению.

Шаг 0:

- $\{\emptyset\} \in FK$;
- $\{\mathsf{e}, \mathsf{p}\} \in FK$, $\{\mathsf{e}, \mathsf{d}\} \in FK$, $\{\mathsf{p}, \mathsf{d}\} \in FK$;

Шаг $i > 0$:

- если $\mathsf{A} \in FK$ — пучок размерности n; $\mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}} \in FK$ — 2^n пучков размерности m, причем A, $\mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}$ построены на предыдущих шагах, то $W(\mathsf{A} \mid \mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}) \in FK$;
- если $\mathsf{A} \in FK$ — пучок размерности n, построенный на предыдущих шагах, $i_1, \ldots, i_n$ — перестановка, то $I(\mathsf{A} \mid i_1, \ldots, i_n) \in FK$.

Класс, состоящий из всех пучков, матрицы которых можно привести к диагональному виду перестановкой строк и столбцов, называется *диагональным* и обозначается D.

Класс, состоящий из всех обратимых пучков, обозначается R.

Класс, состоящий из всех пучков, матрицы которых можно привести к треугольному виду перестановкой строк и столбцов, называется *треугольным* и обозначается T.

Класс всех базисных пучков обозначается OF.

Введенные классы базисных пучков образуют иерархию по включению, приведенную на рисунке 1. На нижнем уровне находятся классы без подписи. Это классы, состоящие из одного базисного пучка.

Каждому классу C пучков из иерархии соответствуют одноименные классы полиномиальных форм, то есть представлений вида (1.4), в котором используются пучки только из класса C и фиксированная базисная функция g.

Обозначения, использованные для классов операторных пучков, навеяны работами [36] и [56].

Обозначение K является сокращением от «Kronecker Form» [36]. Обозначение $K(\mathfrak{a})$ выбрано, потому что пучки, входящие в этот класс, строятся по тем же правилам, что и в K. В литературе часто исследуются классы, соответствующие $K(\mathsf{d} \ldots \mathsf{d})$, например, «Reed-Muller Form».

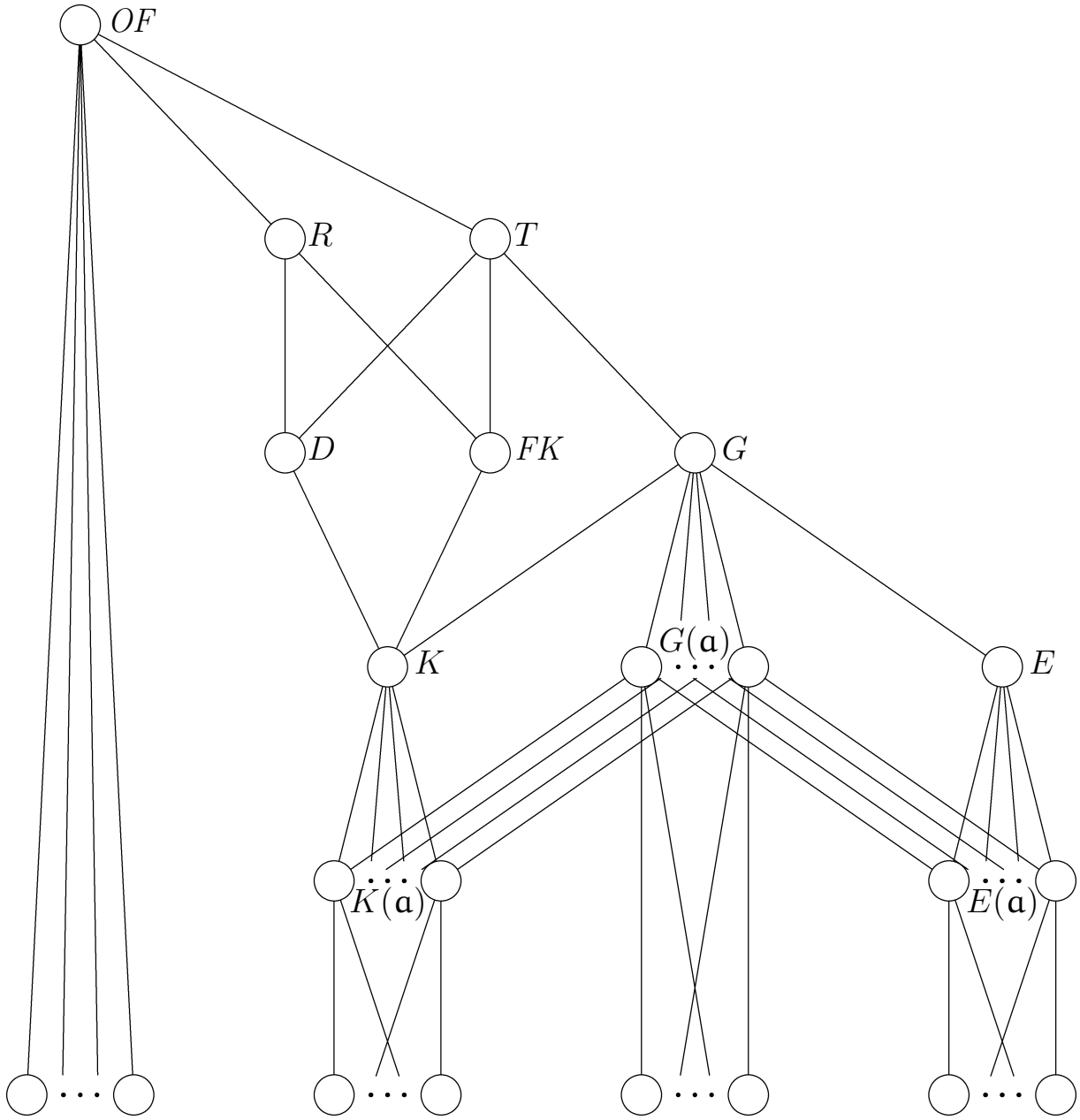

Рис. 1. Иерархия классов операторных пучков

Другие классы, соответствующие семейству $K(\mathfrak{a})$, ранее нигде не встречались, за исключением $K(\mathfrak{e}\dots\mathfrak{e})$ и $K(\mathfrak{p}\dots\mathfrak{p})$ [56].

Обозначение G — это сокращение от «Generalize Kronecker Form» [36]. Класс E до работы [56] нигде не встречался, его название происходит от «Extended». Обозначения $G(\mathfrak{a})$ и $E(\mathfrak{a})$ выбраны по тем же причинам, что и $K(\mathfrak{a})$. Ранее в литературе встречались аналоги классов $G(\mathfrak{d}\dots\mathfrak{d})$,

$G(\mathsf{e}\dots\mathsf{e})$, $G(\mathsf{p}\dots\mathsf{p})$, $E(\mathsf{d}\dots\mathsf{d})$. Для первого использовалось, например, название «pD/nD Fixed/Mixed Reed-Muller Form» [36].

Обозначение FK происходит от Free Kronecker Form [36]. Классы D и T предложены в [56], исходя из названий матриц (Diagonal, Triangle). Обозначение R — от Reversible. Класс OF (от Operator Form, [56]) — класс всех операторных пучков.

§ 3. Обзор результатов по полиномиальным формам

Первыми исследованиями по полиномиальным представлениям булевых функций были работы И.И. Жегалкина [9, 10].

В 50-х годах XX вновь возник интерес к полиномиальным формам в связи с приложениями в теории кодирования. Тогда же появились первые работы по сложности полиномиальных представлений булевых функций.

До конца 80-х годов XX века эти исследования ограничивались в основном полиномиальными нормальными формами, поляризованными полиномами Жегалкина, формами Рида-Маллера и кронекеровыми формами. Эти формы в терминологии диссертации соответствуют классам OF, $K(\mathsf{d}\dots\mathsf{d})$, K с фиксированной базисной функцией — многоместной конъюнкцией.

В работе [7] были рассмотрены полиномиальные формы по функциям, отличным от многоместной конъюнкции. Исследования в этой области привели к следующему результату.[1]

Теорема I ([5]) *По произвольному базисному пучку* A *с нумерацией* $\left(\mathfrak{a}^{\tilde{0}},\dots,\mathfrak{a}^{\tilde{1}}\right)$, *произвольной базисной функции* $g \in F_n$, *любая функция* $f \in F_n$ *имеет единственное представление вида:*

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}), \qquad \textit{где} \qquad \alpha_{\tilde{\sigma}} = \sum_{\tilde{\tau}} c_{\tilde{\sigma}\tilde{\tau}} \cdot f(\tilde{\tau}).$$

[1] Здесь и далее формулировки изменены в соответствии со введенной в диссертации терминологией.

В этой теореме вычисление $c_{\tilde{\sigma}\tilde{\tau}}$ связано с нахождением обратной матрицы к некоторой матрице размера $2^n \times 2^n$.

С конца 80-х годов XX века в связи с приложениями в цифровой технике стали рассматриваться самые разнообразные полиномиальные формы. Они стали объединяться в различные иерархии. Одна из них представлена в диссертации.

Встали вопросы эффективного нахождения коэффициентов представлений без нахождения обратной матрицы. В этом направлении были получены следующие результаты.

Теорема II ([3]) *По любому пучку $\mathsf{A} \in K$ с естественной нумерацией $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$, любой базисной функции $g \in F_n$, любая функция $f \in F_n$ имеет единственное представление вида:*

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}), \qquad \textit{при этом} \quad \alpha_{\tilde{\sigma}} = \left(f(\tilde{x}) \cdot \mathfrak{a}^{\overline{\tilde{\sigma}}} g(\overline{\tilde{x}})\right)'^{\ \ldots\ '}_{x_1 \ldots x_n}.$$

Теорема III ([6]) *По любому пучку $\mathsf{A} \in G$ с естественной нумерацией $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$, любой базисной функции $g \in F_n$, любая функция $f \in F_n$ имеет единственное представление вида:*

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}), \qquad \textit{при этом} \quad \alpha_{\tilde{\sigma}} = \sum_{\tilde{\tau}} c_{\tilde{\sigma}\tilde{\tau}}.$$

Здесь $c_{\tilde{\sigma}\tilde{\tau}}$ вычисляются по операторам пучка A с привлечением понятия сопутствующего пучка (см. [56]), но без вычисления обратной матрицы.

Теорема IV ([56]) *По любому пучку $\mathsf{A} \in E(\mathfrak{b})$ с естественной нумерацией $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$, любой базисной функции $g \in F_n$, любая функция $f \in F_n$ имеет единственное представление вида:*

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}),$$

$$\textit{при этом} \quad \alpha_{\tilde{\sigma}} = \begin{cases} \left(f(\tilde{x}) \cdot \mathfrak{a}^{\overline{\tilde{\sigma}}} g(\overline{\tilde{x}}) \oplus f(\tilde{x}) \cdot \mathfrak{b} g(\overline{\tilde{x}})\right)'^{\ \ldots\ '}_{x_1 \ldots x_n}, & \textit{если } \mathfrak{a}^{\tilde{\sigma}} \neq \mathfrak{b}; \\ \left(f(\tilde{x}) \cdot \mathfrak{a}^{\overline{\tilde{\sigma}}} g(\overline{\tilde{x}})\right)'^{\ \ldots\ '}_{x_1 \ldots x_n}, & \textit{если } \mathfrak{a}^{\tilde{\sigma}} = \mathfrak{b}. \end{cases}$$

Теорема 1 *Пусть* A *— обратимый пучок размерности* n *и* B *— пучок, обратный к нему,* $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ *и* $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$ *— их нумерации, такие что матрица*

$$\begin{bmatrix} \mathfrak{a}^{\tilde{0}} \circ \mathfrak{b}^{\tilde{0}} & \cdots & \mathfrak{a}^{\tilde{0}} \circ \mathfrak{b}^{\tilde{1}} \\ \vdots & \ddots & \vdots \\ \mathfrak{a}^{\tilde{1}} \circ \mathfrak{b}^{\tilde{0}} & \cdots & \mathfrak{a}^{\tilde{1}} \circ \mathfrak{b}^{\tilde{1}} \end{bmatrix}$$

является диагональной. Тогда для любой базисной функции $g \in F_n$ *любая функция* $f \in F_n$ *имеет единственное полиномиальное представление вида*

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}), \qquad \textit{при этом} \qquad \alpha_{\tilde{\sigma}} = \left(f(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)'^{\ \ldots\ '}_{x_1 \ldots x_n}.$$

Следствие ([54]) *Для любого пучка* $\mathsf{A} \in FK$ *размерности* n *с естественной нумерацией* $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$*, любой базисной функции* $g \in F_n$ *любая функция* $f \in F_n$ *имеет единственное представление вида*

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}), \qquad \textit{при этом} \qquad \alpha_{\tilde{\sigma}} = \left(f(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)'^{\ \ldots\ '}_{x_1 \ldots x_n},$$

и компоненты операторов $\mathfrak{b}^{\tilde{\sigma}}$ *определяются по формулам:* $\mathfrak{b}_i^{\tilde{\sigma}} = \mathfrak{a}_i^{\tilde{\tau}}$*, где* $\tilde{\tau} = \sigma_1, \ldots, \sigma_{i-1}, \bar{\sigma}_i, \sigma_{i+1}, \ldots, \sigma_n$.

Вопросы сложности представления булевых функций традиционно являются наиболее интересными и в теории, и в практических приложениях. Связь между сложностью операторных полиномиальных форм и сложностью полиномиальных нормальных форм была установлена в [3].

Теорема V ([3]) *Для любой функции* $f \in F_n$

$$L_{\text{пнф}}(f) = L^{\&}_{OF}(f).$$

Зависимость функции Шеннона от выбора базисной функции исследовалась в [55].

Теорема 2 ([55]) *Для любого класса* C *базисных пучков значение функции Шеннона* $L^g_C(n)$ *не зависит от выбора базисной функции* g.

В дальнейшем вместо $L_C^g(n)$ используется обозначение $L_C(n)$.

Точные оценки сложности являются самыми желанными результатами. Впервые точная оценка сложности полиномиальных форм была получена в [24].

Теорема VI ([24]) *Значение функции Шеннона для класса* $K(\mathfrak{d}\ldots\mathfrak{d})$ *по функции многоместной конъюнкции определяется по формуле:*

$$L^{\&}_{K(\mathfrak{d}\ldots\mathfrak{d})}(n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

Затем еще для серии классов были найдены точные оценки сложности.

Теорема VII ([2, 55]) *Значение функции Шеннона для класса* K *определяется по формуле:*

$$L_K(n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

Теорема VIII ([56]) *Для любого оператора* $\mathfrak{a}$ *длины* n *значение функции Шеннона для класса* $E(\mathfrak{a})$ *вычисляется по формуле:*

$$L_{E(\mathfrak{a})}(n) = \frac{1}{2} \cdot 2^n.$$

Теорема 3 ([59]) *Пусть* $\mathfrak{a}$ *— произвольный оператор длины* n*. Тогда*

$$L_{K(\mathfrak{a})}(n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

Теорема 4 ([54]) *Точное значение функции Шеннона для класса* FK *вычисляется по следующей формуле:*

$$L_{FK}(n) = \frac{1}{2} \cdot 2^n.$$

С 60-х годов известна нижняя оценка сложности полиномиальных нормальных форм.

Теорема IX ([37]) *Для функции Шеннона для класса полиномиальных нормальных форм справедлива следующая оценка:*

$$L_{\text{пнф}}(n) \geq \frac{2^n}{n \cdot \log_2 3}.$$

Наилучшая из верхних оценок для этого класса получена в [13].

Теорема X ([13]) *При $n = 2^k$ справедливо следующее неравенство:*

$$L_{\text{пнф}}(n) \leq \frac{2^n \cdot (1 + \log_2 n)}{n}.$$

Несмотря на существование высокой нижней оценки функции Шеннона класса полиномиальных форм, поиск функций большой сложности представляет определенный интерес, так как теорема IX не дает метода нахождения таких функций. В следующей теореме из [58] доказана экспоненциальная нижняя оценка для эффективно заданных функций.

Теорема 5 ([58]) *Если $f \in M_n$, то*

$$L_{\text{пнф}}(f) \geq \left(\frac{3}{2}\right)^{n-1}.$$

Поиск сложных функций для других классов полиномиальных форм привел к следующим результатам, в которых описаны все функции наибольшей сложности для различных классов операторных полиномиальных форм.

Теорема 6 ([52]) *Пусть $f \in F_n$, $n \geq 1$. Тогда следующие условия эквивалентны:*

1) $L^{\&}_{K(\mathrm{d}\ldots\mathrm{d})}(f) = L_{K(\mathrm{d}\ldots\mathrm{d})}(n)$;
2) $f \in M_n^{\Diamond}$ *при нечетном* n, $f \in \widetilde{M}_n^{\Diamond}$ *при четном* n.

Теорема 7 ([52, 57]) *Если $f \in F_n$, $n \geq 1$, то $L^{\&}_K(f) = L_K(n)$ тогда и только тогда, когда $f \in M_n^{\Diamond}$.*

Теорема 8 ([54, 59]) *Если $f \in F_n$, $n \geq 1$, то $L^{\&}_{FK}(f) = L_{FK}(n)$ тогда и только тогда, когда $f \in M_n^{\Diamond}$.*

Теорема 9 ([59]) *Если $f \in F_n$, $n \geq 1$, то $L^{\&}_{E(\mathrm{d}\ldots\mathrm{d})}(f) = L_{E(\mathrm{d}\ldots\mathrm{d})}(n)$ тогда и только тогда, когда*

$$\frac{1}{2} \cdot 2^n \leq \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \leq \frac{1}{2} \cdot 2^n + 1.$$

Глава 2. Функция Шеннона и нахождение коэффициентов полиномиальных форм

Вторая глава посвящена нахождению функции Шеннона для некоторых классов полиномиальных форм и формул для вычисления коэффициентов разложений.

В четвертом параграфе рассматривается вопрос нахождения коэффициентов полиномиальных форм. В настоящей работе получены ранее неизвестные формулы вычисления коэффициентов в классе полиномиальных форм относительно обратимых пучков. Для пучков из свободно-кронекерова класса удалось явно выразить операторы обратного пучка.

В пятом параграфе исследуется функция Шеннона для классов полиномиальных форм. Выясняется, как отражаются отношения между классами пучков на поведение функции Шеннона для полиномиальных форм, как влияет на ее поведение выбор базисной функций.

В шестом параграфе рассматривается проблема точных оценок сложности полиномиальных форм. В диссертации найдены точные значения функции Шеннона для некоторых классов полиномиальных форм.

§ 4. Коэффициенты полиномиальных форм по обратимым операторам

Следующая теорема дает формулы вычисления коэффициентов полиномиальных форм по обратимым операторным пучкам.

Теорема 1 *Пусть* A *— обратимый пучок размерности* n *и* B *— пучок, обратный к нему,* $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ *и* $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$ *— их нумерации, такие что матрица*

$$\begin{bmatrix} \mathfrak{a}^{\tilde{0}} \circ \mathfrak{b}^{\tilde{0}} & \cdots & \mathfrak{a}^{\tilde{0}} \circ \mathfrak{b}^{\tilde{1}} \\ \vdots & \ddots & \vdots \\ \mathfrak{a}^{\tilde{1}} \circ \mathfrak{b}^{\tilde{0}} & \cdots & \mathfrak{a}^{\tilde{1}} \circ \mathfrak{b}^{\tilde{1}} \end{bmatrix} \tag{2.1}$$

является диагональной. Тогда для любой базисной функции $g \in F_n$ любая функция $f \in F_n$ имеет единственное полиномиальное представление вида

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}), \qquad \textit{при этом} \qquad \alpha_{\tilde{\sigma}} = \left(f(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)'^{\dots\,'}_{x_1 \dots x_n}.$$

▶ Для доказательства воспользуемся методом, предложенным в [14].

По определению производной, справедлива следующая цепочка равенств:

$$\left(f(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)'^{\dots\,'}_{x_1 \dots x_n} = \sum_{\tilde{\tau}} \left(f(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n} = \sum_{\tilde{\tau}} f(\tilde{\tau}) \cdot \left(\mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n}.$$

Введем обозначение

$$h(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}).$$

и проведем несколько преобразований:

$$\begin{aligned} h(\tilde{x}) &= \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}) = \\ &= \sum_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}) \cdot \left(f(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)'^{\dots\,'}_{x_1 \dots x_n} = \\ &= \sum_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}) \cdot \sum_{\tilde{\tau}} f(\tilde{\tau}) \cdot \left(\mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n} = \\ &= \sum_{\tilde{\tau}} f(\tilde{\tau}) \cdot \sum_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}) \cdot \left(\mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n}. \end{aligned}$$

Значение $h(\tilde{x})$ на наборе $\tilde{\delta}$ будет равно

$$h(\tilde{\delta}) = \sum_{\tilde{\tau}} f(\tilde{\tau}) \cdot \sum_{\tilde{\sigma}} \left(\mathfrak{a}^{\tilde{\sigma}} g(\tilde{x})\right)^{\delta_1 \dots \delta_n}_{x_1 \dots x_n} \cdot \left(\mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n}.$$

Пусть V, W — матрицы размера $2^n \times 2^n$, элементы которых вычисляются по формулам:

$$v_{\tilde{\sigma}\tilde{\tau}} = \left(\mathfrak{a}^{\tilde{\sigma}} g(\tilde{x})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n}, \qquad w_{\tilde{\tau}\tilde{\sigma}} = \left(\mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n}.$$

Рассмотрим элемент произведения матриц $U = V \cdot W$:

$$u_{\tilde{\sigma}\tilde{\tau}} = \sum_{\tilde{\delta}} v_{\tilde{\sigma}\tilde{\delta}} \cdot w_{\tilde{\delta}\tilde{\tau}}.$$

Из [3] известно, что для любой базисной функции $g \in F_n$, для любых двух пучков $\mathfrak{a}$ и $\mathfrak{b}$ размерности n выполняется:

$$\mathfrak{a} \circ \mathfrak{b} = (\mathfrak{a}g(\tilde{x}) \cdot \mathfrak{b}g(\tilde{x}))'^{\dots\,'}_{x_1 \dots x_n}.$$

Используя это равенство, получим:

$$u_{\tilde{\sigma}\tilde{\tau}} = \sum_{\tilde{\delta}} \left(\mathfrak{a}^{\tilde{\sigma}} g(\tilde{x})\right)^{\delta_1 \dots \delta_n}_{x_1 \dots x_n} \cdot \left(\mathfrak{b}^{\tilde{\tau}} g(\overline{\tilde{x}})\right)^{\delta_1 \dots \delta_n}_{x_1 \dots x_n} =$$

$$= \sum_{\tilde{\delta}} \left(\mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\tau}} g(\overline{\tilde{x}})\right)^{\delta_1 \dots \delta_n}_{x_1 \dots x_n} = \left(\mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\tau}} g(\overline{\tilde{x}})\right)'^{\dots\,'}_{x_1 \dots x_n} = \mathfrak{a}^{\tilde{\sigma}} \circ \mathfrak{b}^{\tilde{\tau}}.$$

Поскольку матрица (2.1) — диагональная, то

$$u_{\tilde{\sigma}\tilde{\tau}} = \begin{cases} 1, & \text{если } \tilde{\sigma} = \tilde{\tau}; \\ 0, & \text{если } \tilde{\sigma} \neq \tilde{\tau}. \end{cases}$$

Таким образом, матрица U — единичная. Поэтому $U = W \cdot V$. Тогда

$$u_{\tilde{\tau}\tilde{\delta}} = \sum_{\tilde{\sigma}} w_{\tilde{\tau}\tilde{\sigma}} \cdot v_{\tilde{\sigma}\tilde{\delta}} = \sum_{\tilde{\sigma}} \left(\mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n} . \cdot \left(\mathfrak{a}^{\tilde{\sigma}} g(\tilde{x})\right)^{\delta_1 \dots \delta_n}_{x_1 \dots x_n}.$$

Следовательно, для $h(\tilde{\delta})$ справедливо:

$$h(\tilde{\delta}) = \sum_{\tilde{\tau}} f(\tilde{\tau}) \cdot \sum_{\tilde{\sigma}} \left(\mathfrak{a}^{\tilde{\sigma}} g(\tilde{x})\right)^{\delta_1 \dots \delta_n}_{x_1 \dots x_n} . \left(\mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)^{\tau_1 \dots \tau_n}_{x_1 \dots x_n} = \sum_{\tilde{\tau}} f(\tilde{\tau}) \cdot u_{\tilde{\tau}\tilde{\delta}} = f(\tilde{\delta}).$$

Поскольку $\tilde{\delta}$ — произвольный набор, $h(\tilde{x}) = f(\tilde{x})$, то есть

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}).$$

Теорема доказана. ◀

Следствие *Для любого пучка $\mathsf{A} \in FK$ размерности n с естественной нумерацией $\left(\mathfrak{a}^{\tilde{0}}, \dots, \mathfrak{a}^{\tilde{1}}\right)$, любой базисной функции $g \in F_n$ любая функция $f \in F_n$ имеет единственное представление вида*

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}), \qquad \textit{при этом} \quad \alpha_{\tilde{\sigma}} = \left(f(\tilde{x}) \cdot \mathfrak{b}^{\tilde{\sigma}} g(\overline{\tilde{x}})\right)'^{\dots\,'}_{x_1 \dots x_n},$$

и $\left(\mathfrak{b}^{\tilde{0}}, \dots, \mathfrak{b}^{\tilde{1}}\right)$ — нумерация обратного к A пучка B, компоненты операторов которого определяются по формулам:

$$\mathfrak{b}_i^{\tilde{\sigma}} = \mathfrak{a}_i^{\tilde{\tau}}, \qquad \textit{где} \quad \tilde{\tau} = \sigma_1, \dots, \sigma_{i-1}, \bar{\sigma}_i, \sigma_{i+1}, \dots, \sigma_n, \quad \tilde{\sigma} \in E^n. \qquad (2.2)$$

▷ Доказательство. Индукцией по построению пучка A покажем, что $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$ является нумерацией некоторого пучка B, и что $\mathfrak{a}^{\tilde{\tau}} \circ \mathfrak{b}^{\tilde{\sigma}} = 1$ тогда и только тогда, когда $\tilde{\tau} = \tilde{\sigma}$. Это будет означать, что матрица (2.1) — диагональная, и тогда, применив теорему 1, получим утверждение следствия.

Базис индукции. Для пучка $\{\emptyset\}$ доказывать нечего. Если A — один из пучков $\{e, \mathfrak{p}\}$, $\{e, \mathfrak{d}\}$, $\{\mathfrak{p}, \mathfrak{d}\}$ и $\left(\mathfrak{a}^0, \mathfrak{a}^1\right)$ — его произвольная нумерация, которая по определению является естественной, то из (2.2) следует, что $\left(\mathfrak{b}^0, \mathfrak{b}^1\right) = \left(\mathfrak{a}^1, \mathfrak{a}^0\right)$. Тогда $\mathsf{B} = \mathsf{A}$ и очевидно, что $\mathfrak{a}^\tau \circ \mathfrak{b}^\sigma = 1$ тогда и только тогда, когда $\tau = \sigma$.

Шаг индукции. По определению класса FK, пучок A построен перестановкой или слиянием пучков из FK.

Пусть $\mathsf{A} = I(\hat{\mathsf{A}} \mid i_1, \ldots, i_n)$, $\left(\hat{\mathfrak{a}}^{\tilde{0}}, \ldots, \hat{\mathfrak{a}}^{\tilde{1}}\right)$ — естественная нумерация пучка $\hat{\mathsf{A}}$. По предположению индукции набор операторов $\left(\hat{\mathfrak{b}}^{\tilde{0}}, \ldots, \hat{\mathfrak{b}}^{\tilde{1}}\right)$, компоненты операторов которых определяются по формулам (2.2) с использованием операторов из пучка $\hat{\mathsf{A}}$, является нумерацией обратного к $\hat{\mathsf{A}}$ пучка $\hat{\mathsf{B}}$. Тогда $\mathfrak{b}^{\tilde{\sigma}}_{i_j} = \mathfrak{a}^{\tilde{\tau}}_{i_j} = \hat{\mathfrak{a}}^{\tilde{\upsilon}}_j = \hat{\mathfrak{b}}^{\tilde{\delta}}_j$, где $\tilde{\sigma}$, $\tilde{\tau}$, $\tilde{\upsilon}$ и $\tilde{\delta}$ связаны соотношениями:

$$\tilde{\tau} = \sigma_1, \ldots, \sigma_{i_j-1}, \bar{\sigma}_{i_j}, \sigma_{i_j+1}, \ldots, \sigma_n; \quad \tilde{\tau} = \upsilon_{i_1}, \ldots, \upsilon_{i_n};$$
$$\tilde{\upsilon} = \delta_1, \ldots, \delta_{j-1}, \bar{\delta}_j, \delta_{j+1}, \ldots, \delta_n.$$

Тогда $\tilde{\sigma} = \delta_{i_1}, \ldots, \delta_{i_n}$, и, следовательно, набор $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$ является нумерацией пучка $\mathsf{B} = I(\hat{\mathsf{B}} \mid i_1, \ldots, i_n)$.

По предположению индукции $\hat{\mathfrak{a}}^{\tilde{\upsilon}} \circ \hat{\mathfrak{b}}^{\tilde{\delta}} = 1$ тогда и только тогда, когда $\tilde{\upsilon} = \tilde{\delta}$. Тогда из определения перестановки следует, что $\mathfrak{a}^{\tilde{\tau}} \circ \mathfrak{b}^{\tilde{\sigma}} = 1$ тогда и только тогда, когда $\tilde{\tau} = \tilde{\sigma}$.

Пусть $\mathsf{A} = W(\hat{\mathsf{A}} \mid \check{\mathsf{A}}_{\tilde{0}}, \ldots, \check{\mathsf{A}}_{\tilde{1}})$, где размерность пучка $\hat{\mathsf{A}}$ равна k, а размерность пучков $\check{\mathsf{A}}_{\tilde{0}}, \ldots, \check{\mathsf{A}}_{\tilde{1}}$ равна $n - k$. Пусть

$$\left(\hat{\mathfrak{a}}^{\tilde{0}}, \ldots, \hat{\mathfrak{a}}^{\tilde{1}}\right), \left(\check{\mathfrak{a}}^{\tilde{0}}_{\tilde{0}}, \ldots, \check{\mathfrak{a}}^{\tilde{1}}_{\tilde{0}}\right), \ldots, \left(\check{\mathfrak{a}}^{\tilde{0}}_{\tilde{1}}, \ldots, \check{\mathfrak{a}}^{\tilde{1}}_{\tilde{1}}\right) \ —$$

естественные нумерации соответствующих пучков. Наборы $\bigl(\hat{\mathsf{b}}^{\tilde{0}},\dots,\hat{\mathsf{b}}^{\tilde{1}}\bigr)$, $\bigl(\check{\mathsf{b}}^{\tilde{0}}_{\tilde{\sigma}},\dots,\check{\mathsf{b}}^{\tilde{1}}_{\tilde{\sigma}}\bigr)$, где $\tilde{\sigma}\in E^n$, построенные по формулам (2.2) с использованием операторов из пучков $\hat{A}$, $\check{A}_{\tilde{\sigma}}$ соответственно, удовлетворяют предположению индукции. Поэтому, $\hat{\mathsf{a}}^{\tilde{\delta}}\circ\hat{\mathsf{b}}^{\tilde{\tau}}=1$ тогда и только тогда, когда $\tilde{\delta}=\tilde{\tau}$, и $\check{\mathsf{a}}^{\tilde{\delta}}_{\tilde{\sigma}}\circ\check{\mathsf{b}}^{\tilde{\tau}}_{\tilde{\sigma}}=1$ тогда и только тогда, когда $\tilde{\delta}=\tilde{\tau}$.

По определению слияния

$$\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}=\hat{\mathsf{a}}^{\tilde{\sigma}}_1\dots\hat{\mathsf{a}}^{\tilde{\sigma}}_k\mathsf{c}_1\dots\mathsf{c}_{n-k},\quad\text{где}\quad\mathsf{c}_1\dots\mathsf{c}_{n-k}=\check{\mathsf{a}}^{\tilde{\tau}}_{\tilde{\sigma}},\quad\tilde{\sigma}\in E^k,\quad\tilde{\tau}\in E^{n-k}.$$

Пусть $\tilde{\upsilon}\neq\tilde{\sigma}$, $\tilde{\upsilon}\in E^k$, и пусть $\tilde{\delta}\in E^{n-k}$. По предположению индукции $\hat{\mathsf{a}}^{\tilde{\sigma}}\circ\hat{\mathsf{b}}^{\tilde{\upsilon}}=0$, то есть существует $i\in\{1,\dots,k\}$, такое что $\hat{\mathsf{a}}^{\tilde{\sigma}}_i=\hat{\mathsf{b}}^{\tilde{\upsilon}}_i$. Тогда $\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}_i=\hat{\mathsf{a}}^{\tilde{\sigma}}_i=\hat{\mathsf{b}}^{\tilde{\upsilon}}_i$. С другой стороны,

$$\mathsf{b}^{\tilde{\upsilon},\tilde{\delta}}_i=\mathsf{a}^{\tilde{\varrho},\tilde{\delta}}_i=\hat{\mathsf{a}}^{\tilde{\varrho}}_i=\hat{\mathsf{b}}^{\tilde{\upsilon}}_i,\quad\text{где}\quad\tilde{\varrho}=\upsilon_1,\dots,\upsilon_{i-1},\bar{\upsilon}_i,\upsilon_{i+1},\dots\upsilon_k.$$

Поэтому $\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}_i=\mathsf{b}^{\tilde{\upsilon},\tilde{\delta}}_i$. Следовательно,

$$\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}\circ\mathsf{b}^{\tilde{\upsilon},\tilde{\delta}}=0\qquad\text{при}\quad\tilde{\upsilon}\neq\tilde{\sigma}.\tag{2.3}$$

Пусть $\tilde{\delta}\neq\tilde{\tau}$, $\tilde{\delta}\in E^{n-k}$. По предположению индукции $\check{\mathsf{a}}^{\tilde{\tau}}_{\tilde{\sigma}}\circ\check{\mathsf{b}}^{\tilde{\delta}}_{\tilde{\sigma}}=0$. Введем обозначения: $\mathsf{s}=\check{\mathsf{a}}^{\tilde{\tau}}_{\tilde{\sigma}}$, $\mathsf{t}=\check{\mathsf{a}}^{\tilde{\tau}}_{\tilde{\sigma}}$. По определению функционала «$\circ$» существует $i\in\{1,\dots,n-k\}$, такое что $\mathsf{s}_i=\mathsf{t}_i$. Тогда $\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}_{k+i}=\mathsf{s}_i=\mathsf{t}_i$. С другой стороны,

$$\mathsf{b}^{\tilde{\sigma},\tilde{\delta}}_{n+i}=\mathsf{a}^{\tilde{\sigma},\tilde{\varrho}}_{n+i}=\mathsf{c}_i=\mathsf{t}_i,\quad\text{где}\quad\mathsf{c}=\check{\mathsf{a}}^{\tilde{\varrho}}_{\tilde{\sigma}},\quad\tilde{\varrho}=\delta_1,\dots,\delta_{i-1},\bar{\delta}_i,\delta_{i+1},\dots\delta_k.$$

Поэтому $\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}_i=\mathsf{b}^{\tilde{\sigma},\tilde{\delta}}_i$. Следовательно,

$$\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}\circ\mathsf{b}^{\tilde{\sigma},\tilde{\delta}}=0\qquad\text{при}\quad\tilde{\delta}\neq\tilde{\tau}.\tag{2.4}$$

Рассмотрим значение выражение $\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}\circ\mathsf{b}^{\tilde{\sigma},\tilde{\tau}}$. Пусть $i\in\{1,\dots,k\}$. Тогда по предположению индукции и по определению слияния пучков $\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}_i=\hat{\mathsf{a}}^{\tilde{\sigma}}_i\neq\hat{\mathsf{b}}^{\tilde{\sigma}}_i=\mathsf{b}^{\tilde{\sigma},\tilde{\tau}}_i$. Пусть $i\in\{k+1,\dots,n\}$, $\mathsf{s}=\check{\mathsf{a}}^{\tilde{\tau}}_{\tilde{\sigma}}$, $\mathsf{t}=\check{\mathsf{b}}^{\tilde{\tau}}_{\tilde{\sigma}}$. Тогда $\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}_i=\mathsf{s}_{i-k}\neq\mathsf{t}_{i-k}=\mathsf{b}^{\tilde{\sigma},\tilde{\tau}}_i$. Таким образом, $\mathsf{a}^{\tilde{\sigma},\tilde{\tau}}\circ\mathsf{b}^{\tilde{\sigma},\tilde{\tau}}=1$.

Учитывая (2.4) и (2.3), окончательно получим, что $\mathsf{a}^{\tilde{\sigma}}\circ\mathsf{b}^{\tilde{\tau}}=1$ тогда и только тогда, когда $\tilde{\sigma}=\tilde{\tau}$, где $\tilde{\sigma},\tilde{\tau}\in E^n$.

Таким образом, матрица 2.1 имеет диагональный вид. Следовательно, пучок B, определяемый нумерацией $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$, является обратным к A.

Осталось только применить теорему 1. $\lhd$

§ 5. Общие свойства функции Шеннона для операторных полиномиальных формах

Введем специальным образом отношение эквивалентности на классах базисных пучков. Пусть $\psi : \{\mathfrak{e}, \mathfrak{p}, \mathfrak{d}\} \to \{\mathfrak{e}, \mathfrak{p}, \mathfrak{d}\}$ — взаимнооднозначное отображение. Обобщим это отображение на операторы, пучки и классы пучков. Пусть $\psi_n : \{\mathfrak{e}, \mathfrak{p}, \mathfrak{d}\} \to \{\mathfrak{e}, \mathfrak{p}, \mathfrak{d}\}$, $n \in \mathbb{N}$, — последовательность взаимнооднозначных отображений. Обозначим её Ψ:

$$\Psi = \{\psi_n \mid n \in \mathbb{N}\}.$$

- Пусть $\mathfrak{a}$ — произвольный оператор длины n. Определим отображение Ψ по правилу $\Psi(\mathfrak{a}) = \mathfrak{b}$, где $\mathfrak{b}_i = \psi_i(\mathfrak{a}_i)$, $i \in \{0, \ldots, n\}$.
- Отображение Ψ продолжается на пучок следующим образом. Пусть A — пучок операторов размерности n и $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — его нумерация, тогда $\Psi(\mathsf{A}) = \mathsf{B}$, где B — пучок размерности n, который определяется своей нумерацией $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$, в которой $\mathfrak{b}^{\tilde{\sigma}} = \Psi(\mathfrak{a}^{\tilde{\sigma}})$, $\tilde{\sigma} \in E^n$.
- Отображение Ψ продолжается на класс пучков C следующим образом: $\Psi(C) = \{\Psi(\mathsf{A}) \mid \mathsf{A} \in C\}$.

Классы пучков C_1 и C_2 будем называть ψ-эквивалентными, если существует определенное выше отображение Ψ, такое что $\Psi(C_1) = C_2$. Очевидно, что ψ-эквивалентность является отношением эквивалентности.

Легко видеть, что для любых двух операторов $\mathfrak{a}$ и $\mathfrak{b}$ одинаковой длины, классы $K(\mathfrak{a})$ и $K(\mathfrak{b})$, $E(\mathfrak{a})$ и $E(\mathfrak{b})$, $G(\mathfrak{a})$ и $G(\mathfrak{b})$ попарно ψ-эквивалентны.

Введем еще несколько обозначений. Пусть $\mathfrak{a}$ — оператор длины n. Определим множество $I(\mathfrak{a})$ индексов, при которых $\mathfrak{a}_i = \mathfrak{d}$:

$$I(\mathfrak{a}) = \{\ i \mid \mathfrak{a}_i = \mathfrak{d},\ i \in \{1, \ldots, n\}\ \}.$$

Множество всех подмножеств множества $I(\mathfrak{a})$ обозначим $PI(\mathfrak{a})$.

Предложение 1 *Пусть* $\mathfrak{a}$ *— произвольный оператор длины* n, Ψ *— отображение, фигурирующее в определении* ψ*-эквивалентности. Тогда для любой функции* $f \in F_n$ *выполняется:*

$$\Psi(\mathfrak{a}) f(\tilde{x}) = \sum_{J \in PI(\mathfrak{a})} \Psi(\mathfrak{c}^J) f(\tilde{x}),$$

где операторы $\mathfrak{c}^J$ *длины* n *состоят только из символов* $\mathfrak{e}$ *и* $\mathfrak{p}$ *и определяются следующим образом:*

$$\mathfrak{c}^J_j = \begin{cases} \mathfrak{e}, & \text{если } j \in J; \\ \mathfrak{p}, & \text{если } j \in I(\mathfrak{a}) \backslash J; \\ \mathfrak{a}_j, & \text{если } j \notin I(\mathfrak{a}). \end{cases}$$

$\triangleright$ Покажем это, воспользовавшись определением отображения, которое задает оператор $\mathfrak{a}$. Введем обозначение:

$$PI_i = \{J \mid J = I \cap \{1, \ldots, i\},\ I \in PI(\mathfrak{a})\}.$$

Индукцией по i будем доказывать следующее утверждение:

$$f_i(\tilde{x}) = \sum_{J \in PI_i} f_i^J(\tilde{x}),$$

где $f_i(\tilde{x})$, $f_i^J(\tilde{x})$ — это функции из (1.3), используемые для построения образов операторов $\Psi(\mathfrak{a}) f(\tilde{x})$, $\Psi(\mathfrak{c}^J) f(\tilde{x})$ соответственно. Для упрощения записи, будем употреблять $\hat{f}_{i-1}(\tilde{x})$ вместо $f_{i-1}(x_1, \ldots, x_{i-1}, \bar{x}_i, x_{i+1}, \ldots, x_n)$ и $\hat{f}^J_{i-1}(\tilde{x})$ вместо $f^J_{i-1}(x_1, \ldots, x_{i-1}, \bar{x}_i, x_{i+1}, \ldots, x_n)$.

Базис индукции:

$$\sum_{J \in PI_0} f_0^J(\tilde{x}) = f_0^{\varnothing}(\tilde{x}) = f(\tilde{x}) = f_0(\tilde{x}).$$

Шаг индукции разбивается два подслучая.

1. $\mathfrak{a}_i \in \{\mathsf{e}, \mathsf{p}\}$. Тогда $PI_i = PI_{i-1}$;

$$\mathfrak{c}_i^J = \mathfrak{a}_i, \quad \psi_i(\mathfrak{c}_i^J) = \psi_i(\mathfrak{a}_i), \qquad J \in PI_i;$$

$$f_i(\tilde{x}) = \begin{cases} f_{i-1}(\tilde{x}), & \text{если } \psi_i(\mathfrak{a}_i) = \mathsf{e}; \\ \hat{f}_{i-1}(\tilde{x}), & \text{если } \psi_i(\mathfrak{a}_i) = \mathsf{p}; \\ f_{i-1}(\tilde{x}) \oplus \hat{f}_{i-1}(\tilde{x}), & \text{если } \psi_i(\mathfrak{a}_i) = \mathsf{d}; \end{cases}$$

$$f_i^J(\tilde{x}) = \begin{cases} f_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{a}_i) = \mathsf{e}; \\ \hat{f}_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{a}_i) = \mathsf{p}; \\ f_{i-1}^J(\tilde{x}) \oplus \hat{f}_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{a}_i) = \mathsf{d}; \end{cases} \qquad J \in PI_i.$$

По предположению индукции:

$$\sum_{J \in PI_{i-1}} f_{i-1}^J(\tilde{x}) = f_{i-1}(\tilde{x}); \qquad \sum_{J \in PI_{i-1}} \hat{f}_{i-1}^J(\tilde{x}) = \hat{f}_{i-1}(\tilde{x}).$$

Значит, при любом значении $\psi_i(\mathfrak{a}_i)$ выполняется:

$$\sum_{J \in PI_i} f_i^J(\tilde{x}) = f_i(\tilde{x}).$$

2. $\mathfrak{a}_i = \mathsf{d}$. Тогда $PI_i = PI_{i-1} \cup \{I \mid I = \{i\} \cup J,\ J \in PI_{i-1}\}$;

$$f_i(\tilde{x}) = \begin{cases} f_{i-1}(\tilde{x}), & \text{если } \psi_i(\mathsf{d}) = \mathsf{e}; \\ \hat{f}_{i-1}(\tilde{x}), & \text{если } \psi_i(\mathsf{d}) = \mathsf{p}; \\ f_{i-1}(\tilde{x}) \oplus \hat{f}_{i-1}(\tilde{x}), & \text{если } \psi_i(\mathsf{d}) = \mathsf{d}; \end{cases}$$

$$\mathfrak{c}_i^J = \begin{cases} \mathsf{e}, & \text{если } i \in J; \\ \mathsf{p}, & \text{если } i \notin J; \end{cases} \qquad J \in PI_i.$$

Первые $i-1$ компонентов операторов $\mathfrak{c}^J$ и $\mathfrak{c}^{\{i\}\cup J}$, а следовательно, и операторов $\Psi(\mathfrak{c}^J)$ и $\Psi(\mathfrak{c}^{\{i\}\cup J})$ совпадают, поэтому $f_{i-1}^{\{i\}\cup J}(\tilde{x}) = f_{i-1}^J(\tilde{x})$ при $J \in PI_{i-1}$. Следовательно,

$$f_i^J(\tilde{x}) = \begin{cases} g_{i-1}^{J\setminus\{i\}}(\tilde{x}), & \text{если } i \in J; \\ h_{i-1}^J(\tilde{x}), & \text{если } i \notin J; \end{cases} \qquad J \in PI_i;$$

где g_{i-1}^J и h_{i-1}^J определяются по формулам:

$$g_{i-1}^J(\tilde{x}) = \begin{cases} f_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathsf{e}) = \mathsf{e}; \\ \hat{f}_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathsf{e}) = \mathsf{p}; \\ f_{i-1}^J(\tilde{x}) \oplus \hat{f}_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathsf{e}) = \mathsf{d}; \end{cases}$$

$$h_{i-1}^J(\tilde{x}) = \begin{cases} f_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{p}) = \mathfrak{e}; \\ \hat{f}_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{p}) = \mathfrak{p}; \\ f_{i-1}^J(\tilde{x}) \oplus \hat{f}_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{p}) = \mathfrak{d}. \end{cases}$$

Теперь найдем $g_{i-1}^J(\tilde{x}) \oplus h_{i-1}^J(\tilde{x})$. Так как ψ_i — взаимноодназначное отображение, получим:

$$g_{i-1}^J(\tilde{x}) \oplus h_{i-1}^J(\tilde{x}) = \begin{cases} f_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{d}) = \mathfrak{e}; \\ \hat{f}_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{d}) = \mathfrak{p}; \\ f_{i-1}^J(\tilde{x}) \oplus \hat{f}_{i-1}^J(\tilde{x}), & \text{если } \psi_i(\mathfrak{d}) = \mathfrak{d}. \end{cases}$$

По предположению индукции:

$$\bigoplus_{J \in PI_{i-1}} f_{i-1}^J(\tilde{x}) = f_{i-1}(\tilde{x}); \qquad \bigoplus_{J \in PI_{i-1}} \hat{f}_{i-1}^J(\tilde{x}) = \hat{f}_{i-1}(\tilde{x}).$$

Тогда

$$\bigoplus_{J \in PI_i} f_i^J(\tilde{x}) = \bigoplus_{J \in PI_{i-1}} \left(g_{i-1}^J(\tilde{x}) \oplus h_{i-1}^J(\tilde{x}) \right) = f_i(\tilde{x}).$$

Поскольку

$$PI_n = PI(\mathfrak{a}), \quad f_n(\tilde{x}) = \Psi(\mathfrak{a}) f(\tilde{x}), \quad f_n^J(\tilde{x}) = \Psi(\mathfrak{c}^J) f(\tilde{x})$$

при $J \in PI(\mathfrak{a})$, окончательно получаем

$$\Psi(\mathfrak{a}) f(\tilde{x}) = \bigoplus_{J \in PI(\mathfrak{a})} \Psi(\mathfrak{c}^J) f(\tilde{x}).$$

◁

Следствие *Для любого оператора* $\mathfrak{a}$ *длины* n *и любой функции* $f \in F_n$ *выполняется:*

$$\mathfrak{a} f(\tilde{x}) = \bigoplus_{J \in PI(\mathfrak{a})} \mathfrak{c}^J f(\tilde{x}). \tag{2.5}$$

▷ Для доказательства достаточно взять в качестве отображения Ψ последовательность тождественных преобразований и применить предложение 1. ◁

Теорема 2 *Для любого класса C базисных пучков значение функции Шеннона $L_C^g(n)$ не зависит от выбора базисной функции $g(x_1, \ldots, x_n)$.*

► Доказательство. Рассмотрим двупорожденный пучок B размерности n, $\mathsf{B} = D(\mathfrak{u}, \mathfrak{v})$, где

$$\mathfrak{u}_i = \mathfrak{e}, \quad \mathfrak{v}_i = \mathfrak{p}, \qquad i \in \{1, \ldots, n\}.$$

Пучок B содержит всевозможные операторы длины n, составленные из символов $\mathfrak{e}$ и $\mathfrak{p}$, в том числе и операторы $\mathfrak{c}^J$, из (2.5). Пусть g и h — произвольные базисные функции размерности n, а $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$ — произвольная нумерация пучка B. Системы операторных образов

$$\{\mathfrak{b}^{\tilde{0}} g(\tilde{x}), \ldots, \mathfrak{b}^{\tilde{1}} g(\tilde{x})\} \quad \text{и} \quad \{\mathfrak{b}^{\tilde{0}} h(\tilde{x}), \ldots, \mathfrak{b}^{\tilde{1}} h(\tilde{x})\}$$

являются базисами линейного пространства всех булевых функций, зависящих от набора переменных $\tilde{x}$. Поэтому найдется единственное линейное преобразование φ, переводящее один базис в другой таким образом, что

$$\varphi\left(\mathfrak{b}^{\tilde{\sigma}} g(\tilde{x})\right) = \mathfrak{b}^{\tilde{\sigma}} h(\tilde{x}), \qquad \tilde{\sigma} \in E^n.$$

Пусть A — произвольный базисный пучок размерности n с нумерацией $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$, и пусть $f \in F_n$ — произвольная функция. Тогда f представляется в виде полиномиальной формы по A:

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}). \tag{2.6}$$

Применяя к $f(\tilde{x})$ преобразование φ и пользуясь тем, что операторы c^J из (2.5) содержатся в B, то есть $\varphi\left(\mathfrak{c}^J g(\tilde{x})\right) = \mathfrak{c}^J h(\tilde{x})$, получим:

$$\begin{gathered} \varphi\left(f(\tilde{x})\right) = \varphi\Big(\sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x})\Big) = \\ = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \varphi\Big(\sum_{J \in PI(\mathfrak{a}^{\tilde{\sigma}})} \mathfrak{c}^J g(\tilde{x})\Big) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \sum_{J \in PI(\mathfrak{a}^{\tilde{\sigma}})} \varphi\left(\mathfrak{c}^J g(\tilde{x})\right) = \\ = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \sum_{J \in PI(\mathfrak{a}^{\tilde{\sigma}})} \mathfrak{c}^J h(\tilde{x}) = \sum_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} h(\tilde{x}). \end{gathered} \tag{2.7}$$

Из (2.6), (2.7) и определения сложности функции относительно пучка, следует:

$$L^g_{\mathsf{A}}(f) = L^h_{\mathsf{A}}(\varphi(f)).$$

Пусть теперь C — произвольный класс базисных пучков. По определению сложности в классе полиномиальных форм (1.6):

$$L^g_C(f) = L^h_C(\varphi(f)).$$

Наконец, используя определение функции Шеннона (1.7) и учитывая невырожденность линейного преобразования φ ($\varphi(F_n) = F_n$), окончательно получаем:

$$L^g_C(n) = L^h_C(n).$$

Этим завершается доказательство теоремы. ◀

В дальнейшем, кроме десятого параграфа третьей главы, в качестве базисной функции всегда будем брать многоместную конъюнкцию и использовать введенные выше обозначения: $L^{\&}_{\mathsf{A}}(f)$ и $L^{\&}_C(f)$. В обозначении функции Шеннона верхний индекс будем опускать и использовать запись $L_C(n)$ вместо $L^g_C(n)$.

Предложение 2 *Если C_1 и C_2 — два класса базисных пучков, причем $C_1 \subset C_2$, то*

$$L_{C_2}(n) \le L_{C_1}(n).$$

▷ Доказательство легко следует из определения функции Шеннона (1.7). ◁

Предложение 3 *Если классы базисных пучков C_1, C_2 ψ-эквивалентны, то $L_{C_1}(n) = L_{C_2}(n)$.*

▷ Пусть Ψ — отображение, фигурирующее в определении ψ-эквивалентности, такое что $\Psi(C_1) = C_2$. Пусть $g(\tilde{x}) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$. Напомним, что g является базисной функцией. Рассмотрим двупорожденный пучок B размерности n, $\mathsf{B} = D(\mathfrak{u}, \mathfrak{v})$, где

$$\mathfrak{u}_i = \mathfrak{e}, \quad \mathfrak{v}_i = \mathfrak{p}, \qquad i \in \{1, \ldots, n\}.$$

Операторный пучок $\Psi(\mathsf{B})$ является базисным, так как он двупорожденный: $\Psi(\mathsf{B}) = D(\Psi(\mathfrak{u}), \Psi(\mathfrak{v}))$. Пусть $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$ — нумерация пучка B. Тогда $\left(\Psi(\mathfrak{b}^{\tilde{0}}), \ldots, \Psi(\mathfrak{b}^{\tilde{1}})\right)$ — нумерация пучка $\Psi(\mathsf{B})$. Системы функций

$$\{\mathfrak{b}^{\tilde{0}} g(\tilde{x}), \ldots, \mathfrak{b}^{\tilde{1}} g(\tilde{x})\} \qquad \text{и} \qquad \{\Psi(b^{\tilde{0}}) g(\tilde{x}), \ldots, \Psi(b^{\tilde{1}}) g(\tilde{x})\}$$

являются базисами линейного пространства функций размерности n. Поэтому существует единственное линейное преобразование $\varphi : F_n \to F_n$, такое что

$$\varphi\left(\mathfrak{b}^{\tilde{\sigma}} g(\tilde{x})\right) = \Psi(\mathfrak{b}^{\tilde{\sigma}}) g(\tilde{x}), \qquad \tilde{\sigma} \in E^n.$$

Пусть A — пучок длины n из класса C_1, $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — его нумерация и $f \in F_n$ — произвольная функция. Тогда существует полиномиальное представление:

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x}).$$

Найдем представление функции $\varphi(f)$ относительно пучка $\Psi(\mathsf{A}) \in C_2$ по функции g, воспользовавшись тем, что операторы $\mathfrak{c}^J$ из предложения 1 входят в B:

$$\varphi\left(f(\tilde{x})\right) = \varphi\left(\sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}} g(\tilde{x})\right) =$$

$$= \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \varphi\left(\sum_{J \in PI(\mathfrak{a}^{\tilde{\sigma}})} \mathfrak{c}^J g(\tilde{x})\right) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \sum_{J \in PI(\mathfrak{a}^{\tilde{\sigma}})} \varphi\left(\mathfrak{c}^J g(\tilde{x})\right) =$$

$$= \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \sum_{J \in PI(\mathfrak{a}^{\tilde{\sigma}})} \Psi(\mathfrak{c}^J) g(\tilde{x}) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \Psi(\mathfrak{a}^{\tilde{\sigma}}) g(\tilde{x}).$$

Таким образом,

$$L^{\&}_{\mathsf{A}}(f) = L^{\&}_{\Psi(\mathsf{A})}(\varphi(f)).$$

Рассуждая, как в доказательстве теоремы 2, и учитывая, что $C_2 = \Psi(C_1)$, получим

$$L_{C_1}(n) = L_{C_2}(n).$$

$\lhd$

§ 6. Точные значения функции Шеннона для $\mathfrak{a}$-кронекеровых и свободно-кронекеровых классов полиномиальных форм

В следующей теореме найдено точное значение функции Шеннона для $\mathfrak{a}$-кронекеровых классов полиномиальных форм.

Теорема 3 *Пусть* $\mathfrak{a}$ *— произвольный оператор длины* n*. Тогда*

$$L_{K(\mathfrak{a})}(n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

► Доказательство. Пусть $\mathfrak{b}$ — оператор длины n, все компоненты которого равны $\mathfrak{d}$. Так как

$$K(\mathfrak{b}) = \{\mathsf{A} \mid \mathsf{A} \in K(\mathfrak{d}\ldots\mathfrak{d}),\ \text{размерность } \mathsf{A} \text{ равна } n\ \},$$

имеем:

$$L_{K(\mathfrak{b})}(n) = L_{K(\mathfrak{d}\ldots\mathfrak{d})}(n).$$

Классы $K(\mathfrak{a})$ и $K(\mathfrak{b})$ ψ-эквивалентны. Из предложения 3, и теорем VI, 2 следует, что

$$L_{K(\mathfrak{a})}(n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor. \qquad \blacktriangleleft$$

Сейчас докажем несколько предложений о функциях из множества M_n, которые нам потребуются в дальнейшем.

Предложение 4 *Все функции из* M_n *— симметрические.*

▷ Доказательство. Нам нужно доказать, что для любой перестановки $i_1, \ldots, i_n$, для любой функции $f \in M_n$

$$f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n).$$

Воспользуемся индукцией по размерности функции f.

Базис индукции при $n = 0$ тривиален.

Шаг индукции. Доказательство проведем только для функции p_n, для функций q_n и r_n доказательства аналогичны. По определению

$$p_n(x_{i_1}, \ldots, x_{i_n}) = x_{i_n} \cdot q_{n-1}(x_{i_1}, \ldots, x_{i_{n-1}}) \oplus \bar{x}_{i_n} \cdot r_{n-1}(x_{i_1}, \ldots, x_{i_{n-1}}).$$

Если $i_n = n$, то по предположению индукции для q_{n-1} и r_{n-1}

$$p_n(x_{i_1}, \ldots, x_{i_n}) = x_n \cdot q_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot r_{n-1}(x_1, \ldots, x_{n-1}) = \\ = p_n(x_1, \ldots, x_n).$$

Пусть $i_n \neq n$. Рассмотрим перестановку $j_1, \ldots, j_{n-1}, j_n$, в которой $j_{n-1} = n$ и $j_n = i_n$. По предположению индукции для q_{n-1} и r_{n-1}

$$p_n(x_{i_1}, \ldots, x_{i_n}) = x_{j_n} \cdot q_{n-1}(x_{j_1}, \ldots, x_{j_{n-1}}) \oplus \bar{x}_{j_n} \cdot r_{n-1}(x_{j_1}, \ldots, x_{j_{n-1}}).$$

По определению функций q_{n-1} и r_{n-1}

$$p_n(x_{i_1}, \ldots, x_{i_n}) = \\ = x_{j_n} \cdot \big(x_{j_{n-1}} \cdot r_{n-2}(x_{j_1}, \ldots, x_{j_{n-2}}) \oplus \bar{x}_{j_{n-1}} \cdot p_{n-2}(x_{j_1}, \ldots, x_{j_{n-2}})\big) \oplus \\ \oplus \bar{x}_{j_n} \cdot \big(x_{j_{n-1}} \cdot p_{n-2}(x_{j_1}, \ldots, x_{j_{n-2}}) \oplus \bar{x}_{j_{n-1}} \cdot q_{n-2}(x_{j_1}, \ldots, x_{j_{n-2}})\big) = \\ = x_{j_{n-1}} \cdot \big(x_{j_n} \cdot r_{n-2}(x_{j_1}, \ldots, x_{j_{n-2}}) \oplus \bar{x}_{j_n} \cdot p_{n-2}(x_{j_1}, \ldots, x_{j_{n-2}})\big) \oplus \\ \oplus \bar{x}_{j_{n-1}} \cdot \big(x_{j_n} \cdot p_{n-2}(x_{j_1}, \ldots, x_{j_{n-2}}) \oplus \bar{x}_{j_n} \cdot q_{n-2}(x_{j_1}, \ldots, x_{j_{n-2}})\big) = \\ = p_n(x_{j_1}, \ldots, x_{j_{n-2}}, x_{j_n}, x_{j_{n-1}}),$$

где в перестановке $j_1, \ldots, j_{n-2}, j_n, j_{n-1}$ последний элемент $j_{n-1} = n$. По доказанному выше

$$p_n(x_{i_1}, \ldots, x_{i_n}) = p_n(x_1, \ldots, x_n).$$

◁

Предложение 5 *Для любого $n \geq 0$ выполняется:*

$$p_n(\tilde{x}) \oplus q_n(\tilde{x}) \oplus r_n(\tilde{x}) = 0.$$

▷ Доказательство проведем индукцией по n.

Базис индукции при $n = 0$:

$$p_0 \oplus q_0 \oplus r_0 = 0 \oplus 1 \oplus 1 = 0.$$

Шаг индукции.

$$p_n(\tilde{x}) \oplus q_n(\tilde{x}) \oplus r_n(\tilde{x}) =$$
$$= x_n \cdot q_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot r_{n-1}(x_1, \ldots, x_{n-1}) \oplus$$
$$\oplus x_n \cdot r_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}) \oplus$$
$$\oplus x_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot q_{n-1}(x_1, \ldots, x_{n-1}) =$$
$$= x_n \cdot (q_{n-1}(x_1, \ldots, x_{n-1}) \oplus r_{n-1}(x_1, \ldots, x_{n-1}) \oplus p_{n-1}(x_1, \ldots, x_{n-1})) \oplus$$
$$\oplus \bar{x}_n \cdot (r_{n-1}(x_1, \ldots, x_{n-1}) \oplus p_{n-1}(x_1, \ldots, x_{n-1}) \oplus q_{n-1}(x_1, \ldots, x_{n-1}))$$

Воспользовавшись предположением индукции, получим:

$$p_n(\tilde{x}) \oplus q_n(\tilde{x}) \oplus r_n(\tilde{x}) = 0.$$

$\triangleleft$

Следствие *Если функция $f \in M_n$, то все её обобщенно остаточные функции порядка k принадлежат множеству M_{n-k}.*

$\triangleright$ Доказательство. Пусть $f \in M_n$. Рассмотрим остаточные и производную функции $f(\tilde{x})$ по одной переменной. Из предложения 4 следует, что нам достаточно ограничиться только переменной x_n. Из (1.1) видно, что единичными остаточными по x_n для функций $p_n(\tilde{x})$, $q_n(\tilde{x})$, $r_n(\tilde{x})$ являются соответственно функции

$$q_{n-1}(x_1, \ldots, x_{n-1}), \quad r_{n-1}(x_1, \ldots, x_{n-1}), \quad p_{n-1}(x_1, \ldots, x_{n-1});$$

нулевыми остаточными — функции

$$r_{n-1}(x_1, \ldots, x_{n-1}), \quad p_{n-1}(x_1, \ldots, x_{n-1}), \quad q_{n-1}(x_1, \ldots, x_{n-1}).$$

По предложению 5 производными по x_n функций $p_n(\tilde{x})$, $q_n(\tilde{x})$, $r_n(\tilde{x})$ являются соответственно функции

$$p_{n-1}(x_1, \ldots, x_{n-1}), \quad q_{n-1}(x_1, \ldots, x_{n-1}), \quad r_{n-1}(x_1, \ldots, x_{n-1}).$$

Теперь остается только воспользоваться индукцией. $\triangleleft$

Теорема 4 *Точное значение функции Шеннона для класса FK вычисляется по следующей формуле:*

$$L_{FK}(n) = \frac{1}{2} \cdot 2^n.$$

► Для доказательства этого мы сначала для каждой функции $f \in F_n$ построим пучок A из класса FK, такой что $L^{\&}_{\mathsf{A}}(f) \leq 2^{n-1}$, затем покажем, что для любого пучка $\mathsf{A} \in FK$ сложность $L^{\&}_{\mathsf{A}}(f)$ функций из M_n не меньше, чем 2^{n-1}. Доказательство оформим в виде трех лемм. Верхняя оценка будет следовать из леммы 4.1, нижняя из леммы 4.3, лемма 4.2 используется для доказательства леммы 4.3.

Лемма 4.1 *Для любой функции $f \in F_n$ существует базисный пучок $\mathsf{A} \in FK$, такой что*

$$L^{\&}_{\mathsf{A}}(f) \leq \frac{1}{2} \cdot 2^n.$$

▷ Доказательство. Рассмотрим совершенную полиномиальную нормальную форму для функции f:

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \cdot x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}.$$

Выделим из наборов $\tilde{\sigma}$ последний компонент σ_n и сгруппируем некоторые слагаемые:

$$f(\tilde{x}) = \sum_{\tilde{\sigma} \in E^n} f(\tilde{\sigma}) \cdot x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} =$$

$$= \sum_{\tilde{\tau} \in E^{n-1}} \left(f(\tilde{\tau}, 0) \cdot x_1^{\tau_1} \cdot \ldots \cdot x_{n-1}^{\tau_{n-1}} \cdot \bar{x}_n \oplus f(\tilde{\tau}, 1) \cdot x_1^{\tau_1} \cdot \ldots \cdot x_{n-1}^{\tau_{n-1}} \cdot x_n \right).$$

Здесь и далее $f(\tilde{\tau}, 0)$, $f(\tilde{\tau}, 1)$ означают, соответственно, $f(\tau_1, \ldots, \tau_{n-1}, 0)$, $f(\tau_1, \ldots, \tau_{n-1}, 1)$. Вынесем в каждом слагаемом за скобки $x_1^{\tau_1} \cdot \ldots \cdot x_{n-1}^{\tau_{n-1}}$. Получим:

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^{n-1}} x_1^{\tau_1} \cdot \ldots \cdot x_{n-1}^{\tau_{n-1}} \cdot \left(f(\tilde{\tau}, 0) \cdot \bar{x}_n \oplus f(\tilde{\tau}, 1) \cdot x_n \right). \qquad (2.8)$$

Определим 2^{n-1} пучков $\mathsf{B}_{\tilde{\sigma}}$, $\tilde{\sigma} \in E^{n-1}$ размерности 1 по их естественным нумерациям следующим образом:

$$\left(\mathsf{b}^0_{\tilde{\sigma}}, \mathsf{b}^1_{\tilde{\sigma}}\right) = \begin{cases} \left(\mathsf{e}, \mathsf{p}\right), & \text{если } f(\tilde{\tau}, 0) = 0; \\ \left(\mathsf{p}, \mathsf{e}\right), & \text{если } f(\tilde{\tau}, 0) = 1,\ f(\tilde{\tau}, 1) = 0; \\ \left(\mathsf{d}, \mathsf{e}\right), & \text{если } f(\tilde{\tau}, 0) = 1,\ f(\tilde{\tau}, 1) = 1; \end{cases} \qquad \tilde{\sigma} \in E^{n-1}.$$

Построим пучок A размерности n как слияние пучка $D(\mathfrak{u}, \mathfrak{v})$ с пучками $\mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}$:

$$\mathsf{A} = W(D(\mathfrak{u}, \mathfrak{v}) \mid \mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}),$$

где $\mathfrak{u}$ и $\mathfrak{v}$ — операторы длины $n-1$, компоненты которых определяются по формулам:

$$\mathfrak{u}_i = \mathsf{p}, \quad \mathfrak{v}_i = \mathsf{e}, \qquad i \in \{1, \ldots, n-1\}.$$

Пусть $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — естественная нумерация пучка A. По определению слияния пучков, $\mathfrak{a}^{\tilde{\sigma}}$ определяется следующим образом:

$$\mathfrak{a}^{\tilde{\sigma}}_i = \begin{cases} \mathsf{p}, & \text{если } \sigma_i = 0, \\ \mathsf{e}, & \text{если } \sigma_i = 1, \end{cases} \qquad i \in \{1, \ldots, n-1\}, \quad \tilde{\sigma} \in E^n;$$

$$\mathfrak{a}^{\tilde{\tau},0}_n = \begin{cases} \mathsf{e}, & \text{если } f(\tilde{\tau}, 0) = 0, \\ \mathsf{p}, & \text{если } f(\tilde{\tau}, 0) = 1,\ f(\tilde{\tau}, 1) = 0, \\ \mathsf{d}, & \text{если } f(\tilde{\tau}, 0) = 1,\ f(\tilde{\tau}, 1) = 1, \end{cases} \qquad \tilde{\tau} \in E^{n-1};$$

$$\mathfrak{a}^{\tilde{\tau},1}_n = \begin{cases} \mathsf{e}, & \text{если } f(\tilde{\tau}, 0) = 1, \\ \mathsf{p}, & \text{если } f(\tilde{\tau}, 0) = 0, \end{cases} \qquad \tilde{\tau} \in E^{n-1}.$$

Напомним, что $\tilde{\tau}, 0$ и $\tilde{\tau}, 1$ означают $\tau_1, \ldots, \tau_{n-1}, 0$ и $\tau_1, \ldots, \tau_{n-1}, 1$, соответственно. Рассмотрим образ функции $g(\tilde{x}) = x_1 \cdot \ldots \cdot x_n$ при действии на нее оператором $\mathfrak{a}^{\tilde{\tau},0}$. По определению, $\mathfrak{a}^{\tilde{\tau},0} g(\tilde{x}) = g_n(\tilde{x})$, где $g_0(\tilde{x}) = g(\tilde{x})$, а $g_i(\tilde{x})$ определяются по формулам (1.3). Легко видеть, что

$$g_{n-1}(\tilde{x}) = x_1^{\tau_1} \cdot \ldots \cdot x_{n-1}^{\tau_{n-1}} \cdot x_n.$$

Тогда

$$g_n(\tilde{x}) = \begin{cases} x_1^{\tau_1} \cdot \ldots \cdot x_{n-1}^{\tau_{n-1}} \cdot x_n, & \text{если } f(\tilde{\tau}, 0) = 0; \\ x_1^{\tau_1} \cdot \ldots \cdot x_{n-1}^{\tau_{n-1}} \cdot \bar{x}_n, & \text{если } f(\tilde{\tau}, 0) = 1,\ f(\tilde{\tau}, 1) = 0; \\ x_1^{\tau_1} \cdot \ldots \cdot x_{n-1}^{\tau_{n-1}} \cdot (x_n \oplus \bar{x}_n), & \text{если } f(\tilde{\tau}, 0) = 1,\ f(\tilde{\tau}, 1) = 1. \end{cases}$$

В любом случае,

$$(f(\tilde{\tau},0)\vee f(\tilde{\tau},1))\cdot \mathfrak{a}^{\tilde{\tau},0}g(\tilde{x}) = x_1^{\tau_1}\cdot\ldots\cdot x_{n-1}^{\tau_{n-1}}\cdot(f(\tilde{\tau},0)\cdot\bar{x}_n\oplus f(\tilde{\tau},1)\cdot x_n)\,.$$

Положим

$$\alpha_{\tilde{\sigma}} = \begin{cases} f(\tilde{\tau},0)\vee f(\tilde{\tau},1),\ \text{где } \tilde{\tau}=\sigma_1,\ldots,\sigma_{n-1}, & \text{если } \sigma_n=0;\\ 0, & \text{если } \sigma_n=1. \end{cases}$$

Тогда (2.8) запишется в виде:

$$f(\tilde{x}) = \sum_{\tilde{\tau}\in E^{n-1}} (f(\tilde{\tau},0)\vee f(\tilde{\tau},1))\cdot\mathfrak{a}^{\tilde{\tau},0}g(\tilde{x}) = \sum_{\tilde{\sigma}\in E^n}\alpha_{\tilde{\sigma}}\mathfrak{a}^{\tilde{\sigma}}g(\tilde{x}),$$

причем по крайней мере половина из коэффициентов $\alpha_{\tilde{\sigma}}$ равны нулю. Поэтому:

$$L^{\&}_{\mathsf{A}}(f) = \sum_{\tilde{\sigma}}\alpha_{\tilde{\sigma}} \le \frac{1}{2}\cdot 2^n.$$

$\lhd$

Лемма 4.2 *Пусть* A *— пучок размерности* n *из класса* FK *с естественной нумерацией* $\left(\mathfrak{a}^{\tilde{0}},\ldots,\mathfrak{a}^{\tilde{1}}\right)$. *Тогда для любой функции* $f\in F_{n+m}$ *имеет место разложение:*

$$f(\tilde{x},\tilde{y}) = \sum_{\tilde{\sigma}\in E^n} f^{\omega_1^{\tilde{\sigma}}\ldots\omega_n^{\tilde{\sigma}}}_{x_1\ldots x_n}(\tilde{x},\tilde{y})\cdot\mathfrak{a}^{\tilde{\tau}}_{\tilde{x}}(x_1\cdot\ldots\cdot x_n),$$

в котором функции $f^{\omega_1^{\tilde{\sigma}}\ldots\omega_n^{\tilde{\sigma}}}_{x_1\ldots x_n}(\tilde{x},\tilde{y})$ *являются обобщенно остаточными ранга* n *и определяются по индукции следующим образом:*

$$f^{\omega_1^{\tilde{\sigma}}\ldots\omega_i^{\tilde{\sigma}}}_{x_1\ldots x_i} = \begin{cases} \left(f^{\omega_1^{\tilde{\sigma}}\ldots\omega_{i-1}^{\tilde{\sigma}}}_{x_1\ldots x_{i-1}}\right)^0_{x_i}, & \textit{если } \mathfrak{a}_i^{\tilde{\tau}}=\mathsf{e};\\ \left(f^{\omega_1^{\tilde{\sigma}}\ldots\omega_{i-1}^{\tilde{\sigma}}}_{x_1\ldots x_{i-1}}\right)^1_{x_i}, & \textit{если } \mathfrak{a}_i^{\tilde{\tau}}=\mathsf{p};\\ \left(f^{\omega_1^{\tilde{\sigma}}\ldots\omega_{i-1}^{\tilde{\sigma}}}_{x_1\ldots x_{i-1}}\right)'_{x_i}, & \textit{если } \mathfrak{a}_i^{\tilde{\tau}}=\mathsf{d};\end{cases}$$

где $\tilde{\tau}=(\sigma_1,\ldots,\sigma_{i-1},\bar{\sigma}_i,\sigma_{i+1},\ldots,\sigma_n)$, $\tilde{\sigma}\in E^n$. *Запись* $f(\tilde{x},\tilde{y})$ *означает* $f(x_1,\ldots,x_n,y_1,\ldots,y_m)$.

$\rhd$ Доказательство проведем индукцией по построению пучка $\mathsf{A}\in FK$. Базис индукции. Класс FK содержит три пучка размерности 1:

$$\{\mathsf{e},\mathsf{p}\},\quad \{\mathsf{e},\mathsf{d}\},\quad \{\mathsf{p},\mathsf{d}\}.$$

Соответствующие разложения имеют вид:

$$f(x_1,\tilde{y}) = f^1_{x_1}(x_1,\tilde{y})\cdot \mathsf{e}x_1 \oplus f^0_{x_1}(x_1,\tilde{y})\cdot \mathsf{p}x_1 = x_1\cdot f^1_{x_1}(x_1,\tilde{y}) \oplus \bar{x}_1\cdot f^0_{x_1}(x_1,\tilde{y});$$
$$f(x_1,\tilde{y}) = f'_{x_1}(x_1,\tilde{y})\cdot \mathsf{e}x_1 \oplus f^0_{x_1}(x_1,\tilde{y})\cdot \mathsf{d}x_1 = x_1\cdot f'_{x_1}(x_1,\tilde{y}) \oplus f^0_{x_1}(x_1,\tilde{y});$$
$$f(x_1,\tilde{y}) = f'_{x_1}(x_1,\tilde{y})\cdot \mathsf{p}x_1 \oplus f^1_{x_1}(x_1,\tilde{y})\cdot \mathsf{d}x_1 = \bar{x}_1\cdot f'_{x_1}(x_1,\tilde{y}) \oplus f^1_{x_1}(x_1,\tilde{y}).$$

Поскольку все нумерации пучков размерности 1 естественные, то при $n = 1$ лемма справедлива.

Шаг индукции. По определению класса FK, пучок A размерности $n > 1$ образован путем слияния или перестановки пучков из класса FK.

Предположим, что $\mathsf{A} = I(\mathsf{C} \mid i_1,\ldots,i_n)$, и $\left(\mathsf{c}^{\tilde{0}},\ldots,\mathsf{c}^{\tilde{1}}\right)$ — естественная нумерация пучка C. Рассмотрим функцию $h(\tilde{x},\tilde{y})$, такую что

$$h(\tilde{x},\tilde{y}) = f(x_{i_1},\ldots,x_{i_n},\tilde{y}).$$

По предположению индукции,

$$h(\tilde{x},\tilde{y}) = \sum_{\tilde{\sigma}} h^{\omega_1^{\tilde{\sigma}}\ldots\omega_n^{\tilde{\sigma}}}_{x_1\ldots x_n}(\tilde{x},\tilde{y})\cdot \mathsf{c}^{\tilde{\sigma}}(x_1\cdot\ldots\cdot x_n)$$

Поэтому,

$$f(x_{i_1},\ldots,x_{i_n},\tilde{y}) = \sum_{\tilde{\sigma}} f^{\omega_{i_1}^{\tilde{\sigma}}\ldots\omega_{i_n}^{\tilde{\sigma}}}_{x_{i_1}\ldots x_{in}}(x_{i_1},\ldots,x_{i_n},\tilde{y})\cdot \mathsf{c}^{\tilde{\sigma}}(x_1\cdot\ldots\cdot x_n).$$

По определению перестановки пучка, $\mathsf{c}^{\tilde{\sigma}}(x_1\cdot\ldots\cdot x_n) = \mathsf{a}^{\tilde{\tau}}(x_{i_1}\cdot\ldots\cdot x_{i_n})$, где $\tilde{\tau} = \sigma_{i_1},\ldots,\sigma_{i_n}$. Тогда

$$f^{\omega_{i_1}^{\tilde{\sigma}}\ldots\omega_{i_n}^{\tilde{\sigma}}}_{x_{i_1}\ldots x_{i_n}} = f^{\omega_1^{\tilde{\tau}}\ldots\omega_n^{\tilde{\tau}}}_{x_{i_1}\ldots x_{i_n}}.$$

Поэтому,

$$f(x_{i_1},\ldots,x_{i_n},\tilde{y}) = \sum_{\tilde{\sigma}} f^{\omega_1^{\tilde{\tau}}\ldots\omega_n^{\tilde{\tau}}}_{x_{i_1}\ldots x_{in}}(x_{i_1},\ldots,x_{i_n},\tilde{y})\cdot \mathsf{a}^{\tilde{\sigma}}(x_{i_1}\cdot\ldots\cdot x_{i_n}).$$

После переобозначения переменных получим:

$$f(\tilde{x},\tilde{y}) = \sum_{\tilde{\sigma}} f^{\omega_1^{\tilde{\sigma}}\ldots\omega_n^{\tilde{\sigma}}}_{x_1\ldots x_n}(\tilde{x},\tilde{y})\cdot \mathsf{a}^{\tilde{\sigma}}(x_1\cdot\ldots\cdot x_n).$$

Допустим $\mathsf{A} = W(\mathsf{C} \mid \mathsf{B}_{\tilde{0}},\ldots,\mathsf{B}_{\tilde{1}})$, где у пучка C размерность равна k, а размерность пучков $\mathsf{B}_{\tilde{\sigma}}$, $\tilde{\sigma}\in E^k$, равна $n-k$. Пусть $\left(\mathsf{a}^{\tilde{0}},\ldots,\mathsf{a}^{\tilde{1}}\right)$ —

естественная нумерация пучка C, а $\left(\mathsf{b}^{\tilde{0}}_{\tilde{\sigma}}, \ldots, \mathsf{b}^{\tilde{l}}_{\tilde{\sigma}}\right)$ — естественные нумерации пучков $\mathsf{B}_{\tilde{\sigma}}$, $\tilde{\sigma} \in E^k$. По предположению индукции для пучка C

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma} \in E^k} f^{\omega_1^{\tilde{\sigma}} \ldots \omega_k^{\tilde{\sigma}}}_{x_1 \ldots x_k}(\tilde{x}, \tilde{y}) \cdot \mathsf{c}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_k).$$

Применим предположение индукции к пучкам $\mathsf{B}_{\tilde{\sigma}}$:

$$f^{\omega_1^{\tilde{\sigma}} \ldots \omega_k^{\tilde{\sigma}}}_{x_1 \ldots x_k}(\tilde{x}, \tilde{y}) = \sum_{\tilde{\tau} \in E^{n-k}} f^{\omega_1^{\tilde{\sigma}} \ldots \omega_k^{\tilde{\sigma}} \omega_{k+1}^{\tilde{\sigma},\tilde{\tau}} \ldots \omega_n^{\tilde{\sigma},\tilde{\tau}}}_{x_1 \ldots x_k\, x_{k+1} \ldots x_n}(\tilde{x}, \tilde{y}) \cdot \mathsf{b}^{\tilde{\tau}}_{\tilde{\sigma}}(x_{k+1} \cdot \ldots \cdot x_n).$$

Тогда

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma} \in E^k} \sum_{\tilde{\tau} \in E^{n-k}} f^{\omega_1^{\tilde{\sigma}} \ldots \omega_k^{\tilde{\sigma}} \omega_{k+1}^{\tilde{\sigma},\tilde{\tau}} \ldots \omega_n^{\tilde{\sigma},\tilde{\tau}}}_{x_1 \ldots x_k\, x_{k+1} \ldots x_n}(\tilde{x}, \tilde{y}) \cdot \mathsf{b}^{\tilde{\tau}}_{\tilde{\sigma}}(x_{k+1} \cdot \ldots \cdot x_n) \cdot \mathsf{c}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_k).$$

По определению слияния пучков,

$$\mathsf{b}^{\tilde{\tau}}_{\tilde{\sigma}}(x_{k+1} \cdot \ldots \cdot x_n) \cdot \mathsf{c}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_k) = \mathsf{a}^{\tilde{\sigma},\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n).$$

Поскольку символ $\omega_i^{\tilde{\sigma}}$ действует только по переменной i, можно ввести переобозначение:

$$f^{\omega_1^{\tilde{\sigma}} \ldots \omega_k^{\tilde{\sigma}} \omega_{k+1}^{\tilde{\sigma},\tilde{\tau}} \ldots \omega_n^{\tilde{\sigma},\tilde{\tau}}}_{x_1 \ldots x_k\, x_{k+1} \ldots x_n}(\tilde{x}, \tilde{y}) = f^{\omega_1^{\tilde{\sigma},\tilde{\tau}} \ldots \omega_n^{\tilde{\sigma},\tilde{\tau}}}_{x_1 \ldots x_n}(\tilde{x}, \tilde{y}).$$

Тогда

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma} \in E^n} f^{\omega_1^{\tilde{\sigma}} \ldots \omega_n^{\tilde{\sigma}}}_{x_1 \ldots x_n}(\tilde{x}, \tilde{y}) \cdot \mathsf{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n).$$

Лемма доказана. ◁

Лемма 4.3 *Для любого пучка $\mathsf{A} \in FK$ размерности $n \geq 1$, для любой функции $f \in M_n$ выполняется:*

$$L^{\&}_{\mathsf{A}}(f) \geq \frac{1}{2} \cdot 2^n.$$

▷ Доказательство проведем индукцией по построению пучка A.

Базис индукции. Класс FK содержит три пучка размерности 1:

$$\{\mathsf{e}, \mathsf{p}\}, \quad \{\mathsf{e}, \mathsf{d}\}, \quad \{\mathsf{p}, \mathsf{d}\}.$$

Соответствующие полиномиальные представления функций p_1, q_1, r_1 имеют вид:

$$p_1(x_1) = 1 = 1 \cdot \mathsf{e}x_1 \oplus 1 \cdot \mathsf{p}x_1 = 0 \cdot \mathsf{e}x_1 \oplus 1 \cdot \mathsf{d}x_1 = 0 \cdot \mathsf{p}x_1 \oplus 1 \cdot \mathsf{d}x_1;$$
$$q_1(x_1) = x_1 = 1 \cdot \mathsf{e}x_1 \oplus 0 \cdot \mathsf{p}x_1 = 1 \cdot \mathsf{e}x_1 \oplus 0 \cdot \mathsf{d}x_1 = 1 \cdot \mathsf{p}x_1 \oplus 1 \cdot \mathsf{d}x_1;$$
$$r_1(x_1) = \bar{x}_1 = 0 \cdot \mathsf{e}x_1 \oplus 1 \cdot \mathsf{p}x_1 = 1 \cdot \mathsf{e}x_1 \oplus 1 \cdot \mathsf{d}x_1 = 1 \cdot \mathsf{p}x_1 \oplus 0 \cdot \mathsf{d}x_1.$$

Таким образом, полиномиальные представления функций p_1, q_1, r_n имеют сложность не менее $1 = \frac{1}{2} \cdot 2^1$ для любого пучка размерности 1 из *FK*.

Шаг индукции. По определению класса *FK* пучок A размерности $n > 1$ образован путем слияния или перестановки пучков из класса *FK*.

Предположим, что $\mathsf{A} = I(\mathsf{C} \mid i_1, \ldots, i_n)$, $\left(\mathsf{c}^{\tilde{0}}, \ldots, \mathsf{c}^{\tilde{1}}\right)$ — некоторая нумерация пучка C и $f \in M_n$. Пользуясь определением перестановки пучка и предложением 4, получим следующую цепочку равенств:

$$f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n) =$$
$$= \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \mathsf{c}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) = \sum_{\tilde{\tau}} \beta_{\tilde{\tau}} \mathsf{a}^{\tilde{\tau}}(x_{i_1} \cdot \ldots \cdot x_{i_n}),$$

где $\left(\mathsf{a}^{\tilde{0}}, \ldots, \mathsf{a}^{\tilde{1}}\right)$ — нумерация пучка A, построенная по определению перестановки, и $\beta_{\tilde{\tau}} = \alpha_{\tilde{\sigma}}$, где $\tilde{\tau} = \sigma_{i_1}, \ldots, \sigma_{i_n}$. После переименования переменных получим:

$$f(x_1, \ldots, x_n) = \sum_{\tilde{\sigma}} \alpha_{\tilde{\sigma}} \mathsf{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n).$$

Осталось воспользоваться предположением индукции:

$$L^{\&}_{\mathsf{A}}(f) = L^{\&}_{\mathsf{C}} \geq \frac{1}{2} \cdot 2^n.$$

Допустим $\mathsf{A} = W(\mathsf{C} \mid \mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}})$, где у пучка C размерность равна k, а размерность пучков $\mathsf{B}_{\tilde{\sigma}}$, $\tilde{\sigma} \in E^k$, равна $n-k$. Пусть $\left(\mathsf{a}^{\tilde{0}}, \ldots, \mathsf{a}^{\tilde{1}}\right)$ — нумерация пучка A, построенная по определению слияния пучков из нумерации $\left(\mathsf{c}^{\tilde{0}}, \ldots, \mathsf{c}^{\tilde{1}}\right)$ пучка C и нумераций $\left(\mathsf{b}^{\tilde{0}}_{\tilde{\sigma}}, \ldots, \mathsf{b}^{\tilde{1}}_{\tilde{\sigma}}\right)$ пучков $\mathsf{B}_{\tilde{\sigma}}$, $\tilde{\sigma} \in E^k$. Полиномиальная форма для функции $f \in M_n$ относительно пучка A

имеет вид:

$$f(\tilde{x}) = \bigvee_{\tilde{\sigma} \in E^n} \alpha_{\tilde{\sigma}} \mathsf{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n).$$

По определению слияния пучков:

$$f(\tilde{x}) = \bigvee_{\tilde{\sigma} \in E^k} \bigvee_{\tilde{\tau} \in E^{n-k}} \alpha_{\tilde{\sigma},\tilde{\tau}} \cdot \mathsf{c}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_k) \cdot \mathsf{b}^{\tilde{\tau}}_{\tilde{\sigma}}(x_{k+1} \cdot \ldots \cdot x_n) =$$
$$= \bigvee_{\tilde{\sigma} \in E^k} \mathsf{c}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_k) \cdot \Big(\bigvee_{\tilde{\tau} \in E^{n-k}} \alpha_{\tilde{\sigma},\tilde{\tau}} \cdot \mathsf{b}^{\tilde{\tau}}_{\tilde{\sigma}}(x_{k+1} \cdot \ldots \cdot x_n) \Big).$$

Из леммы 4.2 и следствия к предложению 5 следует, что внутренние суммы реализуют функции из множества M_{n-k}. Пусть это будут функции $h_{\tilde{\sigma}}(x_{k+1}, \ldots, x_n)$, $\tilde{\sigma} \in E^k$. Используя определение сложности полиномиальной формы и предположение индукции, получим:

$$L^{\&}_{\mathsf{A}}(f) = \sum_{\tilde{\sigma} \in E^k} L^{\&}_{\mathsf{B}_{\tilde{\sigma}}}(h_{\tilde{\sigma}}) \geq \sum_{\tilde{\sigma} \in E^k} \frac{1}{2} \cdot 2^{n-k} = \frac{1}{2} \cdot 2^n.$$

Лемма доказана. ◁

Из лемм 4.1, 4.3 и теоремы 2 следует, что

$$L_{FK}(n) = \frac{1}{2} \cdot 2^n.$$

Теорема доказана. ◀

Глава 3. Сложные функции в классах полиномиальных форм

Третья глава посвящена нахождению булевых функций, имеющих большую сложность в классах полиномиальных форм.

В седьмом параграфе диссертации найдена последовательность эффективно заданных функций, имеющих экспоненциальную сложность.

В восьмом параграфе доказывается ряд вспомогательных предложений, которые используются в дальнейшем изложении. Приведены некоторые свойства булевых функций, а также свойства сложности их представлений относительно различных операторных пучков.

В девятом параграфе для некоторых классов полиномиальных форм описаны все функции, имеющие в них наибольшую сложность.

В десятом параграфе описывается метод, позволяющий на основе результатов девятого параграфа найти функции наибольшей сложности в полиномиальных формах, построенных по произвольной базисной функции, относительно достаточно широкого круга классов пучков.

§ 7. Функции экспоненциальной сложности в классе полиномиальных нормальных форм

В следующей теореме доказывается, что функции из множества M_n имеют экспоненциальную сложность в классе полиномиальных нормальных форм.

Теорема 5 *Если* $f \in M_n$, *то*

$$L_{\text{пнф}}(f) \geq \left(\frac{3}{2}\right)^{n-1}.$$

► Напомним, что $M_n = \{p_n, q_n, r_n\}$, а функции p_n, q_n, r_n определяются по формулам (1.1).

Для начала покажем, что

$$L_{\text{пнф}}(p_n) = L_{\text{пнф}}(q_n) = L_{\text{пнф}}(r_n).$$

Пусть Φ — минимальная полиномиальная нормальная форма, реализующая функцию p_n. Вынесем в ней за скобки x_n и $\bar{x}_n$, тогда Φ примет вид:

$$\Phi = x_n \cdot \Phi_1 \oplus \bar{x}_n \cdot \Phi_2 \oplus \Phi_3,$$

где Φ_1, Φ_2, Φ_3 — полиномиальные нормальные формы, в которые не входит переменная x_n, и при этом справедливы равенства:

$$L_{\text{пнф}}(p_n) = L(\Phi) = L(\Phi_1) + L(\Phi_2) + L(\Phi_3).$$

Рассмотрим остаточные функции по переменной x_n для функции p_n:

$$p_{n\,x_n}^{0}(x_1, \ldots, x_n) = r_{n-1}(x_1, \ldots, x_{n-1}),$$
$$p_{n\,x_n}^{1}(x_1, \ldots, x_n) = q_{n-1}(x_1, \ldots, x_{n-1}),$$
$$p_{n\,x_n}'(x_1, \ldots, x_n) = p_{n-1}(x_1, \ldots, x_{n-1}).$$

Они реализуются полиномиальными нормальными формами, соответственно:

$$\Psi_1 = \Phi_2 \oplus \Phi_3,$$
$$\Psi_2 = \Phi_1 \oplus \Phi_3,$$
$$\Psi_3 = \Phi_1 \oplus \Phi_2.$$

С другой стороны, выполняются равенства:

$$q_n(x_1, \ldots, x_n) = x_n \cdot r_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}),$$
$$r_n(x_1, \ldots, x_n) = x_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot q_{n-1}(x_1, \ldots, x_{n-1}).$$

Поэтому q_n и r_n реализуются термами, соответственно:

$$x_n \cdot \Psi_1 \oplus \bar{x}_n \cdot \Psi_3 =$$
$$= x_n \cdot (\Phi_2 \oplus \Phi_3) \oplus \bar{x}_n \cdot (\Phi_1 \oplus \Phi_2) =$$
$$= x_n \cdot \Phi_3 \oplus \bar{x}_n \cdot \Phi_1 \oplus \Phi_2,$$

$$x_n \cdot \Psi_3 \oplus \bar{x}_n \cdot \Psi_2 =$$
$$= x_n \cdot (\Phi_1 \oplus \Phi_2) \oplus \bar{x}_n \cdot (\Phi_1 \oplus \Phi_3) =$$
$$= x_n \cdot \Phi_2 \oplus \bar{x}_n \cdot \Phi_3 \oplus \Phi_1.$$

Таким образом, получим полиномиальные нормальные формы с числом слагаемых

$$L(\Phi_1) + L(\Phi_2) + L(\Phi_3) = L(\Phi).$$

Значит, справедливы два неравенства:

$$L_{\text{пнф}}(q_n) \le L_{\text{пнф}}(p_n), \qquad L_{\text{пнф}}(r_n) \le L_{\text{пнф}}(p_n).$$

Аналогичным образом получаются следующие неравенства:

$$L_{\text{пнф}}(p_n) \le L_{\text{пнф}}(q_n), \qquad L_{\text{пнф}}(q_n) \le L_{\text{пнф}}(r_n).$$

Отсюда следует равенство сложностей:

$$L_{\text{пнф}}(p_n) = L_{\text{пнф}}(q_n) = L_{\text{пнф}}(r_n).$$

Поскольку термы Ψ_1, Ψ_2, Ψ_3 реализуют соответственно функции r_{n-1}, q_{n-1}, p_{n-1}, то выполняется:

$$3 \cdot L_{\text{пнф}}(p_{n-1}) = L_{\text{пнф}}(r_{n-1}) + L_{\text{пнф}}(q_{n-1}) + L_{\text{пнф}}(p_{n-1}) \le$$
$$\le L(\Psi_1) + L(\Psi_2) + L(\Psi_3) =$$
$$= L(\Phi_2) + L(\Phi_3) + L(\Phi_1) + L(\Phi_3) + L(\Phi_1) + L(\Phi_2) =$$
$$= 2 \cdot (L(\Phi_1) + L(\Phi_2) + L(\Phi_3)) = 2 \cdot L(\Phi) = 2 \cdot L_{\text{пнф}}(p_n).$$

Таким образом,

$$L_{\text{пнф}}(p_n) \ge \frac{3}{2} \cdot L_{\text{пнф}}(p_{n-1}).$$

Учитывая, что $L_{\text{пнф}}(p_1) = 1$, и применяя индукцию, окончательно получим:

$$L_{\text{пнф}}(p_n) \ge \left(\frac{3}{2}\right)^{n-1}.$$

◀

§ 8. Свойства специальных булевых функций

Далее нам потребуются множества $M_n^\Diamond$, $\widetilde{M}_n^\Diamond$, $\overline{M}_n^\Diamond$, для которых, очевидно, справедливы включения:

$$M_n^\Diamond \subset \widetilde{M}_n^\Diamond \subset \overline{M}_n^\Diamond.$$

Заметим, что поскольку функции $p_n(\tilde{x})$, $q_n(\tilde{x})$, $r_n(\tilde{x})$, а следовательно и функции $\bar{p}_n(\tilde{x})$, $\bar{q}_n(\tilde{x})$, $\bar{r}_n(\tilde{x})$ — симметрические, то все однотипные им функции имеют вид $f(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n})$, где $f \in \overline{M}_n$. Этот факт будет в дальнейшем использоваться безо всякого упоминания.

Предложение 6 *Пусть тройка функций $f, g, h \in M_n^\Diamond$, удовлетворяет условию:*

$$f(\tilde{x}) \oplus g(\tilde{x}) \oplus h(\tilde{x}) = 0.$$

Тогда для любого набора $\tilde{\sigma} \in E^n$, такого что

$$f(\tilde{x}^{\tilde{\sigma}}) \in \left\{p_n(\tilde{x}), q_n(\tilde{x}), r_n(\tilde{x})\right\},$$

выполняется:

$$\left\{f(\tilde{x}^{\tilde{\sigma}}), g(\tilde{x}^{\tilde{\sigma}}), h(\tilde{x}^{\tilde{\sigma}})\right\} = \left\{p_n(\tilde{x}), q_n(\tilde{x}), r_n(\tilde{x})\right\}.$$

▷ Доказательство проведем индукцией по n.

Базис индукции. При $n = 1$ множества $M_n^\Diamond$ и M_n совпадают:

$$M_1^\Diamond = M_1 = \left\{p_1, q_1, r_1\right\}.$$

Пусть $f, g, h \in M_1$. Поскольку $f(x_1) \neq 0$, то

$$f(x_1) \oplus f(x_1) \oplus f(x_1) \neq 0,$$
$$f(x_1) \oplus g(x_1) \oplus g(x_1) \neq 0.$$

Таким образом, все функции f, g, h различны, а значит, по предложению 5,

$$\left\{f(x_1), g(x_1), h(x_1)\right\} = \left\{p_1(x_1), q_1(x_1), r_1(x_1)\right\}.$$

Шаг индукции. Пусть $f, g, h \in M_n^{\Diamond}$,

$$f(\tilde{x}) \oplus g(\tilde{x}) \oplus h(\tilde{x}) = 0,$$
$$f(\tilde{x}^{\tilde{\sigma}}) \in \left\{p_n(\tilde{x}), q_n(\tilde{x}), r_n(\tilde{x})\right\}.$$

Для определённости предположим, что $f(\tilde{x}^{\tilde{\sigma}}) = p_n(\tilde{x})$. Тогда

$$f_{x_n}^{\sigma_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = q_{n-1}(x_1, \ldots, x_{n-1});$$
$$f_{x_n}^{\bar{\sigma}_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = r_{n-1}(x_1, \ldots, x_{n-1});$$
$$f'_{x_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = p_{n-1}(x_1, \ldots, x_{n-1}).$$

По следствию к предложению 5 тройка функций $f_{x_n}^{\sigma_n}(\tilde{x})$, $g_{x_n}^{\sigma_n}(\tilde{x})$, $h_{x_n}^{\sigma_n}(\tilde{x})$ удовлетворяет предположению индукции, поэтому

$$\left\{f_{x_n}^{\sigma_n}(\tilde{x}^{\tilde{\sigma}}), g_{x_n}^{\sigma_n}(\tilde{x}^{\tilde{\sigma}}), h_{x_n}^{\sigma_n}(\tilde{x}^{\tilde{\sigma}})\right\} =$$
$$= \left\{p_{n-1}(x_1, \ldots, x_{n-1}), q_{n-1}(x_1, \ldots, x_{n-1}), r_{n-1}(x_1, \ldots, x_{n-1})\right\}.$$

Пусть для определённости $g_{x_n}^{\sigma_n}(\tilde{x}^{\tilde{\sigma}}) = p_{n-1}(x_1, \ldots, x_{n-1})$. Тогда

$$h_{x_n}^{\sigma_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = r_{n-1}(x_1, \ldots, x_{n-1}).$$

Тройки функций

$$\begin{array}{lll}
g_{x_n}^{\sigma_n}(x_1, \ldots, x_n), & g_{x_n}^{\bar{\sigma}_n}(x_1, \ldots, x_n), & g'_{x_n}(x_1, \ldots, x_n); \\
h_{x_n}^{\sigma_n}(x_1, \ldots, x_n), & h_{x_n}^{\bar{\sigma}_n}(x_1, \ldots, x_n), & h'_{x_n}(x_1, \ldots, x_n); \\
f_{x_n}^{\bar{\sigma}_n}(x_1, \ldots, x_n), & g_{x_n}^{\bar{\sigma}_n}(x_1, \ldots, x_n), & h_{x_n}^{\bar{\sigma}_n}(x_1, \ldots, x_n); \\
f'_{x_n}(x_1, \ldots, x_n), & g'_{x_n}(x_1, \ldots, x_n), & h'_{x_n}(x_1, \ldots, x_n)
\end{array}$$

также удовлетворяют предположению индукции. Поэтому

$$g_{x_n}^{\bar{\sigma}_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = q_{n-1}(x_1, \ldots, x_{n-1});$$
$$g'_{x_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = r_{n-1}(x_1, \ldots, x_{n-1});$$
$$h_{x_n}^{\bar{\sigma}_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = p_{n-1}(x_1, \ldots, x_{n-1});$$
$$h'_{x_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = q_{n-1}(x_1, \ldots, x_{n-1}).$$

Отсюда получается:

$$g(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = x_n \cdot g_{x_n}^{\sigma_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) \oplus \bar{x}_n \cdot g_{x_n}^{\bar{\sigma}_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) =$$

$$= x_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot q_{n-1}(x_1, \ldots, x_{n-1}) = r_n(x_1, \ldots, x_n);$$
$$h(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = x_n \cdot h_{x_n}^{\sigma_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) \oplus \bar{x}_n \cdot h_{x_n}^{\bar{\sigma}_n}(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) =$$
$$= x_n \cdot r_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}) = q_n(x_1, \ldots, x_n).$$

Таким образом,

$$\left\{f(\tilde{x}^{\tilde{\sigma}}), g(\tilde{x}^{\tilde{\sigma}}), h(\tilde{x}^{\tilde{\sigma}})\right\} = \left\{p_n(\tilde{x}), q_n(\tilde{x}), r_n(\tilde{x})\right\}.$$

$\triangleleft$

Предложение 7 *Если $n \geq 2$, то $f \in M_n^{\Diamond}$ тогда и только тогда, когда для любого $i \in \{1, \ldots, n\}$ справедливо включение $\{f_i^1, f_i^0, f_i'\} \subset M_n^{\Diamond}$.*

$\triangleright$ Доказательство. Пусть $f \in M_n^{\Diamond}$. Тогда из следствия к предложению 5 и определения однотипности следует, что $\{f_i^1, f_i^0, f_i'\} \subset M_{n-1}^{\Diamond}$.

Пусть теперь $\{f_i^1, f_i^0, f_i'\} \subset M_{n-1}^{\Diamond}$. Поскольку функции f_i^1, f_i^0, f_i' однотипны симметрическим функциям, можно считать, что $i = n$. По определению производной

$$f_{x_n}^0(\tilde{x}) \oplus f_{x_n}^1(\tilde{x}) \oplus f_{x_n}'(\tilde{x}) = 0.$$

Поэтому тройка функций f_i^1, f_i^0, f_i' удовлетворяет условиям предложения 6. Следовательно, найдётся набор $\sigma_1, \ldots, \sigma_{n-1}$, такой что

$$\left\{f_{x_n}^0(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n), f_{x_n}^1(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n), f_{x_n}'(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n)\right\} =$$
$$= \left\{p_{n-1}(x_1, \ldots, x_{n-1}), q_{n-1}(x_1, \ldots, x_{n-1}), r_{n-1}(x_1, \ldots, x_{n-1})\right\}.$$

Пусть для определённости

$$f_{x_n}^1(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n) = q_{n-1}(x_1, \ldots, x_{n-1}),$$
$$f_{x_n}^0(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n) = p_{n-1}(x_1, \ldots, x_{n-1}),$$
$$f_{x_n}'(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n) = r_{n-1}(x_1, \ldots, x_{n-1}).$$

Тогда справедлива следующая цепочка равенств:

$$f(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n) =$$

$$= x_n \cdot f^1_{x_n}(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n) \oplus \bar{x}_n \cdot f^0_{x_n}(x_1^{\sigma_1}, \ldots, x_{n-1}^{\sigma_{n-1}}, x_n) =$$
$$= x_n \cdot q_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n \cdot p_{n-1}(x_1, \ldots, x_{n-1}) =$$
$$= r_n(x_1, \ldots, x_{n-1}, \bar{x}_n).$$

Полагая $\sigma_n = 0$, получим

$$f(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = r_n(x_1, \ldots, x_n).$$

По определению однотипности $f \in M_n^{\Diamond}$. $\lhd$

Предложение 8 *Пусть f и g — однотипные функции, а C — один из классов $K(\mathtt{d}\ldots\mathtt{d})$, K или FK. Тогда*

$$L^{\&}_C(f) = L^{\&}_C(g).$$

$\rhd$ Доказательство. Вначале рассмотрим случай $C = K$. Пусть f и g — однотипные функции размерности n и $\mathsf{A} \in K$ — пучок размерности n, такой что

$$L^{\&}_{\mathsf{A}}(f) = L^{\&}_K(f).$$

По определению класса K существуют операторы $\mathfrak{u}$, $\mathfrak{v}$ длины n, такие что $\mathsf{A} = D(\mathfrak{u}, \mathfrak{v})$. Пусть $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — естественная нумерация пучка A, в которой:

$$\mathfrak{a}_i^{\tilde{\sigma}} = \begin{cases} \mathfrak{u}_i, & \text{если } \sigma_i = 0, \\ \mathfrak{v}_i, & \text{если } \sigma_i = 1, \end{cases} \qquad \tilde{\sigma} \in E^n.$$

По определению отношения однотипности существует перестановка индексов $i_1, \ldots, i_n$ и набор $\tilde{\tau} \in E^n$, такие что

$$f(x_{i_1}^{\tau_{i_1}}, \ldots, x_{i_n}^{\tau_{i_n}}) = g(x_1, \ldots, x_n).$$

Используя полиномиальное представление функции f по пучку A, получим:

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} \!\!\!\!\bigcirc\;\; \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n).$$

Поэтому

$$g(\tilde{x}) = f(x_{i_1}^{\tau_{i_1}}, \ldots, x_{i_n}^{\tau_{i_n}}) = \sum_{\tilde{\sigma}} \!\!\!\!\bigcirc\;\; \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}}(x_{i_1}^{\tau_{i_1}} \cdot \ldots \cdot x_{i_n}^{\tau_{i_n}}).$$

Определим пучок B размерности n по его нумерации $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$, где компоненты операторов $\mathfrak{b}^{\tilde{\sigma}}$ находятся по формулам:

$$\mathfrak{b}_{i_j}^{\tilde{\sigma}} = \begin{cases} \mathfrak{e}, & \text{если } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{e} \text{ и } \tau_{i_j} = 1, \text{ или } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{p} \text{ и } \tau_{i_j} = 0; \\ \mathfrak{p}, & \text{если } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{e} \text{ и } \tau_{i_j} = 0, \text{ или } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{p} \text{ и } \tau_{i_j} = 1; \\ \mathfrak{d}, & \text{если } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{d}; \end{cases} \tag{3.1}$$

$j \in \{1, \ldots, n\}$, $\tilde{\sigma} \in E^n$. Тогда

$$g(\tilde{x}) = \sum_{\tilde{\sigma}} \!\!\!\!\bigcirc\, \alpha_{\tilde{\sigma}} \cdot \mathfrak{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n),$$

то есть

$$L^{\&}_{\mathsf{B}}(g) = L^{\&}_{\mathsf{A}}(f) = L^{\&}_{K}(f).$$

Поскольку $\mathsf{A} = D(\mathfrak{a}^{\tilde{0}}, \mathfrak{a}^{\tilde{1}})$, то $\mathsf{B} = D(\mathfrak{b}^{\tilde{0}}, \mathfrak{b}^{\tilde{1}})$, то есть $\mathsf{B} \in K$. В силу симметричности отношения однотипности, получаем:

$$L^{\&}_{K}(g) = L^{\&}_{K}(f).$$

Заметим, что если пучок A лежит в классе $K(\mathfrak{d} \ldots \mathfrak{d})$, то и пучок B также лежит в $K(\mathfrak{d} \ldots \mathfrak{d})$. Таким образом,

$$L^{\&}_{K(\mathfrak{d}\ldots\mathfrak{d})}(g) = L^{\&}_{K(\mathfrak{d}\ldots\mathfrak{d})}(f).$$

Теперь рассмотрим случай $C = FK$. Пусть f и g — однотипные функции размерности n и $\mathsf{A} \in FK$ — пучок размерности n, такой что

$$L^{\&}_{\mathsf{A}}(f) = L^{\&}_{FK}(f).$$

По определению отношения однотипности существует набор $\tilde{\tau} \in E^n$ и перестановка $i_1, \ldots, i_n$, такие что

$$f(x_{i_1}^{\tau_{i_1}}, \ldots, x_{i_n}^{\tau_{i_n}}) = g(x_1, \ldots, x_n).$$

Пусть $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — нумерация пучка A. Зададим пучок B по его нумерации $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$, где компоненты операторов $\mathfrak{b}^{\tilde{\sigma}}$ определяются по формулам (3.1). Тогда

$$L^{\&}_{\mathsf{B}}(g) = L^{\&}_{\mathsf{A}}(f) = L^{\&}_{FK}(f).$$

Остается только показать, что $\mathsf{B} \in FK$. Рассмотрим операторный пучок $\mathsf{C} = W(B \mid i_1, \ldots, i_n)$. Если $\mathsf{C} \in FK$, то, очевидно, $\mathsf{B} \in FK$. Нумерация $\left(\mathfrak{c}^{\tilde{0}}, \ldots, \mathfrak{c}^{\tilde{1}}\right)$, где

$$\mathfrak{c}_j^{\tilde{\sigma}} = \begin{cases} \mathfrak{e}, & \text{если } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{e} \text{ и } \tau_j = 1, \text{ или } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{p} \text{ и } \tau_j = 0; \\ \mathfrak{p}, & \text{если } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{e} \text{ и } \tau_j = 0, \text{ или } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{p} \text{ и } \tau_j = 1; \\ \mathfrak{d}, & \text{если } \mathfrak{a}_j^{\tilde{\sigma}} = \mathfrak{d}; \end{cases} \qquad \tilde{\sigma} \in E^n,$$

является нумерацией пучка C. Индукцией по построению пучка A легко показать, что $\mathsf{C} \in FK$. Значит $\mathsf{B} \in FK$, и в силу симметричности отношения однотипности, получаем:

$$L^{\&}_{FK}(g) = L^{\&}_{FK}(g).$$

$\lhd$

Предложение 9 *Для любой функции $f \in F_n$, любого базисного пучка A размерности $n-1$, любого $i \in \{1, \ldots, n\}$ справедливо неравенство:*

$$L^{\&}_{\mathsf{A}}(f_i^1) + L^{\&}_{\mathsf{A}}(f_i^0) + L^{\&}_{\mathsf{A}}(f_i') \leq 2^n.$$

$\rhd$ Доказательство. Пусть $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — некоторая нумерация пучка A. Тогда

$$f^1_{x_i}(\tilde{x}) = \sum_{\tilde{\sigma} \in E^{n-1}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_{i-1} \cdot x_{i+1} \cdot \ldots \cdot x_n);$$
$$f^0_{x_i}(\tilde{x}) = \sum_{\tilde{\sigma} \in E^{n-1}} \beta_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_{i-1} \cdot x_{i+1} \cdot \ldots \cdot x_n).$$

Рассмотрим следующие множества:

$$I_1 = \left\{\tilde{\sigma} \in E^{n-1} \mid \alpha_{\tilde{\sigma}} = 1,\ \beta_{\tilde{\sigma}} = 0\right\};$$
$$I_2 = \left\{\tilde{\sigma} \in E^{n-1} \mid \alpha_{\tilde{\sigma}} = 0,\ \beta_{\tilde{\sigma}} = 1\right\};$$
$$I_3 = \left\{\tilde{\sigma} \in E^{n-1} \mid \alpha_{\tilde{\sigma}} = 1,\ \beta_{\tilde{\sigma}} = 1\right\}.$$

Поскольку $f'_{x_i}(\tilde{x}) = f^1_{x_i}(\tilde{x}) \oplus f^0_{x_i}(\tilde{x})$, то справедливы следующие полиномиальные представления:

$$f^1_{x_i}(\tilde{x}) = \sum_{\tilde{\sigma} \in I_1 \cup I_3} \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_{i-1} \cdot x_{i+1} \cdot \ldots \cdot x_n);$$

$$f^0_{x_i}(\tilde{x}) = \sum_{\tilde{\sigma}\in I_2\cup I_3} \mathfrak{a}^{\tilde{\sigma}}(x_1\cdot\ldots\cdot x_{i-1}\cdot x_{i+1}\cdot\ldots\cdot x_n);$$
$$f'_{x_i}(\tilde{x}) = \sum_{\tilde{\sigma}\in I_1\cup I_2} \mathfrak{a}^{\tilde{\sigma}}(x_1\cdot\ldots\cdot x_{i-1}\cdot x_{i+1}\cdot\ldots\cdot x_n).$$

Так как множества I_1, I_2, I_3 попарно не пересекаются, и $I_1\cup I_2\cup I_3 \subset E^{n-1}$, то $|I_1| + |I_2| + |I_3| \le 2^{n-1}$, где $|M|$ означает количество элементов во множестве M. Тогда очевидно, что

$$L^{\&}_{\mathsf{A}}(f^1_i) + L^{\&}_{\mathsf{A}}(f^0_i) + L^{\&}_{\mathsf{A}}(f'_i) = 2\cdot(|I_1| + |I_2| + |I_3|) \le 2^n.$$

◁

§ 9. Функции наибольшей сложности в классах операторных полиномиальных нормальных форм

В следующей теореме найден вид всех функций, имеющих наибольшую сложность в $\mathfrak{d}$-кронекеровом классе полиномиальных форм по базисной функции многоместной конъюнкции.

Теорема 6 *Пусть $f \in F_n$, $n \ge 1$. Тогда следующие условия эквивалентны:*

1) $L^{\&}_{K(\mathfrak{d}\ldots\mathfrak{d})}(f) = L_{K(\mathfrak{d}\ldots\mathfrak{d})}(n)$;
2) $f \in M^{\Diamond}_n$ *при нечетном* n, $f \in \widetilde{M}^{\Diamond}_n$ *при четном* n.

► Приведем схему доказательства теоремы.

По теореме 3

$$L_{K(\mathfrak{d}\ldots\mathfrak{d})}(n) = \left\lfloor \frac{2}{3}\cdot 2^n \right\rfloor.$$

В [24] показано, что если $f \in M_n$, то для любого пучка $\mathsf{A} \in K(\mathfrak{d}\ldots\mathfrak{d})$ размерности n справедливо:

$$\left\lfloor \frac{2}{3}\cdot 2^n \right\rfloor \le L^{\&}_{\mathsf{A}}(f) \le \left\lfloor \frac{2}{3}\cdot 2^n \right\rfloor + 1. \qquad (3.2)$$

Из этого и предложения 8 следует, что для любой функции $f \in M_n^{\Diamond}$

$$L^{\&}_{K(\mathrm{d}\ldots\mathrm{d})}(f) = L_{K(\mathrm{d}\ldots\mathrm{d})}(n).$$

В лемме 6.3 утверждение теоремы докажем для $n \in \{1, 2, 3\}$. Затем в лемме 6.8 для функций из множества $F_n \backslash \overline{M_n^{\Diamond}}$ установим неравенство

$$L_{K(\mathrm{d}\ldots\mathrm{d})}(f) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

Доказательство леммы 6.8 опирается на леммы 6.3 и 6.7. Леммы 6.4, 6.5, 6.6 — это последовательное доказательство леммы 6.7.

Затем для $n \geq 2$ установим соотношения:

$$L^{\&}_{K(\mathrm{d}\ldots\mathrm{d})}(\bar{p}_n) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor, \text{ если } n \text{ нечетное};$$

$$L^{\&}_{K(\mathrm{d}\ldots\mathrm{d})}(\bar{p}_n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor, \text{ если } n \text{ четное};$$

$$L^{\&}_{K(\mathrm{d}\ldots\mathrm{d})}(\bar{q}_n) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor, \text{ при любых } n.$$

Они следуют из лемм 6.9 и 6.10.

Леммы 6.1 и 6.2 носят вспомогательный характер и часто применяются в доказательстве.

Наконец, применив предложение 8, получим утверждение теоремы.

Лемма 6.1 *Для любого $\tau \in \{0, 1\}$, любого пучка $\mathsf{A} \in K(\mathrm{d}\ldots\mathrm{d})$ размерности $n-1$, любого аргумента $i \in \{1, \ldots, n\}$ существует пучок $\mathsf{B} \in K(\mathrm{d}\ldots\mathrm{d})$ размерности n, такой что для любой функции $f \in F_n$ выполняется:*

$$L^{\&}_{\mathsf{A}}(f_i^{\tau}) + L^{\&}_{\mathsf{A}}(f_i') = L^{\&}_{\mathsf{B}}(f).$$

$\triangleright$ Доказательство. По определению d-кронекерова класса $K(\mathrm{d}\ldots\mathrm{d})$ для некоторого оператора ν длины $n-1$ выполняется: $\mathsf{A} = D(\mathrm{d}\ldots\mathrm{d}, \nu)$. Пусть $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — естественная нумерация пучка A, в которой компоненты операторов $\mathfrak{a}^{\tilde{\sigma}}$ вычисляются по формулам:

$$\mathfrak{a}_i^{\tilde{\sigma}} = \begin{cases} \mathrm{d}, & \text{если } \sigma_i = 0; \\ \nu_i, & \text{если } \sigma_i = 1; \end{cases} \qquad i \in \{1, \ldots, n-1\}, \quad \tilde{\sigma} \in E^{n-1}.$$

Для любой функции $f \in F_n$ справедливо разложение

$$f(\tilde{x}) = x_i^{\bar{\tau}} \cdot f'_{x_i}(\tilde{x}) \oplus f^{\tau}_{x_i}(\tilde{x}).$$

Используя полиномиальные представления функций f'_i и f_i^{τ} по пучку A, получим следующую цепочку равенств:

$$\begin{gathered} f(\tilde{x}) = f^{\tau}_{x_i}(\tilde{x}) \oplus x_i^{\bar{\tau}} \cdot f'_{x_i}(\tilde{x}) = \\ = \sum_{\tilde{\sigma} \in E^{n-1}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_{i-1} \cdot x_{i+1} \cdot \ldots \cdot x_n) \oplus \\ \oplus x_i^{\bar{\tau}} \cdot \sum_{\tilde{\sigma} \in E^{n-1}} \beta_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_{i-1} \cdot x_{i+1} \cdot \ldots \cdot x_n). \end{gathered} \tag{3.3}$$

Положим $\mathfrak{u} = \nu_1 \ldots \nu_{i-1} \mathfrak{u}_i \nu_i \ldots \nu_{n-1}$, где

$$\mathfrak{u}_i = \begin{cases} \mathfrak{e}, & \text{если } \tau = 0; \\ \mathfrak{p}, & \text{если } \tau = 1; \end{cases}$$

$\mathsf{B} = D(\mathfrak{d} \ldots \mathfrak{d}, \mathfrak{u})$, и пусть $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$ — естественная нумерация пучка $D(\mathfrak{d} \ldots \mathfrak{d}, \mathfrak{u})$. Тогда из (3.3) следует:

$$f(\tilde{x}) = \sum_{\tilde{\sigma} \in E^n} \gamma_{\tilde{\sigma}} \cdot \mathfrak{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n), \qquad \text{где} \quad \gamma_{\tilde{\sigma}} = \begin{cases} \alpha_{\tilde{\tau}}, & \text{если } \sigma_i = 0; \\ \beta_{\tilde{\tau}}, & \text{если } \sigma_i = 1; \end{cases}$$

$\tilde{\tau} = \sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n$, $\tilde{\sigma} \in E^n$. По определению сложности функции относительно пучка получим:

$$L^{\&}_{\mathsf{A}}(f_i^{\tau}) + L^{\&}_{\mathsf{A}}(f'_i) = L^{\&}_{\mathsf{B}}(f).$$

$\lhd$

В следующих леммах функции будут часто представляться двоичными и шестнадцатеричными векторами.

Лемма 6.2 *Пусть $f \in F_n \backslash M_n^{\Diamond}$, где $n \geq 1$. Тогда найдется пучок $\mathsf{A} \in K(\mathfrak{d} \ldots \mathfrak{d})$ размерности $n-1$, и натуральное число $i \in \{1, \ldots, n\}$, такие что выполняется:*

$$L^{\&}_{\mathsf{A}}(f_i^1) + L^{\&}_{\mathsf{A}}(f_i^0) + L^{\&}_{\mathsf{A}}(f'_i) \leq 2^n - 2.$$

▷ Доказательство проведем индукцией по n.

Базис индукции при $n = 1$. Поскольку $F_1 \backslash M_1^{\Diamond} = \{(00)_2\}$, то для любой функции $f \in F_1 \backslash M_1^{\Diamond}$, для любого пучка A размерности 1 выполняется:

$$L^{\&}_{\mathsf{A}}(f_1^1) + L^{\&}_{\mathsf{A}}(f_1^0) + L^{\&}_{\mathsf{A}}(f_1') = 0 \leq 2^1 - 2.$$

Шаг индукции при $n \geq 2$. Пусть $f \in F_n \backslash M_n^{\Diamond}$. По предложению 7 хотя бы одна из функций f_n^1, f_n^0, f_n' не принадлежит множеству $M_{n-1}^{\Diamond}$. Пусть для определенности это функция f_n', для остальных случаев доказательства аналогичны. По предположению индукции для f_n' существует пучок $\mathsf{B} \in K(\mathsf{d} \dots \mathsf{d})$ и аргумент $i \in \{1, \dots, n-1\}$, такие что

$$L^{\&}_{\mathsf{B}}(f_{ni}'^{1}) + L^{\&}_{\mathsf{B}}(f_{ni}'^{0}) + L^{\&}_{\mathsf{B}}(f_{ni}'') \leq 2^{n-1} - 2.$$

По предложению 9

$$L^{\&}_{\mathsf{B}}(f_{ni}^{0\,1}) + L^{\&}_{\mathsf{B}}(f_{ni}^{0\,0}) + L^{\&}_{\mathsf{B}}(f_{ni}^{0\,\prime}) \leq 2^{n-1}.$$

По лемме 6.1 существует пучок $\mathsf{A} \in K(\mathsf{d} \dots \mathsf{d})$, такой что

$$L^{\&}_{\mathsf{A}}(f_i^1) = L^{\&}_{\mathsf{B}}(f_{ni}'^{1}) + L^{\&}_{\mathsf{B}}(f_{ni}^{0\,1});$$
$$L^{\&}_{\mathsf{A}}(f_i^0) = L^{\&}_{\mathsf{B}}(f_{ni}'^{0}) + L^{\&}_{\mathsf{B}}(f_{ni}^{0\,0});$$
$$L^{\&}_{\mathsf{A}}(f_i') = L^{\&}_{\mathsf{B}}(f_{ni}'') + L^{\&}_{\mathsf{B}}(f_{ni}^{0\,\prime}).$$

Поэтому

$$L^{\&}_{\mathsf{A}}(f_i^1) + L^{\&}_{\mathsf{A}}(f_i^0) + L^{\&}_{\mathsf{A}}(f_i^1) =$$
$$= \left(L^{\&}_{\mathsf{B}}(f_{ni}'^{1}) + L^{\&}_{\mathsf{B}}(f_{ni}'^{0}) + L^{\&}_{\mathsf{B}}(f_{ni}'')\right) \oplus \left(L^{\&}_{\mathsf{B}}(f_{ni}^{0\,1}) + L^{\&}_{\mathsf{B}}(f_{ni}^{0\,0}) + L^{\&}_{\mathsf{B}}(f_{ni}^{0\,\prime})\right) \leq$$
$$\leq 2^{n-1} - 2 + 2^{n-1} = 2^n - 2.$$

◁

Лемма 6.3

1) *Пусть* $f \in F_1$. *Тогда* $L^{\&}_{K(\mathsf{d}\dots\mathsf{d})}(f) \iff f \in M_1^{\Diamond}$.
2) *Пусть* $f \in F_2$. *Тогда* $L^{\&}_{K(\mathsf{d}\dots\mathsf{d})}(f) \iff f \in \widetilde{M_2^{\Diamond}}$.
3) *Пусть* $f \in F_3$. *Тогда* $L^{\&}_{K(\mathsf{d}\dots\mathsf{d})}(f) \iff f \in M_3^{\Diamond}$.

$\triangleright$ Множество F_1 состоит из четырех элементов:

$$F_1 = \{(00)_2, (01)_2, (10)_2, (11)_2\}.$$

Полиномиальная форма для функции $(00)_2$ относительно любого пучка имеет сложность $0 < 1 = \left\lfloor \frac{2}{3} \cdot 2^1 \right\rfloor$. Поэтому остальные функции имеют ненулевую сложность. Следующие представления показывают, что их сложность в классе $K(\mathtt{d} \ldots \mathtt{d})$ не больше 1:

$$\begin{aligned} f(x_1) &= 0 \cdot \mathtt{d}x_1 \oplus 1 \cdot \mathtt{e}x_1, \quad && \text{для } f = (01)_2; \\ f(x_1) &= 0 \cdot \mathtt{d}x_1 \oplus 1 \cdot \mathtt{p}x_1, \quad && \text{для } f = (10)_2; \\ f(x_1) &= 1 \cdot \mathtt{d}x_1 \oplus 0 \cdot \mathtt{e}x_1, \quad && \text{для } f = (11)_2. \end{aligned}$$

Так как $M_1^{\Diamond} = \{(01)_2, (10)_2, (11)_2\}$, первый пункт леммы доказан.

Множество F_2 можно разбивается на классы однотипных функций следующим образом:

$$\begin{gathered} F_2 = \left\{(0000)_2\right\} \cup \left\{(0001)_2, (0010)_2, (0100)_2, (1000)_2\right\} \cup \\ \cup \left\{(0011)_2, (0101)_2, (1010)_2, (1100)_2\right\} \cup \left\{(0110)_2, (1001)_2\right\} \cup \\ \cup \left\{(0111)_2, (1011)_2, (1101)_2, (1110)_2\right\} \cup \left\{(1111)_2\right\}. \end{gathered}$$

По предложению 8 сложности однотипных функций равны, поэтому лемму нужно доказать только для представителей классов однотипных функций. Поскольку $p_2 = (1001)_2$, $q_2 = (1110)_2$, $\bar{p}_2 = (0110)_2$, то $\widetilde{M_2^{\Diamond}} = M_2^{\Diamond}$, и по предложениям VI, 8 и неравенствам (3.2) для любой функции $f \in \widetilde{M_2^{\Diamond}}$

$$L^{\&}_{K(\mathtt{d}\ldots\mathtt{d})}(f) = L_{K(\mathtt{d}\ldots\mathtt{d})}(2).$$

Рассмотрим полиномиальные представления функций $(0000)_2$, $(0001)_2$, $(0011)_2$ и $(1111)_2$ относительно пучка $\{\mathtt{dd}, \mathtt{de}, \mathtt{ed}, \mathtt{ee}\}$:

$$\begin{aligned} &0 \cdot \mathtt{dd}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{de}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{ed}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{ee}(x_1 \cdot x_2); \\ &0 \cdot \mathtt{dd}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{de}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{ed}(x_1 \cdot x_2) \oplus 1 \cdot \mathtt{ee}(x_1 \cdot x_2); \\ &0 \cdot \mathtt{dd}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{de}(x_1 \cdot x_2) \oplus 1 \cdot \mathtt{ed}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{ee}(x_1 \cdot x_2); \\ &1 \cdot \mathtt{dd}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{de}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{ed}(x_1 \cdot x_2) \oplus 0 \cdot \mathtt{ee}(x_1 \cdot x_2). \end{aligned}$$

Сложность этих форм не превосходит $1 < L_{K(\mathtt{d}\ldots\mathtt{d})}(2) = 2$. Мы рассмотрели представителей всех классов однотипных функций, поэтому для $n = 2$ лемма справедлива.

Пусть $f \in F_3 \backslash M_3^{\Diamond}$. Возможны два случая: $f_3' \in M_2^{\Diamond}$ и $f_3' \notin M_2^{\Diamond}$.

Рассмотрим случай $f_3' \in M_2^{\Diamond}$. По лемме 6.2 найдется оператор $\nu_1\nu_2$, такой что для пучка $\mathsf{A} = D(\mathtt{dd}, \nu_1\nu_2)$ справедливо неравенство:

$$L_{\mathsf{A}}^{\&}(f_3^1) + L_{\mathsf{A}}^{\&}(f_3^0) + L_{\mathsf{A}}^{\&}(f_3') \leq 2^3 - 2.$$

По предложениям 8 и неравенствам (3.2)

$$L_{\mathsf{A}}^{\&}(f_3') \leq 3 = \left\lfloor \frac{2}{3} \cdot 2^2 \right\rfloor + 1.$$

Сложим два последних неравенства, получим:

$$\left(L_{\mathsf{A}}^{\&}(f_3^1) + L_{\mathsf{A}}^{\&}(f_3')\right) + \left(L_{\mathsf{A}}^{\&}(f_3^0) + L_{\mathsf{A}}^{\&}(f_3')\right) \leq 9.$$

Поэтому хотя бы одно из выражений в скобках меньше 5. Тогда по лемме 6.1 существует пучок $\mathsf{B} \in K(\mathtt{d}\ldots\mathtt{d})$, такой что

$$L_{\mathsf{B}}^{\&}(f) < 5 = \left\lfloor \frac{2}{3} \cdot 2^3 \right\rfloor.$$

Теперь рассмотрим случай $f_3' \notin M_2^{\Diamond}$. Поскольку $\widetilde{M_2^{\Diamond}} = M_2^{\Diamond}$, существует оператор $\nu_1\nu_2$, такой что для пучка $\mathsf{A} = D(\mathtt{dd}, \nu_1\nu_2)$ справедливо:

$$L_{\mathsf{A}}^{\&}(f_3') \leq 1 < 2 = \left\lfloor \frac{2}{3} \cdot 2^2 \right\rfloor.$$

По предложению 9

$$L_{\mathsf{A}}^{\&}(f_3^1) + L_{\mathsf{A}}^{\&}(f_3^0) + L_{\mathsf{A}}^{\&}(f_3') \leq 2^3.$$

Сложим два последних неравенства, получим:

$$\left(L_{\mathsf{A}}^{\&}(f_3^1) + L_{\mathsf{A}}^{\&}(f_3')\right) + \left(L_{\mathsf{A}}^{\&}(f_3^0) + L_{\mathsf{A}}^{\&}(f_3')\right) \leq 9.$$

По лемме 6.1 существует пучок $\mathsf{B} \in K(\mathtt{d}\ldots\mathtt{d})$, такой что

$$L_{\mathsf{B}}^{\&}(f) < \left\lfloor \frac{2}{3} \cdot 2^3 \right\rfloor.$$

Тем самым лемма 6.3 доказана. $\lhd$

Лемма 6.4 *Пусть* $f \in F_3 \backslash \overline{M}_3^{\Diamond}$, *и* f *не является однотипной* $(17)_{16}$. *Тогда существует* $i \in \{1,2,3\}$, *такое что* $f_i' \in F_2 \backslash M_2^{\Diamond}$.

$\triangleright$ Доказательство. Сначала предположим, что у функции f есть остаточная или производная функция $f_j^{\omega_j}$ с фиктивным аргументом $k \in \{1,2\}$. В этом случае ${f_j^{\omega_j}}'_k = (00)_2$. Поскольку $(00)_2 \notin M_1^{\Diamond}$, то по предложению 7 $f_i' \in F_2 \backslash M_2^{\Diamond}$, где

$$i = \begin{cases} k, & \text{если } k < j; \\ k+1, & \text{если } k \geq j. \end{cases}$$

Пусть теперь у функции $f \in F_3$ все остаточные по первому аргументу существенные. С точностью до отношения однотипности можно считать, что $f_1^1 \in \{(0001)_2, (0110)_2, (0111)_2\}$. Кроме того, будем рассматривать только те функции, у которых $f_1' \in M_2^{\Diamond}$, поскольку для остальных функций лемма справедлива. Легко проверить, что

$$M_2^{\Diamond} = \{(0110)_2, (1001)_2, (0111)_2, (1011)_2, (1101)_2, (1110)_2\}.$$

Составим таблицу остаточных функций f_1^0 в зависимости от f_1^1 и f_1'.

f_1^0		f_1^1		
		$(0001)_2$	$(0110)_2$	$(0111)_2$
f_1'	$(0110)_2$	$(0111)_2$	$(0000)_2$	$(0001)_2$
	$(1001)_2$	$(1000)_2$	$(1111)_2$	$(1110)_2$
	$(0111)_2$	$(0110)_2$	$(0001)_2$	$(0000)_2$
	$(1011)_2$	$(1010)_2$	$(1101)_2$	$(1100)_2$
	$(1101)_2$	$(1100)_2$	$(1011)_2$	$(1010)_2$
	$(1110)_2$	$(1111)_2$	$(1000)_2$	$(1001)_2$

Таблица 3

Функции $(0000)_2$, $(1010)_2$, $(1100)_2$ имеют фиктивные аргументы, поэтому в дальнейшем мы их не рассматриваем. Из остальных построим функции размерности 3, используя разложение Шеннона

$$f(\tilde{x}) = x_1 \cdot f_{x_1}^1(\tilde{x}) \oplus \bar{x}_1 \cdot f_{x_1}^0(\tilde{x}).$$

Эти функции разбиваются на следующие множества однотипных функций:

$$\{(71)_{16},(17)_{16}\}\subset\{(17)_{16}\}^{\Diamond};$$
$$\{(81)_{16}\}\subset\{\bar{p}_3\}^{\Diamond};$$
$$\{(\mathrm{E7})_{16}\}\subset\{p_3\}^{\Diamond};$$
$$\{(61)_{16},(16)_{16},(81)_{16}\}\subset\{\bar{q}_3\}^{\Diamond};$$
$$\{(\mathrm{D6})_{16},(\mathrm{B6})_{16},(97)_{16}\}\subset\{q_3\}^{\Diamond}.$$

Лемма доказана. $\lhd$

Лемма 6.5 *Пусть $f\in F_4\backslash\overline{M}_4^{\Diamond}$. Тогда существует $i\in\{1,2,3,4\}$, такое что $f'_i\in F_3\backslash M_3^{\Diamond}$.*

$\rhd$ Доказательство. Пусть $f\in F_4\backslash\overline{M}_4^{\Diamond}$.

Сначала предположим, что у функции f есть остаточная или производная функция $f_j^{\omega_j}\notin\overline{M}_3^{\Diamond}\cup\{(17)_{16}\}^{\Diamond}$. По лемме 6.4 существует такое $k\in\{1,2,3\}$, такое что $f_{j\,k}^{\omega_j\,\prime}\notin M_2^{\Diamond}$. Тогда по предложению 7 $f'_i\notin M_3^{\Diamond}$, где

$$i=\begin{cases}k, & \text{если } k<j;\\ k+1, & \text{если } k\geq j.\end{cases}$$

Пусть теперь у функции f все остаточные по первому аргументу принадлежат множеству $\overline{M}_3^{\Diamond}\cup\{(17)_{16}\}^{\Diamond}$. С точностью до отношения однотипности можно считать, что

$$f_1^1\in\{(16)_{16},(17)_{16},(18)_{16},(6\mathrm{B})_{16},(7\mathrm{E})_{16}\}.$$

Будем рассматривать только те функции, у которых $f'_1\in M_3^{\Diamond}$, поскольку для остальных функций лемма справедлива. Нетрудно проверить, что

$$M_3^{\Diamond}\in\big\{(6\mathrm{B})_{16},(97)_{16},(9\mathrm{E})_{16},(6\mathrm{D})_{16},(\mathrm{B6})_{16},(79)_{16},$$
$$(\mathrm{E9})_{16},(\mathrm{D6})_{16},(7\mathrm{E})_{16},(\mathrm{BD})_{16},(\mathrm{E7})_{16},(\mathrm{DB})_{16}\big\}.$$

Составим таблицу остаточных функций f_1^0 в зависимости от f_1^1 и f_1'.

f_1^0		f_1^1				
		$(16)_{16}$	$(17)_{16}$	$(18)_{16}$	$(6B)_{16}$	$(7E)_{16}$
f_1'	$(6B)_{16}$	$(7D)_{16}$	$(7C)_{16}$	$(73)_{16}$	$(00)_{16}$	$(15)_{16}$
	$(97)_{16}$	$(81)_{16}$	$(80)_{16}$	$(8F)_{16}$	$(FC)_{16}$	$(E9)_{16}$
	$(9E)_{16}$	$(88)_{16}$	$(89)_{16}$	$(86)_{16}$	$(F5)_{16}$	$(E0)_{16}$
	$(6D)_{16}$	$(7B)_{16}$	$(7A)_{16}$	$(75)_{16}$	$(06)_{16}$	$(13)_{16}$
	$(B6)_{16}$	$(A0)_{16}$	$(A1)_{16}$	$(AE)_{16}$	$(DD)_{16}$	$(C8)_{16}$
	$(79)_{16}$	$(6F)_{16}$	$(6E)_{16}$	$(61)_{16}$	$(12)_{16}$	$(07)_{16}$
	$(E9)_{16}$	$(FF)_{16}$	$(FE)_{16}$	$(F1)_{16}$	$(82)_{16}$	$(97)_{16}$
	$(D6)_{16}$	$(C0)_{16}$	$(C1)_{16}$	$(CE)_{16}$	$(BD)_{16}$	$(A8)_{16}$
	$(7E)_{16}$	$(68)_{16}$	$(69)_{16}$	$(66)_{16}$	$(15)_{16}$	$(00)_{16}$
	$(BD)_{16}$	$(AB)_{16}$	$(AA)_{16}$	$(A5)_{16}$	$(D6)_{16}$	$(C3)_{16}$
	$(E7)_{16}$	$(F1)_{16}$	$(F0)_{16}$	$(FF)_{16}$	$(8C)_{16}$	$(99)_{16}$
	$(DB)_{16}$	$(CD)_{16}$	$(CC)_{16}$	$(C3)_{16}$	$(B0)_{16}$	$(A5)_{16}$

Таблица 4

Исключим из рассмотрения функции f_1^0, которые не принадлежат множеству $\overline{M}_3^{\Diamond} \cup \{(17)_{16}\}^{\Diamond}$. Нетрудно видеть, что

$$\overline{M}_3^{\Diamond} \cup \{(17)_{16}\}^{\Diamond} =$$
$$= \{(16)_{16}, (29)_{16}, (49)_{16}, (86)_{16}, (61)_{16}, (92)_{16}, (94)_{16}, (68)_{16},$$
$$(17)_{16}, (2B)_{16}, (4D)_{16}, (8E)_{16}, (71)_{16}, (B2)_{16}, (D4)_{16}, (E8)_{16},$$
$$(6B)_{16}, (97)_{16}, (9E)_{16}, (6D)_{16}, (B6)_{16}, (79)_{16}, (E9)_{16}, (D6)_{16},$$
$$(18)_{16}, (24)_{16}, (42)_{16}, (81)_{16}, (7E)_{16}, (BD)_{16}, (DB)_{16}, (E7)_{16}\}.$$

Из остальных построим функции размерности 4, используя разложение Шеннона

$$f(\tilde{x}) = x_1 \cdot f_{x_1}^1(\tilde{x}) \oplus \bar{x}_1 \cdot f_{x_1}^0(\tilde{x}).$$

Эти функции разбиваются на следующие множества однотипных функций:

$$\{(6816)_{16}\} \subset \{\bar{p}_4\}^{\Diamond};$$

$$\{(\mathrm{D66B})_{16}\} \subset \{p_4\}^{\Diamond};$$
$$\{(8116)_{16}, (8618)_{16}, (6118)_{16}\} \subset \{\bar{q}_4\}^{\Diamond};$$
$$\{(\mathrm{E97E})_{16}, (977\mathrm{E})_{16}, (\mathrm{BD6B})_{16}\} \subset \{q_4\}^{\Diamond}.$$

Лемма доказана. $\triangleleft$

Лемма 6.6 *Пусть* $n \geq 4$, $f \in F_n \backslash \overline{M}_n^{\Diamond}$. *Тогда существует* $i \in \{1, \ldots, n\}$, *такой что* $f_i' \in F_{n-1} \backslash M_{n-1}^{\Diamond}$.

$\triangleright$ Доказательство проведем индукцией по n.

Базис индукции при $n = 4$ доказан в лемме 6.5.

Шаг индукции при $n \geq 5$ будем доказывать от противного. Пусть $f \in F_n \backslash \overline{M}_n^{\Diamond}$, и для любого $i \in \{1, \ldots, n\}$ выполняется: $f_i' \in M_{n-1}^{\Diamond}$. По предложению 7 для любых $i \in \{1, \ldots, n\}$ и $j \in \{1, \ldots, n-1\}$ справедливо включение:

$$\{\, f_{ij}'^{1},\ f_{ij}'^{0},\ f_{ij}'',\ f_{ij}^{0\prime},\ f_{ij}^{1\prime} \,\} \subset M_{n-2}^{\Diamond}. \tag{3.4}$$

Поскольку $f \notin M_n^{\Diamond}$ и $f_i' \notin M_{n-1}^{\Diamond}$, для любого $i \in \{1, \ldots, n\}$, то по предложению 7 для любого аргумента $j \in \{1, \ldots, n\}$ существует $\sigma_j \in \{0, 1\}$, такое что $f_j^{\sigma_j} \notin M_{n-1}^{\Diamond}$. Дальнейшее доказательство разобьем на два случая.

1. Существуют $i \in \{1, \ldots, n\}$ и $\sigma_i \in \{0, 1\}$, такие что $f_i^{\sigma_i} \notin \overline{M}_{n-1}^{\Diamond}$. Тогда по предположению индукции существует $j \in \{1, \ldots, n-1\}$, такое что $f_{i\,j}^{\sigma_i\prime} \notin M_{n-2}^{\Diamond}$, что противоречит (3.4).

2. Для любых $i \in \{1, \ldots, n\}$ и $\sigma_i \in \{0, 1\}$ выполняется: $f_i^{\sigma_i} \in \overline{M}_{n-1}^{\Diamond}$. Тогда справедливо ровно одно из двух условий:

$$\begin{array}{lll} 1) & f_i^1 \in M_{n-1}^{\Diamond} & \text{и} \quad \bar{f}_{\,i}^{\,0} \in M_{n-1}^{\Diamond}, \\ 2) & f_i^0 \in M_{n-1}^{\Diamond} & \text{и} \quad \bar{f}_{\,i}^{\,1} \in M_{n-1}^{\Diamond}, \end{array} \tag{3.5}$$

ибо в противном случае, учитывая условие $f_i' \in M_{n-1}^{\Diamond}$, по предложению 7 либо $f \in M_n^{\Diamond}$, либо $\bar{f} \in M_n^{\Diamond}$, то есть $f \in \overline{M}_n^{\Diamond}$, что противоречит предположению. Для определенности предположим, что $f_i^1 \in M_{n-1}^{\Diamond}$.

Пусть $j \in \{1, \ldots, n-1\}$. Без ограничения общности будем считать, что $j < i$. Для j-го аргумента также справедливо одно из условий (3.5). Для определенности будем считать, что $\bar{f}^{\,1}_{j} \in M^{\Diamond}_{n-1}$. Тогда, с одной стороны, $f^{1\,1}_{i\,j} \in M^{\Diamond}_{n-2}$, с другой стороны, $\bar{f}^{\,1\,1}_{i\,j} \in M^{\Diamond}_{n-2}$.

Индукцией по m легко доказать, что функции из $M^{\Diamond}_{m}$ принимают значение 1 не менее чем на $2^{m-1}+1$ наборе при $m \geq 3$. Учитывая это и условие $n \geq 5$, приходим к выводу, что никакая функция $g \in F_{n-2}$ не может удовлетворять условию:

$$\{g, \bar{g}\} \subset M^{\Diamond}_{n-2}.$$

Однако для функции $f^{1\,1}_{i\,j}$ это условие выполнено. Получили противоречие. $\lhd$

Лемма 6.7 *Пусть $n \geq 2$, $f \in F_n \backslash \overline{M}^{\Diamond}$ и существует $i \in \{1, \ldots, n\}$, такое что $f'_i \notin M^{\Diamond}_{n-1}$. Тогда существует пучок $\mathsf{A} \in K(\mathsf{d} \ldots \mathsf{d})$ размерности $n-1$, и $j \in \{1, \ldots, n\}$, такие что выполняются неравенства:*

$$L^{\&}_{\mathsf{A}}(f^1_j) + L^{\&}_{\mathsf{A}}(f^0_j) + L^{\&}_{\mathsf{A}}(f'_j) \leq 2^n - 2;$$
$$L^{\&}_{\mathsf{A}}(f'_j) < \frac{1}{3} \cdot 2^n + \frac{1}{2}.$$

$\rhd$ Доказательство проведем индукцией по n.

Базис индукции при $n = 2$. Поскольку

$$\{(0000)_2, (0011)_2, (1111)_2\}^{\Diamond} = F_2 \backslash \overline{M}^{\Diamond}_2,$$

достаточно рассмотреть только функции $(0000)_2$, $(0011)_2$, $(1111)_2$. Положим $\mathsf{A} = D(\mathsf{d}, \mathsf{e})$. Тогда для этих функций справедливы следующие равенства:

$$L^{\&}_{\mathsf{A}}(f^1_2) + L^{\&}_{\mathsf{A}}(f^0_2) + L^{\&}_{\mathsf{A}}(f'_2) = 0, \quad L^{\&}_{\mathsf{A}}(f'_2) = 0 \quad \text{для } f = (0000)_2;$$
$$L^{\&}_{\mathsf{A}}(f^1_2) + L^{\&}_{\mathsf{A}}(f^0_2) + L^{\&}_{\mathsf{A}}(f'_2) = 2, \quad L^{\&}_{\mathsf{A}}(f'_2) = 0 \quad \text{для } f = (0011)_2;$$
$$L^{\&}_{\mathsf{A}}(f^1_2) + L^{\&}_{\mathsf{A}}(f^0_2) + L^{\&}_{\mathsf{A}}(f'_2) = 2, \quad L^{\&}_{\mathsf{A}}(f'_2) = 0 \quad \text{для } f = (1111)_2.$$

Во всех случаях утверждение леммы выполняется.

Шаг индукции при $n \geq 3$ разобьем на два случая.

1. Существует $i \in \{1, \ldots, n\}$, такое что $f'_i \notin \overline{M}^{\Diamond}_{n-1} \cup \{(17)_{16}\}^{\Diamond}$. Тогда по предположению индукции существует $j \in \{1, \ldots, n-1\}$ и пучок $\mathsf{A} \in K(\mathsf{d} \ldots \mathsf{d})$ размерности $n-2$, такие что

$$L^{\&}_{\mathsf{A}}(f'_{ij}) < \frac{1}{3} \cdot 2^{n-1} + \frac{1}{2}; \tag{3.6}$$

$$L^{\&}_{\mathsf{A}}(f'^{1}_{ij}) + L^{\&}_{\mathsf{A}}(f'^{0}_{ij}) + L^{\&}_{\mathsf{A}}(f'_{ij}) \leq 2^{n-1} - 2. \tag{3.7}$$

По предложению 9

$$L^{\&}_{\mathsf{A}}(f^{11}_{ij}) + L^{\&}_{\mathsf{A}}(f^{10}_{ij}) + L^{\&}_{\mathsf{A}}(f^{1}_{ij}) \leq 2^{n-1}; \tag{3.8}$$

$$L^{\&}_{\mathsf{A}}(f^{01}_{ij}) + L^{\&}_{\mathsf{A}}(f^{00}_{ij}) + L^{\&}_{\mathsf{A}}(f^{0}_{ij}) \leq 2^{n-1}. \tag{3.9}$$

$$L^{\&}_{\mathsf{A}}(f^{1}_{ij}) + L^{\&}_{\mathsf{A}}(f^{0}_{ij}) + L^{\&}_{\mathsf{A}}(f'_{ij}) \leq 2^{n-1}. \tag{3.10}$$

По лемме 6.1 существуют пучки $\mathsf{B}, \mathsf{C} \in K(\mathsf{d} \ldots \mathsf{d})$ размерности $n-1$, такие что

$$L^{\&}_{\mathsf{A}}(f^{11}_{ij}) + L^{\&}_{\mathsf{A}}(f'^{1}_{ij}) = L^{\&}_{\mathsf{B}}(f^{1}_{k}); \qquad L^{\&}_{\mathsf{A}}(f^{01}_{ij}) + L^{\&}_{\mathsf{A}}(f'^{1}_{ij}) = L^{\&}_{\mathsf{C}}(f^{1}_{k});$$

$$L^{\&}_{\mathsf{A}}(f^{10}_{ij}) + L^{\&}_{\mathsf{A}}(f'^{0}_{ij}) = L^{\&}_{\mathsf{B}}(f^{0}_{k}); \qquad L^{\&}_{\mathsf{A}}(f^{00}_{ij}) + L^{\&}_{\mathsf{A}}(f'^{0}_{ij}) = L^{\&}_{\mathsf{C}}(f^{0}_{k});$$

$$L^{\&}_{\mathsf{A}}(f^{1}_{ij}) + L^{\&}_{\mathsf{A}}(f'_{ij}) = L^{\&}_{\mathsf{B}}(f'_{k}); \qquad L^{\&}_{\mathsf{A}}(f^{0}_{ij}) + L^{\&}_{\mathsf{A}}(f'_{ij}) = L^{\&}_{\mathsf{C}}(f'_{k});$$

здесь и далее

$$k = \begin{cases} j, & \text{если } j < i; \\ j+1, & \text{если } j \geq i. \end{cases}$$

Тогда, используя (3.8) и (3.9), получим:

$$L^{\&}_{\mathsf{B}}(f^{1}_{k}) + L^{\&}_{\mathsf{B}}(f^{0}_{k}) + L^{\&}_{\mathsf{B}}(f'_{k}) \leq 2^{n} - 2;$$

$$L^{\&}_{\mathsf{C}}(f^{1}_{k}) + L^{\&}_{\mathsf{C}}(f^{0}_{k}) + L^{\&}_{\mathsf{C}}(f'_{k}) \leq 2^{n} - 2.$$

Из (3.6) и (3.7) следует, что

$$\left(L^{\&}_{\mathsf{A}}(f'^{1}_{ij}) + L^{\&}_{\mathsf{A}}(f'_{ij})\right) + \left(L^{\&}_{\mathsf{A}}(f'^{0}_{ij}) + L^{\&}_{\mathsf{A}}(f'_{ij})\right) <$$

$$< 2^{n-1} + \frac{1}{3} \cdot 2^{n-1} + \frac{1}{2} < 2 \cdot \left(\frac{1}{3} \cdot 2^{n} + \frac{1}{2}\right).$$

Поэтому выполняется хотя бы одно из неравенств:

$$L^{\&}_{\mathsf{B}}(f'_{k}) < \frac{1}{3} \cdot 2^{n} + \frac{1}{2}, \qquad L^{\&}_{\mathsf{C}}(f'_{k}) < \frac{1}{3} \cdot 2^{n} + \frac{1}{2}.$$

Таким образом, утверждение леммы в этом случае справедливо.

2. Для любого $i \in \{1, \ldots, n\}$ выполняется: $f'_i \in \overline{M}^{\Diamond}_{n-1} \cup \{(17)_{16}\}^{\Diamond}$. Легко проверить, что производные функций из $\{(17)_{16}\}^{\Diamond}$ по любому аргумету принадлежат множеству $M^{\Diamond}_2$. Поскольку $f'_i \notin M^{\Diamond}_{n-1}$, по лемме 6.2 найдется пучок $\mathsf{A} \in K(\mathsf{d} \ldots \mathsf{d})$ размерности $n-2$ и аргумент $j \in \{1, \ldots, n-1\}$, такие что

$$L^{\&}_{\mathsf{A}}(f'^{\,1}_{i\,j}) + L^{\&}_{\mathsf{A}}(f'^{\,0}_{i\,j}) + L^{\&}_{\mathsf{A}}(f'^{\,\prime}_{i\,j}) \leq 2^{n-1} - 2.$$

По предложению 9 справедливы неравенства (3.8), (3.9), (3.10). Строя пучки B и C, как в случае 1, получим:

$$L^{\&}_{\mathsf{B}}(f^1_k) + L^{\&}_{\mathsf{B}}(f^0_k) + L^{\&}_{\mathsf{B}}(f'_k) \leq 2^n - 2;$$
$$L^{\&}_{\mathsf{C}}(f^1_k) + L^{\&}_{\mathsf{C}}(f^0_k) + L^{\&}_{\mathsf{C}}(f'_k) \leq 2^n - 2;$$

где

$$k = \begin{cases} j, & \text{если } j < i; \\ j+1, & \text{если } j \geq i. \end{cases}$$

По предложениям 8, следствию к предложению 5 и неравенствам (3.2)

$$L^{\&}_{\mathsf{A}}(f'^{\,\prime}_{i\,j}) \leq \left\lfloor \frac{2}{3} \cdot 2^{n-2} \right\rfloor + 1.$$

Используя неравенство (3.10), получим:

$$\left(L^{\&}_{\mathsf{A}}(f'^{\,1}_{i\,j}) + L^{\&}_{\mathsf{A}}(f'^{\,\prime}_{i\,j})\right) + \left(L^{\&}_{\mathsf{A}}(f'^{\,0}_{i\,j}) + L^{\&}_{\mathsf{A}}(f'^{\,\prime}_{i\,j})\right) \leq$$
$$\leq 2^{n-1} + \left\lfloor \frac{2}{3} \cdot 2^{n-2} \right\rfloor + 1 < 2 \cdot \left(\frac{1}{3} \cdot 2^n + \frac{1}{2} \right).$$

Как и в случае 1, выполняется хотя бы одно из неравенств:

$$L^{\&}_{\mathsf{B}}(f'_k) < \frac{1}{3} \cdot 2^n + \frac{1}{2}, \qquad L^{\&}_{\mathsf{C}}(f'_k) < \frac{1}{3} \cdot 2^n + \frac{1}{2}.$$

Лемма доказана. ◁

Лемма 6.8 *Пусть $n \geq 1$, $f \in F_n \backslash \overline{M}^{\Diamond}_n$. Тогда*

$$L^{\&}_{K(\mathsf{d}\ldots\mathsf{d})}(f) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

▷ Доказательство. При $n \in \{1, 2, 3\}$ это утверждение доказано в лемме 6.3.

Пусть $n \geq 4$. Тогда по лемме 6.6 существует аргумент $i \in \{1, \ldots, n\}$, такой что $f_i' \notin M_{n-1}^{\Diamond}$. По лемме 6.7 существует пучок $\mathsf{A} \in K(\mathsf{d} \ldots \mathsf{d})$ размерности $n-1$ и аргумент $j \in \{1, \ldots, n\}$, такие что выполняются неравенства:

$$L_{\mathsf{A}}^{\&}(f_j^1) + L_{\mathsf{A}}^{\&}(f_j^0) + L_{\mathsf{A}}^{\&}(f_j') \leq 2^n - 2; \qquad L_{\mathsf{A}}^{\&}(f_j') < \frac{1}{3} \cdot 2^n + \frac{1}{2}.$$

Сложим эти неравенства и получим:

$$\begin{gathered}\left(L_{\mathsf{A}}^{\&}(f_j^1) + L_{\mathsf{A}}^{\&}(f_j')\right) + \left(L_{\mathsf{A}}^{\&}(f_j^0) + L_{\mathsf{A}}^{\&}(f_j')\right) < \\ < 2^n - 2 + \frac{1}{3} \cdot 2^n + \frac{1}{2} = 2 \cdot \left(\frac{2}{3} \cdot 2^n - \frac{3}{4}\right) < 2 \cdot \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.\end{gathered}$$

Следовательно, выполняется хотя бы одно из неравенств:

$$L_{\mathsf{A}}^{\&}(f_j^1) + L_{\mathsf{A}}^{\&}(f_j') < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor; \qquad L_{\mathsf{A}}^{\&}(f_j^0) + L_{\mathsf{A}}^{\&}(f_j') < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor. \qquad (3.11)$$

По лемме 6.1 существует пучок $\mathsf{B} \in K(\mathsf{d} \ldots \mathsf{d})$ размерности n, такой что

$$L_{\mathsf{B}}^{\&}(f) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

◁

Лемма 6.9 *Пусть n нечетное, $f \in F_n \backslash M^{\Diamond}$. Тогда*

$$L_{K(\mathsf{d} \ldots \mathsf{d})}^{\&}(f) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

▷ Доказательство. В лемме 6.8 это утверждение доказывается для случая $f \notin \overline{M}_n^{\Diamond}$. Поэтому остается рассмотреть случай $f \in \overline{M}_n^{\Diamond}$.

По лемме 6.2 существует пучок A размерности $n-1$ и аргумент $i \in \{1, \ldots, n\}$, такие что

$$L_{\mathsf{A}}^{\&}(f_i^1) + L_{\mathsf{A}}^{\&}(f_i^0) + L_{\mathsf{A}}^{\&}(f_i') \leq 2^n - 2.$$

Из того что $f \in \overline{M}_n^{\Diamond}$, следует: $f_i' \in M_{n-1}^{\Diamond}$. По предложениям 8, неравенствам (3.2) и учитывая, что f_i' однотипна симметрической функции,

выполняется неравенство:

$$L^{\&}_{\mathsf{A}}(f'_i) \le \left\lfloor \frac{2}{3} \cdot 2^{n-1} \right\rfloor + 1 = \frac{2}{3} \cdot 2^{n-1} + \frac{1}{3}.$$

Сложим два предыдущих неравенства и получим:

$$\begin{gathered}\left(L^{\&}_{\mathsf{A}}(f^1_i) + L^{\&}_{\mathsf{A}}(f'_i)\right) + \left(L^{\&}_{\mathsf{A}}(f^0_i) + L^{\&}_{\mathsf{A}}(f'_i)\right) \le \\ \le 2^n - 2 + \frac{2}{3} \cdot 2^{n-1} + \frac{1}{3} < 2 \cdot \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.\end{gathered}$$

Поэтому выполняется хотя бы одно из неравенств:

$$L^{\&}_{\mathsf{A}}(f^1_i) + L^{\&}_{\mathsf{A}}(f'_i) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor; \qquad L^{\&}_{\mathsf{A}}(f^0_i) + L^{\&}_{\mathsf{A}}(f'_i) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

Тогда, по лемме 6.1, найдется пучок $\mathsf{B} \in K(\mathtt{d} \ldots \mathtt{d})$, такой что

$$L^{\&}_{\mathsf{B}}(f) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

$\lhd$

Лемма 6.10 *Пусть n четное. Тогда*

$$L^{\&}_{K(\mathtt{d}\ldots\mathtt{d})}(\bar{p}_n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor; \qquad L^{\&}_{K(\mathtt{d}\ldots\mathtt{d})}(\bar{q}_n) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

$\rhd$ Доказательство. Введем в рассмотрение множество упорядоченных наборов целых чисел V_n Множеству V_n принадлежат те и только те наборы вида $(v_1, v_2, v_3, v_4, v_5, v_6)$, для которых найдется пучок $\mathsf{A} \in K(\mathtt{d} \ldots \mathtt{d})$ размерности n, такой что

$$L^{\&}_{\mathsf{A}}(p_n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor + v_1, \quad L^{\&}_{\mathsf{A}}(q_n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor + v_2, \quad L^{\&}_{\mathsf{A}}(r_n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor + v_3,$$
$$L^{\&}_{\mathsf{A}}(\bar{p}_n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor + v_4, \quad L^{\&}_{\mathsf{A}}(\bar{q}_n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor + v_5, \quad L^{\&}_{\mathsf{A}}(\bar{r}_n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor + v_6.$$

Сейчас мы докажем, что если n — четное, то множество V_n содержит только наборы

$$(0, 1, 1, 1, 0, 0), \quad (1, 0, 1, 0, -1, 2), \quad (1, 1, 0, 0, 2, -1).$$

Доказательство проведем индукцией по четным n.

Базис индукции. При $n = 0$ существует только один пучок: $\{\emptyset\}$. Тогда $V_0 = \{(0, 1, 1, 1, 0, 0)\}$.

Шаг индукции будем доказывать для $n + 2$, где $n \geq 0$ — четное число. Пусть $\mathsf{A} \in K(\mathsf{d} \dots \mathsf{d})$ — пучок размерности $n + 2$. По определению класса $K(\mathsf{d} \dots \mathsf{d})$ существует оператор $\mathfrak{u}$ длины $n + 2$, такой что $\mathsf{A} = D(\mathsf{d} \dots \mathsf{d}, \mathfrak{u})$. Пусть $\left(\mathfrak{a}^{\tilde{0}}, \dots, \mathfrak{a}^{\tilde{1}}\right)$ — естественная нумерация пучка $D(\mathsf{d} \dots \mathsf{d}, \mathfrak{u})$. Положим $\mathsf{C} = D(\mathsf{d} \dots \mathsf{d}, \mathfrak{u}_1 \dots \mathfrak{u}_n)$, и пусть $\left(\mathfrak{c}^{\tilde{0}}, \dots, \mathfrak{c}^{\tilde{1}}\right)$ — его естественная нумерация. Далее определим пучок $\mathsf{B} = D(\mathsf{dd}, \mathfrak{v})$ размерности 2, где $\mathfrak{v} = \mathfrak{u}_{n+1}\mathfrak{u}_{n+2}$, и пусть $\left(\mathfrak{b}^{\tilde{0}}, \dots, \mathfrak{b}^{\tilde{1}}\right)$ — естественная нумерация пучка B. Легко видеть, что

$$\mathfrak{a}^{\tilde{\sigma},\tilde{\tau}} = \mathfrak{c}_1^{\tilde{\sigma}} \dots \mathfrak{c}_n^{\tilde{\sigma}} \mathfrak{b}_1^{\tilde{\tau}} \mathfrak{b}_2^{\tilde{\tau}}, \qquad \tilde{\sigma} \in E^n, \quad \tilde{\tau} \in E^2.$$

Таким образом, $\mathsf{A} = W(\mathsf{C} \mid \mathsf{B}, \dots, \mathsf{B})$. Для оператора $\mathfrak{v}$ возможны 4 варианта: $\mathfrak{v} = \mathfrak{e}\mathfrak{e}$, $\mathfrak{v} = \mathfrak{e}\mathfrak{p}$, $\mathfrak{v} = \mathfrak{p}\mathfrak{e}$, $\mathfrak{v} = \mathfrak{p}\mathfrak{p}$.

Рассмотрим случай $\mathfrak{v} = \mathfrak{e}\mathfrak{e}$. Справедливы следующие разложения:

$$\begin{aligned}
p_{n+2}(x_1, \dots, x_{n+2}) &= x_{n+1} \cdot x_{n+2} \cdot p_n(\tilde{x}) \oplus x_{n+2} \cdot r_n(\tilde{x}) \oplus x_{n+1} \cdot r_n(\tilde{x}) \oplus q_n(\tilde{x});\\
q_{n+2}(x_1, \dots, x_{n+2}) &= x_{n+1} \cdot x_{n+2} \cdot q_n(\tilde{x}) \oplus x_{n+2} \cdot p_n(\tilde{x}) \oplus x_{n+1} \cdot p_n(\tilde{x}) \oplus r_n(\tilde{x});\\
r_{n+2}(x_1, \dots, x_{n+2}) &= x_{n+1} \cdot x_{n+2} \cdot r_n(\tilde{x}) \oplus x_{n+2} \cdot q_n(\tilde{x}) \oplus x_{n+1} \cdot q_n(\tilde{x}) \oplus p_n(\tilde{x});\\
\bar{p}_{n+2}(x_1, \dots, x_{n+2}) &= x_{n+1} \cdot x_{n+2} \cdot p_n(\tilde{x}) \oplus x_{n+2} \cdot r_n(\tilde{x}) \oplus x_{n+1} \cdot r_n(\tilde{x}) \oplus \bar{q}_n(\tilde{x});\\
\bar{q}_{n+2}(x_1, \dots, x_{n+2}) &= x_{n+1} \cdot x_{n+2} \cdot q_n(\tilde{x}) \oplus x_{n+2} \cdot p_n(\tilde{x}) \oplus x_{n+1} \cdot p_n(\tilde{x}) \oplus \bar{r}_n(\tilde{x});\\
\bar{r}_{n+2}(x_1, \dots, x_{n+2}) &= x_{n+1} \cdot x_{n+2} \cdot r_n(\tilde{x}) \oplus x_{n+2} \cdot q_n(\tilde{x}) \oplus x_{n+1} \cdot q_n(\tilde{x}) \oplus \bar{p}_n(\tilde{x}).
\end{aligned}$$

Докажем только первое из них, остальные доказываются аналогично:

$$\begin{aligned}
&p_{n+2}(x_1, \dots, x_n, x_{n+1}, x_{n+2}) =\\
&= x_{n+2} \cdot p_{n+1}(x_1, \dots, x_n, x_{n+1}) \oplus r_{n+1}(x_1, \dots, x_n, x_{n+1}) =\\
&= x_{n+1} \cdot x_{n+2} \cdot p_n(\tilde{x}) \oplus x_{n+2} \cdot r_n(\tilde{x}) \oplus x_{n+1} \cdot r_n(\tilde{x}) \oplus q_n(\tilde{x}).
\end{aligned}$$

Заметим, что

$$4 \cdot \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor = \left\lfloor \frac{2}{3} \cdot 2^{n+2} \right\rfloor - 2.$$

Используя приведенные выше разложения, легко видеть, что если $v \in V_n$, то $u \in V_{n+2}$, где

$$v = (v_1, v_2, v_3, v_4, v_5, v_6); \quad u = (u_1, u_2, u_3, u_4, u_5, u_6),$$
$$u_1 = v_1 + 2v_3 + v_2 - 2, \quad u_2 = v_2 + 2v_1 + v_3 - 2, \quad u_3 = v_3 + 2v_2 + v_1 - 2,$$
$$u_4 = v_1 + 2v_3 + v_5 - 2, \quad u_5 = v_2 + 2v_1 + v_6 - 2, \quad u_6 = v_3 + 2v_2 + v_4 - 2.$$

Приведем значения u соответствующие всевозможным значениям v:

если $v = (0, 1, 1, 1, 0, 0)$, то $u = (1, 0, 1, 0, -1, 2)$;
если $v = (1, 0, 1, 0, -1, 2)$, то $u = (1, 1, 0, 0, 2, -1)$;
если $v = (1, 1, 0, 0, 2, -1)$, то $u = (0, 1, 1, 1, 0, 0)$.

Рассматривая случаи $\boldsymbol{\nu} = \mathfrak{ep}$ и $\boldsymbol{\nu} = \mathfrak{pe}$, получим следующие формулы для u:

$$u_1 = 2v_1 + v_3 + v_2 - 2, \quad u_2 = 2v_2 + v_1 + v_3 - 2, \quad u_3 = 2v_3 + v_2 + v_1 - 2,$$
$$u_4 = v_1+v_2+v_3+v_4-2, \quad u_5 = v_2+v_3+v_1+v_5-2, \quad u_6 = v_3+v_1+v_2+v_6-2.$$

В случае $\boldsymbol{\nu} = \mathfrak{pp}$, имеем:

$$u_1 = v_1 + 2v_2 + v_3 - 2, \quad u_2 = v_2 + 2v_3 + v_1 - 2, \quad u_3 = v_3 + 2v_1 + v_2 - 2,$$
$$u_4 = v_1 + 2v_2 + v_6 - 2, \quad u_5 = v_2 + 2v_3 + v_4 - 2, \quad u_6 = v_3 + 2v_1 + v_5 - 2.$$

Во всех случаях мы не выходим за пределы множества

$$\{(0, 1, 1, 1, 0, 0), (1, 0, 1, 0, -1, 2), (1, 1, 0, 0, 2, -1)\}.$$

Заметим также, что при $n \geq 2$ в V_n встречается каждый из этих наборов.

Вид наборов из множества V_n означает, что существуют операторные пучки $\mathsf{A}_1, \mathsf{A}_2 \in K(\mathtt{d} \ldots \mathtt{d})$, такие что

$$L^{\&}_{\mathsf{A}_1}(\bar{q}_n) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor, \qquad L^{\&}_{\mathsf{A}_2}(\bar{r}_n) < \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor,$$

и для любого пучка $\mathsf{A} \in K(\mathtt{d} \ldots \mathtt{d})$

$$L^{\&}_{\mathsf{A}}(\bar{p}_n) \geq \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

$\lhd$

Подытожим полученные результаты. По лемме 6.3 теорема 6 справедлива при $n \in \{1, 2, 3\}$. Из предложения 8, леммы 6.10 и неравенств 3.2 следует, что $L^{\&}_{K(\mathtt{d}\ldots\mathtt{d})} = L_{K(\mathtt{d}\ldots\mathtt{d})}(n)$, если $f \in \widetilde{M}^{\Diamond}_n$ при четном n и $f \in M^{\Diamond}_n$ при нечетном n. По леммам 6.8, 6.9, 6.10 $L^{\&}_{K(\mathtt{d}\ldots\mathtt{d})} < L_{K(\mathtt{d}\ldots\mathtt{d})}(n)$, если $f \notin \widetilde{M}^{\Diamond}_n$ при четном n и $f \notin M^{\Diamond}_n$ при нечетном n.

Таким образом, теорема доказана. ◀

Теорема 7 *Если $f \in F_n$, $n \geq 1$, то $L^{\&}_K(f) = L_K(n)$ тогда и только тогда, когда $f \in M^{\Diamond}_n$.*

▶ Напомним, что

$$L_K(n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

В [3] показано, что для любой функции $f \in M_n$ выполняется:

$$L^{\&}_K(f) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor.$$

Используя это неравенство и предложение 8, получаем, что для любой функции $f \in M^{\Diamond}_n$

$$L^{\&}_K(f) = L_K(n).$$

Пусть теперь $f \notin M^{\Diamond}_n$. Поскольку $K(\mathtt{d}\ldots\mathtt{d}) \subset K$, то по лемме 6.2 существует аргумент $i \in \{1, \ldots, n\}$ и пучок $\mathsf{A} \in K$ размерности $n-1$, такие что

$$L^{\&}_{\mathsf{A}}(f^1_i) + L^{\&}_{\mathsf{A}}(f^0_i) + L^{\&}_{\mathsf{A}}(f'_i) \leq 2^n - 2.$$

Умножим это неравенство на 2 и получим:

$$\begin{gathered}\left(L^{\&}_{\mathsf{A}}(f^1_i) + L^{\&}_{\mathsf{A}}(f^0_i)\right) + \left(L^{\&}_{\mathsf{A}}(f^1_i) + L^{\&}_{\mathsf{A}}(f'_i)\right) + \left(L^{\&}_{\mathsf{A}}(f^0_i) + L^{\&}_{\mathsf{A}}(f'_i)\right) \leq \\ \leq 2 \cdot (2^n - 2) = 3 \cdot \left(\frac{2}{3} \cdot 2^n - \frac{4}{3}\right) < 3 \cdot L_K(n).\end{gathered}$$

Поэтому выполняется хотя бы одно из неравенств:

$$\begin{gathered}L^{\&}_{\mathsf{A}}(f^1_{x_i}) + L^{\&}_{\mathsf{A}}(f^0_{x_i}) < L_K(n); \\ L^{\&}_{\mathsf{A}}(f^1_{x_i}) + L^{\&}_{\mathsf{A}}(f'_{x_i}) < L_K(n); \\ L^{\&}_{\mathsf{A}}(f^0_{x_i}) + L^{\&}_{\mathsf{A}}(f'_{x_i}) < L_K(n).\end{gathered}$$

Если выполняется второе или третье неравенство, то по лемме 6.1 существует пучок $\mathsf{B} \in K$ размерности n, такой что

$$L^{\&}_{\mathsf{B}}(f) < L_K(n).$$

Пусть теперь выполняется неравенство $L^{\&}_{\mathsf{A}}(f^1_{x_i}) + L^{\&}_{\mathsf{A}}(f^0_{x_i}) < L_K(n)$. Поскольку пучок A принадлежит классу K, существуют операторы $\mathfrak{u}, \mathfrak{v}$, такие что $\mathsf{A} = D(\mathfrak{u}, \mathfrak{v})$. Положим

$$\mathsf{B} = D(\mathfrak{u}_1 \dots \mathfrak{u}_{i-1} \mathfrak{e} \mathfrak{u}_i \dots \mathfrak{u}_{n-1}, \mathfrak{v}_1 \dots \mathfrak{v}_{i-1} \mathfrak{p} \mathfrak{v}_i \dots \mathfrak{v}_{n-1}).$$

Пусть $\left(\mathfrak{a}^{\tilde{0}}, \dots, \mathfrak{a}^{\tilde{1}}\right)$ и $\left(\mathfrak{b}^{\tilde{0}}, \dots, \mathfrak{b}^{\tilde{1}}\right)$ — естественные нумерации пучков A и B, соответственно. Тогда справедливы следующие равенства:

$$\begin{aligned} f(\tilde{x}) &= x_i \cdot f^1_{x_i}(\tilde{x}) \oplus \bar{x}_i \cdot f^0_{x_i}(\tilde{x}) = \\ &= x_i \cdot \bigoplus_{\tilde{\sigma} \in E^{n-1}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_{i-1} \cdot x_{i+1} \cdot \ldots \cdot x_n) \oplus \\ &\oplus \bar{x}_i \cdot \bigoplus_{\tilde{\sigma} \in E^{n-1}} \beta_{\tilde{\sigma}} \cdot \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_{i-1} \cdot x_{i+1} \cdot \ldots \cdot x_n) = \\ &= \bigoplus_{\substack{\tilde{\sigma} \in E^n \\ \sigma_i = 1}} \alpha_{\tilde{\sigma}} \cdot \mathfrak{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \oplus \bigoplus_{\substack{\tilde{\sigma} \in E^n \\ \sigma_i = 0}} \beta_{\tilde{\sigma}} \cdot \mathfrak{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \end{aligned}$$

По определению сложности функции относительно пучка, получаем:

$$L^{\&}_{\mathsf{B}}(f) = L^{\&}_{\mathsf{A}}(f^1_i) + L^{\&}_{\mathsf{A}}(f^0_i) < L_K(n).$$

Таким образом, теорема доказана. ◀

Теорема 8 *Если $f \in F_n$, $n \geq 1$, то $L^{\&}_{FK}(f) = L_{FK}(n)$ тогда и только тогда, когда $f \in M^{\Diamond}_n$.*

► Доказательство. Напомним, что по теореме 4

$$L_{FK}(n) = \frac{1}{2} \cdot 2^n.$$

Из леммы 4.3 и предложения 8 следует, что для функций $f \in M^{\Diamond}_n$ выполняется:

$$L^{\&}_{FK}(f) = L_{FK}(n).$$

Для функций $f \in F_n \backslash M_n^{\Diamond}$ индукцией по n покажем, что

$$L_{FK}^{\&}(f) < \frac{1}{2} \cdot 2^n.$$

Базис индукции при $n = 1$. Поскольку $F_1 \backslash M_1^{\Diamond} = \{(00)_2\}$, и функция $f = (00)_2$ имеет нулевую сложность относительно любого пучка, то $L_{FK}(f) < \frac{1}{2} \cdot 2^1$.

Шаг индукции при $n \geq 2$. Пусть $f \in F_n \backslash M_n^{\Diamond}$. По предложению 7 хотя бы одна из функций f_1^1, f_1^0, f_1' не принадлежит множеству $M_{n-1}^{\Diamond}$. Пусть для определенности это функция f_1^1. Тогда по предположению индукции и теореме 4 существуют пучки A и B размерности $n-1$ из класса FK, такие что

$$L_{\mathsf{A}}^{\&}(f_1^1) < \frac{1}{2} \cdot 2^{n-1}; \qquad L_{\mathsf{B}}^{\&}(f_1^0) \leq \frac{1}{2} \cdot 2^{n-1}. \tag{3.12}$$

По определению класса FK из того что пучок $\{\mathsf{e}, \mathsf{p}\}$ лежит в классе FK следует, что пучок $\mathsf{C} = W(\{\mathsf{e}, \mathsf{p}\} \mid \mathsf{A}, \mathsf{B})$ тоже принадлежит FK. Пусть $\left(\mathsf{a}^{\tilde{0}}, \ldots, \mathsf{a}^{\tilde{1}}\right)$ и $\left(\mathsf{b}^{\tilde{0}}, \ldots, \mathsf{b}^{\tilde{1}}\right)$ — нумерации пучков A и B соответственно, $\left(\mathsf{c}^{\tilde{0}}, \ldots, \mathsf{c}^{\tilde{1}}\right)$ — нумерация пучка C, построенная по определению слияния из нумераций $\left(\mathsf{a}^{\tilde{0}}, \ldots, \mathsf{a}^{\tilde{1}}\right)$, $\left(\mathsf{b}^{\tilde{0}}, \ldots, \mathsf{b}^{\tilde{1}}\right)$ и (e, p). Используя разложение Шеннона, получим следующую цепочку равенств:

$$\begin{gathered} f(\tilde{x}) = x_1 \cdot f_{x_1}^1(\tilde{x}) \oplus \bar{x}_1 \cdot f_{x_1}^0(\tilde{x}) = \\ = x_1 \cdot \bigoplus_{\tilde{\sigma} \in E^{n-1}} \alpha_{\tilde{\sigma}} \cdot \mathsf{a}^{\tilde{\sigma}}(x_2 \cdot \ldots \cdot x_n) \oplus \bar{x}_1 \cdot \bigoplus_{\tilde{\sigma} \in E^{n-1}} \beta_{\tilde{\sigma}} \cdot \mathsf{b}^{\tilde{\sigma}}(x_2 \cdot \ldots \cdot x_n) = \\ = \bigoplus_{\tilde{\sigma} \in E^{n-1}} \alpha_{\tilde{\sigma}} \cdot \mathsf{c}^{0,\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \oplus \bigoplus_{\tilde{\sigma} \in E^{n-1}} \beta_{\tilde{\sigma}} \cdot \mathsf{c}^{1,\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \end{gathered}$$

По определению сложности функции относительно пучка и неравенствам (3.12) получаем:

$$L_{\mathsf{C}}^{\&}(f) = L_{\mathsf{A}}^{\&}(f_1^1) + L_{\mathsf{A}}^{\&}(f_1^0) < \frac{1}{2} \cdot 2^{n-1} + \frac{1}{2} \cdot 2^{n-1} = \frac{1}{2} \cdot 2^n.$$

Таким образом, теорема доказана. ◀

Теорема 9 *Если* $f \in F_n$, $n \geq 1$, *то* $L^{\&}_{E(\mathtt{d}\ldots\mathtt{d})}(f) = L_{E(\mathtt{d}\ldots\mathtt{d})}(n)$ *тогда и только тогда, когда*

$$\frac{1}{2}\cdot 2^n \leq \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \leq \frac{1}{2}\cdot 2^n + 1.$$

► Доказательство. По теореме VIII

$$L_{E(\mathtt{d}\ldots\mathtt{d})}(n) = \frac{1}{2}\cdot 2^n. \tag{3.13}$$

Пучок размерности n из $E(\mathtt{d}\ldots\mathtt{d})$ по определению строится из некоторого двупорожденного пучка $\mathsf{A} = D(\mathfrak{a}^{\tilde{0}}, \mathfrak{a}^{\tilde{1}})$, в котором операторы $\mathfrak{a}^{\tilde{0}}$ и $\mathfrak{a}^{\tilde{1}}$ состоят только из символов $\mathtt{e}$ и $\mathtt{p}$. Тогда по определению двупорожденного пучка все операторы в пучке A состоят только из символов $\mathtt{e}$ и $\mathtt{p}$. Всего существует 2^n операторов такого вида, и все они входят в пучок A. Таким образом все пучки размерности n из $E(\mathtt{d}\ldots\mathtt{d})$ строятся из одного и того же пучка $\mathsf{A} = D(\mathtt{p}\ldots\mathtt{p}, \mathtt{e}\ldots\mathtt{e})$.

Пусть f — функция размерности n, $\mathsf{A} = D(\mathtt{p}\ldots\mathtt{p}, \mathtt{e}\ldots\mathtt{e})$ — пучок той же размерности, $\left(\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}}\right)$ — его естественная нумерация, в которой компоненты операторов $\mathfrak{a}^{\tilde{\sigma}}$ задаются следующим образом:

$$\mathfrak{a}_i^{\tilde{\sigma}} = \begin{cases} \mathtt{p}, & \text{если } \sigma_i = 0, \\ \mathtt{e}, & \text{если } \sigma_i = 1, \end{cases} \qquad \tilde{\sigma} \in E^n.$$

Рассмотрим совершенную полиномиальную нормальную форму:

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \cdot x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} = \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \cdot \mathfrak{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n).$$

Далее рассмотрим три случая:

$$\sum_{\tilde{\sigma}} f(\tilde{\sigma}) < \frac{1}{2}\cdot 2^n; \quad \sum_{\tilde{\sigma}} f(\tilde{\sigma}) > \frac{1}{2}\cdot 2^n + 1; \quad \frac{1}{2}\cdot 2^n \leq \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \leq \frac{1}{2}\cdot 2^n + 1.$$

Пусть

$$\sum_{\tilde{\sigma}} f(\tilde{\sigma}) < \frac{1}{2}\cdot 2^n.$$

Очевидно, найдется набор $\tilde{\tau}$, такой что $f(\tilde{\tau}) = 0$. Построим расширенный пучок B по его нумерации $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$, операторы в которой определя-

ются следующим образом:

$$\mathsf{b}^{\tilde{\sigma}} = \begin{cases} \mathsf{a}^{\tilde{\sigma}}, & \text{если } \tilde{\sigma} \neq \tilde{\tau}; \\ \mathsf{d} \dots \mathsf{d}, & \text{если } \tilde{\sigma} = \tilde{\tau}; \end{cases} \qquad \tilde{\sigma} \in E^n.$$

Тогда получим полиномиальную форму относительно пучка B:

$$f(\tilde{x}) = \bigoplus_{\tilde{\sigma}} f(\tilde{\sigma}) \cdot \mathsf{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n).$$

По определению сложности функции относительно пучка, имеем:

$$L^{\&}_{\mathrm{B}}(f) = \sum_{\tilde{\sigma}} f(\tilde{\sigma}) < \frac{1}{2} \cdot 2^n.$$

Пусть

$$\sum_{\tilde{\sigma}} f(\tilde{\sigma}) > \frac{1}{2} \cdot 2^n + 1.$$

Очевидно, что существует набор $\tilde{\tau}$, такой что $f(\tilde{\tau}) = 1$. Построим расширенный пучок B, по его нумерации $\left(\mathsf{b}^{\tilde{0}}, \ldots, \mathsf{b}^{\tilde{1}}\right)$, операторы в которой определяются следующим образом:

$$\mathsf{b}^{\tilde{\sigma}} = \begin{cases} \mathsf{a}^{\tilde{\sigma}}, & \text{если } \tilde{\sigma} \neq \tilde{\tau}; \\ \mathsf{d} \dots \mathsf{d}, & \text{если } \tilde{\sigma} = \tilde{\tau}; \end{cases} \qquad \tilde{\sigma} \in E^n.$$

Учитывая, что

$$\bigoplus_{\tilde{\sigma}} \mathsf{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) = \bigoplus_{\tilde{\sigma}} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} = 1 \quad \text{и}$$
$$\mathsf{b}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) = \mathsf{d} \dots \mathsf{d}(x_1 \cdot \ldots \cdot x_n) = 1,$$

получим:

$$f(\tilde{x}) = \bigoplus_{\tilde{\sigma}} f(\tilde{\sigma}) \cdot \mathsf{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \oplus \bigoplus_{\tilde{\sigma}} \mathsf{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \oplus \mathsf{b}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) =$$
$$= \bigoplus_{\tilde{\sigma} \neq \tilde{\tau}} \bar{f}(\tilde{\sigma}) \cdot \mathsf{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \oplus \bar{f}(\tilde{\tau}) \cdot \mathsf{a}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) \oplus \mathsf{b}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n).$$

Так как $\bar{f}(\tilde{\tau}) = 0$, то

$$f(\tilde{x}) = \bigoplus_{\tilde{\sigma} \neq \tilde{\tau}} \bar{f}(\tilde{\sigma}) \cdot \mathsf{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \oplus \mathsf{b}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n).$$

Получили полиномиальную форму для функции f относительно пучка B. Тогда

$$L^{\&}_{\mathsf{B}}(f) = \sum_{\tilde{\sigma}} \bar{f}(\tilde{\sigma}) + 1 = 2^n - \sum_{\tilde{\sigma}} f(\tilde{\sigma}) + 1 < 2^n - \left(\frac{1}{2}\cdot 2^n + 1\right) + 1 = \frac{1}{2}\cdot 2^n.$$

Наконец, рассмотрим случай

$$\frac{1}{2}\cdot 2^n \le \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \le \frac{1}{2}\cdot 2^n.$$

Пусть $\mathsf{B} \in E(\mathsf{d}\ldots\mathsf{d})$, и $\left(\mathsf{b}^{\tilde{0}}, \ldots, \mathsf{b}^{\tilde{1}}\right)$ — его естественная нумерация, построенная на основе естественной нумерации двупорожденного пучка $D(\mathsf{e}\ldots\mathsf{e}, \mathsf{p}\ldots\mathsf{p})$. По определению, существует набор $\tilde{\tau}$, такой что

$$\mathsf{b}^{\tilde{\sigma}} = \begin{cases} \mathsf{a}^{\tilde{\sigma}}, & \text{если } \tilde{\sigma} \neq \tilde{\tau}; \\ \mathsf{d}\ldots\mathsf{d}, & \text{если } \tilde{\sigma} = \tilde{\tau}; \end{cases} \qquad \tilde{\sigma} \in E^n.$$

Возможны два случая: $f(\tilde{\tau}) = 0$ и $f(\tilde{\tau}) = 1$. В первом случае

$$f(\tilde{x}) = \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \cdot \mathsf{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n);$$

$$L^{\&}_{\mathsf{B}}(f) = \sum_{\tilde{\sigma}} f(\tilde{\sigma}) \ge \frac{1}{2}\cdot 2^n.$$

Во втором случае

$$f(\tilde{x}) = \sum_{\tilde{\sigma}\neq\tilde{\tau}} \bar{f}(\tilde{\sigma}) \cdot \mathsf{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \oplus \mathsf{b}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n);$$

$$L^{\&}_{\mathsf{B}}(f) = 2^n - \sum_{\tilde{\sigma}} f(\tilde{\sigma}) + 1 \ge \frac{1}{2}\cdot 2^n.$$

Из (3.13) следует, что

$$L^{\&}_{E(\mathsf{d}\ldots\mathsf{d})}(f) = \frac{1}{2}\cdot 2^n.$$

Теорема доказана. ◀

§ 10. Функции наибольшей сложности в классах операторных полиномиальных форм

В представленных выше результатах этой главы найдены функции наибольшей сложности в некоторых классах полиномиальных форм по

базисной функции многоместной конъюнкции. Однако возникают два вопроса.

- Как получить функции наибольшей сложности для полиномиальных форм, построенных по тем же классам операторных пучков, но по другим базисным функциям?
- Как найти функции наибольшей сложности в классе C_1, если известны функции наибольшей сложности в ψ-эквивалентном ему классе C_2?

Для ответа на эти вопросы нужно вернуться к теореме 2 и предложению 3. Из доказательств этих утверждений следует, что что существует некоторое невырожденное линейное преобразование пространства булевых функций фиксированной размерности, при котором прообраз и образ имеют одну и ту же сложность в соответствующих классах. Таким образом, ответы на поставленные вопросы сводятся к нахождению соответствующего линейного преобразования.

Опишем метод нахождения наиболее сложных функций в классе пучков C по базисной функции $g \in F_n$, если известны самые сложные функции в классе C по функции многоместной конъюнкции. Как и в доказательстве теоремы 2, рассмотрим пучок

$$\mathsf{B} = D(\mathsf{p} \ldots \mathsf{p}, \mathsf{e} \ldots \mathsf{e})$$

размерности n и его естественную нумерацию $\left(\mathsf{b}^{\tilde{0}}, \ldots, \mathsf{b}^{\tilde{1}}\right)$, в которой компоненты операторов определяются по формулам:

$$\mathsf{b}_i^{\tilde{\sigma}} = \begin{cases} \mathsf{p}, & \text{если } \sigma_i = 0; \\ \mathsf{e}, & \text{если } \sigma_i = 1; \end{cases} \qquad i \in \{1, \ldots, n\}, \quad \tilde{\sigma} \in E^n.$$

Базисная функция — это многоместная конъюнкция $x_1 \cdot \ldots \cdot x_n$. Составим матрицу $[\alpha_{\tilde{\sigma}\tilde{\tau}}]$ размера $2^n \times 2^n$, в которой

$$\alpha_{\tilde{\sigma}\tilde{\tau}} = \left(\mathsf{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n)\right)_{x_1 \ldots x_n}^{\tau_1 \ldots \tau_n}, \qquad \tilde{\sigma}, \tilde{\tau} \in E^n.$$

Пусть $g \in F_n$ — произвольная базисная функция. Составим матрицу $[\beta_{\tilde{\sigma}\tilde{\tau}}]$ размера $2^n \times 2^n$, в которой

$$\beta_{\tilde{\sigma}\tilde{\tau}} = \left(\mathfrak{b}^{\tilde{\sigma}} g(x_1, \ldots, x_n)\right)_{x_1 \ldots x_n}^{\tau_1 \ldots \tau_n}, \qquad \tilde{\sigma}, \tilde{\tau} \in E^n.$$

Тогда матрицу A линейного преобразования φ, фигурирующего в доказательстве теоремы 2, можно найти из матричного уравнения:

$$A \cdot [\alpha_{\tilde{\sigma}\tilde{\tau}}] = [\beta_{\tilde{\sigma}\tilde{\tau}}].$$

Но как легко заметить, матрица $[\alpha_{\tilde{\sigma}\tilde{\tau}}]$ — единичная, поэтому $[\beta_{\tilde{\sigma}\tilde{\tau}}]$ и есть искомая матрица линейного преобразования φ. Построение этой матрицы не составляет особого труда.

Теперь для того чтобы найти функции наибольшей сложности в классе C по базисной функции g, нужно взять функции наибольшей сложности в классе C по функции многоместной конъюнкции и применить к ней преобразование φ. В матричном виде это выглядит следующим образом:

$$\begin{bmatrix} f^*(\tilde{0}) \\ \vdots \\ f^*(\tilde{1}) \end{bmatrix} = \begin{bmatrix} \beta_{\tilde{0}\tilde{0}} & \cdots & \beta_{\tilde{0}\tilde{1}} \\ \vdots & \ddots & \vdots \\ \beta_{\tilde{1}\tilde{0}} & \cdots & \beta_{\tilde{1}\tilde{1}} \end{bmatrix} \cdot \begin{bmatrix} f(\tilde{0}) \\ \vdots \\ f(\tilde{1}) \end{bmatrix}.$$

Здесь f — функция наибольшей сложности в классе C по многоместной конъюнкции, f^* — соответствующая ей функция наибольшей сложности в классе C по базисной функции g.

Метод нахождения наиболее сложных функций в классе C_2 по известным функциям наибольшей сложности в ψ-эквивалентном ему классе C_1 похож на описанный выше метод.

Пусть Ψ — последовательность взаимнооднозначных отображений из $\{\mathsf{e}, \mathsf{p}, \mathsf{d}\}$ в $\{\mathsf{e}, \mathsf{p}, \mathsf{d}\}$, такая что $\Psi(C_1) = C_2$. Как в доказательстве предложения 3, рассмотрим двупорожденный пучок $\mathsf{B} = D(\mathsf{p} \ldots \mathsf{p}, \mathsf{e} \ldots \mathsf{e})$ и его естественную нумерацию $\left(\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}}\right)$, в которой компоненты операторов $\mathfrak{b}^{\tilde{\sigma}}$ определяются по формулам:

$$\mathfrak{b}_i^{\tilde{\sigma}} = \begin{cases} \mathsf{p}, & \text{если } \sigma_i = 0; \\ \mathsf{e}, & \text{если } \sigma_i = 1; \end{cases} \qquad i \in \{1, \ldots, n\}, \quad \tilde{\sigma} \in E^n.$$

В качестве базисной функции возьмем многоместную конъюнкцию $x_1 \cdot \ldots \cdot x_n$. Составим матрицу $[\alpha_{\tilde{\sigma}\tilde{\tau}}]$ размера $2^n \times 2^n$, в которой

$$\alpha_{\tilde{\sigma}\tilde{\tau}} = \left(\mathfrak{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n)\right)_{x_1 \ldots x_n}^{\tau_1 \ldots \tau_n},$$

Упорядоченный набор $\left(\Psi(\mathfrak{b}^{\tilde{0}}), \ldots, \Psi(\mathfrak{b}^{\tilde{1}})\right)$ является нумерацией пучка $\Psi(\mathsf{B})$. Построим матрицу $[\gamma_{\tilde{\sigma}\tilde{\tau}}]$, в которой

$$\gamma_{\tilde{\sigma}\tilde{\tau}} = \left(\Psi(\mathfrak{b}^{\tilde{\sigma}})(x_1 \cdot \ldots \cdot x_n)\right)_{x_1 \ldots x_n}^{\tau_1 \ldots \tau_n}.$$

Тогда матрица A линейного преобразования φ, фигурирующего в доказательстве предложения 3, может быть найдена из матричного уравнения

$$A \cdot [\alpha_{\tilde{\sigma}\tilde{\tau}}] = [\gamma_{\tilde{\sigma}\tilde{\tau}}].$$

Поскольку $[\alpha_{\tilde{\sigma}\tilde{\tau}}]$ — единичная матрица, то искомой матрицей преобразования φ будет $[\gamma_{\tilde{\sigma}\tilde{\tau}}]$. По известной последовательности Ψ, точнее по ее первым $n+1$, членам построить матрицу $[\gamma_{\tilde{\sigma}\tilde{\tau}}]$ не составляет труда.

Теперь если известна функция наибольшей сложности в классе C_1 по многоместной конъюнкции, то легко найти функцию f^*, наиболее сложную в классе C_2 по многоместной конъюнкции: нужно применить преобразование φ к функции f. В матричном виде это выглядит следующим образом:

$$\begin{bmatrix} f^*(\tilde{0}) \\ \vdots \\ f^*(\tilde{1}) \end{bmatrix} = \begin{bmatrix} \gamma_{\tilde{0}\tilde{0}} & \cdots & \beta_{\tilde{0}\tilde{1}} \\ \vdots & \ddots & \vdots \\ \gamma_{\tilde{1}\tilde{0}} & \cdots & \beta_{\tilde{1}\tilde{1}} \end{bmatrix} \cdot \begin{bmatrix} f(\tilde{0}) \\ \vdots \\ f(\tilde{1}) \end{bmatrix}.$$

Комбинируя эти два метода, можно из известных функций наибольшей сложности в классе C_1 по базисной функции многоместной конъюнкции получить самые сложные функции в любом ψ-эквивалентном ему классе C_2 по любой базисной функции g.

Описанные методы и теоремы 6, 9 позволяют получить самые сложные функции в классах $K(\mathfrak{a})$ и $E(\mathfrak{a})$ по любой базисной функции для любого оператора $\mathfrak{a}$, а теоремы 7 и 8 — самые сложные функции в классах K и FK по произвольной базисной функции.

Заключение

На защиту выносятся следующие результаты.

1. Для полиномиальных форм, построенных по операторным пучкам доказана независимость функции Шеннона от выбора базисной функции.
2. Найдены точные оценки сложности для $\mathfrak{a}$-кронекеровых и свободно-кронекеровых классов полиномиальных форм.
3. Найдены все функции наибольшей сложности в $\mathfrak{d}$-кронекеровом, кронекеровом, свободно-кронекеровом и $\mathfrak{d}$-расширенном классах полиномиальных форм по базисной функций многоместной конъюнкции. Разработан метод нахождения функций, имеющих наибольшую сложность в $\mathfrak{a}$-кронекеровых, кронекеровых, $\mathfrak{a}$-расширенных, свободно-кронекеровых классов полиномиальных форм по произвольной базисной функции.
4. Получена экспоненциальная нижняя оценка сложности последовательности эффективно заданных булевых функций в классе полиномиальных нормальных форм.
5. Получены формулы для вычисления коэффициентов полиномиальных форм по обратимым операторным пучкам и из свободно-кронекеровых классов.

Выражаю благодарность своим научным руководителям, Н.А. Перязеву и С.Ф. Винокурову, за всестороннюю поддержку во время работы над диссертацией, а также всем участникам семинара «Теория булевых функций», который проходит при Иркутском государственном университете, за творческую атмосферу, в которой приятно работать.

Список литературы

[1] Бохманн Д., Постхоф Х. Двоичные динамические системы. — М.: Энергоатомиздат, 1986. — 401 с.

[2] Винокуров С. Ф. Некоторые оценки сложности булевых функций в классе полиномов // Синтез и сложность управляющих систем, VII Межгосударственная школа-семинар. — Минск, 1995. — С. 4–5.

[3] Винокуров С. Ф. Смешанные операторы в булевых функциях и их свойства. — Иркутский Университет. Серия: Дискретная математика и информатика. Вып. 12. — Иркутск, 2000. — 36 с.

[4] Винокуров С. Ф., Перязев Н. А. Полиномиальная декомпозиция булевых функций по образам однородных операторов от невырожденных функций // Изв. вузов. Матем. — 1996. — № 1. — С. 17–21.

[5] Винокуров С. Ф., Перязев Н. А. Полиномиальные разложения булевых функций // Кибернетика и системный анализ. — 1993. — № 6. — С. 34–47.

[6] Винокуров С. Ф., Перязев Н. А. Полиномиальные разложения булевых функций по образам неоднородных операторов // Кибернетика и системный анализ. — 2000. — № 4. — С. 40–55.

[7] Винокуров С. Ф., Перязев Н. А. Представление булевых функций полиномиальными формами // Кибернетика и системный анализ. — 1992. — № 3. — С. 175–179.

[8] Грэхэм Р., Кнут Д., Паташник О. Конкретная математика. Основание информатики: Пер. с англ. — М.: Мир, 1998. — 703 с.

[9] Жегалкин И. И. Арифметизация символической логики. — Мат. сборник. — 1928. — Т. 35. — С. 311–373.

[10] Жегалкин И. И. Арифметизация символической логики. — Мат. сборник. — 1929. — Т. 36. — С. 305–338.

[11] Закревский А. Д. Минимизация систем булевых функций в полиномах Жегалкина // Докл. Белорусской АН. — 1995. — Т. 39, № 6. — С. 11–14.

[12] Кириченко К. Д. Верхняя оценка сложности полиномиальных нормальных форм булевых функций // Труды XII Международной школы-семинара „Синтез и сложность управляющих систем“. — М., 2001. — Т. 1. — С. 115–120.

[13] Кириченко К. Д. Верхняя оценка функции Шеннона сложности полиномиальных форм булевых функций // Дискретная математика: Труды XII Байкальской международной конференции «Методы оптимизации и их приложения». — Иркутск, 2001. — Т. 5. — С. 66–70.

[14] Корсуков А. В. Разложения булевых функций с оператором векторной производной // Алгебра, логика и приложения. — Иркутск: Иркут. ун-т, 1994. — С. 116–124.

[15] Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Моск. ун-та, 1984.

[16] Лупанов О. Б. Об асимптотических оценках сложности формул, реализующих функции алгебры логики // Докл. АН СССР. — 1959. — Т. 128, № 3. — С. 464–467.

[17] Лупанов О. Б. Об одном методе синтеза схем // Известия высших учебных заведений. Радиофизика. — 1958. — Т. 1, № 1. — С. 120–140.

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

[19] Лупанов О. Б. О реализаций функций алгебры логики формулами из конечных классов (формулами ограниченной глубины) в базисе $\&, \vee, \overline{\ }$ // Проблемы кибернетики. Вып. 6. — М.: Физматгиз, 1961. — С. 5–14.

[20] Марченков С. С. Замкнутые классы булевых функций. — М.: Физматлит, 2000. — 128 с.

[21] Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991. — 240 с.

[22] Пантелеев В. И., Перязев Н. А. Об операторах булевых функций // Труды XI Межгос. школы-семинара „Синтез и сложность управляющих систем“. — М.: Изд-во Московск. ун-та, 2000. — Часть. 2. — С. 141–146.

[23] Перязев Н. А. Основы теории булевых функций — М.: Физматлит, 1999. — 112 с.

[24] Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика — 1995. — Т. 34. — №. 3. — С. 323–326.

[25] Порецкий П. С. О способе решения логических равенств и об обратном способе математической логики // Собр. протоколов заседаний секции физ.-мат. наук Об-ва испытателей природы при Казанском ун-те. Т. 2. — 1884.

[26] Сапоженко А. А., Чухров И. П. Минимизация булевых функций в классе дизъюнктивных нормальных форм // ВИНИТИ. Итоги науки и техники. Теоретическая кибернетика. — 1987. — Вып. 25. — С. 68–116.

[27] Сэвидж Д. Э. Сложность вычислений: пер. с англ. — М.: Изд-во «Факториал», 1998. — 368. с.

[28] Храпченко В. М. Нижние оценки сложности схем из функциональных элементов // Кибернетич. сб. Новая серия. Вып. 21. — М.: Мир, 1984. — С. 3–54.

[29] Яблонский С. В. Введение в дискретную математику: Учеб. пособие для вузов. / под ред. В. А. Садовничего. — 3-е изд., стер. — М.: Высш. шк., 2001. — 384 с.

[30] Яблонский С. В. О невозможности элиминации перебора всех функций из P_2 при решении некоторых задач теории схем // Докл. АН СССР. — 1959. — Т. 124, № 1. — С. 44–47.

[31] Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем // Проблемы кибернетики. Вып. 2. — М.: Физматгиз, 1959. — С. 75–121.

[32] Besslich Ph. W., Riege M. W. An efficient program for logic synthesis of mod-2 sum expressions // Proc. EUROASIC. Paris, France, 1991. — P. 136–141.

[33] Blake A. Canonical expression in Boolean algebra. Dissertation — Chicago, 1937.

[34] Blum N. A. A Boolean function requiring $3n$ network size // Theoret. Comput. Sci. — 1984. — V. 28, N 3. — P. 337–345.

[35] Chrzanowska-Jeske M., Perkowski M., Mishchenko A. How to catch the golden fish of minimum ESOP into the net of canonical forms. — Portland State Univer., USA, 2001 — 11 p.

[36] Drechsler R., Jóźwiak L., Perkowski M. New hierarchies of and/exor trees, decision diagrams, lattice diagrams, canonical forms, and regular layouts // 3rd International Workshop on Applications of the Reed-Muller Expansion in Circuit Design (Reed-Muller 97). Sept. 19–20. — Oxford/UK, 1997 — P. 115–132.

[37] Even S., Kohavi I., Paz A. On minimal modulo 2 sums of products for switching functions // IEEE Trans. Electron. Comput. — 1967. — V. EC-16, N 10. — P. 671–674.

[38] Gaidukov A. I., Vinokurov S. F. Operator polynomial expansions of Boolean functions// 4^{th} International Workshop on Boolean Problems. — Freiberg, Germany, 2000. — P. 63–68.

[39] Green D. H. Families of Reed-Muller Canonical Forms // Intern. J. of Electr. — Febr. 1991 — N. 2 — P. 259–280.

[40] Koda N., Sasao T. An upper bound on the number of products in minimum ESOPs // IFIP wg 10.5. Workshop on application of the Reed-Muller expansion application in cicuit design. Japan, 1995 — P. 94–101.

[41] Logic synthesis and optimization / ed. T. Sasao. — Kluwer Academic Publishers, 1993. — 320 p.

[42] McCluskey E. J. Minimisation of Boolean functions // Bell Syst. Techn. J. — 1956. — N 35. — P. 1417–1444.

[43] Muller D. E. Application of Boolean to switching circuit desing and error detection // IRE Trans. Electron. Comput. — 1954. — V 3, N. 3. — P. 6–12.

[44] Post E. L. Introduction to a general theory of elementary propositions // Amer J. Math. — 1921. — V. 43, N 4. — P. 163–185.

[45] Post E. L. Two-valued iterative systems of mathematical logic // Annals of Math. Studies. Princeton Univ. Press. — 1941. — V. 5.

[46] Quine W. V. A way to simplify truth functions // J. Symbol. Logic. — 1955. — N 20. — P. 105–108.

[47] Reed I. S. A class of multiply-error-correcting codes and decoding scheme // IRE Trans. Inform. Theory. — 1954. — V 4, N. 9. — P. 38–49.

[48] Schnorr C. P. Zwei lineare untere Schranken für die Komplexität Boolescher Funktionen // Computing. Archiv für elektronisches Rechnen. — 1974. — V. 13, N 2. — P. 155–171.

Работы автора по теме диссертации

[49] Балюк А. С. Симметрические булевы функции, имеющие наибольшую сложность в классах поляризованных полиномов Жегалкина и кронекеровских полиномиальных форм // Студент и научно-технический прогресс (Молодые ученые к 80-летию ИГУ): тез. докл. студ. и асп. — Иркутск: Иркут. ун-т, 1998. — С. 36.

[50] Балюк А. С. Сложные симметрические булевы функции в классах поляризованных полиномиальных форм // Труды Восточно-Сибирской зональной межвузовской конференции по математике и проблемам ее преподавания в вузе. — Иркутск, 1999. — С. 148–149.

[51] Балюк А. С. Сложные в полиномиальных поляризованных формах симметричные булевы функции // XII Международная конференция по проблемам теоретической кибернетики. Тезисы докл. — Нижний Новгород, 1999. — С. 17.

[52] Балюк А. С. Булевы функции, имеющие наибольшую сложность в классах поляризованных полиномов Жегалкина и кронекеровских форм // Студент и научно-технический прогресс: тез. докл. студ. и асп. — Иркутск: Иркут. ун-т, 1999. — С. 63.

[53] Балюк А. С. Сложные в полиномиальных поляризованных формах функции алгебры логики // Международная конференция по математической логике. Тезисы докл. — Новосибирск, 1999. — С. 9–10.

[54] Балюк А. С., Винокуров С. Ф. Функция Шеннона для некоторых классов операторных полиномиальных форм // Оптимизация, управление, интеллект. — Иркутск, 2000. — Вып 5. — С. 111–121.

[55] Балюк А. С., Винокуров С. Ф. О полиномиальных представлениях булевых функций // Материалы VII Международного семинара «Дискретная математика и ее приложения». — М.: Изд-во Центра прикладных исследований МГУ, 2001. — С. 100–101.

[56] Избранные вопросы теории булевых функций / А. С. Балюк, С. Ф. Винокуров, А. И. Гайдуков, О. В. Зубков, К. Д. Кириченко, В. И. Пантелеев, Н. А. Перязев, Ю. В. Перязева; Под ред. С. Ф. Винокурова и Н. А. Перязева. — М.: Физматлит, 2001. — 192 с.

[57] Балюк А. С. Сложные булевы функции в классах двупорожденных операторных пучков // Дискретная математика: Труды XII Байкальской международной конференции «Методы оптимизации и их приложения». — Иркутск, 2001. — Т. 5. — С. 17–21.

[58] Балюк А. С. Нижняя оценка сложности одной последовательности булевых функций в классе полиномиальных нормальных форм // Труды XII Международной школы-семинара „Синтез и сложность управляющих систем“. — М., 2001. — Т. 1. — С. 18–21.

[59] Balyuk A., Vinokurov S. Classes of Operator Forms // 5^{th} International Workshop on Boolean Problems. — Freiberg, Germany, 2002. — P. 217–224.