ФЕДЕРАЛЬНАЯ ЦЕЛЕВАЯ ПРОГРАММА
«ГОСУДАРСТВЕННАЯ ПОДДЕРЖКА ИНТЕГРАЦИИ
ВЫСШЕГО ОБРАЗОВАНИЯ И
ФУНДАМЕНТАЛЬНОЙ НАУКИ НА 1997–2000 ГОДЫ»

ИЗБРАННЫЕ ВОПРОСЫ ТЕОРИИ БУЛЕВЫХ ФУНКЦИЙ

Под редакцией
С.Ф.Винокурова и Н.А.Перязева

Москва
ФИЗМАТЛИТ
2001

УДК 519.7
ББК 22.174
И 32

Издание осуществлено при финансовой поддержке Федеральной целевой программы «Государственная интеграция высшего образования и фундаментальной науки на 1997–2000 годы»

Авторы:
А.С. БАЛЮК, С.Ф. ВИНОКУРОВ, А.И. ГАЙДУКОВ,
О.В. ЗУБКОВ, К.Д. КИРИЧЕНКО, В.И. ПАНТЕЛЕЕВ,
Н.А. ПЕРЯЗЕВ, Ю.В. ПЕРЯЗЕВА

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.– ISBN 5-9221-0085-8.

Рассматриваются разделы булевых функций, интенсивно развивающиеся в настоящее время: представления функций бинарными термами, бесповторными термами и полиномиальными формами. Все необходимые для чтения известные определения и утверждения приведены в вводной главе.

Книга предназначена для научных работников и аспирантов. Она может также служить учебным пособием для студентов, специализирующихся в области дискретной математики и информатики.

Библиогр. 52 назв.

ISBN 5-9221-0085-8

© Центр «Интеграция», 2001

Оглавление

Предисловие

Для современного уровня развития общества характерным является переработка громадного объема информации, что естественным образом связано с развитием вычислительной техники, которая зависит от уровня разработки математических моделей дискретных преобразователей информации. На сегодняшний день булевы функции являются основным аппаратом для построения таких математических моделей. Теория булевых функций находит применение не только в логических системах и при синтезе различного рода схем, но и в диагностике и контроле схем, в теории кодирования, в теории конечных автоматов, в теории игр, в языках программирования и даже для математического моделирования природных процессов.

Суперпозиция выделенных функций — один из основных способов задания булевых функций. Такое задание принято называть термальным или формульным. При этом часто имеют место определенные ограничения, например, термы должны быть фиксированного вида. В исследованиях таких представлений булевых функций можно отметить следующие фундаментальные проблемы:

1. Характеризация функций, представляющихся термами заданного вида, без привлечения понятия суперпозиции.

2. Нахождение таких специальных видов термов, что любые булевы функции из некоторого множества K представляются термами этих видов.

3. Разработка простых алгоритмов для нахождения представлений функций термами заданного вида.

4. Оценка сложности представлений функций, исходя из определенных критериев.

Монография является попыткой коллектива авторов, исходя из перечисленных проблем, систематизировать некоторые разделы булевых функций, интенсивно развивающиеся в последнее время: бесповторные функции, полиномиальные представления и методы нахождения представления бинарными термами специальных видов.

Первая глава носит вспомогательный характер. В ней приведены необходимые определения и простые свойства функций, введены обозначения, которые используются в других главах. Остальные главы в основном не зависят друг от друга. В конце каждой главы приведены сведения о публикациях, не претендующие на полноту.

Бесповторные булевы функции представляют интерес, как наиболее простые, в некотором смысле, функции. Не всякая функция может быть представлена в виде бесповторного терма над заданным базисным множеством. Однако если такое представление для функции имеется, то оно является в определенном роде единственным. Описание функций, бесповторных в некотором базисе, имеет практическую ценность, в связи с их широким использованием при разработке дискретных управляющих устройств.

Интерес к полиномиальным представлениям булевых функций, как объектам исследования, связан в первую очередь с практическими приложениями. Распространение в электронике серии интегральных микросхем, содержащих в своем составе элементы «сложение по модулю два», особенно программируемых логических матриц, заставило вплотную заняться полиномиальными представлениями. Попытки напрямую перенести методы работы с дизъюнктивных на полиномиальные формы не принесли ощутимых результатов. Это стимулировало исследования по полиномиальным каноническим формам, поскольку имеется большое количество классов таких канонических представлений. Введение операторов в полиномиальные формы позволило получить общую картину полиномиальных разложений, построить классы полиномов, охватывающие известные полиномы, начиная с полинома Жегалкина и совершенной полиномиальной нормальной формы. Более того, операторы открыли возможность построения канонических форм, основанных не только на функции моногоместной конъюнкции.

В настоящее время по устоявшемуся мнению, впервые высказанному С.В.Яблонским, при решении задачи нахождения представлений булевых функций невозможно избежать «почти полного» перебора. Практическое исполнение таких алгоритмов минимизации возможно только для функций небольшой размерности. Более того, применение вычислительной техники не дает заметных преимуществ по сравнению с возможностями челове-

ка. Поэтому приходится видоизменять постановку общей задачи минимизации, вводя определенные ограничения. Возможны два пути:

— отказаться от нахождения минимальных термов, а находить представления термами, которые удовлетворяют определенной границе сложности;

— разрабатывать алгоритмы минимизации не для всего класса булевых функций, а для некоторым образом выделенных собственных подклассов.

Чаще всего для нахождения приемлемого решения задачи минимизации приходится вводить оба ограничения. При такой постановке проблема минимизации булевых функций разбивается на две фундаментальные задачи, не зависимые по методам их решения:

— *задача эффективных верхних оценок сложности*: разработка алгоритмов нахождения для булевых функций из конкретных подклассов представления их термами, близкими к минимальным;

— *задача эффективных нижних оценок сложности*: разработка новых методов получения нижних оценок сложности представлений эффективно определенных последовательностей булевых функций.

С одной стороны, разрабатываются приближенные алгоритмы представления булевых функций термами, с другой, — методы оценок таких представлений. Нужно отметить, что при решении задачи эффективных нижних оценок сложности возникают трудности принципиального характера. Поэтому оценка алгоритмов минимизации булевых функций в настоящее время производится применением к известным тестовым примерам и общими статистическими данными работы алгоритма.

В книге используются следующие утверждения: теоремы, предложения, следствия. Следствия не нумеруются, а теоремы и предложения имеют двойную нумерацию — номер главы и номер теоремы (предложения) внутри главы. Конец доказательства утверждений обозначается значком □.

Изложенные в книге результаты, за небольшим исключением, принадлежат авторам и получены при финансовой поддержке по гранту № А0037 ФЦП "Интеграция" и гранту РФФИ № 01–00–00556.

С.Ф. Винокуров, Н.А. Перязев

Глава I

Введение в теорию булевых функций

В данной главе приведены предварительные сведения, которые потребуются для изложения результатов последующих глав. Дополнительные источники приведены в списке литературы к первой главе. Терминология, принятая в книге, ближе всего к терминологии, использованной в [6].

§ 1. Определение и формы представления функций

Пусть $\sigma_i \in \{0,1\}$, $i \in \{1,\ldots,n\}$, тогда выражение $(\sigma_1,\ldots,\sigma_n)$ будем называть *двоичным набором*, а σ_i — *i-й компонентой двоичного набора*. Обозначим этот набор через $\tilde{\sigma}$. Для простоты изложения под двоичным набором понимаем и выражение без скобок, т.е. $\sigma_1,\ldots,\sigma_n$. В словосочетании «двоичный набор» слово «двоичный» часто будем опускать.

Длиной набора $\tilde{\sigma} = (\sigma_1,\ldots,\sigma_n)$ называют число n и обозначают длину через $|\tilde{\sigma}|$. Очевидно, что число всех наборов длины n равно 2^n. Через E^n обозначают множество всех двоичных наборов длины n, через E — множество E^1.

Набор, все компоненты которого нули, называют *нулевым* и обозначают через $\tilde{0}$, а набор, все компоненты которого единицы, называют *единичным* и обозначают через $\tilde{1}$.

Весом $||\tilde{\sigma}||$ двоичного набора $\tilde{\sigma}$ длины n будем называть число его компонент, равных единице, т.е. $||\tilde{\sigma}|| = \sum_{i=1}^{n} \sigma_i$.

Расстоянием (Хэмминга) между наборами $\tilde{\sigma}$ и $\tilde{\tau}$ длины n называется число, равное $\sum_{i=1}^{n} (\sigma_i \oplus \tau_i)$, где символ $\oplus$ означает сложение по модулю 2, другими словами — это число позиций, в которых эти наборы различны. Наборы, расстояние между которыми равно единице, называют *соседними*, а если это расстояние совпадает с их длиной, то — *противоположными*.

На множестве E^n естественным образом устанавливается частичный порядок. А именно: $(\sigma_1,\ldots,\sigma_n)\leqslant(\tau_1,\ldots,\tau_n)$ тогда и только тогда, когда $\sigma_i\leqslant\tau_i$ для всех $i\in\{1,\ldots,n\}$. Будем считать, что $\tilde\sigma=\tilde\tau$, если $\tilde\sigma\leqslant\tilde\tau$ и $\tilde\tau\leqslant\tilde\sigma$.

Введем в рассмотрение линейный порядок на E^n. Будем считать, что двоичные наборы $\tilde\sigma_1,\ldots,\tilde\sigma_m$ $(m=2^n)$ упорядочены по *натуральному порядку*, если для всех $s\in\{1,\ldots,m\}$ выполняется условие $s=1+\sum\limits_{i=1}^{n}2^{n-i}\cdot\sigma_{s,i}$, где $\tilde\sigma_s=(\sigma_{s,1},\ldots,\sigma_{s,n})$.

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.

Введем еще несколько употребляемых обозначений. Если $\tilde\sigma=(\sigma_1,\ldots,\sigma_{i-1},\sigma_i,\sigma_{i+1},\ldots,\sigma_n)$ — двоичный набор, то $\tilde\sigma_i$ определим как $\tilde\sigma_i=(\sigma_1,\ldots,\sigma_{i-1},\sigma_{i+1},\ldots,\sigma_n)$.

Для натуральных индексов введем следующее обозначение: $\tilde m=(1,\ldots,m)$, при этом запись $i\in\tilde m$ означает $i\in\{1,\ldots,m\}$. Запись $\tilde s\subseteq\tilde m$ означает, что $\tilde s$ — подмножество множества $\{1,\ldots,m\}$. При этом будем считать, если не оговаривается специально, что $\tilde m$ и $\tilde s$ упорядочены естественным образом.

Булевой функцией называется отображение из E^n в E. При этом n называется *размерностью* функции.

Слово «булева» в словосочетании «булева функция» часто для краткости будем опускать.

Обозначим произвольные булевы функции символами f, g, h (возможно с индексами), размерность функции f через $\dim f$; множество всех функций размерности n через F^n, а множество всех функций через F.

Для некоторых часто употребляемых функций будут введены специальные обозначения.

Функции размерности нуль — это константы: 0 и 1, называемые соответственно *нулевой* и *единичной* функциями.

Функций размерности один всего четыре:

$$f_1(0)=0,\quad f_2(0)=1,\quad f_3(0)=0,\quad f_4(0)=1,$$
$$f_1(1)=0,\quad f_2(1)=1,\quad f_3(1)=1,\quad f_4(1)=0.$$

Функция f_4 называется *отрицанием* и обозначается символом $-$, а функция f_3 — *тождественной* и обозначается символом e.

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 $(i \in \tilde{n})$. *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 $(\tau_1, \ldots, \tau_{n-1}) \in E^{n-1}$. Если $\sigma_i = 0$, то остаточная функция называется *нулевой остаточной*; если $\sigma_i = 1$, то — *единичной остаточной*. Индуктивно распространяется понятие остаточной функции на множество аргументов $i_1, \ldots, i_s$ по набору $\sigma_{i_1}, \ldots, \sigma_{i_s}$ $(s \leqslant n)$:

$$f^{\sigma_{i_1}, \ldots, \sigma_{i_s}}_{i_1, \ldots, i_s} = \left(f^{\sigma_{i_1}, \ldots, \sigma_{i_{s-1}}}_{i_1, \ldots, i_{s-1}}\right)^{\sigma_{i_s}}_{i_s},$$

где s называется *порядком* остаточной функции. Непосредственно из определения следует, что

$$f^{\sigma_{i_1}, \ldots, \sigma_{i_s}}_{i_1, \ldots, i_s} = f^{\sigma_{j_1}, \ldots, \sigma_{j_s}}_{j_1, \ldots, j_s},$$

где $j_1, \ldots, j_s$ любая перестановка $i_1, \ldots, i_s$.

Назовем i-й аргумент функции f *фиктивным*, если $f_i^0 = f_i^1$ и *существенным* в противном случае.

Функция называется *существенной*, если у нее нет фиктивных аргументов и *несущественной* в противном случае. *Рангом* функции называется число ее существенных аргументов, для функции f он обозначается как $\operatorname{rang} f$. Очевидно, что $\operatorname{rang} f \leqslant \dim f$, причем равенство выполняется тогда и только тогда, когда функция f существенная.

Пусть X — некоторое множество символов, называемых переменными (для переменных будем использовать символы x, y, z, u, v, w, возможно с различными индексами). Если X и Y — некоторые множества переменных, то через $\tilde{x}$ и $\tilde{y}$ будем обозначать некоторые упорядочения множеств X и Y. Запись $\tilde{x} \subseteq \tilde{y}$ означает, что $\tilde{x}$ — подмножество $\tilde{y}$ как упорядоченное множество, а запись $X \subseteq \tilde{y}$ и $\tilde{x} \subseteq Y$ не учитывает порядка. Через $|\tilde{x}|$ обозначаем длину набора $\tilde{x}$.

Если аргументы функции f именованы переменными $x_1, \ldots, x_n$, то говорят, что функция зависит от $x_1, \ldots, x_n$ или

$\tilde{x}$ и обозначают это так: $f(x_1,\ldots,x_n)$ или $f(\tilde{x})$. При переходе к остаточным функциям будем сохранять именование аргументов, если имеется функция $f(x_1,\ldots,x_n)$, то остаточная функция будет $f^{\sigma_i}_{x_i}(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)$. Будем использовать запись $f^{\tilde{\sigma}}_{\tilde{y}}$ для остаточных функций по множеству аргументов.

Для краткости записи для набора $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n$ введем обозначение $\tilde{x}_i$, тогда для остаточной функции от $f(\tilde{x})$ по аргументу x_i употребляется запись $f^{\sigma_i}_{x_i}(\tilde{x}_i)$. Очевидно, что если переменная — существенная в некоторой остаточной функции от функции f, то она — существенная и в f.

Для неупорядоченных множеств всех переменных, всех существенных и всех фиктивных переменных функции f введем обозначения $\chi(f)$, $\rho(f)$, $\delta(f)$ соответственно.

Отметим, что для функций e и $-$ вместо записи $e(x)$ и $-(x)$ будем использовать более простую запись x и $\bar{x}$. Введем также обозначение

$$x^{\sigma} = \begin{cases} x, & \text{если } \sigma = 1; \\ \bar{x}, & \text{если } \sigma = 0. \end{cases}$$

Под $\bar{\tilde{\sigma}}$ понимаем $\bar{\sigma}_1,\ldots,\bar{\sigma}_n$, под $\bar{\tilde{x}}$ — $\bar{x}_1,\ldots,\bar{x}_n$, а под $\tilde{x}^{\tilde{\sigma}}$ — $x_1^{\sigma_1},\ldots,x_n^{\sigma_n}$.

Предложение 1.1 (о существенном аргументе). *Для любой функции $f(\tilde{x})$ выполняется следующее условие: аргумент x_i является существенным в f тогда и только тогда, когда имеется набор $\tilde{\sigma}$ длины $|\tilde{x}|$ такой, что $f^{\tilde{\sigma}_i}_{\tilde{x}_i} = x_i^{\sigma_i}$.*

Доказательство. ($\Rightarrow$). Так как $x_i \in \rho(f)$, то $f^0_{x_i} \neq f^1_{x_i}$, а значит найдется такой набор $\tilde{\sigma}_i$, что $f^{0,\tilde{\sigma}_i}_{x_i,\tilde{x}_i} \neq f^{1,\tilde{\sigma}_i}_{x_i,\tilde{x}_i}$, т.е. $f^{1,\tilde{\sigma}_i}_{x_i,\tilde{x}_i} = \sigma_i$, $f^{0,\tilde{\sigma}_i}_{x_i,\tilde{x}_i} = \bar{\sigma}_i$ для некоторого $\sigma_i \in E$.

Тогда если $\sigma_i = 0$, то функция $f^{\tilde{\sigma}_i}_{\tilde{x}_i}(x_i) = \bar{x}_i = x_i^0 = x_i^{\sigma_i}$, а если $\sigma_i = 1$, то $f^{\tilde{\sigma}_i}_{\tilde{x}_i}(x_i) = x_i = x_i^1 = x_i^{\sigma_i}$.

($\Leftarrow$). В силу того, что $x_i \in \rho(f^{\tilde{\sigma}_i}_{\tilde{x}_i})$, имеем: $x_i \in \rho(f)$. □

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

Вектор $\tilde{\sigma}$ представляет функцию f, если $\sigma_i = f(\tilde{\alpha}_i)$, где $\tilde{\alpha}_i$ является i-м набором при натуральном упорядочении наборов. Записываем так: $f = \tilde{\sigma}$. Запись $f(\tilde{x}) = \tilde{\sigma}$ означает что i-й аргумент функции f именован переменной x_i и $f = \tilde{\sigma}$. Заметим, что вектор, представляющий функцию размерности n, имеет

длину 2^n. Вектор $\tilde{\sigma}$ будем записывать, как в виде строки, так и в виде столбца.

Еще одно часто используемое представление функций — представление посредством характеристических множеств.

Для функции f размерности n определим *нулевое характеристическое множество* $H_0(f)$ и *единичное характеристическое множество* $H_1(f)$ следующим образом:

$$H_0(f) = \{\tilde{\sigma} | \, \tilde{\sigma} \in E^n \text{ и } f(\tilde{\sigma}) = 0\}, H_1(f) = \{\tilde{\sigma} | \, \tilde{\sigma} \in E^n \text{ и } f(\tilde{\sigma}) = 1\}.$$

Очевидно, что $H_0(f)$ и $H_1(f)$ однозначно представляют функцию f. Это представление функции удобно при незначительном числе нулевых или единичных значений функции. Далее будем использовать обозначение $f = H_\sigma(f)$, где $\sigma \in E$.

Теорема 1.1. *Число всех функций размерности n равно 2^{2^n}, среди них существенных функций будет $\sum\limits_{i=0}^{n}(-1)^i C_n^i \cdot 2^{2^n-i}$.*

Доказательство. В силу векторного представления функций их число совпадает с числом различных наборов длины 2^n. Таких наборов будет 2^{2^n}.

Для подсчета числа существенных функций понадобится следующее свойство биномиальных коэффициентов:

$$\sum_{i=1}^{m}(-1)^{i+1} C_n^i C_{n-i}^{m-i} = C_n^m. \tag{1.1}$$

Доказательство формулы $A_n = \sum\limits_{k=0}^{n}(-1)^k C_n^k \cdot 2^{2^{n-k}}$, где A_n — число существенных функций размерности n, проведем индукцией по n.

Базис индукции. При $n = 0$ таких функций две: нулевая и единичная.

Шаг индукции. Число существенных функций размерности n равно разности числа всех функций и числа несущественных функций. Отсюда получаем

$$A_n = 2^{2^n} - C_n^1 A_{n-1} - C_n^2 A_{n-2} - \ldots - C_n^n A_0,$$

где $C_n^k A_{n-k}$ — это число функций, имеющих размерность n и ранг $n-k$.

Воспользуемся предположением индукции для A_{n-k}, при всех $k \in \tilde{n}$:

$$A_n = 2^{2^n} - C_n^1 \sum_{i=0}^{n-1} (-1)^i C_{n-1}^i \cdot 2^{2^{n-1-i}} - \ldots$$

$$\ldots - C_n^k \sum_{i=0}^{n-k} (-1)^i C_{n-k}^i \cdot 2^{2^{n-k-i}} - \ldots - C_n^n \sum_{i=0}^{0} (-1)^i C_0^i \cdot 2^{2^{0-i}}.$$

Группируя слагаемые при одинаковых степенях 2, получим

$$A_n = 2^{2^n} - (C_n^1 C_{n-1}^0) \cdot 2^{2^{n-1}} - \ldots - \Big(\sum_{i=1}^{k} (-1)^{i+k} C_n^i C_{n-i}^{k-i}\Big) \cdot 2^{2^{n-k}} - \ldots$$

$$\ldots - \Big(\sum_{i=1}^{n} (-1)^{i+n} C_n^i C_{n-i}^{n-i}\Big) \cdot 2^{2^{n-n}} = 2^{2^n} + (-1)^1 (C_n^1 C_{n-1}^0) \cdot 2^{2^{n-1}} + \ldots$$

$$\ldots + (-1)^k \Big(\sum_{i=1}^{k} (-1)^{i+1} C_n^i C_{n-i}^{k-i}\Big) \cdot 2^{2^{n-k}} + \ldots$$

$$+ (-1)^n \Big(\sum_{i=1}^{n} (-1)^{i+1} C_n^i C_{n-i}^{k-i}\Big) \cdot 2^{2^{n-n}}.$$

Используя тождество (1.1) для всех $k \in \tilde{n}$, имеем

$$A_n = C_n^0 \cdot 2^{2^n} + (-1)^1 C_n^1 \cdot 2^{2^{n-1}} + \ldots + (-1)^k C_n^k \cdot 2^{2^{n-k}} + \ldots$$

$$\ldots + (-1)^n C_n^n \cdot 2^{2^{n-n}} = \sum_{k=0}^{n} (-1)^k C_n^k \cdot 2^{2^{n-k}}. \quad \square$$

Отметим, что число различных функций размерности 0, 1, 2, 3 равно 2, 4, 16, 256 соответственно, а существенных функций — 2, 2, 10, 218.

Введем названия и обозначения для всех 10 существенных функций ранга 2, при этом, как принято, вместо записи вида $f(x, y)$ будем использовать запись вида xfy:

$f_1 = (0001)$ называют *конъюнкцией*, $f_1(x, y) = x \cdot y$;

$f_2 = (0111)$ — *дизъюнкцией*, $f_2(x, y) = x \vee y$;

$f_3 = (0110)$ — *сложением*, $f_3(x, y) = x \oplus y$;

$f_4 = (1110)$ — *штрихом (Шеффера)*, $f_4(x, y) = x|y$;

$f_5 = (1000)$ — *стрелкой (Пирса)*, $f_5(x, y) = x \downarrow y$;

$f_6 = (1101)$ — *импликацией*, $f_6(x, y) = x \to y$;

$f_7 = (1001)$ — *эквивалентностью*, $f_7(x, y) = x \leftrightarrow y$;

$f_8 = (0010)$ — *коимпликацией*, $f_8(x, y) = x \nrightarrow y$;
$f_9 = (1011)$ — *обратной импликацией*, $f_9(x, y) = x \leftarrow y$;
$f_{10} = (0100)$ — *обратной коимпликацией*, $f_{10}(x, y) = x \nleftarrow y$.

Функция называется *четной*, если число наборов, на которых функция равна 1, является четным и *нечетной* в противном случае.

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.

Для обозначения термов используем символы Φ, Ψ, Υ возможно с различными индексами. 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 $\Phi \equiv f(\Phi_1, ..., \Phi_n)$.

С определением терма связано несколько сопутствующих понятий: *подтерм терма* Φ, *глубина* $d(\Phi)$ *терма* Φ, *множество* $\chi(\Phi)$ *переменных терма* Φ:

1) если $\Phi \equiv x$, то единственным подтермом Φ является x; $d(\Phi) = 0$; $\chi(\Phi) = \{x\}$;

2) если $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)$, то подтермами Φ являются сам терм Φ и все подтермы термов $\Phi_1, \ldots, \Phi_m$;

$$d(f(\Phi_1, \ldots, \Phi_m)) = 1 + \max_{i \in \tilde{m}} d(\Phi_i); \quad \chi(\Phi) = \chi(\Phi_1) \cup \ldots \cup \chi(\Phi_m).$$

Подчеркнем, что подтерм Ψ терма Φ определяется своим местом вхождения в Φ. Заметим, что одинаковые термы могут быть различными как подтермы некоторого терма, в случае, если их вхождения в Φ разные.

Если множество $\chi(\Phi)$ упорядочить как $\tilde{x}$, то применяем запись $\Phi(\tilde{x})$.

Множество B будем называть *базисным множеством*, а функции из B *базисными функциями*. При этом говорят, что терм является *термом над базисным множеством* B.

Если нужно подчеркнуть, какие функциональные символы входят в построение терма Φ, употребляем запись $\Phi[f_1, \ldots, f_k]$, что означает, что в Φ есть подтермы вида $f_i(\Phi_{i_1}, \ldots, \Phi_{i_s})$, $i \in \{1, \ldots, k\}$ и $f_i \neq f_j$ для $i \neq j$, а все остальные подтермы являются переменными.

Если $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)$, то f — *внешняя* функция терма Φ.

Замечание. Если в определение терма входят функции ранга 0, 1, 2, то для них используются обозначения, введенные выше.

При этом, чтобы уменьшить число скобок в термах, часть скобок будем опускать, договорившись о приоритете функций для единственности восстановления скобок: $-, \cdot, \vee, \oplus$, все остальные функции. В записи термов символ конъюнкции «$\cdot$» часто будет опускаться.

Сопоставим набору переменных $\tilde{x}$ один из наборов множества E^n, при этом считаем, что задано *значение переменных* $\tilde{x}$. Определим *значение терма* Φ при заданных значениях переменных $\tilde{x}$, где $\chi(\Phi) \subseteq \tilde{x}$:

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 $\sigma_1, \ldots, \sigma_m$ соответственно, то значение терма Φ есть $f(\sigma_1, \ldots, \sigma_m)$.

Будем считать, что *функция g представима термом* $\Phi(x_1, \ldots, x_n)$, если $\dim g = n$ и для любого набора $\alpha_1, \ldots, \alpha_n$, задающего значение переменных, значение терма $\Phi(x_1, \ldots, x_n)$ при этом значении переменных совпадает с $g(\alpha_1, \ldots, \alpha_n)$. И также считаем, что *функция g представима термом* Φ, если существует такое упорядочение $\tilde{x}$ переменных $\chi(\Phi)$, при котором функция g представима термом $\Phi(\tilde{x})$. Для этих понятий используем обозначения $g = \Phi(\tilde{x})$ и $g = \Phi$.

Если $g = \Phi[f_1, \ldots, f_n]$, то говорят, что g есть *суперпозиция* функций $f_1, \ldots, f_n$.

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

Функции $f(\tilde{x})$ и $g(\tilde{y})$ называются *эквивалентными*, если они эквивалентны как термы. Функции, эквивалентные функциям размерности 0, 1, 2, назовем соответственно *константны-*

ми, унарными, бинарными. Бинарные функции, за исключением функций эквивалентных $\oplus$ и $\leftrightarrow$, называются *элементарными.*

Базисное множество, состоящее из всех бинарных функций, назовем бинарным базисным множеством, а состоящее из всех элементарных функций — элементарным. Для базисных множеств $\{\cdot, \vee, -\}$ и $\{\oplus, \cdot, \vee, -\}$ будем использовать обозначения B_0 и B_1.

Введем обозначение $\Phi_{\Phi_1}^{\Psi_1}$ для терма, получаемого из Φ заменой подтерма Φ_1 на терм Ψ_1 (для удобства будем считать, что если Φ_1 не является подтермом Φ, то $\Phi_{\Phi_1}^{\Psi_1} \equiv \Phi$). Договоримся также о том, что если Φ имеет несколько подтермов, равных Φ_1, и не указывается, какой именно заменяется, то считаем, что заменяются все. В случае, когда Φ_1 является переменной x, а Ψ_1 — константа σ, будем говорить об остаточных термах — Φ_x^σ. По аналогии с x^σ будем использовать обозначение

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

Следующие два утверждения носят технический характер и многократно используются в дальнейшем.

Предложение 1.2 (о замене). *Пусть* Φ, Ψ — *термы и* Υ — *подтерм* Φ. *Тогда если* $\Upsilon = \Psi$, *то* $\Phi = \Phi_\Upsilon^\Psi$.

Доказательство проведем индукцией по глубине терма Φ.

Базис индукции. Пусть $d(\Phi) = 0$. Тогда терм Φ является переменной, и у него единственный подтерм — сама переменная, т.е. $\Phi \equiv \Upsilon$. Поэтому $\Phi \equiv \Phi_\Upsilon^\Psi$, а значит $\Phi = \Phi_\Upsilon^\Psi$.

Шаг индукции. Пусть $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)$ и $\tilde{x} = \chi(\Phi)$, тогда, по определению подтерма, Υ — это либо сам терм Φ, либо подтерм некоторого Φ_i. В первом случае доказательство аналогично доказательству базиса индукции. Во втором случае по предположению индукции $\Phi_i = \Psi_i$, где $\Psi_i \equiv (\Phi_i)_\Upsilon^\Psi$. Тогда для любого набора $\tilde{\sigma}$, получаем, что

$$f((\Phi_1)_{\tilde{x}}^{\tilde{\sigma}}, \ldots, (\Phi_i)_{\tilde{x}}^{\tilde{\sigma}}, \ldots, (\Phi_m)_{\tilde{x}}^{\tilde{\sigma}}) = f((\Phi_1)_{\tilde{x}}^{\tilde{\sigma}}, \ldots, (\Psi_i)_{\tilde{x}}^{\tilde{\sigma}}, \ldots, (\Phi_m)_{\tilde{x}}^{\tilde{\sigma}}),$$

поэтому $f(\Phi_1, \ldots, \Phi_i, \ldots, \Phi_m) = f(\Phi_1, \ldots, \Phi_{i-1}, \Psi_i, \Phi_{i+1}, \ldots, \Phi_m)$. Отсюда $\Phi = \Phi_{\Phi_i}^{\Psi_i} = \Phi_\Upsilon^\Psi$, так как очевидно, что $\Phi_{\Phi_i}^{(\Phi_i)_\Upsilon^\Psi} \equiv \Phi_\Upsilon^\Psi$. $\square$

Предложение 1.3 (о подстановке). *Пусть* Φ, Ψ, Υ — *термы. Если* $\Phi = \Psi$, *то* $\Phi_x^\Upsilon = \Psi_x^\Upsilon$, *где* $x \in \chi(\Phi) \cup \chi(\Psi)$.

Доказательство проведем индукцией по глубине терма Υ.

Базис индукции. Пусть $d(\Upsilon) = 0$. Тогда $\Upsilon \equiv z$, поэтому $\Phi_x^\Upsilon = \Psi_x^\Upsilon$, так как $\Phi_x^\Upsilon \equiv \Phi_x^z$ и $\Psi_x^\Upsilon \equiv \Psi_x^z$.

Шаг индукции. Пусть $\Upsilon \equiv f(\Phi_1, \ldots, \Phi_m)$, $u_i \notin \chi(\Phi) \cup \chi(\Psi)$ для всех $i \in \tilde{m}$, тогда

$$\Phi_x^\Upsilon \equiv \left(\Phi_x^{f(u_1,\ldots,u_m)}\right)_{u_1,\ldots,u_m}^{\Phi_1,\ldots,\Phi_m} \text{ и } \Psi_x^\Upsilon \equiv \left(\Psi_x^{f(u_1,\ldots,u_m)}\right)_{u_1,\ldots,u_m}^{\Phi_1,\ldots,\Phi_m}.$$

Из $\Phi = \Psi$ очевидно следует, что $\Phi_x^{f(u_1,\ldots,u_m)} = \Psi_x^{f(u_1,\ldots,u_m)}$. Теперь, применив m раз предположение индукции, воспользовавшись тем, что $d(\Phi_i) < d(f(\Phi_1, \ldots, \Phi_m))$, получим

$$\left(\Phi_x^{f(u_1,\ldots,u_m)}\right)_{u_1,\ldots,u_m}^{\Phi_1,\ldots,\Phi_m} = \left(\Psi_x^{f(u_1,\ldots,u_m)}\right)_{u_1,\ldots,u_m}^{\Phi_1,\ldots,\Phi_m},$$

а значит $\Phi_x^\Upsilon = \Psi_x^\Upsilon$. □

Пусть f и g — функции размерности n, f и g называются *двойственными*, если $f(\tilde{\sigma}) = \bar{g}(\bar{\tilde{\sigma}})$ для любого $\tilde{\sigma} \in E^n$, другими словами $f(x_1, \ldots x_n) = \bar{g}(\bar{x}_1, \ldots, \bar{x}_n)$.

Для двойственных функций f и g введем обозначения $g = f^*$ и $f = g^*$. Очевидно, что $(f^*)^* = f$.

Определим терм Φ^* — *двойственный* к терму Φ:

1) если $\Phi \equiv x$, то $\Phi^* \equiv x$;

2) если $\Phi \equiv f(\Phi_1, \ldots, \Phi_s)$, то $\Phi^* \equiv f^*(\Phi_1^*, \ldots, \Phi_s^*)$.

При этом, очевидно, если $\Phi[f_1, \ldots, f_n]$, то $\Phi^* \equiv \Phi[f_1^*, \ldots, f_n^*]$.

Предложение 1.4. *Пусть функция* f *представима термом* Φ. *Тогда функция* f^* *представима термом* Φ^*.

Доказательство проведем индукцией по глубине терма Φ.

Базис индукции. Пусть $d(\Phi) = 0$. Тогда f — тождественная функция. Получаем $\Phi^* \equiv \Phi$, $f^* = f$.

Шаг индукции. Пусть $\Phi \equiv g(\Phi_1, \ldots, \Phi_m)$. Тогда так как $d(\Phi_i) < d(\Phi)$, то, используя предположение индукции для $\Phi_1, \ldots, \Phi_m$, получим

$$f^* = \bar{g}(\Phi_1, \ldots \Phi_m)(\bar{x}_1, \ldots, \bar{x}_k) = \bar{g}(\bar{\Phi}_1, \ldots, \bar{\Phi}_m)(\bar{x}_1, \ldots, \bar{x}_k) =$$

$$= \bar{g}(\overline{(\bar{\Phi}_1(\bar{x}_1,\ldots,\bar{x}_k)}),\ldots,\overline{(\bar{\Phi}_m(\bar{x}_1,\ldots,\bar{x}_k))}) = \bar{g}(\bar{g}_1^*,\ldots,\bar{g}_m^*) =$$
$$= g^*(g_1^*,\ldots,g_m^*) = g^*(\Phi_1^*,\ldots,\Phi_m^*) = \Phi^*,$$

где g_i представима термом $\Phi_i(\tilde{x})$ для всех $i \in \tilde{m}$. □

Следствие (принцип двойственности). *Пусть* Φ *и* Ψ — *термы. Тогда из* $\Phi = \Psi$ *следует* $\Phi^* = \Psi^*$.

Доказательство. Из $\Phi = \Psi$ следует, что $f(\tilde{x}) = g(\tilde{y})$, где $f(\tilde{x})$ представима термом Φ, а $g(\tilde{y})$ представима термом Ψ. Значит $f^*(\tilde{x}) = g^*(\tilde{y})$. По предложению 1.4 функция $f^*(\tilde{x})$ представима термом Φ^*, а функция $g^*(\tilde{y})$ — термом Ψ^*. Отсюда $\Phi^* = \Psi^*$. □

В заключение параграфа приведем утверждение, дающее множество часто используемых тождеств.

Предложение 1.5. *Выполняются следующие тождества:*

1) $x \cdot y = y \cdot x$; $x \vee y = y \vee x$; $x \oplus y = y \oplus x$ — ***коммутативность***;
2) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$; $x \vee (y \vee z) = (x \vee y) \vee z$; $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ — *ассоциативность*;
3) $1 \cdot x = x$; $0 \cdot x = 0$; $1 \vee x = 1$; $0 \vee x = x$; $0 \oplus x = x$; $1 \oplus x = \bar{x}$;
4) $x \cdot x = x$; $x \vee x = x$ — *идемпотентность*;
5) $\bar{\bar{x}} = x$;
6) $\overline{x \cdot y} = \bar{x} \vee \bar{y}$; $\overline{x \vee y} = \bar{x} \cdot \bar{y}$; $\overline{x \oplus y} = x \oplus y \oplus 1$;
7) $x \cdot (y \vee z) = x \cdot y \vee x \cdot z$; $x \vee (y \cdot z) = (x \vee y) \cdot (x \vee z)$; $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$; $x \vee (y \oplus z) = x \vee y \oplus x \vee z \oplus x$; $x \vee (y \oplus z \oplus u) = x \vee y \oplus x \vee z \oplus x \vee u$ — *дистрибутивность*;
8) $x \oplus y = \bar{x} \cdot y \vee x \cdot \bar{y}$; $x|y = \bar{x} \vee \bar{y}$; $x \downarrow y = \bar{x} \cdot \bar{y}$; $x \leftrightarrow y = x \cdot y \vee \bar{x} \cdot \bar{y}$; $x \leftrightarrow y = \bar{x} \oplus y$; $x \to y = \bar{x} \vee y$; $x \leftarrow y = x \vee \bar{y}$; $x \not\to y = x \cdot \bar{y}$; $x \not\leftarrow y = \bar{x} \cdot y$; $x \vee y = xy \oplus x \oplus y$;
9) $x \vee x \cdot y = x$; $\bar{x} \vee x \cdot y = \bar{x} \vee y$; $x \cdot (x \vee y) = x$; $\bar{x} \cdot (x \vee y) = \bar{x} \cdot y$; $x \oplus x \cdot y = x \cdot \bar{y}$; $x \oplus x \vee y = \bar{x} \cdot y$ — *поглощения*;
10) $x \cdot \bar{x} = 0$; $x \vee \bar{x} = 1$; $x \oplus x = 0$.

Доказательство. Непосредственно по определению проверяется, что термы в обеих частях тождеств являются эквивалентными. Отметим, что часть тождеств следует из других тождеств по принципу двойственности и поэтому для них можно не проверять эквивалентность по определению. □

Замечание. В силу тождеств ассоциативности договоримся опускать скобки в подтермах, в которых внешней функцией

является одна и та же функция: конъюнкция, дизъюнкция или сложение.

Предложение 1.6. *Выполняются следующие тождества обобщенной дистрибутивности:*

1) $x \circ \sum\limits_{i=1}^{2n+1} y_i = \sum\limits_{i=1}^{2n+1} x \circ y_i;$

2) $x \circ \sum\limits_{i=1}^{2n} y_i = \sum\limits_{i=1}^{2n} x \circ y_i \oplus x \circ 0,$

где $\circ \in \{\cdot, \vee, |, \downarrow, \to, \nrightarrow, \leftarrow, \nleftrightarrow\}$.

Доказательство заключается в непосредственной проверке указанных свойств. □

В сочетании предложений о замене и подстановке, а также полученных тождеств, можно доказывать эквивалентность термов над базисным множеством F^2, не пользуясь определением эквивалентности.

Точнее, будем говорить, *что тождество* $\Phi = \Psi$ *применимо к терму* Υ, если из Υ получаем эквивалентный ему терм $\Upsilon_{\Phi_0}^{\Psi_0}$, где Φ_0 — подтерм Υ вида $\Phi_0 \equiv \Phi_{x_1,\ldots,x_n}^{\Phi_1,\ldots,\Phi_n}$, а $\Psi_0 \equiv \Psi_{x_1,\ldots,x_n}^{\Psi_1,\ldots,\Psi_n}$, где $\tilde{x} \in \chi(\Phi) \cup \chi(\Psi)$. Эквивалентность $\Upsilon = \Upsilon_{\Phi_0}^{\Psi_0}$ следует из предложений о замене и подстановке.

Предложение 1.7. *Выполняются утверждения:*

1) $\sum\limits_{\{\tilde{\sigma} \in E^n\}} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} = 1;$

2) $\sum\limits_{\{\tilde{\sigma} \in E^n\}} x_1^{\sigma_1} \vee \ldots \vee x_n^{\sigma_n} = 1;$

3) $\sum\limits_{k=1}^{n} \sum\limits_{\substack{i_1,\ldots,i_k \in \tilde{n} \\ i_1 < \ldots < i_k}} x_{i_1} \cdot \ldots \cdot x_{i_k} = x_1 \vee \ldots \vee x_n;$

4) *если произведение* $f_i \cdot f_j$ *равно* 0 *для всех* $i, j \in \tilde{n}, i \neq j$, *то* $f_1 \vee \ldots \vee f_n = f_1 \oplus \ldots \oplus f_n$.

Доказательство. 1) Пусть $\tilde{\tau}$ — произвольный набор из E^n, тогда

$$\left(\sum_{\tilde{\sigma} \in E^n} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}\right)_{\tilde{x}}^{\tilde{\tau}} = \sum_{\tilde{\sigma} \in E^n} \tau_1^{\sigma_1} \cdot \ldots \cdot \tau_n^{\sigma_n} = 1,$$

поскольку для всех i имеем $\tau_i^{\sigma_i} = 1$ тогда и только тогда, когда $\tau_i = \sigma_i$.

2) Следует из 1) по принципу двойственности, в силу тождества $x_1 \leftrightarrow x_2 \leftrightarrow \ldots \leftrightarrow x_m = x_1 \oplus \ldots \oplus x_m \oplus 1$ при четном m.

3) Докажем индукцией по n.

Базис индукции. При $n = 2$ справедливость утверждения следует из тождеств предыдущего предложения.

Шаг индукции. Используя тождества, получим

$$\sum_{k=1}^{n} \sum_{\substack{i_1, \ldots, i_k \in \tilde{n} \\ i_1 < \ldots < i_k}} x_{i_1} \cdot \ldots \cdot x_{i_k} = \sum_{k=1}^{n-1} \sum_{\substack{i_1, \ldots, i_k \in \widetilde{n-1} \\ i_1 < \ldots < i_k}} x_{i_1} \cdot \ldots \cdot x_{i_k} \oplus$$

$$\oplus\, x_n \left(1 \oplus \sum_{k=1}^{n-1} \sum_{\substack{i_1, \ldots, i_k \in \widetilde{n-1} \\ i_1 < \ldots < i_k}} x_{i_1} \cdot \ldots \cdot x_{i_k} \right).$$

Применяя предположение индукции, получаем

$$\sum_{k=1}^{n} \sum_{\substack{i_1, \ldots, i_k \in \tilde{n} \\ i_1 < \ldots < i_k}} x_{i_1} \cdot \ldots \cdot x_{i_k} = x_1 \vee \ldots \vee x_{n-1} \oplus$$

$$\oplus\, x_n(1 \oplus x_1 \vee \ldots \vee x_{n-1}) = x_1 \vee \ldots \vee x_{n-1} \oplus$$

$$\oplus\, x_n(x_1 \vee \ldots \vee x_{n-1}) \oplus x_n = (x_1 \vee \ldots \vee x_{n-1})\bar{x}_n \oplus$$

$$\oplus\, \bar{x}_n \oplus 1 = \overline{(x_1 \vee \ldots \vee x_{n-1})}\bar{x}_n \oplus 1 = x_1 \vee \ldots \vee x_{n-1} \vee x_n.$$

4) Является непосредственным следствием пункта 3). □

§ 2. Декомпозиция функций

Функция f при разбиении множества аргументов на $\tilde{u}, \tilde{v}, \tilde{w}$ *допускает декомпозицию*, если существуют функции h и g такие, что выполняется:

$$f(\tilde{u}, \tilde{v}, \tilde{w}) = h(\tilde{u}, \tilde{w}, g(\tilde{u}, \tilde{v})). \tag{1.2}$$

При этом h называется *внешней*, а g — *внутренней* функцией декомпозиции. Если $\tilde{u} = \varnothing$, то такая декомпозиция называется *разделительной*. При $\tilde{w} \neq \varnothing$ множество переменных $\tilde{v}$ называется *выделимым*.

Теорема 1.2. *Для любой функции f равносильны следующие условия:*

1) *f допускает декомпозицию при разбиении множества аргументов на $\tilde{u}, \tilde{v}, \tilde{w}$;*

2) *для любого набора $\tilde{\alpha}$ ($|\tilde{\alpha}| = |\tilde{u}|$) среди всех остаточных функций от функции $f_{\tilde{u}}^{\tilde{\alpha}}$ по аргументам $\tilde{v}$ не более двух различных;*

3) *для любого набора $\tilde{\alpha}$ ($|\tilde{\alpha}| = |\tilde{u}|$) существует функция t такая, что любая остаточная функция от функции $f_{\tilde{u}}^{\tilde{\alpha}}$ по аргументам $\tilde{w}$ является либо константной, либо функцией t, либо функцией $\bar{t}$.*

Доказательство. 1) $\Rightarrow$ 3). Существуют функции h и g такие, что $f(\tilde{u}, \tilde{v}, \tilde{w}) = h(\tilde{u}, \tilde{w}, g(\tilde{u}, \tilde{v}))$. Поэтому для любого набора $\tilde{\alpha}$ определим $t(\tilde{v}) = g_{\tilde{u}}^{\tilde{\alpha}}(\tilde{v})$. Тогда любая остаточная $f_{\tilde{u},\tilde{w}}^{\tilde{\alpha},\tilde{\beta}} = h(\tilde{\alpha}, \tilde{\beta}, g(\tilde{\alpha}, \tilde{v}))$ очевидно равна либо константной функции, либо t, либо $\bar{t}$.

3) $\Rightarrow$ 2). Для произвольного набора $\tilde{\alpha}$ предположим противное, т.е. что существует не менее трех различных остаточных функций от функции $f_{\tilde{u}}^{\tilde{\alpha}}$ по аргументам $\tilde{v}$.

Пусть три из них это функции: $f_{\tilde{u},\tilde{v}}^{\tilde{\alpha},\tilde{\gamma}_1}, f_{\tilde{u},\tilde{v}}^{\tilde{\alpha},\tilde{\gamma}_2}, f_{\tilde{u},\tilde{v}}^{\tilde{\alpha},\tilde{\gamma}_3}$. Так как $f_{\tilde{u},\tilde{v}}^{\tilde{\alpha},\tilde{\gamma}_1} \neq f_{\tilde{u},\tilde{v}}^{\tilde{\alpha},\tilde{\gamma}_2}$, то найдется набор $\tilde{\beta}_1$ такой, что $f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_1,\tilde{\beta}_1} \neq f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_2,\tilde{\beta}_1}$. Тогда $f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_1,\tilde{\beta}_1} = f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_3,\tilde{\beta}_1}$ или $f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_2,\tilde{\beta}_1} = f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_3,\tilde{\beta}_1}$.

Для определенности, пусть $f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_1,\tilde{\beta}_1} = f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_3,\tilde{\beta}_1}$. Так как $f_{\tilde{u},\tilde{v}}^{\tilde{\alpha},\tilde{\gamma}_1} \neq f_{\tilde{u},\tilde{v}}^{\tilde{\alpha},\tilde{\gamma}_3}$, то существует набор $\tilde{\beta}_2$ при котором выполняется $f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_1,\tilde{\beta}_2} \neq f_{\tilde{u},\tilde{v},\tilde{w}}^{\tilde{\alpha},\tilde{\gamma}_3,\tilde{\beta}_2}$.

Получим, что остаточные функции $f_{\tilde{u},\tilde{w}}^{\tilde{\alpha},\tilde{\beta}_1}$ и $f_{\tilde{u},\tilde{w}}^{\tilde{\alpha},\tilde{\beta}_2}$ — неконстантные, неравные и $f_{\tilde{u},\tilde{w}}^{\tilde{\alpha},\tilde{\beta}_1} \neq \overline{f}_{\tilde{u},\tilde{w}}^{\tilde{\alpha},\tilde{\beta}_2}$, что противоречит 3).

2) $\Rightarrow$ 1). Так как для произвольного набора $\tilde{\sigma}_i$ среди остаточных функций от функции $f_{\tilde{u}}^{\tilde{\sigma}_i}$ по аргументам $\tilde{v}$ не более двух различных, то введем для них обозначения $f_{\tilde{u}}^{\tilde{\sigma}_i,\diamond} = f_{\tilde{u},\tilde{v}}^{\tilde{\sigma}_i,\tilde{0}}$ и $f_{\tilde{u}}^{\tilde{\sigma}_i,\#}$.

Теперь определим $g(\tilde{u}, \tilde{v})$, $h(\tilde{u}, \tilde{w}, y)$ следующим образом ($|u| = k$, $s = 2^k$):
$g(\tilde{u}, \tilde{v}) = u_1^{\sigma_{1,1}} \cdot \ldots \cdot u_k^{\sigma_{1,k}} \cdot g_1(\tilde{\sigma}_1, \tilde{v}) \vee \ldots \vee u_1^{\sigma_{s,1}} \cdot \ldots \cdot u_k^{\sigma_{s,k}} \cdot g_s(\tilde{\sigma}_s, \tilde{v})$,

где $g_i(\tilde{\sigma}_i, \tilde{v})$ определяется так:

$$g_i(\tilde{\sigma}_i, \tilde{\beta}) = \begin{cases} 0, \text{ если } f^{\tilde{\sigma}_i,\tilde{\beta}}_{\tilde{u},\tilde{v}} = f^{\tilde{\sigma}_i,\diamond}_{\tilde{u}}, \\ 1, \text{ если } f^{\tilde{\sigma}_i,\tilde{\beta}}_{\tilde{u},\tilde{v}} = f^{\tilde{\sigma}_i,\#}_{\tilde{u}}, \end{cases}$$

$$h(\tilde{u}, \tilde{w}, y) = \\ = u_1^{\sigma_{1,1}} \cdot \ldots \cdot u_k^{\sigma_{1,k}} \cdot h_1(\tilde{\sigma}_1, \tilde{w}, y) \vee \ldots \vee u_1^{\sigma_{s,1}} \cdot \ldots \cdot u_k^{\sigma_{si}} \cdot h_s(\tilde{\sigma}_s, \tilde{w}, y),$$

где $h_i(\tilde{\sigma}_i, \tilde{w}, y) = \bar{y} f^{\tilde{\sigma}_i,\diamond}_{\tilde{u}} \vee y f^{\tilde{\sigma}_i,\#}_{\tilde{u}}$.

Покажем, что равенство (1.2) при определенных таким образом функциях g и h выполняется:

$$h(\tilde{\sigma}_i, \tilde{\gamma}, g(\tilde{\sigma}_i, \tilde{\beta})) = \sigma_{i,1}^{\sigma_{1,1}} \cdot \ldots \cdot \sigma_{i,k}^{\sigma_{1,k}} \cdot h_1(\tilde{\sigma}_1, \tilde{\gamma}, g(\tilde{\sigma}_i, \tilde{\beta})) \vee \ldots \\ \ldots \vee \sigma_{i,1}^{\sigma_{s,1}} \cdot \ldots \cdot \sigma_{i,k}^{\sigma_{s,k}} \cdot h_s(\tilde{\sigma}_s, \tilde{\gamma}, g(\tilde{\sigma}_i, \tilde{\beta})) = h_i(\tilde{\sigma}_i, \tilde{\gamma}, g(\tilde{\sigma}_i, \tilde{\beta})) = \\ = h_i(\tilde{\sigma}_i, \tilde{\gamma}, (\sigma_{i,1}^{\sigma_{1,1}} \cdot \ldots \cdot \sigma_{i,k}^{\sigma_{1,k}} \cdot g_1(\tilde{\sigma}_1, \tilde{\beta}) \vee \ldots \vee \sigma_{i,1}^{\sigma_{s,1}} \cdot \ldots \\ \ldots \cdot \sigma_{i,k}^{\sigma_{s,k}} g_s(\tilde{\sigma}_s, \tilde{\beta}))) = h_i(\tilde{\sigma}_i, \tilde{\gamma}, g_i(\tilde{\sigma}_i, \tilde{\beta})) = \bar{g}_i(\tilde{\sigma}_i, \tilde{\beta}) \cdot f^{\tilde{\sigma}_i,*}_{\tilde{u}}(\tilde{\gamma}) \vee \\ \vee g_i(\tilde{\sigma}_i, \tilde{\beta}) \cdot f^{\tilde{\sigma}_i,\#}_{\tilde{u}}(\tilde{\gamma}).$$

В силу определения g_i получаем, что если $g_i(\tilde{\sigma}_i, \tilde{\beta}) = 0$, то $h_i(\tilde{\sigma}_i, \tilde{\gamma}, g_i(\tilde{\sigma}_i, \tilde{\beta})) = f^{\tilde{\sigma}_i *}_{\tilde{u}}(\tilde{\gamma}) = f(\tilde{\sigma}_i, \tilde{\beta}, \tilde{\gamma})$; а если $g_i(\tilde{\sigma}_i, \tilde{\beta}) = 1$, то $h_i(\tilde{\sigma}_i, \tilde{\gamma}, g_i(\tilde{\sigma}_i, \tilde{\beta})) = f^{\tilde{\sigma}_i \#}_{\tilde{u}}(\tilde{\gamma}) = f(\tilde{\sigma}_i, \tilde{\beta}, \tilde{\gamma})$.

Так как это выполнилось для произвольных $\tilde{\sigma}_i, \tilde{\gamma}, \tilde{\beta}$, то равенство (1.2) верно. □

Следствие (критерий разделительной декомпозиции). *Для любой функции f следующие условия эквивалентны:*

1) *f допускает разделительную декомпозицию при разбиении множества аргументов на $\tilde{v}$ и $\tilde{w}$;*

2) *среди всех остаточных функций от f по аргументам $\tilde{v}$ не более двух различных;*

3) *существует функция t такая, что любая остаточная функция от f по аргументам $\tilde{w}$ является либо константной, либо функцией t, либо функцией $\bar{t}$.*

Доказательство получается из доказательства теоремы 1.2 при условии $\tilde{u} = \varnothing$. □

§ 3. Разложения функций по переменным

Существуют представления булевых функций термами, в которых внешней функцией может быть любая наперед заданная существенная функция, т.е. верно следующее утверждение.

Теорема 1.3. *Для любой существенной функции h ранга m, для любого k такого, что $2^k = s \leq m$ существуют функции $g_1, \ldots, g_m$ такие, что для любой функции f ранга n при $n \geq k$, для любого разбиения множества переменных $\tilde{x}$ на $\tilde{y}$ и $\tilde{z}$, где $|\tilde{y}| = k$ выполняется:*

$$f(\tilde{x}) = h(g_1(\tilde{y}, f_{\tilde{y}}^{\tilde{\sigma}_1}(\tilde{z})), \ldots, g_s(\tilde{y}, f_{\tilde{y}}^{\tilde{\sigma}_s}(\tilde{z})), g_{s+1}(\tilde{y}), \ldots, g_m(\tilde{y})), \tag{1.3}$$

где $\{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_s\} = E^k$.

Доказательство. Так как h — существенная функция, то для любого $i \leqslant m$ найдется набор $\tilde{\alpha}_i = \alpha_{i,1}, \ldots, \alpha_{i,m}$ такой, что $h_{\tilde{u}_i}^{\tilde{\alpha}_{i,i}}(u_i) = u_i^{\alpha_{i,i}}$, где $\tilde{\alpha}_{i,i} = \alpha_{i,1}, \ldots, \alpha_{i,i-1}, \alpha_{i,i+1}, \ldots, \alpha_{i,m}$.

Определим функции $g_j(\tilde{y}, \tau)$, $j \in \tilde{s}$, $|\tilde{y}| = k$, следующим образом:

$$g_j(\tilde{\sigma}_i, \tau) = \begin{cases} \alpha_{i,j}, & \text{если } i \neq j, \\ \tau^{\alpha_{i,i}}, & \text{если } i = j, \end{cases}$$

а функции $g_j(\tilde{y})$, $j \in \{s+1, ..., m\}$ так: $g_j(\tilde{\sigma}_i) = \alpha_{i,j}$. Для всех наборов $\tilde{\sigma}_i$ получаем

$$h(g_1(\tilde{\sigma}_i, f_{\tilde{y}}^{\tilde{\sigma}_1}(\tilde{z})), \ldots, g_s(\tilde{\sigma}_i, f_{\tilde{y}}^{\tilde{\sigma}_s}(\tilde{z})), g_{s+1}(\tilde{\sigma}_i), \ldots, g_m(\tilde{\sigma}_i)) =$$
$$= h(\alpha_{i,1}, \ldots, \alpha_{i,i-1}, (f_{\tilde{y}}^{\tilde{\sigma}_i}(\tilde{z}))^{\alpha_{i,i}}, \alpha_{i,i+1}, \ldots, \alpha_{i,m}) = f_{\tilde{y}}^{\tilde{\sigma}_i}(\tilde{z}).$$

Так как это верно для всех $\tilde{\sigma}_i \in E^k$, то выполняется (1.3). □

Рассмотрим разложение (1.3) в случае $m = 2^k$.

1. Пусть $h = u_1 \vee \ldots \vee u_m$. Тогда для любого $i \leqslant m$ существует только один набор $\tilde{\alpha}_i$, для которого $h_{\tilde{u}_i}^{\tilde{\alpha}_{i,i}}(u_i) = u_i^{\alpha_{i,i}}$, а именно, $\alpha_{i,j} = 0$ при $i \neq j$, $\alpha_{i,i} = 1$. Поэтому $g_j(\tilde{y}, w) = y_1^{\sigma_{i,1}} \cdot \ldots \cdot y_k^{\sigma_{i,k}} \cdot w$, где $\tilde{\sigma}_i = \sigma_{i,1}, \ldots, \sigma_{i,k}$.

Отсюда следует, что для h существует только одно разложение (1.3), которое принимает следующий вид:

$$f(\tilde{y}, \tilde{z}) = y_1^{\sigma_{1,1}} \cdot \ldots \cdot y_k^{\sigma_{1,k}} \cdot f_{\tilde{y}}^{\tilde{\sigma}_1}(\tilde{z}) \vee \ldots \vee y_1^{\sigma_{m,1}} \cdot \ldots \cdot y_k^{\sigma_{m,k}} \cdot f_{\tilde{y}}^{\tilde{\sigma}_m}(\tilde{z}).$$

Назовем это разложение *дизъюнктивным по переменным $\tilde{y}$.*

2. Пусть $h = u_1 \cdot \ldots \cdot u_m$. Тогда, рассуждая аналогично, получим единственное разложение вида:

$$f(\tilde{y}, \tilde{z}) = (y_1^{\bar{\sigma}_{1,1}} \vee \ldots \vee y_k^{\bar{\sigma}_{1,k}} \vee f_{\tilde{y}}^{\tilde{\sigma}_1}(\tilde{z})) \ldots (y_1^{\bar{\sigma}_{m,1}} \vee \ldots \vee y_k^{\bar{\sigma}_{m,k}} \vee f_{\tilde{y}}^{\tilde{\sigma}_m}(\tilde{z})).$$

Это разложение назовем *конъюнктивным по переменным* $\tilde{y}$.

3. Пусть $h = u_1 \oplus \ldots \oplus u_m$. Тогда для любого $i \leqslant m$ любой набор $\tilde{\alpha}_i$ подходит для определения функций g_j. В этом случае возможно максимальное число различных разложений. Все такие разложения называем *полиномиальными по переменным* $\tilde{y}$.

В частности выделим два таких разложения:

$$f(\tilde{y}, \tilde{z}) = y_1^{\sigma_{1,1}} \cdot \ldots \cdot y_k^{\sigma_{1,k}} \cdot f_{\tilde{y}}^{\tilde{\sigma}_1}(\tilde{z}) \oplus \ldots \oplus y_1^{\sigma_{m,1}} \cdot \ldots \cdot y_k^{\sigma_{m,k}} \cdot f_{\tilde{y}}^{\tilde{\sigma}_m}(\tilde{z}),$$

$$f(\tilde{y}, \tilde{z}) = (y_1^{\bar{\sigma}_{1,1}} \vee \ldots \vee y_k^{\bar{\sigma}_{1,k}} \vee \bar{f}_{\tilde{y}}^{\tilde{\sigma}_1}(\tilde{z})) \oplus \ldots \oplus (y_1^{\bar{\sigma}_{m,1}} \vee \ldots \vee y_k^{\bar{\sigma}_{m,k}} \vee \bar{f}_{\tilde{y}}^{\tilde{\sigma}_m}(\tilde{z}));$$

первое будем называть *полиномиальным конъюнктивно-нормальным разложением по переменным* $\tilde{y}$, а второе — *полиномиальным дизъюнктивно-нормальным разложением по переменным* $\tilde{y}$.

Канонической формой для класса функций R называются термы определенного вида, такие что для любой $f \in R$ существует терм этого вида, эквивалентный $f(\tilde{y})$, причем единственный в некотором заданном смысле.

Совершенная дизъюнктивная нормальная форма (СДНФ). Терм Φ от множества переменных $\tilde{y} = y_1, \ldots, y_n$, называется *совершенной дизъюнктивной нормальной формой от* $\tilde{y}$, если $\Phi \equiv K_1 \vee \ldots \vee K_s$, где $K_i \equiv y_1^{\sigma_{i_1}} \cdot \ldots \cdot y_n^{\sigma_{i_n}}$, и все наборы $(\sigma_{i_1}, \ldots, \sigma_{i_n})$ для $i \in \tilde{s}$ — различные; K_i называются *полными элементарными конъюнкциями*.

Две СДНФ будем считать равными, если они состоят из одинакового множества полных элементарных конъюнкций.

Предложение 1.8. *Для класса R всех ненулевых функций* СДНФ *является канонической формой.*

Доказательство. Для любой функции $f(\tilde{y})$ сделаем дизъюнктивное разложение по всем переменным $\tilde{y}$:

$$f(\tilde{y}) = y_1^{\tau_{1,1}} \cdot \ldots \cdot y_n^{\tau_{1,n}} \cdot f_{\tilde{y}}^{\tilde{\tau}_1} \vee \ldots \vee y_1^{\tau_{m,1}} \cdot \ldots \cdot y^{\tau_{m,n}} \cdot f_{\tilde{y}}^{\tilde{\tau}_m},$$

где $m = 2^n$, $\{\tilde{\tau}_1, \ldots, \tilde{\tau}_m\} = E^m$.

Если f — ненулевая функция, то хотя бы одна из остаточных функций $f_{\tilde{y}}^{\tilde{\tau}_1}, \ldots, f_{\tilde{y}}^{\tilde{\tau}_m}$ — единичная. Поэтому функция

$$f(\tilde{y}) = \bigvee_{\tilde{\tau}_i \in V} y_1^{\tau_{i,1}} \cdot \ldots \cdot y_n^{\tau_{i,n}},$$

где $V = \{\tilde{\tau}_i | f_{\tilde{y}}^{\tilde{\tau}_i} = 1 \text{ и } \tilde{\tau}_i \in E^n\}$, т.е. в разложение входят все полные элементарные конъюнкции $y_1^{\tau_{i,1}} \cdot \ldots \cdot y_n^{\tau_{i,n}}$, для которых $(\tau_{i,1}, \ldots, \tau_{i,n})$ — это все такие наборы, где значение функции равно 1.

В итоге получаем, что любая ненулевая функция представима СДНФ. Единственность СДНФ очевидна. □

Совершенная конъюнктивная нормальная форма (СКНФ). Терм Ф от множества переменных $\tilde{y} = y_1, \ldots, y_n$ называется *совершенной конъюнктивной нормальной формой от* $\tilde{y}$, если он имеет следующий вид

$$\Phi \equiv \mathcal{D}_1 \cdot \ldots \cdot \mathcal{D}_s,$$

где $\mathcal{D}_i \equiv (y_1^{\sigma_{i_1}} \vee \ldots \vee y_n^{\sigma_{i_n}})$ и все наборы $(\sigma_{i_1}, \ldots, \sigma_{i_n})$ для $i \in \tilde{s}$ — различные; $\mathcal{D}_i$ называются *полными элементарными дизъюнкциями.*

Две СКНФ считаются равными, если они состоят из равных множеств полных элементарных дизъюнкций.

Предложение 1.9. *Для класса R всех неединичных функций* СКНФ *является канонической формой.*

Доказательство аналогично доказательству предыдущего предложения, только используется конъюнктивное разложение. Приведем только вычислительную формулу

$$f(\tilde{y}) = \prod_{\tilde{\tau}_i \in V} (y_1^{\bar{\tau}_{i,1}} \vee \ldots \vee y_n^{\bar{\tau}_{i,n}}),$$

где $V = \{\tilde{\tau}_i | f_{\tilde{y}} \tilde{\tau}_i = 0 \text{ и } \tilde{\tau}_i \in E^n\}$.

Заметим также, что это предложение можно получить из предложения 1.8 по принципу двойственности. □

Совершенная полиномиальная конъюнктивно-нормальная форма (СПКНФ). Терм Ф от множества переменных $\tilde{y} = y_1, \ldots, y_n$ называется *совершенной полиномиальной конъюнктивно-нормальной формой от* $\tilde{y}$, если имеет следующий вид:

$$\Phi \equiv K_1 \oplus \ldots \oplus K_s,$$

где K_i — различные полные элементарные конъюнкции. Равенство для СПКНФ, также как для вышеприведенных канонических форм, определяется равенством множества полных элементарных конъюнкций.

Предложение 1.10. *Для класса R всех ненулевых функций* СПКНФ *является канонической формой.*

Доказательство следует из предложения 1.8 и при этом выполняется формула

$$f(\tilde{y}) = \sum_{\tilde{\tau}_i \in V} y_1^{\tau_{i,1}} \cdot \ldots \cdot y_n^{\tau_{i,n}},$$

где $V = \{\tilde{\tau}_i | f_{\tilde{y}}^{\tilde{\tau}_i} = 1 \text{ и } \tilde{\tau}_i \in E^n.\}$ □

Совершенная полиномиальная дизъюнктивно-нормальная форма (СПДНФ). Если в определении СПДНФ полные элементарные конъюнкции заменить на полные элементарные дизъюнкции, то получаем *совершенную полиномиальную дизъюнктивно-нормальную форму от переменных $\tilde{y}$.*

Предложение 1.11. *Для класса R всех ненулевых функций* СПДНФ *является канонической формой.*

Доказательство. Для доказательства существования СПДНФ для произвольной функции сделаем полиномиальное дизъюнктивно-нормальное разложение по всем аргументам.

$$f(\tilde{y}) = (y_1^{\bar{\sigma}_{1,1}} \vee \ldots \vee y_k^{\bar{\sigma}_{1,k}} \vee f_{\tilde{y}}^{\bar{\sigma}_1}) \oplus \ldots \oplus (y_1^{\bar{\sigma}_{m,1}} \vee \ldots \vee y_k^{\bar{\sigma}_{m,k}} \vee f_{\tilde{y}}^{\bar{\sigma}_k}).$$

Учитывая, что $f_{\tilde{y}}^{\bar{\sigma}_1}, \ldots, f_{\tilde{y}}^{\bar{\sigma}_k}$ — константные функции, получаем

$$f(\tilde{y}) = \left(\sum_{\tilde{\tau}_i \in V'} y_1^{\bar{\tau}_{i,1}} \vee \ldots \vee y_k^{\bar{\tau}_{i,k}} \right) \oplus \left(\sum_{\tilde{\tau}_i \in V''} 1 \right),$$

где $V' = \{\tilde{\tau}_i | f_{\tilde{y}}^{\tilde{\tau}_i} = 1 \text{ и } \tilde{\tau}_i \in E^n.\}$, $V'' = \{\tilde{\tau}_i | f_{\tilde{y}}^{\tilde{\tau}_i} = 0 \text{ и } \tilde{\tau}_i \in E^n\}$.

Второе слагаемое в правой части этой эквивалентности равно нулю, если функция f — четная, и единице, если f — нечетная. В первом случае правая часть эквивалентности уже имеет вид СПДНФ, а во втором случае:

$$f(\tilde{y}) = \sum_{\tilde{\tau}_i \in V'} (y_1^{\bar{\tau}_{i,1}} \vee \ldots \vee y_k^{\bar{\tau}_{i,k}}) \oplus \sum_{\tilde{\tau}_i \in E^k} (y_1^{\bar{\tau}_{i,1}} \vee \quad \ldots$$

$$\ldots \vee y_k^{\bar{\tau}_{i,k}}) = \sum_{\tilde{\tau}_i \in V''} (y_1^{\bar{\tau}_{i,1}} \vee \ldots \vee y_k^{\bar{\tau}_{i,k}}).$$

где $V' = \{\tilde{\tau}_i | f_{\tilde{y}}^{\tilde{\tau}_i} = 1 \text{ и } \tilde{\tau}_i \in E^n\}$, $V'' = \{\tilde{\tau}_i | f_{\tilde{y}}^{\tilde{\tau}_i} = 0 \text{ и } \tilde{\tau}_i \in E^n\}$. Получаем СПДНФ. Если обозначить $V' = \{\tilde{\tau}_i | f_{\tilde{y}}^{\tilde{\tau}_i} = 1 \text{ и } \tilde{\tau}_i \in E^n\}$, $V'' = \{\tilde{\tau}_i | f_{\tilde{y}}^{\tilde{\tau}_i} = 0 \text{ и } \tilde{\tau}_i \in E^n\}$, то вычислительная формула для СПДНФ имеет вид

$$f(\tilde{y}) = \begin{cases} \sum\limits_{\tilde{\tau}_i \in V'} (y_1^{\tilde{\tau}_{i,1}} \vee \ldots \vee y_k^{\tilde{\tau}_{i,k}}), & \text{если } f \text{ — четная;} \\ \sum\limits_{\tilde{\tau}_i \in V''} (y_1^{\tilde{\tau}_{i,1}} \vee \ldots \vee y_k^{\tilde{\tau}_{i,k}}), & \text{если } f \text{ — нечетная.} \end{cases}$$

Единственность СПДНФ очевидна. □

В доказательствах предложений 1.8–1.11 получены формулы для нахождения совершенных нормальных форм по векторному представлению функций.

Сокращенная дизъюнктивная нормальная форма (сокращенная ДНФ). Терм вида $y_{i_1}^{\sigma_{i_1}} \cdot \ldots \cdot y_{i_s}^{\sigma_{i_s}}$, $(i_1, \ldots, i_s \in \tilde{n}, i_1 < \ldots < i_s)$ будем называть *элементарной конъюнкцией* от множества переменных $\tilde{y} = y_1, \ldots, y_n$.

Очевидно, что полные элементарные конъюнкции являются элементарными конъюнкциями.

Импликантой функции $f(\tilde{y})$ называется элементарная конъюнкция K от $\tilde{y}$ такая, что $K \vee f = f$. Несложно понять, что элементарная конъюнкция $K \equiv y_{i_1}^{\sigma_{i_1}} \cdot \ldots \cdot y_{i_s}^{\sigma_{i_s}}$ является импликантой функции $f(\tilde{y})$ тогда и только тогда, когда $f_{y_{i_1}, \ldots, y_{i_s}}^{\sigma_{i_1}, \ldots, \sigma_{i_s}} = 1$. Импликанта $K \equiv y_{i_1}^{\sigma_{i_1}} \cdot \ldots \cdot y_{i_s}^{\sigma_{i_s}}$ функции f называется *простой*, если для любого $l (l \in \tilde{s})$ элементарная конъюнкция $y_{i_1}^{\sigma_{i_1}} \cdot \ldots \cdot y_{i_{l-1}}^{\sigma_{i_{l-1}}} \cdot y_{i_{l+1}}^{\sigma_{i_{l+1}}} \cdot \ldots \cdot y_{i_s}^{\sigma_{i_s}}$ не является импликантой f.

Терм Ф от множества переменных $\tilde{y} = y_1, \ldots, y_n$ называется *сокращенной дизъюнктивной нормальной формой* функции $f(\tilde{y})$, если он имеет вид $\Phi \equiv K_1 \vee \ldots \vee K_s$, где $K_1, \ldots, K_s$ — все простые импликанты функции f. Две сокращенные ДНФ будем считать равными, если они состоят из одинакового множества импликант.

Предложение 1.12. *Для класса R всех ненулевых функций сокращенная* ДНФ *является канонической формой.*

Доказательство. Покажем, что $f(\tilde{y})$ представима сокращенной ДНФ, т.е. $f = K_1 \vee \ldots \vee K_s$, где $K_1, \ldots, K_s$ это все простые импликанты f. Очевидно множество простых импликант непусто, если функция ненулевая. Для произ-

вольного набора $\tilde{\sigma}$, если $f(\tilde{\sigma}) = 0$, то для всех $i \in \tilde{s}$ в силу эквивалентности $K_i \vee f = f$ следует, что $K_i(\tilde{\sigma}) = 0$, а значит $K_1(\tilde{\sigma}) \vee \ldots \vee K_s(\tilde{\sigma}) = 0$. Если $f(\tilde{\sigma}) = 1$, то элементарная конъюнкция $K = y_1^{\sigma_1} \cdot \ldots \cdot y_n^{\sigma_n}$ является импликантой $f(\tilde{y})$. Если она не является простой, то какая-то $K_i = y_{i_1}^{\sigma_{i_1}} \cdot \ldots \cdot y_{i_s}^{\sigma_{i_s}}$, $i_1, \ldots, i_s \in \tilde{n}$ уже будет простой импликантой, причем $K_i(\tilde{\sigma}) = \sigma_{i_1}^{\sigma_{i_1}} \cdot \ldots \cdot \sigma_{i_s}^{\sigma_{i_s}} = 1$. Поэтому

$$K_1(\tilde{\sigma}) \vee \ldots \vee K_i(\tilde{\sigma}) \vee \ldots \vee K_s(\tilde{\sigma}) = 1.$$

Единственность сокращенной ДНФ непосредственно следует из ее определения, так как в дизъюнкцию входят все простые импликанты, а порядок для равенства сокращенных ДНФ не имеет значения. □

Терм Ф от множества переменных $\tilde{x}$, $|\tilde{x}| = n$, находится в *полиномиальной нормальной форме Жегалкина (*ПНФ *Жегалкина) по набору* $\tilde{\alpha}$ от множества переменных $\tilde{x}$, если он имеет вид $K_1 \oplus \ldots \oplus K_m$, где $K_1, \ldots, K_m$ — либо элементарные конъюнкции вида $x_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot x_{i_s}^{\alpha_{i_s}}$ $(i_1 < \ldots < i_s,\ i_1, \ldots, i_s \in \tilde{n})$, либо 1 и $K_i \neq K_j$ при $i \neq j$. ПНФ Жегалкина по единичному набору называем полиномом Жегалкина.

Предложение 1.13. *Для любого* $\tilde{\alpha}$, $|\tilde{\alpha}| = n$ ПНФ *Жегалкина по набору* $\tilde{\alpha}$ *для класса* R *всех ненулевых функций размерности* n *является канонической формой.*

Доказательство несложно получается с использованием СПКНФ. □

Наряду с введенными каноническими формами будет рассматриваться *полиномиальная нормальная форма* (ПНФ) от множества переменных $\tilde{y}$, которая является термом вида

$$K_1 \oplus \ldots \oplus K_s,$$

где K_i $(i \in \tilde{s})$ — элементарные коъюнкции от множества переменных $\tilde{y}$.

Комментарии. Многие результаты этой главы в настоящее время являются математическим фольклором. Отметим только, что критерии декомпозиции (теорема 1.2 и следствие к ней) восходят к работе Г.Н. Поварова [7]. Общая теорема о разложении булевых функций (теорема 1.3) по переменным принадлежит О.Б. Лупанову (см., например [2]).

Глава II

Бесповторные булевы функции

Бесповторные функции являются важным классом булевых функции и, помимо теоретического значения, применяются в математическом моделировании дискретных преобразователей информации. Эта глава посвящена характеризации бесповторных булевых функций, нахождению числа бесповторных булевых функций и описанию алгоритма нахождения бесповторного представления функций в бинарных базисных множествах.

§ 1. Бесповторные разложения

Терм от множества переменных $\tilde{x}$ называется *бесповторным*, если каждая переменная входит в него не более одного раза.

Булева функция f называется *бесповторной* в базисном множестве B, если найдется бесповторный терм Φ над B, представляющий функцию f.

Функцию назовем *разделимой*, если ее можно представить в виде суперпозиции двух неунарных функций с непересекающимися множествами переменных. В противном случае функция называется *неразделимой*.

Для любой разделимой функции осуществима разделительная декомпозиция, поэтому ее можно представить бесповторным термом над множеством неконстантных неразделимых функций. При этом оказывается, что такое представление в определенном смысле единственное. Строгой формулировке этого факта предпошлем определения и вспомогательное утверждение, которое имеет и самостоятельный интерес.

Функции f и g называются *однотипными*, если

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

где $i_1,\ldots,i_n$ — некоторая перестановка $1,\ldots,n$. В противном случае функции *неоднотипные*.

Очевидно, что отношение однотипности является отношением эквивалентности.

Пусть g — неразделимая функция ранга $m \geqslant 2$. Функция f называется *g-функцией*, если существуют функции $h_1, \ldots, h_m$ такие, что

$$f(\tilde{x}) = g(h_1(\tilde{x}_1), \ldots, h_m(\tilde{x}_m)),$$

где $\tilde{x}_1, \ldots, \tilde{x}_m$ — разбиение $\tilde{x}$.

Теорема 2.1. *Пусть g, h — неразделимые, неоднотипные функции ранга не меньше 2. Тогда $K_g \cap K_h = \varnothing$, где K_g — множество всех существенных g-функций, K_h — множество всех существенных h-функций.*

Доказательство. Предположим противное. Пусть $f \in K_g \cap K_h$. Тогда

$$f(\tilde{x}) = g(g_1(\tilde{x}_1), \ldots, g_m(\tilde{x}_m)) = h(h_1(\tilde{y}_1), \ldots, h_s(\tilde{y}_s)),$$

где $\tilde{x}_1, \ldots, \tilde{x}_m$ и $\tilde{y}_1, \ldots, \tilde{y}_s$ — разбиения переменных $\tilde{x}$.

Для определенности можно считать, что $m \geqslant s$.

Рассмотрим два случая.

1. Пусть существуют $x_1 \in \tilde{x}_1, \ldots, x_m \in \tilde{x}_m$ такие, что все они лежат в разных классах разбиения $\tilde{y}_1, \ldots, \tilde{y}_s$. Отсюда следует, что $m = s$.

В частности, при $m = 2$ такие x_1, x_2 заведомо существуют.

По предложению о существенном аргументе существует остаточная функция по всем остальным аргументам такая, что

$$f^{\tilde{\sigma}}_{\tilde{x}\setminus\{x_1,\ldots,x_m\}} = g(x_1^{\sigma_1}, \ldots, x_m^{\sigma_m}) \text{ для некоторых } \sigma_1, \ldots, \sigma_m.$$

С другой стороны

$$f^{\tilde{\sigma}}_{\tilde{x}\setminus\{x_1,\ldots,x_m\}} = h(x_{i_1}^{\alpha_{i_1}}, \ldots, x_{i_m}^{\alpha_{i_m}}),$$

для некоторых $\alpha_{i_1}, \ldots, \alpha_{i_m}$, где $i_1, \ldots, i_m$ — перестановка элементов $1, \ldots, m$.

Отсюда получаем противоречие с неоднотипностью функций g и h.

2. Если условие первого пункта не выполняется, то существуют $x_1 \in \tilde{x}_1, \ldots, x_m \in \tilde{x}_m$ такие, что как минимум две из этих переменных попали в один класс разбиения $\tilde{y}_1, \ldots, \tilde{y}_s$, и все $x_1, \ldots, x_m$ лежат не в одном классе разбиения $\tilde{y}_1, \ldots, \tilde{y}_s$.

Тогда, по предложению о существенном аргументе существует остаточная функция от всех остальных аргументов такая, что для некоторых $\sigma_1, \ldots, \sigma_m$ выполняется

$$f^{\tilde{\sigma}}_{\tilde{x}\setminus\{x_1,\ldots,x_m\}} = g(x_1^{\sigma_1}, \ldots, x_m^{\sigma_m}).$$

С другой стороны $f^{\tilde{\sigma}}_{\tilde{x}\setminus\{x_1,\ldots,x_m\}} = h(h_1^\diamond, \ldots, h_s^\diamond)$, где $h_i^\diamond$ — соответствующие остаточные функции от h_i. Так как среди функций $h_1^\diamond, \ldots, h_s^\diamond$ как минимум две — неконстантные, причем как минимум одна из них ранга не меньше двух, получаем противоречие с неразделимостью функции g. □

Замечание. Отметим, что любая функция ранга 2 однотипна либо конъюнкции, либо дизъюнкции, либо сложению, что непосредственно следует из тождеств эквивалентности. В силу этого часто ограничиваются рассмотрением среди таких функций только функций, эквивалентных $\cdot, \vee, \oplus$. В дальнейшем мы также в основном будем использовать эти функции.

Термы Φ и Ψ над базисным множеством B назовем *близкими* и обозначим это как $\Phi \simeq \Psi$, если существует последовательность термов $\Phi_1, \ldots, \Phi_m$ такая, что $\Phi \equiv \Phi_1, \Psi \equiv \Phi_m$ и Φ_{k+1} получается из Φ_k $(k \in \{1, \ldots, m-1\})$ применением одного из следующих тождеств близости:

1) $f(x_1, \ldots, x_i, \ldots, x_n) \simeq g(x_1, \ldots, \bar{x}_i, \ldots, x_n)$ для всех функций f, g таких, что $f(x_1, \ldots, x_i, \ldots, x_n) = g(x_1, \ldots, \bar{x}_i, \ldots, x_n)$;

2) $f(x_1, \ldots, x_n) \simeq \bar{g}(x_1, \ldots, x_n)$ для всех функций f, g таких, что $f(x_1, \ldots, x_n) = \bar{g}(x_1, \ldots, x_n)$;

3) $f(x_1, \ldots, x_n) \simeq g(x_{i_1}, \ldots, x_{i_n})$ для всех функций f, g таких, что $f(x_1, \ldots, x_n) = g(x_{i_1}, \ldots, x_{i_n})$, где $i_1, \ldots, i_n$ — перестановка чисел $1, \ldots, n$;

4) $f(f(x,y),z) \simeq f(x, f(y,z))$, для всех бинарных функций f таких, что $f(f(x,y),z) = f(x, f(y,z))$.

Замечание. Применение тождеств близости к терму определяется аналогично применению тождеств эквивалентности.

Теорема 2.2. *Бесповторные термы от более чем одной переменной над множеством неконстантных неразделимых функций эквивалентны тогда и только тогда, когда они являются близкими.*

Доказательство. ($\Leftarrow$). Доказательство в эту сторону очевидно, так как тождества 1)–4) по определению сохраняют эквивалентность термов.

($\Rightarrow$). Пусть Φ и Ψ — бесповторные термы и $\Phi = \Psi$; отсюда $\chi(\Phi) = \chi(\Psi)$. Доказательство теоремы в эту сторону проведем индукцией по числу $|\chi(\Phi)|$.

Базис индукции при $|\chi(\Phi)| = 2$ очевидно выполняется.

Шаг индукции. В силу тождества 2) можно считать, что внешней функцией терма не является отрицание. Пусть

$$\Phi \equiv g(\Phi_1, \ldots, \Phi_s),\ \Psi \equiv h(\Psi_1, \ldots, \Psi_m) \text{ и } s \geqslant 2,\ m \geqslant 2.$$

Так как g и h неразделимы, то по теореме 2.1 они являются однотипными, следовательно $s = m$.

Рассмотрим отдельно случаи $s \geqslant 3$ и $s = 2$.

1. Пусть $g(\Phi_1(\tilde{x}_1), \ldots, \Phi_s(\tilde{x}_s)) = h(\Psi_1(\tilde{y}_1), \ldots, \Psi_s(\tilde{y}_s))$, где $\tilde{x}_1, \ldots, \tilde{x}_s$ и $\tilde{y}_1, \ldots, \tilde{y}_s$ — разбиения множества переменных $\tilde{x}$ и $s \geqslant 3$.

Во-первых, эти разбиения совпадают. Действительно, если не совпадают, то существуют переменные $x_{i_1} \in \tilde{x}_1, \ldots, x_{i_s} \in \tilde{x}_s$ такие, что по крайней мере две из них принадлежат одному классу разбиения $\tilde{y}_1, \ldots, \tilde{y}_s$, и как минимум две принадлежат разным классам разбиения $\tilde{y}_1, \ldots, \tilde{y}_s$. По лемме о существенном аргументе по всем остальным переменным существует остаточная функция такая, что в силу $\Phi = \Psi$ выполняется $g(x_{i_1}^{\sigma_{i_1}}, \ldots, x_{i_s}^{\sigma_{i_s}}) \leftarrow h(\Psi_1^\circ, \ldots, \Psi_s^\circ)$, где Ψ_i° — остаточные от Ψ_i.

Так как все переменные в получившейся остаточной функции существенные, то получается противоречие с неразделимостью g.

Во-вторых, покажем, что для любого $i \in \{1, \ldots, s\}$ существует α_i такое, что $\Phi_i = (\Psi_j)^{\alpha_i}$, где терм Ψ_j такой, что $\chi(\Psi_j) = \tilde{x}_i$. Действительно, по предложению о существенном аргументе существуют $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{i-1}, \tilde{\sigma}_{i+1}, \ldots, \tilde{\sigma}_s, \alpha_i$ такие, что

$$\Phi_{\tilde{x}_1, \ldots, \tilde{x}_{i-1}, \tilde{x}_{i+1}, \ldots, \tilde{x}_s}^{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{i-1}, \tilde{\sigma}_{i+1}, \ldots, \tilde{\sigma}_s} = (\Phi_i)^{\alpha_i}(\tilde{x}_i).$$

С другой стороны, так как $\tilde{x}_i$ — существенные в этом остаточном терме, то должны быть существенными и в эквивалентном ему терме, поэтому

$$(h(\Psi_1(\tilde{y}_1), \ldots, \Psi_s(\tilde{y}_s)))_{\tilde{x}_1, \ldots, \tilde{x}_{i-1}, \tilde{x}_{i+1}, \ldots, \tilde{x}_s}^{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{i-1}, \tilde{\sigma}_{i+1}, \ldots, \tilde{\sigma}_s} = (\Psi_j)^{\beta_i}(\tilde{x}_i)$$

для некоторого β_i. Отсюда $\Phi_i(\tilde{x}_i) = (\Psi_j)^{\alpha_i \oplus \beta_i}(\tilde{x}_i)$.

В итоге получим $g(\Phi_1, \ldots, \Phi_s) = h((\Phi_{j_1})^{\alpha_{j_1}}, \ldots, (\Phi_{j_s})^{\alpha_{j_s}})$, где $(j_1, \ldots, j_s)$ — перестановка $(1, \ldots, s)$.

По предложению о существенном аргументе существуют переменные $x_{i_1} \in \tilde{x}_1, \ldots, x_{i_s} \in \tilde{x}_s$ такие, что имеет место эквивалентность $g(x_{i_1}^{\beta_{i_1}}, \ldots, x_{i_s}^{\beta_{i_s}}) = h(x_{l_1}^{\gamma_{l_1}}, \ldots, x_{l_s}^{\gamma_{l_s}})$, где $(i_1, \ldots, i_s)$ и $(l_1, \ldots, l_s)$ — перестановки $(1, \ldots, s)$.

В силу тождеств близости 1), 3) и предположения индукции для термов $\Phi_1(\tilde{x}_1), \ldots, \Phi_s(\tilde{x}_s)$, так как они от меньшего числа переменных, получаем $\Phi \simeq \Psi$.

2. Пусть $s = 2$. В силу 1), 2) можно перейти к близким термам, все бинарные функции в которых либо конъюнкция, либо дизъюнкция, либо сложение. А так как g и h — однотипные, то при этом получаем $g = h$.

Так как $\cdot, \vee, \oplus$ ассоциативны, то термы Φ, Ψ запишем в виде $\Phi = g(\Phi_1(\tilde{x}_1), \ldots, \Phi_s(\tilde{x}_s)), \Psi = g(\Psi_1(\tilde{y}_1), \ldots, \Psi_s(\tilde{y}_m))$, в силу тождеств близости 4), а $g(z_1, \ldots, z_n)$ — обозначение для функции $g(z_1, g(z_2, \ldots, g(z_{n-1}, z_n) \ldots))$, $g \in \{\cdot, \vee, \oplus\}$, причем термы Φ_i, Ψ_j уже не представляют g-функции.

Покажем, во-первых, что разбиения переменных $\tilde{x}_1, \ldots, \tilde{x}_s$ и $\tilde{y}_1, \ldots, \tilde{y}_m$ совпадают. Предположим противное, что существует $\tilde{x}_i$, который пересекается с не менее чем двумя множествами $\tilde{y}_{j_1}, \tilde{y}_{j_2}$, т.е. $\tilde{x}_i = \tilde{y}_1^\circ \cup \ldots \cup \tilde{y}_m^\circ$, где $\tilde{y}_j^\circ \subseteq \tilde{y}_j$. Тогда существует остаточный терм по $\tilde{x}_1, \ldots, \tilde{x}_{i-1}, \tilde{x}_{i+1}, \ldots, \tilde{x}_s$ такой, что

$$\Phi^{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{i-1}, \tilde{\sigma}_{i+1}, \ldots, \tilde{\sigma}_s}_{\tilde{x}_1, \ldots, \tilde{x}_{i-1}, \tilde{x}_{i+1}, \ldots, \tilde{x}_s} = \Phi_i(\tilde{x}_i).$$

С другой стороны,

$$\Psi^{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{i-1}, \tilde{\sigma}_{i+1}, \ldots, \tilde{\sigma}_s}_{\tilde{x}_1, \ldots, \tilde{x}_{i-1}, \tilde{x}_{i+1}, \ldots, \tilde{x}_s} = g(\Psi_1(\tilde{y}_1^\circ, \tilde{\sigma}_1^\circ), \ldots, \Psi_m(\tilde{y}_m^\circ, \tilde{\sigma}_m^\circ)).$$

Отсюда получаем, что

$$\Phi_i(\tilde{x}_i) = g(\Psi_1^\circ(\tilde{y}_1^\circ), \ldots, \Psi_m^\circ(\tilde{y}_m^\circ))$$

где $\Psi_r^\circ(\tilde{y}_r^\circ) = \Psi_r(\tilde{y}_r^\circ, \tilde{\sigma}_r^\circ)$, $r \in \tilde{m}$.

Так как по крайней мере два набора $\tilde{y}_{j_1}^\circ$ и $\tilde{y}_{j_2}^\circ$ не пустые, то получаем, что Φ_i представляет g-функцию, что противоречит построению разложения.

Далее рассуждения полностью аналогичны тем, что были в пункте 1. □

§ 2. Бесповторные функции в элементарном базисном множестве

Легко заметить, что неконстантная функция является бесповторной в элементарном базисном множестве тогда и только тогда, когда она представляется бесповторным термом над B_0 с использованием отрицания только над переменными.

Предложение 2.1 (о свойствах бесповторных функций в базисном множестве B_0). *Пусть f — бесповторная неунарная функция в базисном множестве B_0. Тогда f обладает следующими свойствами:*

1) *для любого аргумента $x \in \rho(f)$ выполняется ровно одно из условий: либо $\delta(f) \subset \delta(f_x^0)$, либо $\delta(f) \subset \delta(f_x^1)$;*

2) *для любого $x \in \rho(f)$ множество аргументов $\{x\} \cup \delta(f_x^0) \cup \cup \delta(f_x^1)$ является выделимым в f;*

3) *для любого x существуют функции g, h и константы σ, τ такие, что либо $f_x^\sigma = g(\tilde{u}, h(\tilde{v}))$, либо $f_x^{\bar{\sigma}} = g(\tilde{u}, \tau)$, где $\tilde{u}, \tilde{v}$ разбиение множества $\chi(f) \setminus \{x\}$;*

4) *если функция f существенная, то она нечетная.*

Доказательство. Проведем доказательство пунктов 1) и 2) в случае, когда функция f является существенной, это не ограничивает общности рассуждений, но зато упрощает изложение.

Доказательство проводится индукцией по глубине $d(\Phi)$ бесповторного терма Φ, представляющего f.

Базис индукции при $d(\Phi) = 2$ легко проверяется. Действительно, в $f(x_1, x_2) = (x_1^{\sigma_1} \cdot x_2^{\sigma_2})^\tau$ остаточная $f_{x_i}^{\bar{\sigma}_i}$ будет иметь фиктивную переменную и множество $\{x_1, x_2\}$ будет выделимым.

Шаг индукции. Так как функция $f(\tilde{y}, \tilde{z})$ бесповторная в B_0, то она представляется в виде

$$f(\tilde{y}, \tilde{z}) = (h^{\sigma_1}(\tilde{y}) \cdot g^{\sigma_2}(\tilde{z}))^\tau,$$

где $h(\tilde{y})$ — бесповторная, а $g(\tilde{z})$ — неунарная, бесповторная в B_0 функции.

Пусть $h(\tilde{y})$ — неунарная функция. Тогда если переменная $x \in \tilde{y}$, то обе остаточные функции по переменной x от функции g будут существенными функциями и h_x^γ будет несущественной

функцией, а $h_x^{\bar{\gamma}}$ — существенной функцией (константа γ существует по индуктивному предположению). Тогда f_x^{γ} будет несущественной функцией, а $f_x^{\bar{\gamma}}$ — существенной остаточной функцией и множество переменных $\{x\}\cup\delta(h_x^{\gamma})$ выделимо в f, так как оно выделимо в h.

Теперь пусть $h = x$ является унарной функцией. Тогда $f(x,\tilde{z}) = (x^{\sigma_1}\cdot g^{\sigma_2}(\tilde{z}))^{\tau}$. Теперь все переменные из $\tilde{z}$ фиктивны в $f_x^{\sigma_1}$, и множество переменных $\{x\}\cup\tilde{z}$ выделимо в f. Для переменных из $\tilde{z}$ доказательство аналогично доказательству в случае неунарных функций. Этим закончили доказательсто пунктов 1) и 2).

Пункт 3) выполняется из пункта 2) по критерию разделительной декомпозиции.

Пункт 4) легко доказать индукцией по рангу функции f с использованием пункта 3), так как несущественная функция всегда является четной. □

Булева функция называется *вырожденной*, если эквивалентная ей существенная функция является четной.

Булева функция f называется *жесткой*, если она неунарная, и существует аргумент $x\in\rho(f)$, такой, что выполняются равенства $\delta(f)=\delta(f_x^0)=\delta(f_x^1)$.

Булева функция f называется *строго нежесткой*, если для любого аргумента $x\in\rho(f)$ либо $\delta(f)\neq\delta(f_x^0)$, либо $\delta(f)\neq\delta(f_x^1)$ или она унарная.

Булева функция g называется *недиффузной*, если любая простая импликанта K функции g имеет одну общую переменную с любой простой импликантой J функции $\bar{g}$, т.е. $|\chi(K)\cap\chi(J)|=1$.

Теорема 2.3 (критерий бесповторности в B_0). *Для любой булевой функции f равносильны следующие условия*:

1) f — *бесповторная в* B;
2) f — *недиффузная*;
3) f — *наследственно нежесткая*;
4) f — *наследственно строго нежесткая*;
5) f — *наследственно невырожденная*.

Доказательство. 1) $\Rightarrow$ 2). Обозначим через $\mathcal{K}(f)$ множество всех простых импликант функции f. Вначале докажем вспомогательное утверждение: если для неконстантных функций $f(\tilde{x})$ и $g(\tilde{y})$ выполняется $\rho(f)\cap\rho(g)=\varnothing$ и $K_1\in\mathcal{K}(f)$,

а $K_2 \in \mathcal{K}(g)$, то $K_1K_2 \in \mathcal{K}(fg)$; и наоборот, если $K \in \mathcal{K}(fg)$, то найдутся $K_1 \in \mathcal{K}(f)$ и $K_2 \in \mathcal{K}(g)$ такие, что $K_1 \cdot K_2 = K$.

По определению $K_1 \vee f = f$, $K_2 \vee g = g$. Следовательно,

$$gf = K_1 \cdot K_2 \vee g \cdot K_1 \vee f \cdot K_2 \vee f \cdot g = K_1 \cdot K_2 \vee g \cdot K_1 \vee (K_2 \vee g) \cdot f = \\ = K_1 \cdot K_2 \vee g \cdot K_1 \vee f \cdot g = K_1 \cdot K_2 \vee f \cdot g.$$

Значит, $K_1 \cdot K_2$ — импликанта функции $f \cdot g$. Докажем, что $K_1 \cdot K_2$ это простая импликанта. Допустим противное: пусть существуют импликанты K_1' и K_2', такие что $K_1' \cdot K_1 = K_1$, $K_2' \cdot K_2 = K_2$ и $K_1' \cdot K_2'$ импликанта fg. По определению $K_1' \cdot K_2' \vee f \cdot g = f \cdot g$. По крайней мере одна из импликант K_1', K_2' не равна соответственно K_1, K_2. Пусть $K_1' \neq K_1$. Тогда найдется такая подстановка констант $\tilde{\sigma}$ вместо всех переменных $\tilde{y}$, что $(K_2')_{\tilde{y}}^{\tilde{\sigma}} = 1$ и $g_{\tilde{y}}^{\tilde{\sigma}} = 1$. Тогда $K_1' \vee f = f$, т.е. K_1' — импликанта f, что противоречит предположению о том, что K_1 — простая импликанта.

Докажем вторую часть утверждения. Пусть $\rho(f) \cap \rho(g) = \varnothing$, $K \in \mathcal{K}(f \cdot g)$. K можно разбить на произведение $K = K_1 \cdot K_2$, так что $\chi(K_1) \subseteq \rho(f)$, $\chi(K_2) \subseteq \rho(g)$:

$$K_1 \cdot K_2 \vee f \cdot g = (K_1 \cdot K_2 \vee f)(K_1 \cdot K_2 \vee g) = f \cdot g.$$

Допустим, существует набор $\tilde{\sigma}$, такой что $K_1(\tilde{\sigma}) \vee f(\tilde{\sigma}) \neq f(\tilde{\sigma})$, т.е. $K_1(\tilde{\sigma}) = 1$, $f(\tilde{\sigma}) = 0$. Тогда $K_2 \cdot (K_2 \vee g) = 0$. Значит, $K_2 = 0$, $K_1 \cdot K_2 = 0$, $K = 0$, что невозможно. Таким образом, K_1 — импликанта функции f. Аналогично, K_2 — импликанта функции g.

Пусть хотя бы одна из импликант K_1, K_2 не является простой. Тогда существуют простые импликанты K_1', K_2', такие что $K_1' \cdot K_1 = K_1$, $K_2' \cdot K_2 = K_2$. Тогда из доказанного $K_1' \cdot K_2'$ является импликантой $f \cdot g$, что противоречит предположению о том, что K является простой импликантой $f \cdot g$.

Теперь переходим к доказательству основного утверждения, которое проведем индукцией по $n = \operatorname{rang} f$.

Базис индукции. Пусть $n = 1$, т.е. $\rho(f) = \{x\}$. Тогда множество $\mathcal{K}(f) = \{x^\sigma\}$, а $\mathcal{K}(\bar{f}) = \{x^{\bar{\sigma}}\}$. Так как существует только одна $K \in \mathcal{K}(f)$ и только одна $M \in \mathcal{K}(\bar{f})$, то $|\chi(K) \cap \chi(M)| = 1$, и функция недиффузная.

Шаг индукции. Пусть для всех $k < n$ все бесповторные функции ранга k являются недиффузными, и $f(\tilde{u})$ — бесповторная в B_0 функция ранга n.

Если $K \in \mathcal{K}(f)$ и $M \in \mathcal{K}(\bar{f})$ — произвольные импликанты соответствующих функций, то в силу бесповторности f в B_0, возможны два случая:

1) существует g, h, такие что $f = h \vee g$ и $K \in \mathcal{K}(h)$;

2) существует g, h, такие что $\bar{f} = h \vee g$ и $K \in \mathcal{K}(h)$,

где $\rho(h) \cap \rho(g) = \varnothing$.

Очевидно, что эти случаи являются симметричными, поэтому ограничимся рассмотрением первого случая. Очевидно, что $\bar{f} = \bar{h} \cdot \bar{g}$.

Тогда, из доказанного выше утверждения, $M = M_1 \cdot M_2$, где $M_1 \in \mathcal{K}(\bar{h})$, $M_2 \in \mathcal{K}(\bar{g})$. Для h выполнено предположение индукции, значит $|\chi(K) \cap \chi(M_1)| = 1$. Тогда

$$|\chi(K) \cap \chi(M)| = |\chi(K) \cap (\chi(M_1) \cup \chi(M_2))| =$$
$$= |(\chi(K) \cap \chi(M_1)) \cup (\chi(K) \cap \chi(M_2))| = |\chi(K) \cap \chi(M_1)| = 1.$$

2) $\Rightarrow$ 3). Предварительно докажем следующее утверждение.

Пусть для любых простых импликант $K \in \mathcal{K}(f)$ и $M \in \mathcal{K}(\bar{f})$ выполняется условие: $|\chi(K) \cap \chi(M)| = 1$. Тогда любая переменная x входит в простые импликанты функции f только в одной степени σ, а в простые импликанты функции $\bar{f}$ только в степени $\bar{\sigma}$.

Пусть $x \in \chi(K) \cap (\chi(M))$. Тогда

$$\bar{f} \cdot f = (M \vee \bar{f})(K \vee f) = K \cdot M \vee K \cdot \bar{f} \vee M \cdot f \vee \bar{f} \cdot f = 0.$$

Отсюда следует, что $K \cdot M = 0$. Так как простые импликанты K и M имеют ровно одну общую переменную x, то x входит в K в степени σ, а в M в степени $\bar{\sigma}$. Импликанты K и M выбирались произвольно, значит x входит в простые импликанты функции f только в одной степени σ, а в простые импликанты $\bar{f}$ только в степени $\bar{\sigma}$.

Теперь переходим непосредственно к доказательству основного утверждения. Доказательство проведем индукцией по размерности функции.

Базис индукции. Справедливость утверждения при $n = 2$ проверяется непосредственно.

Шаг индукции. Если f — несущественная функция, то по индуктивному предположению f — наследственно нежесткая функция. Теперь пусть f — существенная функция. Покажем, что для любого аргумента x по крайней мере одна из остаточных f_x^0, f_x^1 является несущественной функцией.

В силу доказанного выше утверждения сокращенная ДНФ функции f представляется в виде

$$f = xK_1 \vee \ldots \vee xK_m \vee S_1 \vee \ldots \vee S_l,$$

где $x \notin \chi(K_i)$, $x \notin \chi(S_i)$. Тогда $\bar{f}$ представляется в виде

$$\begin{aligned}\bar{f} &= (\bar{x} \vee \bar{K}_1) \cdot \ldots \cdot (\bar{x} \vee \bar{K}_m)\bar{S}_1 \cdot \ldots \cdot \bar{S}_l = \\ &= \bar{x}(D_1 \vee \ldots \vee D_t) \vee (M_1 \vee \ldots \vee M_g)(D_1 \vee \ldots \vee D_t) = \\ &= \bar{x}(D_1 \vee \ldots \vee D_t) \vee M_1 D_1 \vee \ldots \vee M_q D_t,\end{aligned}$$

где D_i — импликанты сокращенной ДНФ функции $\bar{K}_1 \cdot \ldots \cdot \bar{K}_m$, а M_i — импликанты сокращенной ДНФ функции $\bar{S}_1 \cdot \ldots \cdot \bar{S}_l$. Эти импликанты могут быть получены опусканием отрицаний до переменных, раскрытием скобок по дистрибутивности и сокращением по тождеству поглощения.

Если $\operatorname{rang}(S_1 \vee \ldots \vee S_l) < n-1$, то f_x^0 — несущественная, так как $f_x^0 = S_1 \vee \ldots \vee S_l$. Пусть $\operatorname{rang}(S_1 \vee \ldots \vee S_l) = n-1$. Если $\chi(K_1) = \varnothing$, то $f_x^1 = 1$, и f_x^1 — несущественная. Пусть $K_1 \neq 1$. Существует S_r такая, что $K_1 \cdot S_r = S_r$ и $\chi(S_r) \neq \varnothing$, иначе возникает противоречие с определением недиффузности f. Поэтому $K_1 \cdot S_r = S_r$ и $\chi(S_r) \neq \varnothing$, иначе xK_1 и K_1 не могли бы входить в сокращенную ДНФ для f.

Пусть $u \in \chi(S_r')$. Так как во все $M_i \cdot L_j$ входит одна переменная из K_1, то u не может входить во все $M_i \cdot L_j$, иначе возникает противоречие с недиффузностью f. Поэтому элементарные конъюнкции, содержащие u, не будут входить в множество всех простых импликант для $\bar{f}$, не содержащих x.

Получили, что переменная $u \notin \rho(\bar{f}_x^1)$. Так как

$$f_x^1 = (K_1 \vee \ldots \vee K_m) \vee (S_1 \vee \ldots \vee S_l),$$

то f_x^1 — несущественная. С учетом выбора переменной x получаем, что f — нежесткая.

Так как в остаточных ДНФ для остаточных функций f все переменные входят в одной и той же степени, то обобщенное

склеивание

$$yK_1 \vee \bar{y}K_2 = yK_1 \vee \bar{y}K_2 \vee K_1K_2$$

не применимо. Значит, для получения сокращенной ДНФ достаточно применять поглощение, т.е. все простые импликанты содержатся в остаточных ДНФ. При этом $f_{x_1}^{\sigma_1} = h_1$, $f_{x_1}^{\bar{\sigma}_1} = g_2 \vee h_2$ и для элементарной конъюнкции, входящей в h_1 и в $g_2(h_2)$ имеют пересечения по одной переменной, и для $f_{x_1}^{\bar{\sigma}_1} = g_1 \vee h_1$, $f_{x_1}^{\sigma_1} = h_2$ элементарные конъюнкции удовлетворяют этому свойству. В итоге получаем, что $f_{x_1}^0$ и $f_{x_1}^1$ — недиффузные функции. Тогда в силу индуктивного предположения $f_{x_1}^0$ и $f_{x_1}^1$ — наследственно нежесткие функции; следовательно и f — наследственно нежесткая функция.

3) $\Rightarrow$ 4). Доказательство проведем индукцией по рангу функции f.

Базис индукции. Унарная функция по определению является строго нежесткой.

Шаг индукции. Так как f — наследственно нежесткая функция, то $\delta(f) \subset \delta(f_x^0)$ или $\delta(f) \subset \delta(f_x^1)$. Предположим, что выполняются оба эти условия. Введем обозначения $\tilde{v} = \delta(f_x^0) \setminus \delta(f)$, $\tilde{w} = \delta(f_x^1) \setminus \delta(f)$ и $\tilde{u} = \rho(f) \setminus (\tilde{v} \cup \tilde{w})$. Очевидно, что $\tilde{v} \cap \tilde{w} = \varnothing$. Рассмотрим два случая.

a. Если выполняется хотя бы одно из условий: $|\tilde{u}| \geqslant 1$, $|\tilde{v}| \geqslant 2$, $|\tilde{w}| \geqslant 2$), то для остаточной функции по аргументу y из одного из множеств $\tilde{u}, \tilde{v}, \tilde{w}$, для которого выполняется указанное условие, получаем $\delta(f_y^\sigma) \subset \delta(f_{y,x}^{\sigma,0})$ и $\delta(f_y^\sigma) \subset \delta(f_{y,x}^{\sigma,1})$. Так как f — наследственно нежесткая функция, то и f_y^σ — наследственно нежесткая, и по индуктивному предположению f_y^σ — наследственно строго нежесткая, что неверно, так как оба эти условия не могут выполняться одновременно.

b. Если $|\tilde{u}| = 0$ и $|\tilde{v}| = |\tilde{w}| = 1$, то $f = \bar{x}f_x^0 \vee xf_x^1 = \tilde{x}w^\sigma \vee xv^\tau$, где $w \in \tilde{w}$ и $v \in \tilde{v}$. Получаем, что $f_w^\sigma = \tilde{x} \vee v^\tau$ и $f_w^{\bar{\sigma}} = xv^\tau$, и $\delta(f) = \delta(f_w^0) = \delta(f_w^1)$, что противоречит нежесткости f.

В итоге получаем, что может выполниться ровно одно из условий: либо $\delta(f) \subset \delta(f_x^0)$, либо $\delta(f) \subset \delta(f_x^1)$. Так как по индуктивному предположению функции f_x^0 и f_x^1 являются наследственно строго нежесткими, то функция f также будет наследственно строго нежесткой.

(4 $\Rightarrow$ 5). Доказательство проведем индукцией по рангу функции f.

Базис индукции. Унарная функция по определению является невырожденной.

Шаг индукции. Пусть функция f — неунарная, наследственно строго нежесткая. Тогда одна остаточная функция является существенной, и по индуктивному предположению невырожденной, поэтому нечетной. Вторая остаточная функция — несущественная, а значит — четная. Поэтому функция f является нечетной.

В итоге получаем, что f — невырожденная функция, а любая ее остаточная функция — наследственно невырожденная по индуктивному предположению, значит функция f является наследственно невырожденой.

(5 $\Rightarrow$ 3). Доказательство проведем индукцией по рангу f.

Базис индукции. Унарные функции по определению нежесткие.

Шаг индукции. Пусть f — неунарная наследственно невырожденная функция, тогда f является нечетной и для любого существенного аргумента x одна из остаточных функций f_x^σ является четной, а другая — нечетной. Функция f_x^σ является наследственно невырожденной и четной, тогда она имеет фиктивный аргумент, а значит f является нежесткой.

Из индуктивного предположения следует, что функция f — наследственно нежесткая.

4) $\Rightarrow$ 1). Доказательство проведем индукцией по размерности функции f.

Базис индукции. Унарные функции, очевидно, бесповторны в базисном множестве B_0.

Шаг индукции. Будем считать, что функция f — существенная, иначе из индуктивного предположения сразу следует, что f — бесповторная функция.

Докажем следующее утверждение. Для любой функции f, если в остаточной функции f_x^σ фиктивен аргумент y и в остаточной функции f_y^τ фиктивен аргумент z, то в остаточной функции f_x^σ фиктивен аргумент z. Если y фиктивен в f_x^σ, то выполняется равенство $f_{x,y}^{\sigma,0} = f_{x,y}^{\sigma,1}$, а значит выполняются и равенства $f_{x,y,z}^{\sigma,0,0} = f_{x,y,z}^{\sigma,1,0}$ и $f_{x,y,z}^{\sigma,0,1} = f_{x,y,z}^{\sigma,1,1}$. Если z фиктивен в f_y^τ, то выполняется равенство $f_{y,z}^{\tau,0} = f_{y,z}^{\tau,1}$, а значит выполняются и равенства $f_{x,y,z}^{0,\tau,0} = f_{x,y,z}^{0,\tau,1}$ и $f_{x,y,z}^{1,\tau,0} = f_{x,y,z}^{1,\tau,1}$. Отсюда

$f^{\sigma,0,0}_{x,y,z} = f^{\sigma,0,1}_{x,y,z} = f^{\sigma,1,0}_{x,y,z} = f^{\sigma,1,1}_{x,y,z}$. Тогда z фиктивен в функции f^{σ}_{x}.

Из строгой нежесткости функции f следует, что для любого аргумента $x \in \rho(f)$ существует константа σ, такая что функция f^{σ}_{x} — несущественная, а $f^{\bar{\sigma}}_{x}$ — существенная. Тогда найдется набор аргументов $\tilde{x} = x_1, \ldots, x_k$ и констант $\tilde{\sigma} = \sigma_1, \ldots, \sigma_k$, таких что $x_2 \in \delta(f^{\sigma_1}_{x_1}), x_3 \in \delta(f^{\sigma_2}_{x_2}), \ldots, x_k \in \delta(f^{\sigma_{k-1}}_{x_{k-1}}), x_1 \in \delta(f^{\sigma_k}_{x_k})$; при этом для всех x_i выполняется $\tilde{x} \in \delta(f^{\sigma_i}_{x_i})$.

Докажем, что для всех наборов $\tilde{\tau} = \tau_1, \ldots, \tau_k$, кроме набора $\bar{\sigma}_1, \ldots, \bar{\sigma}_k$, выполняется равенство: $f^{\tilde{\tau}}_{\tilde{x}} = f^{\tilde{\sigma}}_{\tilde{x}}$. Найдется такой индекс i, что $\tau_i = \sigma_i$. Поэтому для $\tilde{\tau}' = \tau_1, \ldots, \tau_{i-1}, \tau_{i+1}, \ldots, \tau_k$ и $\tilde{\sigma}' = \sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_k$ выполняется $(f^{\tau_i})^{\tilde{\tau}'}_{\tilde{x}} = (f^{\tau_i})^{\tilde{\sigma}'}_{\tilde{x}}$, так как $\tilde{x} = \delta(f^{\tau_i}_{x_i})$, что доказывает утверждение.

Получили, что среди остаточных по $\tilde{u}$ функций есть всего лишь две различных. Обозначим их через f_1 и f_2. Тогда, по критерию разделительной декомпозиции, получаем

$$f(\tilde{v}, \tilde{u}) = g(\tilde{v}, h(\tilde{u})),$$

где функции g и h определяются так:

$$g(\tilde{v}, z) = \bar{z} f_1(\tilde{w}) \vee z f_2(\tilde{w}), \quad h(\tilde{\tau}) = \begin{cases} 0, & \text{если } f^{\tilde{\tau}}_{\tilde{u}} = f_1, \\ 1, & \text{если } f^{\tilde{\tau}}_{\tilde{u}} = f_2. \end{cases}$$

Заметим, что функции $g(\tilde{v}, z)$ и $h(\tilde{u})$ являются остаточными от функции f, а значит, по индуктивному предположению, бесповторны в B_0. Суперпозиция бесповторных функций с разделенными переменными также является бесповторной функцией, т.е. f бесповторна в B_0. □

§ 3. Бесповторные функции в бинарном базисном множестве

Как и в случае элементарного базисного множества в бинарном базисном множестве неконстантная функция является бесповторной тогда и только тогда, когда она представима бесповторным термом над B_1 с использованием отрицания только для переменных.

Для функции f определяем *сопряженную* по аргументу x функцию f^{∇}_{x} следующим образом:

$$f^{\nabla}_{x} = \overline{x} \cdot (f^0_x \cdot f^1_x) \vee x \cdot (f^0_x \vee f^1_x).$$

Предложение 2.2 (о свойствах бесповторных функций в базисном множестве B_1). *Для неунарной функции f — бесповторной в базисном множестве B_1 — выполняются следующие свойства:*

1) *для любого $x \in \rho(f)$ либо $\delta(f) \in \delta(f_x^0)$, либо $\delta(f) \in \delta(f_x^1)$, либо $\delta(f) \in \delta(f_x^\nabla)$;*

2) *для любого $x \in \rho(f)$ множество аргументов $\{x\} \cup \delta(f_x^0) \cup \cup \delta(f_x^1) \cup \delta(f_x^\nabla)$ является выделимым в f;*

3) *для любого $x \in \rho(f)$ существуют функции g, h и константы σ, τ такие, что $f_x^\sigma = g(\tilde{u}, h(\tilde{v}))$ и либо $f_x^{\bar{\sigma}} = g(\tilde{u}, \tau)$, либо $f_x^{\bar{\sigma}} = g(\tilde{u}, \bar{h}(\tilde{v}))$;*

4) *если функция f является повторной в базисном множестве B_0, то f — четная функция.*

Доказательство. Проведем доказательство пунктов 1) и 2) в случае, когда функция f является существенной. Это не ограничивает общности рассуждений, но зато упрощает изложение.

Доказательство проводится индукцией по глубине $d(\Phi)$ бесповторного терма Φ, представляющего f.

Базис индукции. Справедливость утверждения при $d(\Phi) = 2$ легко проверяется.

Шаг индукции. Пусть функции $f(\tilde{y})$, $g(\tilde{z})$ реализуются бесповторными термами. Ровно одна из функций f_y^0, f_y^1, f_y^∇ и ровно одна из g_z^0, g_z^1, g_z^∇ являются несущественными, причем по аргументам y (соответственно z) и фиктивным аргументам f (соответственно g) существует ровно две различные остаточные функции от f (соответственно g). Покажем что эти свойства будут выполняться для любой функции h, представимой одним из следующих термов: $\overline{f}(\tilde{y}), f(\tilde{y}) \cdot g(\tilde{z}), f(\tilde{y}) \vee g(\tilde{z}), f(\tilde{y}) \oplus g(\tilde{z})$.

Подсчитаем для каждого случая остаточные и сопряженную функции по переменной $y \in \tilde{y}$:

для случая $h(\tilde{y}) = \overline{f}(\tilde{y})$ получаем $h_y^\sigma = \overline{f}_y^\sigma$, $h_y^\nabla = \overline{y} \cdot (\overline{f}_y^0 \cdot \overline{f}_y^1) \vee \vee y \cdot (\overline{f}_y^0 \vee \overline{f}_y^1) = \overline{y} \cdot \overline{(f_y^0 \vee f_y^1)} \vee y \cdot \overline{(f_y^0 \cdot f_y^1)}$;

для случая $h(\tilde{y}, \tilde{z}) = f(\tilde{y}) \cdot g(\tilde{z})$ получаем $h_y^\sigma = f_y^\sigma \cdot g$, $h_y^\nabla = \overline{y} \cdot ((f_y^0 \cdot g) \cdot (f_y^1 \cdot g)) \vee y \cdot ((f_y^0 \cdot g) \vee (f_y^1 \cdot g)) = f_y^\nabla \cdot g$;

для случая $h(\tilde{y}, \tilde{z}) = f(\tilde{y}) \vee g(\tilde{z})$ имеем $h_y^\sigma = f_y^\sigma \vee g$, $h_y^\nabla = \overline{y} \cdot ((f_y^0 \vee g) \cdot (f_y^1 \vee g)) \vee y \cdot ((f_y^0 \vee g) \vee (f_y^1 \vee g)) = f_y^\nabla \vee g$;

для случая $h(\tilde{y},\tilde{z}) = f(\tilde{y}) \oplus g(\tilde{z})$ получаем $h_y^\sigma = f_y^\sigma \oplus g$, $h_y^\nabla = f_y^\nabla \oplus g\overline{((f_y^0 \vee f_y^1) \oplus (f_y^0 \cdot f_y^1))}$, $f_y^\nabla = h_y^\nabla \oplus g\overline{((h_y^0 \vee h_y^1) \oplus (h_y^0 \cdot h_y^1))}$.

Из этих равенств следует, что остаточные и сопряженная функции h существенные тогда и только тогда, когда такими являются соответствующие функции f, причем необходимое условие о числе остаточных функций также выполняется. По аргументам z доказательство полностью аналогичное. Отсюда следует выполнимость пункта 1). Так как среди остаточных функций только две различные, то из этого следует выполнимость пункта 2).

Пункт 3) выполняется в силу того, что каждая переменная входит в бесповторный терм одним из трех способов: либо $x_i^{\sigma_i} \cdot h(y)$, либо $x_i^{\sigma_i} \vee h(y)$, либо $x_i^{\sigma_i} \oplus h(y)$. Пункт 4) является непосредственным следствием пункта 3), если учитывать, что существенная неконстантная функция, бесповторная в базисном множестве B_0 является нечетной. □

Булеву неунарную функцию f называем *плотной*, если для некоторого существенного аргумента x выполняются равенства $\delta(f) = \delta(f_x^0) = \delta(f_x^1) = \delta(f_x^\nabla)$.

Назовем функцию *строго неплотной*, если для любого аргумента $x \in \rho(f)$ либо $\delta(f) \neq \delta(f_x^0)$, либо $\delta(f) \neq \delta(f_x^1)$, либо $\delta(f) \neq \delta(f_x^\nabla)$ или она унарная функция.

Теорема 2.4 (критерий бесповторности в B_1). *Следующие условия для любой булевой функции f равносильны:*

1) *f — бесповторная в B_1;*

2) *f — наследственно неплотная;*

3) *f — наследственно строго неплотная.*

Доказательство. 1) ⇒ 2). Пусть функция f реализуется бесповторным термом. Тогда она является неплотной, а значит и наследственно неплотной, так как любая остаточная функция f, очевидно, также реализуется бесповторным термом.

2) ⇒ 3). Доказательство будем проводить индукцией по $\dim f$.

Базис индукции при $n = 1$ тривиален.

Шаг индукции. По индуктивному предположению все наследственно неплотные функции менее чем от n аргументов реализуются бесповторными термами. Пусть функция $f(x_1, \ldots, x_n)$ наследственно неплотная, причем существенная, иначе по ин-

дуктивному предположению она сразу реализуется бесповторным термом.

Зафиксируем произвольно аргумент x_i и докажем, что ровно одна из функций $f^0_{x_i}$, $f^1_{x_i}$, $f^{\nabla}_{x_i}$ является несущественной.

По определению неплотности одна из этих функций заведомо будет несущественной. Покажем, что несущественность любых двух из них приведет к противоречию.

Пусть $f^0_{x_i}$ и $f^1_{x_i}$ — несущественные функции. Очевидно множества их фиктивных аргументов не пересекаются, иначе f была бы несущественной. Переобозначим аргументы f следующим образом: $x_1 = x_i$, $\tilde{y}$ — набор фиктивных аргументов функции $f^0_{x_i}$, $\tilde{z}$ — набор фиктивных аргументов функции $f^1_{x_i}$, $\tilde{v}$ — остальные аргументы.

Если вектор $\tilde{v}$ размерности больше нуля или векторы $\tilde{y}$ или $\tilde{z}$ размерности больше единицы, то для остаточной функции по одному аргументу из соответствующего вектора остаточные функции по x_i будут также несущественными. С другой стороны, остаточные функции являются наследственно неплотными и по индуктивному предположению реализуются бесповторными термами, а значит только одна из остаточных и сопряженной функций несущественная. Получили противоречие. Осталось рассмотреть случай, когда вектор $\tilde{v}$ размерности 0, а векторы $\tilde{y}$ или $\tilde{z}$ размерности 1, т.е. $f = f(x_1, y_1, z_1)$.

Покажем, что функции $f^0_{y_1}$, $f^1_{y_1}$, $f^{\nabla}_{y_1}$ будут существенными. Рассмотрим функцию $f^0_{y_1}$. Аргумент x_1 — существенный, иначе $f(0,0,z_1) = f(1,0,z_1)$ и получим, что в $f^0_{x_1}$ — фиктивный аргумент z_1, что не так. Аргумент z_1 — существенный в $f^0_{y_1}$, иначе $f(x_1,0,0) = f(x_1,0,1)$ и получаем также, что у функции $f^0_{x_1}$ аргумент z_1 — фиктивный. Функция $f^1_{y_1}$ рассматривается аналогично.

У функции $f^{\nabla}_{y_1}$ аргументы x_1 и y_1 являются существенными. В противном случае имеем

$$f(1,0,z_1) \cdot f(1,1,z_1) = f(1,0,z_1) \vee f(1,1,z_1).$$

Тогда $f(1,0,z_1) = f(1,1,z_1)$ и получили противоречие. Аргумент z_1 — существенный, иначе получаем

$$f(0,0,0) \cdot f(0,1,0) = f(0,0,1) \cdot f(0,1,1),$$

и отсюда $f(0,0,0) = f(0,0,1)$, т.е. у функции $f^0_{x_1}$ аргумент z_1 является фиктивным, что не так.

Получили, что функции $f^0_{y_1}$, $f^1_{y_1}$, $f^\nabla_{y_1}$ — существенные, а это противоречит наследственной неплотности f.

Пусть функции $f^0_{x_i}$ и $f^\nabla_{x_i}$ — несущественные. Множества их фиктивных аргументов не пересекаются, иначе в силу тождества

$$f = f^0_{x_i} \oplus x_i \cdot (f^0_{x_i} \oplus f^1_{x_i}) = f^0_{x_i} \oplus x_i \cdot (f^0_{x_i} \cdot f^1_{x_i} \oplus (f^0_{x_i} \vee f^1_{x_i}))$$

функция f была бы несущественной.

Как и в предыдущем случае переобозначим аргументы функции f: $x_1 = x_i$, $\tilde{y}$ — набор фиктивных аргументов функции $f^0_{x_i}$, $\tilde{z}$ — набор фиктивных аргументов функции $f^\nabla_{x_i}$, $\tilde{v}$ — остальные аргументы. Рассуждая аналогично, достаточно рассмотреть только случай $f = f(x_1, y_1, z_1)$.

Рассмотрим функцию $f^0_{y_1}$. Аргумент x_1 — существенный, иначе $f(0,1,z_1) = f(0,0,z_1) = f(1,0,z_1) = f(0,0,z_1) \cdot f(1,0,z_1)$ и мы получаем, что в $f^0_{x_1}$ аргумент z_1 является фиктивным, что не так. Аргумент z_1 будет существенным в функции $f^0_{y_1}$, иначе $f(x_1,0,0) = f(x_1,0,1)$ и мы получаем, что в $f^0_{x_1}$ аргумент z_1 — фиктивный, что не так. Функция $f^1_{y_1}$ рассматривается аналогично.

Осталось рассмотреть функцию $f^\nabla_{y_1}$. Аргументы x_1 и y_1 — существенные, иначе выполняется условие

$$f(1,0,z_1) \cdot f(1,1,z_1) = f(1,0,z_1) \vee f(1,1,z_1),$$

отсюда $f(1,0,z_1) = f(1,1,z_1)$, что не так. Аргумент z_1 — существенный, иначе

$$f(0,0,0) \cdot f(0,1,0) = f(0,0,1) \cdot f(0,1,1),$$

отсюда $f(0,0,0) = f(0,0,1)$ и мы получаем, что в $f^0_{x_1}$ аргумент z_1 — фиктивный, что не так.

Получается противоречие с наследственной неплотностью функции f.

Случай когда $f^1_{x_i}$ и $f^\nabla_{x_i}$ — несущественные, рассматривается аналогично предыдущему.

3) $\Rightarrow$ 1). В силу того, что ровно одна из функций $f^0_{x_i}$, $f^1_{x_i}$, $f^\nabla_{x_i}$ имеет фиктивные аргументы, однозначно определяется следующее переименование аргументов функции $f(\tilde{x})$: $\tilde{y}$ —такой

вектор, что $y_1 = x_i$, а остальные компоненты — фиктивные аргументы либо $f^0_{x_i}$, либо $f^1_{x_i}$, либо $f^\nabla_{x_i}$; $\tilde{z}$ — вектор остальных аргументов f.

Если при таком переименовании размерность вектора $\tilde{z}$ равна нулю, то либо $f^\sigma_{x_i} = 0$, либо $f^\sigma_{x_i} = 1$, либо $f^\nabla_{x_i} = x_i$. В этих случаях, соответственно, имеем представления либо $f = \overline{x}^\sigma_i \cdot \overline{f}^\sigma_{x_i}$, либо $f = x^\sigma_i \vee \overline{f}_{x^\sigma_i}$, либо $f = x_i \oplus f^0_{x_i}$. Применяя индуктивное предположение к остаточным функциям по x_i получим реализацию f бесповторным термом.

Пусть вектор $\tilde{z}$ ненулевой размерности. Покажем, что $f(\tilde{y}, \tilde{z})$ содержит ровно две различные остаточные по $\tilde{y}$ функции.

Отдельно рассмотрим случай, когда размерность вектора $\tilde{y}$ равна 2. Так как функция f — неплотная, то ровно одна из функций $f^0_{y_1}$, $f^1_{y_1}$, $f^\nabla_{y_1}$ является несущественной с фиктивным аргументом y_2 и ровно одна из функций $f^0_{y_2}, f^1_{y_2}, f^\nabla_{y_2}$ также несущественная, причем с единственным фиктивным аргументом y_1. Действительно, это не сложно показать. Рассмотрим наиболее сложный случай: $f^\nabla_{y_1}$ и $f^\nabla_{y_2}$ — несущественные. Пусть в $f^\nabla_{y_2}$ есть отличный от y_1 фиктивный аргумент z, тогда он фиктивен и в

$$f(0,0,\tilde{z}) \cdot f(0,1,\tilde{z}) \text{ и } f(1,0,\tilde{z}) \cdot f(1,1,\tilde{z}),$$

а значит и в их конъюнкции

$$f(0,0,\tilde{z}) \cdot f(1,0,\tilde{z}) \cdot f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z}).$$

В силу фиктивности y_2 в $f^\nabla_{y_1}$ выполняется тождество

$$f(0,0,\tilde{z}) \cdot f(1,0,\tilde{z}) = f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z}).$$

Поэтому получаем

$$f(0,0,\tilde{z}) \cdot f(1,0,\tilde{z}) \cdot f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z}) =$$

$$= f(0,0,\tilde{z}) \cdot f(1,0,\tilde{z}) = f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z}),$$

и z фиктивен в $f(0,0,\tilde{z}) \cdot f(1,0,\tilde{z})$ и в $f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z})$. Аналогично получаем, что z фиктивен в $f(0,0,\tilde{z}) \vee f(1,0,\tilde{z})$ и в $f(0,1,\tilde{z}) \vee f(1,1,\tilde{z})$). Поэтому z фиктивен в $f^\nabla_{y_1}$, но в $f^\nabla_{y_1}$ единственным фиктивным аргументом является y_2. Получили противоречие.

Для завершения рассмотрения этого случая нужно разобрать следующие 9 вариантов.

Пусть функции $f^0_{y_1}$ и $f^0_{y_2}$ — несущественные (варианты, когда $f^0_{y_1}$ и $f^1_{y_2}$, $f^1_{y_1}$ и $f^0_{y_2}$, $f^1_{y_1}$ и $f^1_{y_2}$ — несущественные функции, рассматриваются аналогично). Тогда получаем

$$f(0,1,\tilde{z}) = f(0,0,\tilde{z}) = f(1,0,\tilde{z}).$$

Пусть функции $f^\nabla_{y_1}$ и $f^0_{y_2}$ — несущественные (варианты, когда $f^1_{y_1}$ и $f^\nabla_{y_2}$, $f^0_{y_1}$ и $f^\nabla_{y_2}$, $f^\nabla_{y_1}$ и $f^1_{y_2}$ — несущественные функции рассматриваются аналогично). Тогда выполняются тождества

$$f(0,0,\tilde{z}) \cdot f(1,0,\tilde{z}) = f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z}),$$

$$f(0,0,\tilde{z}) \vee f(1,0,\tilde{z}) = f(0,1,\tilde{z}) \vee f(1,1,\tilde{z}), f(0,0,\tilde{z}) = f(1,0,\tilde{z}).$$

Отсюда получаем

$$f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z}) = f(0,0,\tilde{z}) = f(0,1,\tilde{z}) \vee f(1,1,\tilde{z}),$$

т.е. $f(0,1,\tilde{z}) = f(1,1,\tilde{z})$. В итоге имеем только две остаточные функции по $\tilde{y}$.

Пусть функции $f^\nabla_{y_1}$ и $f^\nabla_{y_2}$ — несущественные. Тогда выполняются тождества

$$f(0,0,\tilde{z}) \cdot f(1,0,\tilde{z}) = f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z}),$$
$$f(0,0,\tilde{z}) \vee f(1,0,\tilde{z}) = f(0,1,\tilde{z}) \vee f(1,1,\tilde{z})$$

и

$$f(0,0,\tilde{z}) \cdot f(0,1,\tilde{z}) = f(1,0,\tilde{z}) \cdot f(1,1,\tilde{z}),$$
$$f(0,0,\tilde{z}) \vee f(0,1,\tilde{z}) = f(1,0,\tilde{z}) \vee f(1,1,\tilde{z}).$$

Взяв конъюкцию первого тождества с $f(0,1,\tilde{z})$ и учитывая третье тождество, получаем

$$f(1,0,\tilde{z}) \cdot f(1,1,\tilde{z}) = f(0,1,\tilde{z}) \cdot f(1,1,\tilde{z}).$$

Аналогично, из второго и четвертого тождеств получаем

$$f(1,0,\tilde{z}) \vee f(1,1,\tilde{z}) = f(0,1,\tilde{z}) \vee f(1,1,\tilde{z}).$$

Отсюда $f(0,1,\tilde{z}) = f(1,0,\tilde{z})$.

Учитывая при этом первоначальные два тождества, также получаем $f(0,0,\tilde{z}) = f(1,1,\tilde{z})$. В силу этих тождеств имеем только две остаточные функции по $\tilde{y}$.

Пусть теперь размерность вектора $\tilde{y}$ не меньше 3, и предположим противное, т.е. что различных остаточных по $\tilde{y}$ функций больше двух. При этом возможны только следующие два случая.

1. Существуют наборы $\tilde{\sigma},\tilde{\tau},\tilde{\gamma}$ такие, что $f(\tilde{\sigma},\tilde{z})$, $f(\tilde{\tau},\tilde{z})$, $f(\tilde{\gamma},\tilde{z})$ попарно не равны и при этом $\sigma_j = \tau_j = \gamma_j$ хотя бы для одного индекса j. Тогда остаточная функция $f_{y_i}^{\sigma_i}$ также содержит три остаточные функции по $\tilde{y}$. С другой стороны по индуктивному предположению она реализуется бесповторным термом и, по выше доказанному, имеет только две остаточные функции по $\tilde{y}$. Получили противоречие.

2. Существуют противоположные наборы $\tilde{\sigma}$ и $\tilde{\tau}$ такие, что остаточные функции $f(\tilde{\sigma},\tilde{z})$, $f(\tilde{\tau},\tilde{z})$ не равны, а все остальные остаточные функции $f(\tilde{\gamma},\tilde{z})$ равны между собой. Тогда $f_{y_1}^0, f_{y_1}^1$ — существенные функции, а значит $f_{y_1}^{\nabla}$ — несущественная. Отсюда получаем

$$f(\tilde{\sigma},\tilde{z}) \cdot f(\tilde{\gamma},\tilde{z}) = f(\tilde{\gamma},\tilde{z}) = f(\tilde{\sigma},\tilde{z}) \vee f(\tilde{\sigma},\tilde{z}),$$

поэтому $f(\tilde{\sigma},\tilde{z}) = f(\tilde{\sigma},\tilde{z})$, что противоречит предположению о том, что остаточных функций по $\tilde{y}$ не менее трех.

Доказали, что остаточных по аргументам $\tilde{y}$ различных функций имеется две. Введем для них следующие обозначения: $f^{\diamond}(\tilde{z}) = f(\tilde{0},\tilde{z})$ и $f^{\sharp}(\tilde{z}) \neq f(\tilde{0},\tilde{z})$.

Теперь, по критерию разделительной декомпозиции, функцию f можно представить в виде: $f(\tilde{y},\tilde{z}) = f_0(f_1(\tilde{y}),\tilde{z})$, где функции $f_0(w,\tilde{z})$ и $f_1(\tilde{y})$ определяются так:

$$f_0(w,\tilde{z}) = \overline{w}\cdot f^{\diamond}(\tilde{z}) \vee w \cdot f^{\sharp}(\tilde{z}),\ f_1(\tilde{\sigma}) = \begin{cases} 0, & \text{если } f(\tilde{\sigma},\tilde{z}) = f^{\diamond}(\tilde{z}), \\ 1, & \text{если } f(\tilde{\sigma},\tilde{z}) = f^{\sharp}(\tilde{z}). \end{cases}$$

Действительно, для произвольного набора $\tilde{\sigma}$ остаточная функция $f(\tilde{\sigma},\tilde{z})$ равна либо $f^{\diamond}(\tilde{z})$, либо $f^{\sharp}(\tilde{z})$. В первом случае получаем тождества

$$f_0(f_1(\tilde{\sigma}),\tilde{z}) = f_0(0,\tilde{z}) = f^{\diamond}(\tilde{z}) = f(\tilde{\sigma},\tilde{z}),$$

а во втором тождества

$$f_0(f_1(\tilde{\sigma}),\tilde{z}) = f_0(1,\tilde{z}) = f^{\sharp}(\tilde{z}) = f(\tilde{\sigma},\tilde{z}).$$

Покажем, что функции $f_0(w, \tilde{z})$ и $f_1(\tilde{y})$ будут наследственно неплотными. Существуют два соседних набора $\tilde{\sigma} \leqslant \tilde{\tau}$ таких, что $f(\tilde{\sigma}, \tilde{z}) = f^{\diamond}(\tilde{z})$ и $f(\tilde{\tau}, \tilde{z}) = f^{\natural}(\tilde{z})$. Для переменной y_i, на которой эти наборы различаются, получаем $f_1(\sigma_1, \ldots, y_i, \ldots, \sigma_m) = y_i$, отсюда

$$f(\sigma_1, \ldots, y_i, \ldots, \sigma_m, \tilde{z}) = f_0(f_1(\sigma_1, \ldots, y_i, \ldots, \sigma_m), \tilde{z}) = f_0(\tilde{y}, \tilde{z}),$$

а значит $f_0(v, \tilde{z})$ — наследственно неплотная как остаточная функция f. Существует набор $\tilde{\tau}$ такой, что $f^{\diamond}(\tilde{\tau}) \neq f^{\natural}(\tilde{\tau})$, поэтому выполняются тождества:

$$f_1(\sigma) = 0 = f^{\diamond}(\tilde{\tau}) \oplus f^{\diamond}(\tilde{\tau}) = f(\tilde{\sigma}, \tilde{\tau}) \oplus f^{\diamond}(\tilde{\tau}) = f^{\gamma}(\tilde{\sigma}, \tilde{\tau})$$

и

$$f_1(\tilde{\sigma}) = 1 = f^{\natural}(\tilde{\tau}) \oplus f^{\diamond}(\tilde{\tau}) = f(\tilde{\sigma}, \tilde{\tau}) \oplus f^{\diamond}(\tilde{\tau}) = f^{\gamma}(\tilde{\sigma}, \tilde{\tau}),$$

где $\gamma = \overline{f}^{\diamond}(\tilde{\sigma})$. Теперь функция $f_1(\tilde{y})$ — наследственно неплотная как остаточная функция f, если $\gamma = 1$, или как отрицание остаточной функции f, если $\gamma = 0$.

Следующие рассуждения заканчивают доказательство теоремы. По индуктивному предположению функции $f_0(w, \tilde{z})$ и $f_1(\tilde{y})$ реализуются бесповторными термами $F_0(w, \tilde{z})$ и $F_1(\tilde{y})$. В силу представления $f(\tilde{y}, \tilde{z}) = f_0(f_1(\tilde{y}), \tilde{z})$ получаем реализацию функции $f(\tilde{y}, \tilde{z})$ бесповторным термом $F_0(F_1(\tilde{y}), \tilde{z})$, что и требовалось. □

§ 4. Алгоритм нахождения бесповторных представлений

В ряде теоретических и практических приложений необходимо уметь находить бесповторные представления конкретных булевых функций. В этом параграфе будет описан алгоритм, позволяющий эффективно получать такие представления для элементарного и бинарного базисных множеств, основанный на соответствующих критериях бесповторности, полученных в предыдущих параграфах.

Алгоритм является рекурсивным, на вход подается существенная булева функция $f(\tilde{u})$, зависящая не менее чем от одного аргумента, на выходе получаем бесповторный терм $\Phi(\tilde{u})$, представляющий функцию f. В том случае, если функция не

допускает бесповторного представления, алгоритм заканчивает работу с сообщением о недопустимости бесповторного представления заданной функции в бинарном базисном множестве. Алгоритм позволяет не только найти бесповторное представление заданной функции, но и определить, в каком из бинарных базисных множеств функция является бесповторной. Если исходная функция содержит фиктивные переменные, то необходим дополнительный шаг, состоящий в удалении фиктивных переменных.

Перейдем к описанию алгоритма.

A. Если функция является одноместной, т.е. $\tilde{u} = x_i$, то $\Psi(x_i) = x_i$ или $\Psi(x_i) = \bar{x}_i$. Одноместная функция f не может быть константой, так как по условию f существенна.

B. К этому шагу переходим, если функция не является одноместной.

B.1. Выбираем переменную y из множества переменных $\tilde{u}$. Находим множества переменных $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$ по следующим формулам: $\tilde{u}_0 = \delta(f_y^0)$, $\tilde{u}_1 = \delta(f_y^1)$, $\tilde{u}_2 = \delta(f_y^\nabla)$. Если только одно из множеств $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$ непусто, то переходим к шагу B.2, иначе работа алгоритма заканчивается, так как функция не допускает бесповторной реализации ни в каком бинарном базисном множестве.

B.2a. К этому шагу переходим, если $\tilde{u}_0 \cup \{y\} = \tilde{u}$, т.е. f_y^0 — константная. Применив алгоритм к $f_y^1(\tilde{u}_0)$, найдем бесповторный терм $\Psi(\tilde{u}_0)$, представляющий функцию $f_y^1(\tilde{u}_0)$. Тогда искомый терм $\Phi(\tilde{u})$ будет определяться следующим образом:

$$\Phi(\tilde{u}) = (y \cdot (\Psi(\tilde{u}_0))^{\bar{\sigma}})^{\bar{\sigma}},$$

где $\sigma = f_y^0$.

B.2b. К этому шагу переходим, если $\tilde{u}_1 \cup \{y\} = \tilde{u}$, т.е. функция f_y^1 — константная. Применив алгоритм к $f_y^1(\tilde{u}_1)$, найдем бесповторный терм $\Psi(\tilde{u}_1)$, представляющий функцию $f_y^1(\tilde{u}_1)$. Тогда искомый терм $\Phi(\tilde{u})$ будет определяться следующим образом:

$$\Phi(\tilde{u}) = (y \vee (\Psi(\tilde{u}_1))^{\sigma})^{\sigma},$$

где $\sigma = f_y^1$.

B.2c. К этому шагу переходим, если $\tilde{u}_2 \cup \{y\} = \tilde{u}$. Применив алгоритм к $f_y^1(\tilde{u}_0)$, найдем бесповторный терм $\Psi(\tilde{u}_2)$, представляющий функцию $f_y^1(\tilde{u}_0)$. Тогда искомый терм $\Phi(\tilde{u})$ будет

определяться следующим образом:

$$\Phi(\tilde{u}) = y \oplus \Psi(\tilde{u}_2).$$

B.2d. Обозначим $\tilde{v} = \{y\} \cup \tilde{u}_0 \cup \tilde{u}_1 \cup \tilde{u}_2$ и $\tilde{w} = \tilde{u} \setminus \tilde{v}$. Этот шаг выполняется, если $\tilde{v}$ и $\tilde{w}$ оба не пусты. Среди остаточных функций $f_{\tilde{v}}^{\tilde{\tau}}$ найдем две различных. Обозначим их через $f_1(\tilde{w})$ и $f_2(\tilde{w})$. Если число различных остаточных функций будет другим, то работа алгоритма заканчивается, так как функция не допускает бесповторной реализации ни в каком бинарном базисном множестве.

Определим функции $g(\tilde{w}, z)$ и $h(\tilde{v})$ следующим образом:

$$g(\tilde{w}, z) = \bar{z} f_1(\tilde{w}) \vee z f_2(\tilde{w}), h(\tilde{\tau}) = \begin{cases} 0, & \text{если } f_{\tilde{v}}^{\tilde{\tau}} = f_1, \\ 1, & \text{если } f_{\tilde{v}}^{\tilde{\tau}} = f_2. \end{cases}$$

Теперь дважды применяем алгоритм для нахождения бесповторных термов, представляющих $g(\tilde{w}, z)$ и $h(\tilde{v})$. Получим соответственно термы $\Psi_g(\tilde{w}, z)$ и $\Psi_h(\tilde{v})$. Тогда искомый терм $\Phi(\tilde{w}, \tilde{v})$ будет определяться так:

$$\Phi(\tilde{w}, \tilde{v}) = \Psi_g(\tilde{w}, \Psi_h(\tilde{v})).$$

На этом описание алгоритма окончено.

Если в процессе выполнения, хотя бы однажды, на шаге B.1 множество переменных $\tilde{u}_2$ является непустым, то функция может иметь бесповторное представление только в бинарном базисном множестве, в противном случае достаточно элементарного базисного множества. Отрицания в полученном терме можно сделать тесными.

Далее будет доказано, что приведенный алгоритм является корректным. Под корректностью здесь понимается то, что при выполнении исходных условий алгоритм завершит работу. Если исходная функция имеет бесповторное представление в элементарном или бинарном базисном множестве, то одно из таких представлений будет найдено.

Теорема 2.5. *Алгоритм нахождения бесповторных представлений булевых функций в бинарном базисном множестве является корректным.*

Доказательство этой теоремы проведем индукцией по числу аргументов функции.

Базис индукции. Если функция зависит от одного аргумента, то выполняется шаг A, который, очевидно, является корректным.

Шаг индукции. Пусть для всех функций размерности меньше n алгоритм работает корректно. Рассмотрим выполнение шага B.1. По теореме 2.4, если функция является бесповторной в бинарном базисном множестве, то только один из векторов $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$ непуст. Таким образом, если это условие не выполняется, то исходная функция не является бесповторной, и этот шаг корректен.

Пусть выполняется шаг B.1a. Остаточная $f_y^1(\tilde{u}_0)$ не имеет фиктивных аргументов, так как на предыдущем шаге было наложено условие $\tilde{u}_1 = \varnothing$. Итак, рекурсивный вызов алгоритма является корректным. В силу индуктивного предположения терм $\Psi(\tilde{u}_0)$ представляет функцию $f_y^1(\tilde{u}_0)$ и выполняются следующие равенства:

$$((y \cdot (f_y^1(\tilde{u}_0))^{\bar{\sigma}})^{\bar{\sigma}})_y^0 = (0 \cdot (f_y^1(\tilde{u}_0))^{\bar{\sigma}})^{\bar{\sigma}} = 0^{\bar{\sigma}} = \sigma = f_y^0(\tilde{u}_0),$$

$$((y \cdot (f_y^1(\tilde{u}_0))^{\bar{\sigma}})^{\bar{\sigma}})_y^1 = (1 \cdot (f_y^1(\tilde{u}_0))^{\bar{\sigma}})^{\bar{\sigma}} = ((f_y^1(\tilde{u}_0))^{\bar{\sigma}})^{\bar{\sigma}} = f_y^1(\tilde{u}_0).$$

Таким образом, полученный терм действительно представляет функцию f, и по построению является бесповторным.

Корректность терма, получаемого на шаге B.1b. доказывается аналогично.

Пусть выполняется шаг B.1c. Если в функции $f_y^{\nabla}(\tilde{u})$ все переменные, кроме y, несущественны, то это означает, что существуют две константы σ_1 и σ_2 $(\sigma_1 \leqslant \sigma_2)$ такие, что для всех множеств $\tilde{\tau}$ выполняются равенства

$$f(0, \tilde{\tau}) \cdot f(1, \tilde{\tau}) = \sigma_1,$$
$$f(0, \tilde{\tau}) \vee f(1, \tilde{\tau}) = \sigma_2.$$

Если бы эти константы были равны, то вся функция f также была бы константой, что невозможно. Остается, что $\sigma_1 = 0$ и $\sigma_2 = 1$, т.е. для всех множеств $\tilde{\tau}$ выполняется равенство

$$f(0, \tilde{\tau}) = \bar{f}(1, \tilde{\tau}),$$

а значит выполняется и тождество

$$f(0, \tilde{u}_2) = \bar{f}(1, \tilde{u}_2).$$

Легко убедиться и в справедливости тождества

$$f(y, \tilde{u}_2) = y \oplus f(0, \tilde{u}_2).$$

Таким образом, используя индуктивное предположение, получаем, что терм, полученный на этом шаге, представляет функцию f, и является бесповторным по построению.

Остается проверить шаг B.1d. Из доказательства теоремы 2.4 следует, что множество переменных $\tilde{v}$ является выделимым, т.е. существует представление функции $f(\tilde{w}, \tilde{v})$ в виде $f(\tilde{w}, \tilde{v}) = g(\tilde{w}, h(\tilde{v}))$. Функции $g(\tilde{w}, z), h(\tilde{v})$ являются существенными, так как в противном случае, если бы одна из этих функций содержала фиктивные аргументы, то эти же аргументы были бы фиктивными и в $f(\tilde{w}, \tilde{v})$, что неверно. По критерию разделительной декомпоцизии среди остаточных по выделимому множеству аргументов найдется не более двух различных. Все остаточные по выделимому множеству $\tilde{v}$ не могут быть равными, так как в этом случае переменные из $\tilde{v}$ будут фиктивными, что неверно. Из доказательства теоремы 2.4 следует, что для функций g и h, построенных в соответствии с алгоритмом, выполняется тождество

$$f(\tilde{v}, \tilde{w}) = g(\tilde{w}, h(\tilde{v})).$$

Отсюда, с использованием индуктивного предположения получаем, что терм, полученный на этом шаге представляет функцию f и, по построению, является бесповторным. □

Нахождение бесповторнго терма, представляющего функцию по приведенному алгоритму продемонстрируем на следующем примере:

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = (10011001\ 10010000\ 10011001\ 10010000\ 00000000\ 00001001\ 10011001\ 10010000)$$

Каждый рекурсивный вызов алгоритма будет нумероваться и описываться отдельно.

Вызов алгоритма 1.

B.1. Находим функции $f^0_{x_1}$, $f^1_{x_1}$, $f^{\nabla}_{x_1}$ и множества переменных $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$:

$$p_0(x_2, x_3, x_4, x_5, x_6) = f^0_{x_1}(x_2, x_3, x_4, x_5, x_6) = (10011001\ 10010000\ 10011001\ 10010000) = p_0(x_3, x_4, x_5, x_6) = (10011001\ 10010000),\ \tilde{u}_0 = \{x_2\};$$

$f_1(x_2,x_3,x_4,x_5,x_6) = f^1_{x_2}(x_2,x_3,x_4,x_5,x_6) =$
$= (00000000\ 00001001\ 10011001\ 10010000),\ \tilde{u}_1 = \varnothing;$

$f_2(x_1,x_2,x_3,x_4,x_5,x_6) = f^{\nabla}_{x_1}(x_1,x_2,x_3,x_4,x_5,x_6) = (00000000\ 00$
$000000\ 10011001\ 10010000\ 10011001\ 10011001\ 10011001\ 10010000),$

$\tilde{u}_2 = \varnothing.$

Переходим к шагу B.2d, так как множество переменных $\tilde{u}_0$ не пустое и остаточная функция $f^0_{x_1}$ не равна константе.

B.2d. Находим множества переменных $\tilde{v}, \tilde{w}$.

$$\tilde{v} = \{x_1, x_2\}, \tilde{w} = \{x_3, x_4, x_5, x_6\}.$$

Вычисляем остаточные функции f по переменным x_1, x_2:

$$f_1(\tilde{w}) = (10011001\ 10010000),\ f_2(\tilde{w}) = (00000000\ 00001001).$$

Находим функции g и h:

$$g(z_1,\tilde{w}) = (10011001\ 10010000\ 00000000\ 00001001),\ h(\tilde{v}) = (0010).$$

Применяем алгоритм к функции $g(z_1,\tilde{w})$ (вызов 2), получаем терм

$$\Psi_g(z_1,\tilde{w}) = \overline{(z_1 \oplus x_3x_4) \vee \overline{(x_5 \oplus \bar{x}_6)}}.$$

Применяем алгоритм к функции $h(x_1,x_2)$ (вызов 9) получаем терм

$$\Phi_h(\tilde{v}) = x_1\bar{x}_2.$$

В итоге получаем ответ

$$\Phi(\tilde{u}) = \overline{((x_1\bar{x}_2) \oplus x_3x_4) \vee \overline{(x_5 \oplus \bar{x}_6)}}.$$

Вызов алгоритма 2.

B.1. $f(z_1,x_3,x_4,x_5,x_6) =$
$= (10011001100100000000000000001001).$

Находим функции $f^0_{z_1}$, $f^1_{z_1}$, $f^{\nabla}_{z_1}$ и множества переменных $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$:

$f_0(x_3,x_4,x_5,x_6) = f^0_{z_1}(x_3,x_4,x_5,x_6) =$
$= (1001100110010000), \tilde{u}_0 = \varnothing$

$$f_1(x_3,x_4,x_5,x_6)=f^1_{z_1}(x_3,x_4,x_5,x_6)=$$
$$=(0000000000001001),\tilde{u}_1=\varnothing$$

$$f_2(z_1,x_3,x_4,x_5,x_6)=f^{\nabla}_{z_1}(z_1,x_3,x_4,x_5,x_6)=$$
$$=(00000000\ 00000000\ 10011001\ 10011001)=$$
$$=f_2(z_1,x_5,x_6)=(00001001),\tilde{u}_2=\{x_3,x_4\}$$

Переходим к шагу B.2d, так как вектор переменных $\tilde{u}_0$ не пустой и остаточная $f^0_{z_1}$ не равна константе.

B.2d. Находим векторы переменных $\tilde{v},\tilde{w}$:

$$\tilde{v}=\{z_1,x_3,x_4\},\tilde{w}=\{x_5,x_6\}.$$

Вычисляем остаточные функции f по переменным z_1,x_3,x_4:

$$f_1(x_5,x_6)=(1001),\ \ f_2(x_5,x_6)=(0000).$$

Находим функции g и h:

$$g(z_2,x_5,x_6)=(10010000),\ \ h(z_1,x_3,x_4)=(00011110).$$

Применяем алгоритм к функции $g(z_2,x_5,x_6)$ (вызов 3) и получаем терм $\Psi_g(z_2,x_5,x_6)=\overline{z_2\vee\overline{(x_5\oplus\bar{x}_6)}}$. Применив алгоритм к функции $h(z_1,x_3,x_4)$ (вызов 6), получили терм

$$\Phi_h(z_1,x_3,x_4)=z_1\oplus x_3x_4.$$

В итоге получаем ответ

$$\Phi(\tilde{u})=\overline{(z_1\oplus x_3x_4)\vee\overline{(x_5\oplus\bar{x}_6)}}.$$

Вызов алгоритма 3.

B.1. $f(z_2,x_5,x_6)=(10010000)$. Находим функции $f^0_{z_2}$, $f^1_{z_2}$, $f^{\nabla}_{z_2}$ и множества переменных $\tilde{u}_0,\tilde{u}_1,\tilde{u}_2$:

$$p_0(x_5,x_6)=f^0_{z_2}(x_5,x_6)=(1001),\ \ \tilde{u}_0=\varnothing,$$

$$p_1(x_5,x_6)=f^1_{z_2}(x_5,x_6)=0,\ \ \tilde{u}_1=\{x_5,x_6\},$$

$$p_2(z_2,x_5,x_6)=f^{\nabla}_{z_2}(z_2,x_5,x_6)=(00001001),\ \ \tilde{u}_2=\varnothing.$$

Переходим к шагу B.2b, так как вектор переменных $\tilde{u}_1$ не пустой и остаточная $f^1_{z_2}$ равна константе.

B.1b. Применяем алгоритм к $p_0(x_5, x_6) = f^0_{z_2} = (1001)$ (вызов 4) и получаем терм $\Psi(x_5, x_6) = x_5 \oplus \bar{x}_6$. В итоге имеем

$$\Phi(z_2, x_5, x_6) = \overline{z_2 \vee \overline{(x_5 \oplus \bar{x}_6)}}.$$

Вызов алгоритма 4.

B.1. $f(x_5, x_6) = (1001)$. Находим функции $f^0_{x_5}$, $f^1_{x_5}$, $f^\nabla_{x_5}$ и множества переменных $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$.

$$p_0(x_6) = f^0_{x_5}(x_6) = (10), \quad \tilde{u}_0 = \varnothing,$$

$$p_1(x_6) = f^1_{x_5}(x_6) = (01), \quad \tilde{u}_1 = \varnothing,$$

$$p_2(x_5, x_6) = f^\nabla_{x_5}(x_5, x_6) = (0011) = p_2(x_5) = (01), \quad \tilde{u}_2 = \{x_6\}.$$

Переходим к шагу B.2c, так как вектор переменных $\tilde{u}_2$ не пустой и $\tilde{u}_2 \cup \{x_5\} = \tilde{u}$.

B.2c. Применив алгоритм к функции $p_0(x_6) = f^0_{x_5} = (10)$ (вызов 5), получим терм $\Psi(x_6) = \bar{x}_6$. В итоге имеем

$$\Phi(x_5, x_6) = x_5 \oplus \bar{x}_6.$$

Вызов алгоритма 5.

A. $f(x_6) = (10)$. Так как функция одноместная, сразу получаем ответ

$$\Phi(x_6) = \bar{x}_6.$$

Вызов алгоритма 6.

B.1. $(f(z_1, x_3, x_4) = (00011110)$. Находим функции $f^0_{z_1}$, $f^1_{z_1}$, $f^\nabla_{z_1}$ и множества переменных $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$:

$$p_0(x_3, x_4) = f^0_{z_1}(x_3, x_4) = (0001), \quad \tilde{u}_0 = \varnothing,$$

$$p_1(x_3, x_4) = f^1_{z_1}(x_3, x_4) = (1110), \quad \tilde{u}_1 = \varnothing,$$

$$p_2(z_1, x_3, x_4) = f^\nabla_{z_1}(z_1, x_3, x_4) = (00001111). \quad \tilde{u}_2 = \{x_3, x_4\}.$$

Переходим к шагу *B.2c*, так как вектор переменных $\tilde{u}_2$ не пустой и $\tilde{u}_2 \cup \{x_5\} = \tilde{u}$.

B.2c. Применив алгоритм к $p_0(x_3, x_4) = f^0_{z_1} = (0001)$ (вызов 7), получим терм $\Psi(x_3, x_4) = x_3 x_4$. В итоге имеем

$$\Phi(z_1, x_3, x_4) = z_1 \oplus x_3 x_4.$$

Вызов алгоритма 7.

В.1. $f(x_3, x_4) = (0001)$ Находим функции $f^0_{x_3}$, $f^1_{x_3}$, $f^\nabla_{x_3}$ и множества переменных $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$:

$$p_0(x_4) = f^0_{x_3} = (00) = 0, \quad \tilde{u}_0 = \{x_4\},$$

$$p_1(x_4) = f^1_{x_3} = (01), \quad \tilde{u}_1 = \varnothing,$$

$$p_2(x_3, x_4) = f^\nabla_{x_3}(x_3, x_4) = (0001), \quad \tilde{u}_2 = \varnothing.$$

Переходим к шагу В.2а, так как множество переменных $\tilde{u}_0$ не пустое и $f^0_{x_3}$ равна константе.

В.2а. Применив алгоритм к функции $p_1(x_4) = f^1_{x_3} = (01)$ (вызов 8), получим терм $\Psi(x_4) = x_4$. В итоге имеем ответ

$$\Phi(x_3, x_4) = x_3 x_4.$$

Вызов алгоритма 8.

А. $f(x_4) = (01)$ Так как функция одноместная, сразу получаем ответ

$$\Phi = x_4.$$

Вызов алгоритма 9.

В.1. $f(x_1, x_2) = (0010)$. Находим функции $f^0_{x_1}$, $f^1_{x_1}$, $f^\nabla_{x_1}$ и множества переменных $\tilde{u}_0, \tilde{u}_1, \tilde{u}_2$:

$$p_0(x_2) = f^0_{x_1}(x_2) = (00) = 0, \quad \tilde{u}_0 = \{x_2\},$$

$$p_1(x_2) = f^0_{x_1}(x_2) = (10), \quad \tilde{u}_1 = \varnothing,$$

$$p_2(x_1, x_2) = f^\nabla_{x_1}(x_1, x_2) = (0010), \quad \tilde{u}_2 = \varnothing.$$

Переходим к шагу В.2а, так как множество переменных $\tilde{u}_0$ не пусто и $f^0_{x_1}$ равна константе.

В.2а. Применив алгоритм к функции $p_1(x_2) = f^1_{x_1} = (01)$ (вызов 10), получим терм $\Psi(x_2) = \bar{x}_2$. В итоге получаем ответ

$$\Phi(x_1, x_2) = x_1 \bar{x}_2.$$

Вызов алгоритма 10.

А. $f(x_2) = (10)$. Так как функция одноместная, сразу получаем ответ

$$\Phi(x_2) = \bar{x}_2.$$

§ 5. Количество бесповторных функций

Одной из важнейших характеристик базисного множества является количество бесповторных функций ранга n в этом множестве. В следующих двух утверждениях получены рекуррентные формулы для вычисления числа бесповторных функций в базисных множествах B_0 и B_1.

Упорядоченным термом над бинарным базисным множеством будем называть бесповторный терм, удовлетворяющий следующим требованиям:

1. В терме могут быть использованы только тесные отрицания.

2. В записи любого подтерма переменная с минимальным индексом стоит раньше других переменных в лексикографическом смысле.

3. В терме не содержится подтермов следующих видов:

$$(F_1 \cdot F_2) \cdot F_3, (F_1 \vee F_2) \vee F_3, (F_1 \oplus F_2) \oplus F_3.$$

4. В терме использованы только существенные переменные.

При выполнении вышеизложенных условий получим каноническое представление для бесповторной функции в базисных множествах B_0 и B_1. Подсчитав количество упорядоченных термов, можно найти количество бесповторных функций.

Теорема 2.6. *Верна следующая рекуррентная формула для вычисления K_n — числа бесповторных булевых функций ранга n в базисном множестве B_0:*

$$K_1 = 2, \quad K_n = 2 \cdot K_{n-1} + \sum_{i=1}^{n-1} C_{n-1}^{i-1} \cdot K_i \cdot K_{n-i}.$$

Доказательство. Как было указано выше, подсчитаем количество упорядоченных термов. От одной переменной таких термов будет $K_1 = 2$, а именно x_1 и $\overline{x}_1$. От двух переменных будет $K_2 = 8$ термов: $x_1 \cdot x_2$, $x_1 \cdot \overline{x}_2$, $\overline{x}_1 \cdot x_2$, $\overline{x}_1 \cdot \overline{x}_2$, $x_1 \vee x_2$, $x_1 \vee \overline{x}_2$, $\overline{x}_1 \vee x_2$, $\overline{x}_1 \vee \overline{x}_2$. Таким образом, получен базис для рекуррентной формулы.

Число термов вида $x_1 \cdot F(x_2, \ldots, x_n)$, $\overline{x}_1 \cdot F(x_2, \ldots, x_n)$, $x_1 \vee F(x_2, \ldots, x_n)$, $\overline{x}_1 \vee F(x_2, \ldots, x_n)$, где $F(x_2, \ldots, x_n)$ — тоже упорядоченный терм, будет $4 \cdot K_{n-1}$.

Теперь пусть A_i — это количество упорядоченных термов от i переменных, у которых внешней функцией является конъюнкция. Тогда количество упорядоченных термов вида $\Phi(x_1, y_2, \ldots, y_i) \vee \Psi(y_{i+1}, \ldots, y_n)$, где Φ и Ψ — упорядоченные термы, а $y_2, \ldots, y_n$ — перестановка переменных $x_2, \ldots, x_n$, будет выражаться формулой $C_{n-1}^{i-1} \cdot A_i \cdot K_{n-i}$.

Так как количество термов, у которых внешней функцией является конъюнкция, совпадает, в силу закона двойственности, с количеством термов, у которых внешней функцией является дизъюнкция, то проведя суммирование, получим:

$$K_n = 4 \cdot K_{n-1} + 2 \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot A_i \cdot K_{n-i}.$$

Подставляя в эту формулу очевидное значение $A_i = \frac{1}{2} K_i$, приходим к итоговой формуле:

$$K_1 = 2, \quad K_n = 2 \cdot K_{n-1} + \sum_{i=1}^{n-1} C_{n-1}^{i-1} \cdot K_i \cdot K_{n-i},$$

выражающей количество бесповторных функций. □

Теорема 2.7. *Верна следующая рекуррентная формула для вычисления S_n — числа бесповторных булевых функций ранга n в базисном множестве B_1:*

$$S_0 = 0, \quad S_1 = 2,$$

$$S_n = 3 \cdot S_{n-1} + \sum_{i=1}^{n-1} C_{n-1}^{i-1} \cdot (S_i + S_{i-1} + \sum_{j=1}^{i-1} C_{i-1}^{j-1} \cdot S_j \cdot S_{i-j}) \cdot S_{n-i}.$$

Доказательство. Если в упорядоченном терме нет сложения по модулю два, то такой терм будет единственным для соответствующей функции. Если же в терме k раз встречается сложение по модулю два, то таких термов будет 2^k, что происходит вследствие тождества

$$F_1 \oplus F_2 = \overline{F}_1 \oplus \overline{F}_2.$$

Число упорядоченных термов от одной переменной будет $S_1 = 2$. От двух переменных $S_2 = 10$, так как к восьми упорядоченным термам над B_0 добавляются еще два: $x_1 \oplus x_2$ и $\overline{x}_1 \oplus x_2$. Так получен базис для рекуррентной формулы.

Число упорядоченных термов вида $x_1 \cdot F$, $\overline{x}_1 \cdot F$, $x_1 \vee F$, $\overline{x}_1 \vee F$, $x_1 \oplus F$, где $F(x_2, \ldots, x_n)$ — упорядоченный терм, будет $5 \cdot S_{n-1}$.

Пусть A_i — это количество упорядоченных термов от i переменных, у которых внешней функцией является либо конъюнкция, либо сложение по модулю два. Тогда количество упорядоченных термов вида $\Phi(x_1, y_2, \ldots, y_i) \vee \Psi(y_{i+1}, \ldots, y_n)$, где Φ и Ψ — упорядоченные термы, а $y_2, \ldots, y_n$ — перестановка переменных $x_2, \ldots, x_n$, будет выражаться формулой $C_{n-1}^{i-1} \cdot A_i \cdot S_{n-i}$.

Пусть H_i — это количество упорядоченных термов от i переменных, у которых внешней функцией является либо конъюнкция, либо дизъюнкция. Тогда количество упорядоченных термов вида $\Phi(x_1, y_2, \ldots, y_i) \oplus \Psi(y_{i+1}, \ldots, y_n)$, где Φ и Ψ упорядоченные термы, а $y_2, \ldots, y_n$ — перестановка переменных $x_2, \ldots, x_n$, будет выражаться формулой $\frac{1}{2} C_{n-1}^{i-1} \cdot A_i \cdot S_{n-i}$.

Проводя суммирование, получаем

$$S_n = 5 \cdot S_{n-1} + 2 \cdot \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot A_i \cdot S_{n-i} + \tfrac{1}{2} \cdot \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot H_i \cdot S_{n-i},$$

$$A_n = 3 \cdot S_{n-1} + \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot A_i \cdot S_{n-i} + \tfrac{1}{2} \cdot \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot H_i \cdot S_{n-i}.$$

Преобразуем эти формулы

$$S_n = 5 \cdot S_{n-1} + \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot (2A_i + \tfrac{1}{2} H_i) \cdot S_{n-i}, \qquad (2.1)$$

$$A_n = 3 \cdot S_{n-1} + \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot (A_i + \tfrac{1}{2} H_i) \cdot S_{n-i}. \qquad (2.2)$$

Нетрудно заметить, что $S_i = A_i + \frac{1}{2} H_i$. Исходя из этого и формул (2.1) и (2.2), получим

$$S_n = 5 \cdot S_{n-1} + \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot (A_i + S_i) \cdot S_{n-i}, \qquad (2.3)$$

$$A_n = 3 \cdot S_{n-1} + \sum_{i=2}^{n-1} C_{n-1}^{i-1} \cdot S_i \cdot S_{n-i}. \qquad (2.4)$$

Осталось подставить (2.4) в (2.3) и произвести преобразования

$$S_0 = 0, \quad S_1 = 2,$$

$$S_n = 3 \cdot S_{n-1} + \sum_{i=1}^{n-1} C_{n-1}^{i-1} \cdot (S_i + S_{i-1} + \sum_{j=1}^{i-1} C_{i-1}^{j-1} \cdot S_j \cdot S_{i-j}) \cdot S_{n-i}.$$

□

Следующее утверждение дает прямую формулу вычисления числа бесповторных булевых функций в базисном множестве B_0.

Теорема 2.8. *Число K_n бесповторных булевых функций ранга n в элементарном базисном множестве может быть вычислено по формуле*

$$K_n = \sum_{j=0}^{n-2} 2^{n+j+1} \cdot B(n-2-j\ ,\ j),$$

где $B(0,j) = 1,$

$$B(i,j) = \sum_{0 \leqslant k_1 \leqslant \ldots \leqslant k_i \leqslant k_{i+1} = j} \Big(\prod_{s=2}^{i+1} s^{(k_s - k_{s-1})} \cdot (2k_{s-1} + s) \Big), \quad \textit{при } i > 0.$$

Доказательство. Пусть $\circ$ — некоторый символ бинарной функции. Построим множество M упорядоченных термов над $\{\circ\}$. Это множество будет содержать бесповторные термы, удовлетворяющие следующему условию: в записи любого подтерма переменная с минимальным индексом стоит раньше других в лексикографическом смысле.

Обозначим множество термов из M от n переменных x_1, x_2, ..., x_n через M_n. Рассмотрим терм $T \in M_n$. Он состоит из n переменных $x_1, x_2, \ldots, x_n$ и $n-1$ вхождения функции $\circ$. Далее рассмотрим все подтермы терма T. Очевидно, что если подтерм отличен от переменной, то у него будет своя внешняя функция $\circ$, и наоборот, каждому вхождению функции $\circ$ можно поставить в соответствие подтерм, в котором она будет внешней. Подтермы такого вида будем называть узлами. Каждая переменная образует свой подтерм, который будем называть концом. Пусть $T_1 \circ T_2$ — произвольный подтерм терма T. Если T_1 — узел, то подтерм T_1 будем называть левым узлом, если T_1 — конец, то

подтерм T_1 будем называть левым концом, если T_2 — узел, то подтерм T_2 будем называть правым узлом, если T_2 — конец, то подтерм T_2 будем называть правым концом. Очевидно, что весь терм T не является ни левым, ни правым узлом. Будем называть его главным узлом.

Нетрудно показать, что для любого терма из $T \in M_n$ сумма левых концов и левых узлов равна сумме правых концов и правых узлов и равна $n-1$.

Если терм из M_n имеет i левых и j правых узлов, то будем говорить, что он входит в класс $B(i,j)$, где $i+j=n-2$. В дальнейшем изложении, в формулах будем под $B(i,j)$ понимать число элементов в классе $B(i,j)$. Рассмотрим произвольный подтерм T_1 терма T. На место его вхождения в терм T подставим подтерм $T_1 \circ x_{n-1}$. Так как число подтермов в терме T будет $2n-1$, то каждому терму из M_n будет поставлено в соответствие $2n-1$ термов из M_{n+1}.

Очевидно, что совокупность всех термов от $n+1$ переменной, получаемых таким образом из всех термов из M_n, будет образовывать все термы из M_{n+1}, причем каждый будет получен ровно один раз. Отсюда следует, что $|M_{n+1}| = (2n-1) \cdot |M_n|$.

Далее рассмотрим следующие случаи для $T \in B(i,j)$:

1) если T_1 — левый узел, то добавится левый узел, и образуется i термов из $B(i+1,j)$;

2) если T_1 — правый узел, то добавится левый узел, и образуется j термов из $B(i+1,j)$;

3) если T_1 — главный узел, то добавится левый узел, и образуется 1 терм из $B(i+1,j)$;

4) если T_1 — левый конец, то добавится левый узел, и образуется $(n-1)-i$ термов из $B(i+1,j)$;

5) если T_1 — правый конец, то добавится правый узел, и образуется $(n-1)-j$ термов из $B(i,j+1)$.

Учитывая, что $n=i+j+2$, в итоге получим, что терм из $B(i,j)$ образует $1+i+j+(n-1)-i$ или $2j+i+2$ термов из $B(i+1,j)$ и $i+1$ термов из $B(i,j+1)$. И наоборот, в класс $B(i,j)$ входят $2j+i+1$ термов для каждого терма из $B(i-1,j)$ и $i+1$ термов для каждого терма из $B(i,j-1)$.

Эти рассуждения являются доказательством следующего утверждения, что число термов из M с i левыми и j правыми узлами $B(i,j)$ можно вычислить с помощью рекуррентной

формулы:

$$B(i,-1) = B(-1,j) = 0, \quad B(0,0) = 1,$$

$$B(i,j) = (i+1)\cdot B(i,j-1) + (2j+i+1)\cdot B(i-1,j).$$

Далее за два приема избавимся от рекуррентности в формуле.

Верно, что $B(0,j) = 1$, и

$$B(i,j) = \sum_{k=0}^{j} (i+1)^{j-k}\cdot(2k+i+1)\cdot B(i-1,k), \text{ при } i>0.$$

Краевое условие $B(0,j)$ получим из предыдущего утверждения при подстановке в формулу $i=0$. Дальнейшее доказательство проводится индукцией по j.

Базис индукции. При $j=0$ имеем $B(i,0) = (i+1)\cdot B(i-1,0)$, что согласуется с доказываемой формулой при $j=0$.

Шаг индукции. Предположим, что для любого $j \leqslant n$ утверждение верно и, опираясь на это, докажем его для $j = n+1$:

$$B(i,n+1) = (i+1)\cdot B(i,n) + (2(n+1)+i+1\cdot B(i-1,n+1)) =$$

$$= (i+1)\cdot\sum_{k=0}^{n}(i+1)^{n-k}\cdot(2k+i+1)\cdot B(i-1,k)+$$

$$+(i+1)^{(n+1)-(n+1)}\cdot(2(n+1)+i+1)\cdot B(i-1,n+1) =$$

$$= \sum_{k=0}^{n+1}(i+1)^{(n+1)-k}\cdot(2k+i+1)\cdot B(i-1,k).$$

Далее покажем, что

$$B(i,j) = \sum_{0\leqslant k_1\leqslant\ldots\leqslant k_i\leqslant k_{i+1}=j}\left(\prod_{s=2}^{i+1} s^{(k_s-k_{s-1})}\cdot(2k_{s-1}+s)\right), \text{ при } i>0.$$

Доказательство проведем индукцией по i.

Базис индукции. При $i=1$ из предыдущего утверждения получим

$$B(1,j) = \sum_{k=0}^{j} 2^{j-k}\cdot(2k+2).$$

То же самое получим из доказываемой формулы при $i = 1$, т.е. базис индукции проверен.

Шаг индукции. Пусть утверждение верно для всех $i \leqslant n$ и докажем формулу для $i = n + 1$:

$$B(n+1,j) = \sum_{k_{n+1}=0}^{j} (n+2)^{j-k_{n+1}} \cdot (2k_{n+1} + (n+2) \cdot B(n, k_{n+1}) =$$

$$= \sum_{k_{n+1}=0}^{j} (n+2)^{j-k_{n+1}} \cdot (2k_{n+1} + (n+2)) \cdot$$

$$\sum_{0 \leqslant k_1 \leqslant \ldots \leqslant k_n \leqslant k_{n+1}} (\prod_{s=2}^{n+1} s^{(k_s - k_{s-1})} \cdot (2k_{s-1} + s)) =$$

$$= \sum_{0 \leqslant k_1 \leqslant \ldots \leqslant k_{n+1} \leqslant k_{n+2} = j} (\prod_{s=2}^{n+2} s^{(k_s - k_{s-1})} \cdot (2k_{s-1} + s))).$$

Следует отметить, что в только что доказанном утверждении сумма берется по всевозможным неубывающим наборам длины $i + 1$, у которых последний член равен j.

Для завершения доказательства теоремы необходимо каждому терму из M_n поставить в соответствие термы над $\{\cdot, \vee\}$ путем замены $\circ$ на $\cdot$ или $\vee$, учитывая, что в упорядочнных термах над $\{\cdot, \vee\}$ запрещены подтермы вида $(F_1 \cdot F_2) \cdot F_3$ и $(F_1 \vee F_2) \vee F_3$. Если $T \in B(i,j)$, то внешнюю функцию $\circ$ можно заменить на $\cdot$ или на $\vee$, j внешних функций $\circ$ правых узлов можно так же произвольно заменить на $\cdot$ или на $\vee$, а i внешних функций $\circ$ левых узлов будут определены однозначно, с учетом вышеуказанных запретов.

Таким образом, каждому терму из M_n, содержащему i левых и j правых узлов, ставится в соответствие 2^{j+1} упорядоченных термов над $\{\cdot, \vee\}$ и 2^{n+j+1} упорядоченных термов над B_0.

Осталось просуммировать $2^{n+j+1} \cdot B(i,j)$ по всем j от 0 до $n-2$; учитывая, что $i = n - 2 - j$, получаем

$$K_n = \sum_{j=0}^{n-2} 2^{n+j+1} \cdot B(n-2-j\ ,\ j),$$

где $B(i,j)$ находится из последнего утверждения. □

Используя полученные формулы, можно подсчитать количество бесповторных булевых функций в базисных множествах B_0 и B_1. Результаты вычислений для $n \leqslant 10$ приведены в табл. 1.

Таблица 1.

Количество бесповторных булевых функций

n	Базисное множество	
	B_0	B_1
1	2	2
2	8	10
3	64	114
4	832	2 154
5	15 104	56 946
6	352 256	1 935 210
7	10 037 248	80 371 122
8	337 936 384	3 944 568 042
9	13 126 565 888	223 374 129 138
10	577 818 263 552	14 335 569 726 570

Из таблицы видно, что количество бесповторных булевых функций в базисном множестве B_1 растет намного быстрее, чем в базисном множестве B_0. Следующее утверждение показывает, что бесповторных булевых функций в базисном множестве B_1 намного больше, чем в базисном множестве B_0.

Теорема 2.9. *Пусть K_n — число бесповторных булевых функций в B_0, S_n — число бесповторных булевых функций в базисном множестве B_1, тогда* $\lim\limits_{n\to\infty} \frac{K_n}{S_n} = 0$.

Доказательство. При доказательстве будем использовать то, что любые бесповторные функции над B_0 и B_1 почти однозначно (с точностью до выполнения соотношений $F_1 \oplus F_2 = \overline{F}_1 \oplus \overline{F}_2$) можно представить упорядоченными термами.

Пусть P_n^1 — множество булевых функций, представимых бесповторными термами, содержащими одно вхождение $\oplus$. Яс-

но, что при этом $S_n \geqslant K_n + |P_n^1|$, значит и

$$\frac{S_n}{K_n} \geqslant 1 + \frac{|P_n^1|}{K_n}.$$

Каждой бесповторной над B_0 функции f ранга n поставим в соответствие функцию h из P_n^1 следующим образом: в записи упорядоченного терма, представляющего f, заменим внешнюю $\cdot$ или $\vee$ на $\oplus$. Попутно заметим, что получившийся терм будет так же упорядоченным, но уже в базисном множестве B_1. Функция, которую реализует полученный терм, и будет h из P_n^1. Учитывая, что мы заменяем и $\cdot$ и $\vee$ на $\oplus$, а так же тождество для сложения $F_1 \oplus F_2 = \overline{F}_1 \oplus \overline{F}_2$, можно прийти к выводу, что в полученную одну функцию h из P_n^1 отобразится не более четырех бесповторных над B_0 функций.

Аналогичную функцию для всех бесповторных над B_0 функций ранга n произведем для внешней функции подтерма, находящегося на первом аргументе внешней функции всего терма. Полученные термы из P_n^1 не могут представлять ни одной функции из тех, что были получены на предыдущем шаге, так как в них $\oplus$ один, стоит в разных местах, а вновь полученные термы так же являются упорядоченными.

Так как в терме от n переменных $n-1$ вхождение $\cdot$ или $\vee$, то каждой бесповторной над B_0 функции f ранга n ставится $n-1$ различная функция h из P_n^1. K_n различным функциям, бесповторным над B_0 ранга n, ставится в соответствие не менее $K_n \cdot \frac{n-1}{4}$ различных функций из P_n^1 и значит $|P_n^1| \geqslant K_n \cdot \frac{n-1}{4}$. Отсюда получаем

$$\frac{S_n}{K_n} \geqslant 1 + \frac{n-1}{4},$$

и следовательно

$$\lim_{n\to\infty} \frac{K_n}{S_n} = 0. \qquad \square$$

Комментарии. Фундаментальный результат А.В. Кузнецова (теорема 2.2) о бесповторных разложениях булевых функций был опубликован в работе [15]. Критерии бесповторности для элементарного базисного множества (теорема 2.3) получены в работах Б.А. Субботовской [20] (наследственные нежесткость и строгая нежесткость), В.А. Гурвич [11, 12] (недиффузность), Н.А. Перязева [18] (наследственная невырожденность).

Отметим, что в приведенных работах терминология отлична от используемой в книге.

Первые результаты по исследованиям бесповторных функций в бинарном базисном множестве были приведены в работе [10]. Критерий бесповторности для этого базисного множества (теорема 2.4) и алгоритм нахождения бесповторных представлений (§ 4) получен Н.А. Перязевым [17]. Еще один критерий для бинарного базисного множества, основанный на общей методике, получен К.Д. Кириченко [14].

Первые результаты по подсчету количества бесповторных булевых функций в элементарном базисном множестве приведены в [19]. Рекуррентные формулы для числа бесповторных функций в элементарном и бинарном базисном множестве (теоремы 2.6 и 2.7) приведены в [16]. Прямая формула для элементарного базисного множества получена О.В. Зубковым. Им же предложены рекуррентные формулы для подсчета числа бесповторных функций в произвольных базисах. Теорема 2.9 является частным случаем общей ситуации [13].

Глава III

Полиномиальные представления булевых функций

Основной идеей построения операторных полиномиальных форм служит представление базисных функций канонической формы в виде операторных образов некоторой функции от определенного набора (базисного пучка) операторов. Существование такой функции (по крайней мере — одной) и таких пучков гарантируют приведенные канонические формы — полином Жегалкина и его обобщения. Общая форма таких полиномов выглядит следующим образом:

$$f(x_1, ..., x_n) = \sum_{\bar{\tau} \in E^n} \varphi_{\bar{\tau}}(g(x_1, ..., x_n)),$$

где $\sum$ — сложение по модулю 2, $\varphi_{\bar{\tau}} : F^n \to F^n$ — операторы на множестве всех булевых функций от n переменных.

Операторы — весьма удобный инструмент для описания разложений булевых функций. Операторный подход позволил получить общую картину полиномиальных разложений, построить классы полиномов охватывающие все известные полиномы, начиная с полинома Жегалкина и совершенной полиномиальной нормальной формы. Более того, с помощью операторов открылась возможность построения канонических форм, основанных не только на функции моногоместной конъюнкции.

Естественно, рассматриваются далеко не все операторы в булевых функциях [33]. Построен и применен в разложениях класс операторов, являющихся обобщением операторов расстановки отрицания, взятия производной и оператора подстановки. Разложения с оператором частной производной имеют с одной стороны технические приложения, с другой — дают элегантные доказательства известных результатов о связи частной и кратной производных.

Сокращения и обозначения, относящиеся непосредственно к тексту главы:

— в случае использования двоичного вектора $\tilde{\tau}$ в качестве номера, он будет отождествляется с числом $\tau_1 2^{n-1} + ... + \tau_n 2^0$;

— символ $\oplus$ будет использоваться для обозначения сложения наборов:

$$\tilde{\tau} \oplus \tilde{\sigma} = (\tau_1 \oplus \sigma_1, ..., \tau_n \oplus \sigma_n);$$

— символом $\vee$ будет обозначаться дизъюнкция наборов:

$$\tilde{\tau} \vee \tilde{\sigma} = (\tau_1 \vee \sigma_1, ..., \tau_n \vee \sigma_n);$$

— символом $\lfloor a \rfloor$ обозначается наибольшее целое число, не превосходящее рациональное число a.

Оператор подстановки обозначается $s_{\tilde{x}}^{\tilde{z}} f(\tilde{x}, \tilde{y}) = f_{\tilde{x}}^{\tilde{z}}(\tilde{x}, \tilde{y})$. При изложении некоторых результатов оказалось полезно ввести два частных случая оператора подстановки:

— $\mathrm{i}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x})$ для взятия остаточной единичной;

— $\mathrm{o}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x})$ для взятия остаточной нулевой по переменным x_i, для которых соответствующее $\tau_i = 0$.

Кратной производной функции $f(x_1, ..., x_n)$ по аргументу x_j называется функция $f'_{x_j}(\tilde{x}) = f_{x_j}^{\overline{x}_j}(\tilde{x}) \oplus f(\tilde{x})$. Это определение индуктивно распространяется на подмножество аргументов:

$$f(\tilde{x}, \tilde{y})_{\tilde{x}}^{(n)} = \sum_{\tilde{\tau} \in E^n} f(\tilde{x}^{\tilde{\tau}}, \tilde{y}).$$

Из определения следует, что $f_{x_j}^{\overline{x}_j}(\tilde{x}) \oplus f(\tilde{x}) = f_{x_j}^0(\tilde{x}) \oplus f_{x_j}^1(\tilde{x})$, а следовательно переменные, по которым берется производная, становятся фиктивными. Можно заметить, что производная по фиктивному аргументу равна 0.

Для удобства изложения в основном будет использоваться операторная запись: $\mathrm{d}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x})$ обозначает производную по всем переменным x_i, таким что соответствующее $\tau_i = 0$.

Частной производной функции $f(\tilde{x}, \tilde{z})$ по набору аргументов $\tilde{x}$ называется функция $f_{\tilde{x}}^{(\tilde{0})}(\tilde{x}, \tilde{z}) = f(\tilde{x}, \tilde{z}) \oplus f(\overline{\tilde{x}}, \tilde{z})$. Операторная запись выглядит так:

$$f_{\tilde{x}}^{(\tilde{0})}(\tilde{x}, \tilde{z}) = \partial_{\tilde{x}}^{\tilde{0}} f(\tilde{x}, \tilde{z})$$

или так:

$$f_{\tilde{x}}^{(\tilde{0})}(\tilde{x}, \tilde{z}) = \partial_{x_1 ... x_n z_1 ... z_m}^{0 \ ... \ 0 \ 1 \ ... \ 1} f(\tilde{x}, \tilde{z}).$$

Аналогично используется операторная запись: $\mathrm{p}^{\tilde{\tau}}_{\tilde{x}} f(\tilde{x})$ для функции отрицания на переменных x_i, для которых соответствующее $\tau_i = 0$.

Оператор $\mathrm{e}^{\tilde{\tau}}_{\tilde{x}} f(\tilde{x}) = f(\tilde{x})$ (для любого $\tilde{\tau}$) обозначает тождественный оператор.

Оператор сплетения $\mathrm{q}^{\tilde{\tau}}_{\tilde{x}}[g(\tilde{x})] f(\tilde{x}, \tilde{y})$ обозначает результат подстановки функции $g(\tilde{x})$ в функцию $f(\tilde{x}, \tilde{y})$ вместо переменных x_i, если соответствующее $\tau_i = 0$.

Во всех определениях подразумевается, что наборы $\tilde{x}$ и $\tilde{\tau}$ должны быть одинаковой размерности.

Для примера:

$$\mathrm{d}^{0\,0\,1}_{x_1x_2x_3} f(x_1, x_2, x_3) = f(x_1, x_2, x_3)''_{x_1x_2} = \sum_{(\tau_1,\tau_2)\in E^2} f(\tau_1, \tau_2, x_3);$$

$$\partial^{0\,0\,1}_{x_1x_2x_3} f(x_1, x_2, x_3) = f(x_1, x_2, x_3) \oplus f(\overline{x}_1, \overline{x}_2, x_3);$$

$$\mathrm{p}^{0\,0\,1}_{x_1x_2x_3} f(x_1, x_2, x_3) = f(\overline{x}_1, \overline{x}_2, x_3);$$

$$\mathrm{i}^{0\,0\,1}_{x_1x_2x_3} f(x_1, x_2, x_3) = f(1, 1, x_3);$$

$$\mathrm{o}^{0\,0\,1}_{x_1x_2x_3} f(x_1, x_2, x_3) = f(0, 0, x_3);$$

$$\mathrm{q}^{0\,0\,1}_{x_1x_2x_3}[x_1 \cdot x_2 \cdot x_3](x_1 \vee x_2 \vee x_3 \vee y_1) = \\ = (x_1 \cdot x_2 \cdot x_3) \vee (x_1 \cdot x_2 \cdot x_3) \vee x_3 \vee y_1.$$

В операторной записи верхний индекс иногда будет опускаться. В этом случае считается, что действие имеется по всем переменным, указанным в нижнем индексе. Например:

$$\mathrm{d}_{x_1x_2} f(x_1, x_2, ..., x_n) = \mathrm{d}^{0\,0\,1\,\ldots\,1}_{x_1x_2x_3\ldots x_n} f(x_1, x_2, ..., x_n).$$

Заметим, что функция $f(\tilde{x})$ является нечетной, если $\mathrm{d}^{\tilde{0}}_{\tilde{x}} f(\tilde{x}) = 1$, и четной — в противном случае.

§ 1. Свойства операторов и операторных пучков

Пусть задана последовательность $\mathrm{t} = \mathrm{t}_1 \ldots \mathrm{t}_n$, в которой компоненты $\mathrm{t}_i \in \{\mathrm{e}, \mathrm{p}, \mathrm{d}\}$. Весом этой последовательности $w(\mathrm{t})$ будет называться натуральное число:

$$w(\mathrm{t}) = \sum_{i=1}^{n} \alpha_i, \quad \alpha_i = \begin{cases} 1, & \text{если } \mathrm{t}_i \neq \mathrm{e}, \\ 0, & \text{если } \mathrm{t}_i = \mathrm{e}. \end{cases}$$

По последовательности $\mathrm{t} = \mathrm{t}_1 \ldots \mathrm{t}_n$ определим оператор, действующий по переменным $x_1, \ldots, x_n$ на функцию $f(x_1, \ldots, x_n, \tilde{y})$. Оператор определяется индуктивно по весу $w(\mathrm{t})$:

при $w(\mathrm{t}) = 0$ $\quad \mathrm{t}(f(\tilde{x})) = f(\tilde{x})$;

при $w(\mathrm{t}) = 1$ $\quad \mathrm{t}(f(\tilde{x})) = \begin{cases} \mathrm{d}_{x_i} f(\tilde{x}), & \text{если } \mathrm{t}_i = \mathrm{d}; \\ \mathrm{p}_{x_i} f(\tilde{x}), & \text{если } \mathrm{t}_i = \mathrm{p}; \end{cases}$

при $w(\mathrm{t}) = k$ $\quad \mathrm{t}(f(\tilde{x})) = \mathrm{b}(\mathrm{a}(f(\tilde{x})))$,

где $\mathrm{b} = \mathrm{b}_1 \ldots \mathrm{b}_n$, $w(\mathrm{b}) = 1$, $\mathrm{a} = \mathrm{a}_1 \ldots \mathrm{a}_n$, $w(\mathrm{a}) = k - 1$ и для некоторого $1 \leqslant s \leqslant n$ выполняется $\mathrm{b}_i \neq e$, $\mathrm{a}_i = e$ при $i = s$; для $i \neq s$ выполняется $\mathrm{a}_i = \mathrm{t}_i$.

Число n будет называться *размерностью оператора.*

Обозначение $\mathrm{a}_{\tilde{x}}$ используется для указания переменных. Если из контекста ясно, по каким переменным действует оператор, то нижний индекс будет отсутствовать. Обозначение без нижнего индекса употребляется также и в случае, когда оператор действует по всем переменным. Для оператора $\mathrm{a} = e \ldots e \mathrm{a}_s e \ldots e$ используется запись a_s.

Упорядоченный набор $(\mathrm{t}^{\tilde{0}}, \ldots, \mathrm{t}^{\tilde{\tau}}, \ldots, \mathrm{t}^{\tilde{1}})$, состоящий из 2^n операторов, действующих по переменным $(x_1, \ldots, x_n)$, называется *пучком операторов* или *операторным пучком.* В пучке все операторы имеют одну размерность, длина или количество операторов пучка всегда связана с этой размерностью. А именно, длина пучка операторов размерности n всегда равна 2^n.

Пучок $(\mathrm{b}^{\tilde{0}}_{\tilde{x}}, \ldots, \mathrm{b}^{\tilde{\tau}}_{\tilde{x}}, \ldots, \mathrm{b}^{\tilde{1}}_{\tilde{x}})$ операторов размерности n будет называться базисным, если существует функция $f(\tilde{x})$ такая, что ее операторные образы $\{\mathrm{b}^{\tilde{0}} f(\tilde{x}), \ldots, \mathrm{b}^{\tilde{1}} f(\tilde{x})\}$ образуют базис линейного пространства всех булевых функций от n переменных.

Для примера рассмотрим два базисных пучка операторов:

1) (ppp, ppe, pep, pee, epp, epe, eep, eee),

2) (ddd, dde, ded, dee, edd, ede, eed, eee).

Пусть $f(x_1, x_3, x_3) = x_1 \cdot x_2 \cdot x_3$. Тогда наборы функций, построенные из f по данным пучкам:

1) $\{\mathrm{ppp}(x_1 \cdot x_2 \cdot x_3), \mathrm{ppe}(x_1 \cdot x_2 \cdot x_3), \mathrm{pep}(x_1 \cdot x_2 \cdot x_3), \mathrm{pee}(x_1 \cdot x_2 \cdot x_3),$
$\mathrm{epp}(x_1 \cdot x_2 \cdot x_3), \mathrm{epe}(x_1 \cdot x_2 \cdot x_3), \mathrm{eep}(x_1 \cdot x_2 \cdot x_3), \mathrm{eee}(x_1 \cdot x_2 \cdot x_3)\} =$

$= \{\bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \bar{x}_1 \cdot \bar{x}_2 \cdot x_3, \bar{x}_1 \cdot x_2 \cdot \bar{x}_3, \bar{x}_1 \cdot x_2 \cdot x_3,$

$x_1 \cdot \bar{x}_2 \cdot \bar{x}_3, x_1 \cdot \bar{x}_2 \cdot x_3, x_1 \cdot x_2 \cdot \bar{x}_3, x_1 \cdot x_2 \cdot x_3\}$;

$$2)\{\mathbf{ddd}(x_1\cdot x_2\cdot x_3), \mathbf{dde}(x_1\cdot x_2\cdot x_3), \mathbf{ded}(x_1\cdot x_2\cdot x_3), \mathbf{dee}(x_1\cdot x_2\cdot x_3),$$
$$\mathbf{edd}(x_1\cdot x_2\cdot x_3), \mathbf{ede}(x_1\cdot x_2\cdot x_3), \mathbf{eed}(x_1\cdot x_2\cdot x_3), \mathbf{eee}(x_1\cdot x_2\cdot x_3)\} =$$
$$= \{1, x_3, x_2, x_2\cdot x_3, x_1, x_1\cdot x_3, x_1\cdot x_2, x_1\cdot x_2\cdot x_3\}$$

определяют базис СПКНФ и базис полинома Жегалкина соответственно для функций от трех переменных.

Несколько основных свойств операторов оформлены в виде предложений.

Следующее предложение показывает линейность введенных операторов.

Предложение 3.1. *Для любых функций $f(\tilde{x})$ и $g(\tilde{x})$, для любого оператора* $\mathbf{a}$ *выполняется*:

$$\mathbf{a}(f(\tilde{x})\oplus g(\tilde{x})) = \mathbf{a}f(\tilde{x})\oplus \mathbf{a}g(\tilde{x}).$$

Доказательство будем проводить индукцией по весу $l = w(\mathbf{a})$.

Базис индукции. Пусть $l = 0$. Тогда оператор $\mathbf{a}$ имеет вид $\mathbf{a} = \mathbf{e}\ldots\mathbf{e}$. По определению тождественного оператора выполняется равенство $\mathbf{e}_{\tilde{x}}f(\tilde{x}) = f(\tilde{x})$, откуда следует выполнение условий предложения.

Шаг индукции. Пусть $l > 0$ и в операторе $\mathbf{a}$ компонента $\mathbf{a}_s \neq \mathbf{e}$. Рассмотрим оператор $\mathbf{b} = \mathbf{b}_1\ldots\mathbf{b}_n$, где $\mathbf{b}_i = \mathbf{a}_i$ при $i \neq s$ и $\mathbf{b}_i = \mathbf{e}$ при $i = s$. Тогда оператор $\mathbf{a}$ может быть представлен в следующем виде:

$$\mathbf{a}f(\tilde{x}) = \mathbf{a}_s(\mathbf{b}f(\tilde{x}))\,.$$

Откуда по предположению индукции следует цепочка тождеств:

$$\mathbf{a}[f(\tilde{x})\oplus g(\tilde{x})] = \mathbf{a}_s(\mathbf{b}[f(\tilde{x})\oplus g(\tilde{x})]) = \mathbf{a}_s[\mathbf{b}f(\tilde{x})\oplus \mathbf{b}g(\tilde{x})] =$$
$$= \mathbf{a}_s[\mathbf{b}f(\tilde{x}))\oplus \mathbf{a}_s(\mathbf{b}g(\tilde{x})] = \mathbf{a}f(\tilde{x})\oplus \mathbf{a}g(\tilde{x}). \quad \square$$

Следующее предложение говорит о сохранении свойства быть четной функцией в операторном образе четной функции.

Предложение 3.2. *Если функция $f(\tilde{x})$ — четная, то для любого оператора* $\mathbf{a}$ *функция $\mathbf{a}f(\tilde{x})$ также является четной.*

Доказательство легко следует из определения оператора. Очевидно, что расстановка отрицаний над переменными не меняет четность функции, а производная любой функции

всегда является четной функцией (поскольку становится фиктивной та переменная, по которой бралась производная). □

Свойство операторов, сформулированное в предложении 3.3, дает возможность разбивать в некотором смысле сложные операторы на более простые.

Предложение 3.3. *Пусть* $f(\tilde{x}) = g(\tilde{y}) \cdot h(\tilde{z})$, *где набор* $\tilde{x}$ *разбит на непересекающиеся наборы* $\tilde{y} = (y_1, ..., y_n)$ *и* $\tilde{z} = (z_1, ..., z_m)$. *Тогда для любого оператора* $\mathrm{t} = \mathrm{t}_1 ... \mathrm{t}_{n+m}$ *выполняется равенство*:

$$\mathrm{t}_{\tilde{x}} f(\tilde{x}) = \mathrm{a}_{\tilde{y}} g(\tilde{y}) \cdot \mathrm{b}_{\tilde{z}} h(\tilde{z}),$$

где операторы имеют вид: $\mathrm{t} = \mathrm{a}_1 \ldots \mathrm{a}_n \mathrm{b}_1 \ldots \mathrm{b}_m$, $\mathrm{a} = \mathrm{a}_1 \ldots \mathrm{a}_n$, $\mathrm{b} = \mathrm{b}_1 \ldots \mathrm{b}_m$.

Доказательство. Рассмотрим действие оператора t на функцию $f(\tilde{x})$.

Пусть $w(\mathrm{t}) = 1$ и $\mathrm{a}_s \neq e$. Тогда $\mathrm{b}_{\tilde{z}} = e_{\tilde{z}}$ и для оператора t имеет место цепочка тождеств:

$$\mathrm{t} f(\tilde{x}) = \mathrm{a}_s \left(e_{\tilde{x}}(f(\tilde{x}))\right) = \mathrm{a}_s \left(e_{\tilde{y}}(g(\tilde{y})) \cdot e_{\tilde{z}}(h(\tilde{z}))\right) = \\ = \left(\mathrm{a}_s(e_{\tilde{y}}(g(\tilde{y}))) \cdot e_{\tilde{z}}(h(\tilde{z})\right) = \mathrm{a}_{\tilde{y}} g(\tilde{y}) \cdot \mathrm{b}_{\tilde{z}} h(\tilde{z}).$$

Пусть $w(\mathrm{t}) = k$ и $\mathrm{a}_s \neq e$. Тогда по определению оператора:

$$\mathrm{t} f(\tilde{x}) = \mathrm{a}_s(\mathrm{t}' f(\tilde{x})),$$

где $w(\mathrm{t}') = k - 1$, $(\mathrm{t}')_s = e$ и $(\mathrm{t}')_i = \mathrm{t}_i$ для остальных $i \neq s$.

По индукции имеем

$$\mathrm{a}_s(\mathrm{t}' f(\tilde{x})) = \mathrm{a}_s(\mathrm{a}' g(\tilde{y}) \cdot \mathrm{b} h(\tilde{z})) = \\ = \mathrm{a}_s(\mathrm{a}'_{\tilde{y}} g(\tilde{y})) \cdot \mathrm{b}_{\tilde{z}} h(\tilde{z}) = \mathrm{a}_{\tilde{y}} g(\tilde{y}) \cdot \mathrm{b}_{\tilde{z}} h(\tilde{z}),$$

символом a' обозначен оператор, совпадающий с оператором a на всех позициях i при $i \neq s$; $(\mathrm{a}')_s = e$.

Случай $\mathrm{b}_s \neq e$, очевидно, полностью аналогичен рассмотренному. □

Предложение 3.4. *Для любых операторов* a *и* b, *для любых функций* $f(\tilde{x})$ *и* $g(\tilde{x})$ *имеет место тождество*:

$$\mathrm{d}_{\tilde{x}}[\mathrm{a} f(\tilde{x}) \cdot \mathrm{b} g(\tilde{x}) \oplus \mathrm{a} g(\overline{\tilde{x}}) \cdot \mathrm{b} f(\overline{\tilde{x}})] = 0.$$

Доказательство будем вести индукцией по числу $k = w(\mathfrak{a}) + w(\mathfrak{b})$.

Базис индукции при $k = 0$:

$$\mathrm{d}_{\tilde{x}}[f(\tilde{x}) \cdot g(\tilde{x}) \oplus g(\overline{\tilde{x}}) \cdot f(\overline{\tilde{x}})] = \sum_{\tilde{\tau} \in E^n} \left(f(\tilde{\tau}) \cdot g(\tilde{\tau}) \oplus g(\overline{\tilde{\tau}}) \cdot f(\overline{\tilde{\tau}}) \right) = 0,$$

поскольку полная производная функции есть сумма значений этой функции по всем наборам значений переменных. Очевидно, что в этой сумме слагаемые с индексами $\tilde{\tau}$ и $\overline{\tilde{\tau}}$ совпадают.

Шаг индукции. Пусть теперь $k > 0$ и $a_s \neq e$. Здесь символом $\mathfrak{a}'$ обозначен оператор, совпадающий с оператором $\mathfrak{a}$ на всех позициях i при $i \neq s$, и $(\mathfrak{a}')_s = e$. Тогда оператор $\mathfrak{a}$ можно представить:

$$\mathfrak{a} f(\tilde{x}) = \mathfrak{a}_s \left(\mathfrak{a}' \left(\bar{x}_s \cdot f^0_{x_s}(\tilde{x}) \oplus x_s \cdot f^1_{x_s}(\tilde{x}) \right) \right).$$

Вынесем переменную x_s из функции и воспользуемся предложением 3.1:

$$\mathfrak{a} f(\tilde{x}) = \mathfrak{a} \left(\bar{x}_s \cdot f^0_{x_s}(\tilde{x}) \oplus x_s \cdot f^1_{x_s}(\tilde{x}) \right) = \\ = \mathfrak{a} \left(\bar{x}_s \cdot f^0_{x_s}(\tilde{x}) \right) \oplus \mathfrak{a} \left(x_s \cdot f^1_{x_s}(\tilde{x}) \right).$$

По предложению 3.3 можно провести несколько преобразований:

$$\mathfrak{a} f(\tilde{x}) = (\mathfrak{a}_s \bar{x}_s) \cdot \left(\mathfrak{a}' f^0_{x_s}(\tilde{x}) \right) \oplus (\mathfrak{a}_s x_s) \cdot \left(\mathfrak{a}' f^1_{x_s}(\tilde{x}) \right);$$

$$\mathfrak{a} g(\overline{\tilde{x}}) = (\mathfrak{a}_s \bar{x}_s) \cdot \left(\mathfrak{a}' g^0_{x_s}(\overline{\tilde{x}}) \right) \oplus (\mathfrak{a}_s x_s) \cdot \left(\mathfrak{a}' g^1_{x_s}(\overline{\tilde{x}}) \right);$$

$$\mathfrak{b} f(\tilde{x}) = (\mathfrak{b}_s \bar{x}_s) \cdot \left(\mathfrak{b}' f^0_{x_s}(\tilde{x}) \right) \oplus (\mathfrak{b}_s x_s) \cdot \left(\mathfrak{b}' f^1_{x_s}(\tilde{x}) \right);$$

$$\mathfrak{b} g(\overline{\tilde{x}}) = (\mathfrak{b}_s \bar{x}_s) \cdot \left(\mathfrak{b}' g^0_{x_s}(\overline{\tilde{x}}) \right) \oplus (\mathfrak{b}_s x_s) \cdot \left(\mathfrak{b}' g^1_{x_s}(\overline{\tilde{x}}) \right).$$

Теперь можно раскрыть скобки по дистрибутивности:

$$\mathrm{d}_{\tilde{x}}[\mathfrak{a} f(\tilde{x}) \cdot \mathfrak{b} g(\tilde{x}) \oplus \mathfrak{a} g(\overline{\tilde{x}}) \cdot \mathfrak{b} f(\overline{\tilde{x}})] = \\ = \mathrm{d}_{\tilde{x}} \left[\mathfrak{a}_s \bar{x}_s \cdot \mathfrak{b}_s \bar{x}_s \cdot \mathfrak{a}' f^0_{x_s}(\tilde{x}) \cdot \mathfrak{b}' g^0_{x_s}(\tilde{x}) \oplus \right. \\ \oplus \mathfrak{a}_s \bar{x}_s \cdot \mathfrak{b}_s x_s \cdot \mathfrak{a}' f^0_{x_s}(\tilde{x}) \cdot \mathfrak{b}' g^1_{x_s}(\tilde{x}) \oplus \\ \left. \oplus \mathfrak{a}_s x_s \cdot \mathfrak{b}_s \bar{x}_s \cdot \mathfrak{a}' f^1_{x_s}(\tilde{x}) \cdot \mathfrak{b}' g^0_{x_s}(\tilde{x}) \oplus \right.$$

$$\oplus\, \mathrm{a}_s x_s \cdot \mathrm{b}_s x_s \cdot \mathrm{a}' f^1_{x_s}(\tilde{x}) \cdot \mathrm{b}' g^1_{x_s}(\tilde{x}) \oplus \qquad (3.5)$$
$$\oplus\, \mathrm{a}_s \bar{x}_s \cdot \mathrm{b}_s \bar{x}_s \cdot \mathrm{a}' g^0_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^0_{x_s}(\bar{\tilde{x}}) \oplus$$
$$\oplus\, \mathrm{a}_s \bar{x}_s \cdot \mathrm{b}_s x_s \cdot \mathrm{a}' g^0_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^1_{x_s}(\bar{\tilde{x}}) \oplus$$
$$\oplus\, \mathrm{a}_s x_s \cdot \mathrm{b}_s \bar{x}_s \cdot \mathrm{a}' g^1_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^0_{x_s}(\bar{\tilde{x}}) \oplus$$
$$\oplus\, \mathrm{a}_s x_s \cdot \mathrm{b}_s x_s \cdot \mathrm{a}' g^1_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^1_{x_s}(\bar{\tilde{x}})\Big].$$

Рассмотрим все возможные варианты для операторов a_s и b_s:

а) $\mathrm{a}_s = \mathrm{b}_s = \mathrm{d}$. В этом случае переменная x_s фиктивна, и производная по ней равна нулю.

б) $\mathrm{a}_s \neq \mathrm{d}$ и $\mathrm{b}_s = \mathrm{d}$. В этом случае выражение (3.5) примет вид

$$\mathrm{d}_{\tilde{x}}[\mathrm{a} f(\tilde{x}) \cdot \mathrm{b} g(\tilde{x}) \oplus \mathrm{a} g(\bar{\tilde{x}}) \cdot \mathrm{b} f(\bar{\tilde{x}})] =$$
$$= \mathrm{d}_{\tilde{x}}[\mathrm{a}' f^0_{x_s}(\tilde{x}) \cdot \mathrm{b}' g^0_{x_s}(\tilde{x}) \oplus \mathrm{a}' g^1_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^1_{x_s}(\bar{\tilde{x}})] \oplus$$
$$\oplus\, \mathrm{d}_{\tilde{x}}[\mathrm{a}' f^0_{x_s}(\tilde{x}) \cdot \mathrm{b}' g^1_{x_s}(\tilde{x}) \oplus \mathrm{a}' g^0_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^1_{x_s}(\bar{\tilde{x}})] \oplus$$
$$\oplus\, \mathrm{d}_{\tilde{x}}[\mathrm{a}' f^1_{x_s}(\tilde{x}) \cdot \mathrm{b}' g^0_{x_s}(\tilde{x}) \oplus \mathrm{a}' g^1_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^0_{x_s}(\bar{\tilde{x}})] \oplus$$
$$\oplus\, \mathrm{d}_{\tilde{x}}[\mathrm{a}' f^1_{x_s}(\tilde{x}) \cdot \mathrm{b}' g^1_{x_s}(\tilde{x}) \oplus \mathrm{a}' g^0_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^0_{x_s}(\bar{\tilde{x}})].$$

По индуктивному предположению каждое из четырех слагаемых равно нулю.

в) $\mathrm{a}_s = \mathrm{d}$ и $\mathrm{b}_s \neq \mathrm{d}$. Доказательство аналогично пункту б).

г) $\mathrm{a}_s \neq \mathrm{d}$ и $\mathrm{b}_s \neq \mathrm{d}$. Тогда либо $\mathrm{a}_s = \mathrm{b}_s$, либо $\mathrm{a}_s \neq \mathrm{b}_s$. В первом случае 2-е, 3-е, 6-е, 7-е слагаемые суммы (3.5) равны нулю, поскольку в них входит произведение $x_s \cdot \bar{x}_s$, и выражение (3.5) примет вид

$$\mathrm{d}_{\tilde{x}}[\mathrm{a} f(\tilde{x}) \cdot \mathrm{b} g(\tilde{x}) \oplus \mathrm{a} g(\bar{\tilde{x}}) \cdot \mathrm{b} f(\bar{\tilde{x}})] =$$
$$= \mathrm{d}_{\tilde{x}}[\mathrm{a}_s \bar{x}_s \cdot \mathrm{b}_s \bar{x}_s \cdot \mathrm{a}' f^0_{x_s}(\tilde{x}) \cdot \mathrm{b}' g^0_{x_s}(\tilde{x})] \oplus$$
$$\oplus\, \mathrm{d}_{\tilde{x}}[\mathrm{a}_s x_s \cdot \mathrm{b}_s x_s \cdot \mathrm{a}' f^1_{x_s}(\tilde{x}) \cdot \mathrm{b}' g^1_{x_s}(\tilde{x})] \oplus$$
$$\oplus\, \mathrm{d}_{\tilde{x}}[\mathrm{a}_s \bar{x}_s \cdot \mathrm{b}_s \bar{x}_s \cdot \mathrm{a}' g^0_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^0_{x_s}(\bar{\tilde{x}})] \oplus$$
$$\oplus\, \mathrm{d}_{\tilde{x}}[\mathrm{a}_s x_s \cdot \mathrm{b}_s x_s \cdot \mathrm{a}' g^1_{x_s}(\bar{\tilde{x}}) \cdot \mathrm{b}' f^1_{x_s}(\bar{\tilde{x}})].$$

Аналогично, для второго случая равны нулю 1-е, 4-е, 5-е, 8-е слагаемые:

$$\mathrm{d}_{\tilde{x}}[\mathrm{a} f(\tilde{x}) \cdot \mathrm{b} g(\tilde{x}) \oplus \mathrm{a} g(\bar{\tilde{x}}) \cdot \mathrm{b} f(\bar{\tilde{x}})] =$$

$$= \mathrm{d}_{\tilde{x}}[\mathtt{a}_s\bar{x}_s \cdot \mathtt{b}_s x_s \cdot \mathtt{a}' f^0_{x_s}(\tilde{x}) \cdot \mathtt{b}' g^1_{x_s}(\tilde{x})] \oplus$$
$$\oplus \mathrm{d}_{\tilde{x}}[\mathtt{a}_s x_s \cdot \mathtt{b}_s\bar{x}_s \cdot \mathtt{a}' f^1_{x_s}(\tilde{x}) \cdot \mathtt{b}' g^0_{x_s}(\tilde{x})] \oplus$$
$$\oplus \mathrm{d}_{\tilde{x}}[\mathtt{a}_s\bar{x}_s \cdot \mathtt{b}_s x_s \cdot \mathtt{a}' g^0_{x_s}(\bar{\tilde{x}}) \cdot \mathtt{b}' f^1_{x_s}(\bar{\tilde{x}})] \oplus$$
$$\oplus \mathrm{d}_{\tilde{x}}[\mathtt{a}_s x_s \cdot \mathtt{b}_s\bar{x}_s \cdot \mathtt{a}' g^1_{x_s}(\bar{\tilde{x}}) \cdot \mathtt{b}' f^0_{x_s}(\bar{\tilde{x}})].$$

В обоих случаях для остальных слагаемых применимо предположение индукции. Это завершает доказательство предложения. □

Предложение 3.4 носит технический характер, но оно позволяет доказать следующее важное свойство операторов.

Предложение 3.5. *Пусть заданы операторы* $\mathtt{a} = \mathtt{a}_1 \dots \mathtt{a}_n$ *и* $\mathtt{b} = \mathtt{b}_1 \dots \mathtt{b}_n$. *Тогда для любой функции* $f(\tilde{x})$ *равенство*

$$\mathrm{d}_{\tilde{x}}[\mathtt{a}f(\tilde{x}) \cdot \mathtt{b}f(\bar{\tilde{x}})] = 1$$

выполняется тогда и только тогда, когда f *— нечетная функция и* $\mathtt{a}_i \neq \mathtt{b}_i$ *для любого* $i \in \{1, \dots, n\}$.

Доказательство проведем индукцией по n.

Базис индукции. Пусть $n = 1$. Тогда

$$\mathrm{d}_{\tilde{x}}[\mathtt{a}f(\tilde{x}) \cdot \mathtt{b}f(\bar{\tilde{x}})] = \mathrm{d}_{x_1}[\mathtt{a}_1 f(x_1) \cdot \mathtt{b}_1 f(\bar{x}_1)]. \tag{3.6}$$

1) $\mathtt{a}_1 = \mathtt{b}_1 = \mathtt{d}$. В этом случае переменная x_1 фиктивна и выражение (3.6) равно $\mathbf{0}$.

2) $\mathtt{a}_1 = \mathtt{b}_1 \neq \mathtt{d}$. В этом случае получаем

$$\mathrm{d}_{x_1}[\mathtt{a}_1 f(x_1) \cdot \mathtt{b}_1 f(\bar{x}_1)] = \mathrm{d}_{x_1}[f(x_1) \cdot f(\bar{x}_1)] = 0.$$

3) $\mathtt{a}_1 \neq \mathtt{b}_1$. Тогда все возможные случаи можно объединить в два:

а) $\mathrm{d}_{x_1}[\mathtt{a}_1 f(x_1) \cdot \mathtt{b}_1 f(\bar{x}_1)] = \mathrm{d}_{x_1} f(x_1^{\sigma_1})$,

б) $\mathrm{d}_{x_1}[\mathtt{a}_1 f(x_1) \cdot \mathtt{b}_1 f(\bar{x}_1)] = \mathrm{d}_{x_1} f(x_1) \cdot \mathrm{d}_{x_1} f(\bar{x}_1)$.

В обоих случаях равенство $\mathrm{d}_{x_1}(\mathtt{a}_1 f(x_1) \cdot \mathtt{b}_1 f(\bar{x}_1)) = 1$ выполняется тогда и только тогда, когда функция $f(x_1)$ — нечетная.

Шаг индукции. Для $n > 1$ доказательство проводится индукцией по сумме весов: $l = w(\mathtt{a}) + w(\mathtt{b})$.

При $l = 0$ равенство следует из свойств производной:

$$\mathrm{d}_{\tilde{x}}[\mathtt{a}f(\tilde{x}) \cdot \mathtt{b}f(\bar{\tilde{x}})] = \mathrm{d}_{\tilde{x}}[f(\tilde{x}) \cdot f(\bar{\tilde{x}})] = 0.$$

Пусть $l > 0$, $\mathfrak{a}' = \mathfrak{a}_1 \dots \mathfrak{a}_{n-1}\mathfrak{e}$ и $\mathfrak{b}' = \mathfrak{b}_1 \dots \mathfrak{b}_{n-1}\mathfrak{e}$. Тогда $\mathfrak{a}$ и $\mathfrak{b}$ можно представить в виде:

$$\mathfrak{a}f(\tilde{x}) = \mathfrak{a}_n(\mathfrak{a}'f(\tilde{x})) \text{ и } \mathfrak{b}f(\tilde{x}) = \mathfrak{b}_n(\mathfrak{b}'f(\tilde{x})).$$

Такое представление позволяет сделать несколько несложных преобразований:

$$\begin{aligned}
\mathfrak{d}_{\tilde{x}}[\mathfrak{a}f(\tilde{x}) \cdot \mathfrak{b}f(\bar{\tilde{x}})] &= \mathfrak{d}_{\tilde{x}}[\mathfrak{a}_n(\mathfrak{a}'f(\tilde{x})) \cdot \mathfrak{b}_n(\mathfrak{b}'f(\bar{\tilde{x}}))] = \\
&= \mathfrak{d}_{\tilde{x}}\left[\mathfrak{a}_n\left(\mathfrak{a}'(\bar{x}_n f^0_{x_n}(\tilde{x}) \oplus x_n f^1_{x_n}(\tilde{x}))\right) \cdot \right. \\
&\quad \left. \cdot\, \mathfrak{b}_n\left(\mathfrak{b}'(x_n f^0_{x_n}(\bar{\tilde{x}}) \oplus \bar{x}_n f^1_{x_n}(\bar{\tilde{x}}))\right)\right] = \\
&= \mathfrak{d}_{\tilde{x}}\left[\left((\mathfrak{a}_n\bar{x}_n)(\mathfrak{a}'f^0_{x_n}(\tilde{x})) \oplus (\mathfrak{a}_n x_n)(\mathfrak{a}'f^1_{x_n}(\tilde{x}))\right) \cdot \right. \\
&\quad \left. \cdot\, \left((\mathfrak{b}_n x_n)(\mathfrak{b}'f^0_{x_n}(\bar{\tilde{x}})) \oplus (\mathfrak{b}_n\bar{x}_n)(\mathfrak{b}'f^1_{x_n}(\bar{\tilde{x}}))\right)\right] = \qquad (3.7) \\
&= \mathfrak{d}_{\tilde{x}}\left[(\mathfrak{a}_n\bar{x}_n)(\mathfrak{b}_n\bar{x}_n)\left(\mathfrak{a}'f^0_{x_n}(\tilde{x})\right)\left(\mathfrak{b}'f^0_{x_n}(\bar{\tilde{x}})\right)\right] \oplus \\
&\oplus \mathfrak{d}_{\tilde{x}}\left[(\mathfrak{a}_n\bar{x}_n)(\mathfrak{b}_n x_n)\left(\mathfrak{a}'f^0_{x_n}(\tilde{x})\right)\left(\mathfrak{b}'f^1_{x_n}(\bar{\tilde{x}})\right)\right] \oplus \\
&\oplus \mathfrak{d}_{\tilde{x}}\left[(\mathfrak{a}_n x_n)(\mathfrak{b}_n\bar{x}_n)\left(\mathfrak{a}'f^1_{x_n}(\tilde{x})\right)\left(\mathfrak{b}'f^0_{x_n}(\bar{\tilde{x}})\right)\right] \oplus \\
&\oplus \mathfrak{d}_{\tilde{x}}\left[(\mathfrak{a}_n x_n)(\mathfrak{b}_n x_n)\left(\mathfrak{a}'f^1_{x_n}(\tilde{x})\right)\left(\mathfrak{b}'f^1_{x_n}(\bar{\tilde{x}})\right)\right].
\end{aligned}$$

В полученном представлении выражения $\mathfrak{d}_{\tilde{x}}[\mathfrak{a}f(\tilde{x}) \cdot \mathfrak{b}f(\bar{\tilde{x}})]$ рассмотрим возможные значения для $\mathfrak{a}_n$ и $\mathfrak{b}_n$.

1) $\mathfrak{a}_n = \mathfrak{b}_n$.

а) $\mathfrak{a}_n = \mathfrak{d}$. В этом случае x_n фиктивная, следовательно

$$\mathfrak{d}\left(\mathfrak{a}f(\tilde{x}) \cdot \mathfrak{b}f(\bar{\tilde{x}})\right) = 0.$$

б) $\mathfrak{a}_n \neq \mathfrak{d}$. В этом случае равенство (3.7) примет вид

$$\begin{aligned}
&\mathfrak{d}_{\tilde{x}}\left(\mathfrak{a}f(\tilde{x}) \cdot \mathfrak{b}f(\bar{\tilde{x}})\right) = \\
&\quad = \mathfrak{d}_{\tilde{x}_n}\left[\mathfrak{a}'f^0_{x_n}(\tilde{x}) \cdot \mathfrak{b}'f^0_{x_n}(\bar{\tilde{x}})\right] \oplus \mathfrak{d}_{\tilde{x}_n}\left[\mathfrak{a}'f^1_{x_n}(\tilde{x}) \cdot \mathfrak{b}'f^1_{x_n}(\bar{\tilde{x}})\right].
\end{aligned}$$

По предложению 3.4 полученное выражение равно нулю.

2) $\mathfrak{a}_n \neq \mathfrak{b}_n$, $\mathfrak{a}_n \neq \mathfrak{d}$, $\mathfrak{b}_n \neq \mathfrak{d}$. В этом случае имеем

$$\begin{aligned}
&\mathfrak{d}_{\tilde{x}}[\mathfrak{a}f(\tilde{x}) \cdot \mathfrak{b}f(\bar{\tilde{x}})] = \\
&= \mathfrak{d}_{\tilde{x}_n}\left[\mathfrak{a}'f^0_{x_n}(\tilde{x}) \cdot \mathfrak{b}'f^1_{x_n}(\bar{\tilde{x}})\right] \oplus \mathfrak{d}_{\tilde{x}_n}\left[\mathfrak{a}'f^1_{x_n}(\tilde{x}) \cdot \mathfrak{b}'f^0_{x_n}(\bar{\tilde{x}})\right]. \qquad (3.8)
\end{aligned}$$

При четной функции $f(\tilde{x})$ могут быть два случая:

i) $f^0_{x_n}(\tilde{x})$ и $f^1_{x_n}(\tilde{x})$ — четные;
ii) $f^0_{x_n}(\tilde{x})$ и $f^1_{x_n}(\tilde{x})$ — нечетные.

В случае i) по индуктивному предположению оба слагаемых равны 0. В случае ii) также по индукции оба слагаемых одновременно равны 0, либо одновременно равны 1. В обоих случаях выражение (3.7) равно 0.

При нечетной $f(\tilde{x})$ ровно одна из остаточных четная. Пусть $f^0_{x_n}(\tilde{x})$ — четная. Тогда по индуктивному предположению для четной функции имеет место:

$$\mathrm{d}_{\tilde{x}}\left[\mathrm{a}' f^0_{x_n}(\tilde{x}) \cdot \mathrm{b}' f^1_{x_n}(\bar{\tilde{x}})\right] = 0.$$

Откуда получаем, что равенство (3.8) примет вид

$$\mathrm{d}_{\tilde{x}_n}[\mathrm{a} f(\tilde{x}) \cdot \mathrm{b} f(\bar{\tilde{x}})] = \mathrm{d}_{\tilde{x}_n}[\mathrm{a}' f^1_{x_n}(\tilde{x}) \cdot \mathrm{b}' f^0_{x_n}(\bar{\tilde{x}})],$$

и к нему применимо предположение индукции.

3) $\mathrm{a}_n \neq \mathrm{b}_n$ и $\mathrm{a}_n = \mathrm{d}$ или $\mathrm{b}_n = \mathrm{d}$. Тогда

$$\begin{aligned}\mathrm{d}_{\tilde{x}}[\mathrm{a} f(\tilde{x}) \cdot \mathrm{b} f(\bar{\tilde{x}})] = \\ = \mathrm{d}_{\tilde{x}_n}[\mathrm{a}' f^0_{x_n}(\tilde{x}) \cdot \mathrm{b}' f^0_{x_n}(\bar{\tilde{x}})] \oplus \mathrm{d}_{\tilde{x}_n}[\mathrm{a}' f^0_{x_n}(\tilde{x}) \cdot \mathrm{b}' f^1_{x_n}(\bar{\tilde{x}})] \oplus \\ \oplus \mathrm{d}_{\tilde{x}_n}[\mathrm{a}' f^1_{x_n}(\tilde{x}) \cdot \mathrm{b}' f^0_{x_n}(\bar{\tilde{x}})] \oplus \mathrm{d}_{\tilde{x}_n}[\mathrm{a}' f^1_{x_n}(\tilde{x}) \cdot \mathrm{b}' f^1_{x_n}(\bar{\tilde{x}})].\end{aligned}$$

По предложению 3.4 имеем тождество:

$$\mathrm{d}_{\tilde{x}_n}[\mathrm{a}' f^0_{x_n}(\tilde{x}) \cdot \mathrm{b}' f^0_{x_n}(\bar{\tilde{x}})] \oplus \mathrm{d}_{\tilde{x}_n}[\mathrm{a}' f^1_{x_n}(\tilde{x}) \cdot \mathrm{b}' f^1_{x_n}(\bar{\tilde{x}})] = 0.$$

Теперь достаточно повторить доказатедьство, аналогичное пункту 2), рассмотрев случаи четной и нечетной функции $f(\tilde{x})$.

Пункты 1)–3) дают полный набор значений для a_n и b_n. Таким образом, равенство:

$$\mathrm{d}_{\tilde{x}}[\mathrm{a} f(\tilde{x}) \cdot \mathrm{b} f(\bar{\tilde{x}})] = 1$$

выполняется тогда и только тогда, когда f — нечетная функция и $\mathrm{a}_i \neq \mathrm{b}_i$ для любого $i \in \tilde{n}$. □

§ 2. Два критерия существования базисных пучков

Нас будут интересовать базисные пучки, поскольку именно они дают возможность построения разложений булевых функций.

Предложение 3.5 позволяет в некоторых случаях рассматривать свойства непосредственно операторов, не обращаясь к функции, на которую они действуют. Действительно, значение

$$\alpha = \mathrm{d}_{\tilde{x}}[\mathrm{a}f(\tilde{x}) \cdot \mathrm{b}f(\bar{\tilde{x}})]$$

не зависит от функции $f(\tilde{x})$, единственное условие — эта функция должна быть нечетной.

Пусть $\mathrm{a} = \mathrm{a}_1 \dots \mathrm{a}_n$ и $\mathrm{b} = \mathrm{b}_1 \dots \mathrm{b}_n$ — два оператора. На этих операторах определим функционал "$\circ$" следующим образом:

$$\mathrm{a} \circ \mathrm{b} = \begin{cases} 1, & \text{если } \mathrm{a}_i \neq \mathrm{b}_i \text{ для любого } i \in \tilde{n}, \\ 0, & \text{в противном случае.} \end{cases}$$

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

$$M_{\mathrm{A}\times\mathrm{B}} = \begin{pmatrix} \mathrm{b}^{\tilde{1}} \circ \mathrm{a}^{\tilde{0}} & \cdots & \mathrm{b}^{\tilde{1}} \circ \mathrm{a}^{\tilde{\tau}} & \cdots & \mathrm{b}^{\tilde{1}} \circ \mathrm{a}^{\tilde{1}} \\ \vdots & & \vdots & & \vdots \\ \mathrm{b}^{\tilde{\tau}} \circ \mathrm{a}^{\tilde{0}} & \cdots & \mathrm{b}^{\tilde{\tau}} \circ \mathrm{a}^{\tilde{\tau}} & \cdots & \mathrm{b}^{\tilde{\tau}} \circ \mathrm{a}^{\tilde{1}} \\ \vdots & & \vdots & & \vdots \\ \mathrm{b}^{\tilde{0}} \circ \mathrm{a}^{\tilde{0}} & \cdots & \mathrm{b}^{\tilde{0}} \circ \mathrm{a}^{\tilde{\tau}} & \cdots & \mathrm{b}^{\tilde{0}} \circ \mathrm{a}^{\tilde{1}} \end{pmatrix}.$$

Если $\mathrm{A} = \mathrm{B}$, тогда $M_{\mathrm{A}\times\mathrm{A}}$ будет называться матрицей пучка A и обозначаться M_{A}.

Первый критерий базисного пучка. С матрицей пучка тесно связано свойство пучка быть базисным.

Теорема 3.1. *Пучок операторов* A *является базисным тогда и только тогда, когда*

$$\det M_{\mathrm{A}} \neq 0.$$

Доказательство. По определению базисного пучка для некоторой функции $f(\tilde{x})$ матрица $M_{\mathrm{A}f}$, построенная из

операторных образов этой функции:

$$M_{\mathbf{A}f} = \left(\mathrm{a}^{\tilde{0}} f(\tilde{x}) \quad \ldots \quad \mathrm{a}^{\tilde{1}} f(\tilde{x}) \right),$$

является невырожденной. Здесь $\mathrm{a}^{\tilde{\tau}} f(\tilde{x})$ — операторные образы функции $f(\tilde{x})$ являются столбцами матрицы.

Тогда матрица

$${}^{t}M_{\mathbf{A}f} = \begin{pmatrix} \mathrm{a}^{\tilde{1}} f(\overline{\tilde{x}}) \\ \vdots \\ \mathrm{a}^{\tilde{0}} f(\overline{\tilde{x}}) \end{pmatrix}$$

также является невырожденной. Здесь функции $\mathrm{a}^{\tilde{\tau}} f(\overline{\tilde{x}})$ — строки матрицы. ${}^{t}M_{\mathbf{A}f}$ получена из $M_{\mathbf{A}f}$ транспонированием по побочной диагонали.

Нужно заметить, что функция $f(\tilde{x})$ должна быть нечетной, иначе по предложению 3.2 сумма всех строк матрицы будет равна нулевой строке.

Рассмотрим произведение $M = {}^{t}M_{\mathbf{A}f} \times M_{\mathbf{A}f}$. Поскольку обе матрицы — невырожденные, их произведение — также невырожденная матрица, следовательно, имеем равенство:

$$\det \left({}^{t}M_{\mathbf{A}f} \times M_{\mathbf{A}f} \right) \neq 0.$$

Пусть $m_{\tilde{\tau}\tilde{\sigma}}$ элементы матрицы M. Тогда

$$m_{\tilde{\tau}\tilde{\sigma}} = \sum_{\tilde{\delta} \in E^n} \mathrm{a}^{\overline{\tilde{\tau}}} f(\overline{\tilde{\delta}}) \cdot \mathrm{a}^{\tilde{\sigma}} f(\tilde{\delta}) = \mathrm{d}_{\tilde{x}} [\mathrm{a}^{\overline{\tilde{\tau}}} f(\overline{\tilde{x}}) \cdot \mathrm{a}^{\tilde{\sigma}} f(\overline{\tilde{x}})] = \mathrm{a}^{\overline{\tilde{\tau}}} \circ \mathrm{a}^{\tilde{\sigma}}.$$

Таким образом, $M = M_{\mathbf{A}}$ и, следовательно:

$$\det M_{\mathbf{A}} = \det M \neq 0.$$

В обратную сторону доказательство аналогично. Поскольку невырожденная матрица представляется произведением матриц такого же порядка, то сомножители также должны быть невырожденными. Один из сомножителей и есть матрица соответствующего базисного пучка, столбцы которой дают базис пространства всех функций от соответствующего числа переменных. □

В следующем утверждении введено разложение операторного образа функции по операторным образам базисного пучка этой же функции.

Предложение 3.6. *Для любого базисного пучка операторов* $(\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{1}})$, *для любого оператора* t *найдутся* $\tilde{\tau}_1, \ldots, \tilde{\tau}_k$ *такие, что для любой функции* $f(\tilde{x})$ *имеет место разложение*:

$$\mathrm{t}f(\tilde{x}) = \mathrm{a}^{\tilde{\tau}_1} f(\tilde{x}) \oplus \ldots \oplus \mathrm{a}^{\tilde{\tau}_k} f(\tilde{x}).$$

Доказательство. Согласно определению базисного пучка, пусть $g(\tilde{x})$ — такая функция, что система

$$\left\{\mathrm{a}^{\tilde{0}} g(\tilde{x}), \ldots, \mathrm{a}^{\tilde{\tau}} g(\tilde{x}), \ldots, \mathrm{a}^{\tilde{1}} g(\tilde{x})\right\}$$

является базисом.

Тогда любая функция может быть разложена по базису:

$$f(\tilde{x}) = \alpha_{\tilde{0}} \mathrm{a}^{\tilde{0}} g(\tilde{x}) \oplus \ldots \oplus \alpha_{\tilde{1}} \mathrm{a}^{\tilde{1}} g(\tilde{x}).$$

В матричной форме это выглядит так:

$$\left(\mathrm{a}^{\tilde{0}} g(\tilde{x}) \ldots \mathrm{a}^{\tilde{1}} g(\tilde{x})\right) \begin{pmatrix} \alpha_{\tilde{0}} \\ \vdots \\ \alpha_{\tilde{1}} \end{pmatrix} = f(\tilde{x}). \tag{3.9}$$

Поскольку система функций

$$\left\{\mathrm{a}^{\tilde{1}} g(\bar{\tilde{x}}), \ldots, \mathrm{a}^{\tilde{0}} g(\bar{\tilde{x}})\right\}$$

— линейно независима, можно умножить обе части равенства (3.9) на невырожденную матрицу

$${}^{t}M_{\mathrm{A}g} = \begin{pmatrix} \mathrm{a}^{\tilde{1}} g(\bar{\tilde{x}}) \\ \vdots \\ \mathrm{a}^{\tilde{0}} g(\bar{\tilde{x}}) \end{pmatrix}.$$

Равенство (3.9) примет вид:

$$\begin{pmatrix} \mathrm{a}^{\tilde{1}} g(\bar{\tilde{x}}) \\ \vdots \\ \mathrm{a}^{\tilde{0}} g(\bar{\tilde{x}}) \end{pmatrix} \left(\mathrm{a}^{\tilde{0}} g(\tilde{x}) \ldots \mathrm{a}^{\tilde{1}} g(\tilde{x})\right) \begin{pmatrix} \alpha_{\tilde{0}} \\ \vdots \\ \alpha_{\tilde{1}} \end{pmatrix} = \begin{pmatrix} \mathrm{a}^{\tilde{1}} g(\bar{\tilde{x}}) \\ \vdots \\ \mathrm{a}^{\tilde{0}} g(\bar{\tilde{x}}) \end{pmatrix} f.$$

По предложению 3.5 произведение двух первых матриц не зависит от функции $g(\tilde{x})$ и может быть представлено через функционал "o":

$$\begin{pmatrix} \mathrm{a}^{\tilde{1}} g(\tilde{\bar{x}}) \\ \vdots \\ \mathrm{a}^{\tilde{0}} g(\tilde{\bar{x}}) \end{pmatrix} \left(\mathrm{a}^{\tilde{0}} g(\tilde{x}) \dots \mathrm{a}^{\tilde{1}} g(\tilde{x}) \right) = \begin{pmatrix} \mathrm{a}^{\tilde{1}} \circ \mathrm{a}^{\tilde{0}} & \dots & \mathrm{a}^{\tilde{1}} \circ \mathrm{a}^{\tilde{1}} \\ \vdots & \ddots & \vdots \\ \mathrm{a}^{\tilde{0}} \circ \mathrm{a}^{\tilde{0}} & \dots & \mathrm{a}^{\tilde{0}} \circ \mathrm{a}^{\tilde{1}} \end{pmatrix} = M_{\mathrm{A}}.$$

Получена матрица оператора M_{A}, являющаяся невырожденной. Следовательно существует обратная к ней матрица M_{A}^{-1}. Тогда умножив обе части равенства на M_{A}^{-1}, имеем

$$M_{\mathrm{A}}^{-1} \cdot M_{\mathrm{A}} \cdot \begin{pmatrix} \alpha_{\tilde{0}} \\ \vdots \\ \alpha_{\tilde{1}} \end{pmatrix} = M_{\mathrm{A}}^{-1} \cdot \begin{pmatrix} \mathrm{a}^{\tilde{1}} g(\tilde{\bar{x}}) \\ \vdots \\ \mathrm{a}^{\tilde{0}} g(\tilde{\bar{x}}) \end{pmatrix} f.$$

Поскольку полученное равенство имеет место для любой функции $f(\tilde{x})$, положим $f(\tilde{x}) = \mathrm{t}g(\tilde{x})$. Тогда

$$\begin{pmatrix} \alpha_{\tilde{0}} \\ \vdots \\ \alpha_{\tilde{1}} \end{pmatrix} = M_{\mathrm{A}}^{-1} \cdot \begin{pmatrix} \mathrm{a}^{\tilde{1}} g(\tilde{\bar{x}}) \\ \vdots \\ \mathrm{a}^{\tilde{0}} g(\tilde{\bar{x}}) \end{pmatrix} \cdot \mathrm{t}g(\tilde{x}) = M_{\mathrm{A}}^{-1} \cdot \begin{pmatrix} \mathrm{a}^{\tilde{1}} \circ \mathrm{t} \\ \vdots \\ \mathrm{a}^{\tilde{0}} \circ \mathrm{t} \end{pmatrix}.$$

Полученные значения для $\alpha_{\tilde{\tau}}$ не зависят от конкретной функции $g(\tilde{x})$. Таким образом, теорема выполняется, если функция $f(\tilde{x})$ — нечетная.

В случае, когда функция $f(\tilde{x})$ — четная, положим $g(\tilde{x}) = f(\tilde{x}) \oplus x_1 \cdot \ldots \cdot x_n$. Очевидно, полученная функция $g(\tilde{x})$ — нечетная. Следовательно, по доказанному имеем

$$\mathrm{t}g(\tilde{x}) = \mathrm{a}^{\tilde{\tau}_1} g(\tilde{x}) \oplus \ldots \oplus \mathrm{a}^{\tilde{\tau}_k} g(\tilde{x}).$$

Проведем несколько преобразований, воспользовавшись свойством операторов из предложения 3.1:

$$\mathrm{t}\left(f(\tilde{x}) \oplus (x_1 \cdot \ldots \cdot x_n)\right) = \mathrm{t}f(\tilde{x}) \oplus \mathrm{t}\left(x_1 \cdot \ldots \cdot x_n\right) =$$
$$= \mathrm{a}^{\tilde{\tau}_1} f(\tilde{x}) \oplus \ldots \oplus \mathrm{a}^{\tilde{\tau}_k} f(\tilde{x}) \oplus \mathrm{a}^{\tilde{\tau}_1}\left(x_1 \cdot \ldots \cdot x_n\right) \oplus \ldots \oplus \mathrm{a}^{\tilde{\tau}_k}\left(x_1 \cdot \ldots \cdot x_n\right).$$

Поскольку функция $x_1 \cdot \ldots \cdot x_n$ — нечетная, для нее выполняется:

$$\mathrm{t}\left(x_1 \cdot \ldots \cdot x_n\right) = \mathrm{a}^{\tilde{\tau}_1}\left(x_1 \cdot \ldots \cdot x_n\right) \oplus \ldots \oplus \mathrm{a}^{\tilde{\tau}_1}\left(x_1 \cdot \ldots \cdot x_n\right).$$

После соответствующих сокращений получаем, что и для четной функции $f(\tilde{x})$ выполняется:

$$\mathrm{t}f(\tilde{x}) = \mathrm{a}^{\tilde{\tau}_1} f(\tilde{x}) \oplus \ldots \oplus \mathrm{a}^{\tilde{\tau}_k} f(\tilde{x})$$

при тех же самых $\tilde{\tau}_1, \ldots, \tilde{\tau}_k$. □

Второй критерий базисного пучка.

Из предложения 3.6 следует, что набор $\tilde{\tau}_1, \ldots, \tilde{\tau}_k$ в разложении функции $\mathrm{t}f(\tilde{x})$ зависит от вида оператора t и не зависит от конкретной функции $f(\tilde{x})$. Это позволяет ввести еще один критерий базисного пучка.

Теорема 3.2. *Пучок операторов* $(\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{1}})$ *— базисный тогда и только тогда, когда для любого оператора* t *найдутся* $\tilde{\tau}_1, \ldots, \tilde{\tau}_k$ *такие, что имеет место следующее разложение для любой функции* $f(\tilde{x})$:

$$\mathrm{t}f(\tilde{x}) = \mathrm{a}^{\tilde{\tau}_1} f(\tilde{x}) \oplus \ldots \oplus \mathrm{a}^{\tilde{\tau}_k} f(\tilde{x}).$$

Доказательство. Если A — базисный пучок операторов, тогда по предложению 3.6 для любого оператора t существует набор констант $(\alpha_{\tilde{0}}, \ldots, \alpha_{\tilde{1}})$, такой что для любой функции $f(\tilde{x})$ имеет место разложение:

$$\mathrm{t}f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \mathrm{a}^{\tilde{\tau}} f(\tilde{x}).$$

Для доказательства в обратную сторону определим набор операторов $\mathrm{t}^{\tilde{0}}, \ldots, \mathrm{t}^{\tilde{1}}$. Оператор $\mathrm{t}^{\tilde{\tau}}$ определяется покомпонентно следующим образом:

$$\mathrm{t}_i^{\tilde{\tau}} = \begin{cases} \mathrm{d}, & \text{если } \tau_i = 0, \\ e, & \text{если } \tau_i = 1. \end{cases}$$

Рассмотрим набор функций: $\{\mathrm{t}^{\tilde{0}}(x_1 \cdot \ldots \cdot x_n), \ldots, \mathrm{t}^{\tilde{1}}(x_1 \cdot \ldots \cdot x_n)\}$.

Очевидно, что этот набор функций совпадает с базисными функциями полинома Жегалкина и для любой функции $f(\tilde{x})$ имеем следующее представление:

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \mathrm{t}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n).$$

По условию теоремы получаем

$$\mathrm{t}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) = \sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\sigma}}^{\tilde{\tau}} \mathrm{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n).$$

Таким образом, для любой функции $f(\tilde{x})$ выполняется равенство

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \left(\sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\sigma}}^{\tilde{\tau}} \mathrm{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) \right) =$$

$$= \sum_{\tilde{\sigma} \in E^n} \left(\sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\sigma}}^{\tilde{\tau}} \cdot \alpha_{\tilde{\tau}} \right) \cdot \mathrm{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n) =$$

$$= \sum_{\tilde{\sigma} \in E^n} \gamma_{\tilde{\sigma}} \cdot \mathrm{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n),$$

где $\gamma_{\tilde{\sigma}} = \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\sigma}}^{\tilde{\tau}} \cdot \alpha_{\tilde{\tau}}$.

Из последнего равенства следует, что операторный пучок $\{\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{1}}\}$ — базисный. □

Доказанная теорема позволяет ввести операцию «сложение» непосредственно на операторах. Для такого сложения будет использоваться символ «$\oplus$». Это не вызывает коллизий и хорошо согласуется с определением операции:

$\mathrm{c} = \mathrm{a} \oplus \mathrm{b}$ тогда и только тогда, когда имеет место равенство

$$\mathrm{c}f(\tilde{x}) = \mathrm{a}f(\tilde{x}) \oplus \mathrm{b}f(\tilde{x}) \quad \text{для любой функции } f(\tilde{x}).$$

Очевидно, что эта операция частичная. Она определена на парах операторов, отличающихся только по одной компоненте. Пусть $\mathrm{a} = \mathrm{a}_1 \ldots \mathrm{a}_n$ и $\mathrm{b} = \mathrm{b}_1 \ldots \mathrm{b}_n$ — два оператора, отличающиеся в позиции с номером s. Результат такой операции выглядит так:

$$\mathrm{a}_1 \ldots \mathrm{a}_n \oplus \mathrm{b}_1 \ldots \mathrm{b}_n = \mathrm{c}_1 \ldots \mathrm{c}_n,$$

где $\mathrm{c}_i = \mathrm{a}_i$ для $i \neq s$; $\mathrm{c}_i \neq \mathrm{a}_i$ и $\mathrm{c}_i \neq \mathrm{b}_i$ для $i = s$.

Поскольку $\mathrm{a}_i, \mathrm{b}_i, \mathrm{c}_i \in \{\mathrm{e}, \mathrm{p}, \mathrm{d}\}$, то для так определенных пар операторов a и b оператор c всегда существует. Определение является следствием свойства, что для любой функции $f(\tilde{x})$ имеет место равенство:

$$\mathrm{d}_{x_s} f(\tilde{x}) \oplus \mathrm{p}_{x_s} f(\tilde{x}) = \mathrm{e}_{x_s} f(\tilde{x}).$$

В случаях, когда легко показать определенность этой операции, переход на "сложение" операторов позволяет сократить и упростить изложение доказательств.

Для следующего свойства пучков будет применяться термин «дистрибутивность».

Предложение 3.7. *Если для операторов* $\mathtt{a}$, $\mathtt{b}$ *и* $\mathtt{c}$ *выполняется* $\mathtt{c} = \mathtt{a} \oplus \mathtt{b}$, *тогда для любого оператора* $\mathtt{t}$ *выполняется равенство*:

$$\mathtt{t} \circ (\mathtt{a} \oplus \mathtt{b}) = (\mathtt{t} \circ \mathtt{a}) \oplus (\mathtt{t} \circ \mathtt{b}). \tag{3.10}$$

Доказательство. Согласно определению операции "$\oplus$" на операторах, операторы $\mathtt{a}$, $\mathtt{b}$ и $\mathtt{c}$ должны различаться только по одной — s-й компоненте. Для упрощения записи пусть $s = n$, тогда операторы должны иметь вид

$$\mathtt{a} = \mathtt{a}_1 \ldots \mathtt{a}_{n-1}\mathtt{a}_n;\ \mathtt{b} = \mathtt{a}_1 \ldots \mathtt{a}_{n-1}\mathtt{b}_n;\ \mathtt{c} = \mathtt{a}_1 \ldots \mathtt{a}_{n-1}\mathtt{c}_n,$$

где $\mathtt{a}_n \neq \mathtt{b}_n$, $\mathtt{a}_n \neq \mathtt{c}_n$, $\mathtt{c}_n \neq \mathtt{b}_n$.

Если $\mathtt{t} \circ \mathtt{c} = 1$, тогда для любого i должно выполняться $\mathtt{t}_i \neq \mathtt{c}_i$. Имеют место два случая:

1) либо $\mathtt{t}_n = \mathtt{a}_n$ и $\mathtt{t}_n \neq \mathtt{b}_n$,

2) либо $\mathtt{t}_n \neq \mathtt{a}_n$ и $\mathtt{t}_n = \mathtt{b}_n$.

В обоих случаях получаются тождества:

1) $1 = (\mathtt{t} \circ \mathtt{a}) \oplus (\mathtt{t} \circ \mathtt{b}) = 0 \oplus 1 = 1$;

2) $1 = (\mathtt{t} \circ \mathtt{a}) \oplus (\mathtt{t} \circ \mathtt{b}) = 1 \oplus 0 = 1$.

Если $\mathtt{t} \circ \mathtt{c} = 0$, тогда существует хотя бы одно i, для которого выполняется $\mathtt{t}_i = \mathtt{c}_i$.

Если $i < n$, то равенство нулю правой части (3.10) очевидно.

Если $i = n$, то из равенства $\mathtt{t}_n = \mathtt{c}_n$ следует, что $\mathtt{t}_n \neq \mathtt{a}_n$ и $\mathtt{t}_n \neq \mathtt{b}_n$. Откуда следует тождество:

$$0 = (\mathtt{t} \circ \mathtt{a}) \oplus (\mathtt{t} \circ \mathtt{b}) = 1 \oplus 1 = 0. \qquad \square$$

Способы порождения базисных пучков.

Пусть имеются $\mathrm{A} = (\mathtt{a}^{\tilde{0}}, \ldots, \mathtt{a}^{\tilde{1}})$ — пучок операторов размерности n и набор из 2^n пучков

$$\{\mathrm{B}_{\tilde{\sigma}} | \mathrm{B}_{\tilde{\sigma}} = (\mathtt{b}_{\tilde{\sigma}}^{\tilde{0}}, \ldots, \mathtt{b}_{\tilde{\sigma}}^{\tilde{1}})\}$$

операторов размерности m. Пучок $\mathrm{C} = (\mathtt{c}^{\tilde{0}}, \ldots, \mathtt{c}^{\tilde{1}})$ операторов размерности $m + n$ называется слиянием пучков $\mathrm{B}_{\tilde{0}}, \ldots, \mathrm{B}_{\tilde{1}}$ по

пучку A, если компоненты $c^{\tilde{\tau}} = t_1 \dots t_{n+m}$ пучка C определены так:

$$(t_1 \dots t_n) = a^{\tilde{\tau}'} \quad (t_{n+1} \dots t_{n+m}) = b^{\tilde{\tau}''}_{\tilde{\tau}'},$$

где $\tilde{\tau}' = (\tau_1, \dots, \tau_n)$, $\tilde{\tau}'' = (\tau_{n+1}, \dots, \tau_{n+m})$.

Пучок $B = (b^{\tilde{0}}, \dots, b^{\tilde{1}})$ операторов размерности n называется перестановкой пучка $A = (a^{\tilde{0}}, \dots, a^{\tilde{1}})$, если компоненты $b^{\tilde{\tau}} = t_1 \dots t_n$ пучка B построены из соответствующих компонент пучка A следующим образом:

$$t_{i_1} \dots t_{i_n} = a^{\tilde{\tau}},$$

где $I = i_1, \dots, i_n$ — некоторая перестановка $1, \dots, n$ и обозначается символом $B = I(A)$. Это обозначение перестановки будет применяться и для операторов: $b = I(a)$.

Пучок операторов $B = (b^{\tilde{0}}, \dots, b^{\tilde{1}})$ назовем *линейным преобразованием пучка* $A = (a^{\tilde{0}}, \dots, a^{\tilde{1}})$, если компоненты $b^{\tilde{\tau}}$ пучка B являются линейными комбинациями компонент пучка A:

$$b^{\tilde{\tau}} = j^{\tilde{\tau}}_{\tilde{0}} a^{\tilde{0}} \oplus \dots \oplus j^{\tilde{\tau}}_{\tilde{\sigma}} a^{\tilde{\sigma}} \oplus \dots \oplus j^{\tilde{\tau}}_{\tilde{1}} a^{\tilde{1}},$$

где $j^{\tilde{\tau}}_{\tilde{\sigma}} \in \{0, 1\}$.

Пусть $J = [j^{\tilde{\tau}}_{\tilde{\sigma}}]$ — матрица, столбцы которой соответствуют компонентам пучка B (или линейным комбинациям компонент пучка A). Тогда линейное преобразование пучка A можно представить в виде «произведения»: $B = A \times J$. Такая запись достаточно удобна и будет использоваться в последующем изложении.

Теорема 3.3. *Пусть имеются набор базисных пучков операторов* $B_{\tilde{\sigma}}$ *и базисный пучок* A. *Тогда имеют место следующие утверждения:*

1. *Слияние пучков* B_σ *по пучку* A *является базисным пучком.*

2. *Перестановка* $C = I(A)$ *является базисным пучком.*

3. *Пусть* J *— матрица, в которой каждый столбец соответствует некоторому оператору, являющемуся линейной комбинацией пучка* A, *тогда если* J *— невырожденная матрица, то линейное преобразование* $C = A \times J$ *является базисным пучком.*

Доказательство. 1. По определению базисного пучка достаточно доказать линейную независимость образов пучка C для функции $x_1 \cdot \ldots \cdot x_n \cdot y_1 \cdot \ldots \cdot y_m$.

По определению базисного пучка системы функций

$$\{\mathrm{a}^{\tilde{0}}(x_1 \cdot \ldots \cdot x_n), \ldots, \mathrm{a}^{\tilde{1}}(x_1 \cdot \ldots \cdot x_n)\},$$
$$\{\mathrm{b}^{\tilde{0}}_{\tilde{\sigma}}(y_1 \cdot \ldots \cdot y_m), \ldots, \mathrm{b}^{\tilde{1}}_{\tilde{\sigma}}(y_1 \cdot \ldots \cdot y_m)\}$$

— линейно независимы.

Предположим, что существует набор из 2^{m+n} констант $\alpha_{\tilde{\tau}}$, такой что

$$\sum_{\tilde{\tau} \in E^{n+m}} \alpha_{\tilde{\tau}} \mathrm{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n \cdot y_1 \cdot \ldots \cdot y_m) = 0.$$

Эту сумму можно преобразовать, согласно свойствам пучков:

$$\sum_{\tilde{\tau} \in E^{n+m}} \alpha_{\tilde{\tau}} \mathrm{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n \cdot y_1 \cdot \ldots \cdot y_m) =$$
$$= \sum_{\tilde{\tau} \in E^{n+m}} \alpha_{\tilde{\tau}} \mathrm{a}^{\tilde{\tau}'}(x_1 \cdot \ldots \cdot x_n) \mathrm{b}^{\tilde{\tau}''}_{\tilde{\tau}'}(y_1 \cdot \ldots \cdot y_m) =$$
$$= \sum_{\tilde{\tau}' \in E^n} \mathrm{a}^{\tilde{\tau}'}(x_1 \cdot \ldots \cdot x_n) \sum_{\tilde{\tau}'' \in E^m} \alpha_{\tilde{\tau}} \mathrm{b}^{\tilde{\tau}''}_{\tilde{\tau}'}(y_1 \cdot \ldots \cdot y_m) = 0.$$

Из линейной независимости операторных образов функции $x_1 \cdot \ldots \cdot x_n$ по пучку A следует, что для любого $\tilde{\tau}'$:

$$\sum_{\tilde{\tau}'' \in E^m} \alpha_{\tilde{\tau}} \mathrm{b}^{\tilde{\tau}''}_{\tilde{\tau}'}(y_1 \cdot \ldots \cdot y_m) = 0.$$

В свою очередь операторные образы функции $y_1 \cdot \ldots \cdot y_m$ по любому из пучков $\mathrm{B}_{\tilde{\tau}'}$ также линейно независимы. Что влечет $\alpha_{\tilde{\tau}} = 0$ при любом $\tilde{\tau}$ и, следовательно, так построенный операторный пучок C — базисный.

2. Из определения базисного пучка следует, что система операторных образов функции $x_1 \cdot \ldots \cdot x_n$

$$\{\mathrm{a}^{\tilde{0}}(x_1 \cdot \ldots \cdot x_n), \ldots, \mathrm{a}^{\tilde{1}}(x_1 \cdot \ldots \cdot x_n)\}$$

— линейно независима.

В силу симметричности функции $x_1 \cdot \ldots \cdot x_n$ данная система совпадает со следующей:

$$\{\mathrm{b}^{\tilde{0}}(x_{i_1} \cdot \ldots \cdot x_{i_n}), \ldots, \mathrm{b}^{\tilde{1}}(x_{i_1} \cdot \ldots \cdot x_{i_n})\}.$$

Таким образом, имеется линейно независимая система образов некоторой функции по пучку B. Согласно определению пучок B — базисный.

3. Пусть $g(x_1, \ldots, x_n)$ — нечетная функция. Рассмотрим матрицу

$$M_{C_g} = \left(\mathrm{c}^{\tilde{0}} g(\tilde{x}) \quad \ldots \quad \mathrm{c}^{\tilde{1}} g(\tilde{x}) \right).$$

Здесь $\mathrm{c}^{\tilde{\tau}} g(\tilde{x})$ — столбцы матрицы.

Согласно определению пучка C эта матрица может быть представлена так:

$$M_{C_g} = \left(\mathrm{a}^{\tilde{0}} g(\tilde{x}) \quad \ldots \quad \mathrm{a}^{\tilde{1}} g(\tilde{x}) \right) \times J = M_{A_g} \times J.$$

По условию матрицы M_{A_g} и J — невырожденные. Следовательно матрица M_{C_g} также является невырожденной, как произведение невырожденных. Эта матрица представляет собой векторную запись системы образов функции g по пучку операторов C. □

Класс функций, образы которых по базисному пучку операторов порождают базисы.

Итак, мы определили базисный пучок, нашли критерии существования и способы построения таких пучков. В определении базисного пучка присутствует только одна функция, образы которой и порождают базис пространства всех функций от n переменных. Естественно рассмотреть вопрос о существовании других функций, позволяющих строить базисы, и тем самым — канонические формы. Описание класса таких функций дает следующая теорема.

Теорема 3.4. *Пусть* A — *базисный пучок операторов. Множество функций*

$$\{\mathrm{a}^{\tilde{0}}(g), \ldots, \mathrm{a}^{\tilde{\tau}}(g), \ldots, \mathrm{a}^{\tilde{1}}(g)\}$$

является базисом линейного пространства всех функций от n переменных тогда и только тогда, когда функция $g(x_1, \ldots, x_n)$ — *нечетная.*

Доказательство. Достаточно показать, что для любого базисного пучка операторов A матрица

$$M_{\mathrm{A}g} = \begin{pmatrix} \mathrm{a}^{\tilde{0}} g(\tilde{x}) & \dots & \mathrm{a}^{\tilde{1}} g(\tilde{x}) \end{pmatrix}$$

является невырожденной тогда и только тогда, когда выполняется равенство $\mathrm{d}_{\tilde{x}}(g(\tilde{x})) = 1$.

В теореме 3.1 доказано, что если функция — нечетная, т.е. $\mathrm{d}_{\tilde{x}}(g(\tilde{x})) = 1$, то $M_{\mathrm{A}g}$ является невырожденной. Если функция $g(\tilde{x})$ — четная, то по предложению 3.2 операторный образ четной функции — четная функция. Откуда следует вырожденность матрицы $M_{\mathrm{A}g}$. □

§ 3. Специальные классы базисных пучков

В этом параграфе введены и исследованы несколько специальных классов базисных пучков операторов.

Однородные пучки операторов.
Пучок операторов $\mathrm{A} = (\mathrm{a}^{\tilde{0}}, \dots, \mathrm{a}^{\tilde{\tau}}, \dots, \mathrm{a}^{\tilde{1}})$ будем называть однородно двупорожденным (или просто — однородным), если существуют такие операторы $\mathrm{b} = \mathrm{b}_0 \dots \mathrm{b}_n$ и $\mathrm{c} = \mathrm{c}_0 \dots \mathrm{c}_n$, $\mathrm{b}_i \neq \mathrm{c}_i$ для любого i, что оператор $\mathrm{a}^{\tilde{\tau}} = \mathrm{t}_1 \dots \mathrm{t}_n$ пучка A определяется следующим образом:

$$\mathrm{t}_i = \begin{cases} \mathrm{b}_i, & \text{если } \tau_i = 0, \\ \mathrm{c}_i, & \text{если } \tau_i = 1. \end{cases}$$

Предложение 3.8. *Пусть* $\mathrm{A} = (\mathrm{a}^{\tilde{0}}, \dots, \mathrm{a}^{\tilde{1}})$ — *однородный пучок операторов. Пучок* $\mathrm{B} = (\mathrm{b}^{\tilde{0}}, \dots, \mathrm{b}^{\tilde{1}})$ *получен из пучка* A *перестановкой операторов по следующему правилу:*

$$\mathrm{b}^{\tilde{\sigma}} = \mathrm{a}^{\tilde{\sigma} \oplus \tilde{\tau}},$$

где $\tilde{\sigma} \oplus \tilde{\tau}$ — *покомпонентное сложение векторов* $\tilde{\sigma} = \sigma_1 \dots \sigma_n$ *и* $\tilde{\tau} = \tau_1 \dots \tau_n$. *Тогда пучок* B *также является однородным.*

Доказательство. Поскольку пучок B является перестановкой операторов в базисном пучке, он является базисным.

Для доказательства его однородности достаточно показать, что выполняется свойство:

$$\mathrm{b}^{\tilde{\sigma}} \circ \mathrm{b}^{\tilde{\tau}} = 1$$

тогда и только тогда, когда $\tilde{\sigma} = \overline{\tilde{\tau}}$. А это свойство непосредственно следует из соотношения:

$$\overline{\tilde{\sigma}} \oplus \tilde{\tau} = \overline{\tilde{\sigma} \oplus \tilde{\tau}}.$$

Это соотношение гарантирует, что если выполняется равенство $\mathrm{b}^{\tilde{\sigma}} = \mathrm{a}^{\tilde{\tau}}$, тогда выполняется и равенство $\mathrm{b}^{\overline{\tilde{\sigma}}} = \mathrm{a}^{\overline{\tilde{\tau}}}$. □

Предложение 3.9. *Для любых* A *и* B — *однородных пучков операторов существуют такие* $\tilde{\sigma}$ *и* $\tilde{\tau}$, *что* $\mathrm{a}^{\tilde{\sigma}} = \mathrm{b}^{\tilde{\tau}}$.

Доказательство. Пусть пучки порождены парами операторов:

$$\mathrm{A} = (\mathrm{a}_1 \dots \mathrm{a}_n, \dots, \mathrm{b}_1 \dots \mathrm{b}_n), \quad \mathrm{B} = (\mathrm{c}_1 \dots \mathrm{c}_n, \dots, \mathrm{d}_1 \dots \mathrm{d}_n).$$

Оператор $\mathrm{c}_1 \dots \mathrm{c}_n$ относительно порождающих операторов пучка A можно представить в виде:

$$\mathrm{c}_1 \dots \mathrm{c}_n = \mathrm{a}_1 \dots \mathrm{a}_k \mathrm{b}_{k+1} \dots \mathrm{b}_m \mathrm{c}_{m+1} \dots \mathrm{c}_n.$$

Для упрощения записи считаем, что индексы идут по порядку. Это не влияет на общность рассуждений.

Аналогично представляем оператор $\mathrm{d}_1 \dots \mathrm{d}_n$ относительно тех же операторов, при этом не забывая, что $\mathrm{c}_i \neq \mathrm{d}_i$ для любого i. Получаем представление второго порождающего оператора пучка B:

$$\mathrm{d}_1 \dots \mathrm{d}_n = \\ = \mathrm{b}_1 \dots \mathrm{b}_s \mathrm{d}_{s+1} \dots \mathrm{d}_k \mathrm{a}_{k+1} \dots \mathrm{a}_l \mathrm{d}_{l+1} \dots \mathrm{d}_m \mathrm{a}_{m+1} \dots \mathrm{a}_r \mathrm{b}_{r+1} \dots \mathrm{b}_n.$$

Откуда получаем требуемые номера одинаковых операторов:

$$\tilde{\tau} = 0 \dots 0_k 0 \dots 0_m 1 \dots 1_n,$$
$$\tilde{\sigma} = 0 \dots 0_s 1 \dots 1_k 0 \dots 0_l 1 \dots 1_m 0 \dots 0_r 0 \dots 0_n.$$

Нижние индексы вставлены неформально для обозначения места смены нулей на единицы и наоборот. □

Предложение 3.10. *Пусть* $\mathrm{A} = (\mathrm{a}^{\tilde{0}}, \dots, \mathrm{a}^{\tilde{\tau}}, \dots, \mathrm{a}^{\tilde{1}})$ — *однородный пучок операторов. Тогда существует оператор* $\mathrm{b} = \mathrm{b}_1 \dots \mathrm{b}_n$ *такой, что*

$$\mathrm{b} = \sum_{\tilde{\tau} \in E^n} \mathrm{a}^{\tilde{\tau}},$$

причем если $\mathfrak{a}^{\tilde{0}} = \mathfrak{c}_1 \dots \mathfrak{c}_n$, $\mathfrak{a}^{\tilde{1}} = \mathfrak{t}_1 \dots \mathfrak{t}_2$, *тогда* $\mathfrak{b}_i \neq \mathfrak{c}_i$ *и* $\mathfrak{b}_i \neq \mathfrak{t}_i$ *для любого* i.

Доказательство проведем индукцией по n.

Базис индукции. При $n = 1$ однородный пучок выглядит так: $(\mathfrak{a}^{\tilde{0}}, \mathfrak{a}^{\tilde{1}})$, причем $\mathfrak{a}^{\tilde{0}} = \mathfrak{c}_1$, $\mathfrak{a}^{\tilde{1}} = \mathfrak{t}_1$ и $\mathfrak{c}_1 \neq \mathfrak{t}_1$. Имеется свойство операторов:

$$\mathfrak{e}f(\tilde{x}) \oplus \mathfrak{p}f(\tilde{x}) = \mathfrak{d}f(\tilde{x}).$$

Отсюда получаем, что существует оператор $\mathfrak{b} = \mathfrak{b}_1$, $\mathfrak{b}_1 \neq \mathfrak{c}_1$ и $\mathfrak{b}_1 \neq \mathfrak{t}_1$ и

$$\mathfrak{b} = \mathfrak{a}^{\tilde{0}} \oplus \mathfrak{a}^{\tilde{1}}.$$

Шаг индукции. Пусть $n > 1$. Разобьем сумму на две:

$$\sum_{\tilde{\tau} \in E^n} \mathfrak{a}^{\tilde{\tau}} = \sum_{\tilde{\tau}' \in V'} \mathfrak{a}^{\tilde{\tau}'} \oplus \sum_{\tilde{\tau}'' \in V''} \mathfrak{a}^{\tilde{\tau}''},$$

где $V' = \{\tilde{\tau} | \tilde{\tau} \in E^n \text{ и } \tau_n = 0\}$, $V'' = \{\tilde{\tau} | \tilde{\tau} \in E^n \text{ и } \tau_n = 1\}$.

По определению однородных пучков существует пучок $(\mathfrak{a}^0, \mathfrak{a}^1)$ операторов размерности 1, что $(\mathfrak{a}^{\tilde{\tau}'})_n = \mathfrak{a}^0$ для любого $\tilde{\tau}'$ и $(\mathfrak{a}^{\tilde{\tau}''})_n = \mathfrak{a}^1$ для любого $\tilde{\tau}''$.

По индукции можно сделать следующее преобразование указанных двух сумм:

$$\sum_{\tilde{\tau}' \in V'} \mathfrak{a}^{\tilde{\tau}'} \oplus \sum_{\tilde{\tau}'' \in V''} \mathfrak{a}^{\tilde{\tau}''} =$$

$$= \sum_{\tilde{\sigma} \in E^{n-1}} \left(\mathfrak{a}_1 \dots \mathfrak{a}_{n-1} \mathfrak{a}^0\right)^{\tilde{\sigma}} \oplus \sum_{\tilde{\sigma} \in E^{n-1}} \left(\mathfrak{a}_1 \dots \mathfrak{a}_{n-1} \mathfrak{a}^1\right)^{\tilde{\sigma}} =$$

$$= \mathfrak{b}_1 \dots \mathfrak{b}_{n-1} \mathfrak{a}^0 \oplus \mathfrak{b}_1 \dots \mathfrak{b}_{n-1} \mathfrak{a}^1 = \mathfrak{b}_1 \dots \mathfrak{b}_{n-1} \mathfrak{b}_n,$$

где $\mathfrak{b}_n \neq \mathfrak{a}^0$ и $\mathfrak{b}_n \neq \mathfrak{a}^1$. □

Однопорожденные пучки операторов.

Пучок операторов $\mathfrak{A} = (\mathfrak{a}^{\tilde{0}}, \dots, \mathfrak{a}^{\tilde{\tau}}, \dots, \mathfrak{a}^{\tilde{1}})$ будем называть однородным однопорожденным (для краткости — однопорожденным), если существует оператор $\mathfrak{b} = \mathfrak{b}_0 \dots \mathfrak{b}_n$ такой, что оператор $\mathfrak{a}^{\tilde{\tau}} = \mathfrak{t}_1 \dots \mathfrak{t}_n$ пучка $\mathfrak{A}$ определяется следующим образом:

$$\mathfrak{t}_i = \begin{cases} \mathfrak{b}_i, & \text{если } \tau_i = 0, \\ \mathfrak{c}_i, & \text{если } \tau_i = 1, \end{cases}$$

где $\mathfrak{c}_i \in \{\mathfrak{e}, \mathfrak{d}, \mathfrak{p}\}$ и $\mathfrak{c}_i \neq \mathfrak{b}_i$ для любого i.

Очевидно, что класс всех однородных операторных пучков включается в класс однопорожденных.

Пусть $A = (a^{\tilde{0}}, \ldots, a^{\tilde{\tau}}, \ldots, a^{\tilde{1}})$ — однопорожденный операторный пучок. Оператор b будем называть *согласованным* с оператором $a^{\tilde{\tau}}$ пучка A, если $b_i = a_i^{\tilde{0}}$ тогда и только тогда, когда $\tau_i = 0$.

Однородный операторный пучок $B = (b^{\tilde{0}}, \ldots, b^{\tilde{\tau}}, \ldots, b^{\tilde{1}})$ будем называть *сопутствующим* однопорожденному пучку A, если $b^{\tilde{0}} = a^{\tilde{0}}$ и $b^{\tilde{1}} = a^{\tilde{1}}$. Легко заметить, что в таких пучках для любого τ оператор $a^{\tilde{\tau}}$ пучка A согласован с оператором $b^{\tilde{\tau}}$ пучка B и наоборот. Из определения также непосредственно следует, что для любого однопорожденного пучка существует единственный сопутствующий.

Для оператора $b^{\tilde{\tau}}$ и согласованного с ним оператора a определяется вектор различия $\tilde{\rho} = \rho(a, b^{\tilde{\tau}}) = (\rho_1, \ldots, \rho_n)$, компоненты которого имеют вид

$$\rho_i = \begin{cases} 1, & \text{если } \tau_i = 1 \text{ и } a_i \neq b_i^{\tilde{\tau}}, \\ 0, & \text{в противном случае.} \end{cases}$$

Через $wt(\tilde{\rho})$ обозначим количество ненулевых компонент вектора $\tilde{\rho}$.

Предложение 3.11. *Пусть оператор a согласован с оператором $b^{\tilde{\tau}}$, входящего в однородный операторный пучок $(b^{\tilde{0}}, \ldots, b^{\tilde{\tau}}, \ldots, b^{\tilde{1}})$. Тогда оператор a имеет разложение:*

$$a = \sum_{\tilde{\sigma} \in V} b^{\tilde{\sigma}},$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\tau} \oplus \tilde{\rho} \leqslant \tilde{\sigma} \leqslant \tilde{\tau}\}$, $\tilde{\rho}$ — вектор различия операторов a и $b^{\tilde{\tau}}$.

Доказательство проведем индукцией по $wt(\tilde{\tau})$. Если $wt(\tilde{\tau}) = 0$, то $wt(\tilde{\rho}(a, b^{\tilde{\tau}})) = 0$ и

$$a = b^{\tilde{\tau}} = \sum_{\tilde{\sigma} \in V},$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\tau} \leqslant \tilde{\sigma} \leqslant \tilde{\tau}\}$.

Пусть $wt(\tilde{\tau}) > 0$. Если $wt(\tilde{\rho}(a, b^{\tilde{\tau}})) = 0$, то

$$a = b^{\tilde{\tau}} = \sum_{\tilde{\sigma} \in V} b^{\tilde{\sigma}},$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\tau} \oplus \tilde{\rho} \leqslant \tilde{\sigma} \leqslant \tilde{\tau}\}$.

Пусть $wt(\tilde{\rho}(\mathrm{a}, \mathrm{b}^{\tilde{\tau}})) = l > 0$ и пусть $\rho_i = 1$ и $\mathrm{a}_i \neq \mathrm{b}_i^{\tilde{\tau}}$. Оператор a можно представить в виде суммы операторов d и c, где

$$\mathrm{d} = \mathrm{a}_1 \ldots \mathrm{a}_{i-1} \mathrm{b}_i \mathrm{a}_{i+1} \ldots \mathrm{a}_n, \quad \mathrm{c} = \mathrm{a}_1 \ldots \mathrm{a}_{i-1} (\mathrm{b}^{\tilde{0}})_i \mathrm{a}_{i+1} \ldots \mathrm{a}_n.$$

При таком представлении

$$wt(\tilde{\rho}(\mathrm{d}, \mathrm{b}^{\tilde{\tau}})) < wt(\tilde{\rho}(\mathrm{a}, \mathrm{b}^{\tilde{\tau}}))$$

и оператор c согласован с оператором $\mathrm{b}^{\tilde{\delta}}$, где $wt(\tilde{\delta}) < wt(\tilde{\tau})$ и $\tilde{\delta} < \tilde{\tau}$:

$$\tilde{\rho}'(\mathrm{d}, \mathrm{b}^{\tilde{\tau}}) = (\rho_1, \ldots, \rho_{i-1}, 0, \rho_{i+1}, \ldots, \rho_n),$$

$$\mathrm{d} = \sum_{\tilde{\sigma} \in V} \mathrm{b}^{\tilde{\sigma}},$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\tau} \oplus \tilde{\rho}' \leqslant \tilde{\sigma} \leqslant \tilde{\tau}\}$. Заметим, что $\tau_i = 1$.

Оператор c согласован с $\mathrm{b}^{\tilde{\delta}}$, где $\tilde{\delta} = (\delta_1, \ldots, \delta_n)$ ($\delta_j = \tau_j$ при $j \neq i$ и $\delta_j = 0$ при $j = i$ и $wt(\tilde{\delta}) < wt(\tilde{\tau})$):

$$\mathrm{c} = \sum_{\tilde{\sigma} \in V} \mathrm{b}^{\tilde{\sigma}},$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\delta} \oplus \tilde{\rho}' \leqslant \tilde{\sigma} \leqslant \tilde{\delta}\}$.

Заметим, что $\delta_i = 0$ и $\rho_i = 0$. Тогда

$$\mathrm{a} = \mathrm{d} \oplus \mathrm{c} = \sum_{\tilde{\sigma} \in V'} \mathrm{b}^{\tilde{\sigma}} \oplus \sum_{\tilde{\sigma} \in V''} \mathrm{b}^{\tilde{\sigma}} = \sum_{\tilde{\sigma} \in V} \mathrm{b}^{\tilde{\sigma}},$$

где

$$V' = \{\tilde{\sigma} | \tilde{\sigma} \in E^n \text{ и } \tilde{\tau} \oplus \tilde{\rho}' \leqslant \tilde{\sigma} \leqslant \tilde{\tau}\},$$
$$V'' = \{\tilde{\sigma} | \tilde{\sigma} \in E^n \text{ и } \tilde{\delta} \oplus \tilde{\rho}' \leqslant \tilde{\sigma} \leqslant \tilde{\delta}\},$$
$$V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n \text{ и } \tilde{\tau} \oplus \tilde{\rho} \leqslant \tilde{\sigma} \leqslant \tilde{\tau}\}. \qquad \square$$

Предложение 3.12. *Пусть* $\mathrm{A} = (\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{\tau}}, \ldots, \mathrm{a}^{\tilde{1}})$ — *неоднородный операторный пучок,* $\mathrm{B} = (\mathrm{b}^{\tilde{0}}, \ldots, \mathrm{b}^{\tilde{\tau}}, \ldots, \mathrm{b}^{\tilde{1}})$ — *сопутствующий операторный пучок. Тогда оператор* $\mathrm{b}^{\tilde{\tau}}$ *имеет разложение*:

$$\mathrm{b}^{\tilde{\tau}} = \sum_{\tilde{\sigma} \in V} \alpha_{\tilde{\sigma}}^{\tilde{\tau}} \mathrm{a}^{\tilde{\sigma}},$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ *и* $\tilde{\sigma} \leqslant \tilde{\tau}\}$, *а коэффициенты* $\alpha_{\tilde{\sigma}}$ *вычисляются следующим образом:*

$$\alpha_{\tilde{\tau}}^{\tilde{\tau}} = 1, \quad \alpha_{\tilde{\sigma}}^{\tilde{\tau}} = \sum_{\tilde{\delta} \in V} \alpha_{\tilde{\sigma}}^{\tilde{\delta}},$$

где $V = \{\tilde{\delta} | \tilde{\delta} \in E^n$ *и* $(\tilde{\tau} \oplus \tilde{\rho}) \vee \tilde{\sigma} \leqslant \tilde{\delta} < \tilde{\tau}\}$, $\tilde{\rho} = \tilde{\rho}(\mathfrak{b}^{\tilde{\tau}}, \mathfrak{a}^{\tilde{\tau}})$.

Доказательство проведем индукцией по $l = wt(\tilde{\tau})$. Пусть $wt(\tilde{\tau}) = 0$. В этом случае $\tilde{\tau} = \tilde{0}$ и по определению $\mathfrak{b}^{\tilde{\tau}} = \mathfrak{a}^{\tilde{\tau}}$, $\alpha_{\tilde{0}}^{\tilde{0}} = 1$.

Пусть $wt(\tilde{\tau}) = l > 0$ и для всех $\tilde{\delta} \leqslant \tilde{\tau}$ уже определены коэффициенты $\alpha_{\tilde{\sigma}}^{\tilde{\delta}}$ разложений

$$\mathfrak{b}^{\tilde{\delta}} = \sum_{\tilde{\sigma} \in V} \alpha_{\tilde{\sigma}}^{\tilde{\delta}} \mathfrak{a}^{\tilde{\sigma}},$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\sigma} \leqslant \tilde{\delta}\}$.

По предложению 3.11 имеем

$$\mathfrak{a}^{\tilde{\tau}} = \sum_{\tilde{\sigma} \in V} \mathfrak{b}^{\tilde{\sigma}},$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\tau} \oplus \tilde{\rho} \leqslant \sigma \leqslant \tilde{\tau}\}$, $\tilde{\rho} = \tilde{\rho}(\mathfrak{a}^{\tilde{\tau}}, \mathfrak{b}^{\tilde{\tau}})$.

Преобразуем данное равенство

$$\mathfrak{b}^{\tilde{\tau}} = \mathfrak{a}^{\tilde{\tau}} \oplus \sum_{\tilde{\delta} \in V} \mathfrak{b}^{\tilde{\delta}}, \tag{3.11}$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\tau} \oplus \tilde{\rho} \leqslant \delta < \tilde{\tau}\}$. По индуктивному предположению

$$\mathfrak{b}^{\tilde{\delta}} = \sum_{\tilde{\sigma} \in V} \alpha_{\tilde{\sigma}}^{\tilde{\delta}} \mathfrak{a}^{\tilde{\sigma}}, \tag{3.12}$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\sigma} \leqslant \tilde{\delta}\}$.

Сделаем подстановку (3.12) в (3.11):

$$\mathfrak{b}^{\tilde{\tau}} = \mathfrak{a}^{\tilde{\tau}} \oplus \sum_{\tilde{\delta} \in V'} \left(\sum_{\tilde{\delta} \in V''} \alpha_{\tilde{\sigma}}^{\tilde{\delta}} \mathfrak{a}^{\tilde{\sigma}} \right) = \mathfrak{a}^{\tilde{\tau}} \oplus \sum_{\tilde{\delta} \in V} \beta_{\tilde{\sigma}} \mathfrak{a}^{\tilde{\sigma}},$$

где

$$V' = \{\tilde{\delta} | \tilde{\delta} \in E^n \text{ и } \tilde{\tau} \oplus \tilde{\rho} \leqslant \tilde{\delta} < \tilde{\tau}\},$$
$$V'' = \{\tilde{\sigma} | \tilde{\sigma} \in E^n \text{ и } \tilde{\sigma} \leqslant \tilde{\delta}\},$$
$$V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n \text{ и } \tilde{\sigma} < \tilde{\tau}\}.$$

В этом разложении коэффициент $\beta_{\tilde{\sigma}}$ очевидно имеет вид

$$\beta_{\tilde{\sigma}} = \sum_{\tilde{\delta} \in V} \alpha^{\tilde{\delta}}_{\tilde{\sigma}},$$

где $V = \{\tilde{\delta} | \tilde{\delta} \in E^n$ и $(\tilde{\tau} \oplus \tilde{\rho}) \vee \tilde{\sigma} \leqslant \tilde{\delta} < \tilde{\tau}\}$. □

Однородно смешанные пучки операторов.

Класс МН однородно смешанных пучков (для краткости — смешанные пучки) определяется индуктивно:

1) все однородные пучки операторов размерности 1 являются смешанными;

2) если A — пучок операторов размерности n лежит в классе МН, $\mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}$ — 2^n однородных пучков операторов размерности m, то $\mathsf{C} \in MH$, где C — слияние указанных пучков;

3) если $\mathsf{A} \in MH$ — пучок операторов размерности n, а пучок $\mathsf{B} = I(\mathsf{A})$ для некоторой перестановки I, то $\mathsf{B} \in MH$.

Предложение 3.13. *Матрица однородно смешанного пучка может быть приведена к треугольному виду перестановкой строк (столбцов).*

Доказательство. Пусть пучок C является слиянием однородных пучков $\mathsf{B}_{\tilde{0}}, \ldots, \mathsf{B}_{\tilde{1}}$ по однородному пучку A.

Легко заметить, что матрица M_C имеет блочно-диагональный вид: на главной диагонали этой матрицы расположены блоки, имеющие вид $M_{\mathsf{B}_{\tilde{\tau}} \times \mathsf{B}_{\tilde{\sigma}}}$.

Теперь достаточно показать, что матрица $M_{\mathsf{A} \times \mathsf{B}}$ приводится к треугольной для любых однородных пучков A и B.

Заметим, что если $\mathsf{a}^{\tilde{0}} = \mathsf{b}^{\tilde{0}}$, то матрица $M_{\mathsf{A} \times \mathsf{B}}$ имеет треугольный вид.

По предложению 3.9 найдутся $\tilde{\sigma}$ и $\tilde{\tau}$ такие, что $\mathsf{a}^{\tilde{\sigma}} = \mathsf{b}^{\tilde{\tau}}$. По предложению 3.8 преобразуем пучок A относительно $\tilde{\sigma}$, пучок B относительно $\tilde{\tau}$. Теперь в полученных пучках совпадают операторы с индексом $\tilde{0}$.

Очевидно, что перестановки операторов в пучках соответствуют перестановкам строк и столбцов матрицы их произведения, а перестановка в операторах пучка не меняет матрицу этого пучка. □

Для дальнейшего изложения потребуется подкласс однородно смешанных пучков. Он будет обозначаться символом KH и определяется следующим образом:

1) все пучки операторов размерности 1 принадлежат классу KH;

2) если $A \in KH$ — пучок операторов размерности $n-1$, $B_{\tilde{0}}, \ldots, B_{\tilde{1}} \in KH$ — пучки операторов размерности 1, а пучок C — слияние указанных пучков, то $C \in KH$.

Предложение 3.14. *Пусть* $C \in KH$, $C = (c^{\tilde{0}}, \ldots, c^{\tilde{1}})$ *и пусть* $c^{\tilde{\tau}} = t_1 \ldots t_n$ *и* $c^{\tilde{\sigma}} = c_1 \ldots c_n$. *Тогда*

1) $t_1 = c_1$ *тогда и только тогда, когда* $\tau_1 = \sigma_1$;

2) *при* $n \geqslant 2$ *пучки* $P = (p^{\tilde{0}}, \ldots, p^{\tilde{1}})$ *и* $Q = (q^{\tilde{0}}, \ldots, q^{\tilde{1}})$ *операторов размерности* $n-1$ *лежат в классе* K, *где* $p^{\tilde{\delta}} = t_2 \ldots t_n$ *при* $\tau_1 = 0, q_2^{\tilde{\delta}} = t_2 \ldots t_n$ *при* $\tau_1 = 1$ *и* $\tilde{\delta} = (\tau_2, \ldots, \tau_n)$.

Доказательство. Если $n = 1$, то по определению пучок C состоит из двух различных операторов, и утверждение, очевидно, выполняется.

При $n = 2$ пучок C построен по $A, C_1, C_2 \in K$, причем $(c^{(\alpha_1,\alpha_2)})_1 = (a^{(\alpha)})_1$ и $(a^{(\alpha)})_1 = (a^{(\beta)})_1 \iff \alpha = \beta$, поэтому утверждение также справедливо.

При $n > 2$ пучок C строится из $A, B_{\tilde{0}}, \ldots, B_{\tilde{1}}$, причем размерность операторов в $b_{\tilde{\tau}'}$ равна 1. По индукции, для A утверждение справедливо. Поэтому соответствующим образом построенные пучки A_1 и A_2 лежат в классе K. По определению K получаем

$$(c^{\tilde{\tau}})_1 = (a^{\tilde{\tau}'})_1, \quad \text{где } \tilde{\tau}' = (\tau_1, \ldots, \tau_{n-1}).$$
$$(c^{\tilde{\tau}})_1 = (c^{\tilde{\sigma}})_1 \iff (a^{\tilde{\tau}'})_1 = (a^{\tilde{\sigma}'})_1 \iff \tau_1 = \sigma_1.$$

По пучкам A_1 и $B_{\tilde{\tau}'}$ при $\tau_1 = 0$ построим в соответствии с определением KH пучок $T_1 \in KH$.

Аналогично, по A_2 и $B_{\tilde{\tau}'}$ при $\tau_1 = 1$ построим $T_2 \in KH$.

При $1 \leqslant i \leqslant n-2$ выполняется:

$$\left(t_1^{(\tau_2,\ldots,\tau_n)}\right)_i = \left(a_1^{(\tau_2,\ldots,\tau_{n-1})}\right)_i = \left(a^{(0,\tau_2,\ldots,\tau_{n-1})}\right)_{i+1} = \left(c^{(0,\tau_2,\ldots,\tau_n)}\right)_{i+1} = \left(c_1^{(\tau_2,\ldots,\tau_n)}\right)_i,$$

$$\left(t_1^{(\tau_2,\ldots,\tau_n)}\right)_{n-1} = \left(b_{(0,\tau_2,\ldots,\tau_{n-1})}^{(\tau_n)}\right)_1 = \left(c^{(0,\tau_2,\ldots,\tau_n)}\right)_n = \left(c_1^{(\tau_2,\ldots,\tau_n)}\right)_{n-1}.$$

Таким образом, получили $C_1 = T_1$. Равенство $C_2 = T_2$ получается аналогично. Следовательно, $C_1, C_2 \in KH$. □

Диагональные пучки операторов.

Пучок A называется *диагональным*, если матрица этого пучка совпадает с единичной $M_A = E_{2^n}$.

Пучок A называется *обратимым*, если найдется пучок B такой, что матрица произведения этих пучков совпадает с единичной $M_{A \times B} = E_{2^n}$.

Ввиду коммутативности свойства обратимости, пучки будем называть взаимообратимыми.

Предложение 3.15. *Пусть пучок* C *является слиянием пучков* $B_{\tilde{0}}, \ldots, B_{\tilde{1}}$ *по пучку* A. *Тогда, если пучок* A — *диагональный, а пучки* $B_{\tilde{\tau}}$ *и* $B_{\overline{\tilde{\tau}}}$ *взаимообратимы для любого* τ, *то пучок* C *также является диагональным.*

Доказательство. Пусть пучок C является слиянием пучков $B_{\tilde{0}}, \ldots, B_{\tilde{1}}$ по диагональному пучку A.

Аналогично случаю однородных смешанных пучков матрица слияния M_C имеет блочно-диагональный вид: на главной диагонали этой матрицы расположены блоки, имеющие вид $M_{B_{\tilde{\tau}} \times B_{\overline{\tilde{\tau}}}}$. Согласно условию пары пучков $B_{\tilde{\tau}}$ и $B_{\overline{\tilde{\tau}}}$ взаимообратимы для любого τ, что гарантирует диагональный вид блоков-матриц $M_{B_{\tilde{\tau}} \times B_{\overline{\tilde{\tau}}}}$. □

Пусть $A = (a^{\tilde{0}}, \ldots, a^{\tilde{1}})$ — пучок операторов, и для некоторых $\tilde{\mu}$, $\tilde{\nu}$, операция $a^{\tilde{\mu}} \oplus a^{\tilde{\nu}}$ и $a^{\overline{\tilde{\mu}}} \oplus a^{\overline{\tilde{\nu}}}$ является определенной. В этом случае будем говорить, что существует преобразование $\varphi_{\tilde{\mu}\tilde{\nu}}$, переводящее пучок A в пучок $B = (b^{\tilde{0}}, \ldots, b^{\tilde{1}})$, который определяется следующим образом:

$$b^{\tilde{\sigma}} = \begin{cases} a^{\tilde{\mu}} \oplus a^{\tilde{\nu}}, & \text{если } \tilde{\sigma} = \tilde{\mu}, \\ a^{\overline{\tilde{\mu}}} \oplus a^{\overline{\tilde{\nu}}}, & \text{если } \tilde{\sigma} = \overline{\tilde{\nu}}, \\ a^{\tilde{\sigma}}, & \text{в остальных случаях.} \end{cases}$$

Результат этого преобразования будет обозначаться следующим образом: $B = \varphi_{\tilde{\mu}\tilde{\nu}}(A)$.

Предложение 3.16. *Если к диагональному пучку* A *применимо преобразование* $\varphi_{\tilde{\mu}\tilde{\nu}}$, *то пучок* $\varphi_{\tilde{\mu}\tilde{\nu}}(A)$ *также диагональный.*

Доказательство. Пусть $\mathsf{A} = (\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{1}})$ — диагональный пучок, $\varphi_{\tilde{\mu}\tilde{\nu}}(\mathsf{A}) = \mathsf{B} = (\mathfrak{b}^{\tilde{0}}, \ldots, \mathfrak{b}^{\tilde{1}})$. Рассмотрим элементы матрицы M_{B}: $m_{\tilde{\sigma}\tilde{\tau}} = \mathfrak{b}^{\overline{\tilde{\sigma}}} \circ \mathfrak{b}^{\tilde{\tau}}$.

Из соображений симметрии и произведенных изменений достаточно рассмотреть $\tilde{\sigma} = \overline{\tilde{\nu}}$ и $\tilde{\sigma} = \tilde{\mu}$.

Каждый из этих случаев можно представить так:

$$m_{\tilde{\mu}\tilde{\tau}} = \begin{cases} (\mathfrak{a}^{\overline{\tilde{\mu}}} \oplus \mathfrak{a}^{\overline{\tilde{\nu}}}) \circ (\mathfrak{a}^{\tilde{\mu}} \oplus \mathfrak{a}^{\tilde{\nu}}), & \text{если } \tilde{\tau} = \tilde{\mu}; \\ (\mathfrak{a}^{\overline{\tilde{\mu}}} \oplus \mathfrak{a}^{\overline{\tilde{\nu}}}) \circ \mathfrak{a}^{\tilde{\nu}}, & \text{если } \tilde{\tau} = \tilde{\nu}; \\ (\mathfrak{a}^{\overline{\tilde{\mu}}} \oplus \mathfrak{a}^{\overline{\tilde{\nu}}}) \circ (\mathfrak{a}^{\overline{\tilde{\mu}}} \oplus \mathfrak{a}^{\overline{\tilde{\nu}}}), & \text{если } \tilde{\tau} = \overline{\tilde{\nu}}; \\ (\mathfrak{a}^{\overline{\tilde{\mu}}} \oplus \mathfrak{a}^{\overline{\tilde{\nu}}}) \circ \mathfrak{a}^{\overline{\tilde{\mu}}}, & \text{если } \tilde{\tau} = \overline{\tilde{\mu}}; \\ (\mathfrak{a}^{\overline{\tilde{\mu}}} \oplus \mathfrak{a}^{\overline{\tilde{\nu}}}) \circ \mathfrak{a}^{\tilde{\tau}}, & \text{в остальных случаях,} \end{cases}$$

$$m_{\overline{\tilde{\nu}}\tilde{\tau}} = \begin{cases} (\mathfrak{a}^{\tilde{\mu}} \oplus \mathfrak{a}^{\tilde{\nu}}) \circ (\mathfrak{a}^{\tilde{\mu}} \oplus \mathfrak{a}^{\tilde{\nu}}), & \text{если } \tilde{\tau} = \tilde{\mu}; \\ (\mathfrak{a}^{\tilde{\mu}} \oplus \mathfrak{a}^{\tilde{\nu}}) \circ \mathfrak{a}^{\tilde{\nu}}, & \text{если } \tilde{\tau} = \tilde{\nu}; \\ (\mathfrak{a}^{\tilde{\mu}} \oplus \mathfrak{a}^{\tilde{\nu}}) \circ (\mathfrak{a}^{\overline{\tilde{\mu}}} \oplus \mathfrak{a}^{\overline{\tilde{\nu}}}), & \text{если } \tilde{\tau} = \overline{\tilde{\nu}}; \\ (\mathfrak{a}^{\tilde{\mu}} \oplus \mathfrak{a}^{\tilde{\nu}}) \circ \mathfrak{a}^{\overline{\tilde{\mu}}}, & \text{если } \tilde{\tau} = \overline{\tilde{\mu}}; \\ (\mathfrak{a}^{\tilde{\mu}} \oplus \mathfrak{a}^{\tilde{\nu}}) \circ \mathfrak{a}^{\tilde{\tau}}, & \text{в остальных случаях.} \end{cases}$$

Проведем преобразования согласно предложения 3.7:

$$m_{\tilde{\mu}\tilde{\tau}} = \begin{cases} 0, \text{ если } \tilde{\tau} = \tilde{\mu}; \\ 1, \text{ если } \tilde{\tau} = \tilde{\nu}; \\ 0, \text{ если } \tilde{\tau} = \overline{\tilde{\nu}}; \\ 0, \text{ если } \tilde{\tau} = \overline{\tilde{\mu}}; \\ 0 \text{ в остальных случаях .} \end{cases}$$

После аналогичных преобразований для второго случая получаем

$$m_{\overline{\tilde{\nu}}\tilde{\tau}} = \begin{cases} 0, \text{ если } \tilde{\tau} = \tilde{\mu}; \\ 0, \text{ если } \tilde{\tau} = \tilde{\nu}; \\ 0, \text{ если } \tilde{\tau} = \overline{\tilde{\nu}}; \\ 1, \text{ если } \tilde{\tau} = \overline{\tilde{\mu}}; \\ 0 \text{ в остальных случаях .} \end{cases}$$

В итоге получили: $m_{\tilde{\sigma}\tilde{\tau}} = 1$, если $\tilde{\sigma} = \tilde{\tau}$ и $m_{\tilde{\sigma}\tilde{\tau}} = 0$ — в противном случае.

Таким образом, матрица M_{B} — диагональная. □

§ 4. Разложения функций по операторным пучкам

Разложения по сопряженным базисным пучкам.

Для пучка операторов $\mathrm{A} = (\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{\tau}}, \ldots, \mathrm{a}^{\tilde{1}})$ пучок операторов $\mathrm{B} = (\mathrm{b}^{\tilde{0}}, \ldots, \mathrm{b}^{\tilde{\tau}}, \ldots, \mathrm{b}^{\tilde{1}})$ будет называться *сопряженным*, если

1) оба пучка однородны,

2) $\mathrm{b}^{\tilde{1}} = \mathrm{a}^{\tilde{1}}$ и для любого i выполняется $\mathrm{b}_i^{\tilde{1}} \neq \mathrm{d}$,

3) для любого i выполняется $\mathrm{b}_i^{\tilde{0}} \neq \mathrm{a}_i^{\tilde{0}}$.

Легко заметить, что не каждый однородный пучок имеет сопряженный, например, пучок $(\mathrm{de}, \ldots, \mathrm{pd})$ не имеет сопряженного.

Пусть символ $\hat{\mathrm{A}}$ обозначает сопряженный операторный пучок для однородного пучка A.

Теорема 3.5. *Для любой функции $f(\tilde{x}, \tilde{z})$, для любого однородного пучка операторов* $\mathrm{B} = (\mathrm{b}^{\tilde{0}}, \ldots, \mathrm{b}^{\tilde{1}})$, *имеющего сопряженный, имеет место разложение*:

$$f(\tilde{x}, \tilde{z}) = \sum_{\tilde{\tau} \in E^n} \mathrm{b}_{\tilde{x}}^{\tilde{\tau}} \left(\hat{\mathrm{b}}_{\tilde{x}}^{\overline{\tilde{\tau}}} f(\tilde{x}, \tilde{z}) \right).$$

Доказательство. Пусть на операторах b и c покомпонентно определена бинарная операция $\times$: $\mathrm{b} \times \mathrm{c} = \mathrm{a}$, где $\mathrm{a} = \mathrm{a}_1 \ldots \mathrm{a}_n$ и компонента $\mathrm{a}_i = \mathrm{b}_i \times \mathrm{c}_i$ определяется по следующей схеме:

$\times$	d	p	e
d		d	d
p	d	e	p
e	d	p	e

Очевидно, что если в операторах b и c для любого i имеет место: $\mathrm{b}_i \neq \mathrm{d}$ или $\mathrm{c}_i \neq \mathrm{d}$, то $\mathrm{b}(\mathrm{c} f(\tilde{x})) = (\mathrm{b} \times \mathrm{c}) f(\tilde{x})$.

Рассмотрим $\mathrm{a}^{\tau} = \mathrm{b}^{\tau} \times \hat{\mathrm{b}}^{\overline{\tau}}$. Если $\tau_i = 1$, то $\mathrm{b}_i = e$ или $\mathrm{b}_i = \mathrm{p}$; $\overline{\tau}_i = 0$ и $\hat{\mathrm{b}}_i \neq e$ или $\hat{\mathrm{b}}_i \neq \mathrm{p}$ соответственно. Из таблицы получаем, что $\mathrm{a}_i = \mathrm{p}$ или $\mathrm{a}_i = \mathrm{d}$.

Покажем, что $\mathrm{a}^{\tilde{\tau}} \neq \mathrm{a}^{\tilde{\sigma}}$ при $\tilde{\tau} \neq \tilde{\sigma}$.

Пусть $\tau_i \neq \sigma_i$.

Рассмотрим $\tau_i = 0$. В этом случае выполняется $\bar{\tau}_i = 1$ и $\sigma_i = 1$. Согласно определению сопряженного пучка $\hat{\mathrm{b}}$:

$$\mathrm{d} \neq \hat{\mathrm{b}}^{\bar{\tau}_i} = \left(\mathrm{b}^{\tilde{\sigma}}\right)_i \neq \mathrm{d} \quad \text{и} \quad \left(\mathrm{b}^{\tilde{\tau}}\right)_i \neq \left(\hat{\mathrm{b}}^{\bar{\tilde{\sigma}}}\right)_i.$$

Отсюда следует

$$\left(\mathrm{a}^{\tilde{\tau}}\right)_i = \left(\mathrm{b}^{\tilde{\tau}}\right)_i \times \left(\hat{\mathrm{b}}^{\bar{\tilde{\tau}}}\right)_i \neq \left(\mathrm{b}^{\tilde{\sigma}}\right)_i \times \left(\hat{\mathrm{b}}^{\bar{\tilde{\sigma}}}\right)_i = \left(\mathrm{a}^{\tilde{\sigma}}\right)_i.$$

Аналогично рассматривается случай $\tau_i = 1$.

Преобразуем сумму согласно приведенным рассуждениям:

$$\sum_{\tilde{\tau} \in E^n} \mathrm{b}_{\tilde{x}}^{\tilde{\tau}} \left(\hat{\mathrm{b}}_{\tilde{x}}^{\bar{\tilde{\tau}}} f(\tilde{x}, \tilde{z})\right) = \sum_{\tilde{\tau} \in E^n} \left(\mathrm{b}_{\tilde{x}}^{\tilde{\tau}} \times \hat{\mathrm{b}}_{\tilde{x}}^{\bar{\tilde{\tau}}}\right) (f(\tilde{x}, \tilde{z})) = \sum_{\tilde{\tau} \in E^n} \mathrm{a}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}),$$

где $\mathrm{a}^{\tilde{\tau}} = \mathrm{a}_1^{\tilde{\tau}} \ldots \mathrm{a}_n^{\tilde{\tau}}$ и $\mathrm{a}_i^{\tilde{\tau}} \in \{\mathrm{d}, \mathrm{p}\}$.

Доказательство теоремы проводится индукцией по n — длине набора $\tilde{x} = (x_1, \ldots, x_n)$. При $n = 1$ имеем

$$\sum_{\tilde{\tau} \in E^1} \mathrm{a}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}) = \mathrm{d}_{x_1} f(\tilde{x}, \tilde{z}) \oplus \mathrm{p}_{x_1} f(\tilde{x}, \tilde{z}) = f(\tilde{x}, \tilde{z}).$$

Пусть $n > 1$ и пусть оператор $\mathrm{b} = \mathrm{a}_1 \ldots \mathrm{a}_{n-1}$ обозначает часть оператора a.

Тогда сумма может быть представлена так:

$$\sum_{\tilde{\tau} \in E^n} \mathrm{a}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}) = \sum_{\tilde{\tau}' \in V'} \mathrm{a}^{\tilde{\tau}'} f(\tilde{x}, \tilde{z}) \oplus \sum_{\tilde{\tau}'' \in V''} \mathrm{a}^{\tilde{\tau}''} f(\tilde{x}, \tilde{z}),$$

где $V' = \{\tilde{\tau} | \tilde{\tau} \in E^n \text{ и } \tau_n = 0\}$, $V'' = \{\tilde{\tau} | \tilde{\tau} \in E^n \text{ и } \tau_n = 1\}$.

Пусть $\mathrm{c}^{\tilde{\sigma}_n} = \mathrm{a}_1 \ldots \mathrm{a}_{n-1}$ обозначает оператор размерности $n-1$, построенный по первым $n-1$ компонентам оператора $\mathrm{a}^{\tilde{\sigma}}$. Тогда сумма может быть преобразована:

$$\sum_{\tilde{\tau}' \in V'} \mathrm{a}^{\tilde{\tau}'} f(\tilde{x}, \tilde{z}) \oplus \sum_{\tilde{\tau}'' \in V''} \mathrm{a}^{\tilde{\tau}''} f(\tilde{x}, \tilde{z}) =$$

$$= \mathrm{d}_{x_n} \Big(\sum_{\tilde{\tau}_n \in E^{n-1}} \mathrm{b}_{\tilde{x}_n}^{\tilde{\tau}_n} f(\tilde{x}, \tilde{z}) \Big) \oplus \mathrm{p}_{x_n} \Big(\sum_{\tilde{\tau}_n \in E^{n-1}} \mathrm{b}_{\tilde{x}_n}^{\tilde{\tau}_n} f(\tilde{x}, \tilde{z}) \Big).$$

По индуктивному предположению:

$$\sum_{\tilde{\tau}_n \in E^{n-1}} \mathrm{b}_{\tilde{x}_n}^{\tilde{\tau}_n} f(\tilde{x}, \tilde{z}) = f(\tilde{x}, \tilde{z}).$$

Окончательно получаем

$$\mathrm{d}_{x_n}\left(\sum_{\tilde{\tau}_n\in E^{n-1}}\mathrm{b}_{\tilde{x}_n}^{\tilde{\tau}_n}f(\tilde{x},\tilde{z})\right)\oplus\mathrm{p}_{x_n}\left(\sum_{\tilde{\tau}_n\in E^{n-1}}\mathrm{b}_{\tilde{x}_n}^{\tilde{\tau}_n}f(\tilde{x},\tilde{z})\right)=$$
$$=\mathrm{d}_{x_n}f(\tilde{x},\tilde{z})\oplus\mathrm{p}_{x_n}f(\tilde{x},\tilde{z})=f(\tilde{x},\tilde{z}).\quad\square$$

Следствие. *Любая булева функция $f(\tilde{x},\tilde{z})$ имеет разложение вида:*

$$f(\tilde{x},\tilde{z})=\sum_{\tilde{\tau}\in E^n}\mathrm{d}_{\tilde{x}}^{\tilde{\tau}}\mathrm{p}_{\tilde{x}}^{\bar{\tilde{\tau}}}f(\tilde{x},\tilde{z}).$$

Доказательство. Рассмотрим два операторных пучка:

$$\mathsf{A}=(\mathrm{a}^{\tilde{0}},\ldots,\mathrm{a}^{\tilde{\tau}},\ldots,\mathrm{a}^{\tilde{1}}),\ \mathsf{B}=(\mathrm{b}^{\tilde{0}},\ldots,\mathrm{b}^{\tilde{\tau}},\ldots,\mathrm{b}^{\tilde{1}}),$$

компоненты которых построены следующим образом:

$$\mathrm{a}_i^{\tilde{\tau}}=\begin{cases}\mathrm{d}, & \text{если } \tau_i=0,\\ \mathrm{e}, & \text{если } \tau_i=1,\end{cases}$$
$$\mathrm{b}_i^{\tilde{\tau}}=\begin{cases}\mathrm{p}, & \text{если } \tau_i=0,\\ \mathrm{e}, & \text{если } \tau_i=1.\end{cases}$$

Легко заметить, что эти два операторных пучка являются однородными, $\mathrm{d}_{\tilde{x}}^{\tilde{\tau}}=\mathrm{a}_{\tilde{x}}^{\tilde{\tau}}$ и $\mathrm{p}_{\tilde{x}}^{\tilde{\tau}}=\mathrm{b}_{\tilde{x}}^{\tilde{\tau}}$ и, согласно определению сопряженных пучков, $\mathsf{B}=\hat{\mathsf{A}}$.

Теперь, во введенных обозначениях, доказательство следствия очевидно. $\square$

Разложение в следствии интересно не только как возможность представления функции через свои производные, но также позволяет коротко изложить доказательство известного результата о выразимости частной производной булевой функции через кратные производные.

Следствие. *Частная производная булевой функции $f(\tilde{x},\tilde{z})$ по набору $\tilde{x}$ имеет следующее полиномиальное представление через кратные производные:*

$$\partial_{\tilde{x}}^{(\tilde{0})}f(\tilde{x},\tilde{z})=\sum_{\tilde{\tau}\in E^n\setminus\{\tilde{1}\}}\mathrm{d}_{\tilde{x}}^{\tilde{\tau}}f(\tilde{x},\tilde{z}).$$

Доказательство. Рассмотрим функцию $f(\bar{\tilde{x}}, \tilde{z})$. По первому следствию имеет место разложение:

$$f(\bar{\tilde{x}}, \tilde{z}) = \sum_{\tilde{\tau} \in E^n} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} \mathrm{p}_{\tilde{x}}^{\bar{\tilde{\tau}}} f(\bar{\tilde{x}}, \tilde{z}).$$

После нескольких несложных преобразований получаем разложение

$$f(\bar{\tilde{x}}, \tilde{z}) =. \sum_{\tilde{\tau} \in E^n} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} \mathrm{p}_{\tilde{x}}^{\bar{\tilde{\tau}}} f(\bar{\tilde{x}}, \tilde{z}) = \sum_{\tilde{\tau} \in E^n} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} \mathrm{p}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}) = \sum_{\tilde{\tau} \in E^n} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}).$$

Последнее равенство имеет место в силу свойства оператора дифференцирования:

$$\mathrm{d}_{\tilde{x}}^{\tilde{1}} f(\tilde{x}, \tilde{z}) = \mathrm{d}_{\tilde{x}}^{\tilde{1}} f(\bar{\tilde{x}}, \tilde{z}).$$

Теперь осталось добавить к обеим частям нового разложения функцию $f(\tilde{x}, \tilde{z})$. Окончательно получим

$$\partial_{\tilde{x}}^{(\tilde{0})} f(\tilde{x}, \tilde{z}) = f(\bar{\tilde{x}}, \tilde{z}) \oplus f(\tilde{x}, \tilde{z}) = \\ = \sum_{\tilde{\tau} \in E^n} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}) \oplus f(\tilde{x}, \tilde{z}) = \sum_{\tilde{\tau} \in E^n \setminus \{\tilde{1}\}} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}).$$

□

Следствие. *Частная производная булевой функции $f(\tilde{x}, \tilde{z})$ по переменным $\tilde{x}$ имеет полиномиальное разложение вида*

$$\mathrm{d}_{(\tilde{x})}^{(\tilde{0})} f(\tilde{x}, \tilde{z}) = \sum_{\tilde{\tau} \in E^n} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} \left(f(\tilde{x}, \tilde{z}) \oplus \mathrm{p}_{\tilde{x}}^{\bar{\tilde{\tau}}} f(\tilde{x}, \tilde{z}) \right).$$

Доказательство. Рассмотрим две функции $f(\tilde{x}, \tilde{z})$ и $f(\bar{\tilde{x}}, \tilde{z})$. По теореме имеем разложения:

$$f(\tilde{x}, \tilde{z}) = \sum_{\tilde{\tau} \in E^n} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} \mathrm{p}_{\tilde{x}}^{\bar{\tilde{\tau}}} f(\tilde{x}, \tilde{z}),$$

$$f(\bar{\tilde{x}}, \tilde{z}) = \sum_{\tilde{\tau} \in E^n} \mathrm{d}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}).$$

По определению $\partial_{\tilde{x}}^{\tilde{0}} f(\tilde{x}, \tilde{z}) = f(\bar{\tilde{x}}, \tilde{z}) \oplus f(\tilde{x}, \tilde{z})$. В силу дистрибутивности оператора $\mathrm{d}_{\tilde{x}}^{\tilde{\tau}}$ относительно операции $\oplus$ окончательно

получаем

$$\partial^{\tilde{0}}_{\tilde{x}} f(\tilde{x},\tilde{z}) = f(\overline{\tilde{x}},\tilde{z}) \oplus f(\tilde{x},\tilde{z}) = \sum_{\tilde{\tau}\in E^n} \mathrm{d}^{\tilde{\tau}}_{\tilde{x}} f(\tilde{x},\tilde{z}) \oplus \sum_{\tilde{\tau}\in E^n} \mathrm{d}^{\tilde{\tau}}_{\tilde{x}} \mathrm{p}^{\overline{\tilde{\tau}}}_{\tilde{x}} f(\tilde{x},\tilde{z}) =$$
$$= \sum_{\tilde{\tau}\in E^n} \mathrm{d}^{\tilde{\tau}}_{\tilde{x}} \left(f(\tilde{x},\tilde{z}) \oplus \mathrm{p}^{\overline{\tilde{\tau}}}_{\tilde{x}} f(\tilde{x},\tilde{z}) \right). \quad \square$$

Разложения по оператору подстановки.

Пусть наборы $|\tilde{x}| = |\tilde{\tau}| = n$ и $|\tilde{y}| = |\tilde{\sigma}| = k$.

Матрицу $A = [\alpha_{\tilde{\tau}\tilde{\sigma}}]$ назовем *матрицей булевой функции* $f(\tilde{x},\tilde{y})$, если $\alpha_{\tilde{\tau}\tilde{\sigma}} = f(\tilde{\tau},\tilde{\sigma})$. Столбцы матрицы A — значения $f(\tilde{\tau},\tilde{\sigma})$ при фиксированном $\tilde{\sigma}$, строки — значения $f(\tilde{\tau},\tilde{\sigma})$ при фиксированном $\tilde{\tau}$. Пусть M — квадратная подматрица матрицы $A = [a_{ij}]$. Элементы матрицы $A^{\diamond}(M) = [a^{\diamond}_{ij}]$ определяются следующим образом:

$$a^{\diamond}_{ij} = \begin{cases} 0, & \text{если } a_{ij} \notin M, \\ M_{ij}, & \text{если } a_{ij} \in M, \end{cases}$$

где M_{ij} — алгебраическое дополнение элемента a_{ij}.

Теорема 3.6. *Пусть множество переменных функции $f(x_1,\ldots,x_n)$ разбито на непересекающиеся подмножества*

$$\tilde{x}_1 \cup \ldots \cup \tilde{x}_s = \{x_1,\ldots,x_n\},$$

где $\tilde{x}_i \cap \tilde{x}_j = \varnothing$ при $i \neq j$, $|\tilde{x}_i| = l_i$, и соответствующее разбиение имеет набор $\{\sigma_1,\ldots,\sigma_n\} = \tilde{\sigma}_1 \cup \ldots \cup \tilde{\sigma}_s$ Тогда полиномиальное разложение

$$f(x_1,\ldots,x_n) = \sum_{\tilde{\sigma}\in E^n} \alpha_{\tilde{\sigma}} \mathrm{s}^{\tilde{\sigma}_1}_{\tilde{x}_1} f(x_1,\ldots,x_n) \cdot \ldots \cdot \mathrm{s}^{\tilde{\sigma}_s}_{\tilde{x}_s} f(x_1,\ldots,x_n) \tag{3.13}$$

имеет место тогда и только тогда, когда $s = 2$. Коэффициенты разложения при этом можно определить следующим образом:

$$[\alpha_{\tilde{\sigma}_1\tilde{\sigma}_2}] = A^{\diamond}(M), \tag{3.14}$$

где A — матрица функции $f(\tilde{x}_1,\tilde{x}_2)$, M — подматрица A, соответствующая базисному минору матрицы A.

Доказательство. Пусть $s > 2$. Достаточно показать, что в этом случае для любого s найдется функция, которая не

допускает разложения (3.13). Доказательство разбивается на 2 случая: а) s — нечетное и б) s — четное.

а) $s = n = 2m + 1$. Рассмотрим функцию

$$f(x_1, \ldots, x_{2m+1}) = x_1 \oplus \ldots \oplus x_{2m+1}.$$

Очевидно, что эта функция на всех нулях равна нулю, а на всех единицах равна единице. Пусть разложение (3.13) имеет место для этой функции при $s = 2m + 1$. Тогда

$$f(0, \ldots, 0) = \\ = \sum_{\tilde{\sigma} \in E^n} \alpha_{\tilde{\sigma}} f(\sigma_1, 0, \ldots, 0) \cdot f(0, \sigma_2, \ldots, 0) \cdot \ldots \cdot f(0, 0, \ldots, \sigma_{2m+1}).$$

По определению функции выполняется равенство

$$f(0, \ldots, \sigma_i, 0, \ldots, 0) = \sigma_i,$$

из которого следует, что

$$f(0, \ldots, 0) = \sum_{\tilde{\sigma} \in E^n} a_{\tilde{\sigma}} \sigma_1 \cdot \ldots \cdot \sigma_{2m+1}.$$

Произведение $\sigma_1 \cdot \ldots \cdot \sigma_{2m+1}$ отлично от нуля тогда и только тогда, когда $\sigma_1 = \ldots = \sigma_{2m+1} = 1$. Тогда $f(0, \ldots, 0) = \alpha_{1\ldots1}$, и $\alpha_{1\ldots1} = 0$.

С другой стороны

$$f(1, \ldots, 1) = \sum_{\tilde{\sigma} \in E^n} \alpha_{\tilde{\sigma}} f(\sigma_1, 1, \ldots, 1) \cdot \ldots \cdot f(1, \ldots, \sigma_{2m+1}) = \\ = \sum_{\tilde{\sigma} \in E^n} \alpha_{\tilde{\sigma}} \sigma_1 \cdot \ldots \cdot \sigma_{2m+1} = \alpha_{1\ldots1}.$$

Откуда следует, что $\alpha_{1\ldots1} = 1$. Получено противоречие.

б) $s = n = 2m$. Рассмотрим функцию, которая представляется полиномом Жегалкина, содержащим самое большее число слагаемых и у которого свободный член равен нулю. Очевидно здесь общее число слагаемых — нечетное. Каждая переменная встречается в 2^{2m-1} числе (четном) слагаемых. Из этого полинома уберем слагаемые, в которые входят произведения, содержащие $2m - 1$ переменную. Их будет $2m$ и каждая переменная теперь будет встречаться на $2m - 1$ раз меньше, т.е. меньше на нечетное число раз.

Таким образом, мы построили функцию, которая обладает следующими свойствами: 1) она симметрична, 2) ее полином Жегалкина содержит нечетное количество слагаемых, 3) каждая переменная входит в нечетное количество слагаемых ее полинома Жегалкина, 4) для каждой переменной x_i в ее полиноме Жегалкина есть слагаемое x_i.

Очевидно, что и для этой функции имеют место равенства:

$$\mathrm{o}^{\tilde{0}}_{\tilde{x}}(\mathrm{s}^{\sigma_i}_{x_i} f(x_1,\ldots,x_n)) = \mathrm{i}^{\tilde{1}}_{\tilde{x}}(\mathrm{s}^{\sigma_i}_{x_i} f(x_1,\ldots,x_n)) = \sigma_i.$$

Откуда также получается противоречие:

$$0 = f(0,\ldots,0) = \alpha_{1\ldots1} = f(1,\ldots,1) = 1.$$

Для доказательства существования разложения в случае, когда $s = 2$, подходит метод неопределенных коэффициентов. Для упрощения обозначений будем рассматривать функцию $f(\tilde{x},\tilde{y})$, $|\tilde{x}| = n$, $|\tilde{y}| = k$. Для нахождения коэффициентов $\alpha_{\tilde{\tau}\tilde{\sigma}}$ выражение (3.13) преобразуется в систему из 2^{n+k} уравнений с 2^{n+k} неизвестными:

$$\begin{aligned}
&\alpha_{\tilde{0}\tilde{0}} f(\tilde{0},\tilde{0}) f(\tilde{0},\tilde{0}) \oplus \ldots \oplus \alpha_{\tilde{0}\tilde{1}} f(\tilde{0},\tilde{0}) f(\tilde{0},\tilde{1}) \oplus \ldots \\
&\quad \ldots \oplus \alpha_{\tilde{\tau}\tilde{\sigma}} f(\tilde{\tau},\tilde{0}) f(\tilde{0},\tilde{\sigma}) \oplus \ldots \oplus \alpha_{\tilde{1}\tilde{1}} f(\tilde{1},\tilde{0}) f(\tilde{0},\tilde{1}) = f(\tilde{0},\tilde{0}) \\
&\qquad\qquad \ldots\ldots \\
&\alpha_{\tilde{0}\tilde{0}} f(\tilde{0},\tilde{0}) f(\tilde{1},\tilde{0}) \oplus \ldots \oplus \alpha_{\tilde{0}\tilde{1}} f(\tilde{0},\tilde{0}) f(\tilde{1},\tilde{1}) \oplus \ldots \\
&\quad \ldots \oplus \alpha_{\tilde{\tau}\tilde{\sigma}} f(\tilde{\tau},\tilde{0}) f(\tilde{1},\tilde{\sigma}) \oplus \ldots \oplus \alpha_{\tilde{1}\tilde{1}} f(\tilde{1},\tilde{0}) f(\tilde{1},\tilde{1}) = f(\tilde{1},\tilde{0}) \\
&\qquad\qquad \ldots\ldots \\
&\alpha_{\tilde{0}\tilde{0}} f(\tilde{0},\tilde{1}) f(\tilde{0},\tilde{0}) \oplus \ldots \oplus \alpha_{\tilde{0}\tilde{1}} f(\tilde{0},\tilde{1}) f(\tilde{0},\tilde{1}) \oplus \ldots \\
&\quad \ldots \oplus \alpha_{\tilde{\tau}\tilde{\sigma}} f(\tilde{\tau},\tilde{1}) f(\tilde{0},\tilde{\sigma}) \oplus \ldots \oplus \alpha_{\tilde{1}\tilde{1}} f(\tilde{1},\tilde{1}) f(\tilde{0},\tilde{1}) = f(\tilde{0},\tilde{1}) \\
&\qquad\qquad \ldots\ldots \\
&\alpha_{\tilde{0}\tilde{0}} f(\tilde{0},\tilde{1}) f(\tilde{1},\tilde{0}) \oplus \ldots \oplus \alpha_{\tilde{0}\tilde{1}} f(\tilde{0},\tilde{1}) f(\tilde{1},\tilde{1}) \oplus \ldots \\
&\quad \ldots \oplus \alpha_{\tilde{\tau}\tilde{\sigma}} f(\tilde{\tau},\tilde{1}) f(\tilde{1},\tilde{\sigma}) \oplus \ldots \oplus \alpha_{\tilde{1}\tilde{1}} f(\tilde{1},\tilde{1}) f(\tilde{1},\tilde{1}) = f(\tilde{1},\tilde{1}).
\end{aligned} \tag{3.15}$$

Матрицу B коэффициентов этой системы можно представить в блочном виде:

$$B = \begin{pmatrix} f(\tilde{0},\tilde{0})A & \ldots & f(\tilde{1},\tilde{0})A \\ \vdots & \ddots & \vdots \\ f(\tilde{0},\tilde{1})A & \ldots & f(\tilde{1},\tilde{1})A \end{pmatrix},$$

где A — матрица функции $f(\tilde{x}, \tilde{y})$, а каждый блок $f(\tilde{\tau}, \tilde{\sigma})A$ имеет следующую запись:

$$f(\tilde{\tau}, \tilde{\sigma})A = \begin{pmatrix} f(\tilde{\tau}, \tilde{\sigma})f(\tilde{0}, \tilde{0}) & \dots & f(\tilde{\tau}, \tilde{\sigma})f(\tilde{0}, \tilde{1}) \\ \vdots & \ddots & \vdots \\ f(\tilde{\tau}, \tilde{\sigma})f(\tilde{1}, \tilde{0}) & \dots & f(\tilde{\tau}, \tilde{\sigma})f(\tilde{1}, \tilde{1}) \end{pmatrix}.$$

Это представление является кронекеровским произведением матриц $B = A^t \otimes A$. Для доказательства существования решения системы нужно показать, что если линейными преобразованиями строк матрицы B получена нулевая строка, то эти же преобразования соответствующих значений функции приводят к 0. Покажем это в два этапа: для блочных строк матрицы и для строк блоков.

Пусть

$$\sum_{\tilde{\gamma} \in E^k} f(\tilde{\tau}, \tilde{\gamma})A = 0.$$

В силу дистрибутивности и условия $A \neq 0$ имеем

$$\sum_{\tilde{\gamma} \in E^k} f(\tilde{\tau}, \tilde{\gamma}) = 0;$$

для строк нулевого блока:

$$f(\tilde{\tau}, \tilde{\sigma})A = \begin{pmatrix} f(\tilde{\tau}, \tilde{\sigma})f(\tilde{0}, \tilde{0}) & \dots & f(\tilde{\tau}, \tilde{\sigma})f(\tilde{0}, \tilde{1}) \\ \vdots & \ddots & \vdots \\ f(\tilde{\tau}, \tilde{\sigma})f(\tilde{1}, \tilde{0}) & \dots & f(\tilde{\tau}, \tilde{\sigma})f(\tilde{1}, \tilde{1}) \end{pmatrix}$$

и

$$\sum_{\tilde{\gamma} \in E^n} f(\tilde{\tau}, \tilde{\sigma})f(\tilde{\gamma}, \tilde{\zeta}) = 0.$$

Откуда следует, что

$$\sum_{\tilde{\gamma} \in E^n} f(\tilde{\gamma}, \tilde{\zeta}) = 0.$$

Существование разложения доказано. Разложение (3.13) при вырожденной матрице A неоднозначно. Все такие разложения можно найти методом неопределенных коэффициентов, найдя общее решение системы 2^{n+k} уравнений. Вторая часть теоремы дает возможность нахождения некоторых частных решений

более простым методом. В матрице A фиксируем подматрицу M, соответствующую базисному минору. В матрице B коэффициентов системы (3.15) подматрица $M' \otimes M$ будет определять базисный минор. Все неизвестные $\alpha_{\tilde{\tau}\tilde{\sigma}} = 0$, если столбец $\tilde{\sigma}$ или строка $\tilde{\tau}$ не вошли в подматрицу M. Столбец свободных членов преобразованной системы (3.15) теперь состоит из столбцов матрицы M. Матрица $(M^{-1})^t \otimes M^{-1}$ является обратной к $M^t \otimes M$. Произведение M^{-1} на $\tilde{\tau}$-столбец матрицы M дает столбец ровно с одной единицей на $\tilde{\tau}$-строке. Таким образом, если в матрице $(M^{-1})^t$ элемент с индексом $(\tilde{\tau}\tilde{\sigma})$ равен 1, то $\alpha_{\tilde{\tau}\tilde{\sigma}} = 1$. Так определенные коэффициенты $\alpha_{\tilde{\tau}\tilde{\sigma}}$ порождают матрицу $A^{\diamond}(M)$ из равенства (3.14). □

Для иллюстрации теоремы приведем пример разложения (3.13) для функции $f(x_1, x_2, y_1, y_2, y_3)$, заданной матрицей A:

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Базисный минор стоит на строках $(00), (01), (11)$ и столбцах $(000), (001), (011)$. Соответствующая подматрица

$$M = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Тогда

$$A^{\diamond}(M) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

и соответствующее разложение функции имеет вид

$$f(x_1, x_2, y_1, y_2, y_3) = f(0, 0, y_1, y_2, y_3) f(x_1, x_2, 0, 0, 1) \oplus \\ \oplus f(0, 1, y_1, y_2, y_3) f(x_1, x_2, 0, 0, 0) \oplus \\ \oplus f(1, 1, y_1, y_2, y_3) f(x_1, x_2, 0, 1, 1).$$

Представляя функции $f(\tau_1, \tau_2, y_1, y_2, y_3)$ и $f(x_1, x_2, \sigma_1, \sigma_2, \sigma_3)$ формулами над бинарными функциями, получим разложение в

виде

$$f(x_1,x_2,y_1,y_2,y_3)=(y_1\oplus y_2\oplus y_3)(\bar y_1\vee\bar y_2)(\bar x_1\cdot\bar x_2)\oplus$$
$$\oplus(y_1\oplus\bar y_3)(y_2\oplus\bar y_3)(x_1\oplus x_2)\oplus(\bar y_1\oplus y_2\oplus y_3)(y_1\vee y_2)(x_1\cdot x_2).$$

Весьма интересно, что полученное представление в каком-то смысле предельно. Доказанная теорема ограничивает число сомножителей числом два. Однако разложение такого типа удается распространить на случай, когда в разложении (3.13) теоремы 3.6 вместо умножения используется дизъюнкция.

Теорема 3.7. *Для любой булевой функции $f(\tilde x,\tilde y)$ существует разложение*:

$$f(\tilde x,\tilde y)=\sum_{\tilde\sigma\in E^n}\sum_{\tilde\tau\in E^k}\alpha_{\tilde\sigma\tilde\tau}(s_{\tilde x}^{\tilde\sigma}f(\tilde x,\tilde y)\vee s_{\tilde y}^{\tilde\tau}f(\tilde x,\tilde y)).\qquad(3.16)$$

Доказательство. Разложение (3.16) можно записать следующим образом:

$$f(\tilde x,\tilde y)=\sum_{\tilde\sigma\in E^n}\sum_{\tilde\tau\in E^k}\alpha_{\tilde\sigma\tilde\tau}(s_{\tilde x}^{\tilde\sigma}f\cdot s_{\tilde y}^{\tilde\tau}f(\tilde x,\tilde y)\oplus s_{\tilde x}^{\tilde\sigma}f(\tilde x,\tilde y)\oplus s_{\tilde x_2}^{\tilde\tau}f(\tilde x,\tilde y)).$$

И тогда, воспользовавшись методом неопределенных коэффициентов, получим

$$f(\tilde x,\tilde y)=\alpha_{\tilde0\tilde0}(s_{\tilde x}^{\tilde0}f(\tilde x,\tilde y)\cdot s_{\tilde y}^{\tilde0}f(\tilde x,\tilde y)\oplus s_{\tilde x}^{\tilde0}f(\tilde x,\tilde y)\oplus s_{\tilde x_2}^{\tilde0}f(\tilde x,\tilde y))\oplus\dots$$
$$\dots\oplus\alpha_{\tilde0,\tilde1}(s_{\tilde x}^{\tilde0}f(\tilde x,\tilde y)\cdot s_{\tilde y}^{\tilde1}f(\tilde x,\tilde y)\oplus s_{\tilde x}^{\tilde0}f(\tilde x,\tilde y)\oplus s_{\tilde x_2}^{\tilde1}f(\tilde x,\tilde y))\oplus\dots$$
$$\dots\oplus\alpha_{\tilde1\tilde1}(s_{\tilde x}^{\tilde1}f(\tilde x,\tilde y)\cdot s_{\tilde y}^{\tilde1}f(\tilde x,\tilde y)\oplus s_{\tilde x}^{\tilde1}f(\tilde x,\tilde y)\oplus s_{\tilde x_2}^{\tilde1}f(\tilde x,\tilde y)).$$

Это равенство можно представить в матричном виде $F=B\cdot A$, где F — столбец значений функции f, A — матрица коэффициентов, B — матрица размерности $2^{n+k}\times2^{n+k}$, строки которой занумеруем парами $(\tilde i,\tilde j)$ — всевозможные значения переменных наборов $\tilde x$ и $\tilde y$ соответственно, столбцы — всевозможными значениями наборов $\tilde\sigma$ и $\tilde\tau$. На пересечении строки с номером $(\tilde i,\tilde j)$ и столбца $(\tilde\sigma,\tilde\tau)$ стоит элемент $b_{(\tilde i,\tilde j);(\tilde\sigma,\tilde\tau)}$, равный

$$s_{\tilde x}^{\tilde\sigma}f(\tilde x,\tilde j)\cdot s_{\tilde y}^{\tilde\tau}f(\tilde i,\tilde y)\oplus s_{\tilde x}^{\tilde\sigma}f(\tilde x,\tilde j)\oplus s_{\tilde y}^{\tilde\tau}f(\tilde i,\tilde y).$$

Покажем, что если линейными комбинациями строк матрицы B получена нулевая строка, то эти же преобразования соответствующих значений функции тоже приведут к нулю.

Пусть в линейной комбинации участвуют строки $(\tilde{i}_1, \tilde{j}_1)$, ..., $(\tilde{i}_l, \tilde{j}_l)$, $l > 1$. Множество этих строк обозначим через $S = \{(\tilde{i}_1, \tilde{j}_1), \ldots, (\tilde{i}_l, \tilde{j}_l)\}$. Рассмотрим столбцы с этими же номерами:

$$\sum_{(\tilde{i},\tilde{j})\in S} b_{(\tilde{i},\tilde{j});(\tilde{\sigma},\tilde{\tau})} = 0$$

для каждого столбца $(\tilde{\sigma}, \tilde{\tau}) \in S$. Следовательно, сумма всех элементов, стоящих на пересечении строк из множества S и столбцов с этими же номерами равна нулю.

В этой сумме участвует $3 \cdot l^2$ слагаемых. На пересечении строки с номером $(\tilde{\sigma}_k, \tilde{\tau}_k)$ и столбца с номером $(\tilde{i}_m, \tilde{j}_m)$ находится элемент

$$f(\tilde{i}_m, \tilde{\tau}_k) \cdot f(\tilde{\sigma}_k, \tilde{j}_m) \oplus f(\tilde{i}_m, \tilde{\tau}_k) \oplus f(\tilde{\sigma}_k, \tilde{j}_m),$$

а на пересечении строки с номером $(\tilde{i}_m, \tilde{j}_m)$ и столбца с номером $(\tilde{\sigma}_k, \tilde{\tau}_k)$ находится элемент

$$f(\tilde{\sigma}_k, \tilde{j}_m) \cdot f(\tilde{i}_m, \tilde{\tau}_k) \oplus f(\tilde{\sigma}_k, \tilde{j}_m) \oplus f(\tilde{i}_m, \tilde{\tau}_k).$$

Сумма этих элементов равна нулю, если $(\tilde{i}_m, \tilde{j}_m) \neq (\tilde{\sigma}_k, \tilde{\tau}_k)$, и равна $f(\tilde{i}_m, \tilde{j}_m)$, если $(\tilde{i}_m, \tilde{j}_m) = (\tilde{\sigma}_k, \tilde{\tau}_k)$.

Таким образом получаем, что

$$\sum_{(\tilde{i}_m,\tilde{j}_m)\in S} f(\tilde{i}_m, \tilde{j}_m) = 0.$$

□

Разложения по оператору сплетения.

Для сокращения записи оператора сплетения квадратные скобки вместе с содержимым будем опускать, если из контекста ясно, какая функция имеется в виду.

Теорема 3.8. *Для любой булевой функции $f(\tilde{x}, \tilde{z})$, любой булевой функции $g(\tilde{x})$ такой, что $g(\tilde{0}) = 0$, $g(\tilde{1}) = 1$ имеет место разложение:*

$$f(\tilde{x}, \tilde{z}) = \sum_{\tilde{\tau}\in E^n\setminus\{\tilde{1}\}} q_{\tilde{x}}^{\tilde{\tau}}[g(\tilde{x})] f(\tilde{x}, \tilde{z}).$$

Доказательство. Очевидно, что теорема будет доказана, если для любого набора $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$ выполняется:

$$\sum_{\tilde{\tau} \in E^n} s_{\tilde{x}}^{\tilde{\sigma}} \left(q_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}) \right) = 0.$$

Для доказательства этого равенства достаточно показать, что для любого набора $\tilde{\tau}$ имеет место равенство:

$$s_{\tilde{x}}^{\tilde{\sigma}} \left(q_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}) \right) = s_{\tilde{x}}^{\tilde{\sigma}} \left(q_{\tilde{x}}^{\tilde{\delta}} f(\tilde{x}, \tilde{z}) \right),$$

где $\tilde{\delta} = \tilde{\tau} \oplus \tilde{\sigma}^{g(\tilde{\sigma})}$.

Для того чтобы слагаемые имели различные номера, достаточно выполнения равенства $\tilde{\sigma}^{g(\tilde{\sigma})} \neq \tilde{0}$. Это равенство имеет место тогда и только тогда, когда $g(\tilde{0}) = 0$ и $g(\tilde{1}) = 1$.

Рассмотрим значение переменной x_i в $s_{\tilde{x}}^{\tilde{\sigma}} (q_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}))$ и $s_{\tilde{x}}^{\tilde{\sigma}} \left(q_{\tilde{x}}^{\tilde{\delta}} f(\tilde{x}, \tilde{z}) \right)$.

Согласно определению оператора сплетения

$$x_i = \begin{cases} g(\tilde{\sigma}), & \text{если } \tau_i = 0, \\ \sigma_i, & \text{если } \tau_i = 1 \end{cases}$$

в слагаемом $s_{\tilde{x}}^{\tilde{\sigma}} (q_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}, \tilde{z}))$ и

$$x_i = \begin{cases} g(\tilde{\sigma}), & \text{если } \tau_i \oplus \sigma_i^{g(\tilde{\sigma})} = 0, \\ \sigma_i, & \text{если } \tau_i \oplus \sigma_i^{g(\tilde{\sigma})} = 1 \end{cases}$$

в слагаемом $s_{\tilde{x}}^{\tilde{\sigma}} \left(q_{\tilde{x}}^{\tilde{\delta}} f(\tilde{x}, \tilde{z}) \right)$.

В функциональной записи это можно представить в виде

$$x_i = \bar{\tau}_i g(\tilde{\sigma}) \oplus \tau_i \sigma_i,$$

$$x_i = (\tau_i \oplus \sigma_i^{g(\tilde{\sigma}) \oplus 1}) \cdot g(\tilde{\sigma}) \oplus (\tau_i \oplus \sigma_i^{g(\tilde{\sigma})}) \sigma_i,$$

соответственно.

Несложные преобразования показывают, что значения x_i в том и другом случаях совпадают:

$$\begin{aligned} &(\tau_i \oplus \sigma_i^{g(\tilde{\sigma})} \oplus 1) g(\tilde{\sigma}) \oplus (\tau_i \oplus \sigma_i^{g(\tilde{\sigma})}) \sigma_i = \\ &\quad = (\tau_i \oplus \sigma_i \oplus g(\tilde{\sigma})) g(\tilde{\sigma}) \oplus (\tau_i \oplus \sigma_i \oplus g(\tilde{\sigma}) \oplus 1) \sigma_i = \\ &= \tau_i g(\tilde{\sigma}) \oplus \sigma_i g(\tilde{\sigma}) \oplus g(\tilde{\sigma}) \oplus \tau_i \sigma_i \oplus \sigma_i \oplus g(\tilde{\sigma}) \sigma_i \oplus \sigma_i = \bar{\sigma}_i g(\tilde{\sigma}) \oplus \tau_i \sigma_i. \end{aligned}$$

Отсюда следует, что для любого набора $\tilde{\tau}$ найдется набор $\tilde{\delta}$ такой, что $\tilde{\tau} \neq \tilde{\delta}$, а слагаемые $s^{\tilde{\sigma}}_{\tilde{x}}(q^{\tilde{\tau}}_{\tilde{x}} f(\tilde{x}, \tilde{z}))$ и $s^{\tilde{\sigma}}_{\tilde{x}}(q^{\tilde{\delta}}_{\tilde{x}} f(\tilde{x}, \tilde{z}))$ совпадают. □

Несколько примеров применения этой теоремы.

1) $g(x_1, x_2) = x_1 x_2$,

$$f(x_1, x_2, \tilde{z}) = f(x_1 x_2, x_1 x_2, \tilde{z}) \oplus f(x_1 x_2, x_2, \tilde{z}) \oplus f(x_1, x_1 x_2, \tilde{z}).$$

2) $g(x_1, x_2, x_3) = x_1 x_2 \vee x_1 x_3 \vee x_2 x_3$. В этом случае имеется несколько разложений:

$$f(x_1, x_2, x_3, \tilde{z}) = f(g, g, g, \tilde{z}) \oplus f(g, g, x_3, \tilde{z}) \oplus f(x_1, x_2, g, \tilde{z}),$$
$$f(x_1, x_2, x_3, \tilde{z}) = f(g, x_2, g, \tilde{z}) \oplus f(g, g, x_3, \tilde{z}) \oplus f(x_1, g, g, \tilde{z}).$$

§ 5. Операторные разложения по образам нечетных функций

Пусть имеется пучок операторов $\mathsf{A} = (\mathsf{a}^{\tilde{0}}, \ldots, \mathsf{a}^{\tilde{1}})$ и пусть $h(\tilde{x})$ — некоторая функция. Матрицей функции $h(\tilde{x})$ по операторному пучку A будет называться матрица:

$$M_{\mathsf{A}h} = [\alpha_{\tilde{\sigma}\tilde{\tau}}] = \begin{pmatrix} s^{\tilde{0}}_{\tilde{x}}(\mathsf{a}^{\tilde{0}} h(\tilde{x})) & \ldots & s^{\tilde{0}}_{\tilde{x}}(\mathsf{a}^{\tilde{\tau}} h(\tilde{x})) & \ldots & s^{\tilde{0}}_{\tilde{x}}(\mathsf{a}^{\tilde{1}} h(\tilde{x})) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ s^{\tilde{\sigma}}_{\tilde{x}}(\mathsf{a}^{\tilde{0}} h(\tilde{x})) & \ldots & s^{\tilde{\sigma}}_{\tilde{x}}(\mathsf{a}^{\tilde{\tau}} h(\tilde{x})) & \ldots & s^{\tilde{\sigma}}_{\tilde{x}}(\mathsf{a}^{\tilde{1}} h(\tilde{x})) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ s^{\tilde{1}}_{\tilde{x}}(\mathsf{a}^{\tilde{0}} h(\tilde{x})) & \ldots & s^{\tilde{1}}_{\tilde{x}}(\mathsf{a}^{\tilde{\tau}} h(\tilde{x})) & \ldots & s^{\tilde{1}}_{\tilde{x}}(\mathsf{a}^{\tilde{1}} h(\tilde{x})) \end{pmatrix}.$$

Теорема 3.9. *Для любого базисного пучка операторов* $(\mathsf{a}^{\tilde{0}}_{\tilde{x}}, \ldots, \mathsf{a}^{\tilde{1}}_{\tilde{x}})$, *для любой нечетной функции* $g(\tilde{x}, v)$, *для любой функции* $f(\tilde{x}, \tilde{y})$ *имеет место разложение*:

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma} \in E^n} \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\sigma}\tilde{\tau}} \mathsf{a}^{\tilde{\tau}}_{\tilde{x}} g(\tilde{x}, f^{\gamma}(\tilde{\sigma}, \tilde{y})), \tag{3.17}$$

где $\gamma = \mathrm{d}_{\tilde{x}} g(\tilde{x}, 1)$, $[\beta_{\tilde{\tau}\tilde{\sigma}}] = A^{-1}_{g'_v}$.

Доказательство. Для строк матрицы $[\beta_{\tilde{\tau}\tilde{\sigma}}]$ введем обозначения:

$$[\beta_{\tilde\tau\tilde\sigma}] = \begin{pmatrix} \beta_{\tilde0\tilde0} & \dots & \beta_{\tilde0\tilde\sigma} & \dots & \beta_{\tilde0\tilde1} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \beta_{\tilde\tau\tilde0} & \dots & \beta_{\tilde\tau\tilde\sigma} & \dots & \beta_{\tilde\tau\tilde1} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \beta_{\tilde1\tilde0} & \dots & \beta_{\tilde1\tilde\sigma} & \dots & \beta_{\tilde1\tilde1} \end{pmatrix} = \begin{pmatrix} \varphi_{\tilde0}(\tilde x) \\ \vdots \\ \varphi_{\tilde\tau}(\tilde x) \\ \vdots \\ \varphi_{\tilde1}(\tilde x) \end{pmatrix}.$$

Согласно определению $\beta_{\tilde\tau\tilde\sigma}$ имеем два свойства:

а) $\mathrm{d}_{\tilde x}\left[\varphi_{\tilde\tau}(\tilde x)\cdot \mathfrak{a}^{\tilde\delta} g'_v(\tilde x, v)\right] = 1$ если и только если $\tilde\tau = \tilde\delta$,

б) $\sum\limits_{\tilde\tau\in\tilde E^n} \mathfrak{a}^{\tilde\sigma} g'_v(\tilde\sigma, v)\cdot\varphi_{\tilde\tau}(\tilde\delta) = 1$ если и только если $\tilde\sigma = \tilde\delta$.

Пусть наборы $\{\tilde\tau^1,\dots,\tilde\tau^k\}$ такие, что

$$\mathrm{d}_{\tilde x} g(\tilde x, 0) = \mathfrak{a}^{\tilde\tau^1} g(\tilde x, 0)\oplus\dots\oplus\mathfrak{a}^{\tilde\tau^k} g(\tilde x, 0).$$

По предложению 3.6 такие наборы для базисных пучков всегда существуют. Рассмотрим выражение $\mathrm{d}_{\tilde x}\varphi_{\tilde\tau}(\tilde x)$.

Пусть $\tilde\delta\in\{\tilde\tau^1,\dots,\tilde\tau^k\}$, тогда

$$\mathrm{d}_{\tilde x}[\varphi_{\tilde\delta}(\tilde x)\cdot\mathfrak{a}^{\tilde\delta} g'_v(\tilde x, v)] = \mathrm{d}_{\tilde x}[\varphi_{\tilde\tau}(\tilde x)\cdot\mathrm{d}_{\tilde x} g'_v(\tilde x, v)]\oplus$$
$$\oplus\,\mathrm{d}_{\tilde x}[\varphi_{\tilde\tau}(\tilde x)\cdot\mathfrak{a}^{\tilde\tau^1} g'_v(x, v)]\oplus\dots\oplus\mathrm{d}_{\tilde x}[\varphi_{\tilde\tau}(\tilde x)\cdot\mathfrak{a}^{\tilde\tau^k} g'_v(x, v)]. \quad (3.18)$$

1) если $\tilde\tau = \tilde\delta$, то сумма (3.18) равна 1 и сокращается до одного слагаемого:

$$\mathrm{d}_{\tilde x}[\varphi_{\tilde\tau}(\tilde x)\cdot\mathrm{d}_{\tilde x} g'_v(\tilde x, v)] = 1.$$

Следовательно $\mathrm{d}_{\tilde x}\varphi_{\tilde\tau}(\tilde x) = 1$.

2) если $\tilde\tau\neq\tilde\delta$ и $\tilde\tau\in\{\tilde\tau^1,\dots,\tilde\tau^k\}$, то сумма (3.18) равна 0 и сокращается до двух слагаемых:

$$\mathrm{d}_{\tilde x}\varphi_{\tilde\tau}(\tilde x)\cdot\mathrm{d}_{\tilde x} g'_v(\tilde x, v)\oplus\mathrm{d}_{\tilde x}[\varphi_{\tilde\tau^i}(\tilde x)\cdot\mathfrak{a}^{\tilde\tau^i} g'_v(\tilde x, v)] = 0.$$

По свойству а) выполняется:

$$\mathrm{d}_{\tilde x}[\varphi_{\tilde\tau^i}(\tilde x)\cdot\mathfrak{a}^{\tilde\tau^i} g(\tilde x, v)] = 1,$$

откуда следует, что

$$\mathrm{d}_{\tilde x}\varphi_{\tilde\tau}(\tilde x)\cdot\mathrm{d} g'_v(\tilde x, v) = 1,$$

и, окончательно, $\mathrm{d}_{\tilde{x}}\varphi_{\tilde{\tau}}(\tilde{x}) = 1$.

3) если $\tilde{\tau} \neq \tilde{\delta}$ и $\tilde{\tau} \notin \{\tilde{\tau}^1, \ldots, \tilde{\tau}^k\}$, то сумма (3.18) равна 0 и принимает вид:

$$\mathrm{d}\varphi_{\tilde{\tau}}(\tilde{x}) \cdot \mathrm{d}_{\tilde{x}} g'_v(\tilde{x}, v) = 0.$$

Поскольку функция $g(\tilde{x}, v)$ — нечетная, в этом случае получаем

$$\mathrm{d}\varphi_{\tilde{\tau}}(\tilde{x}) = 0.$$

Для доказательства равенства (3.17) будем преобразовывать его правую часть.

$$\sum_{\tilde{\sigma} \in E^n} \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}} \cdot \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g(\tilde{x}, f^\gamma(\tilde{\sigma}, \tilde{y})) =$$

$$= \sum_{\tilde{\sigma} \in E^n} \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}} \left(\left(\mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g'_v(\tilde{x}, v) \right) \cdot f^\gamma(\tilde{\sigma}, \tilde{y}) \oplus \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g(\tilde{x}, 0) \right) =$$

$$= \sum_{\tilde{\sigma} \in E^n} f^\gamma(\tilde{\sigma}, \tilde{y}) \cdot \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}} \cdot \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g'_v(\tilde{x}, v) \oplus \sum_{\tilde{\tau} \in E^n} \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g(\tilde{x}, 0) \cdot \sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}}.$$

По свойству б) имеем

$$\sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}} \cdot \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g'_v(\tilde{x}, v) = 1$$

тогда и только тогда, когда $\tilde{x} = \tilde{\sigma}$, что влечет

$$\sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}} \cdot \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g'_v(\tilde{x}, v) = \tau_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}.$$

По рассмотренным случаям 1)–3) имеем следующую цепочку равенств:

$$\sum_{\tilde{\tau} \in E^n} \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g(\tilde{x}, 0) \cdot \sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}} = \sum_{\tilde{\tau} \in E^n} \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g(\tilde{x}, 0) \cdot \mathrm{d}_{\tilde{x}} \varphi_{\tilde{\tau}}(\tilde{x}) =$$

$$= \mathrm{d}_{\tilde{x}} g(\tilde{x}, 0) = \mathrm{d}_{\tilde{x}} g(\tilde{x}, 1) \oplus 1 = \overline{\gamma} = \sum_{\tilde{\sigma} \in E^n} \overline{\gamma} \cdot x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}.$$

Заканчивая преобразования (3.17), имеем

$$\sum_{\tilde{\sigma} \in E^n} f^\gamma(\tilde{\sigma}, \tilde{y}) \cdot \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}} \cdot \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g'_v(\tilde{x}, v) \oplus \sum_{\tilde{\tau} \in E^n} \mathrm{a}^{\tilde{\tau}}_{\tilde{x}} g(\tilde{x}, 0) \cdot \sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\tau}\tilde{\sigma}} =$$

$$= \sum_{\tilde{\sigma} \in E^n} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} \cdot f^\gamma(\tilde{\sigma}, \tilde{y}) \oplus \sum_{\tilde{\sigma} \in E^n} \overline{\gamma} \cdot x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} =$$

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

□

Доказанная теорема дает возможность проводить разложения по части переменных.

Как следствие приведем два частных случая теоремы 3.9, имеющие более простой вид разложения.

Следствие. 1. Разложение (3.17) для булевой функции $g(\tilde{x}, v) = h(\tilde{x}) \cdot v$, имеет вид

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma} \in E^n} \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\sigma}\tilde{\tau}} \cdot \mathrm{a}_{\tilde{x}}^{\tilde{\tau}} h(\tilde{x}) \cdot f(\tilde{\sigma}, \tilde{y}).$$

2. Разложение (3.17) для функции $g(\tilde{x}, v) = h(\tilde{x}) \vee v$, имеет вид

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma} \in E^n} \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\sigma}\tilde{\tau}} \cdot (\mathrm{a}_{\tilde{x}}^{\tilde{\tau}}(h(\tilde{x})) \vee \overline{f}(\tilde{\sigma}, \tilde{y})).$$

Разложения по двум типам операторов.

Класс MH однородно смешанных пучков дает интересное разложение по части переменных, упрощающее разложение из теоремы 3.9.

Рассмотрим еще один класс операторов, которые будут называться операторами типа II. Пусть задана последовательность $\mathrm{t} = \mathrm{t}_1 \ldots \mathrm{t}_n$, в которой компоненты $\mathrm{t}_i \in \{\mathrm{i}, \mathrm{o}, \mathrm{d}\}$. По этой последовательности определяется оператор, действующий на булеву функцию $f(x_1, \ldots, x_n)$, как композиция операторов:

при $n = 1$ $\quad \mathrm{t}\,(f(\tilde{x})) = \begin{cases} \mathrm{d}_{x_1} f(\tilde{x}), & \text{если } \mathrm{t} = \mathrm{d}, \\ \mathrm{o}_{x_1} f(\tilde{x}), & \text{если } \mathrm{t} = \mathrm{o}, \\ \mathrm{i}_{x_1} f(\tilde{x}), & \text{если } \mathrm{t} = \mathrm{i}; \end{cases}$

при $n > 1$ $\quad \mathrm{t}\,(f(\tilde{x})) = \mathrm{t}_n(\mathrm{t}_1 \ldots \mathrm{t}_{n-1}(f(\tilde{x}))).$

Индексы в обозначениях операторов типа II будут использоваться аналогично операторам, введенным в параграфе 1. Заметим, что только оператор d...d относится к обоим классам операторов.

Теорема 3.10. *Для любого однородно смешанного пучка* $\mathrm{A} = \{\mathrm{a}^0, \ldots, \mathrm{a}^1\}$, *для любой функции* $f(\tilde{x}, \tilde{y})$ *имеет место разложение:*

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

где $\mathrm{b}_{\tilde{x}}^{\tilde{\tau}}$ *— операторы II типа, которые определяются следующим образом:*

$$\mathrm{b}_i^{\tilde{\tau}} = \begin{cases} \mathrm{o}, & \text{если } \mathrm{a}_i^{\tilde{\sigma}} = e, \\ \mathrm{i}, & \text{если } \mathrm{a}_i^{\tilde{\sigma}} = \mathrm{p}, \\ \mathrm{d}, & \text{если } \mathrm{a}_i^{\tilde{\sigma}} = \mathrm{d}, \end{cases} \tag{3.19}$$

где $\tilde{\sigma} = (\tau_1, \ldots, \tau_{i-1}, \bar{\tau}_i, \tau_{i+1}, \ldots, \tau_n)$.

Доказательство проведем индукцией по длине n набора $\tilde{x}$.

Базис индукции. При $n = 1$ существуют только три однородно смешанных пучка с точностью до перестановки операторов:

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

Соответствующие разложения имеют вид

$$f(\tilde{x}, \tilde{y}) = ex_1 \cdot \mathrm{i}_{x_1} f(\tilde{x}, \tilde{y}) \oplus \mathrm{p}x_1 \cdot \mathrm{o}_{x_1} f(\tilde{x}, \tilde{y})$$
$$f(\tilde{x}, \tilde{y}) = \mathrm{d}x_1 \cdot \mathrm{i}_{x_1} f(\tilde{x}, \tilde{y}) \oplus \mathrm{p}x_1 \cdot \mathrm{d}_{x_1} f(\tilde{x}, \tilde{y}),$$
$$f(\tilde{x}, \tilde{y}) = ex_1 \cdot \mathrm{d}_{x_1} f(\tilde{x}, \tilde{y}) \oplus \mathrm{d}x_1 \cdot \mathrm{o}_{x_1} f(\tilde{x}, \tilde{y}).$$

Легко заметить, что эти разложения удовлетворяют условиям теоремы.

Шаг индукции. При $n > 1$ можно считать, что пучок A образован слиянием однородно смешанных пучков U, V операторов размерности $n - 1$ и однородно смешанного пучка C операторов размерности 1.

Пусть, для определенности, $\mathrm{C} = \{e, \mathrm{p}\}$. Для удобства введем обозначения: $\tilde{x}' = (x_2, \ldots, x_n)$, $\tilde{\tau}' = (\tau_2, \ldots, \tau_n)$. По предположению индукции

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\tau}' \in E^{n-1}} \mathrm{u}^{\tilde{\tau}'}(x_2 \cdot \ldots \cdot x_n) \cdot \mathrm{t}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}, \tilde{y}),$$
$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\tau}' \in E^{n-1}} \mathrm{v}^{\tilde{\tau}'}(x_2 \cdot \ldots \cdot x_n) \cdot \mathrm{s}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}, \tilde{y}),$$

где $\mathrm{t}^{\tilde{\tau}'}$, $\mathrm{s}^{\tilde{\tau}'}$ — операторы II типа, фигурирующие в формулировке теоремы. Применим разложение Шеннона и проведем несколько преобразований.

$$f(\tilde{x}, \tilde{y}) = ex_1 \cdot \mathrm{i}_{x_1} f(\tilde{x}, \tilde{y}) \oplus \mathrm{p}x_1 \cdot \mathrm{o}_{x_1} f(\tilde{x}, \tilde{y}) =$$
$$= ex_1 \cdot \mathrm{i}_{x_1} \sum_{\tilde{\tau}' \in E^{n-1}} \mathrm{u}^{\tilde{\tau}'}(x_2 \cdot \ldots \cdot x_n) \cdot \mathrm{t}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}, \tilde{y}) \oplus$$

$$\oplus\, \mathrm{d}x_1 \cdot \mathrm{o}_{x_1} \sum_{\tilde{\tau}' \in E^{n-1}} \nu^{\tilde{\tau}'}(x_2 \cdot \ldots \cdot x_n) \cdot \mathrm{s}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}, \tilde{y}) =$$

$$= \sum_{\tilde{\tau}' \in E^{n-1}} ex_1 \cdot \mathfrak{u}^{\tilde{\tau}'}(x_2 \cdot \ldots \cdot x_n) \cdot \mathrm{i}_{x_1} \mathrm{t}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}, \tilde{y}) \oplus$$

$$\oplus \sum_{\tilde{\tau}' \in E^{n-1}} \mathrm{p}x_1 \cdot \nu^{\tilde{\tau}'}(x_2 \cdot \ldots \cdot x_n) \cdot \mathrm{o}_{x_1} \mathrm{s}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}, \tilde{y}) =$$

$$= \sum_{\tilde{\tau}' \in E^{n-1}} \mathfrak{a}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) \cdot \left(\mathrm{i}_{x_1} \mathrm{t}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}, \tilde{y}) \oplus \mathrm{o}_{x_1} \mathrm{s}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}, \tilde{y})\right) =$$

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

где

$$\mathrm{b}_i^{\tilde{\tau}} = \begin{cases} \mathrm{t}_i^{\tilde{\tau}'}, & \text{если } 2 \leqslant i \leqslant n \text{ и } \tau_1 = 0, \\ \mathrm{s}_i^{\tilde{\tau}'}, & \text{если } 2 \leqslant i \leqslant n \text{ и } \tau_1 = 1, \\ \mathrm{i}, & \text{если } i = 1 \text{ и } \tau_1 = 0, \\ \mathrm{o}, & \text{если } i = 1 \text{ и } \tau_1 = 1. \end{cases}$$

Осталось проверить условие (3.19). По предположению индукции оно выполняется, если $2 \leqslant i \leqslant n$. С другой стороны

$$\mathfrak{a}_1^{\tilde{\sigma}} = \mathfrak{c}^{\bar{\tau}_1} = \begin{cases} \mathrm{i}, & \text{если } \tau_1 = 0, \\ e, & \text{если } \tau_1 = 1, \end{cases}$$

где $\tilde{\sigma} = (\bar{\tau}_1, \tau_2, \ldots, \tau_n)$. Таким образом, при $i = 1$ условие (3.19) также выполняется.

При рассмотрении других вариантов пучка C можно воспользоваться следующими типами разложений:

$$f(\tilde{x}, \tilde{y}) = \mathrm{d}x_1 \cdot \mathrm{i}_{x_1} f(\tilde{x}, \tilde{y}) \oplus \mathrm{p}x_1 \cdot \mathrm{d}_{x_1} f(\tilde{x}, \tilde{y}),$$
$$f(\tilde{x}, \tilde{y}) = ex_1 \cdot \mathrm{d}_{x_1} f(\tilde{x}, \tilde{y}) \oplus \mathrm{d}x_1 \cdot \mathrm{o}_{x_1} f(\tilde{x}, \tilde{y}).$$

Разбор этих случаев полностью аналогичен предыдущему. □

§ 6. Бинарные термы в разложениях

Будем считать, что булева функция $f(x_1, \ldots, x_n)$ имеет $(\Delta_1, \ldots, \Delta_m)$-разложение по переменным $x_{i_1}, \ldots, x_{i_m}$, если выполняется следующее равенство:

$$f(x_1, \ldots, x_n) = \sum_{\sigma_{i_1}, \ldots, \sigma_{i_m}} \Big(x_{i_1}^{\sigma_{i_1} \oplus \tau_1} \Delta_1 \Big(\ldots$$
$$\ldots \Big(x_{i_m}^{\sigma_{i_m} \oplus \tau_m} \Delta_m f^{\tau'_m}(x_1, \ldots, \sigma_{i_1}, \ldots, \sigma_{i_m}, \ldots, x_n)\Big) \ldots\Big)\Big),$$

где $\tau'_m, \tau_i \in \{0,1\}$, $\Delta_i \in \{\cdot, \vee, |, \downarrow, \to, \nrightarrow, \leftarrow, \nleftrightarrow\}$, $i = 1, \ldots, m$, а суммирование ведется по всем наборам $(\sigma_{i_1}, \ldots, \sigma_{i_m}) \in E^m$.

Можно заметить, что в $(\Delta_1, \ldots, \Delta_m)$-разложении неявно предполагается бесповторность, которая совместно со свойствами бинарных функций гарантирует нечетность функции $x_{i_1}^{\sigma_{i_1} \oplus \tau_1} \Delta_1 \left(\ldots \left(x_{i_m}^{\sigma_{i_m} \oplus \tau_m} \Delta_m y \right) \ldots \right)$. Однако доказательство представляет самостоятельный интерес в связи с нахождением конкретных разложений.

Теорема 3.11. *Любая булева функция $f(x_1, \ldots, x_n)$ имеет $(\Delta_1, \ldots, \Delta_m)$-разложение по переменным $x_{i_1}, \ldots, x_{i_m}$, $m \leqslant n$:*

$$f(x_1, \ldots, x_n) = \sum_{\sigma_{i_1}, \ldots, \sigma_{i_m}} \left(x_{i_1}^{\sigma_{i_1} \oplus \tau_1} \Delta_1 \Big(\ldots \right.$$
$$\left. \ldots \Big(x_{i_m}^{\sigma_{i_m} \oplus \tau_m} \Delta_m f^{\tau'_m}(x_1, \ldots, \sigma_{i_1}, \ldots, \sigma_{i_m}, \ldots, x_n) \Big) \ldots \Big) \right),$$

где для $i = 1, \ldots, m$

$$\tau_i = \begin{cases} 0, & \text{если } \Delta_i \in \{\cdot, |, \to, \nrightarrow\}, \\ 1, & \text{если } \Delta_i \in \{\vee, \downarrow, \leftarrow, \nleftrightarrow\}; \end{cases}$$
$$\tau'_m = \begin{cases} 0, & \text{если } \Delta_m \in \{\vee, \downarrow, \to, \nrightarrow\}, \\ 1, & \text{если } \Delta_m \in \{\cdot, |, \leftarrow, \nleftrightarrow\}. \end{cases}$$

Доказательство. Проведем индукцию по m. Не ограничивая общности, полагаем $i_1 = 1, \ldots, i_m = m$. При $m = 1$ указанное равенство имеет вид

$$f(x_1, \ldots, x_n) =$$
$$= x_1^{0 \oplus \tau_1} \Delta_1 f^{\tau'_1}(0, x_2, \ldots, x_n) \oplus x_1^{1 \oplus \tau_1} \Delta_1 f^{\tau'_1}(1, x_2, \ldots, x_n).$$

Далее перебором всех вариантов Δ_1 имеем восемь равенств, которые проверяются непосредственно:

1) $\Delta_1 \equiv \cdot \quad f(\tilde{x}) = \bar{x}_1 \cdot f(0, x_2, \ldots, x_n) \oplus x_1 \cdot f(1, x_2, \ldots, x_n)$,
2) $\Delta_1 \equiv | \quad f(\tilde{x}) = \bar{x}_1 \mid f(0, x_2, \ldots, x_n) \oplus x_1 \mid f(1, x_2, \ldots, x_n)$,
3) $\Delta_1 \equiv \to \quad f(\tilde{x}) = \bar{x}_1 \to \bar{f}(0, x_2, \ldots, x_n) \oplus x_1 \to \bar{f}(1, x_2, \ldots, x_n)$,
4) $\Delta_1 \equiv \nrightarrow \quad f(\tilde{x}) = \bar{x}_1 \nrightarrow \bar{f}(0, x_2, \ldots, x_n) \oplus x_1 \nrightarrow \bar{f}(1, x_2, \ldots, x_n)$,
5) $\Delta_1 \equiv \vee \quad f(\tilde{x}) = x_1 \vee \bar{f}(0, x_2, \ldots, x_n) \oplus \bar{x}_1 \vee \bar{f}(1, x_2, \ldots, x_n)$,
6) $\Delta_1 \equiv \downarrow \quad f(\tilde{x}) = x_1 \downarrow \bar{f}(0, x_2, \ldots, x_n) \oplus \bar{x}_1 \downarrow \bar{f}(1, x_2, \ldots, x_n)$,
7) $\Delta_1 \equiv \leftarrow \quad f(\tilde{x}) = x_1 \leftarrow f(0, x_2, \ldots, x_n) \oplus \bar{x}_1 \leftarrow f(1, x_2, \ldots, x_n)$,
8) $\Delta_1 \equiv \nleftrightarrow \quad f(\tilde{x}) = x_1 \nleftrightarrow f(0, x_2, \ldots, x_n) \oplus \bar{x}_1 \nleftrightarrow f(1, x_2, \ldots, x_n)$.

По индукции для $m-1$ предполагаем выполнение равенства:

$$f(x_1,\dots,x_n)=\sum_{\sigma_1,\dots,\sigma_{m-1}}\Big(x_1^{\sigma_1\oplus\tau_1}\Delta_1\Big(\dots$$
$$\dots\Big(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}f^{\tau'_{m-1}}(\sigma_1,\dots,\sigma_{m-1},x_m,\dots,x_n)\Big)\dots\Big)\Big).$$

Воспользовавшись доказанным равенством:

$$f^{\tau'_{m-1}}(\sigma_1,\dots,\sigma_{m-1},x_m,\dots,x_n)=$$
$$=x_m^{0\oplus\tau_m}\Delta_m f^{\tau'_m}(\sigma_1,\dots,\sigma_{m-1},0,x_{m+1},\dots,x_n)\oplus$$
$$\oplus x_m^{1\oplus\tau_m}\Delta_m f^{\tau'_m}(\sigma_1,\dots,\sigma_{m-1},1,x_{m+1},\dots,x_n)\oplus\bar\tau'_{m-1},$$

предположением индукции и свойствами дистрибутивности из предложения 1, проведем несколько преобразоваий.

$$f(x_1,\dots,x_n)=\sum_{\sigma_1,\dots,\sigma_{m-1}}\Big(x_1^{\sigma_1\oplus\tau_1}\Delta_1\Big(\dots\Big(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}$$
$$\Delta_{m-1}f^{\tau'_{m-1}}(\sigma_1,\dots,\sigma_{m-1},x_m,\dots,x_n)\Big)\dots\Big)\Big)=$$
$$=\sum_{\sigma_1,\dots,\sigma_{m-1}}\Big(x_1^{\sigma_1\oplus\tau_1}\Delta_1\Big(\dots\Big(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}$$
$$\Delta_{m-1}\Big(x_m^{0\oplus\tau_m}\Delta_m f^{\tau'_m}(\sigma_1,\dots,\sigma_{m-1},0,x_{m+1},\dots,x_n)\oplus$$
$$\oplus x_m^{1\oplus\tau_m}\Delta_m f^{\tau'_m}(\sigma_1,\dots,\sigma_{m-1},1,x_{m+1},\dots,x_n)\oplus\bar\tau'_{m-1}\Big)\Big)\dots\Big)\Big)=$$
$$=\sum_{\sigma_1,\dots,\sigma_{m-1}}\Big(x_1^{\sigma_1\oplus\tau_1}\Delta_1\Big(\dots\Big(x_m^{\sigma_m\oplus\tau_m}\Delta_m$$
$$\Delta_m f^{\tau'_m}(\sigma_1,\dots,\sigma_{m-1},0,x_{m+1},\dots,x_n)\Big)\dots\Big)\Big)\oplus$$
$$\oplus\sum_{\sigma_1,\dots,\sigma_{m-1}}\Big(x_1^{\sigma_1\oplus\tau_1}\Delta_1\Big(\dots\Big(x_m^{\sigma_m\oplus\tau_m}\Delta_m$$
$$\Delta_m f^{\tau'_m}(\sigma_1,\dots,\sigma_{m-1},1,x_{m+1},\dots,x_n)\Big)\dots\Big)\Big)=$$
$$=\sum_{\sigma_1,\dots,\sigma_m}\Big(x_1^{\sigma_1\oplus\tau_1}\Delta_1\Big(\dots\Big(x_m^{\sigma_m\oplus\tau_m}\Delta_m$$
$$\Delta_m f^{\tau'_m}(\sigma_1,\dots,\sigma_{m-1},\sigma_m,x_{m+1},\dots,x_n)\Big)\dots\Big)\Big)\oplus$$
$$\oplus\sum_{\sigma_1,\dots,\sigma_{m-1}}\Big(x_1^{\sigma_1\oplus\tau_1}\Delta_1\Big(\dots\Big(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\bar\tau'_{m-1}\Big)\dots\Big)\Big).$$

Таким образом, теорема будет доказана, если вторая сумма равна нулю:

$$\sum_{\sigma_1,\ldots,\sigma_{m-1}} \left(x_1^{\sigma_1\oplus\tau_1}\Delta_1\left(\ldots\left(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\tau'_{m-1}\right)\ldots\right)\right) = 0.$$

Доказательство этого равенства проведем индукцией от $m-1$ к 1.

$$\sum_{\sigma_{m-1}} \left(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\tau'_{m-1}\right) = \\ = x_{m-1}^{\tau_{m-1}}\Delta_{m-1}\bar{\tau}'_{m-1} \oplus \bar{x}_{m-1}^{\tau_{m-1}}\Delta_{m-1}\bar{\tau}'_{m-1}.$$

Полный перебор случаев показывает равенство нулю данной суммы:

1) $\Delta_1 \equiv \cdot \quad \tau_{m-1}=0,\ \tau'_{m-1}=1,\ \bar{x}_{m-1}\cdot 0 \oplus x_{m-1}\cdot 0 = 0\oplus 0 = 0;$
2) $\Delta_1 \equiv | \quad \tau_{m-1}=0,\ \tau'_{m-1}=1,\ \bar{x}_{m-1} \mid 0 \oplus x_{m-1} \mid 0 = 1\oplus 1 = 0.$

Остальные случаи рассматриваются аналогично.

Введем обозначение:

$$s = \sum_{\sigma_2,\ldots,\sigma_{m-1}} \left(x_2^{\sigma_2\oplus\tau_2}\Delta_2\left(\ldots\left(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\tau'_{m-1}\right)\ldots\right)\right).$$

Далее по индукции, учитывая свойство дистрибутивности и то, что в сумму s входит четное число слагаемых:

$$\sum_{\sigma_1,\ldots,\sigma_{m-1}}\left(x_1^{\sigma_1\oplus\tau_1}\Delta_1\left(x_2^{\sigma_2\oplus\tau_2}\Delta_2\left(\ldots\left(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\tau'_{m-1}\right)\ldots\right)\right)\right) =$$
$$= \sum_{\sigma_2,\ldots,\sigma_{m-1}}\left(x_1^{\tau_1}\Delta_1\left(x_2^{\sigma_2\oplus\tau_2}\Delta_2\left(\ldots\left(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\tau'_{m-1}\right)\ldots\right)\right)\right) \oplus$$
$$\oplus \sum_{\sigma_2,\ldots,\sigma_{m-1}}\left(\bar{x}_1^{\tau_1}\Delta_1\left(x_2^{\sigma_2\oplus\tau_2}\Delta_2\left(\ldots\left(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\tau'_{m-1}\right)\ldots\right)\right)\right) =$$
$$= x_1^{\tau_1}\Delta_1 \sum_{\sigma_2,\ldots,\sigma_{m-1}}\left(x_2^{\sigma_2\oplus\tau_2}\Delta_2\left(\ldots\left(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\tau'_{m-1}\right)\ldots\right)\right) \oplus$$
$$\oplus\, x_1^{\tau_1}\Delta_1 0 \oplus$$
$$\oplus\, \bar{x}_1^{\tau_1}\Delta_1 \sum_{\sigma_2,\ldots,\sigma_{m-1}}\left(x_2^{\sigma_2\oplus\tau_2}\Delta_2\left(\ldots\left(x_{m-1}^{\sigma_{m-1}\oplus\tau_{m-1}}\Delta_{m-1}\tau'_{m-1}\right)\ldots\right)\right) \oplus$$
$$\oplus\, \bar{x}_1^{\tau_1}\Delta_1 0 = x_1^{\tau_1}\Delta_1 s \oplus x_1^{\tau_1}\Delta_1 0 \oplus \bar{x}_1^{\tau_1}\Delta_1 s \oplus \bar{x}_1^{\tau_1}\Delta_1 0.$$

Перебор случаев для $\Delta_1 \in \{\cdot, \vee, |, \downarrow, \to, \leftrightarrow, \leftarrow, \leftrightarrow\}$, аналогичный проведенному выше, с учетом индуктивного предположения завершает доказательство теоремы. □

Представляет интерес рассмотрение вида конкретных $(\Delta_1, \ldots, \Delta_m)$-разложений, например, по одной функции или без использования отрицания — позитивных разложений.

Следствие. *Для любой булевой функции имеют место разложения по одной бинарной функции:*

$$1)\ f(\tilde{x}) = \sum_{\sigma_1,\ldots,\sigma_m} \left(x_1^{\sigma_1} \mid \left(\ldots\left(x_m^{\sigma_m} \mid f(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\right)\ldots\right)\right),$$

$$2)\ f(\tilde{x}) = \sum_{\sigma_1,\ldots,\sigma_m} \left(x_1^{\sigma_1} \leftrightarrow \left(\ldots\left(x_m^{\sigma_m} \leftrightarrow \bar{f}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\right)\ldots\right)\right),$$

$$3)\ f(\tilde{x}) = \sum_{\sigma_1,\ldots,\sigma_m} \left(x_1^{\sigma_1} \to \left(\ldots\left(x_m^{\sigma_m} \to \bar{f}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\right)\ldots\right)\right),$$

$$4)\ f(\tilde{x}) = \sum_{\sigma_1,\ldots,\sigma_m} \left(x_1^{\bar{\sigma}_1} \leftarrow \left(\ldots\left(x_m^{\bar{\sigma}_m} \leftarrow f(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\right)\ldots\right)\right),$$

$$5)\ f(\tilde{x}) = \sum_{\sigma_1,\ldots,\sigma_m} \left(x_1^{\bar{\sigma}_1} \leftrightarrow \left(\ldots\left(x_m^{\bar{\sigma}_m} \leftrightarrow f(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\right)\ldots\right)\right),$$

$$6)\ f(\tilde{x}) = \sum_{\sigma_1,\ldots,\sigma_m} \left(x_1^{\bar{\sigma}_1} \vee \left(\ldots\left(x_m^{\bar{\sigma}_m} \vee \bar{f}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\right)\ldots\right)\right),$$

$$7)\ f(\tilde{x}) = \sum_{\sigma_1,\ldots,\sigma_m} \left(x_1^{\bar{\sigma}_1} \downarrow \left(\ldots\left(x_m^{\bar{\sigma}_m} \downarrow \bar{f}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\right)\ldots\right)\right).$$

Следствие. *Для любой булевой функции имеют место следующие позитивные разложения:*

$$f(x_1,\ldots,x_n) = \sum_{\sigma_1,\ldots,\sigma_m} \left(x_1 \Delta_{\sigma_1} \left(\ldots\left(x_m \Delta_{\sigma_m} f(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\right)\ldots\right)\right),$$

а) $\Delta_{\sigma_i} = \begin{cases} \cdot, & \text{если } \sigma_i = 1, \\ \leftrightarrow, & \text{если } \sigma_i = 0, \end{cases} \qquad i = 1,\ldots,m,$

б) $\Delta_{\sigma_i} = \begin{cases} \to, & \text{если } \sigma_i = 1, \\ \vee, & \text{если } \sigma_i = 0, \end{cases} \qquad i = 1,\ldots,m,$

в) $\Delta_{\sigma_i} = \begin{cases} \leftrightarrow, & \text{если } \sigma_i = 1, \\ \downarrow, & \text{если } \sigma_i = 0, \end{cases} \qquad i = 1,\ldots,m-1,$

$$\Delta_{\sigma_m} = \begin{cases} \cdot, & \text{если } \sigma_m = 1, \\ \leftrightarrow, & \text{если } \sigma_m = 0, \end{cases}$$

г) $\Delta_{\sigma_i} = \begin{cases} |, & \text{если } \sigma_i = 1, \\ \leftarrow, & \text{если } \sigma_i = 0, \end{cases} \qquad i = 1, \ldots, m-1,$

$\Delta_{\sigma_m} = \begin{cases} \rightarrow, & \text{если } \sigma_i = m, \\ \vee, & \text{если } \sigma_m = 0. \end{cases}$

§ 7. Разложения по невырожденным системам функций

Результаты этого параграфа можно рассматривать как пример для сравнения с предыдущими результатами о разложениях по базисным пучкам операторов. Во-первых, произвольный выбор базисной системы функций сложен сам по себе, во-вторых метод вычисления коэффициентов разложения использует нахождение обратной матрицы для матрице из базисных функций, что может оказаться весьма непросто ввиду быстрого роста размеров этой матрицы, в-третьих само разложение имеет более сложный вид по сравнению с операторным.

Теорема 3.12. *Пусть $\{g_{\tilde\tau}(\tilde x, v)\}$ — система булевых функций такая, что матрица $[\alpha_{\tilde\sigma\tilde\tau}]$, где $\alpha_{\tilde\sigma\tilde\tau} = s^{\tilde\sigma}_{\tilde x}[(g_{\tilde\tau}(\tilde x, v))'_v]$, невырожденная. Тогда любая булева функция $f(\tilde x, \tilde y)$ представима в виде*

$$f(\tilde x, \tilde y) = \sum_{\tilde\sigma \in E^n} \sum_{\tilde\tau \in E^n} \beta_{\tilde\sigma\tilde\tau} \left(g_{\tilde\tau}(\tilde x, f(\tilde\sigma, \tilde y)) \oplus g_{\tilde\tau}(\tilde x, 0)\right),$$

где $[\beta_{\tilde\sigma\tilde\tau}]^t = [\alpha_{\tilde\sigma\tilde\tau}]^{-1}$.

Доказательство. Используя равенство

$$g(\tilde x, v) = v \cdot g(\tilde x, 1) \oplus \bar v \cdot g(\tilde x, 0),$$

выполним следующие преобразования:

$$\sum_{\tilde\sigma \in E^n} \sum_{\tilde\tau \in E^n} \beta_{\tilde\sigma\tilde\tau} \left(g_{\tilde\tau}(\tilde x, f(\tilde\sigma, \tilde y)) \oplus g_{\tilde\tau}(\tilde x, 0)\right) =$$

$$= \sum_{\tilde\sigma \in E^n} \sum_{\tilde\tau \in E^n} \beta_{\tilde\sigma\tilde\tau} \left(f(\tilde\sigma, \tilde y) \cdot g_{\tilde\tau}(\tilde x, 1)) \oplus \bar f(\tilde\sigma, \tilde y) \cdot g_{\tilde\tau}(\tilde x, 0) \oplus g_{\tilde\tau}(\tilde x, 0)\right) =$$

$$= \sum_{\tilde\sigma \in E^n} \sum_{\tilde\tau \in E^n} \beta_{\tilde\sigma\tilde\tau} (f(\tilde\sigma, \tilde y) \cdot (g_{\tilde\tau}(\tilde x, v))'_v \oplus g_{\tilde\tau}(\tilde x, 0) \oplus g_{\tilde\tau}(\tilde x, 0)) =$$

$$= \sum_{\tilde\sigma \in E^n} \Big(\sum_{\tilde\tau \in E^n} \beta_{\tilde\sigma\tilde\tau} \cdot (g_{\tilde\tau}(\tilde x, v))'_v \Big) \cdot f(\tilde\sigma, \tilde y) =$$

$$= \sum_{\tilde\sigma \in E^n} x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} \cdot f(\tilde\sigma, \tilde y) = f(\tilde x, \tilde y).$$

Равенство

$$\sum_{\tilde{\tau}\in E^n} \beta_{\tilde{\sigma}\tilde{\tau}} \cdot (g_{\tilde{\tau}}(\tilde{x}, v))'_v = x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m}$$

имеет место, согласно выбору матрицы $[\beta_{\tilde{\sigma}\tilde{\tau}}]$. □

Следующее разложение позволило упростить вид — избавиться от слагаемого $g_{\tilde{\tau}}(\tilde{x}, 0)$. Однако вычисление обратной матрицы остается.

Напомним, что функция называется невырожденной, если производная этой функции по всем существенным переменным отлична от нулевой функции. Единичная функция считается невырожденной.

Теорема 3.13. *Пусть $\{g_{\tilde{\tau}}(\tilde{x}, v)\}$ — система булевых функций, причем существенными переменными функции $g_{\tilde{\tau}}(\tilde{x}, v)$ являются v и только те x_i, которым соответствует $\tau_i = 1$. Любая булева функция $f(\tilde{x}, \tilde{y})$ имеет разложение вида*

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma}\in E^n} \sum_{\tilde{\tau}\in E^n} \beta_{\tilde{\sigma}\tilde{\tau}} g_{\tilde{\tau}}(\tilde{x}, f^{\gamma}(\tilde{\sigma}, \tilde{y}))$$

тогда и только тогда, когда все функции системы невырожденные. Здесь $[\beta_{\sigma\tau}]^t = [\alpha_{\tilde{\sigma}\tilde{\tau}}]^{-1}$, где $\alpha_{\tilde{\sigma}\tilde{\tau}} = s_{\tilde{x}}^{\tilde{\sigma}}[(g_{\tilde{\tau}}(\tilde{x}, v))'_v]$, $\gamma = \mathrm{d}_{\tilde{x}} g_{\tilde{0}}(\tilde{x}, 1)$.

Доказательство. Определение матрицы $[\beta_{\tilde{\sigma}\tilde{\tau}}]$ корректно в силу невырожденности матрицы $[\alpha_{\tilde{\sigma}\tilde{\tau}}]$. Доказательство невырожденности матрицы $[\alpha_{\tilde{\sigma}\tilde{\tau}}]$ основано на том, что произведение $[\alpha_{\tilde{\tau}\tilde{\sigma}}] \cdot [\alpha_{\tilde{\sigma}\tilde{\tau}}]$ есть нижняя треугольная матрица. Рассмотрим элемент этого произведения

$$\varepsilon_{\tilde{\delta}\tilde{\tau}} = \sum_{\tilde{\sigma}\in E^n} \alpha_{\tilde{\tau}\tilde{\sigma}} \cdot \alpha_{\tilde{\sigma}\tilde{\tau}} = \sum_{\tilde{\sigma}\in E^n} (g_{\tilde{\delta}}(\tilde{\sigma}, v))'_v \cdot (g_{\tilde{\tau}}(\tilde{\sigma}, v))'_v =$$

$$= \mathrm{d}_{\tilde{x}}^{\tilde{0}} \left((g_{\tilde{\delta}}(\tilde{x}, v))'_v \cdot (g_{\tilde{\tau}}(\tilde{x}, v))'_v \right).$$

При $\tilde{\delta} = \tilde{\tau}$ функции $(g_{\tilde{\delta}}(\tilde{\tilde{x}}, v))'_v$ и $(g_{\tilde{\tau}}(\tilde{x}, v))'_v$ не имеют общих существенных переменных, поэтому имеет место равенство

$$\varepsilon_{\tilde{\tau}\tilde{\tau}} = \mathrm{d}_{x'}^{\tilde{0}}(g_{\tilde{\sigma}}(\tilde{\tilde{x}}, v))'_v \cdot \mathrm{d}_{x''}^{\tilde{0}}(g_{\tilde{\tau}}(\tilde{x}, v))'_v,$$

где x' и x'' — наборы соответствующих существенных переменных. Для равенства $\varepsilon_{\tilde{\tau}\tilde{\tau}} = 1$ необходимо и достаточно, чтобы функция $(g_{\tilde{\tau}}(\tilde{x}, v))'_v$ была невырожденной. Пусть $\tilde{\delta} \neq \tilde{\tau}$ и в

этих наборах имеется хотя бы один номер i такой, что $\delta_i = 0$ и $\tau_i = 0$, тогда x_i — несущественная переменная и, следовательно, $\varepsilon_{\tilde{\delta}\tilde{\tau}} = 0$ как производная по несущественной переменной. Аналогично доказательству предыдущей теоремы преобразуем правую часть доказываемого равенства:

$$\sum_{\tilde{\sigma}\in E^n}\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}g_{\tilde{\tau}}(\tilde{x},f^\gamma(\tilde{\sigma},\tilde{y})) =$$

$$= \sum_{\tilde{\sigma}\in E^n}\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}(f^\gamma(\tilde{\sigma},\tilde{y})\cdot(g_{\tilde{\tau}}(\tilde{x},v))'_v \oplus g_{\tilde{\tau}}(\tilde{x},0)) =$$

$$= \sum_{\tilde{\sigma}\in E^n}\Big(\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}\cdot(g_{\tilde{\tau}}(\tilde{x},v))'_v\Big)\cdot f^\gamma(\tilde{\sigma},\tilde{y}) \oplus \sum_{\tilde{\sigma}\in E^n}\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}g_{\tilde{\tau}}(\tilde{x},0).$$

Равенство

$$\sum_{\tilde{\sigma}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}} = 1$$

выполняется тогда и только тогда, когда $\tilde{\tau} = \tilde{0}$ в силу того, что $[\beta_{\tilde{\sigma}\tilde{\tau}}]^t = [\alpha_{\tilde{\sigma}\tilde{\tau}}]^{-1}$ и $\alpha_{\tilde{\sigma}\tilde{0}} = (g_{\tilde{0}}(\tilde{\sigma},v))'_v = 1$. Поэтому выполняются равенства:

$$\sum_{\tilde{\sigma}\in E^n}\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}g_{\tilde{\tau}}(\tilde{x},0) = \sum_{\tilde{\sigma}\in E^n}\Big(\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}\Big)g_{\tilde{\tau}}(\tilde{x},0) =$$

$$= g_{\tilde{0}}(\tilde{x},0) = g_{\tilde{0}}(\tilde{x},1)\oplus 1 = \overline{\gamma}.$$

Продолжим преобразования правой части равенства:

$$\sum_{\tilde{\sigma}\in E^n}\Big(\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}\cdot(g_{\tilde{\tau}}(\tilde{x},v))'_v\Big)\cdot f^\gamma(\tilde{\sigma},\tilde{y}) \oplus \sum_{\tilde{\sigma}\in E^n}\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}g_{\tilde{\tau}}(\tilde{x},0) =$$

$$= \sum_{\tilde{\sigma}\in E^n}\Big(\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}\cdot(g_{\tilde{\tau}}(\tilde{x},v))'_v\Big)\cdot f^\gamma(\tilde{\sigma},\tilde{y})\oplus\overline{\gamma} =$$

$$= \sum_{\tilde{\sigma}\in E^n}\Big(\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}\cdot(g_{\tilde{\tau}}(\tilde{x},v))'_v\Big)\cdot f(\tilde{\sigma},\tilde{y}).$$

Согласно определению матрицы $[\beta_{\tilde{\sigma}\tilde{\tau}}]$ имеет место равенство

$$\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}\cdot(g_{\tilde{\tau}}(\tilde{x},v))'_v = x_1^{\sigma_1}\cdot\ldots\cdot x_m^{\sigma_m}.$$

Окончательно получаем

$$\sum_{\tilde{\sigma}\in E^n}\sum_{\tilde{\tau}\in E^n}\beta_{\tilde{\sigma}\tilde{\tau}}g_{\tilde{\tau}}(\tilde{x},f^\gamma(\tilde{\sigma},\tilde{y})) = \sum_{\tilde{\sigma}\in E^n}x_1^{\sigma_1}\cdot\ldots\cdot x_m^{\sigma_m}\cdot f(\tilde{\sigma},\tilde{y}) = f(\tilde{x},\tilde{y}).$$

В обратную сторону доказательство теоремы следует из существования невырожденных функций. Например, оператор повторной производной от нечетной функции дает невырожденные функции. □

§8. Общий вид операторных полиномиальных форм

Результаты предыдущих параграфов позволяют найти полиномиальные разложение по операторному пучку по части переменных. Представляют самостоятельный и не меньший интерес частные случаи таких разложений — разложения по всем переменным или канонические формы. Поскольку в канонических формах присутствуют только операторные образы, естественно ожидать, что такие разложения имеют более простой вид, а нахождение коэффициентов для них менее трудоемко.

С практической стороны необходимость исследования канонических форм основана на том, что только немногие функции реализованы в микросхемах, и для реализации любой функции необходимо иметь ее полные разложения по конкретным функциям.

Рассмотрим систему функций $\{\mathrm{a}^{\tilde{0}}g(\tilde{x}),\ldots,\mathrm{a}^{\tilde{1}}g(\tilde{x})\}$, порожденную нечетной функцией $g(\tilde{x})$ и базисным пучком $\mathrm{A}=(\mathrm{a}^{\tilde{0}},\ldots,\mathrm{a}^{\tilde{1}})$. Согласно определению базисного пучка, матрица

$$M_{\mathrm{A}g}=\begin{pmatrix}\mathrm{a}^{\tilde{0}}g(\tilde{x}) & \ldots & \mathrm{a}^{\tilde{1}}g(\tilde{x})\end{pmatrix}$$

— невырожденная. Здесь $\mathrm{a}^{\tilde{\tau}}g(\tilde{x})$ — столбцы матрицы. Тогда для $M_{\mathrm{A}g}$ существует обратная:

$$M^{-1}_{\mathrm{A}g}=\begin{pmatrix}\varphi_{\tilde{0}}(\tilde{x})\\ \ldots\\ \varphi_{\tilde{\tau}}(\tilde{x})\\ \ldots\\ \varphi_{\tilde{1}}(\tilde{x})\end{pmatrix},$$

здесь функции $\varphi_{\tilde{\tau}}(\tilde{x})$ — строки матрицы.

Теорема 3.14. *По любому базисному пучку* A, *любой нечетной функции* $g(\tilde{x})$ *любая функция* $f(\tilde{x})$ *имеет единственное*

представление вида:

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \cdot \mathrm{a}^{\tilde{\tau}} g(\tilde{x}), \tag{3.20}$$

где $\alpha_{\tilde{\tau}} = \mathrm{d}_{\tilde{x}}[\varphi_{\tilde{\tau}}(\tilde{x}) \cdot f(\tilde{x})]$ *и* $\varphi_{\tilde{\tau}}(\tilde{x})$ *— строки матрицы* $M^{-1}_{\mathbf{A}_g}$.

Доказательство существования таких канонических форм следует из того, что система функций $\{\mathrm{a}^{\tilde{0}} g(\tilde{x}), \ldots, \mathrm{a}^{\tilde{1}} g(\tilde{x})\}$ является базисом, согласно определению базисного пучка операторов.

Для нахождения формулы коэффициентов рассмотрим разложение (3.20) в матричной форме записи:

$$\left(\mathrm{a}^{\tilde{0}} g(\tilde{x}) \quad \ldots \quad \mathrm{a}^{\tilde{1}} g(\tilde{x}) \right) \cdot \begin{pmatrix} \alpha_{\tilde{0}} \\ \ldots \\ \alpha_{\tilde{1}} \end{pmatrix} = \begin{pmatrix} f(\tilde{0}) \\ \ldots \\ f(\tilde{1}) \end{pmatrix}$$

или более коротко

$$M_{\mathbf{A}g} \cdot M_\alpha = M_f,$$

где M_α — вектор коэффициентов разложения и M_f — вектор функции $f(\tilde{x})$.

Умножим обе части равенства на $M^{-1}_{\mathbf{A}_g}$:

$$M^{-1}_{\mathbf{A}_g} \cdot M_{\mathbf{A}g} \cdot M_\alpha = M^{-1}_{\mathbf{A}_g} \cdot M_f.$$

Теперь получается формула вычисления коэффициентов:

$$\alpha_{\tilde{\tau}} = \sum_{\tilde{\sigma} \in E^n} \varphi_{\tilde{\tau}}(\tilde{\sigma}) \cdot f(\tilde{\sigma}) = \mathrm{d}_{\tilde{x}}[\varphi_{\tilde{\tau}}(\tilde{x}) \cdot f(\tilde{x})].$$

□

Эта достаточно простая теорема позволяет вводить различные классы полиномиальных канонических форм, используя два «параметра».

Первый параметр — *класс базисных пучков* операторов.

Рассмотрим соотношения полиномиальных канонических форм, приведенных в первом параграфе этого раздела, и операторных канонических форм. Все ПНФ могут быть изображены в виде:

$$P = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \cdot K^{\tilde{\tau}},$$

где $K^{\tilde{\tau}}$ — некоторые элементарные конъюнкции.

Элементарная конъюнкция имеет вид $K = x_{i_1}^{\sigma_1} \cdot \ldots \cdot x_{i_s}^{\sigma_s}$. Построим оператор $\mathfrak{a} = \mathfrak{a}_1 \ldots \mathfrak{a}_n$:

$$\mathfrak{a}_i = \begin{cases} \mathrm{d}, & \text{если } i \notin \{i_1, \ldots, i_s\}, \\ \mathrm{e}, & \text{если } i \in \{i_1, \ldots, i_s\} \text{ и } \sigma_i = 1, \\ \mathrm{p}, & \text{если } i \in \{i_1, \ldots, i_s\} \text{ и } \sigma_i = 0. \end{cases}$$

Согласно построению оператора $\mathfrak{a}$ имеем отображение:

$$\mathfrak{a}(x_1 \cdot \ldots \cdot x_n) = x_{i_1}^{\sigma_1} \cdot \ldots \cdot x_{i_s}^{\sigma_s} = K.$$

Таким образом, для любой элементарной конъюнкции $K^{\tilde{\tau}}$, входящей в качестве слагаемого в полином P, можно построить оператор $\mathfrak{a}^{\tilde{\tau}}$ такой, что

$$K^{\tilde{\tau}} = \mathfrak{a}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n).$$

Пусть $\mathsf{A} = (\mathfrak{a}^{\tilde{0}}, \ldots, \mathfrak{a}^{\tilde{\tau}}, \ldots, \mathfrak{a}^{\tilde{1}})$ — пучок операторов, такой, что его операторные образы по конъюнкции дают конъюнкции из P. Очевидно, что этот пучок — базисный, поскольку по условию полином P является канонической формой, следовательно слагаемые-функции, входящие в него, образуют базис.

Следствие. *Если имеется каноническая ПНФ или класс канонических ПНФ, тогда можно построить базисный пучок или класс базисных пучков операторов так, что данные канонические ПНФ являются операторными полиномиальными формами от образов функции $x_1 \cdot \ldots \cdot x_n$ по построенным базисным пучкам.*

Итак, все приведенные формы: полином Жегалкина, формы Рида–Маллера, кронекеровские формы и т.д, являются по сути некоторыми классами операторных полиномиальных форм. Операторная классификация полиномов оказывается более широкой по сравнению с традиционными. Причем с операторной точки зрения зачастую нет резона различать традиционные классы, и наоборот, появляется обоснованная необходимость вводить новые. Для примера, формы Рида–Маллера и кронекеровские формы ведут себя одинаково относительно сложности реализации ими класса всех булевых функций, а также имеют одни и те же алгоритмы вычисления коэффициентов форм. Другой пример — канонические формы по диагональным операторным пучкам. По сравнению с кронекеровскими формами реализации в диагональных имеют меньшую сложность и одинаковые

алгоритмы вычисления коэффициентов. Однако этот класс полиномиальных канонических форм до введения операторов не был известен, а был введен и изучался, например, класс псевдокронекеровских форм, имеющих одинаковую с диагональными сложность и значительно более сложные алгоритмы вычисления коэффициентов.

Второй параметр — *функция*, операторные образы которой определяют базис класса канонических форм. Зафиксировав класс базисных операторов, можно рассматривать классы операторных форм относительно какой-либо функции или класса функций. Теорема 3.14 позволяет сделать выбор функции или класса функций из множества 2^{2^n-1} функций. А именно столько существует нечетных функций от n переменных. Такая постановка вопроса о построении классов канонических форм стала возможной благодаря использованию операторного подхода.

§ 9. Классы операторных форм

Результаты предыдущего параграфа дают принципиальную возможность нахождения канонических форм по любым базисным пучкам операторов. Однако для этого необходимо знать обратную матрицу к матрице операторного пучка по нечетной функции, которая и порождает базисную систему функций. А сложность нахождения такой матрицы растет экспоненциально относительно числа аргументов функции. Отсюда естественно возникает вопрос о существовании базисных пучков, для которых коэффициенты разложения можно вычислять без нахождения обратной матрицы.

Однородные операторные пучки.

Следующая теорема вводит класс канонических форм по однородным операторным пучкам на нечетных функциях.

Теорема 3.15. *По любому однородному пучку операторов* $\mathrm{B} = (\mathrm{b}^{\tilde{0}}, \ldots, \mathrm{b}^{\tilde{1}})$, *по любой нечетной функции* $g(\tilde{x})$, *любая функция* $f(\tilde{x})$ *имеет единственное представление вида*

$$f(\tilde{x}) = \sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\sigma}} \mathrm{b}^{\tilde{\sigma}} g(\tilde{x}), \text{ где } \beta_{\tilde{\sigma}} = \mathrm{d}_{\tilde{x}} \left[\mathrm{b}^{\overline{\tilde{\sigma}}} g(\overline{\tilde{x}}) \cdot f(\tilde{x}) \right].$$

Доказательство. В доказательстве теоремы 3.1 имеется соотношение:

$$\begin{pmatrix} \mathfrak{a}^{\tilde{1}} \circ \mathfrak{a}^{\tilde{0}} & \dots & \mathfrak{a}^{\tilde{1}} \circ \mathfrak{a}^{\tilde{1}} \\ \vdots & \ddots & \vdots \\ \mathfrak{a}^{\tilde{0}} \circ \mathfrak{a}^{\tilde{0}} & \dots & \mathfrak{a}^{\tilde{0}} \circ \mathfrak{a}^{\tilde{1}} \end{pmatrix} \begin{pmatrix} \beta_{\tilde{0}} \\ \vdots \\ \beta_{\tilde{1}} \end{pmatrix} = \begin{pmatrix} \mathfrak{a}^{\tilde{1}} g(\bar{\tilde{x}}) \\ \vdots \\ \mathfrak{a}^{\tilde{0}} g(\bar{\tilde{x}}) \end{pmatrix} f.$$

Для любой функции f это равенство будет иметь место тогда и только тогда, когда $M_{\mathfrak{A}}$ — невырожденная матрица.

Пусть $M_{\mathfrak{A}}$ — матрица однородного операторного пучка $\mathfrak{A}$. Очевидно, что выполняется равенство

$$\mathfrak{a}^{\bar{\tilde{\tau}}} \circ \mathfrak{a}^{\tilde{\tau}} = 1.$$

Рассмотрим $\mathfrak{a}^{\tilde{\delta}} \circ \mathfrak{a}^{\tilde{\tau}}$. Очевидно, что если $\tilde{\delta} \neq \bar{\tilde{\tau}}$, то существует i такое, что либо $\delta_i = \tau_i = 0$, либо $\delta_i = \tau_i = 1$. Таким образом матрица однородного операторного пучка $\mathfrak{a}$ является единичной:

$$M_{\mathfrak{A}} = E_{2^n}.$$

Отсюда получаем, что все однородные операторные пучки являются базисными и, следовательно, указанная каноническая форма всегда существует.

Из равенства матрицы однородного операторного пучка единичной матрице также легко получается и формула для вычисления коэффициентов соответствующего представления:

$$\beta_{\tilde{\tau}} = \sum_{\tilde{\sigma} \in E^n} \mathfrak{b}^{\bar{\tilde{\tau}}} g(\bar{\tilde{\sigma}}) \cdot f(\tilde{\sigma}) = \mathrm{d}_{\tilde{x}} \left[\mathfrak{b}^{\bar{\tilde{\tau}}} g(\bar{\tilde{x}}) \cdot f(\tilde{x}) \right]. \qquad \square$$

Несмотря на простоту определения однородных операторных пучков, теорема позволяет ввести широкий класс канонических форм булевых функций.

Для примера рассмотрим несколько операторных канонических форм, причем базисная система функций построена по конъюнкции $g(x_1, \dots, x_n) = x_1 \cdot \ldots \cdot x_n$. Согласно определению, однородный операторный пучок представлен двумя порождающими операторами.

1) операторный пучок — $(e \dots e,\ \dots,\ \mathrm{d} \dots \mathrm{d})$, базисная система функций — $\{x_1 \cdot \ldots \cdot x_n,\ x_1 \cdot \ldots \cdot x_{n-1},\ \dots,\ 1\}$ — полином Жегалкина;

2) операторный пучок — $(e\ldots e, \ldots, p\ldots p)$, базисная система функций — $\{x_1\cdot\ldots\cdot x_n,\ x_1\cdot\ldots\cdot x_{n-1}\cdot\bar{x}_n,\ \ldots,\ \bar{x}_1\cdot\ldots\cdot\bar{x}_n\}$ — совершенная полиномиальная нормальная форма;

3) операторный пучок — $(d\ldots d, \ldots, a_1\ldots a_n)$, в котором $a_i\in\{p,e\}$, базисная система функций — $(1,\ x_n^{v_n},\ \ldots,\ x_1^{v_1}\cdot\ldots\cdot x_n^{v_n})$ — поляризованный полином Жегалкина (форма Рида–Маллера) или HPE-форма;

4) операторный пучок — $(e\ldots e, \ldots, a_1\ldots a_n)$, в котором $a_i\in\{p,d\}$, базисная система функций — $\{x_1\cdot\ldots\cdot x_n,\ x_1\cdot\ldots\cdot x_{n-1}\cdot a_nx_n,\ \ldots,\ a_1x_1\cdot\ldots\cdot a_nx_n\}$ — HPD-форма;

5) операторный пучок — $(p\ldots p, \ldots, a_1\ldots a_n)$, в котором $a_i\in\{e,d\}$, базисная система функций — $\{\bar{x}_1\cdot\ldots\cdot\bar{x}_n,\ \bar{x}_1\cdot\ldots\cdot\bar{x}_{n-1}\cdot a_nx_n,\ \ldots,\ a_1x_1\cdot\ldots\cdot a_nx_n\}$ — HDE-форма;

6) операторный пучок — $(b_1\ldots b_n, \ldots, a_1\ldots a_n)$, в котором $a_i\in\{e,d\}$, $b_i\in\{p,d\}$, базисная система функций — $\{b_1x_1\cdot\ldots\cdot b_nx_n,\ b_1x_1\cdot\ldots\cdot b_{n-1}x_{n-1}\cdot a_nx_n,\ \ldots,\ a_1x_1\cdot\ldots\cdot a_nx_n\}$ — кронекеровская каноническая форма.

Однопорожденные операторные пучки.

Следующая теорема вводит класс канонических форм по неоднородным операторным пучкам.

Теорема 3.16. *По любому неоднородному пучку операторов* $\mathsf{A}=(a^{\tilde{0}},\ldots,a^{\tilde{1}})$, *по любой нечетной функции* $g(\tilde{x})$ *любая функция* $f(\tilde{x})$ *имеет единственное представление вида*

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

где $\alpha_{\tilde{\sigma}}=\sum\limits_{\tilde{\tau}\in V}\alpha_{\tilde{\sigma}}^{\tilde{\tau}}$ $(V=\{\tilde{\tau}|\tilde{\tau}\in E^n$ *и* $\tilde{\sigma}\leqslant\tilde{\tau}\})$, $\alpha_{\tilde{\sigma}}^{\tilde{\tau}}$ — *коэффициенты разложений операторов* $b^{\tilde{\tau}}=\sum\limits_{\tilde{\delta}\in V'}\alpha_{\tilde{\delta}}^{\tilde{\tau}}a^{\tilde{\delta}}$ $(V'=\{\tilde{\delta}|\tilde{\delta}\in E^n$ *и* $\tilde{\delta}\leqslant\tilde{\tau}\})$ *операторного пучка* $\mathsf{B}=(b^{\tilde{0}},\ldots,b^{\tilde{1}})$, *сопутствующего к* A, *причем только для таких* $\tilde{\tau}$, *для которых выполняется равенство*:

$$d_{\tilde{x}}\left[b^{\bar{\tilde{\tau}}}g(\bar{\tilde{x}})\cdot f(\tilde{x})\right]=1.$$

Доказательство. Пусть A — однопорожденный пучок операторов. По критерию существования базисного пучка A достаточно показать невырожденность матрицы пучка M_{A}.

Рассмотрим главную диагональ матрицы M_{A}, где A — однопорожденный пучок операторов. Элементы диагонали имеют представление:

$$m_{\tilde{\tau}\tilde{\tau}} = \mathsf{a}^{\bar{\tilde{\tau}}} \circ \mathsf{a}^{\tilde{\tau}}.$$

По определению однопорожденного пучка операторов существует оператор $\mathsf{b} = \mathsf{b}_1 \ldots \mathsf{b}_n$ такой, что любой оператор $\mathsf{a}^{\tilde{\tau}} = \mathsf{t}_1 \ldots \mathsf{t}_n$ из пучка операторов A имеет структуру:

$$\begin{cases} \mathsf{t}_i = \mathsf{b}_i, & \text{если } \tau_i = 0, \\ \mathsf{t}_i \neq \mathsf{b}_i, & \text{если } \tau_i = 1. \end{cases}$$

Отсюда следует, что для любого $i \in \{1, \ldots, n\}$ выполняется $\mathsf{a}_i^{\tilde{\tau}} \neq \mathsf{a}_i^{\bar{\tilde{\tau}}}$. По определению функционала "$\circ$":

$$m_{\tilde{\tau}\tilde{\tau}} = \mathsf{a}^{\bar{\tilde{\tau}}} \circ \mathsf{a}^{\tilde{\tau}} = 1.$$

Далее необходимо рассмотреть элементы матрицы M_{A}, стоящие под главной диагональю. Для них выполняется условие $\tilde{\sigma} > \tilde{\tau}$.

Пусть $\tilde{\tau} = (\tau_1, \ldots, \tau_n)$ и $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$. Согласно интерпретации $\tilde{\tau}$ и $\tilde{\sigma}$ как чисел, число $\tilde{\sigma}$ больше числа $\tilde{\tau}$, если найдется i такое, что $\sigma_i = 1$ и $\tau_i = 0$ и для любых $j < i$ имеет место $\tau_j = \sigma_j$. Отсюда следует, что $\overline{\tau}_i = 0$. Поэтому $\mathsf{a}_i^{\bar{\tilde{\tau}}} = \mathsf{a}_i^{\tilde{\tau}}$, что окончательно дает $m_{\tilde{\sigma}\tilde{\tau}} = 0$ при $\tilde{\sigma} > \tilde{\tau}$.

Таким образом, любой однопорожденный пучок A имеет треугольную, а следовательно невырожденную, матрицу M_{A}. Значит любой однопорожденный пучок — базисный.

Очевидно, что коэффициенты канонической формы в случае разложения по однопорожденным пучкам операторов по некоторой функции $g(\tilde{x})$ могут быть найдены по теореме 3.14. Однако при этом должна быть найдена обратная матрица к матрице пучка по функции $g(\tilde{x})$. В случае однопорожденных пучков операторов коэффициенты канонических форм можно вычислить без нахождения соответствующей обратной матрицы.

Рассмотрим разложение $f(\tilde{x})$ по $\{\mathsf{b}^{\tilde{0}} g(\tilde{x}), \ldots, \mathsf{b}^{\tilde{1}} g(\tilde{x})\}$:

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\tau}} \cdot \mathsf{b}^{\tilde{\tau}} g(\tilde{x}). \tag{3.21}$$

По предложению 3.12 функция $\mathrm{b}^{\tilde{\tau}} g(\tilde{x})$ имеет разложение

$$\mathrm{b}^{\tilde{\tau}} g(\tilde{x}) = \sum_{\tilde{\sigma} \in V} \alpha_{\tilde{\sigma}}^{\tilde{\tau}} \mathrm{a}^{\tilde{\sigma}} g(\tilde{x}),$$

где $V = \{\tilde{\tau} | \tilde{\tau} \in E^n$ и $\tilde{\sigma} \leqslant \tilde{\tau}\}$.

Сделаем соответствующую подстановку в (3.21):

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \beta_{\tilde{\tau}} \cdot \sum_{\tilde{\sigma} \in V} \alpha_{\tilde{\sigma}}^{\tilde{\tau}} \cdot \mathrm{a}^{\tilde{\sigma}} g(\tilde{x}) =$$

$$= \sum_{\tilde{\sigma} \in E^n} \Big(\sum_{\tilde{\tau} \in V'} \beta_{\tilde{\tau}} \cdot \alpha_{\tilde{\sigma}}^{\tilde{\tau}} \Big) \cdot \mathrm{a}^{\tilde{\sigma}} g(\tilde{x}) = \sum_{\tilde{\sigma} \in E^n} \alpha_{\tilde{\sigma}} \cdot \mathrm{a}^{\tilde{\sigma}} g(\tilde{x}),$$

где $V = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $\tilde{\sigma} \leqslant \tilde{\tau}\}$, $V' = \{\tilde{\tau} | \tilde{\tau} \in E^n$ и $\tilde{\sigma} \leqslant \tilde{\tau}\}$.

Очевидно, что в разложении функции $f(\tilde{x})$ присутствуют только те слагаемые, для которых $\beta_{\tilde{\tau}} = 1$. По теореме 3.14 это имеет место тогда и только тогда, когда

$$\mathrm{d}_{\tilde{x}} \left[\mathrm{b}^{\tilde{\tau}} g(\tilde{x}) \cdot f(\tilde{x}) \right] = 1. \qquad \square$$

Очевидно, что класс канонических форм по неоднородным операторным пучкам включает в себя класс канонических форм по однородным операторным пучкам.

Расширенные формы по однородным операторным пучкам.

Пусть $\mathrm{A} = (\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{1}})$ — однородный операторный пучок. Рассмотрим систему операторов

$$S = \{\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{\tau}}, \ldots, \mathrm{a}^{\tilde{1}}, \mathrm{b}\},$$

где оператор $\mathrm{b} = \mathrm{b}_1 \ldots \mathrm{b}_n$ такой, что $\mathrm{b}_i \neq \mathrm{a}_i^{\tilde{0}}$ и $\mathrm{b}_i \neq \mathrm{a}_i^{\tilde{1}}$ для любого i. По предложению 3.10 такой оператор всегда существует для однородных пучков.

Теорема 3.17. *По пучку операторов* $\mathsf{T} = (\mathrm{t}^{\tilde{0}}, \ldots, \mathrm{t}^{\tilde{1}})$, *где* $\mathrm{t}^{\tilde{\tau}} \in S = \{\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{\tau}}, \ldots, \mathrm{a}^{\tilde{1}}, \mathrm{b}\}$ *и* $\mathrm{t}^{\tilde{\sigma}} \neq \mathrm{t}^{\tilde{\tau}}$ *при* $\tilde{\sigma} \neq \tilde{\tau}$, *по любой нечетной функции* $g(\tilde{x})$ *любая функция* $f(\tilde{x})$ *имеет единственное представление вида*

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \mathrm{t}^{\tilde{\tau}} g(\tilde{x}),$$

где

$$\alpha_{\tilde{\tau}} = \begin{cases} \mathrm{d}_{\tilde{x}}[\mathrm{t}^{\overline{\tilde{\tau}}} g(\overline{\tilde{x}}) \cdot f(\tilde{x})], & \text{если оператор } \mathrm{b} \text{ не входит в } \mathsf{T}, \\ \mathrm{d}_{\tilde{x}}[\mathrm{t}^{\overline{\tilde{\tau}}} g(\overline{\tilde{x}}) \cdot f(\tilde{x}) \oplus \mathrm{t}^{\tilde{\sigma}} g(\overline{\tilde{x}}) \cdot f(\tilde{x})], & \text{если } \mathrm{t}^{\tilde{\sigma}} = \mathrm{b} \text{ и } \tilde{\sigma} \neq \tilde{\tau}, \\ \mathrm{d}_{\tilde{x}}[\mathrm{t}^{\overline{\tilde{\tau}}} g(\overline{\tilde{x}}) \cdot f(\tilde{x})], & \text{если } \mathrm{t}^{\tilde{\sigma}} = \mathrm{b} \text{ и } \tilde{\sigma} = \tilde{\tau}. \end{cases}$$

Доказательство. Пусть T — пучок операторов, построенный так, что операторы в этом пучке имеют тот же порядок, что и в системе S. Пусть оператор b в пучке T имеет номер $\tilde{\tau}$.

Докажем, что T — базисный пучок. Пусть существуют $\tilde{\tau}^1, \ldots, \tilde{\tau}^k$ такие, что

$$\mathrm{t}^{\tilde{\tau}^1} g(\tilde{x}) \oplus \cdots \oplus \mathrm{t}^{\tilde{\tau}^k} g(\tilde{x}) = 0. \tag{3.22}$$

В случае $\mathrm{t}^{\tilde{\tau}^i} \neq \mathrm{b}$ для любого i получаем противоречие, поскольку получаем сумму базисных функций, равную нулю.

Пусть $\mathrm{t}^{\tilde{\tau}^i} = \mathrm{b}$ и $i = 1$ — для упрощения записи. В этом случае имеем представление:

$$\mathrm{b} g(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \mathrm{a}^{\tilde{\tau}} g(\tilde{x}).$$

В (3.22) сделаем замену и сокращения:

$$\Big(\sum_{\tilde{\tau} \in E^n} \mathrm{a}^{\tilde{\tau}} g(\tilde{x}) \Big) \oplus \mathrm{a}^{\tilde{\tau}^2} g(\tilde{x}) \oplus \cdots \oplus \mathrm{a}^{\tilde{\tau}^k} g(\tilde{x}) = \sum_{\tilde{\tau} \in V} \mathrm{a}^{\tilde{\tau}} g(\tilde{x}) = 0,$$

где $V = E^n \backslash \{\tilde{\tau}^2, \ldots, \tilde{\tau}^k\}$.

Снова получено противоречие: сумма базисных функций равна нулю. Таким образом, T — базисный пучок.

Для нахождения формул вычисления коэффициентов канонической формы рассмотрим матрицу A_{T} операторного пучка T. Она имеет следующий вид:

$$A_{\mathsf{T}} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & \cdots & 1 & a_{\tilde{\tau}\tilde{\tau}} = 0 & 1 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

На главной диагонали стоят единицы, кроме $a_{\tilde{\tau}\tilde{\tau}} = 0$; остальные элементы строки и столбца с номером $\tilde{\tau}$ равны 1. Все остальные элементы матрицы нулевые. Такой вид матрицы A_{T} следует из определения функционала "$\circ$".

Оператор b определен так, что $\mathrm{a}^{\tilde{0}} \circ \mathrm{b} = 1$ и $\mathrm{a}^{\tilde{1}} \circ \mathrm{b} = 1$, откуда следует, что для любого $\tilde{\tau}$ и для любого i выполняется $\mathrm{a}_i^{\tilde{\tau}} \neq \mathrm{b}_i$, что влечет для любого $\tilde{\tau}$ выполнение равенства $\mathrm{a}^{\tilde{\tau}} \circ \mathrm{b} = 1$.

Итак, имеем равенство

$$A_{\mathsf{T}} \cdot \begin{pmatrix} \alpha_{\tilde{0}} \\ \vdots \\ \alpha_{\tilde{\tau}} \\ \vdots \\ \alpha_{\tilde{1}} \end{pmatrix} = \begin{pmatrix} \mathrm{d}_{\tilde{x}}[\mathrm{a}^{\tilde{1}} g(\bar{\tilde{x}}) \cdot f(\tilde{x})] \\ \vdots \\ \mathrm{d}_{\tilde{x}}[\mathrm{b} g(\bar{\tilde{x}}) \cdot f(\tilde{x})] \\ \vdots \\ \mathrm{d}_{\tilde{x}}[\mathrm{a}^{\tilde{0}} g(\bar{\tilde{x}}) \cdot f(\tilde{x})] \end{pmatrix}. \tag{3.23}$$

Теперь достаточно линейным преобразованием строк матрицу A_{T} привести к диагональному виду, одновременно преобразуя столбец в правой части равенства (3.23).

Сложив все строки со строкой $\overline{\tilde{\tau}}$ получим, что теперь $\alpha_{\overline{\tilde{\tau}}\tilde{\tau}} = 1$ и $\alpha_{\overline{\tilde{\tau}}\overline{\tilde{\tau}}} = 1$, остальные элементы $\alpha_{\overline{\tilde{\tau}}\tilde{\sigma}}$ определяются так:

$$\alpha_{\overline{\tilde{\tau}}\tilde{\sigma}} = \begin{cases} 1, & \text{если } \tilde{\sigma} = \tilde{\tau} \text{ или } \tilde{\sigma} = \overline{\tilde{\tau}}, \\ 0, & \text{в противном случае.} \end{cases}$$

Одновременно элемент $v_{\overline{\tilde{\tau}}}$ столбца в правой части (3.23) примет вид

$$v_{\overline{\tilde{\tau}}} = \mathrm{d}_{\tilde{x}}\left[\mathrm{b} g(\bar{\tilde{x}}) \cdot f(\tilde{x})\right] \oplus \sum_{\tilde{\sigma} \in E^n \setminus \{\tilde{\tau}\}} \mathrm{d}_{\tilde{x}}\left[\mathrm{a}^{\tilde{\sigma}} g(\bar{\tilde{x}}) \cdot f(\tilde{x})\right] =$$

$$= \sum_{\tilde{\sigma}\in E^n} \mathrm{d}_{\tilde{x}}\left[\mathrm{a}^{\tilde{\sigma}} g(\tilde{\overline{x}})\cdot f(\tilde{x})\right] \oplus \sum_{\tilde{\sigma}\in E^n\setminus\{\tilde{\overline{\tau}}\}} \mathrm{d}_{\tilde{x}}\left[\mathrm{a}^{\tilde{\sigma}} g(\tilde{\overline{x}})\cdot f(\tilde{x})\right] =$$

$$= \mathrm{d}_{\tilde{x}}\left[\mathrm{a}^{\tilde{\overline{\tau}}} g(\tilde{\overline{x}})\cdot f(\tilde{x})\right].$$

Легко заметить, что в строке с номером $\tilde{\tau}$ имеет место

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

Линейные преобразования, соответствующие прибавлению ко всем строкам строки с номером $\tilde{\tau}$ приводят к диагональной матрице. Соответствующие преобразования окончательно приводят элемент $v_{\tilde{\sigma}}$ столбца в правой части (3.23) к виду

$$v_{\tilde{\sigma}} = \begin{cases} \mathrm{d}_{\tilde{x}}[\mathrm{a}^{\tilde{\overline{\sigma}}} g(\tilde{\overline{x}})\cdot f(\tilde{x}) \oplus \mathrm{a}^{\tilde{\tau}} g(\tilde{\overline{\tau}})\cdot f(\tilde{x})], & \text{если } \tilde{\sigma} \neq \tilde{\tau}, \\ \mathrm{d}_{\tilde{x}}[\mathrm{a}^{\tilde{\overline{\sigma}}} g(\tilde{\overline{x}})\cdot f(\tilde{x})], & \text{если } \tilde{\sigma} = \tilde{\tau}. \end{cases}$$

Откуда следует формула для коэффициентов разложения однородной формы. □

Операторные формы по однородно смешанным пучкам.

Следующая теорема вводит класс канонических форм по однородно смешанным пучкам. Для этого класса коэффициенты представлений функций находятся при помощи матрицы.

Теорема 3.18. *По любому однородно смешанному пучку* A, *любой нечетной функции* $g(\tilde{x})$ *любая функция* $f(\tilde{x})$ *имеет единственное представление вида*:

$$f(\tilde{x}) = \sum_{\tilde{\tau}\in E^n} \alpha_{\tilde{\tau}}\cdot \mathrm{a}^{\tilde{\tau}} g(\tilde{x}),$$

где коэффициенты $\alpha_{\tilde{\tau}}$ *вычисляются по теореме* 3.14.

Доказательство. Существование этого класса канонических форм следует из невырожденности матрицы такого пучка. Невырожденность гарантирует предложение 3.13. Теорема 3.14 дает универсальный метод вычисления коэффициентов. □

Операторные формы по диагональным пучкам.

Следующая теорема определяет класс диагональных канонических форм.

Теорема 3.19. *По любому диагональному пучку операторов* $\mathrm{B} = (\mathrm{b}^{\tilde{0}}, \ldots, \mathrm{b}^{\tilde{1}})$, *по любой нечетной функции* $g(\tilde{x})$, *любая функция* $f(\tilde{x})$ *имеет единственное представление вида*

$$f(\tilde{x}) = \sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\sigma}} \mathrm{b}^{\tilde{\sigma}} g(\tilde{x}), \tag{3.24}$$

где

$$\beta_{\tilde{\sigma}} = \mathrm{d}_{\tilde{x}} \left[\mathrm{b}^{\overline{\tilde{\sigma}}} g(\overline{\tilde{x}}) \cdot f(\tilde{x}) \right].$$

Доказательство. Базисность пучков этого класса непосредственно следует из определения диагонального пучка.

По определению диагонального операторного пучка его матрица совпадает с единичной. Формула вычисления коэффициентов получается полностью аналогично формам по однородным пучкам:

$$\beta_{\tilde{\tau}} = \sum_{\tilde{\sigma} \in E^n} \mathrm{s}_{\tilde{x}}^{\tilde{\sigma}} \left(\mathrm{b}^{\overline{\tilde{\tau}}} g(\overline{\tilde{x}}) \cdot f(\tilde{x}) \right) = \mathrm{d}_{\tilde{x}} \left[\mathrm{b}^{\overline{\tilde{\tau}}} g(\overline{\tilde{x}}) \cdot f(\tilde{x}) \right]. \qquad \square$$

Иерархия классов операторных форм.

Появление большого количества классов операторных форм естественно приводит к необходимости их систематизации.

На рисунке приведена структура классов базисных пучков операторов. Классы расположены по включению снизу-вверх. Естественно, что далеко не все классы отображены на диаграмме. Выбор осуществлен по нескольким критериям. Первый критерий — это определение данного класса, которое должно быть "простым", не использующим перебор всех пучков класса. Второй критерий — для данного класса удалось решить, хотя бы частично, вопросы сложности канонических форм. Третий критерий — класс операторных форм по данным пучкам по функции конъюнкции включает известные классы нормальных полиномиальных форм.

Диаграмма имеет следующее строение.

Первый уровень — классы операторных форм, полученные по одному пучку операторов.

Группа классов HPE-HPD-HDE-H — однородные операторные формы,

H — все однородные;

HPE — порожденные операторными пучками вида

$$\{\mathrm{d}\ldots\mathrm{d}\ ,\ldots,\ a_1\ldots a_n\},\ \text{где}\ a_i\in\{\mathrm{p},e\};$$

HPD — порожденные операторными пучками вида

$$\{e\ldots e\ ,\ldots,\ a_1\ldots a_n\},\ \text{где}\ a_i\in\{\mathrm{p},\mathrm{d}\};$$

HDE — порожденные операторными пучками вида

$$\{\mathrm{p}\ldots\mathrm{p}\ ,\ldots,\ a_1\ldots a_n\},\ \text{где}\ a_i\in\{\mathrm{d},e\}.$$

Группа классов NPE-NPD-NDE-N — однопорожденные операторные формы,

N — все однопорожденные;

NPE — порожденные операторными пучками вида

$$\{\mathrm{d}\ldots\mathrm{d}\};$$

NPD — порожденные операторными пучками вида

$$\{e\ldots e\};$$

NDE — порожденные операторными пучками вида

$$\{\mathrm{p}\ldots\mathrm{p}\}.$$

Группа классов ExH_1-...-ExH_t-ExH — операторные формы по расширенным пучкам операторов;

ExH — все операторные формы по расширенным пучкам операторов;

ExH_i — подкласс расширенных форм, порожденный одним однородным пучком операторов.

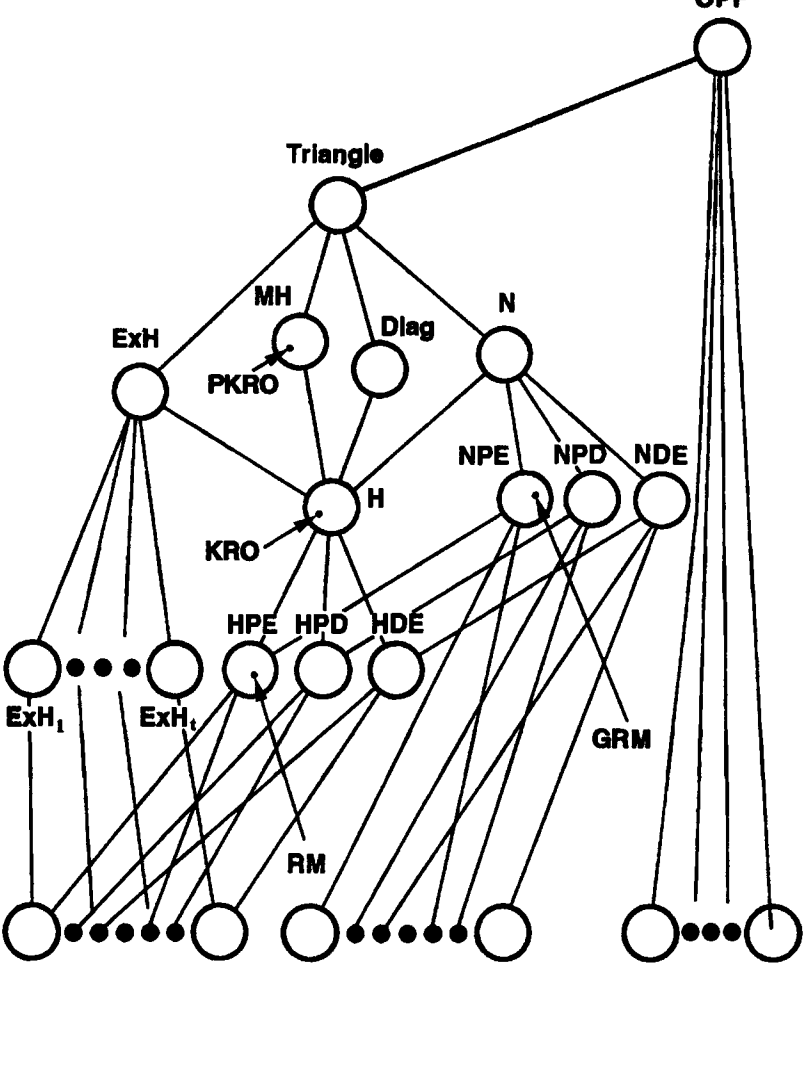
Triangle — операторные формы по пучкам, имеющим треугольные матрицы;

Diag — диагональные операторные формы;

MH — операторные формы по смешанным однородным пучкам;

OPF — класс всех операторных форм.

На диаграмме стрелками показано вхождение следующих известных классов полиномиальных канонических форм:



Структура классов операторных форм

RM — формы Рида–Маллера; KRO — кронекеровские формы; PKRO — псевдокронекеровские формы; GRM — обобщенные формы Рида–Маллера.

Относительно этой структуры можно вводить структуры операторных полиномиальных форм булевых функций. Если рассматриваются полиномиальные формы по образам единственной функции, то картина будет идентичной, за исключением нижнего яруса. На нем будут присутствовать классы операторных форм, содержащих только по одной канонической форме. Например, полином Жегалкина и совершенная полиномиальная нормальная форма лежат в нижнем ярусе.

При рассмотрении операторных форм по образам класса K нечетных функций, каждый узел будет содержать класс канонических форм. Более того, каждый узел может представлять собой структуру относительно подклассов из K.

Если рассмотреть данную диаграмму операторных форм по образам единственной функции — конъюнкции, то известные классы полиномиальных форм имеют следующие вхождения (на диаграмме их вхождения помечены стрелками):

— в классе HPE лежат все поляризованные полиномы Жегалкина;

— в классе H лежат все кронекеровские формы;

— в классе NPE лежат все обобщенные формы Рида–Маллера;

— в классе MH лежат все псевдокронекеровские формы.

Интересно заметить, что все приведенные полиномиальные формы включаются в операторные формы по треугольным пучкам.

Канонические формы по термам над бинарными функциями.

Очевидно, что канонические формы можно рассматривать как предельные случаи соответствующих разложений. Если в разложении участвуют все переменные, то остаточные функции становятся константами. Однако при таком подходе получения канонических форм возникают некоторые затруднения. Рассмотрим предельное разложение в теореме 3.11 для случая $\overset{*}{1}$:

$$f(x_1,\ldots,x_n)=\sum_{\sigma_1,\ldots,\sigma_n}\left(x_1^{\sigma_1}\mid\left(\ldots\left(x_n^{\sigma_n}\mid f(\sigma_1,\ldots,\sigma_n)\right)\ldots\right)\right).$$

При $f(\sigma_1,\dots,\sigma_n)=0$ соответствующее слагаемое примет вид:

$$x_1^{\sigma_1}\mid(\dots(x_n^{\sigma_n}\mid 0)\dots)=x_1^{\sigma_1}\mid(\dots(x_{n-2}^{\sigma_{n-2}}\mid \bar{x}_{n-1}^{\sigma_{n-1}})\dots).$$

Неполные слагаемые могут нарушить единственность представления. Достраивание таких слагаемых до полных весьма затруднительно ввиду специфической дистрибутивности из предложения 1.6. Однако с этой ситуацией удается справиться даже в более общем случае. Пусть $t(\tilde{x})$ — полный бесповторный терм над множеством бинарных функций $\{\cdot,\vee,|,\downarrow,\to,\leftrightarrow,\leftarrow,\nleftrightarrow\}$.

Теорема 3.20. *Любая булева функция $f(\tilde{x})$ по любому $t(\tilde{x})$ имеет единственное представление вида*

$$f(\tilde{x})=\sum_{\tilde{\tau}\in E^n}\alpha_{\tilde{\tau}}t(\tilde{x}^{\tilde{\tau}}),$$

где $\alpha_{\tilde{\tau}}=\mathrm{d}_{\tilde{x}}\left(t(\tilde{x}^{\tilde{\tau}})\cdot f(\tilde{x})\right)$.

Доказательство следует из теоремы 3.15. □

Очевидно, что $(\Delta_1,\dots,\Delta_n)$-разложения проводятся по полным бесповторным термам.

Еще один пример канонических форм — позитивные канонические полиномиальные формы.

Пусть $\tilde{\sigma}=(\sigma_1,\dots,\sigma_{n-1},\sigma_n)$.

Теорема 3.21. *Булева функция $f(x_1,\dots,x_n)$ имеет канонические формы вида*

$$f(x_1,\dots,x_n)=\sum_{\tilde{\sigma}\in E^n}\alpha_{\tilde{\sigma}}\left(x_1\Delta_{\sigma_1}\left(\dots(x_{n-1}\Delta_{\sigma_{n-1}}x_n)\right)\dots\right).$$

а) Если

$$\Delta_{\sigma_i}=\begin{cases}\cdot, & \text{если } \sigma_i=1,\\ \leftrightarrow, & \text{если } \sigma_i=0,\end{cases}\qquad i=1,\dots,n-2,$$

$$\Delta_{\sigma_{n-1}}=\begin{cases}\cdot, & \text{если } \sigma_{n-1}=\sigma_n=1,\\ \leftrightarrow, & \text{если } \sigma_{n-1}=1,\sigma_n=0,\\ \leftrightarrow, & \text{если } \sigma_{n-1}=0,\sigma_n=1,\\ \downarrow, & \text{если } \sigma_{n-1}=\sigma_n=0,\end{cases}$$

то $\alpha_{\tilde{\sigma}}=1$ тогда и только тогда, когда $f(\tilde{\sigma})=1$.

б) Если

$$\Delta_{\sigma_i} = \begin{cases} \to, & \text{если } \sigma_i = 1, \\ \vee, & \text{если } \sigma_i = 0, \end{cases} \qquad i = 1, \ldots, n-2,$$

$$\Delta_{\sigma_{n-1}} = \begin{cases} |, & \text{если } \sigma_{n-1} = \sigma_n = 1, \\ \to, & \text{если } \sigma_{n-1} = 1, \sigma_n = 0, \\ \leftarrow, & \text{если } \sigma_{n-1} = 0, \sigma_n = 1, \\ \vee, & \text{если } \sigma_{n-1} = \sigma_n = 0, \end{cases}$$

то $\alpha_{\tilde{\sigma}} = 1$ тогда и только тогда, когда $f(\tilde{\sigma}) = 0$, при условии $\mathrm{d}_{\tilde{x}} f(\tilde{x}) = 1$ и $\alpha_{\tilde{\sigma}} = 1$ тогда и только тогда, когда $f(\tilde{\sigma}) = 1$, при условии $\mathrm{d}_{\tilde{x}} f(\tilde{x}) = 0$.

Доказательство легко следует из предыдущей теоремы и следствия теоремы 3.11. Можно заметить, что в теореме приведен оригинальный метод нахождения коэффициентов, использующий специфику термов над бинарными функциями. □

§ 10. Сложность операторных форм

По любому базисному пучку A и любой нечетной функции $g(x_1, \ldots, x_n)$ для любой булевой функции $f(x_1, \ldots, x_n)$ существует единственное полиномиальное разложение:

$$f(x_1, \ldots, x_n) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \mathrm{a}^{\tilde{\tau}} g(x_1, \ldots, x_n) = P.$$

Сложностью $L_{\Pi\Phi}(P)$ этого полинома P будем называть число ненулевых коэффициентов $\alpha_{\tilde{\tau}}$.

Пусть K — произвольный класс базисных пучков, $g(x_1, \ldots, x_n)$ — некоторая нечетная функция. Функция Шеннона $L_K^g(f)$ оценки сложности булевой функции в классе K по функции $g(x_1, \ldots, x_n)$ определяется следующим образом:

$$L_K^g(f) = \min L_{\Pi\Phi}(P),$$

где минимум берется по всем полиномам, построенным по пучкам из K и функции g и представляющим булеву функцию $f(x_1, \ldots, x_n)$.

Функция Шеннона $L_K^g(S)$ оценки сложности класса S булевых функций размерности n в классе канонических форм по

пучкам из K по функции $g(x_1, \ldots, x_n)$ определяется следующим образом:

$$L_K^g(S) = \max L_K^g(f),$$

где максимум берется по всем булевым функциям из класса S.

В случае, когда класс S будет совпадать с классом всех функций от n переменных, для функции Шеннона используется обозначение: $L_K^g(n)$.

Аналогично определяется функция Шеннона для полиномиальных нормальных форм. Для одной функции:

$$L_{\text{ПНФ}}(f) = \min L(P),$$

где минимум берется по всем P — полиномиальным нормальным формам, представляющим булеву функцию $f(x_1, \ldots, x_n)$. Для класса всех булевых функций:

$$L_{\text{ПНФ}}(n) = \max L_{\text{ПНФ}}(f),$$

где максимум берется по всем булевым функциям $f(x_1, \ldots, x_n)$ размерности n.

Сложность в операторных формах по различным функциям.

Естественно, что сложность функции $L_K^g(f)$ зависит от выбора функции $g(x_1, \ldots, x_n)$.

Это показывает простой пример. Рассмотрим представление функции $f(x_1, \ldots, x_n) = \bar{x}_1 \cdot \ldots \cdot \bar{x}_n$ полиномом Жегалкина, т.е. класс состоит из одного однородного пучка ($e \ldots e$, $\ldots$, $d \ldots d$). Легко видеть, что выполняется равенство

$$\bar{x}_1 \cdot \ldots \cdot \bar{x}_n = 1 \oplus x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus x_1 x_2 \oplus \ldots \oplus x_1 \cdot \ldots \cdot x_n.$$

В сумме присутствуют все слагаемые, следовательно, имеет место:

$$L_K^{x_1 \cdot \ldots \cdot x_n}(\bar{x}_1 \cdot \ldots \cdot \bar{x}_n) = 2^n.$$

Теперь для той же самой функции построим представление над тем же классом пучков, но по функции $\bar{x}_1 \cdot \ldots \cdot \bar{x}_n$.

$$\bar{x}_1 \cdot \ldots \cdot \bar{x}_n = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \cdot \mathrm{d}_{\tilde{x}}^{\tilde{\tau}}(\bar{x}_1 \cdot \ldots \cdot \bar{x}_n).$$

При $\tilde{\tau} = \tilde{1}$ получаем

$$\mathrm{d}_{\tilde{x}}^{\tilde{1}}(\bar{x}_1 \cdot \ldots \cdot \bar{x}_n) = \bar{x}_1 \cdot \ldots \cdot \bar{x}_n.$$

Откуда следует, что $\alpha_{\tilde{1}} = 1$, остальные коэффициенты равны нулю. Следовательно в этом случае сложность равна 1:

$$L_K^{\bar{x}_1 \cdot \ldots \cdot \bar{x}_n}(\bar{x}_1 \cdot \ldots \cdot \bar{x}_n) = 1.$$

Интересно заметить, что не всегда $L_K^f(f) = 1$. На это есть две причины: во-первых, разложение существуют только по нечетным функциям; во-вторых, среди образов функции по пучку операторов может не оказаться самой функции, например в случае однородного пучка $(\mathrm{d}\ldots\mathrm{d}, \ldots, \mathrm{p}\ldots\mathrm{p})$.

В связи с изложенными замечаниями интересен вопрос о соотношении сложностей класса всех булевых функций в полиномах по разным функциям. Ответ на него дает следующая теорема.

Теорема 3.22. *Для любого класса K базисных пучков операторов значение функции Шеннона $L_K^g(n)$ не зависит от выбора функции $g(x_1, \ldots, x_n)$.*

Доказательство. Рассмотрим базисный пучок $\mathrm{A} = (\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{1}})$ операторов размерности n и две нечетные функции $g(x_1, \ldots, x_n)$, $h(x_1, \ldots, x_n)$. Системы функций

$$\{\mathrm{a}^{\tilde{0}}g, \ldots, \mathrm{a}^{\tilde{1}}g\} \text{ и } \{\mathrm{a}^{\tilde{0}}h, \ldots, \mathrm{a}^{\tilde{1}}h\}$$

являются базисами линейного пространства всех булевых функций от n аргументов. Найдется единственное линейное преобразование φ, переводящее один базис в другой таким образом, что $\varphi(\mathrm{a}^{\tilde{\tau}}g) = \mathrm{a}^{\tilde{\tau}}h$.

По предложению 3.6 существует $\alpha_{\tilde{0}}, \ldots, \alpha_{\tilde{1}}$ такие, что для любой функции $f(\tilde{x})$ имеет место разложение:

$$\mathrm{b}f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \cdot \mathrm{a}^{\tilde{\tau}} f(\tilde{x}).$$

Тогда

$$\varphi(\mathrm{b}g(\tilde{x})) = \varphi\Big(\sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \cdot g(\tilde{x})\Big) =$$

$$= \sum_{\tilde{\tau} \in E^n} \varphi(\alpha_{\tilde{\tau}} \cdot g(\tilde{x})) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \cdot h(\tilde{x}) = \mathrm{b}h(\tilde{x}).$$

Рассмотрим произвольную булеву функцию $f(x_1,\ldots,x_n)$. Для любого базисного пучка $A = (a^0,\ldots,a^{\tilde{\tau}},\ldots,a^1) \in K$ выполняется:

$$\varphi(f(\tilde{x}))=\varphi\Big(\sum_{\tilde{\tau}\in E^n}\alpha_{\tilde{\tau}}a^{\tilde{\tau}}g(\tilde{x})\Big)=\sum_{\tilde{\tau}\in E^n}\alpha_{\tilde{\tau}}\varphi(a^{\tilde{\tau}}g(\tilde{x}))=\sum_{\tilde{\tau}\in E^n}\alpha_{\tilde{\tau}}a^{\tilde{\tau}}h(\tilde{x}).$$

Очевидно, что сложности полиномов, порожденных пучком по функции $g(\tilde{x})$ для булевой функции $f(\tilde{x})$ и этим же пучком по функции $h(\tilde{x})$ для функции $\varphi(f(\tilde{x}))$ совпадают. Отсюда следует, что для класса операторных пучков K будет выполняться равенство

$$L_K^g(f) = L_K^h(\varphi(f)).$$

А поскольку преобразование φ — невырожденное, то $\varphi(F^n) = F^n$, где F^n — множество всех булевых функций от n аргументов. Отсюда $L_K^g(n) = L_K^h(n)$. □

Доказанная теорема позволила при исследовании сложности класса, состоящего из всех булевых функций размерности n, рассматривать полиномы, построенные по образам только одной функции. Поэтому в дальнейшем изложении мы будем пользоваться этим свойством. Термин "операторные формы" будет использоваться для канонических форм, построенных по классам операторных пучков по функции конъюнкции. В обозначении функции Шеннона символ функции g будет отсутствовать.

Сложность в операторных формах и ПНФ.

Итак, по предыдущей теореме сложность зависит только от класса операторов. Естественно рассмотреть вопрос о сравнении по сложности класса всех операторных форм и класса всех полиномиальных нормальных форм булевых функций.

Теорема 3.23. *Для класса всех булевых функций размерности n сложность в классе операторных канонических форм и сложность в полиномиальных нормальных формах совпадают:*

$$L_{OPF}(n) = L_{\text{ПНФ}}(n).$$

Доказательство. Пусть $L_{\text{ПНФ}}(n) = k$ и пусть $f(\tilde{x})$ — функция, на которой достигается максимум $L_{\text{ПНФ}}(f)$. Тогда

$$f(\tilde{x}) = K_1 \oplus K_2 \oplus \ldots \oplus K_k,$$

где K_i — элементарная конъюнкция.

По конъюнкции K_i построим оператор $\mathfrak{a}^i = \mathfrak{a}_1\mathfrak{a}_2\ldots\mathfrak{a}_n$ следующим образом:

$$\mathfrak{a}_i = \begin{cases} \mathfrak{e}, & \text{если } x_i \text{ присутствует в } K_i, \\ \mathfrak{p}, & \text{если } \bar{x}_i \text{ присутствует в } K_i, \\ \mathfrak{d}, & \text{в противном случае.} \end{cases}$$

Тогда по построению получим $K_i = \mathfrak{a}^i(x_1 \cdot \ldots \cdot x_n)$.

Проделав аналогичное построение по всем конъюнкциям получим набор операторов $\mathfrak{a}^1, \mathfrak{a}^2, \ldots, \mathfrak{a}^k$. Построенные операторы порождают линейно независимую систему функций. Это следует из минимальности представления функции. Следовательно, этот набор операторов является частью базисного операторного пучка, в котором функция $f(x_1, \ldots, x_n)$ имеет такую же сложность, что и в полиномиальных нормальных формах. □

Две предыдущие теоремы упростили задачу исследования классов операторных форм относительно сложности в двух направлениях:

1) для всего класса булевых функций достаточно ограничится рассмотрением операторных форм по функции конъюнкции, оценки переносятся на операторные формы по любой нечетной функции, и наоборот;

2) полиномиальные нормальные формы не являются каноническими, однако с операторной точки зрения каждая минимальная форма, реализующая данную функцию, является представлением этой функции некоторой операторной формой. Это дает возможность в задаче минимизации рассматривать канонические формы для нахождения точного минимума.

Сложность в однородных формах.

Для нахождения оценок потребуются три специальные функции. Функции определяются индуктивно:

$$p_0 = 0, \quad q_0 = 1, \quad t_0 = 1,$$
$$p_n(x_1, \ldots, x_n) = x_n q_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n t_{n-1}(x_1, \ldots, x_{n-1}),$$
$$q_n(x_1, \ldots, x_n) = x_n t_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n p_{n-1}(x_1, \ldots, x_{n-1}),$$
$$t_n(x_1, \ldots, x_n) = x_n p_{n-1}(x_1, \ldots, x_{n-1}) \oplus \bar{x}_n q_{n-1}(x_1, \ldots, x_{n-1}).$$

Предварительно докажем несколько свойств введенных функций. Для удобства введем обозначение $M_n = \{p_n, q_n, t_n\}$.

Множество функций, однотипных функциям из M_n, будем обозначать символом $M_n^{\diamond}$.

Предложение 3.17. *Справедливы следующие свойства функций из* M_n:

$$p_n \oplus q_n \oplus t_n = 0 \tag{3.25}$$

$$\begin{aligned} p_n &= x_n q_{n-1} \oplus \bar{x}_n t_{n-1} = x_n p_{n-1} \oplus t_{n-1} = \bar{x}_n p_{n-1} \oplus q_{n-1}, \\ q_n &= x_n t_{n-1} \oplus \bar{x}_n p_{n-1} = x_n q_{n-1} \oplus p_{n-1} = \bar{x}_n q_{n-1} \oplus t_{n-1}, \\ t_n &= x_n p_{n-1} \oplus \bar{x}_n q_{n-1} = x_n t_{n-1} \oplus q_{n-1} = \bar{x}_n t_{n-1} \oplus p_{n-1}. \end{aligned} \tag{3.26}$$

Доказательство свойства (3.25) проведем индукцией по числу аргументов n функций f_n, g_n, h_n.

При $n = 0$

$$p_0 \oplus q_0 \oplus t_0 = 0 \oplus 1 \oplus 1 = 0.$$

По индуктивному предположению (3.25) выполняется для p_{n-1}, q_{n-1}, t_{n-1}. По определению

$$\begin{aligned} p_n \oplus q_n \oplus h_n = \\ = \bar{x}_n q_{n-1} \oplus x_n t_{n-1} \oplus \bar{x}_n t_{n-1} \oplus x_n p_{n-1} \oplus \bar{x}_n p_{n-1} \oplus x_n q_{n-1} = \\ = (p_{n-1} \oplus q_{n-1} \oplus t_{n-1})(x_n \oplus \bar{x}_n) = 0. \end{aligned}$$

Индуктивный шаг доказан.

Теперь покажем выполнимость свойства (3.26). По определению функций p_n, q_n, t_n получаем

$$\begin{aligned} p_n = \bar{x}_n q_{n-1} \oplus x_n t_{n-1} = \\ = \bar{x}_n(\bar{x}_{n-1} t_{n-2} \oplus x_{n-1} p_{n-2}) \oplus x_n(\bar{x}_{n-1} p_{n-2} \oplus x_{n-1} q_{n-2}) = \\ = \bar{x}_n \bar{x}_{n-1} t_{n-2} \oplus (\bar{x}_n x_{n-1} \oplus x_n \bar{x}_{n-1}) p_{n-2} \oplus x_n x_{n-1} q_{n-2}. \end{aligned}$$

В силу свойства (3.25) отсюда получаем

$$\begin{aligned} p_n = \bar{x}_n \bar{x}_{n-1} q_{n-2} \oplus (\bar{x}_n \bar{x}_{n-1} \oplus \bar{x}_n x_{n-1} \oplus \\ \oplus x_n \bar{x}_{n-1} \oplus x_n x_{n-1}) p_{n-2} \oplus x_n x_{n-1} t_{n-2} = \\ = \bar{x}_n \bar{x}_{n-1} q_{n-2} \oplus x_n x_{n-1} t_{n-2} \oplus p_{n-2}. \end{aligned}$$

Аналогичное доказательство и для q_n, t_n. □

Предложение 3.18. *Для любых функций $f, g, h \in M_n^\diamond$, удовлетворяющих условию $f \oplus g \oplus h = 0$, справедливо следующее: если для некоторого набора $\tilde{\tau}$ выполняется $\mathrm{p}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}) \in M_n$, то*

$$\left\{\mathrm{p}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}), \mathrm{p}_{\tilde{x}}^{\tilde{\tau}} g(\tilde{x}), \mathrm{p}_{\tilde{x}}^{\tilde{\tau}} h(\tilde{x})\right\} = M_n.$$

Доказательство проведем индукцией по n.

Базис индукции. При $n = 1$ имеем

$$M_1^\diamond = \{(01), (10), (11)\} = M_1.$$

Шаг индукции. Пусть функции $f, g, h \in M_n^\diamond$, $f \oplus g \oplus h = 0$, $\mathrm{p}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}) \in M_n$. Для определенности предположим, что имеет место равенство $\mathrm{p}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}) = p_n(\tilde{x})$, Для упрощения записи используем обозначения: $\tilde{x}' = (x_1, \ldots, x_{n-1})$, $\tilde{\tau}' = (\tau_1, \ldots, \tau_{n-1})$. В силу предложения 3.17

$$\begin{aligned}
&\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f_{x_n}^{\bar{\tau}_n}(\tilde{x}') = t_{n-1}(\tilde{x}'),\\
&\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f_{x_n}^{\tau_n}(\tilde{x}') = q_{n-1}(\tilde{x}'),\\
&\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f'_{x_n}(\tilde{x}') = p_{n-1}(\tilde{x}').
\end{aligned}$$

Тройка функций $f_{x_n}^{\bar{\tau}_n}(\tilde{x}')$, $g_{x_n}^{\bar{\tau}_n}(\tilde{x}')$, $h_{x_n}^{\bar{\tau}_n}(\tilde{x}')$ удовлетворяет предположению индукции, поэтому

$$\left\{\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f_{x_n}^{\bar{\tau}_n}(\tilde{x}'), \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} g_{x_n}^{\bar{\tau}_n}(\tilde{x}'), \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} h_{x_n}^{\bar{\tau}_n}(\tilde{x}')\right\} = M_{n-1}.$$

Для определенности предположим, что $\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} g_{x_n}^{\bar{\tau}_n}(\tilde{x}') = p_{n-1}(\tilde{x}')$. Тогда $\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} h_{x_n}^{\bar{\tau}_n}(\tilde{x}') = q_{n-1}(\tilde{x}')$. Тройки функций

$$\begin{aligned}
&g_{x_n}^{\bar{\tau}_n}(\tilde{x}'),\ g_{x_n}^{\tau_n}(\tilde{x}'),\ g'_{x_n}(\tilde{x}'); \qquad && h_{x_n}^{\bar{\tau}_n}(\tilde{x}'),\ h_{x_n}^{\tau_n}(\tilde{x}'),\ h'_{x_n}(\tilde{x}');\\
&f_{x_n}^{\tau_n}(\tilde{x}'),\ g_{x_n}^{\tau_n}(\tilde{x}'),\ h_{x_n}^{\tau_n}(\tilde{x}'); && f'_{x_n}(\tilde{x}'),\ g'_{x_n}(\tilde{x}'),\ h'_{x_n}(\tilde{x}')
\end{aligned}$$

также удовлетворяют предположению индукции. Поэтому

$$\begin{aligned}
&\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} g_{x_n}^{\tau_n}(\tilde{x}') = t_{n-1}(\tilde{x}'), \qquad && \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} g'_{x_n}(\tilde{x}') = q_{n-1}(\tilde{x}'),\\
&\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} h_{x_n}^{\tau_n}(\tilde{x}') = p_{n-1}(\tilde{x}'), && \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} h'_{x_n}(\tilde{x}') = t_{n-1}(\tilde{x}').
\end{aligned}$$

Отсюда получается

$$\mathrm{p}_{\tilde{x}}^{\tilde{\tau}} g(\tilde{x}) = \bar{x}_n \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} g_{x_n}^{\bar{\tau}_n}(\tilde{x}') \oplus x_n \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} g_{x_n}^{\tau_n}(\tilde{x}') =$$

$$= \bar{x}_n p_{n-1}(\tilde{x}') \oplus x_n t_{n-1}(\tilde{x}') = q_n(\tilde{x}),$$

$$\mathrm{p}_{\tilde{x}}^{\tilde{\tau}} h(\tilde{x}) = \bar{x}_n \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} h_{x_n}^{\bar{\tau}_n}(\tilde{x}') \oplus x_n \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} h_{x_n}^{\tau_n}(\tilde{x}') =$$

$$= \bar{x}_n q_{n-1}(\tilde{x}') \oplus x_n p_{n-1}(\tilde{x}') = t_n(\tilde{x}).$$

Таким образом,

$$\left\{\mathrm{p}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}), \mathrm{p}_{\tilde{x}}^{\tilde{\tau}} g(\tilde{x}), \mathrm{p}_{\tilde{x}}^{\tilde{\tau}} h(\tilde{x})\right\} = M_n. \qquad \square$$

Предложение 3.19. *Для любой функции f выполняется следующее свойство: $f^0_{x_{n+1}}, f^1_{x_{n+1}}, f'_{x_{n+1}} \in M_n^{\diamond}$ тогда и только тогда, когда $f \in M_{n+1}^{\diamond}$.*

Доказательство. *Достаточность* непосредственно следует из предложения 3.18 и определения однотипности булевых функций.

Необходимость. Для удобства положим $\tilde{x} = (x_1, \ldots, x_{n+1})$, $\tilde{x}' = (x_1, \ldots, x_n)$. По определению производной

$$f^0_{x_{n+1}} \oplus f^1_{x_{n+1}} \oplus f'_{x_{n+1}} = 0,$$

откуда имеем, что тройка функций $f^0_{x_{n+1}}, f^1_{x_{n+1}}, f'_{x_{n+1}}$ удовлетворяет условиям предложения 3.18. Поэтому найдется набор $\tilde{\tau}'$ такой, что

$$\left\{\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f^0_{x_{n+1}}(\tilde{x}'), \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f^1_{x_{n+1}}(\tilde{x}'), \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f'_{x_{n+1}}(\tilde{x}')\right\} = M_n.$$

Пусть для определенности

$$\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f^0_{x_{n+1}}(\tilde{x}') = q_n(\tilde{x}'),$$

$$\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f^1_{x_{n+1}}(\tilde{x}') = t_n(\tilde{x}'),$$

$$\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f'_{x_{n+1}}(\tilde{x}') = p_n(\tilde{x}').$$

Тогда

$$\mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f(\tilde{x}) = \bar{x}_{n+1} \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f^0_{x_{n+1}}(\tilde{x}') \oplus x_{n+1} \mathrm{p}_{\tilde{x}'}^{\tilde{\tau}'} f^1_{x_{n+1}}(\tilde{x}') =$$

$$= \bar{x}_{n+1} q_n(\tilde{x}') \oplus x_{n+1} t_n(\tilde{x}').$$

Полагая $\tau_{n+1} = 0$, получим

$$\mathrm{p}_{\tilde{x}}^{\tilde{\tau}} f(\tilde{x}) = \bar{x}_{n+1} t_n(\tilde{x}') \oplus x_{n+1} q_n(\tilde{x}') = p_{n+1}(\tilde{x}).$$

Откуда следует $f \in M^{\diamond}_{n+1}$. □

Теорема 3.24. *Для класса всех булевых функций в любом из следующих классов операторных форм: однородных, HDE, HPD и HPE имеет место следующее точное значение функции Шеннона:*

$$L_H(n) = \left\lfloor \tfrac{2}{3} 2^n \right\rfloor .$$

Доказательство. Поскольку класс канонических форм по однородным операторным пучкам включает в себя классы HDE, HPD и HPE, достаточно получить нижнюю оценку для однородных операторных форм и верхние оценки для указанных трех классов. Теорема будет иметь место в случае их совпадения.

В качестве кандидата на построение последовательности сложных функций можно рассмотреть три приведенные функции: p_n, q_n, t_n.

Индукцией по n покажем, что при любом однородном операторном пучке тройка сложностей $L_H(p_n)$, $L_H(q_n)$, $L_H(t_n)$ при нечетном n будет состоять из одного числа $(2^{n+1}+2)/3$ и двух чисел $(2^{n+1}-1)/3$, а при четном n из одного числа $(2^{n+1}-2)/3$ и двух чисел $(2^{n+1}+1)/3$.

Имеется только три пучка операторов размерности 1, с точностью до перестановки операторов в пучке:

$$(\mathrm{d}, \mathrm{p}), (\mathrm{d}, \mathrm{e}), (\mathrm{e}, \mathrm{p}).$$

Непосредственная проверка указанных пучков получает одно число 2 и два числа 1.

Для индуктивного шага необходимо построить однородный операторный пучок $\mathrm{C} = \{\mathrm{c}^{\tilde{0}}, \ldots, \mathrm{c}^{\tilde{\tau}}, \ldots, \mathrm{c}^{\tilde{1}}\}$ с компонентами $\mathrm{c}^{\tilde{\tau}} = \mathrm{c}_1 \ldots \mathrm{c}_n$ по имеющемуся однородному пучку $\mathrm{A} = \{\mathrm{a}^{\tilde{0}}, \ldots, \mathrm{a}^{\tilde{1}}\}$ с компонентами $\mathrm{a}^{\tilde{\sigma}} = \mathrm{a}_1 \ldots \mathrm{a}_{n-1}$.

Согласно определению однородных пучков достаточно построить пару операторов длины n по имеющимся двум операторам длины $n-1$.

Итак, пусть имеется операторы $\mathrm{a}_1 \ldots \mathrm{a}_{n-1}$ и $\mathrm{b}_1 \ldots \mathrm{b}_{n-1}$. Рассмотрим все возможные варианты для a_n и b_n.

По условию $\mathrm{a}_n \neq \mathrm{b}_n$, откуда получим следующие варианты:
1) $\mathrm{a}_n = \mathrm{d}$ и $\mathrm{b}_n = \mathrm{p}$; 2) $\mathrm{a}_n = \mathrm{p}$ и $\mathrm{b}_n = \mathrm{e}$;

3) $\mathfrak{a}_n = \mathfrak{e}$ и $\mathfrak{b}_n = \mathfrak{d}$; 4) $\mathfrak{a}_n = \mathfrak{d}$ и $\mathfrak{b}_n = \mathfrak{e}$;
5) $\mathfrak{a}_n = \mathfrak{p}$ и $\mathfrak{b}_n = \mathfrak{d}$; 6) $\mathfrak{a}_n = \mathfrak{e}$ и $\mathfrak{b}_n = \mathfrak{p}$.

В силу симметричности достаточно рассмотреть случаи 1)–3). Пусть функция $f(x_1, \ldots, x_n)$ имеет разложение по однородному операторному пучку C:

$$p(x_1, \ldots, x_n) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \mathfrak{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n).$$

Это разложение можно разбить на две суммы и провести несложное преобразование по свойствам операторов:

$$\begin{aligned}
&\sum_{\tilde{\tau}} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) = \\
&= \sum_{\tau_1, \ldots, \tau_{n-1}, 0} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) \oplus \sum_{\tau_1, \ldots, \tau_{n-1}, 1} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) = \\
&= \mathfrak{a}_n(x_n) \cdot \sum_{\tau_1, \ldots, \tau_{n-1}} \alpha_{\tau_1, \ldots, \tau_{n-1}} \cdot (\mathfrak{c}_1 \ldots \mathfrak{c}_{n-1})^{\tau_1, \ldots, \tau_{n-1}}(x_1 \cdot \ldots \cdot x_{n-1}) \oplus \\
&\oplus \mathfrak{b}_n(x_n) \cdot \sum_{\tau_1, \ldots, \tau_{n-1}} \alpha_{\tau_1, \ldots, \tau_{n-1}} \cdot (\mathfrak{c}_1 \ldots \mathfrak{c}_{n-1})^{\tau_1, \ldots, \tau_{n-1}}(x_1 \cdot \ldots \cdot x_{n-1}).
\end{aligned}$$

Теперь имеем три равенства по 1)–3):

$$\begin{aligned}
p(x_1, \ldots, x_n) = 1 \cdot &\sum_{\tilde{\tau}, \tau_n = 0} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}_1 \ldots \mathfrak{c}_{n-1}^{(\tau_1, \ldots, \tau_{n-1})}(x_1 \cdot \ldots \cdot x_{n-1}) \oplus \\
&\oplus \bar{x}_n \cdot \sum_{\tilde{\tau}, \tau_n = 1} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}_1 \ldots \mathfrak{c}_{n-1}^{(\tau_1, \ldots, \tau_{n-1})}(x_1 \cdot \ldots \cdot x_{n-1}); \quad (3.27)
\end{aligned}$$

$$\begin{aligned}
p(x_1, \ldots, x_n) = \bar{x}_n \cdot &\sum_{\tilde{\tau}, \tau_n = 0} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}_1 \ldots \mathfrak{c}_{n-1}^{(\tau_1, \ldots, \tau_{n-1})}(x_1 \cdot \ldots \cdot x_{n-1}) \oplus \\
&\oplus x_n \cdot \sum_{\tilde{\tau}, \tau_n = 1} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}_1 \ldots \mathfrak{c}_{n-1}^{(\tau_1, \ldots, \tau_{n-1})}(x_1 \cdot \ldots \cdot x_{n-1}); \quad (3.28)
\end{aligned}$$

$$\begin{aligned}
p(x_1, \ldots, x_n) = x_n \cdot &\sum_{\tilde{\tau}, \tau_n = 0} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}_1 \ldots \mathfrak{c}_{n-1}^{(\tau_1, \ldots, \tau_{n-1})}(x_1 \cdot \ldots \cdot x_{n-1}) \oplus \\
&\oplus 1 \cdot \sum_{\tilde{\tau}, \tau_n = 1} \alpha_{\tilde{\tau}} \cdot \mathfrak{c}_1 \ldots \mathfrak{c}_{n-1}^{(\tau_1, \ldots, \tau_{n-1})}(x_1 \cdot \ldots \cdot x_{n-1}). \quad (3.29)
\end{aligned}$$

Согласно определению и предложению 3.17 равенства (3.27), (3.28), (3.29) можно свернуть до следующих соответственно:

$$p_n = \bar{x}_n p_{n-1} \oplus q_{n-1},$$
$$p_n = x_n q_{n-1} \oplus \bar{x}_n t_{n-1},$$
$$p_n = x_n p_{n-1} \oplus t_{n-1}.$$

Аналогичные рассуждения приводят к равенствам для функций q_n, t_n:

$$q_n = x_n t_{n-1} \oplus \bar{x}_n p_{n-1} = x_n q_{n-1} \oplus p_{n-1} = \bar{x}_n q_{n-1} \oplus t_{n-1},$$
$$t_n = x_n p_{n-1} \oplus \bar{x}_n q_{n-1} = x_n t_{n-1} \oplus q_{n-1} = \bar{x}_n t_{n-1} \oplus p_{n-1}.$$

При минимальной операторной форме функций p_{n-1}, q_{n-1}, t_{n-1} одно из трех представлений функций p_n, q_n, t_n будет минимальной формой по однородным операторам в силу единственности представления.

Отсюда при любой компоненте c_n, получаем, что тройка сложностей $L_H(p_n)$, $L_H(q_n)$, $L_H(t_n)$ будет состоять из чисел:

$$L_H^{n-1}(p_{n-1}) + L_H^{n-1}(q_{n-1}),$$
$$L_H^{n-1}(q_{n-1}) + L_H^{n-1}(t_{n-1}),$$
$$L_H^{n-1}(t_{n-1}) + L_G^{n-1}(p_{n-1}).$$

Учитывая индуктивное предположение, при нечетном n получаем числа:

$$\frac{2^n-2}{3} + \frac{2^n+1}{3} = \frac{2^{n+1}-1}{3},$$
$$\frac{2^n-2}{3} + \frac{2^n+1}{3} = \frac{2^{n+1}-1}{3},$$
$$\frac{2^n+1}{3} + \frac{2^n+1}{3} = \frac{2^{n+1}+2}{3},$$

при n — четном:

$$\frac{2^n+2}{3} + \frac{2^n-1}{3} = \frac{2^{n+1}+1}{3},$$
$$\frac{2^n+2}{3} + \frac{2^n-1}{3} = \frac{2^{n+1}+1}{3},$$

$$\frac{2^n-1}{3}+\frac{2^n-1}{3}=\frac{2^{n+1}-2}{3}.$$

Получили, что сложность функций p_n, q_n, t_n при нечетном n не менее $(2^{n+1}-1)/3$, а при четном не менее $(2^{n+1}-2)/3$. Нижняя оценка доказана.

Нахождение верхней оценки проведем для класса HPE-форм индукцией по n. Для $n=1$ очевидно $L_{HPE}(1)=1$, поэтому $L_{HPE}(1)<\frac{2}{3}\cdot 2^1$.

Пусть f призвольная булева функция от n аргументов. По индуктивному предположению для функции от $(n-1)$ аргументов $f'_{x_n}=f^0_{x_n}\oplus f^1_{x_n}$ существует минимальная HPE-форма $P(f'_{x_n})$ такая, что $L_P(f'_{x_n}))<\frac{2}{3}\cdot 2^{n-1}$. Заметим, что сумма различных слагаемых в $P(f^0_{x_n})$ и $P(f^1_{x_n})$ равна $P(f'_{x_n})$. Поэтому можно получить следующее представление:

$$P(f^0_{x_n})=P_0\oplus P_2,\ P(f^1_{x_n})=P_1\oplus P_2,$$

где $P_0\oplus P_1$ совпадает с $P(f'_{x_n})$.

Отсюда получаем представление функции f

$$f=\overline{x}_n f^0_{x_n}\oplus x_n f^1_{x_n}=\overline{x}_n P(f^0_{x_n})\oplus x_n P(f^1_{x_n})=\overline{x}_n P_0\oplus x_n P_1\oplus P_2.$$

Так как общее количество слагаемых в P_0 и P_1 меньше $\frac{2}{3}\cdot 2^{n-1}$, то либо количество слагаемых в P_0 меньше $\frac{2}{3}\cdot 2^{n-2}$, либо количество слагаемых в P_1 меньше $\frac{2}{3}\cdot 2^{n-2}$.

Для определенности пусть $L(P_0)<\frac{2}{3}\cdot 2^{n-2}$, тогда функция $f=x_n(P_0\oplus P_1)\oplus(P_0\oplus P_2)$ и так как P_0,P_1,P_2 не имеют одинаковых слагаемых, то получаем

$$L_{HPE}(f)\leqslant 2L(P_0)+2^{n-1}-L(P_0)=$$
$$=L(P_0)+2^{n-1}<\frac{2}{3}\cdot 2^{n-2}+2^{n-1}=\frac{2}{3}\cdot 2^n.$$

Верхняя оценка доказана. Она совпадает с нижней оценкой для класса однородных операторных форм.

Для классов HPD и HDE доказательство верхней оценки проводится аналогично. □

Следующая теорема позволяет найти все сложные функции в классе однородных операторных форм.

Теорема 3.25. *Если $f\in F^n$, $n\geqslant 1$, то $L_H(f)=\left\lfloor\frac{2}{3}2^n\right\rfloor$ тогда и только тогда, когда $f\in M_n^{\diamond}$.*

Доказательство. *Достаточность* следует из теоремы 3.24 и определения однотипности.

Необходимость. Прежде всего докажем следующее утверждение. Если $f \in F^n \setminus M_n^\diamond$, то найдется однородный пучок операторов $\mathsf{A} = \{\mathsf{a}^{\tilde{0}}, \ldots, \mathsf{a}^{\tilde{1}}\}$ размерности $n-1$ такой, что

$$L_{\mathsf{A}}(f_{x_n}^0) + L_{\mathsf{A}}(f_{x_n}^1) + L_{\mathsf{A}}(f_{x_n}') \leqslant 2^n - 2. \tag{3.30}$$

При $n = 1$ только одна функция, а именно (00), не принадлежит $M_1^\diamond$, и для нее утверждение очевидно выполняется. Пусть теперь $n \geqslant 2$. Из предложения 3.19 следует, что хотя бы одна из функций $f_{x_{n-1}}^0, f_{x_{n-1}}^1, f_{x_{n-1}}'$ удовлетворяет индуктивному предположению. Пусть для определенности это функция $f_{x_{n-1}}^0$. Тогда найдется однородный пучок $\mathsf{B} = \{\mathsf{b}^{\tilde{0}}, \ldots, \mathsf{b}^{\tilde{1}}\}$ операторов размерности $n-2$ такой, что

$$L_{\mathsf{B}}(f_{x_n x_{n-1}}^{00}) + L_{\mathsf{B}}(f_{x_n x_{n-1}}^{10}) + L_{\mathsf{B}}(f_{x_n x_{n-1}}^{\prime 0}) \leqslant 2^{n-1} - 2$$

и

$$L_{\mathsf{B}}(f_{x_n x_{n-1}}^{01}) + L_{\mathsf{B}}(f_{x_n x_{n-1}}^{11}) + L_{\mathsf{B}}(f_{x_n x_{n-1}}^{\prime 1}) \leqslant 2^{n-1}.$$

Зададим пучок A как слияние взятого дважды пучка B с пучком (p, e). Этот пучок — однородный, и для любой функции $g(x_1, \ldots, x_{n-1})$ имеем

$$g(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \mathsf{a}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_{n-1}) =$$

$$= \mathsf{p}x_{n-1} \sum_{\tilde{\tau}' \in E^{n-1}} \alpha_{\tilde{\tau}'0} \mathsf{b}^{\tilde{\tau}'}(x_1 \cdot \ldots \cdot x_{n-2}) \oplus$$

$$\oplus \mathsf{e}x_{n-1} \sum_{\tilde{\tau}' \in E^{n-1}} \alpha_{\tilde{\tau}'1} \mathsf{b}^{\tilde{\tau}'}(x_1 \cdot \ldots \cdot x_{n-2}),$$

Для остаточных функций справедливо:

$$g_{x_{n-1}}^0 = \mathsf{o}_{x_{n-1}} g(\tilde{x}) = \sum_{\tilde{\tau}' \in E^{n-1}} \alpha_{\tilde{\tau}'0} \mathsf{b}^{\tilde{\tau}' \in E^{n-1}}(x_1 \cdot \ldots \cdot x_{n-2}),$$

$$g_{x_{n-1}}^1 = \mathsf{i}_{x_{n-1}} g(\tilde{x}) = \sum_{\tilde{\tau}' \in E^{n-1}} \alpha_{\tilde{\tau}'1} \mathsf{b}^{\tilde{\tau}'}(x_1 \cdot \ldots \cdot x_{n-2}).$$

Поэтому выполняются следующие равенства:

$$L_{\mathsf{A}}(g) = L_{\mathsf{B}}(g_{x_{n-1}}^0) + L_{\mathsf{B}}(g_{x_{n-1}}^1),$$

$$L_{\mathsf{A}}(f^0_{x_n}) + L_{\mathsf{A}}(f^1_{x_n}) + L_{\mathsf{A}}(f'_{x_n}) =$$
$$= L_{\mathsf{B}}(f^{00}_{x_n x_{n-1}}) + L_{\mathsf{B}}(f^{01}_{x_n x_{n-1}}) + L_{\mathsf{B}}(f^{10}_{x_n x_{n-1}}) +$$
$$+ L_{\mathsf{B}}(f^{11}_{x_n x_{n-1}}) + L_{\mathsf{B}}(f^{/0}_{x_n x_{n-1}}) + L_{\mathsf{B}}(f^{/1}_{x_n x_{n-1}}) =$$
$$= L_{\mathsf{B}}(f^{00}_{x_n x_{n-1}}) + L_{\mathsf{B}}(f^{10}_{x_n x_{n-1}}) + L_{\mathsf{B}}(f^{/0}_{x_n x_{n-1}}) +$$
$$+ L_{\mathsf{B}}(f^{01}_{x_n x_{n-1}}) + L_{\mathsf{B}}(f^{11}_{x_n x_{n-1}}) + L_{\mathsf{B}}(f^{/1}_{x_n x_{n-1}})$$
$$\leqslant 2^{n-1} - 2 + 2^{n-1} = 2^n - 2.$$

Зададим однородные операторные пучки C_1, C_2, C_3 как слияние пучка A, взятого дважды, с пучками $\{\mathsf{p}, \mathsf{e}\}$, $\{\mathsf{e}, \mathsf{d}\}$, $\{\mathsf{d}, \mathsf{p}\}$ соответственно. Умножим неравенство (3.30) на 2 и проведем несколько несложных преобразований:

$$2L_{\mathsf{A}}(f^0_{x_n}) + 2L_{\mathsf{A}}(f^1_{x_n}) + 2L_{\mathsf{A}}(f'_{x_n})) =$$
$$= L_{\mathsf{A}}(f^0_{x_n}) + L_{\mathsf{A}}(f^1_{x_n}) + L_{\mathsf{A}}(f^0_{x_n}) +$$
$$+ L_{\mathsf{A}}(f'_{x_n}) + L_{\mathsf{A}}(f'_{x_n}) + L_{\mathsf{A}}(f^1_{x_n}) =$$
$$= L_{\mathsf{C}_1}(f) + L_{\mathsf{C}_2}(f) + L_{\mathsf{C}_3}(f) \leqslant 2^{n+1} - 4.$$

Поэтому для любой функции $f \in F^n \backslash M_n^{\diamondsuit}$

$$L_H(f) \leqslant \min\{L_{\mathsf{C}_1}(f), L_{\mathsf{C}_2}(f), L_{\mathsf{C}_3}(f)\} < \left\lfloor \tfrac{2}{3} 2^n \right\rfloor. \qquad \square$$

Сложность в расширенных однородных формах.

Класс расширенных однородных форм имеет формулы вычисления коэффициентов представлений функций близкие к формулам в однородных формах (теорема 3.17), при этом сложность класса всех булевых функций в расширенных однородных формах оказалась меньшей по сравнению с однородными.

Теорема 3.26. 1. *Для любого класса расширенных операторных форм ExH_i сложность класса всех булевых функций равна*

$$L_{ExH_i}(n) = \tfrac{1}{2} \cdot 2^n.$$

2. *Для класса всех расширенных операторных форм ExH сложность класса всех булевых функций имеет границы:*

$$\tfrac{1}{3} \cdot 2^n < L_{ExH}(n) \leqslant \tfrac{1}{2} \cdot 2^n.$$

Доказательство. 1. Рассмотрим разложение некоторой функции $f(\tilde{x})$ по однородному пучку $\mathsf{A} = (\mathsf{a}^{\tilde{0}}, \ldots, \mathsf{a}^{\tilde{1}})$:

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

Обозначим через $L_{\mathsf{A}}(f)$ число ненулевых коэффициентов $\alpha_{\tilde{\tau}}$ в разложении, иными словами $L_{\mathsf{A}}(f)$ — сложность функции $f(\tilde{x})$ в базисе $\{\mathsf{a}^{\tilde{0}}(x_1 \cdot \ldots \cdot x_n), \ldots, \mathsf{a}^{\tilde{1}}(x_1 \cdot \ldots \cdot x_n)\}$.

Пусть $L_{\mathsf{A}}(f) = \frac{1}{2} \cdot 2^n + k$, $k \geqslant 1$ и для некоторого $\tilde{\tau}$ коэффициент $\alpha_{\tilde{\tau}}$ равен 1.

Пусть c — оператор со свойством $\mathsf{a}^{\tilde{0}} \circ \mathsf{c} = 1$ и $\mathsf{a}^{\tilde{1}} \circ \mathsf{c} = 1$. Такой оператор всегда существует согласно предложения 3.10. Построим операторный пучок $\mathsf{B} = (\mathsf{b}^{\tilde{0}}, \ldots, \mathsf{b}^{\tilde{\tau}}, \ldots, \mathsf{b}^{\tilde{1}})$, в котором операторы определены следующим образом:

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

Тогда имеем разложение для функции $f(\tilde{x})$:

$$f(\tilde{x}) = \sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\sigma}} \mathsf{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n),$$

где

$$\beta_{\tilde{\sigma}} = \begin{cases} 1, & \text{если } \tilde{\sigma} = \tilde{\tau}, \\ \alpha_{\tilde{\sigma}} \oplus 1, & \text{если } \tilde{\sigma} \neq \tilde{\tau}. \end{cases}$$

Теперь

$$L_{\mathsf{B}}(f) = 2^n - L_{\mathsf{A}}(f) + 1 = 2^n - \tfrac{1}{2}2^n - k + 1 = \tfrac{1}{2}2^n + 1 - k \leqslant \tfrac{1}{2}2^n.$$

По построению пучок B принадлежат тому же классу ExH_i, что и пучок A.

Для получения нижней оценки достаточно заметить, что любой пучок A порождает класс операторных форм, состоящий из единственной формы. Отсюда следует, что существует функция f, для которой выполняется:

$$L_{\mathsf{A}}(f) = \tfrac{1}{2} \cdot 2^n.$$

Очевидно, что для любого пучка B, построенного указанным способом, сложность не уменьшается:

$$L_{\mathsf{A}}(f) \leqslant L_{\mathsf{B}}(f).$$

Согласно определению, этот способ строит все пучки из одного класса ExH_i.

Таким образом, $L_{ExH_i} = \frac{1}{2} \cdot 2^n$.

2. Верхняя оценка следует из включения классов, дающего очевидное неравенство: $L_{ExH} \leqslant L_{ExH_i}$.

Нижняя оценка получается из сложности булевых функций в классе однородных операторных форм. Из теоремы 3.24 следует, что существует функция f со сложностью представления любой однородной операторной формой, равной $\left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor$.

Тогда согласно приведенному алгоритму сложность представления этой функции операторной формой по любому построенному пучку не может быть меньше, чем $\frac{1}{3} \cdot 2^n$. □

Сложность в смешанных однородных формах.

Напомним, что для классов MH и KH имеется включение $KH \subset MH$. Откуда следует, что $L_{MH}(n) \leqslant L_{KH}(n)$.

Теорема 3.27.

$$L_{MH}(n) = L_{KH}(n) = \tfrac{1}{2} \cdot 2^n.$$

Доказательство проведем в два этапа: сначала докажем неравенство $L_{KH}(n) \leqslant 2^{n-1}$, а затем $L_{MH}(n) \geqslant 2^{n-1}$.

Рассмотрим произвольную функцию $f(\tilde{x})$, $\tilde{x} = (x_1, \ldots, x_n)$. Для удобства введем обозначение $\tilde{x}' = (x_1, \ldots, x_{n-1})$. Пусть $\mathrm{A} \in KH$ — произвольный пучок операторов размерности $n-1$. По теореме 3.10

$$f(\tilde{x}', x_n) = \sum_{\tilde{\tau}' \in E^{n-1}} \mathfrak{a}^{\tilde{\tau}'}(x_1 \cdot \ldots \cdot x_{n-1}) g_{\tilde{\tau}'}(x_n).$$

Функции $g_{\tilde{\tau}'}$ зависят только от x_n. Это могут быть только следующие функции: 0, 1, x_n, $\bar{x}_n$. Определим 2^{n-1} пучков $\mathrm{B}_{\tilde{\tau}'}$ операторов размерности 1 следующим образом:

$$\mathrm{B}_{\tilde{\tau}'} = \begin{cases} (\mathrm{d}, \mathrm{e}), & \text{если } g_{\tilde{\tau}'}(x_n) \in \{0, 1, x_n\}; \\ (\mathrm{d}, \mathrm{p}), & \text{если } g_{\tilde{\tau}'}(x_n) = \bar{x}_n. \end{cases}$$

При этом сложность полинома, реализующего функцию

$$g_{\tilde{\tau}'}(x_n) = \alpha_{\tilde{\tau}'0} \mathrm{b}^{\tilde{0}}_{\tilde{\tau}'}(x_n) \oplus \alpha_{\tilde{\tau}'1} \mathrm{b}^{\tilde{1}}_{\tilde{\tau}'}(x_n)$$

не превосходит 1.

Пусть пучок C есть слияние пучков $\mathrm{B}_{\tilde{0}}, \ldots, \mathrm{B}_{\tilde{1}}$ по пучку A. По определению пучок C лежит в классе KH. Ему соответствует операторная форма:

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \mathrm{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) =$$

$$= \sum_{\tilde{\tau}' \in E^{n-1}} \mathrm{a}^{\tilde{\tau}'}(x_1 \cdot \ldots \cdot x_{n-1})(\alpha_{\tilde{\tau}'0} \mathrm{b}^{\tilde{0}}_{\tilde{\tau}'}(x_n) \oplus \alpha_{\tilde{\tau}'1} \mathrm{b}^{\tilde{1}}_{\tilde{\tau}'}(x_n)) =$$

$$= \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}'\tau_n} \mathrm{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n).$$

В силу единственности разложения, $\alpha_{\tilde{\tau}} = \alpha_{\tilde{\tau}'\tau_n}$. Но по крайней мере половина коэффициентов $\alpha_{\tilde{\tau}'\tau_n}$ равна нулю. Таким образом, для любой функции в классе KH существует операторная форма P такая, что $L(P)$ не превосходит 2^{n-1}. Следовательно, $L_{KH}(n) \leqslant 2^{n-1}$.

Теперь докажем, что если $f \in M_n^{\diamond}$, то $L_{MH}(f) \geqslant 2^{n-1}$. Из этого следует, что $L_{MH}(n) \geqslant 2^{n-1}$.

При $n = 1$ только три булевы функции, а именно, (01), (10) и (11) имеют сложность 1. Именно эти функции образуют множество $M_1^{\diamond}$.

Пусть теперь $n \geqslant 2$ и P — минимальная операторная форма из класса MH, реализующая какую-нибудь функцию f из $M_n^{\diamond}$. Полином P построен по некоторому пучку C, который является слиянием пучков $\mathrm{B}_{\tilde{0}}, \ldots, \mathrm{B}_{\tilde{1}}$ операторов размерности m и пучка A операторов размерности k, где $m + k = n$.

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} \mathrm{c}^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) =$$

$$= \sum_{\tilde{\tau}' \in E^k} \mathrm{a}^{\tilde{\tau}'}(x'_1 \cdot \ldots \cdot x'_k) \sum_{\tilde{\tau}'' \in E^m} \alpha_{\tilde{\tau}} \mathrm{b}^{\tilde{\tau}''}_{\tilde{\tau}'}(x''_1 \cdot \ldots \cdot x''_m).$$

Здесь $\tilde{x}'$, $\tilde{x}''$ — разбиение $\tilde{x}$, соответствующее разбиению $\tilde{\tau}$ на $\tilde{\tau}'$ и $\tilde{\tau}''$, фигурирующему в определении слияния.

По предложению 3.19 и теореме 3.10 выполняется:

$$\sum_{\tilde{\tau}'' \in E^m} \alpha_{\tilde{\tau}} \mathrm{b}^{\tilde{\tau}''}_{\tilde{\tau}'}(x''_1 \cdot \ldots \cdot x''_m) = \mathrm{t}^{\tilde{\tau}'}(f(\tilde{x}', \tilde{x}'')) \in M_m^{\diamond},$$

где $\mathrm{t}^{\tilde{\tau}'}$ — операторы типа II. Поэтому

$$L_{MH}(f) \geqslant \sum_{\tilde{\tau}'} L_{MH}\left(\mathrm{t}_{\tilde{\tau}'}(f(\tilde{x}', \tilde{x}''))\right) \geqslant 2^k \cdot 2^{m-1} = \tfrac{1}{2} \cdot 2^n. \quad \square$$

Теорема 3.28. *$L_T(f) = 2^{n-1}$ тогда и только тогда, когда $f \in M_n^\diamond$, $T \in \{MH, KH\}$.*

Доказательство. *Достаточность* непосредственно следует из теоремы 3.27.

Необходимость нужно доказать только для L_{KH} в силу неравенства $L_{MH}(f) \leqslant L_{KH}(f)$. Доказательство проведем по индукции.

Базис индукции. Существуют только четыре функции от одного аргумента. Три из них: (01), (10), (11) — образуют множество $M_1^\diamond$ и имеют сложность $1 = 2^{1-1}$. Четвертая, (00), имеет тривиальную сложность. Таким образом базис индукции выполняется.

Шаг индукции. Пусть теперь некоторая функция f, зависящая от n аргументов, имеет сложность $L_{KH}(f) = 2^{n-1}$ и реализуется операторной формой, построенной по некоторому пучку $C \in KH$. Пусть A_1, B_2 — пучки, построенные по предложению 3.14 из пучка C. Тогда получим представление:

$$f(\tilde{x}) = \sum_{\tilde{\tau} \in E^n} \alpha_{\tilde{\tau}} c^{\tilde{\tau}}(x_1 \cdot \ldots \cdot x_n) =$$

$$= t_1(x_1) \sum_{\tilde{\tau}' \in E^{n-1}} \beta_{\tilde{\tau}'} a^{\tilde{\tau}'}(x_2 \cdot \ldots \cdot x_n) \oplus t_2(x_1) \sum_{\tilde{\tau}' \in E^{n-1}} \gamma_{\tilde{\tau}'} b^{\tilde{\tau}'}(x_2 \cdot \ldots \cdot x_n),$$

где $\beta_{\tilde{\tau}'} = \alpha_{\tilde{\tau}}$ при $\tau_1 = 0$, $\gamma_{\tilde{\tau}'} = \alpha_{\tilde{\tau}}$ при $\tau_1 = 1$, $\tau' = (\tau_2, \ldots, \tau_n)$.

Пучок $(t_1, t_2) \in KH$, поэтому для него по теореме 3.10 выполняется:

$$f(\tilde{x}) = t_1(x_1) g_1(\tilde{x}') \oplus t_2(x_1) g_2(\tilde{x}'),$$

где $x' = (x_2, \ldots, x_n)$.

По теореме 3.10 для любых операторов t_1 и t_2 имеет место $g_1, g_2 \in \{f_{x_1}^0, f_{x_1}^1, f_{x_1}'\}$. Поэтому имеет место равенство:

$$L_{KH}(f) = \min\{L_{KH}(f_{x_1}^0) + L_{KH}(f_{x_1}^1),$$
$$L_{KH}(f_{x_1}^0) + L_{KH}(f_{x_1}'),\ L_{KH}(f_{x_1}^1) + L_{KH}(f_{x_1}')\} = 2^{n-1}.$$

Отсюда следует $L_{KH}(f_{x_1}^0) = L_{KH}(f_{x_1}^1) = L_{KH}(f_{x_1}') = 2^{n-2}$. Согласно индуктивному шагу имеем

$$\{f_{x_1}^0, f_{x_1}^1, f_{x_1}'\} \subset M_{n-1}^\diamond.$$

По предложению 3.19 окончательно получаем, что $f \in M_n^\diamond$. □

Сложность в диагональных формах.

Следующая теорема дает верхнюю оценку функции Шеннона диагональных форм.

Теорема 3.29. $L_{\mathrm{Diag}}(n) \leqslant \frac{1}{2} \cdot 2^n$.

Доказательство. Пусть A — однородный пучок. По определению этот пучок является диагональным.

Рассмотрим представление функция $f(x_1, \ldots, x_n)$ по пучку A по функции конъюнкции:

$$f(\tilde{x}) = \sum_{\tilde{\sigma} \in E^n} \alpha_{\tilde{\sigma}} \mathsf{a}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n), \quad L_{\mathsf{A}}(f) = \sum_{\tilde{\sigma} \in E^n} \alpha_{\tilde{\sigma}}.$$

Пусть $\tilde{\tau} = (\tau_1, \ldots, \tau_{n-2})$. Разобьем множество B^n на непересекающиеся подмножества $B^n = \bigcup\limits_{\tilde{\tau}} M_{\tilde{\tau}}$, где

$$M_{\tilde{\tau}} = \{\tilde{\mu}_{\tilde{\tau}}, \tilde{\nu}_{\tilde{\tau}}, \overline{\tilde{\mu}}_{\tilde{\tau}}, \overline{\tilde{\nu}}_{\tilde{\tau}}\}, \ \tilde{\mu} = (\tau_1, \ldots, \tau_{n-2}, 0, 0), \ \tilde{\nu} = (\tau_1, \ldots, \tau_{n-2}, 0, 1).$$

По определению однородного пучка A для любого $\tilde{\tau}$ существуют $\mathsf{c}^1 = \mathsf{a}^{\tilde{\mu}_{\tilde{\tau}}} \oplus \mathsf{a}^{\tilde{\nu}_{\tilde{\tau}}}$ и $\mathsf{c}^2 = \mathsf{a}^{\overline{\tilde{\mu}}_{\tilde{\tau}}} \oplus \mathsf{a}^{\overline{\tilde{\nu}}_{\tilde{\tau}}}$. Поэтому к пучку A применимо преобразование $\varphi_{\tilde{\mu}_{\tilde{\tau}}\tilde{\nu}_{\tilde{\tau}}}$ из предложения 3.16.

Рассмотрим

$$S = \sum_{\tilde{\sigma} \in M_{\tilde{\tau}}} \alpha_{\tilde{\sigma}}.$$

Для каждого $\tilde{\tau}$ определим преобразование $\psi_{\tilde{\tau}}$:

$$\psi_{\tilde{\tau}}(\mathsf{A}) = \begin{cases} \varphi_{\tilde{\mu}_{\tilde{\tau}}\tilde{\nu}_{\tilde{\tau}}}(\mathsf{A}), & \text{если } S \geqslant 3 \text{ и } \alpha_{\tilde{\mu}_{\tilde{\tau}}} = \alpha_{\overline{\tilde{\nu}}_{\tilde{\tau}}} = 1, \\ \varphi_{\tilde{\nu}_{\tilde{\tau}}\tilde{\mu}_{\tilde{\tau}}}(\mathsf{A}) & \text{если } S \geqslant 3 \text{ и } \alpha_{\overline{\tilde{\mu}}_{\tilde{\tau}}} = \alpha_{\tilde{\nu}_{\tilde{\tau}}} = 1, \\ \mathsf{A}, & \text{если } S \leqslant 2. \end{cases}$$

По предложению 3.15 пучок $\psi_{\tilde{\tau}}(\mathsf{A}) = \mathsf{B} = (\mathsf{b}^{\tilde{0}}, \ldots, \mathsf{b}^{\tilde{1}})$ — диагональный. Тогда имеется следующее разложение:

$$f(\tilde{x}) = \sum_{\tilde{\sigma} \in E^n} \beta_{\tilde{\sigma}} \mathsf{b}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n),$$

при этом

$$\sum_{\tilde{\sigma} \in M_{\tilde{\tau}}} \beta_{\sigma} \leqslant 2.$$

Последовательно применяя к пучку A преобразования $\psi_{\tilde{0}}, \ldots, \psi_{\tilde{1}}$, получим диагональный пучок:

$$\psi_{\tilde{0}}(\ldots(\psi_{\tilde{1}}(\mathsf{A}))\ldots) = \mathsf{C} = (\mathsf{c}^{\tilde{0}}, \ldots, \mathsf{c}^{\tilde{1}}).$$

Функция $f(\tilde{x})$ имеет по полученному пучку разложение:

$$f(\tilde{x}) = \sum_{\tilde{\sigma}\in E^n} \gamma_{\tilde{\sigma}} \mathsf{c}^{\tilde{\sigma}}(x_1 \cdot \ldots \cdot x_n),$$

в котором для любого $\tilde{\tau} = (\tau_1, \ldots, \tau_{n-2})$ имеем: $\sum\limits_{\tilde{\sigma}\in M_{\tilde{\tau}}} \gamma_{\tilde{\sigma}} \leqslant 2$.

Тогда $L_{\mathsf{C}}(f) = \sum\limits_{\tilde{\sigma}\in E^n} \gamma_\sigma = \sum\limits_{\tilde{\tau}\in E^n} \left(\sum\limits_{\tilde{\sigma}\in M_{\tilde{\tau}}} \gamma_{\tilde{\sigma}} \right) \leqslant \sum\limits_{\tilde{\tau}} 2 = \frac{1}{2} \cdot 2^n$.

Поскольку оценка получена для любой функции f, окончательно получим

$$L_{\mathrm{Diag}}(n) \leqslant \tfrac{1}{2} \cdot 2^n.$$

□

Комментарий. Первые результаты по представлениям булевых функций в виде полиномов были опубликованы И.И.Жегалкиным в работах 1928 и 1929 гг. [30, 31]. В них впервые в явном виде была введена и исследована каноническая форма, названная впоследствии «полиномом Жегалкина».

К середине пятидесятых годов широкое практическое применение получила теория кодирования. Исследования кодов привели к созданию в 1953 г. класса линейных кодов, основанных на полиноме Жегалкина. В работе Д.Маллера [37] были введены полиномиальные канонические формы, явившиеся теоретической основой для создания таких кодов, а в работе И.Рида [38] был разработан эффективный алгоритм декодирования. Коды получили название «кодов Рида–Маллера», а вместе с кодами введенные формы стали называться «формами Рида–Маллера». Формы Рида–Маллера расширяют класс полиномов Жегалкина, допуская вхождения переменной с отрицанием. Другое название таких представлений — поляризованные полиномы Жегалкина.

Обобщение класса поляризованных полиномов (форм Рида–Маллера с фиксированной полярностью) шло по двум направлениям. Первое направление — полиномы со смешанной полярностью, получившие название кронекеровских форм и их обобщение — псевдокронекеровские формы. Другое направление —

обобщенные формы Рида–Маллера, полиномы, в каждое слагаемое которых переменная может входить с отрицанием или без отрицания, независимо от остальных слагаемых. За подробной информацией по указанным каноническим формам мы отсылаем читателя к монографиям [35, 39].

В последнее десятилетие привлекли внимание полиномиальные формы, построенные с использованием операторов. Обзор по этой проблематике сделан в работе [25].

Построению и исследованию различных классов операторных полиномиальных форм посвящены работы [26, 27, 36, 28]. Естественно, рассматриваются далеко не все операторы в булевых функциях, более полное описание классов операторов булевых функций даны в [33].

Пучки, построенные из введенных операторов, позволили получить классы канонических форм, включившие в себя известные: поляризованные полиномы Жегалкина, различные формы Рида–Маллера, кронекеровские и т.д. Более того, оказалось возможным ввести естественным путем из свойств операторов широкий набор новых классов канонических форм, существенно отличающихся от указанных [36]. Причем этот класс операторов оказался полным в том смысле, что выход за этот класс сильно усложняет вид полиномов [23]. Введенные операторы позволили получить ряд частичных разложений, имеющих вид полиномов и обобщающих известные разложения [29].

Общие свойства операторных пучков позволили вывести формулы нахождения коэффициентов разложений для многих классов канонических форм: однородных [26], диагональных, расширенных однородных, неоднородных [27].

Точное значение функции Шеннона сложности булевых функций в классе поляризованных полиномов Жегалкина получено Н.А.Перязевым [34]. Введенные пучки операторов позволили получить оценки сложности функции Шеннона в классах: однородных операторных форм (откуда следует оценка для кронекеровских форм), расширенных однородных операторных форм, псевдокронекеровских форм, диагональных форм, неоднородных операторных форм [28, 22, 36].

Глава IV

Методы нахождения представлений частичных булевых функций

Одной из задач в теории булевых функций является задача о представлении функций термами над некоторым базисным множеством. При этом, как правило, термы должны удовлетворять определенным условиям. Одним из наиболее часто встречающимся условием является требование наименьшей сложности, где сложность определяется определенным образом. В частности, под сложностью может пониматься количество вхождений переменных в терм, или количество некоторых подтермов.

В практических приложениях находят применение частичные булевы функции, т.е. функции значения которых определены не обязательно на всех наборах значений переменных. Задача представления частичных булевых функций термами в классе термов над базисным множеством B состоит в нахождении по произвольно заданной частичной булевой функции f терма Φ над B такого, что на наборах на которых функция f определена, значения f и терма Φ совпадают.

Если функцию можно представить термом над базисным множеством и требуется найти терм минимальной сложности, то такая задача, как правило, не представляет теоретическую сложность. Достаточно перебирать все неэквивалентные между собой термы над базисным множеством по возрастанию сложности. При этом проверяется для каждого терма из этого перебора представляет ли он рассматриваемую функцию или нет. Так как функцию можно представить термом, то за конечное число шагов такое представление будет найдено. Первый полученный таким образом терм будет иметь наименьшую сложность. Существование переборного алгоритма носит только принципиальный характер, ввиду того, что этот алгоритм совершенно непригоден для практического применения, так как уже при малых размерностях (n=3, 4) возникает проблема полного пе-

ребора. Более того, для любого универсального алгоритма минимизации невозможно избежать этой проблемы [49].

Поэтому наряду с универсальными методами минимизации разрабатываются методы, учитывающие индивидуальные особенности минимизируемых функций и методы, позволяющие строить термы, которые не удовлетворяют всем поставленным условиям, но "достаточны близки" к ним, при этом можно ограничиться рассмотрением функций у которых количество переменных не превосходит некоторого фиксированного числа.

В этом разделе мы рассматриваем алгоритмы, позволяющие представлять булеву функцию в виде каскадных термов, а также в виде полиномиальных нормальных форм и которые имеют минимальную сложность в этих классах. Сложность в классе каскадных термов понимается как количество вхождений переменных, а в классе полиномиальных нормальных форм, как количество слагаемых.

Пусть $f(\tilde{x})$ — частичная булева функция. Ситуацию, что функция $f(\tilde{x})$ не определена на наборе $\tilde{\sigma}$, будем обозначать $f(\tilde{\sigma}) = *$. Через $L(\Phi)$ будем обозначать количество вхождений переменных в терм Φ. Количество слагаемых, входящих в полиномиальную форму F, будем обозначать через $L_{ПНФ}(F)$. Размерность функции иногда будем указывать явно — f^n.

§ 1. Метод разделительной декомпозиции

Распространенный метод нахождения представлений булевых функций бинарными термами — представление булевой функции $f(\tilde{x})$ в виде:

$$f(\tilde{x}) = h(\tilde{u}, \tilde{w}, g(\tilde{u}, \tilde{v})), \tag{4.1}$$

где $\tilde{u}, \tilde{v}, \tilde{w}$ — разбиение множества переменных $\tilde{x}$.

При этом ищется такое представление, чтобы $|\tilde{u}|$ было минимальным среди всех возможных вариантов. В качестве критерия существования такого представления можно использовать следующее утверждение.

Теорема 4.1. *Для любой частичной функции f следующие условия эквивалентны:*

1) *функция f допускает декомпозицию при разбиении множества аргументов на $\tilde{u}, \tilde{v}, \tilde{w}$;*

2) *для любого набора* $\tilde{\alpha}$ ($|\tilde{\alpha}| = |\tilde{u}|$) *функция* f *допускает доопределение такое, что среди всех остаточных функций от функции* $f_{\tilde{u}}^{\tilde{\alpha}}$ *по аргументам* $\tilde{v}$ *не более двух различных*;

3) *для любого набора* $\tilde{\alpha}$ ($|\tilde{\alpha}| = |\tilde{u}|$) *функция* f *допускает доопределение такое, что существует функция* t *такая, что любая остаточная функция от функции* $f_{\tilde{u}}^{\tilde{\alpha}}$ *по аргументам* $\tilde{w}$ *является либо константной, либо функцией* t, *либо* $\bar{t}$.

Доказательство этого утверждения аналогично доказательству теоремы 1.2. □

Если в представлении (4.1) множество $\tilde{u}$ является пустым, то метод называется методом разделительной декомпозиции. Реализация таких разложений может быть осуществлена различными методами и задача сводится к представлению функций g и h, которые являются, в некотором смысле, более простыми, например, имеют меньшую размерность. Далее к функциям g и h можно снова применить метод декомпозиции или любой другой известный метод в данном базисном множестве B. Если не учитывать особенностей базисного множества B, то задача сводится к представлению функций размерности два и получается представление функции бинарным термом.

Рассмотрим метод представления частичной булевой функции термами над базисным множеством B_0, используя разделительную декомпозицию:

$$f(\tilde{x}) = \overline{x}_i f_{x_i}^0(\tilde{x}_i) \vee x_i f_{x_i}^1(\tilde{x}_i),$$

где конъюнкция и дизъюнкция в случае неопределенности $*$ определяется следующим образом:

$$0 \vee * = *; 1 \vee * = 1; 0 \cdot * = 0; 1 \cdot * = *.$$

Если остаточные функции представляются константами, то подставляем их в это разложение, и рассматриваемая функция может быть доопределена до x_i или $\overline{x}_i$, в противном случае рассматриваем аналогичные представления для функций $f_{x_i}^0$ и $f_{x_i}^1$.

Так как с каждым представлением размерность функции уменьшается, то этот процесс прервется. В результате работы алгоритма получится терм над базисным множеством B_0.

Этот метод дает следующую верхнюю оценку для частичных булевых функций f, определенных на m наборах.

Предложение 4.1. *Пусть f — произвольная частичная булева функция, определенная на m наборах. Тогда можно найти бинарный терм Φ над B_0, представляющий f, такой что*

$$L(\Phi) \leqslant \tfrac{3}{2}m - 2.$$

Доказательство проведем индукцией по m.

Базис индукции. При $m = 2$ функция f представляется термом $\Phi = x_i^{\sigma_i}$ и

$$L(\Phi) = 1 = \tfrac{3}{2} - 2 = \tfrac{3}{2}m - 2.$$

Шаг индукции. Пусть функция f определена на $m \geqslant 2$ наборах и для всех функций, определенных менее чем на m наборах, утверждение предложения выполняется.

Пусть в разложении $f(\tilde{x}) = \overline{x}_i f^0_{x_i}(\tilde{x}_i) \vee x_i f^1_{x_i}(\tilde{x}_i)$ ровно одна функция доопределена до константы, тогда $f(\tilde{x}) = x_i^{\sigma_i} \vee f^{\overline{\sigma}}_{x_i}(\tilde{x}_i)$, где $f^{\overline{\sigma}}_{x_i}$ задана не более чем на $m-1$ наборах и представима термом Φ_i, и

$$L(\Phi) = 1 + L(\Phi_i) \leqslant 1 + \tfrac{3}{2}(m-1) - 2 < \tfrac{3}{2}m - 2.$$

Следующий случай, когда функции $f^0_{x_i}$ и $f^1_{x_i}$ не доопределимы до констант и заданы соответственно на m_0 и m_1 наборах, $m = m_0 + m_1$ и функции $f^0_{x_i}$ и $f^1_{x_i}$ представимы термами Φ_0 и Φ_1:

$$L(\Phi) = 2 + L(\Phi_0) + L(\Phi_1) \leqslant 2 + (\tfrac{3}{2}m_0 - 2) + (\tfrac{3}{2}m_1 - 2) = \\ = \tfrac{3}{2}(m_0 + m_1) - 2 = \tfrac{3}{2}m - 2. \quad \square$$

Отсюда для случая всюду определенных функций размерности n можно сформулировать следующее предложение.

Предложение 4.2. *Пусть f — произвольная булева функция размерности n. Тогда можно найти терм над B_0, представляющий f такой, что*

$$L(\Phi) \leqslant \tfrac{3}{2}2^n - 2.$$

Доказательство непосредственно следует из предыдущего предложения для случая $m = 2^n$. $\square$

§ 2. Алгоритм линейной минимизации функций

Определим класс каскадных термов K:

1) $0, 1$ есть термы класса K;

2) если x — переменная, то x^σ есть терм класса K $(\sigma \in E)$;

3) если Φ_1 и Φ_2 — термы класса K, то $(x^\sigma \star \Phi_1) \circ \Phi_2$ — терм класса K, где $\star, \circ \in \{\cdot, \vee, \oplus\}$.

Сложностью каскадного терма назовем количество вхождений переменных в терм.

Опишем алгоритм линейной минимизации булевых функций (ЛМБФ) с помощью которого можно найти терм, имеющий наименьшую сложность среди каскадных термов, представляющих рассматриваемую булеву функцию.

Минимизация называется линейной, так как в основе алгоритма лежат следующие линейные представления булевых функций:

$$
\begin{gathered}
f = (x_i \cdot f_{j_1}) \oplus f_{j_2}, \quad f = (\overline{x}_i \cdot f_{j_1}) \oplus f_{j_2}, \\
f = (x_i \vee f_{j_1}) \cdot f_{j_2}, \quad f = (\overline{x}_i \vee f_{j_1}) \cdot f_{j_2}, \\
f = (x_i \cdot f_{j_1}) \vee f_{j_2}, \quad f = (\overline{x}_i \cdot f_{j_1}) \vee f_{j_2}, \\
f = (x_i \oplus f_{j_1}) \cdot f_{j_2}, \quad f = (\overline{x}_i \oplus f_{j_1}) \cdot f_{j_2}, \\
f = (x_i \oplus f_{j_1}) \vee f_{j_2}, \quad f = (\overline{x}_i \oplus f_{j_1}) \vee f_{j_2}.
\end{gathered}
$$

На их основе рассматривается 18 возможных представлений (табл. 2). Функции f_i $(i = 0, ..., 21)$ определяются через остаточные функции $f^0_{x_i}$, $f^1_{x_i}$, и вид разложения зависит от множества пар значений остаточных функций на одинаковых наборах значений аргументов $\{(f^0_{x_i}(\tilde{\sigma}), f^1_{x_i}(\tilde{\sigma}))\}$.

Для каждого набора пар $\{(f^0_{x_i}(\tilde{\sigma}), f^1_{x_i}(\tilde{\sigma}))\}$ определены соответствующие разложения — от одного до пяти (табл. 3).

Предлагаемый алгоритм заключается в следующем. По аргументу x_i $(i \in \tilde{n})$ булевой функции $f(x_1, ..., x_n)$ находим множество пар $\{(f^0_{x_i}(\tilde{\sigma}), f^1_{x_i}(\tilde{\sigma}))\}$, и соответственно номер множества пар и номер группы в табл. 3.

Перебрав все аргументы, оставляем те, номера множества пар которых принадлежат группе с наименьшим номером.

Для каждого из оставшихся аргументов рассматриваем все разложения, соответствующие им по табл. 3.

При этом сначала рассматриваем те, которые имеют меньший номер.

Получаем разложение рассматриваемой функции по табл. 2 в виде $(x_i^{\sigma} \star f_{j_1}) \circ f_{j_2}$.

Значения функций f_{j_1} и f_{j_2} находятся с помощью табл. 4.

Таблица 2

№ разложения	Представление f	№ разложения	Представление f
1	$f = 0$	10	$f = \overline{x_i} \vee f_5$
2	$f = 1$	11	$f = (x_i \vee f_6) f_7$
3	$f = x_i$	12	$f = x_i f_8 \vee f_9$
4	$f = \overline{x_i}$	13	$f = (\overline{x_i} \vee f_{10}) f_{11}$
5	$f = f_0$	14	$f = \overline{x_i} f_{12} \vee f_{13}$
6	$f = x_i \oplus f_1$	15	$f = (x_i \oplus f_{14}) f_{15}$
7	$f = x_i f_2$	16	$f = (x_i \oplus f_{16}) \vee f_{17}$
8	$f = \overline{x_i} f_3$	17	$f = x_i f_{18} \oplus f_{19}$
9	$f = x_i \vee f_4$	18	$f = \overline{x_i} f_{20} \oplus f_{21}$

В табл. 4 на некоторых значениях $(f^0_{x_i}(\tilde{\sigma}), f^1_{x_i}(\tilde{\sigma}))$ функция f_j может принимать два различных значения, что изображается как τ_1/τ_2, где τ_1, τ_2 могут принимать значения 0, 1, $*$. Пусть в полученном представлении мы определяем значения функций f_{j_1} и f_{j_2} именно на таком наборе, f_{j_1} может принимать значения τ_{11}/τ_{12}, функция f_{j_2} может принимать значения τ_{21}/τ_{22}. Тогда необходимо рассмотреть следующие случаи:

1) f_{j_1} принимает значение τ_{11}, f_{j_2} принимает значение τ_{21};

2) f_{j_1} принимает значение τ_{12}, f_{j_2} принимает значение τ_{22}.

Если существует несколько таких наборов, то необходимо рассмотреть все варианты, т.е. если

$$f_{j_1} = (\tau_1, \tau_{21}/\tau_{22}, \tau_3, \ldots, \tau_{m-1}, \tau_{m1}/\tau_{m2}, \ldots, \tau_n),$$
$$f_{j_2} = (\sigma_1, \sigma_{21}/\sigma_{22}, \sigma_3, \ldots, \sigma_{m-1}, \sigma_{m1}/\sigma_{m2}, \ldots, \sigma_n),$$

то рассматриваем четыре разложения $(x_i^{\sigma_i} \star f_{j_1}) \circ f_{j_2}$:

$$f_{j_1} = (\tau_1, \tau_{21}, \ldots, \tau_{m1}, \ldots, \tau_n), \quad f_{j_2} = (\sigma_1, \sigma_{21}, \ldots, \sigma_{m1}, \ldots, \sigma_n),$$
$$f_{j_1} = (\tau_1, \tau_{22}, \ldots, \tau_{m2}, \ldots, \tau_n), \quad f_{j_2} = (\sigma_1, \sigma_{22}, \ldots, \sigma_{m2}, \ldots, \sigma_n),$$
$$f_{j_1} = (\tau_1, \tau_{21}, \ldots, \tau_{m2}, \ldots, \tau_n), \quad f_{j_2} = (\sigma_1, \sigma_{21}, \ldots, \sigma_{m2}, \ldots, \sigma_n),$$
$$f_{j_1} = (\tau_1, \tau_{22}, \ldots, \tau_{m1}, \ldots, \tau_n), \quad f_{j_2} = (\sigma_1, \sigma_{22}, \ldots, \sigma_{m1}, \ldots, \sigma_n).$$

Таблица 3

Группа множества пар	№ множества пар	$\{(f^0_{x_i}(\tilde{\sigma}), f^1_{x_i}(\tilde{\sigma}))\}$	№ разложений
I	1	(00), (0*), (*0), (**)	1
	2	(11), (1*), (*1), (**)	2
II	3	(01), (0*), (*1), (**)	3
	4	(10), (1*), (*0), (**)	4
III	5	(00), (11), (0*), (*0), (1*), (*1), (**)	5
IV	6	(01), (10), (0*), (*0), (1*), (*1), (**)	6
	7	(00), (01), (0*), (*0), (*1), (**)	7
	8	(00), (10), (0*), (*0), (1*), (**)	8
	9	(01), (11), (0*), (1*), (*1), (**)	9
	10	(10), (11), (*0), (1*), (*1), (**)	10
V	11	(00), (01), (0*), (*0), (1*), (*1), (**)	11,12,15 17,18
	12	(00), (10), (0*), (*0), (1*), (*1), (**)	13,14,15 17,18
	13	(01), (11), (0*), (*0), (1*), (*1), (**)	11,12,16 17,18
	14	(10), (11), (0*), (*0), (1*), (*1), (**)	13,14,16 17,18
VI	15	(00), (01), (11), (0*), (*0), (1*), (*1), (**)	11,12 17,18
	16	(00), (10), (11), (0*), (*0), (1*), (*1), (**)	13,14 17,18
	17	(00), (01), (10), (0*), (*0), (1*), (*1), (**)	15,17,18
	18	(01), (10), (11), (0*), (*0), (1*), (*1), (**)	16,17,18
VII	19	(00), (01), (10), (11), (0*), (*0), (1*), (*1), (**)	17,18

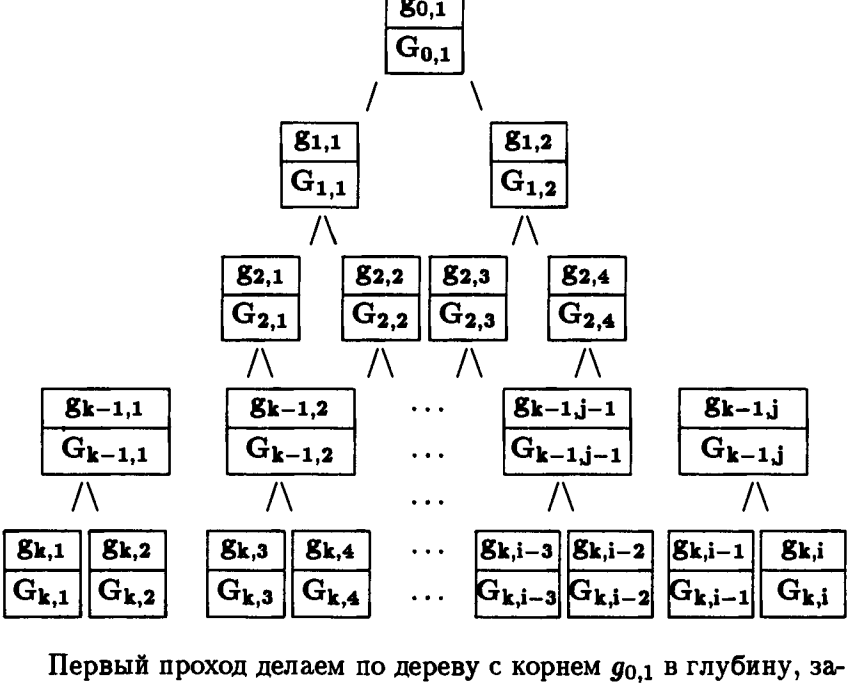
Аналогично для к таких наборов необходимо рассмотреть 2^* разложений.

На следующем шаге алгоритма повторяем все описанные действия для функций f_{j_1} и f_{j_2}. Продолжая процесс, получим представление f каскадным термом. Для каждой из функции f_j необходимо рассмотреть разложения по всем аргументам, множества пар которых принадлежат группе с наименьшим номером. Для каждого разложения необходимо рассмотреть все возможные функции. Сделав перебор всех возможных вариантов и выбрав терм с наименьшей сложностью, получим результат представления функции f алгоритмом ЛМБФ.

Таблица 4

$f^0_{x_i}(\sigma)f^1_{x_i}(\sigma)$	0 0	0 1	1 0	1 1	0 *	* 0	1 *	* 1	**
f_0	0	*	*	1	0	0	1	1	*
f_1	*	0	1	*	0	1	1	0	*
f_2	0	1	*	*	*	0	*	1	*
f_3	0	*	1	*	0	*	1	*	*
f_4	*	0	*	1	0	*	1	*	*
f_5	*	*	0	1	*	0	*	1	*
f_6	*	0	*	1	0/*	*	1	*	*
f_7	0	1	*	1	*/0	0	1	1	*
f_8	0	1	*	*	*	0	*	1/*	*
f_9	0	0	*	1	0	0	1	*/1	*
f_{10}	*	*	0	1	*	*/0	*	1	*
f_{11}	0	*	1	1	0	0/*	1	1	*
f_{12}	0	*	1	*	0	*	*/1	*	*
f_{13}	0	*	0	1	0	0	1/*	1	*
f_{14}	*	0	1	*	*/0	1/*	1	0	*
f_{15}	0	1	1	*	0/*	*/0	1	1	*
f_{16}	*	0	1	*	0	1	1/*	*/0	*
f_{17}	*	0	0	1	0	0	*/1	1/*	*
f_{18}	0	1	1	0	*	0/1	*	0/1	*
f_{19}	0	0	1	1	0	0/1	1	1/0	*
f_{20}	0	1	1	0	0/1	*	0/1	*	*
f_{21}	0	1	0	1	0/1	0	1/0	1	*

Представим процесс нахождения разложения в виде бинарного дерева из векторов функций f_{j_1}, f_{j_2} и термов их представляющих. В корне дерева функция $g_{0,1}$ (функция f), узлы дерева функции $g_{i,j}$ (функции f_{j_1}, f_{j_2}) определяемые по табл. 3 и соответствующие термы $G_{i,j}$ функций $g_{i,j}$ (подтермы терма, представляющего функцию f) определяемые по табл. 1 и 2.



Первый проход делаем по дереву с корнем $g_{0,1}$ в глубину, заполняем все дерево, для каждой функции рассматриваем первое возможное разложение.

В дереве будет $n = k + 1$ уровней, где n — количество переменных функции f. Каждый узел дерева имеет вес 0 или 1, т.е. увеличивает сложность терма f на 1 или не изменяет сложность. Сложность не увеличивается, если разложение принадлежит группе 1 или 3. Для всех остальных групп сложность увеличивается на 1.

Для того чтобы найти минимальный бинарный терм для произвольной функции f^n, согласно алгоритму имеющей представление $f^n = (x_i^{\sigma_i} \star f_1^{n-1}) \circ f_2^{n-1}$, необходимо найти минимальный бинарный терм для f_1^{n-1} и для f_2^{n-1}. Поэтому дерево с

корнем в f^n обрабатывается в симметричном порядке: сначала левое поддерево, а затем правое. Обработка дерева начинается с левого крайнего узла $(n-3)$-уровня, т.е. уровня функций от трех переменных. Для этой функции f_1^3 рассматриваются все варианты разложений, согласно алгоритму, обходя поддерево с корнем в этом узле в глубину и выбирая представление с наименьшей сложностью $L_{\text{мин}}(f_1^3)$. Для сокращения перебора используется метод ветвей и границ. Функция f_1^3 очевидно участвует в разложении некоторой функции $f_1^4 = (x_{i_1}^{\sigma_{i_1}} \star f_1^3) \circ f_2^3$, которая является ее предком в дереве. Следующим шагом необходимо сравнить сложность $L_{\text{мин}}(f_1^3)$ с текущей сложностью $L_{\text{тек}}(f_1^4)$.

Если $L_{\text{мин}}(f_1^3) < L_{\text{тек}}(f_1^4)$, то переходим к нахождению минимального бинарного терма для f_2^3 со сложностью $L_{\text{мин}}(f_2^3)$. Затем сравниваем текущую сложность f_1^4 в общем случае с $1 + L_{\text{мин}}(f_1^3) + L_{\text{мин}}(f_2^3)$ и если текущая сложность больше, то присваиваем ей новое значения и запоминаем вариант разложения. Если сложность не уменьшилась, сразу переходим к следующему разложению.

Если $L_{\text{мин}}(f_1^3) \geqslant L_{\text{тек}}(f_1^4)$, то переходим к рассмотрению следующего варианта разложения для f_1^4.

При переходе к следующему варианту разложения для функции в каком-то узле, поддерево с корнем в этом узле обходится в глубину и заполняется новыми функциями. Затем дерево с корнем в этом узле обрабатывается и так далее до тех пор пока не будут рассмотрены все варианты разложений для функции в этом узле. Таким образом, получаем минимальный терм со сложностью $L_{\text{мин}}(f_1^4)$. В свою очередь функция f_1^4 участвует в разложении

$$f_1^5 = (x_{i_2}^{\sigma_{i_2}} \star f_1^4) \circ f_2^4,$$

поэтому делаем следующий шаг.

Если $L_{\text{мин}}(f_1^4) < L_{\text{тек}}(f_1^5)$, то переходим к нахождению минимального бинарного терма для f_2^4 со сложностью $L_{\text{мин}}(f_2^4)$. Затем сравниваем текущую сложность f_1^5, в общем случае, с $1 + L_{\text{мин}}(f_1^4) + L_{\text{мин}}(f_2^4)$ и если текущая сложность больше, то присваиваем ей новое значения и запоминаем вариант разложения. Также для того, чтобы сократить переборы методом ветвей и границ, необходимо сделать сравнения текущей сложности f_1^5 с $1 + L_{\text{мин}}(f_1^4) + 1, \ldots 1 + L_{\text{мин}}(f_1^4) + 1 + L_{\text{мин}}(f_2^3)$. Если сложность не уменьшилась, сразу переходим к следующему разложе-

нию f_1^5, т.е. переписывается все поддерево с корнем в этом узле и повторяются описанные выше действия.

Если $L_{\text{мин}}(f_1^4) \geqslant L_{\text{тек}}(f_1^5)$, то переходим к рассмотрению следующего варианта разложения для f_1^5, т.е. переписывается все поддерево с корнем в этом узле и повторяются описанные выше действия.

Продолжая таким образом, делаем перебор всех возможных вариантов представлений и выбираем из них минимальное.

Продемонстрируем работу алгоритма на конкретном примере. Будем минимизировать функцию размерности три:

$$f(x_1, x_2, x_3) = (01110110).$$

По переменной x_1 остаточные функции:

$$f_{x_1}^0 = (0111), \quad f_{x_1}^1 = (0110).$$

Соответственно множество пар: $\{(00), (11), (10)\}$. По табл. 2 номер множества пар равен шестнадцати, а номер группы равен шести. Аналогично проверяем для x_2, x_3 и получаем, что для переменной x_2 номер множества пар равен восемнадцати, номер группы равен шести. Для переменной x_3 также соответственно получаем восемнадцать и шесть. Минимальный номер группы равен шести, ей принадлежат разложения по всем переменным, следовательно, необходимо рассмотреть разложения по всем переменным. По переменной x_1 в соответствии с табл. 2 будем рассматривать 13, 14, 17, 18 разложения, по переменным x_2 и x_4 необходимо рассмотреть 16, 17, 18 (см. табл. 1).

Ведем разложение номер 13 по переменной x_1:

$$f(x_1, x_2, x_3) = (\bar{x}_1 \vee g_{1,1}) \cdot g_{1,2}.$$

Согласно табл. 3 получаем

$$g_{1,1}(x_2, x_3) = (*110), \quad g_{1,2}(x_2, x_3) = (0111).$$

От $g_{1,1}$ по переменной x_2 остаточными функциями будут

$$(g_{1,1})_{x_2}^0 = (*1), \quad (g_{1,1})_{x_2}^1 = (10),$$

им соответствует множество пар: $\{(*1), (10)\}$. По табл. 2 номера множества пар и группы соответственно равны шести и четырем. По переменной x_3 аналогично. Минимальная группа —

четвертая. Для функции от двух переменных достаточно рассмотреть разложения по одной переменной. По переменной x_2 разложение, согласно таблицам 1 и 2, будет

$$g_{1,1}(x_2, x_3) = x_2 \oplus g_{2,1}.$$

По табл. 3 находим, что $g_{2,1}(x_3) = (01)$. По таблицам 2 и 3 получаем терм: $g_{2,1}(x_3) = x_3$.

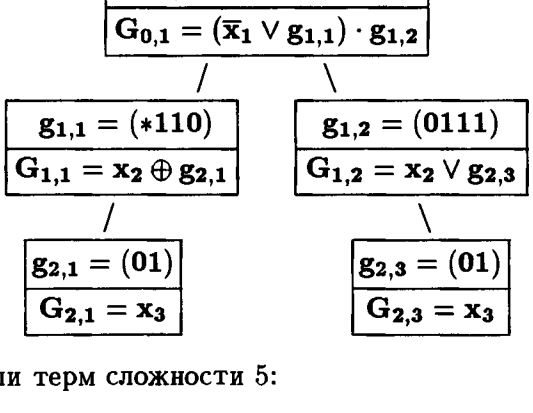
Вернемся к функции $g_{12}(x_2, x_3) = (0111)$, по переменным x_2 и x_3, согласно алгоритму, необходимо рассмотреть девятый номер множества пар из четвертой группы. По x_2 получаем

$$g_{1,2}(x_2, x_3) = x_2 \vee g_{2,3}.$$

Согласно таблицам 1, 2 и 3 находим вектор и терм:

$$g_{2,3}(x_3) = (01), \quad g_{2,3}(x_3) = x_3.$$

Представим описанные выше действия в виде дерева.



Получили терм сложности 5:

$$(\overline{x}_1 \vee (x_2 \oplus x_3)) \cdot (x_2 \vee x_3).$$

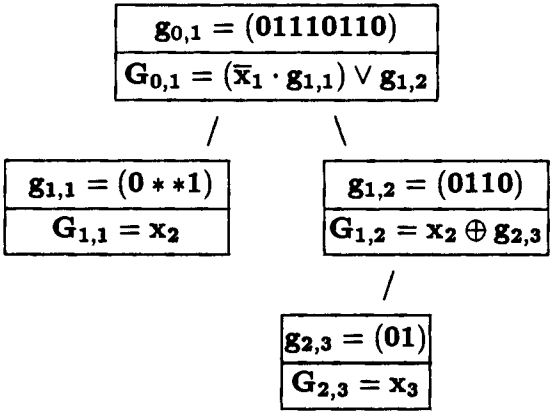
Запоминаем сложность и терм. На следующем шаге рассматриваем представление номер 14 функции $g_{0,1}$. Получаем терм

$$g_{0,1} = (\overline{x}_1 \cdot g_{1,1}) \vee g_{1,2},$$

где функции $g_{1,1}$ и $g_{1,2}$ имеют следующие представления векторами $g_{1,1}(x_2, x_3) = (0 * *1)$, $g_{1,2}(x_2, x_3) = (0110)$.

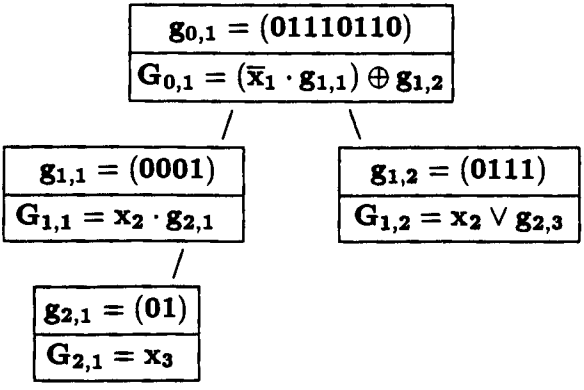
У функции $g_{1,1}$ по переменной x_2 остаточными функциями будут $(g_{1,1})^0_{x_2} = (0*)$ и $(g_{1,1})^1_{x_2} = (*1)$, им соответствует множество пар: $\{(0*), (*1)\}$, что, в свою очередь, соответствует третьему номеру во второй группе. По переменной x_3 аналогично. При разложении по x_2 получаем терм $g_{1,1} = x_2$. Функции $g_{1,2}$ по переменной x_2 соответствует шестое множество пар в четвертой группе, по x_3 также. Согласно алгоритму находим представление термом: $g_{1,2} = x_2 \oplus g_{2,3}$, где $g_{2,3}(x_3) = (01)$ и $g_{2,3} = x_3$.

Представим в виде дерева.



Получили терм сложности 4: $\overline{x}_1 \cdot x_2 \vee (x_2 \oplus x_3)$.

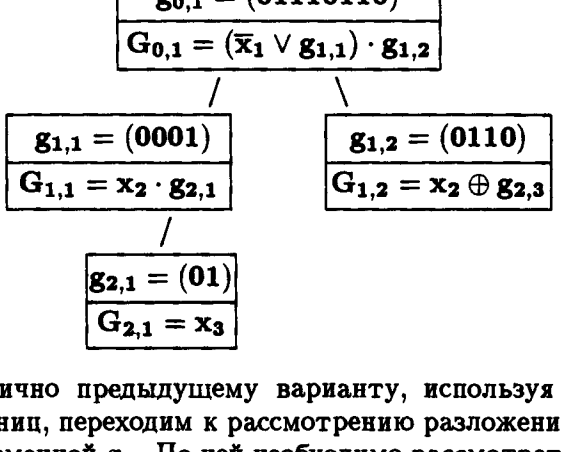
Снова возвращаемся к функции $g_{0,1}$, для рассмотрения следующего варианта разложения (номер семнадцать по переменной x_1):



Так как получается терм, сложность которого больше четырех: $(\overline{x}_1 \cdot (x_2 \cdot x_3)) \oplus x_2 \vee g_{2,3}$, то на этом шаге, согласно методу

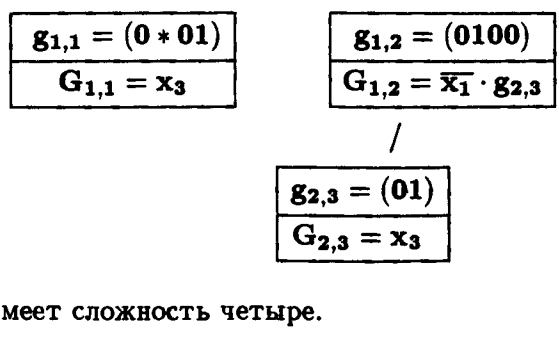
ветвей и границ, представление $g_{2,3}$ не рассматривается, а переходим к следующему разложению для $g_{0,1}$.

Рассмотрим последнее разложение $g_{0,1}$ по переменной x_1 (номер восемнадцать):



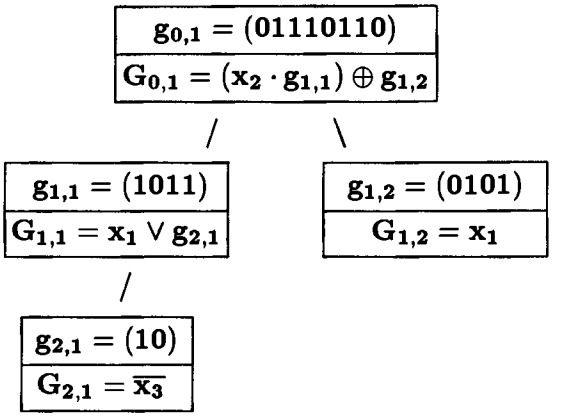
Аналогично предыдущему варианту, используя метод ветвей и границ, переходим к рассмотрению разложений функции $g_{0,1}$ по переменной x_2. По ней необходимо рассмотреть разложения номер 16, 17, 18. Процесс нахождения разложений, также как и в случае переменной x_1 будем сопровождать иллюстрациями в виде бинарных деревьев.

Рассмотрим разложение номер шестнадцать по переменной x_2.



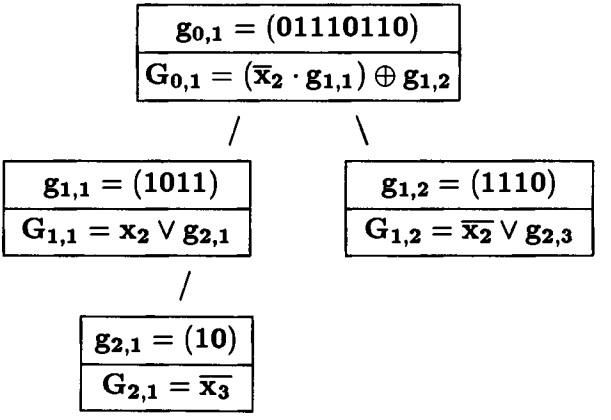
Терм имеет сложность четыре.

Рассмотрим разложение номер семнадцать по переменной x_2.



Терм имеет сложность четыре.

Рассмотрим разложение номер восемнадцать по переменной x_2.



Сложность терма больше четырех, поэтому процесс нахождения такого терма прерывается.

Рассмотрев для функции $g_{0,1}$ разложения по переменной x_3, убедимся что сложность не меньше четырех.

Все варианты рассмотрены. Минимальная сложность равна четырем. В качестве результата работы алгоритма берется первое представление, имеющее сложность четыре:

$$f = \overline{x}_1 \cdot x_2 \vee (x_2 \oplus x_3).$$

§3. Анализ и тестирование алгоритма ЛМБФ

Рассмотрев все возможные наборы $\{(f^0_{x_i}(\tilde{\sigma}), f^1_{x_i}(\tilde{\sigma}))\}$ несложно показать справедливость следующего утверждения.

Предложение 4.3. *Используя алгоритм ЛМБФ, любую булеву функцию можно представить термом класса K.*

С помощью алгоритма можно найти терм из класса K, который представляет рассматриваемую функцию и имеет наименьшую сложность. Но термы, получаемые алгоритмом, не всегда имеют наименьшую сложность в классе всех бинарных термов.

Существуют функции, сложность представления которых в классе всех бинарных термов меньше, чем сложность термов, полученных с использованием алгоритма ЛМБФ. В качестве такой функции можно взять следующую:

$$f = (x_1 \vee x_2) \cdot (x_3 \vee x_4) \vee (x_5 \vee x_6) \cdot (x_7 \vee x_8).$$

Так как функция существенная и бесповторная, то приведенное представление термом является минимальным. По теореме 2.2, в силу того, что функция бесповторная, это представление является единственным с точностью до коммутативности дизъюнкции и конъюнкции. Структура этого терма:

$$f = (f_1 \cdot f_2) \vee (f_3 \cdot f_4),$$

где f_i — неунарные функции.

По алгоритму ЛМБФ получаемые термы принадлежат классу K, и по крайней мере, одна из функций f_i должна быть унарной. Поэтому данный минимальный терм нельзя получить с помощью алгоритма. Используя алгоритм ЛМБФ, получаем терм сложности 10:

$$f = x_1 \cdot (x_3 \vee x_4) \vee x_2 \cdot (x_3 \vee x_4) \vee (x_5 \vee x_6) \cdot (x_7 \vee x_8).$$

Предложение 4.4. *Пусть f — произвольная частичная булева функция определенная на m наборах. Тогда, используя алгоритм ЛМБФ, можно найти терм Φ класса K над B_1, представляющий f такой, что*

$$L(\Phi) \leqslant m - 1.$$

Доказательство проведем индукцией по m.

Базис индукции. При $m = 1$ функция f эквивалентна константной функции, поэтому сложность равна 0. Соответственно выполняется равенство

$$L(\Phi) = 0 \leqslant 1 - 1 = m - 1.$$

Шаг индукции. Пусть функция f определена на $m \geqslant 2$ наборах и для всех функций, определенных менее чем на m наборах, утверждение теоремы выполняется. В этом случае доказательство заключается в проверке справедливости утверждения теоремы для всех разложений из табл. 1. Случаи 1–5 тривиальны.

Для разложений 6–10 по индуктивному предположению существуют термы Φ_i $(i = 1\text{–}5)$, представляющие функции f_i, которые определены менее чем на m наборах:

$$L(\Phi) = 1 + L(\Phi_i) \leqslant 1 + (m - 1) - 1 \leqslant m - 1.$$

Для разложений 11–18 по индуктивному предположению существуют термы Φ_i, Φ_j,

$$(i, j) \in \{(6,7), (8,9), (10,11), (12,13), (14,15), (16,17), (18,19), (20,21)\},$$

которые определены на m_i, m_j наборах, причем $m_i + m_j \leqslant m$. Отсюда получаем

$$L(\Phi) = 1 + L(\Phi_i) + L(\Phi_j) \leqslant 1 + m_i - 1 + m_j - 1 \leqslant (m_i + m_j) - 1 \leqslant m - 1.$$

□

Для оценки алгоритма были проведены следующие эксперименты:

– проведена минимизация всех функций от n переменных при $n \leqslant 4$

n	1	2	3	4
L_{aver}	0,5	1,5	3,3125	5
$L_{\max}$	1	2	6,3762	9

где L_{aver} — средняя сложность функций, $L_{\max}$ — наибольшая сложность.

– проведена минимизация случайно генерируемых частичных функций (для тестирования было случайно сгенерировано по 50 функции для каждого n)

n	3	4	5	6	7
L_{aver}	1,98	3,9412	7,7255	13,7059	31,5926
$L_{\max}$	4	6	12	18	38

Предложение 4.5. *Пусть f — произвольная булева функция размерности n, тогда, используя алгоритм, можно найти терм Φ класса K над B_1, представляющий f такой, что*

$$L(\Phi) \leqslant \tfrac{5}{8}2^n - 1.$$

Доказательство. Для разложений 1–18 в алгоритме выполняется неравенство:

$$L(\Phi) \leqslant 1 + 2L(\Phi_i),$$

где Φ представляет f, а Φ_i — f_i для некоторого $i \in \{1, \ldots, 21\}$. Учитывая, что любая функция размерности 4 имеет сложность не превосходящую 9, получим

$$L(\Phi) \leqslant 1 + 2 + \ldots + 2^{n-5} + 2^{n-4} \cdot 9 = 2^{n-4} - 1 + 9 \cdot 2^{n-4} = \tfrac{5}{8} \cdot 2^n - 1.$$

□

Приведем результаты применения алгоритма в сравнении с результатами, полученными другими алгоритмами.

Пример 1. (Функция Берхарда.) Минимизируем функцию

$$f = (00100011001100110010011111111111)$$

В результате работы алгоритма ЛМБФ получается терм, представляющий f сложности 7:

$$\Phi = (x_1 \vee x_4) \cdot (x_2 \vee (x_3 \vee \overline{x}_5) \cdot (x_4 \vee x_5)).$$

Отметим, что вынесением за скобки переменных из минимальной ДНФ получается терм сложности 8 [41].

Пример 2. Минимизируем функцию

$$f = (10000011100001010101001111011000).$$

Применением алгоритма ЛМБФ получаем терм, представляющий f сложности 13:

$$f = (\overline{x}_4 \cdot (\overline{x}_5 \cdot (x_2 \vee \overline{x}_1) \cdot (x_1 \vee \overline{x}_3) \vee \overline{x}_2 \cdot x_3)) \oplus (\overline{x}_2 \cdot x_3 \vee x_5 \cdot (x_1 \oplus x_3)).$$

В результате применения алгоритма из [46] получается терм сложности 30, а в [41] получен терм сложности 19.

Пример 3. Минимизируем функцию

$f = (00100000000010000100000000010000$
$00000000000110000100000000000110).$

Применяя алгоритм ЛМБФ, получаем терм представляющий f, сложности 14:

$$\Phi = (x_3 \oplus \overline{x}_4) \cdot (x_5 \oplus (x_6 \vee x_4 \cdot (\overline{x}_1 \vee \overline{x}_2))) \cdot$$
$$\cdot (\overline{x}_4 \cdot ((x_1 \oplus x_2) \vee x_2 \cdot x_6) \oplus (x_1 \vee \overline{x}_6)).$$

Терм, полученный в [46] разделительной декомпозиции, имеет сложность 36, а в [41] получен терм сложности 19.

Пример 4. Применим алгоритм ЛМБФ для минимизации порождающей функции настраиваемого модуля [40]. Точная постановка задачи: пусть дан список из k булевых функций, каждая из которых существенно зависит от n переменных:

$$f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n).$$

Требуется найти наиболее простой терм, представляющий функцию:

$$f = \bigvee_{i=1}^{k} y_1^{\sigma_{i1}} \cdot \ldots \cdot y_m^{\sigma_{im}} f_i(x_1, \ldots, x_n),$$

где m — число настроечных переменных, определяемое из соотношения: $m = \lceil \log_2 k \rceil$.

Применим алгоритм для минимизации порождающей функции модуля, который реализует три функции:

$$f_1 = x_1 \cdot x_2; f_2 = x_1 \vee x_2; f_3 = x_1 \oplus x_2.$$

Одномерная одноканальная однородная структура из таких модулей называется настраиваемые каскады Майтра. В [40] получен терм сложности 10. Используя те же настройки с помощью алгоритма ЛМБФ получим терм:

$$\Phi = (y_2 \oplus x_1 \cdot x_2 \cdot y_1) \cdot (x_1 \vee x_2),$$

сложность которого равна 6. Переменные y_1, y_2 — настроечные и при $y_1 = 1,\ y_2 = 0$ получаем $f = x_1 \cdot x_2$; при $y_1 = 0,\ y_2 = 1$ получаем $f = x_1 \vee x_2$; при $y_1 = 1,\ y_2 = 1$ получаем $f = x_1 \oplus x_2$.

Объединением каскадов Майтра получаются структуры, называемые обобщенными каскадами Майтра. Термы класса K непосредственно пригодны для реализации в таких каскадах.

§ 4. Методы нахождения полиномиальных представлений

В отличие от проблемы минимизации булевых функций в классе ДНФ, минимизация в классе ПНФ не сводится к решению задачи о покрытии, поскольку в минимальное представление могут входить члены, не являющиеся простыми импликантами. Поэтому приходится искать другие пути для решения этой проблемы, в частности приближенные методы, дающие не абсолютный минимум, а какой-то приемлимый результат.

В этом параграфе описывается метод нахождения минимальных представлений булевых функций в классе ПНФ. Основная идея метода заключается в следующем:

Предложение 4.6. *Любую булеву функцию $f(x_1, \ldots, x_n)$ можно представить в виде*

$$f(\tilde{x}) = \overline{x}_n \cdot h_1 \oplus h_2 \oplus x_n \cdot h_3,$$

причем если задана функция $h_1 = h(x_1, \ldots, x_{n-1})$, то функции h_2 и h_3 определяются следующими соотношениями: $h_2 = h \oplus f^0_{x_n}$, $h_3 = h \oplus f^0_{x_n} \oplus f^1_{x_n}$.

Доказательство. Достаточно провести несколько несложных преобразований:

$$\overline{x}_n \cdot h_1 \oplus h_2 \oplus x_n \cdot h_3 = \overline{x}_n \cdot h \oplus h \oplus f^0_{x_n} \oplus x_n \cdot (h \oplus f^0_{x_n} \oplus f^1_{x_n}) =$$

$$= \overline{x}_n \cdot f^0_{x_n} \oplus x_n f^1_{x_n} = f. \quad \square$$

Сложность разложения в предложении 4.6 равна сумме сложностей функций h_1, h_2, h_3. Легко видеть, что указанное разложение дает минимальную ПНФ при подходящем выборе h_1. Пусть в таком разложении имеются сокращения, например, в первом и втором слагаемых, т.е. слагаемые имеют минимальные ПНФ:

$$h_1 = F_1 \oplus \ldots \oplus F_k \oplus T;\ \ h_2 = G_1 \oplus \ldots \oplus G_s \oplus T.$$

Тогда при выборе $h_1 \oplus T$ вместо h_1 таких сокращений уже не будет. Аналогично находятся варианты и при наличии других сокращений.

Таким образом, если мы умеем находить сложности функций от $n-1$ переменной, то нахождение сложности любой функции от n переменных сведется к нахождению минимальной суммы сложностей функций h_1, h_2, h_3. Кроме этого, если мы имеем вместе со списком сложностей список минимальных ПНФ, то весьма легко получить и минимальную ПНФ для исследуемой функции.

Опишем алгоритм нахождения минимального представления функции $f(x_1, \ldots, x_n)$ в ПНФ. Пусть мы умеем находить минимумы функций от $n-1$ переменных с минимальными представлениями в ПНФ и сложностями этих представлений.

1. Выбираем функцию $(h_1 = h)$ от $n-1$ переменных и вычисляем ее сложность.

2. Вычисляем функции $h_2 = h \oplus f_x^0$, $h_3 = h_2 \oplus f_x^1$ и их сложности.

3. Складываем полученные сложности и получим сложность полученного представления $f(x)$ в ПНФ.

4. Повторяем предыдущие пункты для всех функций от $n-1$ переменной, выбирая функцию h с наименьшей сложностью $f(x)$.

5. Для найденных h_1, h_2, h_3 находим их формульное представления и по теореме 4.6 получаем представление F функции $f(x)$.

Полученная таким образом форма F будет минимальной по сложности $L_{\text{ПНФ}}(F)$ для функции $f(x)$.

Действительно, выбирая функции h_1, h_2, h_3 и их представление мы можем получить любое представление $f(x)$, так как любой терм, находящийся в ПНФ, можно разложить по предложению 3.17. Очевидно, что, выбирая минимальное представление h_1, h_2, h_3, мы получим сложность F, наименьшую для данной выбранной h. А так как мы выбираем среди всех возможных h, то мы получим абсолютный минимум $L_{\text{ПНФ}}(F)$.

Следовательно можно задавать одну из функций произвольно, при этом две оставшиеся будут полностью определяться значениями исходной функции и выбранной подфункции. Какая-то функция отвечает минимальному разложению исходной функции. Если теперь перебрать всевозможные варианты этой функции и подсчитать минимумы для каждого варианта, то там

окажется и абсолютный минимум. Проблема в том, что для функций уже от пяти переменных непосредственное нахождение минимума методом разложения с терминалом рекурсии для функции от одной переменной вызывает очень большой перебор. Для функций от шести переменных перебор становится необозримым.

Все вышеизложенное послужило доводом для создания приближенного метода нахождения минимума, не дающего гарантированно абсолютного минимума. В этом методе не перебираются все значения свободной функции, а вместо этого использовались несколько заранее определенных вариантов. При этом появилась возможность нахождения приближенного минимума для функций с числом переменных до 16. Следует отметить, что даже приближенные минимумы в классе полиномиальных форм очень часто оказываются лучше абсолютных минимумов в классе ДНФ при более высокой скорости нахождения. Разработанный алгоритм оказался пригодным и для работы с частично определенными функциями.

Алгоритм аналогичен описанному выше для нахождения представления функции в классе каскадных термов, поэтому ограничимся кратким изложением и демонстрацией примера. Если множество пар $\{(f^0_{x_i}(\tilde{\sigma}), f^1_{x_i}(\tilde{\sigma}))\}$ является подмножеством множества $\{(00), (0*), (*0), (**)\}$, то $f = 0$, если подмножеством множества $\{(11), (1*), (*1), (**)\}$, то $f = 1$. В остальных случаях применяем разложение

$$f = \overline{x}_i f_0 \oplus x_i f_1 \oplus f_*,$$

где f_0, f_1, f_* находятся по табл. 5.

Таблица 5

$\{(f^0_{x_i}(\tilde{\sigma}), f^1_{x_i}(\tilde{\sigma}))\}$	(00)	(01)	(10)	(11)	(0*)	(*0)	(1*)	(*1)	(**)
f_0	0/1	1/0	0/1	0/1	0/1	*	1/0	*	*
f_1	0/1	0/1	1/0	0/1	*	0/1	*	1/0	*
f_*	0/1	1/0	1/0	1/0	0/1	0/1	0/1	0/1	*

Дальнейшие рассуждения проводим для функций f_0, f_1, f_* аналогично описанным в § 3.

Продемонстрируем работу алгоритма на примере минимизации функции размерности три. Будем минимизировать функцию, для которой находили представляющий терм в классе каскадных термов: $f = (01110110)$. Так как функция всюду определена, то для нее необходимо рассмотреть шестнадцать вариантов представлений. По первой переменной остаточные функции:

$f^0_{x_1} = (0111)$ и $f^1_{x_1} = (0110)$.

$$f = \overline{x}_1 f_0 \oplus x_1 f_1 \oplus f_*,$$

где по первому варианту $f_0 = (0000), f_1 = (0001), f_* = (0111)$ согласно таблице. Функция f_0 равна нулю. Для функций f_1 и f_* необходимо рассмотреть по четыре варианта представлений.

От f_1 остаточными функциями будут: $(f_1)^0_{x_2} = (00)$, $(f_1)^1_{x_2} = (01)$. По первому варианту в разложении

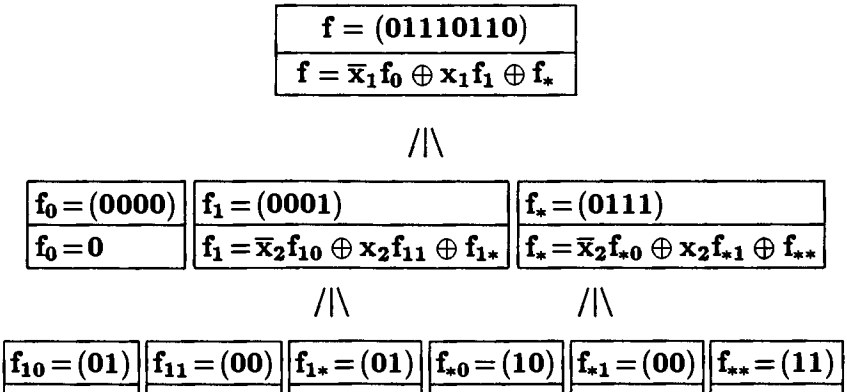
$$f_1 = \overline{x}_2 f_{10} \oplus x_2 f_{11} \oplus f_{1*},$$

функции имеют векторы: $f_{10} = (01), f_{11} = (00), f_{1*} = (01)$. От f_* остаточными функциями будут: $(f_*)^0_{x_2} = (01), (f_*)^1_{x_2} = (11)$. По первому варианту в разложении

$$f_* = \overline{x}_2 f_{*0} \oplus x_2 f_{*1} \oplus f_{**},$$

функции имеют векторы: $f_{*0} = (10), f_{*1} = (00), f_{**} = (11)$.

Представим описанные выше действия в виде дерева:



Текущая сложность функции f равна четырем, текущая сложность функции f_1 равна двум, текущая сложность функции f_* равна двум. Текущее представление:

$$f = x_1\overline{x}_2x_3 \oplus x_1x_2 \oplus \overline{x}_2\overline{x}_3 \oplus 1.$$

Согласно алгориту, для каждой функции предпоследнего уровня рассматриваем все варианты представлений:

$\mathbf{f = (01110110)}$
$\mathbf{f = \overline{x}_1 f_0 \oplus x_1 f_1 \oplus f_*}$

/|\

$\mathbf{f_0 = (0000)}$	$\mathbf{f_1 = (0001)}$	$\mathbf{f_* = (0111)}$
$\mathbf{f_0 = 0}$	$\mathbf{f_1 = \overline{x}_2 f_{10} \oplus x_2 f_{11} \oplus f_{1*}}$	$\mathbf{f_* = \overline{x}_2 f_{*0} \oplus x_2 f_{*1} \oplus f_{**}}$

/|\ /|\

$\mathbf{f_{10} = (10)}$	$\mathbf{f_{11} = (11)}$	$\times$
$\mathbf{f_{10} = \overline{x}_3}$	$\mathbf{f_{11} = 1}$	$\times$

$\mathbf{f_{*0} = (10)}$	$\mathbf{f_{*1} = (00)}$	$\mathbf{f_{**} = (11)}$
$\mathbf{f_{*0} = x_3}$	$\mathbf{f_{*1} = 0}$	$\mathbf{f_{**} = 1}$

$\mathbf{f_{10} = (00)}$	$\mathbf{f_{11} = (01)}$	$\mathbf{f_{1*} = (00)}$
$\mathbf{f_{10} = 0}$	$\mathbf{f_{11} = x_3}$	$\mathbf{f_{1*} = 0}$

$\mathbf{f_{*0} = (11)}$	$\mathbf{f_{*1} = (01)}$	$\times$
$\mathbf{f_{*0} = 1}$	$\mathbf{f_{*1} = x_3}$	$\times$

$\mathbf{f_{10} = (11)}$	$\times$	$\times$
$\mathbf{f_{10} = 1}$	$\times$	$\times$

$\mathbf{f_{*0} = (00)}$	$\mathbf{f_{*1} = (10)}$	$\mathbf{f_{**} = (01)}$
$\mathbf{f_{*0} = 0}$	$\mathbf{f_{*1} = \overline{x}_3}$	$\mathbf{f_{**} = x_3}$

На рисунке знаком $\times$ обозначается, что дальнейшее рассмотрение прерывается по методу ветвей и границ, так как сложность функции заведомо не будет улучшена. Минимальная сложность f_1 получилась равна единице. Минимальная сложность f_* равна двум. Текущая сложность f равна трем, что меньше первоначальной, запоминаем представление:

$$f = x_1x_2x_3 \oplus \overline{x}_2\overline{x}_3 \oplus 1.$$

Рассматриваем следующий вариант для функции f:

$f = (01110110)$
$f = \overline{x}_1 f_0 \oplus x_1 f_1 \oplus f_*$

/|\

$f_0 = (1111)$	$f_1 = (1110)$	$f_* = (1000)$
$f_0 = 1$	$f_1 = \overline{x}_2 f_{10} \oplus x_2 f_{11} \oplus f_{1*}$	$\times$

/|\

$f_{10} = (00)$	$f_{11} = (01)$	$f_{1*} = (11)$
$f_{10} = 0$	$f_{11} = x_3$	$f_{1*} = 1$

$f_{10} = (11)$	$f_{11} = (10)$	$\times$
$f_{10} = 1$	$f_{11} = \overline{x}_3$	$\times$

$f_{10} = (01)$	$f_{11} = (00)$	$f_{1*} = (10)$
$f_{10} = x_3$	$f_{11} = 0$	$f_{1*} = \overline{x}_3$

$f_{10} = (10)$	$f_{11} = (11)$	$\times$
$f_{10} = \overline{x}_3$	$f_{11} = 1$	$\times$

Аналогично рассматривая все шестнадцать вариантов, убеждаемся в том, что сложность минимальной ПНФ рассмотренной функции равна трем и искомое представление:

$$f = x_1 x_2 x_3 \oplus \overline{x}_2 \overline{x}_3 \oplus 1.$$

Понятно, что приведенный алгоритм требует большого перебора, но он допускает простые настройки по ограничению перебора (рассматривать не все виды определенния функций f_0, f_1, f_*). Поэтому этот алгоритм является базовым, общим методом для разработки приближенных алгоритмов.

Этот алгоритм можно настраивать на получение ПНФ функций из некоторого множества K выбором функций разложения f_0, f_1, f_*, получив эвристическую стратегию и ограничиваясь только теми вариантами разложений, которые приводят к более приемлемому результату.

Функции $f(\tilde{x})$ и $g(\tilde{x})$ называются *P-эквивалентными*, если:
a) $g(\tilde{x})$ получена из $f(\tilde{x})$ перестановками переменных;
b) если $f(\tilde{x}) = \overline{x} \cdot h_1 \oplus h_2 \oplus x \cdot h_3$,
то $g(\tilde{x})$ имеет одно из следующих шести представлений:

$$g(\tilde{x}) = \overline{x} \cdot h_1 \oplus h_2 \oplus x \cdot h_3,\ g(\tilde{x}) = \overline{x} \cdot h_1 \oplus h_3 \oplus x \cdot h_2,$$
$$g(\tilde{x}) = \overline{x} \cdot h_2 \oplus h_1 \oplus x \cdot h_3,\ g(\tilde{x}) = \overline{x} \cdot h_2 \oplus h_3 \oplus x \cdot h_1,$$
$$g(\tilde{x}) = \overline{x} \cdot h_3 \oplus h_1 \oplus x \cdot h_2,\ g = \overline{x} \cdot h_3 \oplus h_2 \oplus x \cdot h_1.$$

Несложно показать, что отношение P-эквивалентности является эквивалентностью и кроме того справедливо утверждение.

Предложение 4.7. *Если $f(\tilde{x})$ и $g(\tilde{x})$ принадлежат одному классу P-эквивалентности, то*

$$L_{\text{ПНФ}}(f) = L_{\text{ПНФ}}(g).$$

Доказательство. Пусть для функции f имеется минимальное представление $f = \overline{x} \cdot V_1 \oplus V_2 \oplus x \cdot V_3$. Рассмотрим представление эквивалентной функции:

$$g = \overline{x} \cdot V_1 \oplus V_3 \oplus x \cdot V_2.$$

Если это представление не минимальное, то пусть минимальное выглядит так:

$$g = \overline{x} \cdot T_1 \oplus T_3 \oplus x \cdot T_2.$$

Из двух представлений одной функции следует выполнение тождеств:

1) $V_1 \oplus V_3 = T_1 \oplus T_3$;

2) $V_3 \oplus V_2 = T_3 \oplus T_2$.

Из этих тождеств следует третье:

3) $V_1 \oplus V_2 = T_1 \oplus T_2$.

Из тождеств 2) и 3) следует, что для функции f имеется представление:

$$f = \overline{x} \cdot T_1 \oplus T_2 \oplus x \cdot T_3,$$

сложность которого меньше исходного. Это противоречит условию минимальности представления:

$$f = \overline{x} \cdot V_1 \oplus V_2 \oplus x \cdot V_3.$$

Доказательство остальных случаев аналогично рассмотренному. □

По предложению 4.6 для нахождения минимального представления функции $f = \overline{x} \cdot V_1 \oplus V_2 \oplus x \cdot V_3$ необходим полный перебор V_1. Введенная эквивалентность позволяет перебор функций заменить перебором классов.

Пусть G^n — множество представителей всех классов P-эквивалентности функций размерности n.

Предложение 4.8. *Для нахождения сложности $L_{\text{ПНФ}}(f)$ функции f, зависящей от $n+1$ аргумента, достаточно в классе P-эквивалентности функции f выбрать функцию g, имеющую наименьшую сложность представления*

$$g = \overline{x} \cdot V_1 \oplus V_2 \oplus x \cdot V_3,$$

по всем $V_1 \in G^n$.

Доказательство. Пусть для функции f найдено минимальное представление: $f = \overline{x} \cdot V_1 \oplus V_2 \oplus x \cdot V_3$.

Если $V_1 \notin G^n$, тогда пусть T — представитель класса эквивалентности функции V_1. Обозначим через φ преобразование, переводящее функцию в представителя класса: $\varphi(V_1) = T$.

Тогда и для функции f применим это преобразование:

$$\varphi(f) = \overline{x} \cdot T \oplus \varphi(V_2) \oplus x \cdot \varphi(V_3).$$

Функции f и $\varphi(f)$ — эквивалентны, их сложности совпадают, минимальное представление для $\varphi(f)$ найдено при $T \in G^n$. □

Согласно приведенному предложению для работы с функциями от n переменных достаточно хранить представителей классов функций от $n-1$ переменной.

В табл. 6 приведено сравнение числа классов и числа функций для 5-ти переменных.

Согласно таблице, число классов (а значит и число представителей) равно 6936, что занимает при хранении представителей, их сложностей и даже их минимальных представлений весьма незначительный объем. Естественно, что представители и их сложности должны быть вычислены заранее.

Таблица 6

Число слагаемых	Число классов	Число функций
0	1	1
1	1	243
2	4	24948
3	19	1351836
4	137	39365190
5	971	545193342
6	3572	2398267764
7	2143	1299295404
8	86	11460744
9	2	7824
Всего	6936	4294967296

Комментарии. Обсуждение возникающих принципиальных трудностей при решении проблем минимизации представлений булевых функций имеется в работе С.В. Яблонского [49]. Методы, основанные на полном переборе, возможны только для функций малой размерности (в связи с этим см. работы [44], [50]). Пример функции, которая при применении к ней алгоритма факторизации (т.е. вынесение за скобки переменных из нормальных форм) не представляется минимальным термом, приведен Берхардом [51]. Описание метода, основанного на декомпозиции функции, имеется в книгах [46], [48]. В работе [41] предложен алгоритм минимизации, основанный на композиционном и декомпозиционном анализе. Описание алгоритма линейной минимизации булевых функций (§2, 3) взято из работы [45].

Задача минимизации для нормальных форм булевых функций в подавляющем большинстве исследовалась в классе ДНФ. При этом задача минимизации в классе ПНФ значительно труднее алгоритмизуема, чем в классе ДНФ. Первые попытки исследовать задачу минимизации булевых функций в классе ПНФ сделаны в работах [47], [46]. Описанный в §4 алгоритм был предложен в работе [42]. Описание библиотеки минимиальных ПНФ приведено в работе [43].

Список литературы

К главе I

1. Дискретная математика и математические вопросы кибернетики/ Под ред. С.В. Яблонского и О.Б. Лупанова/– М: Наука, 1974.– Т.1.– 312 с.
2. *Лупанов О. Б.* Асимптотическая оценка сложности управляющих систем.– М.: Изд-во Московск. ун-та, 1984.– 137 с.
3. *Марченков С. С., Угольников А. Б.* Замкнутые классы булевых функций.– М.: Изд-во ИПМ АН СССР, 1990.– 147 с.
4. *Марченков С.С.* Замкнутые классы булевых функций.– М.: Физматлит, 2000.– 128 с.
5. *Нигматуллин Р.Г.* Сложность булевых функций.– М.: Наука, 1991.– 240 с.
6. *Перязев Н.А.* Основы теории булевых функций.– М.: Физматлит, 1999.– 112 с.
7. *Поваров Г.Н.* О функциональной разделимости булевых функций// ДАН СССР.– 1954.– Т. 94, № 5.– С. 801–803.
8. *Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б.* Функции алгебры логики и классы Поста.– М.: Наука, 1966.– 120 с.
9. *Яблонский С. В.* Введение в дискретную математику.– М.: Наука, 1986.– 384 с.

К главе II

10. *Гершкович Ю.Б., Полтерович В.М.* О бесповторных суперпозициях функций алгебры логики от двух переменных// Автоматика и телемех.– 1966.– С. 71–79.
11. *Гурвич В.А.* О бесповторных булевых функциях// Успехи матем. наук.– 1977.– 32, № 1.– С. 183–184.
12. *Гурвич В.А.* Критерий бесповторности функций алгебры логики// ДАН СССР.– 1991.– 318, № 3.– С. 532–537.
13. *Зубков О.В.* Формулы для нахождения числа бесповторных булевых функций в различных базисах// Тез. докл. XII Межд. конф. "Проблемы теоретической кибернетики". Часть I.– М.: Изд-во МГУ, 1999.– С. 83.

14. *Кириченко К.Д.* О критериях бесповторности булевых функций в различных базисах// Оптимизация, управление, интеллект.– 2000, № 4.– С. 186–192.

15. *Кузнецов А.В.* О бесповторных контактных схемах и бесповторных суперпозициях функций алгебры логики// Тр. матем. ин-та им. В.А.Стеклова.– 1958.– Т. 51.– С. 186–225.

16. *Перязев Н.А., Разгильдеев В.Г.* Число бесповторных булевых функций в бинарных базисах// Тез. докл. XI Межд. конф. по проблемам теоретической кибернетики.– Ульяновск, 1996.– С. 161–162.

17. *Перязев Н.А.* Реализация булевых функций бесповторными формулами// Дискр. матем.– 1995.–Т. 7, № 3.– С. 61–68.

18. *Перязев Н.А.* Реализация булевых функций бесповторными формулами в некоторых базисах // Сб. Алгебра, логика и приложения.– Иркутск, 1994.– С. 143–154.

19. *Риордан Дж.* Введение в комбинаторный анализ.– М.: ИЛ, 1963.– 287 с.

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

К главе III

21. *Аксаркисян Г.С.* Представление булевых функций суммой по модулю 2 импликацией аргументов// Автоматика и вычисл. техн.– 1977.– №1.– С. 8–11.

22. *Балюк А.С., Винокуров С.Ф.* Функция Шеннона для некоторых классов операторных полиномиальных форм // Оптимизация, управление, интеллект.– 2000.– Вып 5.– С. 167–180.

23. *Винокуров С.Ф. Перязев Н.А.* Полиномиальная декомпозиция булевых функций // Матем. заметки.– 1993.– Т. 53, вып. 2. – С. 25–29.

24. *Винокуров С.Ф. Перязев Н.А.* Разложение булевых функций на сумму произведений подфункций //Дискр. матем.– 1993.– Т. 5, вып. 3. – С. 102–104.

25. *Винокуров С.Ф. Перязев Н.А.* Полиномиальные разложения булевых функций // Киберн. и системный анализ.– 1993.– № 6.– С. 34-47.

26. *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.

27. *Винокуров С.Ф., Перязев Н.А.* Полиномиальные разложения булевых функций по образам неоднородных операторов // Киберн. и системный анализ.– 2000, № 4.– С. 40–55.

28. *Винокуров С.Ф.* Смешанные операторы булевых функций и их свойства // Тр. Иркут. ун-та. Серия: Дискр. матем. и информатика. Вып. 12.– Иркутск, 2000.– 36 с.

29. *Винокуров С.Ф.* Разложения булевых функций по собственным операторным образам и термам над бинарными функциями // Оптимизация, управление, интеллект.– 2000.– Вып 4.– С. 167–180.

30. *Жегалкин И.И.* Арифметизация символической логики // Матем. сборник.– 1928.– Т.35.– С.311–373.

31. *Жегалкин И.И.* Арифметизация символической логики // Матем. сборник.– 1929.– Т.36.– С.305–338.

32. *Мачикенас Э.К., Супрун В.П.* О полиномиальном разложении булевых функций.– Минск: Изд-во Белорусской АН.– 1988.– 31 с.

33. *Пантелеев В.И., Перязев Н.А.* Об операторах булевых функций// Труды XI Межгос. школы-семинара "Синтез и сложность управляющих систем". Нижний Новгород.– М.: Изд-во Московск. ун-та, 2000. – Часть II. – С. 141-146.

34. *Перязев Н.А.* Сложность булевых функций в классе полиномиальных поляризованных форм// Алгебра и логика.– 1995.– Т. 34, № 3.– С. 323–326.

35. *Fujita M. (Ed.)* Representations of Discrete Function. Kluwer Academic Publishers, 1996.– 450 p.

36. *Gaidukov A.I., Vinokurov S.F.* Operator polynomial expansions of Boolean functions / 4^{th} International Workshop on Boolean Problems. Freiberg, Germany, 2000.– P.63–69.

37. *Muller D.E.* Application of Boollean algebra to switching circuit desing and error detectio// IEEE Trans. Electron. Comput.– 1954.– V.3, No 3.– P. 6–12.

38. *Reed I.S.* A class of multiple-error-correcting codes and decoding scheme // IRE Trans. Inform. Theory.– 1954.– V. 4, N 9.– P. 38–49.

39. *Sasao T. (Ed.)* Logic Synthesis and Optimization. Kluwer Academic Publishers.– 1993.– 320 p.

К главе IV

40. *Артюхов В.Л., Копейкин Г.А., Шалыто А.А.* Настраиваемые модули для управляющих логических устройств.– Л.: Энергоиздат, 1981.– 166 с.

41. *Верзаков А.С.* Абсолютная минимизация логических функций. Челябинск. – 1983. – 30с. – Деп. ВИНИТИ №583-84.

42. *Винокуров С.Ф., Манцивода Ю.В., Перязев Н.А.* Минимизация булевых функций в классах нормальных форм методом разложения/ Фундаментальные пробл. матем. и механики. Математика.– М: Изд-во Московск. ун-та, 1994.– С. 316–317.

43. *Винокуров С.Ф., Гайдуков А.И., Корсуков А.В.* Библиотека классов булевых функций/ Сб. тр. Иркутск. ун-та.– Иркутск, 1995.– Т. 3.– С. 228–229.

44. *Казаков В.Д.* О скобочной минимизации выражений булевых функций// Duexime Congress Mathematique Hongrois.– Budapest, 1961.– V. 2.

45. *Манцивода Ю.В.* Алгоритм линейной минимизации булевых функций и его программная реализация. – Тр. Иркутск. ун-та. Серия: Дискр. матем. и информатика. Вып. 9.– Иркутск, 1999. – 25 с.

46. *Поспелов Д.А.* Логические методы анализа и синтеза схем.– М.: Энергия, 1974.– 368 с.

47. *Тошич Ж.* Полиномиальные представления булевых функций и их минимизация// Изв. АН СССР. Техн. киберн.– 1967.– № 3.– С. 141–143.

48. *Шоломов Л.А.* Основы теории дискретных логических и вычислительных устройств.– М.: Наука, 1980.– 400 с.

49. *Яблонский С.В.* Об алгоритмических трудностях синтеза минимальных контактных схем //Сб. Проблемы кибернетики. Вып.2.– М.: Физматгиз, 1959.– С.75-122.

50. *Abhyankar S.* Absolute minimal expressions of Boolean function./ IRE Tr. on EC., 1959. – V. EC-8, N 1.

51. *Burkhart W.H.* Theorem minimization. Pr. of the ACM Conference, 1952. – N 2, 3.

52. *Zakrevskij A.* Minimizing Polynomial Implementation of Weakly Specified Logic Functions and Systems// 3rd International Workshop on Applications of the Reed-Muller Expansion in Circuit Design, Sept. 19-20, 1997, Oxford.– Oxford, 1997.– P. 157–165.

Научное издание

БАЛЮК Александр Сергеевич
ВИНОКУРОВ Сергей Федорович
ГАЙДУКОВ Алексей Игоревич
ЗУБКОВ Олег Владимирович
КИРИЧЕНКО Константин Дмитриевич
ПАНТЕЛЕЕВ Владимир Иннокентьевич
ПЕРЯЗЕВ Николай Алексеевич
ПЕРЯЗЕВА Юлия Валерьевна

ИЗБРАННЫЕ ВОПРОСЫ ТЕОРИИ БУЛЕВЫХ ФУНКЦИЙ

Редактор Д.А. Миртова
Оригинал-макет: В.И. Пантелеев

ЛР № 071930 от 06.07.99
Подписано в печать 25.05.01. Формат 60×90/16.
Бумага офсетная №1. Печать офсетная.
Усл.печ.л. 12. Уч.-изд.л. 13.9. Тираж 1000 экз.
Заказ № 1659

Издательская фирма
«Физико-математическая литература»
117864 Москва, Профсоюзная ул., 90

Отпечатано с диапозитивов
в ППП «Типография «Наука»
121099, Москва, Шубинский пер., 6