**Московский государственный университет
имени М. В. Ломоносова**

Факультет вычислительной математики и кибернетики

С. А. Ложкин

Лекции по основам кибернетики

(вариант 2014 г., глава 1)

Москва 2014

Оглавление

Введение **4**

1 Представление функций дизъюнктивными нормальными формами и связанные с ним задачи **7**

§1 Основные понятия, относящиеся к множествам, матрицам, функциям, формулам 7

§2 Представление функций алгебры логики с помощью дизъюнктивных нормальных форм (ДНФ) и его «геометрическая» интерпретация. Совершенная ДНФ и разложение Шеннона, критерий единственности ДНФ 14

§3 Сокращенная ДНФ и способы ее построения . 23

§4 Тупиковые ДНФ, ядро и ДНФ пересечение тупиковых. ДНФ Квайна и ДНФ сумма тупиковых, критерий вхождения простых импликант в тупиковые ДНФ, его локальность 31

§5 Особенности ДНФ линейных и монотонных функций. Функция покрытия, таблица Квайна и построение всех тупиковых ДНФ 37

§6 Градиентный алгоритм и оценка длины градиентного покрытия. Использование градиентного алгоритма для построения ДНФ 44

§7 Задача минимизации ДНФ. Поведение функций Шеннона и оценки типичных значений для ранга и длины ДНФ 47
§8 Алгоритмические трудности минимизации ДНФ и оценки максимальных значений некоторых связанных с ней параметров. Теорема Ю. И. Журавлева о ДНФ сумма минимальных 52

Литература **59**

Введение

Курс «Основы кибернетики» (ранее «Элементы кибернетики»), создателем и основным лектором которого был чл.-корр. РАН С. В. Яблонский, читается на факультете ВМиК МГУ с первых лет его существования. В настоящее время он читается в 6–8 семестрах и является обязательным для всех бакалавров (интегрированных магистров) направления 01400 — «Прикладная математика и информатика». При этом объем и, в некоторой степени, программа курса «Основы кибернетики» варьируются в зависимости от профиля.

Курс «Основы кибернетики» посвящен изложению теории дискретных управляющих систем, которая представляет собой часть дискретной математики и математической кибернетики. В ней разрабатываются и изучаются дискретные математические модели, описывающие функционирование и структуру сложных систем преобразования информации (интегральных схем, программ и т. п.). В основе этих моделей лежат различные способы задания функционирования управляющих систем с помощью дискретных функций и их структурная реализация в тех или иных классах графов (классах схем). При исследовании управляющих систем ставятся и решаются две основные задачи: задача анализа и задача синтеза.

Задача анализа состоит в нахождении функционирования данной схемы, а задача синтеза — в построении схемы, имеющей (реализующей) заданное функционирование. Каждая из этих задач может рассматриваться либо как индивидуальная задача, и тогда ее решением является конкрет-

ное функционирование (схема), либо как массовая задача, и тогда ее решением должен быть алгоритм нахождения функционирования (схемы). Задача синтеза имеет, как правило, множество решений, из которых выбирают решение, оптимальное по какому-либо критерию. Чаще всего в качестве такого критерия выступает сложность схемы, понимаемая как сумма сложностей составляющих ее элементов или задержка схемы, понимаемая как максимальная сумма задержек для последовательно соединенных элементов схемы.

С содержательной точки зрения различные критерии оптимальности отражают различные параметры моделируемых электронных схем или программ. Так, например, сложность может характеризовать стоимость, размеры или потребляемую мощность СБИС, а также время выполнения программы на одном процессоре. При этом задержка схемы характеризует время срабатывания СБИС или время выполнения программы на параллельных процессорах и т. п.

Если задача синтеза решена в одной модели, можно пытаться перенести это решение в другие модели с помощью структурного моделирования. Кроме того, полученное решение можно «улучшить» с помощью эквивалентных преобразований. С другой стороны, если задача синтеза решена для одних функций, можно пытаться «разбить» (декомпозировать) новую функцию на уже рассмотренные и построить из синтезированных для них схем схему для новой функции с помощью операции суперпозиции.

Указанные выше задачи рассматриваются в лекциях для всех основных классов схем (дизъюнктивные нормальные формы, формулы и схемы из функциональных элементов, контактные схемы), а также для некоторых модификаций этих классов.

Первая глава посвящена различным вопросам представления функций алгебры логики с помощью таблиц и дизъюн-

ктивных нормальных форм (минимизация дизъюнктивных нормальных форм).

Вторая глава содержит описание структуры и функционирования схем из основных классов управляющих систем, а также из некоторых классов, представляющих собой их обобщения или модификации. В ней устанавливаются верхние оценки числа схем различных типов, рассматриваются особенности применения операции суперпозиции в различных классах схем и некоторые вопросы их структурного моделирования.

В третьей главе подробно рассматривается задача синтеза управляющих систем. В ней приводится целый спектр методов синтеза схем (от простейших до асимптотически оптимальных), устанавливаются нижние мощностные оценки функций Шеннона и оценки сложности ряда конкретных функций, доказывается минимальность некоторых схем.

В четвертой главе изучаются эквивалентные преобразования схем на основе тождеств во всех основных классах управляющих систем. Для каждого из них приводится система «основных» тождеств, доказывается полнота этой системы и изучаются вопросы ее избыточности.

В пятой главе представлены некоторые вопросы надежности и контроля схем (построение тестов для таблиц, синтез самокорректирующихся контактных схем).

Глава 1

Представление функций дизъюнктивными нормальными формами и связанные с ним задачи

§1 Основные понятия, относящиеся к множествам, матрицам, функциям, формулам

Будем считать известными основные понятия и обозначения из теории множеств, математического анализа, дискретной математики, теории вероятностей (см., например, [25, 26, 28, 4]). В дальнейшем через $\mathbb{N}$ (через $\mathbb{N}_0$) обозначается множество всех натуральных (соответственно целых неотрицательных) чисел. Множество всех целых чисел j, для которых $a \leqslant j \leqslant b$, где a, b — целые, называется *отрезком* и обозначается через

$$[a, b] = (a-1, b] = [a, b+1) = (a-1, b+1)\,.$$

При этом отрезки вида

$$[a_1, a_2)\,,\ [a_2, a_3)\,,\ \ldots,$$

где $a_1 < a_2 < a_3 < \ldots$, называются *последовательными.*

Напомним некоторые определения и обозначения, связанные с декартовыми произведениями множеств. Для множества A и $n \in \mathbb{N}$ положим

$$(A)^n = A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ раз}},$$

— n-я декартова степень A, то есть множество наборов (строк, слов, выборок) длины n с элементами (буквами) из A или, иначе, множество упорядоченных n-ок элементов множества A.

Для множества A и $s, n \in \mathbb{N}$ через $(A)^{s,n} = A^{s,n}$ обозначается множество матриц с s строками, n столбцами и элементами из A. При этом предполагается, что $A^n = A^{1,n}$, и что $A^{s,n}$ — n-я декартова степень множества $A^{s,1}$, элементы которого называются столбцами. Число столбцов (строк) матрицы M называется ее *длиной* (соответственно *высотой*). Для матрицы $M \in A^{s,n}$ и $I' \subseteq [1, s]$, $I'' \subseteq [1, n]$ через $M\langle I', I''\rangle$ (при $s = 1$ и $I' = \{1\}$ — через $M\langle I''\rangle$) обозначается ее подматрица, расположенная в строках с номерами из I' и столбцах с номерами из I''. Набор $\Delta = (\delta_1, \ldots, \delta_p)$, состоящий из непустых множеств, будем называть *покрытием* множества $\delta = \delta_1 \cup \ldots \cup \delta_p$. При этом множества $\delta_1, \ldots, \delta_p$ считаются *компонентами* покрытия Δ, а число p — его *длиной* или *рангом*. Покрытие, состоящее из непересекающихся множеств, называется *разбиением*. Покрытие, в котором ни одна из компонент не содержится в другой компоненте (в объединении остальных компонент), считается *неприводимым* (соответственно *тупиковым*) покрытием.

Если A — конечное множество, то его мощность, то есть число элементов, обозначается обычно через $|A|$. Заметим, что при этом

$$|A^n| = |A|^n \text{ и } |A^{s,n}| = |A|^{s \cdot n},$$

где $s, n \in \mathbb{N}$, а если $|A| = a \geqslant n$, то число выборок (слов) длины n из A, в которых все элементы различны, — так называемых выборок без повторений, — равно

$$a\,(a-1)\cdots(a-n+1)\,.$$

Каждое слово (набор) $\alpha = \alpha_1 \ldots \alpha_n = (\alpha_1, \ldots, \alpha_n)$ из A^n при всевозможных перестановках букв порождает множество слов, называемое *сочетанием* длины n из A или,

иначе, *неупорядоченной n-кой* из A, и обозначаемое через $\{\alpha_1, \ldots, \alpha_n\}$. В частности, сочетание, связанное с (упорядоченной) парой (u, v), считается неупорядоченной парой $\{u, v\}$, сочетание, связанное с (упорядоченным) разбиением $(\delta_1, \ldots, \delta_p)$, — неупорядоченным разбиением $\{\delta_1, \ldots, \delta_p\}$, и так далее. Заметим, что сочетание порождается перестановками букв из любого своего слова. При этом сочетание из A без повторений, то есть сочетание, порожденное словом из A^n, все буквы которого различны, с содержательной точки зрения представляет собой «обычное» подмножество, а сочетание с повторениями — «кратное» подмножество множества A, то есть подмножество, в которое его элементы входят с определенной кратностью (в соответствующем числе «экземпляров»).

Число различных сочетаний без повторений длины n из множества A, $|A| = a$, обозначается через $\binom{a}{n}$. Как известно (см., например, [28]),

$$\binom{a}{n} = \frac{a!}{n!\,(a-n)!} = \frac{a\,(a-1)\cdots(a-n+1)}{n!}, \tag{1.1}$$

а число сочетаний с (возможными) повторениями длины n из A равно $\binom{a+n-1}{n}$.

Индукцией по n легко показать, что

$$n! > \left(\frac{n}{3}\right)^n, \tag{1.2}$$

а из формулы Стирлинга [26] следует, что[1]

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}. \tag{1.3}$$

[1] Асимптотическое равенство $a\,(n) \sim b\,(n)$ означает, что $\lim\limits_{n\to\infty} \frac{a(n)}{b(n)} = 1$, то есть

$$a\,(n) = (1 + o\,(1))\, b\,(n)\,.$$

Из (1.1) и (1.2) вытекает, в частности, неравенство

$$\binom{a}{n} \leqslant \left(\frac{3a}{n}\right)^n, \tag{1.4}$$

а из (1.1) и (1.3) — асимптотическое равенство[1]

$$\binom{n}{\lceil \frac{n}{2} \rceil} \sim \frac{2^{n+1}}{\sqrt{2\pi n}}. \tag{1.5}$$

Напомним теперь некоторые понятия, связанные с функциями и отношениями. Пусть $x = (x_1, \ldots, x_n)$, где переменная x_i пробегает значения из множества A и связана с i-й компонентой, $i \in [1, n]$, декартовой степени A^n. Функцию f, определенную на множестве A^n и принимающую значения из множества D (множества A), будем называть *n-местной*, или, иначе, *n-арной функцией из множества A во множество D* (соответственно *над множеством A*) от переменных x и будем представлять ее в виде[2]

$$f = f(x)\,,\ f:\ A^n \longrightarrow D \quad (\text{соответственно } f : A^n \longrightarrow A)\,.$$

При этом в случае $D = B = \{0, 1\}$ функция f считается *отношением над множеством A*, а запись $f(a)$ $(\overline{f(a)})$, где $a = (a_1, \ldots, a_n) \in A^n$, означает, что компоненты набора a находятся (соответственно не находятся) в отношении f, то есть $f(a) = 1$ (соответственно $f(a) = 0$).

Для бинарных отношений, то есть отношений от двух переменных, обычным образом определяются свойства рефлексивности, транзитивности, симметричности и антисимметричности. Отношение, обладающее свойствами рефлексивности, симметричности и транзитивности, будем, как обычно, называть отношением эквивалентности. Напомним, что

[1] Через $\lceil \alpha \rceil$ ($\lfloor \alpha \rfloor$) обозначается ближайшее к α сверху (соответственно снизу) целое число

[2] Функцию f от переменных x_1, x_2 будем, как обычно, представлять в виде $(x_1 f x_2)$.

отношение эквивалентности τ, заданное на множестве A, порождает разбиение этого множества на классы τ-эквивалентности — максимальные по включению подмножества множества A, состоящие из попарно τ-эквивалентных элементов. Примером отношения эквивалентности является отношение *перестановочности* на множестве A^n, в котором слова α' и α'' находятся тогда и только тогда, когда α'' можно получить из α' в результате перестановки букв. Заметим, что классами эквивалентности по этому отношению являются сочетания с повторениями.

Отношение, обладающее свойствами рефлексивности, транзитивности и антисимметричности, будем, как обычно, называть отношением *частичного порядка*. Если τ — отношение частичного порядка на множестве A, то пару (A, τ) будем называть *частично упорядоченным множеством*. В том случае, когда в частично упорядоченном множестве (A, τ) любые два элемента a' и a'' из A сравнимы, то есть либо $a'\tau a''$, либо $a''\tau a'$, пару (A, τ) будем считать *линейно упорядоченным множеством*. Предполагается, что все элементы конечного линейно упорядоченного множества (A, τ), где $|A| = t$, пронумерованы числами отрезка $[0, t)$ так, что для любых a' и a'' из A номер a' не больше, чем номер a'' тогда и только тогда, когда $a'\tau a''$.

Под дискретной функцией понимают, обычно, отображение одного конечного множества в другое. Так, функция над отрезком $[0, k)$, где $k \geqslant 2$, называется *функцией k-значной логики* (при $k = 2$ — *алгебры логики*), а множество всех таких функций обозначается через P_k. Дискретные функции, как правило, могут быть описаны таблицами. Так, бинарная функция $f(x_1, x_2)$ из конечного линейно упорядоченного множества $A = \{a_1, \ldots, a_m\}$ в конечное множество D может быть задана матрицей M, $M \in D^{m,m}$, где $M\langle i, j\rangle = f(a_i, a_j)$ при всех i, j из отрезка $[1, m]$, и обратно.

Пусть $\mathcal{X} = \{x_1, x_2, \ldots, x_n, \ldots\}$ — счетный упорядоченный

алфавит переменных над множеством A и пусть $\mathcal{P}_A = \mathcal{P}_A(\mathcal{X})$ — множество всех функций над A от переменных из $\mathcal{X}$. Переменная x_i, $i \in [1, n]$, называется *несущественной переменной функции* $f(x_1, \ldots, x_n)$ из $\mathcal{P}_A$, если $f(\alpha) = f(\beta)$ для любых отличающихся только по x_i наборов α и β из A^n. В противном случае переменная x_i называется *существенной* переменной функции f. Считается, что функция f существенно (несущественно) зависит от переменной x_i, если x_i — существенная (соответственно несущественная) переменная функции f. Несущественная переменная не влияет на значение функции, поэтому, как обычно, равенство функций будем рассматривать с точностью до добавления или изъятия несущественных переменных. При этом две функции считаются *равными*, если они имеют одни и те же существенные переменные и одинаковым образом отображают декартову степень A, связанную с их существенными переменными, в A. Будем говорить, что f — *существенная* функция, если она существенно зависит от всех своих переменных.

Предполагается, что у нас имеется счетный алфавит функциональных символов (ФС) для обозначения функций из $\mathcal{P}_A$ и что в $\mathcal{P}_A$ выделено «базисное» множество Б. Дадим индуктивное определение формулы над Б и реализуемой ею функции, которое, в отличие от [28], неявно предполагает наличие в Б функции, тождественно равной переменной. Заметим, что с содержательной точки зрения формула представляет собой слово, построенное из ФС «базисных» функций, символов переменных и «разделителей», которое задает последовательность выполнения операций суперпозиции.

Любая переменная x_j из $\mathcal{X}$ считается *формулой глубины* 0 *над множеством* Б, которая реализует функцию x_j. Если $\varphi(x_1, \ldots, x_k) \in$ Б и для каждого i, $i \in [1, k]$, определена формула $\mathcal{F}_i$ глубины q_i над множеством Б, которая реали-

зует функцию f_i из $\mathcal{P}_A$, то запись $\mathcal{F}$ вида

$$\mathcal{F} = \varphi\left(\mathcal{F}_1, \ldots, \mathcal{F}_k\right) \tag{1.6}$$

является *формулой глубины* $q = \max\{q_1, \ldots, q_k\} + 1$ *над* Б, которая реализует функцию f вида $f = \varphi\left(f_1, \ldots, f_k\right)$. Все записи, полученные в результате указанного индуктивного построения, и только они считаются *формулами над множеством* Б. При этом формулы, полученные в процессе индуктивного построения формулы $\mathcal{F}$, называются ее *подформулами*, а те подформулы $\mathcal{F}_1, \ldots, \mathcal{F}_k$, из которых на последнем шаге индуктивного построения строится формула $\mathcal{F}$ вида (1.6), считаются ее *главными* подформулами. Под *сложностью* (*рангом*) формулы $\mathcal{F}$ понимается число вхождений в нее ФС (соответственно символов переменных), которое обозначается через $L\left(\mathcal{F}\right)$ (соответственно $R\left(\mathcal{F}\right)$).

Формулы $\mathcal{F}'$ и $\mathcal{F}''$, реализующие равные функции f' и f'', называются *равными* или, иначе, *эквивалентными*. При этом равенство вида $t: \ \mathcal{F}' = \mathcal{F}''$ считается *тождеством*. Обычным образом вводятся тождества, характеризующие свойства коммутативности, ассоциативности и дистрибутивности бинарных функций из $\mathcal{P}_A$.

Множество всех функций, реализуемых формулами над Б, называется *замыканием* множества Б. При этом множество Б считается *полным*, если его замыкание совпадает с $\mathcal{P}_A$. В дальнейшем любое конечное полное в $\mathcal{P}_A$ базисное множество Б будем называть *базисом*. При этом, в отличие от [28], в Б могут присутствовать ФАЛ, при удалении которых оставшееся множество продолжает быть полным.

§2 Представление функций алгебры логики с помощью дизъюнктивных нормальных форм (ДНФ) и его «геометрическая» интерпретация. Совершенная ДНФ, критерий единственности ДНФ

Множество B^n, где $B = \{0, 1\}$ и $n \in \mathbb{N}$, то есть множество наборов длины n из 0 и 1, обычно называют *единичным кубом* или *гиперкубом* размерности n. Отношение перестановочности разбивает куб B^n на классы эквивалентности (сочетания) B_0^n, B_1^n, $\ldots$, B_n^n, где B_i^n, $i \in [0, n]$, — так называемый i-й слой куба B^n, то есть множество наборов с i единицами, и, очевидно, $|B_i^n| = \binom{n}{i}$.

На множестве B^n введем отношение лексикографического линейного порядка, которое задается взаимно однозначным отображением (нумерацией) $\nu : B^n \to [0, 2^n)$ таким, что

$$\nu(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{n} \alpha_i 2^{n-i}.$$

Заметим, что двоичная запись числа $\nu(\alpha)$, $\alpha \in B^n$, дополненная слева нулями до набора длины n, совпадает с α. Аналогичным образом вводится лексикографический порядок на множестве $([0, k))^n$ при $k > 2$. Множество наборов, являющееся образом отрезка $[a, b]$, где $[a, b] \subseteq [0, 2^n)$, при отображении ν^{-1}, называется *отрезком куба* B^n.

Для наборов α, β из B^n через $\rho(\alpha, \beta)$ обозначается так называемое расстояние Хэмминга между ними, то есть число тех разрядов, в которых они отличаются друг от друга. При этом наборы, находящиеся на расстоянии n, называются *противоположными*, а наборы, отличающиеся только в одном (i-м) разряде, считаются *соседними* (соответственно *соседними по i-й переменной*). При геометрическом изображении куба B^n на плоскости вершины i-го слоя обычно располагаются на одном и том же горизонтальном уровне над

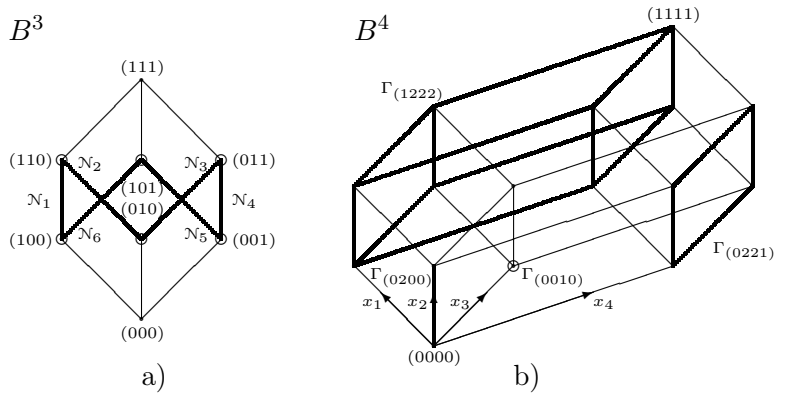

Рис. 2.1: B^3 и B^4, примеры граней

вершинами $(i-1)$-го слоя, $i = 1, \ldots, n$, а соседние вершины соединяются отрезками прямых (см. рис. 2.1). Множество наборов куба B^n, находящихся на расстоянии t (не больше, чем t) от набора α, называется *сферой* (соответственно *шаром*) *радиуса* t *с центром* α. Заметим, что i-й слой куба B^n является сферой радиуса i с центром в наборе $\widetilde{0} = (0, \ldots, 0)$ и сферой радиуса $(n-i)$ с центром в наборе $\widetilde{1} = (1, \ldots, 1)$.

На множестве B^n обычным образом введем отношение частичного порядка $\leqslant$ такое, что

$$\alpha = (\alpha_1, \ldots, \alpha_n) \leqslant \beta = (\beta_1, \ldots, \beta_n)$$

тогда и только тогда, когда $\alpha_i \leqslant \beta_i$ при всех $i \in [1, n]$. При этом считается, что $\alpha < \beta$, если $\alpha \leqslant \beta$ и $\alpha \neq \beta$, а наборы α, β из B^n, для которых $\alpha \leqslant \beta$ или $\beta \leqslant \alpha$ ($\alpha \nleqslant \beta$ и $\beta \nleqslant \alpha$), называются *сравнимыми* (соответственно *несравнимыми*).

Для набора $\gamma = (\gamma_1, \ldots, \gamma_n)$ длины n над множеством $[0, 2]$ через Γ_γ обозначим множество всех тех наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$ куба B^n, для которых $\alpha_i = \gamma_i$ при всех $i \in$

x_1	0	$\overline{x}_1$	x_1	1
0	0	1	0	1
1	0	0	1	1

a)

x_1	x_2	&	$\vee$	$\oplus$	$\sim$	$\rightarrow$	$\mid$	$\downarrow$
0	0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	1	0	0	1	0
1	1	1	1	0	1	1	0	0

b)

$\widetilde{\alpha}_f$	название функции f
(00)	— "0" (константа нуль)
(11)	— "1" (константа единица)
(01)	— тождественная функция
(10)	— отрицание
(0001)	— конъюнкция (умножение)
(0111)	— дизъюнкция
(0110)	— сумма по модулю 2
(1001)	— эквивалентность
(1101)	— импликация
(1110)	— штрих Шеффера
(1000)	— стрелка Пирса

c)

Рис. 2.2: $P_2\,(1)$ и «основные» ФАЛ из $P_2\,(2)$

$[1, n]$ таких, что $\gamma_i \neq 2$. Множество Γ_γ называется *гранью* куба B^n, число $(n-r)$, равное числу "2" в наборе γ, считается *размерностью* этой грани, а число r — ее *рангом*. Заметим, что указанная грань Γ_γ представляет собой подкуб размерности $(n-r)$ куба B^n и состоит из 2^{n-r} наборов, отличающихся друг от друга только в тех разрядах, в которых расположены символы "2" набора γ. В частности, грань размерности 0 представляет собой вершину куба, грань размерности 1 — его ребро, грань размерности 2 — квадрат, и так далее. Так, на рис. 2.1 в кубе B^3 выделены ребра $\mathcal{N}_1, \ldots, \mathcal{N}_6$, а в кубе B^4 выделены грани $\Gamma_{(0010)}$, $\Gamma_{(0200)}$, $\Gamma_{(0221)}$ и $\Gamma_{(1222)}$ размерностей 0, 1, 2 и 3 соответственно. Легко видеть, что грань Γ_γ ранга $(n-r)$ в кубе B^n, где $\gamma = (\alpha, 2, \ldots, 2)$ и $\alpha \in B^{n-r}$, соответствует отрезку куба длины 2^r, а множество всех граней указанного вида образует разбиение B^n на последовательные отрезки.

Будем, как обычно, предполагать, что у нас имеется счетный упорядоченный алфавит булевых переменных (БП) $\mathcal{X} = \{x_1, x_2, \ldots, x_n, \ldots\}$, и будем рассматривать функции алгебры логики (ФАЛ), или, иначе, булевы функции от переменных из $\mathcal{X}$, а множество всех таких функций будем обозначать через $P_2(\mathcal{X})$, или P_2. Будем предполагать также, что каждый рассматриваемый n-мерный куб имеет вид $B^n = B^n(X)$, где множество переменных $X = \{x_{j_1}, \ldots, x_{j_n}\} \subset \mathcal{X}$ и $j_1 < \cdots < j_n$, причем переменная x_{j_i} для всех $i \in [1, n]$ связана с i-м разрядом куба $B^n(X)$. Множество всех функций алгебры логики $f(x_{j_1}, \ldots, x_{j_n})$, отображающих куб $B^n(X)$ в B, будем обозначать через $P_2(X)$, а его m-ю декартову степень, то есть множество систем вида $F = (f_1, \ldots, f_m)$, состоящих из m таких функций, — через $P_2^m(X)$. Как правило, мы будем выделять из $\mathcal{X}$ множество БП $X(n) = \{x_1, \ldots, x_n\}$, где $n \in \mathbb{N}$, будем сопоставлять ему набор БП $x(n) = (x_1, \ldots, x_n)$ и будем рассматривать множество ФАЛ $P_2(n) = P_2(X(n))$, а также его степени $P_2^m(n) = P_2^m(X(n))$.

Для задания ФАЛ f из $P_2(n)$ можно использовать ее таблицу значений, то есть матрицу M из множества $B^{2^n,n+1}$, i-я строка, $i \in [1, 2^n]$, которой имеет вид

$$M\langle i, [1, n+1]\rangle = (\alpha, f(\alpha)),$$

где $\nu(\alpha) = i - 1$. При этом столбец $M\langle [1, 2^n], n+1\rangle$, однозначно задающий ФАЛ f, считается ее столбцом значений и обычно записывается в виде транспонированной строки, обозначаемой через $\widetilde{\alpha}_f$. Отсюда следует, в частности, что $|P_2(n)| = 2^{2^n}$. На рис. 2.2a (2.2b) приведены таблицы всех (соответственно «основных») ФАЛ от БП x_1 (соответственно x_1, x_2), а на рис. 2.2c перечислены столбцы значений $\widetilde{\alpha}_f$ и названия для всех указанных ФАЛ. Столбец значений ФАЛ f из $P_2(n)$ при любом $k \in [1, n)$ можно записать в виде прямоугольной таблицы (матрицы) длины 2^k и высоты 2^{n-k}, i-я строка которой, $i \in \left[1, 2^{n-k}\right]$, имеет вид

$$\widetilde{\alpha}_f\left\langle\left((i-1)\,2^k, i2^k\right]\right\rangle.$$

Кроме того, ФАЛ f однозначно определяется своим *характеристическим множеством*, которое состоит из всех наборов $\alpha \in B^n$ таких, что $f(\alpha) = 1$, и обозначается через N_f, а также его дополнением $\overline{N}_f = N_{\overline{f}} = B^n \setminus N_f$. Заметим, что ФАЛ f является характеристической функцией множества N_f.

На рис. 2.3a показана таблица значений ФАЛ трех переменных $H(x_1, x_2, x_3)$, которая называется функцией *голосования*, на рис. 2.3b приведены прямоугольные таблицы ее значений, а на рис. 2.3c выписаны наборы множеств N_H и $\overline{N}_H$.

Нетрудно убедиться в том, что бинарные операции &, $\vee$, $\oplus$ удовлетворяют обычным «алгебраическим» тождествам ассоциативности и коммутативности, а операция &, кроме того, — тождествам дистрибутивности относительно $\vee$ и $\oplus$,

x_1	x_2	x_3	H
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

a)

x_1 \ x_2 \ x_3	0	1
0 0	0	0
0 1	0	1
1 1	1	1

x_1 \ x_3 \ x_2	0	0	1	1
	0	1	0	1
0	0	0	0	1
1	0	1	1	1

b)

$$N_H = \{(011), (101), (110), (111)\}$$
$$\overline{N}_H = \{(000), (001), (010), (100)\}$$

c)

Рис. 2.3: функция голосования

с помощью которых можно раскрывать скобки[1]. Заметим, также, что имеют место следующие тождества приведения подобных

$$x \cdot 0 = x \cdot \overline{x} = x \oplus x = 0, \quad x \vee 1 = x \vee \overline{x} = x \oplus \overline{x} = 1, \tag{2.1}$$

$$x \cdot x = x \vee x = x \vee 0 = x \oplus 0 = x \cdot 1 = x, \tag{2.2}$$

$$x_1 \vee x_1 x_2 = x_1, \tag{2.3}$$

последнее из которых называется «тождеством поглощения».

Напомним, что ФАЛ вида

$$f(x_1, \ldots, x_n) = \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n \oplus \alpha_0$$

из $P_2(n)$, где $\alpha_0, \ldots, \alpha_n$ — булевы константы, называется *линейной* ФАЛ и заметим, что существенными БП этой ФАЛ являются те и только те БП x_i из множества $X(n)$, для которых «коэффициент» α_i равен 1. Заметим также, что ФАЛ $\ell_n = x_1 \oplus \cdots \oplus x_n$ и $\overline{\ell}_n = x_1 \oplus \cdots \oplus x_n \oplus 1$ являются единственными существенными линейными ФАЛ в $P_2(n)$.

Рассмотрим некоторые формулы «алгебраического» типа над множеством

$$\text{Б}_0 = \{x_1 \cdot x_2,\, x_1 \vee x_2,\, \overline{x}_1\}.$$

Функции x_i и $\overline{x}_i$ будем называть *буквами* БП x_i и, как обычно, будем считать, что $x_i^0 = \overline{x}_i$, $x_i^1 = x_i$. Конъюнкция (дизъюнкция) r, $1 \leqslant r \leqslant n$, букв различных БП из множества $X(n)$ называется *элементарной конъюнкцией* (соответственно *элементарной дизъюнкцией*) *ранга* r *от булевых переменных* $X(n)$. Из (2.1), (2.2) следует, что элементарная

[1]При записи формул над $P_2(2)$ будем применять обычные соглашения о «силе» операций, в соответствии с которыми ФАЛ $\neg$ сильнее ФАЛ &, а ФАЛ & сильнее всех остальных ФАЛ от двух БП. Кроме того, внешние скобки и скобки, задающие порядок многократного выполнения одной и той же бинарной ассоциативной операции &, $\vee$, $\sim$, $\oplus$, будем, как правило, опускать.

конъюнкция (ЭК) $K = x_{i_1}^{\alpha_1} \cdots x_{i_r}^{\alpha_r}$ и элементарная дизъюнкция (ЭД) $J = x_{i_1}^{\overline{\alpha}_1} \vee \ldots \vee x_{i_r}^{\overline{\alpha}_r}$, где $1 \leqslant i_1 < \cdots < i_r \leqslant n$, являются характеристическими ФАЛ грани $N_K = \Gamma_\beta$ и ее дополнения $N_J = B^n \setminus \Gamma_\beta$, где набор β из $([0,2])^n$ обладает тем свойством, что $\beta\langle i_p\rangle = \alpha_p$ при всех $p \in [1,r]$ и $\beta\langle i\rangle = 2$ в остальных случаях. Так, элементарные конъюнкции $\overline{x}_1\overline{x}_2x_3\overline{x}_4$, $\overline{x}_1\overline{x}_3\overline{x}_4$, $\overline{x}_1x_4$ и x_1 ранга 4, 3, 2 и 1 соответственно от БП x_1, x_2, x_3, x_4 являются характеристическими ФАЛ граней куба B^4, показанных на рис. 2.1b. Будем считать, что константа 1 (константа 0) является элементарной конъюнкцией (соответственно элементарной дизъюнкцией) ранга 0. Заметим, что любая отличная от $x_1 \oplus x_2$ и $x_1 \sim x_2$ существенная ФАЛ от БП x_1, x_2 является либо ЭК, либо ЭД ранга 2.

Дизъюнкция различных элементарных конъюнкций называется *дизъюнктивной нормальной формой* (ДНФ), а конъюнкция различных элементарных дизъюнкций — *конъюнктивной нормальной формой* (КНФ). При этом ДНФ (КНФ) считается *совершенной*, если все ее ЭК (соответственно ЭД) существенно зависят от одних и тех же БП, а их ранг равен числу этих БП. Число ЭК (ЭД) в ДНФ (соответственно КНФ) $\mathfrak{A}$ называется ее *длиной* и обозначается через $\lambda(\mathfrak{A})$. Любую ФАЛ $f(x_1,\ldots,x_n)$, отличную от константы, можно представить в виде ее совершенных ДНФ и КНФ следующим образом:

$$f(x_1,\ldots,x_n) = \bigvee_{(\alpha_1,\ldots,\alpha_n)\in N_f} x_1^{\alpha_1}\ldots x_n^{\alpha_n} = \\ = \bigwedge_{(\beta_1,\ldots,\beta_n)\in \overline{N}_f} \left(x_1^{\overline{\beta}_1} \vee \ldots \vee x_n^{\overline{\beta}_n}\right). \quad (2.4)$$

Так, совершенная ДНФ ФАЛ $g(x_1,x_2,x_3)$, для которой $\overline{N}_g =$

$\{(000), (111)\}$, (см. рис. 2.1а) имеет вид

$$g(x_1, x_2, x_3) = \\ = x_1\overline{x}_2\overline{x}_3 \vee x_1x_2\overline{x}_3 \vee \overline{x}_1x_2\overline{x}_3 \vee \overline{x}_1x_2x_3 \vee \overline{x}_1\overline{x}_2x_3 \vee x_1\overline{x}_2x_3.$$

Заметим, что любую ФАЛ f из $P_2(n)$, отличную от константы 0, можно представить ее совершенной ДНФ вида (2.4), а ФАЛ $f \equiv 0$ — формулой $x_1 \cdot \overline{x}_1$. Следовательно, любая ФАЛ из P_2 может быть реализована формулой над $Б_0$, и поэтому множество $Б_0$ является базисом P_2.

Совершенную ДНФ (2.4) обобщает следующее представление, которое называют обычно разложением Шеннона:

$$f(x', x'') = \bigvee_{\sigma''=(\sigma_{q+1},\ldots,\sigma_n)} x_{q+1}^{\sigma_{q+1}} \cdots x_n^{\sigma_n} f_{\sigma''}(x'), \quad (2.5)$$

где $q \in [0, n]$, $x' = (x_1, \ldots, x_q)$, $x'' = (x_{q+1}, \ldots, x_n)$ и $f_{\sigma''}(x') = f(x', \sigma'')$. Заметим, что при $q = 0$ все «остаточные» ФАЛ $f_{\sigma''}(x')$ являются константами.

Представление ФАЛ в виде ДНФ или КНФ имеет простую геометрическую интерпретацию. Пусть

$$f(x_1, \ldots, x_n) = K_1 \vee \ldots \vee K_s = \mathfrak{A}, \quad (2.6)$$

$$f(x_1, \ldots, x_n) = J_1 \cdots J_t = \mathfrak{B}, \quad (2.7)$$

где $K_1, \ldots, K_s$ ($J_1, \ldots, J_t$) — различные ЭК (соответственно ЭД) от БП $x_1, \ldots, x_n$. Из (2.1), (2.2) следует, что представления (2.6) и (2.7) эквивалентны следующим покрытиям множеств N_f и $\overline{N}_f$ гранями куба B^n

$$N_f = N_{K_1} \cup \ldots \cup N_{K_s}; \quad (2.8)$$

$$\overline{N}_f = \overline{N}_{J_1} \cup \ldots \cup \overline{N}_{J_t}. \quad (2.9)$$

Так, представление

$$g(x_1, x_2, x_3) = K_1 \vee \ldots \vee K_6, \quad (2.10)$$

где $\overline{N}_g = \{(000), (111)\}$ и

$$K_1 = x_1\overline{x}_3, \qquad K_2 = x_2\overline{x}_3, \qquad K_3 = \overline{x}_1 x_2,$$
$$K_4 = \overline{x}_1 x_3, \qquad K_5 = \overline{x}_2 x_3, \qquad K_6 = x_1\overline{x}_2,$$

соответствует покрытию $N_g = \mathcal{N}_1 \cup \ldots \cup \mathcal{N}_6$, где $\mathcal{N}_i = N_{K_i}$ при всех $i = 1, \ldots, 6$ (см. рис. 2.1а). Заметим, что совершенные ДНФ и КНФ ФАЛ f из (2.4) задают покрытие множеств N_f и $\overline{N}_f$ соответственно гранями размерности 0. Принимая во внимание указанную выше геометрическую интерпретацию, мы не будем в дальнейшем делать существенных различий между ЭК K_i и соответствующей ей гранью N_{K_i}, а также между ДНФ вида (2.6) и соответствующим ей покрытием (2.7).

Лемма 2.1. *Совершенная ДНФ ФАЛ f, $f \in P_2(n)$, является единственной ДНФ от БП $X(n)$, которая реализует эту ФАЛ, тогда и только тогда, когда во множестве N_f нет соседних наборов.*

Доказательство. Совершенная ДНФ ФАЛ f является единственной ДНФ от БП $X(n)$, которая реализует эту ФАЛ, тогда и только тогда, когда в множестве N_f нет граней размерности больше 0, что эквивалентно тому, что в множестве N_f нет соседних наборов. □

Следствие. *Совершенные ДНФ ФАЛ ℓ_n, $\overline{\ell}_n$ являются единственными ДНФ этих ФАЛ от БП $X(n)$.*

§3 Сокращенная ДНФ и способы ее построения

Рассмотрим теперь некоторые специальные виды ДНФ и их «геометрическую» интерпретацию. Будем говорить, что ФАЛ f' *имплицирует* ФАЛ f'', или, иначе, ФАЛ f'' *поглощает* ФАЛ f', если $N_{f'} \subseteq N_{f''}$, то есть импликация

$(f' \to f'')$ тождественно равна 1. Элементарная конъюнкция, которая имплицирует ФАЛ f, называется *импликантой* этой ФАЛ. Заметим, что отношение имплицируемости является отношением частичного порядка и что f' имплицирует f'' тогда и только тогда, когда $f'' = f' \vee f''$ или $f' = f' \cdot f''$. Отсюда следует, в частности, что ЭК K' имплицирует ЭК K'' тогда и только тогда, когда множество букв K'' содержится во множестве букв K', то есть $K' = K'' \cdot K$ для некоторой ЭК K, не имеющей общих букв с ЭК K''. Это означает, что в данном случае ЭК K' может быть «устранена» из ДНФ $K'' \vee K'$ с помощью тождества поглощения (2.3).

Дизъюнктивную нормальную форму $\mathfrak{A}$ вида (2.6) будем называть ДНФ *без поглощений* ЭК, если ни одна из граней $N_{K_1}, \ldots, N_{K_s}$ не содержится ни в одной из других граней покрытия (2.8). На «языке имплицируемости» это означает, что ни одна из ЭК K_i, $i \in [1, s]$, не является импликантой ЭК K_j, где $j \in [1, s]$ и $i \neq j$. Заметим, что с помощью тождества поглощения (2.3) из любой ДНФ $\mathfrak{A}$ можно получить ДНФ $\widehat{\mathfrak{A}}$. без поглощений ЭК.

Импликанта K ФАЛ f называется *простой импликантой* этой ФАЛ, если она не поглощается никакой другой отличной от нее импликантой ФАЛ f. Из определений и отмеченных выше фактов следует, что в простую импликанту ФАЛ f не входят буквы несущественных БП этой ФАЛ и что из любой импликанты ФАЛ f можно получить ее простую импликанту удалением некоторых букв. Последнее означает, что любая импликанта ФАЛ f имплицирует некоторую простую импликанту f. С «геометрической» точки зрения простые импликанты ФАЛ f соответствуют максимальным по включению граням множества N_f.

Дизъюнкция всех простых импликант ФАЛ f называется ее *сокращенной* ДНФ. Заметим, что сокращенная ДНФ ФАЛ f является ДНФ без поглощений и что ей соответ-

ствует покрытие множества N_f всеми максимальными по включению гранями множества N_f этой ФАЛ. Указанное соответствие позволяет строить сокращенную ДНФ на основе «геометрических» соображений. Так, в соответствии с рис. 2.1 правая часть (2.10) является сокращенной ДНФ ФАЛ g, а из рис. 3.1a вытекает, что сокращенная ДНФ ФАЛ $g'(x_1, x_2, x_3, x_4)$, для которой $\widetilde{\alpha}_{g'} = (1111\,1011\,1101\,1010)$, имеет вид

$$g' = K_1' \vee \ldots \vee K_7', \tag{3.1}$$

где $K_1' = \overline{x}_3\overline{x}_4$, $K_2' = \overline{x}_2\overline{x}_3$, $K_3' = \overline{x}_2 x_4$, $K_4' = \overline{x}_1 x_3$, $K_5' = x_2\overline{x}_4$, $K_6' = \overline{x}_1\overline{x}_4$, $K_7' = \overline{x}_1\overline{x}_2$, причем ЭК K_i', $i = 1, \ldots, 7$, соответствует грани $\mathcal{N}_i' = N_{K_i'}$ на рис. 3.1a. На рис. 3.1b приведена для наглядности «развертка» множества $N_{g'}$ и составляющих его максимальных граней указанной ФАЛ g'. Легко видеть, что сокращенная ДНФ ЭК или ЭД совпадает с ней самой.

Чтобы сделать построение сокращенной ДНФ для ФАЛ f, $f \in P_2(n)$, более наглядным, часто используют ее представление в виде *карты Карно*, то есть в виде таблицы $\Pi_{2,2}(f)$, в которой наборы (10) и (11) переставлены, а противоположные стороны отождествлены по типу «тора». Заметим, что любое ребро куба B^4 соответствует двум соседним клеткам указанной таблицы, а любой квадрат в B^4 — либо квадрату, составленному из четырех соседних клеток таблицы, либо ее строке или столбцу. На рис. 3.2 приведена карта Карно ФАЛ $g'(x_1, x_2, x_3, x_4)$ и указаны все максимальные грани этой ФАЛ.

Теорема 3.1. *Пусть $\mathfrak{A}'$ и $\mathfrak{A}''$ — сокращенные ДНФ ФАЛ f' и f'' соответственно, а ДНФ $\mathfrak{A}$ без поглощений получается из формулы $\mathfrak{A}' \cdot \mathfrak{A}''$ в результате раскрытия скобок и приведения подобных. Тогда $\mathfrak{A}$ — сокращенная ДНФ ФАЛ $f = f' \cdot f''$.*

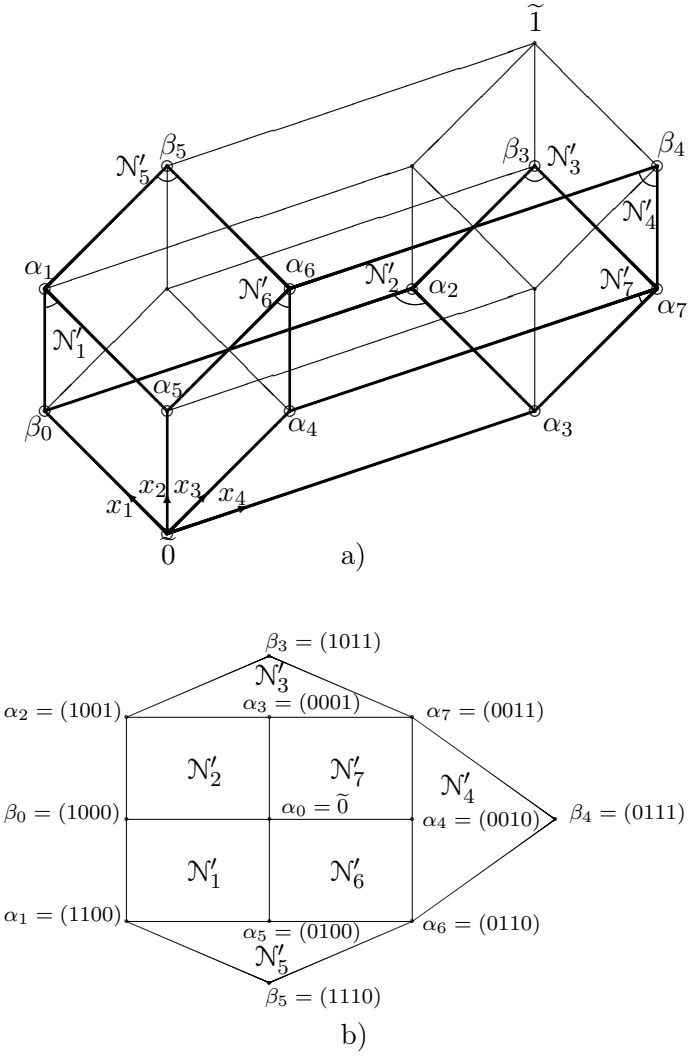

Рис. 3.1: «геометрия» сокращенной ДНФ ФАЛ g'

x_1 x_2 \ x_4	0	1	1	0
x_3	0	0	1	1
0 0				
0 1				
1 1				
1 0				

a)

x_1 x_2 \ x_4	0	1	1	0
x_3	0	0	1	1
0 0	1	1	1	1
0 1	1	0	1	1
1 1	1	0	0	1
1 0	1	1	1	0

b)

Рис. 3.2: карта Карно ФАЛ g'

Доказательство. Достаточно доказать, что в $\mathfrak{A}$ входит любая простая импликанта ФАЛ f. Пусть ЭК K является простой импликантой ФАЛ f и, следовательно, является импликантой как ФАЛ f', так и ФАЛ f''. Из свойств сокращенных ДНФ вытекает, что в $\mathfrak{A}'$ и $\mathfrak{A}''$ найдутся ЭК K' и K'' соответственно, которые имплицируются ЭК K. Таким образом, в ДНФ $\mathfrak{A}$ войдет имплицируемая ФАЛ $K' \cdot K''$ ЭК $\widetilde{K}$, которая получится в результате раскрытия скобок и приведения подобных в формуле $\mathfrak{A}' \cdot \mathfrak{A}''$. Заметим, что при этом ЭК K имплицирует ФАЛ $K' \cdot K''$ и, следовательно, имплицирует ЭК $\widetilde{K}$. Поскольку ЭК $\widetilde{K}$ является импликантой ФАЛ f и, одновременно, имплицируется ЭК K, то $\widetilde{K} = K$, так как K — простая импликанта ФАЛ f.

Теорема доказана. □

Следствие. *Если ДНФ $\mathfrak{A}$ без поглощений получается из КНФ $\mathfrak{B}$ ФАЛ f в результате раскрытия скобок и приведения подобных, то $\mathfrak{A}$ — сокращенная ДНФ ФАЛ f.*

Применяя следствие из теоремы 3.1 к ФАЛ g', показанной на рис. 3.1-3.2, получим (сравните с (3.1))

$$\begin{aligned}\mathfrak{D} = (\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_4)\cdot(x_1 \vee \overline{x}_2 \vee x_3 \vee \overline{x}_4)\cdot(\overline{x}_1 \vee x_2 \vee \overline{x}_3 \vee x_4) = \\ = (\overline{x}_2 \vee \overline{x}_4 \vee \overline{x}_1 x_3) \cdot (\overline{x}_1 \vee x_2 \vee \overline{x}_3 \vee x_4) = \\ = \overline{x}_3\overline{x}_4 \vee \overline{x}_1\overline{x}_4 \vee \overline{x}_1\overline{x}_2 \vee \overline{x}_2\overline{x}_3 \vee x_2\overline{x}_4 \vee \overline{x}_1 x_3 \vee \overline{x}_2 x_4.\end{aligned}$$

Следующий метод (метод Блейка [6]) позволяет получать сокращенную ДНФ ФАЛ f из произвольной ДНФ этой ФАЛ с помощью эквивалентных преобразований на основе тождества обобщенного склеивания:

$$x_1x_2 \vee \overline{x}_1x_3 = x_1x_2 \vee \overline{x}_1x_3 \vee x_2x_3.$$

Любая ДНФ $\mathfrak{A}'$, которую можно получить из ДНФ $\mathfrak{A}$ путем формирования в ней с помощью тождеств ассоциативности и коммутативности подформул вида $x_iK' \vee \overline{x}_iK''$,

применения к этим подформулам тождества обобщенного склеивания

$$x_i K' \vee \overline{x}_i K'' = x_i K' \vee \overline{x}_i K'' \vee K' K'' \tag{3.2}$$

и последующего приведения подобных, называется *расширением* ДНФ $\mathfrak{A}$. Расширение $\mathfrak{A}'$ ДНФ $\mathfrak{A}$ считается *строгим*, если $\mathfrak{A}'$ содержит ЭК, не являющуюся импликантой ни одной ЭК из $\mathfrak{A}$. Заметим, что сокращенная ДНФ не имеет строгих расширений и что в результате построения последовательных строгих расширений и приведения подобных из любой ДНФ можно получить ДНФ без поглощений ЭК, которая не имеет строгих расширений.

Теорема 3.2. *ДНФ без поглощений ЭК является сокращенной ДНФ тогда и только тогда, когда она не имеет строгих расширений.*

Доказательство. Достаточно убедиться в том, что ДНФ $\mathfrak{A}$ без поглощений ЭК, не имеющая строгих расширений, содержит все простые импликанты реализуемой ею ФАЛ f. Пусть $X(n) = \{x_1, \ldots, x_n\}$ — множество БП ДНФ $\mathfrak{A}$, а K — простая импликанта f, которая не входит в $\mathfrak{A}$. Рассмотрим множество $\mathcal{K}$, состоящее из всех тех элементарных конъюнкций от БП $X(n)$, которые являются импликантами f, но не являются импликантами ни одной ЭК из $\mathfrak{A}$. Заметим, что множество $\mathcal{K}$ не пусто, так как содержит ЭК K в силу ее свойств, и что $\mathcal{K}$ не может содержать ЭК ранга n, поскольку любая ЭК вида $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, где $\alpha = (\alpha_1, \ldots, \alpha_n) \in N_f$, является импликантой той ЭК из $\mathfrak{A}$, которая обращается в 1 на наборе α.

Пусть, далее, k — ЭК максимального ранга в $\mathcal{K}$, причем, как было отмечено, $R(k) < n$, и пусть буквы некоторой БП x_i, $1 \leqslant i \leqslant n$, не входят в k. Тогда, в силу выбора ЭК k и свойств ДНФ $\mathfrak{A}$, ЭК вида $x_i \cdot k$ (вида $\overline{x}_i \cdot k$) должна быть импликантой некоторой ЭК вида $x_i \cdot K'$ (соответственно $\overline{x}_i \cdot K''$)

из $\mathfrak{A}$, где ЭК K' и K'' состоят из букв ЭК k. Следовательно, ЭК k является импликантой ЭК $\widetilde{K}$ равной $K' \cdot K''$, а ЭК $\widetilde{K}$, в свою очередь, является импликантой некоторой ЭК из $\mathfrak{A}$. Действительно, ДНФ $\mathfrak{A}$ не имеет строгих расширений и поэтому содержит ЭК, которая имплицируется ЭК $\widetilde{K}$, получающейся из подформулы $x_i K' \vee \overline{x}_i K''$ в результате эквивалентного преобразования (3.2). Таким образом, ЭК k является импликантой некоторой ЭК из $\mathfrak{A}$ и не может входить в $\mathcal{K}$. Полученное противоречие доказывает, что ЭК K входит в $\mathfrak{A}$.

Теорема доказана. □

Следствие. *Из любой ДНФ $\mathfrak{A}$ ФАЛ f можно получить сокращенную ДНФ этой ФАЛ в результате построения последовательных строгих расширений и приведения подобных до получения ДНФ без поглощений ЭК, не имеющей строгих расширений.*

Возьмем для примера в качестве ДНФ $\mathfrak{A}$ совершенную ДНФ ФАЛ голосования $H(x_1, x_2, x_3)$, которая имеет вид

$$\mathfrak{A}(x_1, x_2, x_3) = x_1x_2x_3 \vee \overline{x}_1x_2x_3 \vee x_1\overline{x}_2x_3 \vee x_1x_2\overline{x}_3.$$

Применяя к $\mathfrak{A}$ метод Блейка, получим:

$$\begin{aligned}\mathfrak{A} &= (x_1x_2x_3 \vee \overline{x}_1x_2x_3) \vee x_1\overline{x}_2x_3 \vee x_1x_2\overline{x}_3 = \\ &= x_2x_3 \vee x_1\overline{x}_2x_3 \vee x_1x_2\overline{x}_3 = (x_2x_3 \vee \overline{x}_2x_1x_3) \vee x_1x_2\overline{x}_3 = \\ &= x_2x_3 \vee x_1x_3 \vee x_1x_2\overline{x}_3 = x_2x_3 \vee (x_3x_1 \vee \overline{x}_3x_1x_2) = \\ &= x_2x_3 \vee x_1x_3 \vee x_1x_2. \qquad (3.3)\end{aligned}$$

§4 Тупиковые ДНФ, ядро и ДНФ пересечение тупиковых. ДНФ Квайна и ДНФ сумма тупиковых, критерий вхождения простых импликант в тупиковые ДНФ, его локальность

Будем говорить, что ДНФ $\mathfrak{A}$, реализующая ФАЛ f, является *тупиковой* ДНФ, если $f \neq \mathfrak{A}'$ для любой ДНФ $\mathfrak{A}'$, полученной из $\mathfrak{A}$ в результате удаления некоторых букв или целых ЭК. Из определения вытекает, что в тупиковую ДНФ $\mathfrak{A}$ ФАЛ f могут входить только простые импликанты этой ФАЛ, и что $\mathfrak{A}$ является ДНФ без поглощений ЭК. С «геометрической» точки зрения тупиковая ДНФ $\mathfrak{A}$ ФАЛ f задает тупиковое (см. §1) покрытие множества N_f максимальными гранями ФАЛ f и обратно.

Построение всех или некоторых тупиковых ДНФ для заданной ФАЛ f является, обычно, промежуточным этапом при построении *минимальной* (*кратчайшей*) ДНФ ФАЛ f, то есть ДНФ, которая имеет минимальный ранг (соответственно длину) среди всех ДНФ, реализующих f. Это связано с тем, что минимальная ДНФ обязательно является тупиковой, а среди кратчайших ДНФ всегда есть тупиковая.

При построении тупиковых ДНФ ФАЛ f бывает полезно знать ДНФ *пересечение тупиковых* (ДНФ $\cap T$) ФАЛ f, то есть дизъюнкцию всех тех различных простых импликант этой ФАЛ, которые входят в любую тупиковую ДНФ ФАЛ f.

Набор α, $\alpha \in B^n$, называется *ядровой точкой* ФАЛ $f\,(x_1, \ldots, x_n)$, если $\alpha \in N_f$ и α входит только в одну максимальную грань ФАЛ f. При этом грань N_K, являющаяся максимальной гранью ФАЛ f и содержащая точку α, считается *ядровой гранью* ФАЛ f, а совокупность всех различных ядровых граней ФАЛ f называется *ядром* ФАЛ f.

Лемма 4.1. *Дизъюнктивная нормальная форма $\cap T$ ФАЛ f состоит из тех простых импликант ФАЛ f, которые соответствуют ядровым граням этой ФАЛ.*

Доказательство. Пусть тупиковая ДНФ $\mathfrak{A}$ ФАЛ $f(x_1, \ldots, x_n)$ не включает в себя простую импликанту K, которая соответствует ядровой грани N_K ФАЛ f, содержащей ядровую точку α этой ФАЛ. Поскольку все отличные от K простые импликанты ФАЛ f обращаются в 0 на наборе α, то ДНФ $\mathfrak{A}$ также будет равна 0 на этом наборе и, следовательно, $f(\alpha) = 0$. Полученное противоречие с тем, что $\alpha \in N_f$, доказывает необходимость включения ЭК K в любую тупиковую ДНФ ФАЛ f.

Пусть теперь простая импликанта K ФАЛ f соответствует грани N_K, которая не входит в ядро ФАЛ f. При этом каждая точка грани N_K покрывается хотя бы одной отличной от N_K максимальной гранью ФАЛ f. Следовательно, все отличные от N_K максимальные грани ФАЛ f образуют покрытие множества N_f, из которого можно выделить тупиковое подпокрытие, соответствующее тупиковой ДНФ ФАЛ f, не содержащей ЭК K.

Лемма доказана. □

Исходя из «геометрических» соображений можно находить все или некоторые тупиковые ДНФ для ФАЛ от небольшого числа БП. Так, например, сокращенная ДНФ (3.3) для ФАЛ «голосования» $H(x_1, x_2, x_3)$ является единственной тупиковой ДНФ этой ФАЛ, ФАЛ $g(x_1, x_2, x_3)$ (см. рис. 2.1а и (2.10)) имеет пять тупиковых ДНФ —

$$\mathfrak{A}_1 = K_1 \vee K_3 \vee K_5, \quad \mathfrak{A}_2 = K_2 \vee K_4 \vee K_6, \tag{4.1}$$

$$\begin{gathered} \mathfrak{A}_3 = K_1 \vee K_2 \vee K_4 \vee K_5, \quad \mathfrak{A}_4 = K_2 \vee K_3 \vee K_5 \vee K_6, \\ \mathfrak{A}_5 = K_3 \vee K_4 \vee K_6 \vee K_1, \end{gathered} \tag{4.2}$$

а у ФАЛ $g'(x_1, x_2, x_3, x_4)$ (см. рис. 3.1-3.2 и (3.1)) имеются две тупиковые ДНФ —

$$\mathfrak{A}'_1 = K'_1 \vee K'_3 \vee K'_4 \vee K'_5, \quad \mathfrak{A}'_2 = K'_2 \vee K'_3 \vee K'_4 \vee K'_5. \quad (4.3)$$

При этом ДНФ $\mathfrak{A}_1$, $\mathfrak{A}_2$ в (4.1) и ДНФ $\mathfrak{A}'_1$, $\mathfrak{A}'_2$ в (4.3) являются минимальными и, одновременно, кратчайшими ДНФ ФАЛ g и ФАЛ g' соответственно.

При построении тупиковых ДНФ ФАЛ f наряду с ДНФ пересечение тупиковых полезно знать ДНФ *сумма тупиковых* (ДНФ ΣT) ФАЛ f, то есть дизъюнкцию всех тех различных простых импликант этой ФАЛ, которые входят в хотя бы в одну тупиковую ДНФ ФАЛ f. Заметим, что ДНФ $\cap T$ ФАЛ f в общем случае не реализует саму ФАЛ f, а в некоторых случаях и, в частности, в случае ФАЛ g (см. выше), может быть пустой. В то же время ДНФ ΣT ФАЛ f всегда реализует эту ФАЛ, содержится в ее сокращенной и может с ней совпадать, как это имеет место в случае ФАЛ g или в случае ФАЛ «голосования».

Будем называть ФАЛ *ядровой*, если все ее максимальные грани являются ядровыми. Из леммы 4.1 следует, что сокращенная ДНФ ядровой ФАЛ является ее единственной тупиковой ДНФ. Примером ядровой ФАЛ является ФАЛ голосования (3.3) (см. также §6).

Дизъюнктивная нормальная форма, получающаяся из сокращенной ДНФ ФАЛ f удалением тех ЭК K, для которых грань N_K покрывается ядром ФАЛ f, но не входит в него, называется *ДНФ Квайна* этой ФАЛ. Из определений следует, что ДНФ Квайна ФАЛ f включает в себя ДНФ ΣT этой ФАЛ и содержится в ее сокращенной ДНФ. Заметим, что для ФАЛ $g''(x_1, x_2, x_3)$, показанной на рис. 4.1, ее сокращенная ДНФ имеет вид $g'' = x_2\overline{x}_3 \vee \overline{x}_1 x_2 \vee \overline{x}_1 x_3$, то есть отличается от ДНФ Квайна, которая является единственной тупиковой ДНФ этой ФАЛ и имеет вид $g'' = x_2\overline{x}_3 \vee \overline{x}_1 x_3$. В

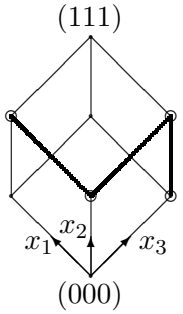

Рис. 4.1: «геометрия» сокращенной ДНФ ФАЛ g''

то же время для ФАЛ g', показанной на рис. 3.1, ДНФ Квайна совпадает с сокращенной ДНФ этой ФАЛ и отличается от ее ДНФ ΣT, которая (см. выше) равна

$$K_1' \vee K_2' \vee K_3' \vee K_4' \vee K_5'.$$

Для ФАЛ $f(x_1, \ldots, x_n)$ и набора α, $\alpha \in N_f$, обозначим через $\Pi_\alpha(f)$ множество всех проходящих через α максимальных граней ФАЛ f, которое мы будем называть *пучком ФАЛ f через точку α*. Точку α, $\alpha \in N_f$, будем называть *регулярной точкой ФАЛ f*, если найдется точка β, $\beta \in N_f$, для которой имеет место строгое включение $\Pi_\beta(f) \subset \Pi_\alpha(f)$. Указанное включение означает, что любая максимальная грань ФАЛ f, проходящая через точку β, проходит и через точку α, причем есть такая максимальная грань ФАЛ f, которая проходит через точку α, но не проходит через точку β. Легко видеть, что для любой регулярной точки α ФАЛ f всегда найдется такая нерегулярная точка β, $\beta \in N_f$, для которой $\Pi_\beta(f) \subset \Pi_\alpha(f)$.

Из определений следует, что любая неядровая точка ядровой грани регулярна, и поэтому точки α_i, $i \in [1, 7]$, ФАЛ g', показанной на рис. 3.1, являются ее регулярными точка-

ми. Кроме того, в силу включения $\Pi_{\beta_0}(g') \subset \Pi_{\alpha_0}(g')$, точка α_0 тоже является регулярной точкой этой ФАЛ.

Грань N_K ФАЛ f называется *регулярной гранью* этой ФАЛ, если все точки N_K регулярны. Заметим, что грань, которая не входит в ядро, но покрывается им, является регулярной. Заметим также, что для ФАЛ g', показанной на рис. 3.1, грани $\mathcal{N}'_6$ и $\mathcal{N}'_7$, которые не входят в ДНФ ΣT, являются регулярными, так как состоят из регулярных точек.

Теорема 4.1 (ср. [28, 6, 23, 10]). *Простая импликанта K ФАЛ f входит в ДНФ ΣT тогда и только тогда, когда грань N_K не является регулярной гранью этой ФАЛ.*

Доказательство. Пусть $\alpha_1, \ldots, \alpha_s$ — все регулярные точки ФАЛ f. Тогда для каждого j, $j = 1, \ldots, s$, в силу регулярности точки α_j, найдется нерегулярная точка β_j ФАЛ f, обладающая тем свойством, что любая максимальная грань ФАЛ f, проходящая через точку β_j, проходит и через точку α_j. Следовательно, любая система максимальных граней ФАЛ f, покрывающая точки $\beta_1, \ldots, \beta_s$, «автоматически» покроет все точки $\alpha_1, \ldots, \alpha_s$. Таким образом, грань N_K, состоящая из регулярных точек, не может входить в тупиковое покрытие множества N_f максимальными гранями, и поэтому ЭК K не может входить в ДНФ ΣT ФАЛ f.

Пусть теперь N_K — нерегулярная грань ФАЛ f, которая содержит нерегулярную точку α, и пусть $N_f \setminus N_K = \{\beta_1, \ldots, \beta_q\}$. Из нерегулярности точки α следует, что для любого j, $j = 1, \ldots, q$, пучок $\Pi_{\beta_j}(f)$ не может быть строго вложен в пучок $\Pi_\alpha(f)$. Кроме того, равенство $\Pi_{\beta_j}(f) = \Pi_\alpha(f)$ тоже невозможно, так как $N_K \in \Pi_\alpha(f) \setminus \Pi_{\beta_j}(f)$, и поэтому в $\Pi_{\beta_j}(f)$ найдется грань N_{K_j}, которая проходит через точку β_j, но не проходит через точку α. Следовательно, из покрытия множества N_f максимальными гранями N_K, N_{K_1}, $\ldots$, N_{K_q} нельзя удалить грань N_K, так как только она покрывает в нем точку α. Таким образом, любое ту-

пиковое покрытие множества N_f, являющееся подпокрытием указанного покрытия, будет соответствовать тупиковой ДНФ, содержащей ЭК K.

Теорема доказана. $\square$

Коснемся, далее, вопроса о локальном характере рассмотренных выше критериев вхождения простых импликант ФАЛ f в ее ДНФ $\cap T$ и ДНФ ΣT (см. [28, 22, 23, 16]). Для каждой максимальной грани $\mathcal{N}$ ФАЛ $f(x_1, \ldots, x_n)$ положим $S_0(\mathcal{N}, f) = \{\mathcal{N}\}$, а затем индукцией по r, $r = 1, 2, \ldots$, определим множество $S_r(\mathcal{N}, f)$ как множество всех тех максимальных граней ФАЛ f, которые имеют непустое пересечение хотя бы с одной гранью из $S_{r-1}(\mathcal{N}, f)$. При этом множество $S_r(\mathcal{N}, f)$ будем называть *окрестностью порядка r грани $\mathcal{N}$ функции f*.

Докажем, что вопрос о вхождении простой импликанты K ФАЛ f в ДНФ $\cap T$ (ДНФ ΣT) этой ФАЛ можно решить, рассматривая окрестность $S_1(N_K, f)$ (соответственно $S_2(N_K, f)$). Действительно, грань N_K является ядровой гранью ФАЛ f тогда и только тогда, когда она не покрывается всеми остальными максимальными гранями этой ФАЛ. Поскольку грани, не входящие в $S_1(N_K, f)$, не имеют общих точек с N_K, грань N_K является ядровой тогда и только тогда, когда она не покрывается всеми остальными гранями из $S_1(N_K, f)$. Из теоремы 4.1 следует, что ЭК K не входит в ДНФ ΣT ФАЛ f тогда и только тогда, когда для любой точки α из N_K найдется точка β, $\beta \in N_f$, для которой $\Pi_\beta(f) \subset \Pi_\alpha(f)$. Заметим, что все грани пучка $\Pi_\alpha(f)$ входят в $S_1(N_K, f)$, а все грани пучка $\Pi_\beta(f)$, если $\Pi_\alpha(f) \cap \Pi_\beta(f) \neq \varnothing$, — в $S_2(N_K, f)$. Следовательно, проверку грани N_K на регулярность можно осуществить на основе анализа ее окрестности порядка 2. Легко показать, что рассмотрение окрестности порядка 2 достаточно для проверки грани N_K на ее вхождение в ДНФ Квайна ФАЛ f. Если же все ядровые гра-

ни ФАЛ f выделены и «помечены» (для этого, как уже говорилось, достаточно рассмотреть их окрестности порядка 1), то невхождение ЭК K в ДНФ Квайна ФАЛ f равносильно покрытию грани N_K отличными от нее «помеченными» гранями из окрестности $S_1(N_K, f)$.

§5 Особенности ДНФ линейных и монотонных функций. Функция покрытия, таблица Квайна и построение всех тупиковых ДНФ

Будем говорить, что ФАЛ $f(x_1, \ldots, x_n)$ *линейно зависит от БП* x_i, или, иначе, что БП x_i является *линейной БП* ФАЛ f, если $f(\alpha) \neq f(\beta)$ для любых соседних по БП x_i наборов α и β куба B^n. При этом для ФАЛ f имеет место равенство

$$f(x_1, \ldots, x_n) = x_i \oplus f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n),$$

которое равносильно линейности БП x_i ФАЛ f, а значит ФАЛ является линейной тогда и только тогда, когда она линейно зависит от всех своих существенных БП.

Заметим, что если ФАЛ f линейно зависит от БП x_i, то в любую импликанту этой ФАЛ входит одна из букв x_i, $\overline{x}_i$.

Рассмотрим далее класс монотонных ФАЛ и некоторые связанные с ним другие классы функций. Напомним, что ФАЛ $f(x_1, \ldots, x_n)$ называется *монотонной*, если $f(\alpha) \leqslant f(\beta)$ для любых наборов α и β куба B^n таких, что $\alpha \leqslant \beta$. Будем говорить, что ФАЛ $f(x_1, \ldots, x_n)$ *монотонно зависит от БП* x_i, или, иначе, БП x_i является *монотонной* БП ФАЛ f, если неравенство $f(\alpha) \leqslant f(\beta)$ выполняется для любых соседних по БП x_i наборов α и β куба B^n таких, что $\alpha \leqslant \beta$. Легко видеть, что монотонная ФАЛ монотонно зависит от всех своих БП и обратно.

Докажем, что если ФАЛ $f(x_1, \ldots, x_n)$ монотонно зависит от БП x_i, то ни одна из ее простых импликант не может содержать букву $\overline{x}_i$. Действительно, пусть импликанта

K' ФАЛ f содержит букву $\overline{x}_i$ и, следовательно, для грани $N_{K'} = \Gamma_{\gamma'}$, где $\gamma' \in ([0,2])^n$ и $\gamma' \langle i \rangle = 0$, имеет место включение $N_{K'} \subseteq N_f$. Тогда, в силу монотонной зависимости ФАЛ f от БП x_i, имеют место включения

$$N_{K''} = \Gamma_{\gamma''} \subseteq N_f \quad \text{и} \quad N_K = \Gamma_\gamma = N_{K'} \cup N_{K''} \subseteq N_f,$$

где набор γ'' (набор γ) получается из набора γ' заменой 0 в i-ом разряде на 1 (соответственно 2). Последнее из этих включений означает, что ЭК не является простой импликантой ФАЛ f, то есть простая импликанта монотонной по БП x_i ФАЛ не может содержать буквы $\overline{x}_i$. Отсюда следует, что любая простая импликанта отличной от 0 монотонной ФАЛ является монотонной ЭК, то есть не содержит отрицаний БП.

Частным случаем монотонной зависимости ФАЛ f от БП x_i является *конъюнктивная* (*дизъюнктивная*) зависимость f от x_i, когда $f = x_i \cdot g$ (соответственно $f = x_i \vee g$), где ФАЛ g получается из f подстановкой константы 1 (соответственно 0) вместо БП x_i. При этом в случае конъюнктивной зависимости буква x_i входит в любую импликанту ФАЛ f, а в случае дизъюнктивной зависимости буква x_i не входит ни в одну простую импликанту ФАЛ f отличную от x_i. Будем говорить, что ФАЛ $f(x_1, \ldots, x_n)$ *инмонотонно* (*инконъюнктивно*, *индизъюнктивно*) зависит от БП x_i, если ФАЛ $f(x_1, \ldots, x_{i-1}, \overline{x}_i, x_{i+1}, \ldots, x_n)$ зависит от x_i монотонно (соответственно конъюнктивно, дизъюнктивно). Очевидно, что все особенности ДНФ, характерные для ФАЛ с той или иной монотонной зависимостью от БП распространяются на ФАЛ с аналогичной инмонотонной зависимостью после инвертирования соответствующих БП.

Сопоставим каждому набору β из B^n, монотонную ЭК K_β^+ от БП $X(n)$, состоящую из тех и только тех букв x_j, $j \in [1, n]$, для которых $\beta \langle j \rangle = 1$, и заметим, что каждая монотонная ЭК от БП $X(n)$ может быть представлена в указанном виде. Легко видеть также, что грань, соответствую-

щая ЭК K_β^+, где $\beta = (\beta_1, \ldots, \beta_n) \in B^n$, имеет вид Γ_γ, где $\gamma = (2 - \beta_1, \ldots, 2 - \beta_n)$. Набор α, $\alpha \in B^n$, называется *нижней единицей* монотонной ФАЛ f, $f \in P_2(n)$, если $\alpha \in N_f$ и $f(\beta) = 0$ для любого отличного от α набора β такого, что $\beta \leqslant \alpha$. Множество всех нижних единиц монотонной ФАЛ f будем обозначать через N_f^+.

В силу введенных определений, $K_\beta^+(\alpha) = 1$ тогда и только тогда, когда $\alpha \geqslant \beta$, откуда следует, что набор β является единственной нижней единицей ЭК K_β^+ и что ЭК $K_{\beta'}^+$ импликирует ЭК $K_{\beta''}^+$ тогда и только тогда, когда $\beta' \geqslant \beta''$. Отсюда вытекает также, что ЭК K_β^+ является простой импликантой монотонной ФАЛ f тогда и только тогда, когда $\beta \in N_f^+$, и что набор β является при этом ядровой точкой ФАЛ f. Таким образом, доказано следующее утверждение.

Лемма 5.1. *Сокращенная ДНФ $\mathfrak{A}$ монотонной ФАЛ f, $f \in P_2(n)$, является единственной тупиковой ДНФ этой ФАЛ и имеет вид:*

$$\mathfrak{A}(x_1, \ldots, x_n) = \bigvee_{\beta \in N_f^+} K_\beta^+(x_1, \ldots, x_n).$$

При этом все наборы из N_f^+ являются ядровыми точками ФАЛ f.

Следствие. *Монотонная ФАЛ является ядровой ФАЛ.*

Напомним, что с «геометрической» точки зрения, сокращенная ДНФ ФАЛ f из $P_2(n)$ представляет собой покрытие множества N_f всеми максимальными гранями, а тупиковая ДНФ соответствует тупиковому подпокрытию, выделяемому из этого покрытия. Рассмотрим сначала метод выделения из заданного покрытия конечного множества всех его тупиковых подпокрытий, основанный на построении сокращенной ДНФ для специальной монотонной ФАЛ, связанной с исходным покрытием.

Пусть $\mathcal{N} = \{\alpha_1, \ldots, \alpha_s\}$ — конечное множество, а $\mathfrak{N} = (\mathcal{N}_1, \ldots, \mathcal{N}_p)$ — система его подмножеств, образующих покрытие множества $\mathcal{N}$. Сопоставим паре $(\mathcal{N}, \mathfrak{N})$ матрицу M, $M \in B^{p,s}$, для которой $M\langle i, j\rangle = 1$ тогда и только тогда, когда $\mathcal{N}_i \ni \alpha_j$. Заметим, что матрица M не имеет нулевых столбцов, так как система $\mathfrak{N}$ образует покрытие множества $\mathcal{N}$. Будем считать, что i-я строка (j-й столбец) матрицы M соответствует подмножеству $\mathcal{N}_i$ системы $\mathfrak{N}$ (элементу α_j множества $\mathcal{N}$) и не будем делать между ними существенных различий. Так, будем говорить, что i-я строка матрицы M *покрывает* ее j-й столбец, если $M\langle i, j\rangle = 1$, то есть $\mathcal{N}_i \ni \alpha_j$, и что система строк с номерами из I, $I \subseteq [1, p]$, образует *покрытие матрицы* M, если каждый ее столбец покрывается хотя бы одной строкой с номером из I, то есть система подмножеств $\{\mathcal{N}_i\}_{i \in I}$ задает покрытие множества $\mathcal{N}$. Аналогичным образом понимается покрытие одного множества строк матрицы M другим множеством ее строк и т. п.

Покрытие матрицы M, в котором ни одна строка не покрывается другой строкой, считается *неприводимым*, а покрытие, не имеющее собственных подпокрытий, называется *тупиковым* и т. п. Заметим, что задача выделения всех тупиковых подпокрытий из покрытия $\mathfrak{N}$ множества $\mathcal{N}$ эквивалентна задаче построения всех тупиковых покрытий матрицы M, соответствующей паре $(\mathcal{N}, \mathfrak{N})$. Для решения этой задачи по аналогии с ДНФ можно ввести понятие ядрового и регулярного столбцов, а также ядровой и регулярной строки, для которых будут справедливы утверждения, аналогичные лемме 4.1 и теореме 4.1.

Пусть M, $M \in B^{p,s}$ — матрица без нулевых столбцов. Сопоставим i-й строке, $i \in [1, p]$, матрицы M БП y_i, а каждому набору β, $\beta \in B^p$, значений этих переменных $y = (y_1, \ldots, y_p)$, — множество строк матрицы M с номерами из множества $I = I(\beta) \subseteq [1, p]$, где $i \in I(\beta)$ тогда и только тогда, когда $\beta\langle i\rangle = 1$. Рассмотрим ФАЛ $F(y)$, для которой

$F(\beta) = 1$ тогда и только тогда, когда система строк матрицы M с номерами из $I(\beta)$ образует ее покрытие, и будем называть эту ФАЛ *функцией покрытия* матрицы M. Заметим, что ФАЛ покрытия $F(y)$ является монотонной ФАЛ, а ее «нижние единицы» соответствуют тупиковым покрытиям матрицы M. Действительно, из неравенства $\beta' \leqslant \beta''$ вытекает, что $I(\beta') \subseteq I(\beta'')$ и потому $F(\beta') \leqslant F(\beta'')$, то есть ФАЛ F является монотонной. Из определений следует также, что набор β, $\beta \in B^p$, являющийся «нижней единицей» ФАЛ F, соответствует множеству $I(\beta)$, которое задает тупиковое покрытие матрицы M, и обратно. Таким образом, в силу леммы 5.1, каждая простая импликанта вида $K = y_{i_1} y_{i_2} \cdots y_{i_r}$, где $1 \leqslant i_1 < \cdots < i_r \leqslant p$, ФАЛ покрытия $F(y)$ соответствует тупиковому покрытию матрицы M, состоящему из строк с номерами из множества $I = \{i_1, \ldots, i_r\}$, и обратно.

Лемма 5.2. *Функция покрытия $F(y_1, \ldots, y_p)$ матрицы M, $M \in B^{p,s}$, без нулевых столбцов задается КНФ вида:*

$$F(y_1, \ldots, y_p) = \bigwedge_{j=1}^{s} \Bigg(\bigvee_{\substack{1 \leqslant i \leqslant p \\ M\langle i,j \rangle = 1}} y_i \Bigg). \tag{5.1}$$

Доказательство. Для каждого j, $j \in [1, s]$, положим

$$J_j(y) = \bigvee_{\substack{1 \leqslant i \leqslant p \\ M\langle i,j \rangle = 1}} y_i,$$

где $y = (y_1, \ldots, y_p)$. Легко видеть, что $J_j(\beta) = 1$ для произвольного набора β, $\beta \in B^p$, тогда и только тогда, когда множество строк с номерами из $I(\beta)$ покрывает j-й столбец матрицы M, $j \in [1, s]$. Отсюда следует, что КНФ в правой части (5.1) обращается в 1 на наборе β тогда и только тогда, когда множество строк с номерами из $I(\beta)$ образует

покрытие матрицы M, то есть тогда и только тогда, когда $F(\beta) = 1$.

Лемма доказана. □

Следствие. *В результате раскрытия скобок и приведения подобных из КНФ* (5.1) *можно получить сокращенную ДНФ ФАЛ* $F(y)$*, простые импликанты которой взаимно однозначно соответствуют тупиковым покрытиям матрицы* M*.*

Задача построения всех тупиковых ДНФ ФАЛ f из $P_2(n)$ на основе ее сокращенной ДНФ сводится к рассмотренной выше задаче о покрытии, если в качестве множества $\mathcal{N}$ взять множество N_f, а в качестве его покрытия $\mathfrak{N}$ — систему всех максимальных граней ФАЛ f. Матрица M, соответствующая указанной паре ($\mathcal{N}$, $\mathfrak{N}$), называется, обычно, *таблицей Квайна* ФАЛ f. Заметим, что ядровой столбец (строка) таблицы Квайна связан с ядровой точкой (соответственно гранью) ФАЛ f, что регулярный столбец (строка) этой таблицы задает регулярную точку (соответственно грань) ФАЛ f, что строка, покрываемая ядровыми строками, соответствует грани, покрываемой ядром и т. п.

Рассмотрим, для примера, задачу построения всех тупиковых ДНФ для ФАЛ $g(x_1, x_2, x_3)$ из ее сокращенной ДНФ, полагая (см. рис. 2.1а, (2.10), (4.1) и (4.2)), что

$$N_g = \{\alpha_1 = (100)\,,\ \alpha_2 = (110)\,,\ \alpha_3 = (010)\,,$$
$$\alpha_4 = (011)\,,\ \alpha_5 = (001)\,,\ \alpha_6 = (101)\},$$
$$\mathfrak{N} = \{\mathcal{N}_1,\ \ldots,\ \mathcal{N}_6\}\,,$$

где $\mathcal{N}_i = N_{K_i} = \{\alpha_i, \alpha_{i+1}\}$ для всех i, $i \in [1, 6]$, причем $\alpha_7 = \alpha_1 = (100)$. Паре $(N_g, \mathfrak{N})$ указанным выше способом

сопоставим таблицу Квайна

$$M = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

ФАЛ покрытия которой в соответствии с (5.1) задается следующей КНФ от переменных $y = (y_1, \ldots, y_6)$:

$$F(y) = (y_6 \vee y_1)(y_1 \vee y_2)(y_2 \vee y_3)(y_3 \vee y_4)(y_4 \vee y_5)(y_5 \vee y_6).$$

Раскрывая в этой КНФ скобки и приводя подобные, получим сокращенную ДНФ ФАЛ $F(y)$ вида

$$F(y) = y_1y_3y_5 \vee y_2y_4y_6 \vee y_1y_2y_4y_5 \vee y_2y_3y_5y_6 \vee y_1y_3y_4y_6,$$

слагаемые которой взаимно однозначно соответствуют тупиковым ДНФ ФАЛ g (см. (4.1), (4.2)).

В общем случае при построении всех тупиковых ДНФ ФАЛ f, $f \in P_2(n)$, с помощью леммы5.2 на основе ее сокращенной ДНФ используют, обычно, следующую модификацию рассмотренного выше подхода, которая позволяет уменьшать размеры матрицы M. Пусть $N_{K_1}, \ldots, N_{K_q}$ — все максимальные грани ФАЛ f, причем грани $N_{K_{p+1}}, \ldots, N_{K_t}$, где $1 \leqslant p \leqslant t \leqslant q$, являются ядровыми, а грани $N_{K_{t+1}}, \ldots$ $\ldots, N_{K_q}$ — регулярными гранями ФАЛ f, и пусть множество $\widehat{\mathcal{N}}$ состоит из всех ядровых и регулярных точек ФАЛ f. Положим

$$\mathcal{N} = N_f \setminus \widehat{\mathcal{N}}, \quad \mathfrak{N} = \{\mathcal{N}_1, \ldots, \mathcal{N}_p\},$$

где $\mathcal{N}_i = N_{K_i} \setminus \widehat{\mathcal{N}}$ при всех i, $i \in [1, p]$, и заметим, что задача построения всех тупиковых ДНФ ФАЛ f эквивалентна

задаче выделения всех тупиковых подпокрытий из покрытия $\mathfrak{N}$ множества $\mathcal{N}$. Действительно, если система подмножеств $\mathcal{N}_{i_1}, \ldots, \mathcal{N}_{i_r}$, где $1 \leqslant i_1 < \cdots < i_r \leqslant p$, является тупиковым покрытием множества $\mathcal{N}$, то система максимальных граней $N_{K_{i_1}}, \ldots, N_{K_{i_r}}, N_{K_{p+1}}, \ldots, N_{K_t}$ задает тупиковое покрытие множества N_f, то есть соответствует тупиковой ДНФ ФАЛ f, и обратно.

Так, применяя указанную модификацию к ФАЛ g' из $P_2(4)$, показанной на рис. 3.1 (см. также (3.1) и (4.3)), получим тривиальную задачу о покрытии множества $\mathcal{N} = \{(1000)\}$ двумя совпадающими с ним подмножествами $\mathcal{N}_1$ и $\mathcal{N}_2$.

§6 Градиентный алгоритм и оценка длины градиентного покрытия. Использование градиентного алгоритма для построения ДНФ

Выделение всех тупиковых подпокрытий из заданного покрытия и, в частности, построение всех тупиковых ДНФ является трудоемкой задачей. В связи с этим, вместо того, чтобы строить все тупиковые ДНФ и выбирать среди них, например, кратчайшую, часто используют эвристические алгоритмы, позволяющие получать не очень «длинные» ДНФ. К числу таких алгоритмов относится и градиентный алгоритм, ориентированный на выделение из заданного покрытия достаточно «коротких» подпокрытий, или, иначе, на построение достаточно «коротких» покрытий для заданной матрицы. На каждом шаге градиентного алгоритма в матрице выбирается и включается в покрытие такая строка, которая покрывает наибольшее число еще не покрытых столбцов (если таких строк несколько, из них выбирается строка с наименьшим номером). Алгоритм заканчивает свою работу после того шага, на котором получилось покрытие.

Следующее утверждение дает верхнюю оценку длины покрытия, получаемого с помощью градиентного алгоритма для матриц с заданной «густотой».

Теорема 6.1 ([6]). *Пусть для действительного* γ, $0<\gamma\leqslant 1$, *в каждом столбце матрицы* M, $M \in B^{p,s}$, *имеется не меньше, чем* $\gamma\cdot p$, *единиц. Тогда покрытие матрицы* M, *получаемое с помощью градиентного алгоритма, имеет длину не больше, чем*[1] $\left\lceil \frac{1}{\gamma}\ln^{+}(\gamma s)\right\rceil + \frac{1}{\gamma}$.

Доказательство. Пусть для построения покрытия матрицы M с помощью градиентного алгоритма потребовалось сделать q шагов, причем на шаге с номером t, $t \in [1,q]$, была выбрана строка с номером i_t. Для каждого t, $t \in [1,q)$, рассмотрим матрицу M_t, которая получается из матрицы M в результате удаления строк с номерами $\{i_1,\ldots,i_t\}$, а также покрываемых ими столбцов, и которая принадлежит множеству B^{p_t,s_t}, где $p_t = p-t$ и $s_t = s\cdot\delta_t$, $0\leqslant\delta_t\leqslant 1$. Для определенности будем считать, что $M_0 = M$, $p_0 = p$, $s_0 = s$, $\delta_0 = 1$ и $p_q = p-q$, $s_q = \delta_q = 0$. Заметим, что при любом t, $t \in [0,q]$, справедливо неравенство

$$q \leqslant t + \delta_t\cdot s, \tag{6.1}$$

так как после выполнения первых t шагов алгоритма остаются не покрытыми $\delta_t\cdot s$ столбцов матрицы M, а на каждом следующем шаге покрывается не менее одного столбца.

Заметим, далее, что в каждом столбце матрицы M_t, $t\in[0,q)$, имеется не менее, чем $\gamma\cdot p$, единиц и поэтому общее число единиц в матрице M_t не меньше, чем $\gamma p s\delta_t$, а значит среднее число единиц в ее строках не меньше, чем $\gamma s\delta_t$. Отсюда вытекает, что строка матрицы M с номером i_{t+1}, которая выбирается на $(t+1)$-м шаге алгоритма и является строкой матрицы M_t с наибольшим числом единиц, содержит не

[1] Полагаем, что $\ln^{+} x = \ln x$, если $x \geqslant 1$, и $\ln^{+} x = 0$, если $0 < x < 1$.

меньше, чем $\gamma s\delta_t$, единиц, то есть покрывает не меньше, чем $\gamma s\delta_t$, еще не покрытых столбцов матрицы M. Таким образом, для любого $t,\ t \in [0, q)$, выполняются соотношения

$$s\delta_{t+1} = s_{t+1} \leqslant s_t - \gamma s\delta_t = s\delta_t\,(1-\gamma)\,,$$

из которых, с учетом $\delta_0 = 1$, следует, что

$$\delta_t \leqslant (1-\gamma)^t \leqslant e^{-\gamma t} \tag{6.2}$$

при любом $t,\ t \in [0, q)$.

Выбирая значение параметра t так, что

$$t = \left\lceil \frac{1}{\gamma} \ln^+ (\gamma s) \right\rceil,$$

подставляя его в (6.2) и учитывая (6.2), получим

$$q \leqslant \left\lceil \frac{1}{\gamma} \ln^+ (\gamma s) \right\rceil + s \cdot e^{-\ln^+(\gamma s)} \leqslant \left\lceil \frac{1}{\gamma} \ln^+ (\gamma s) \right\rceil + \frac{1}{\gamma}.$$

Теорема доказана. □

В качестве примера применения градиентного алгоритма рассмотрим задачу о «протыкании» граней куба его точками. Задача о «протыкании» системы $\mathfrak{N}$, состоящей из подмножеств $\mathcal{N}_1, \mathcal{N}_2, \ldots, \mathcal{N}_p$ множества $\mathcal{N} = \{\alpha_1, \ldots, \alpha_s\}$, заключается в нахождении такого подмножества множества $\mathcal{N}$, в котором при любом $i,\ i \in [1, p]$, имеется хотя бы один элемент из $\mathcal{N}_i$. Эта задача сводится к задаче о выделении подпокрытия из покрытия отрезка $[1, p]$ его подмножествами $I_1,\ \ldots,\ I_s$, где $I_i = \{j :\ \alpha_i \in \mathcal{N}_j\}$ при всех $i,\ i \in [1, s]$. Заметим, что матрица построенной таким образом системы подмножеств отрезка $[1, p]$ получается из матрицы системы $(\mathcal{N}, \mathfrak{N})$ в результате транспонирования.

Лемма 6.1 ([19]). *При любых натуральных n и m, $m \leqslant n$, в кубе B^n всегда найдется подмножество мощности не более, чем $n \cdot 2^m$, протыкающее все грани ранга m.*

Доказательство. Применяя указанный выше подход, рассмотрим множество $\mathcal{N}$, состоящее из всех граней ранга m куба B^n, $|\mathcal{N}| = \binom{n}{m} \cdot 2^m$, а также систему $\mathfrak{N} = \{\mathcal{N}_\alpha\}_{\alpha \in B^n}$ его подмножеств, где $\mathcal{N}_\alpha$ — множество тех граней из $\mathcal{N}$, которые проходят через точку α. Очевидно, что каждая грань из $\mathcal{N}$ содержится в тех 2^{n-m} подмножествах $\mathcal{N}_\alpha$, для которых точка α принадлежит этой грани. Следовательно, матрица M, связанная с парой $(\mathcal{N}, \mathfrak{N})$, состоит из $p = 2^n$ строк и $s = \binom{n}{m} \cdot 2^m$ столбцов, в каждом из которых имеется $p \cdot \gamma$, где $\gamma = 2^{-m}$, единиц. Искомое множество наборов получается в результате применения к матрице M теоремы 6.1 и построения покрытия длины q, где

$$q \leqslant \left\lceil 2^m \ln^+ \left(\binom{n}{m} \right) \right\rceil + 2^m \leqslant \left\lceil 2^m \log \left(\binom{n}{m} \right) \right\rceil + 2^m \leqslant$$
$$\leqslant 2^m (n-1) + 2^m = n \cdot 2^m.$$

Лемма доказана. □

§7 Задача минимизации ДНФ. Поведение функций Шеннона и оценки типичных значений для ранга и длины ДНФ

Как уже отмечалось, ДНФ представляет собой удобную и наглядную (с «геометрической» точки зрения) форму задания ФАЛ. С другой стороны, ДНФ можно рассматривать как простейшую модель, предназначенную для структурной реализации ФАЛ (см. гл. 3).Заметим, что различные параметры ДНФ (ранг, длина и т. п) характеризуют различные

«меры» сложности указанного представления или структурной реализации. В связи с этим часто возникает необходимость построения оптимальной в том или ином смысле ДНФ для заданной ФАЛ, то есть необходимость решения соответствующей задачи *минимизации ДНФ*, которая является частным случаем задачи синтеза управляющих систем (см. гл. 3).

В общем виде задача минимизации ДНФ может быть сформулирована следующим образом. Пусть для каждой ДНФ $\mathfrak{A}$ определена ее «сложность» $\psi(\mathfrak{A})$, $\psi(\mathfrak{A}) \geqslant 0$, для которой $\psi(\mathfrak{A}') \geqslant \psi(\mathfrak{A}'')$, если ДНФ $\mathfrak{A}''$ получается из ДНФ $\mathfrak{A}'$ удалением букв или ЭК. В этом случае будем говорить, что на множестве ДНФ задан неотрицательный *функционал сложности* ψ, обладающий свойством *монотонности*. Примерами таких функционалов могут служить длина $\lambda(\mathfrak{A})$, ранг $R(\mathfrak{A})$ или «формульная» сложность $L(\mathfrak{A})$ ДНФ $\mathfrak{A}$, а также число вхождений БП с отрицаниями и другие параметры ДНФ. Задача минимизации ДНФ относительно функционала сложности ψ состоит в том, чтобы по заданной ФАЛ f построить реализующую ее ДНФ $\mathfrak{A}$ такую, что

$$\psi(\mathfrak{A}) = \min \psi\left(\mathfrak{A}'\right),$$

где минимум берется по всем ДНФ $\mathfrak{A}'$, реализующим ФАЛ f. При этом ДНФ $\mathfrak{A}$ считается *минимальной относительно функционала* ψ, или, иначе, *ψ-минимальной* ДНФ, а значение $\psi(\mathfrak{A})$ называется *сложностью ФАЛ f относительно функционала* ψ, или, иначе, *ψ-сложностью ФАЛ f* в классе ДНФ. В соответствии с введенными ранее определениями, λ-минимальную ДНФ, то есть ДНФ минимальную по длине, будем называть кратчайшей, а R-минимальную ДНФ, то есть ДНФ минимальную по рангу, — просто минимальной. Функцию

$$\psi(n) = \max_{f \in P_2(n)} \psi(f),$$

которая характеризует максимальное значение ψ-сложности ФАЛ из $P_2(n)$, называют, обычно, *функцией Шеннона* для класса ДНФ относительно функционала ψ.

Установим поведение функций Шеннона $\lambda(n)$ и $R(n)$ для длины и ранга ДНФ ФАЛ из $P_2(n)$ соответственно.

Лемма 7.1. *Для любого $n, n \in \mathbb{N}$, имеют место соотношения*

$$\lambda(n) = 2^{n-1}, R(n) = n \cdot 2^{n-1}. \tag{7.1}$$

Доказательство. Нижние оценки (7.1) следуют из того,что $\lambda(l_n) = 2^{n-1}$ и $R(l_n) = n \cdot 2^{n-1}$, так как единственной ДНФ линейной ФАЛ $l_n = x_1 \oplus \cdots \oplus x_n$ является ее совершенная ДНФ. Для получения требуемых в (7.1) верхних оценок возьмем произвольную ФАЛ f из $P_2(n)$ и, в соответствии с (2.5), разложим ее по БП $x_2, \ldots, x_n$ следующим образом:

$$f(x_1, \ldots, x_n) = \bigvee_{\sigma''=(\sigma_2,\ldots,\sigma_n)} x_2^{\sigma_2} \cdots x_n^{\sigma_n} \cdot f\left(x_1, \sigma''\right) \tag{7.2}$$

Легко видеть, что после замены в разложении (7.2) каждой ФАЛ $f(x_1, \sigma'')$ равной ей ФАЛ из множества $\{0,\ 1,\ x_1,\ \overline{x}_1\}$ и приведения подобных мы получим ДНФ $\mathfrak{A}_f$ длины не больше, чем 2^{n-1}, что доказывает верхние оценки в (7.1).

Лемма доказана. □

При изучении того или иного связанного с ДНФ функционала ψ наряду с его максимальным значением, то есть функцией Шеннона $\psi(n)$, представляет интерес соответствующий отрезок "типичных" значений, то есть отрезок $[\psi'(n),\ \psi''(n)]$, в который попадают значения $\psi(f)$ для почти всех ФАЛ f из $P_2(n)$. Если при этом границы $\psi'(n)$ и $\psi''(n)$, где $n = 1, 2, \ldots$, асимптотически равны $\psi(n)$, то говорят, что для параметра ψ имеет место *эффект Шеннона.* Выясним некоторые особенности строения ДНФ у почти всех ФАЛ и установим, в частности, отсутствие эффекта Шеннона для параметров λ и R - длины и ранга ДНФ соответственно.

Введем дискретную векторную случайную величину $\xi^{(n)} = \left(\xi_{\widetilde{0}}, \ldots, \xi_{\widetilde{1}}\right)$, состоящую из 2^n независимых случайных величин $\xi_\alpha,\ \alpha \in B^n$, принимающих значения 0 и 1 с вероятностью $\frac{1}{2}$. При этом, очевидно, для любого α, $\alpha \in B^n$, выполняются равенства

$$\mathbb{E}\xi_\alpha = \frac{1}{2}, \qquad \mathbb{D}\xi_\alpha = \frac{1}{4}, \tag{7.3}$$

где $\mathbb{E}\theta$ и $\mathbb{D}\theta$ - математическое ожидание и дисперсия случайной величины θ (см., например, [25]).

Будем считать, что любая ФАЛ f из $P_2(n)$ является реализацией величины ξ, при которой $\xi_\alpha = f(\alpha)$ для любого $\alpha,\ \alpha \in B^n$, и что вероятность такой реализации равна 2^{-2^n}. Отсюда следует, что для любого множества $\mathcal{Q},\ \mathcal{Q} \subseteq P_2(n)$, отношение $|\mathcal{Q}|/2^{2^n}$, то есть доля тех ФАЛ f из $P_2(n)$, которые принадлежат $\mathcal{Q}$, равна вероятности того, что реализация случайной величины ξ принадлежит $\mathcal{Q}$.

Из независимости случайных величин $\xi_\alpha,\ \alpha \in B^n$, вытекает, что для их суммы $\widetilde{\xi}^{(n)} = \widetilde{\xi}$, которая равна мощности множества N_f для ФАЛ f, являющейся реализацией случайной величины $\xi^{(n)} = \xi$, в силу (7.3) справедливы равенства (см., например, [4])

$$\mathbb{E}\widetilde{\xi}^{(n)} = 2^{n-1}, \qquad \mathbb{D}\widetilde{\xi}^{(n)} = 2^{n-2}, \tag{7.4}$$

Полагая

$$t = \left\lceil n \cdot 2^{\frac{n}{2}} \right\rceil, \qquad I = \left(2^{n-1} - t, 2^{n-1} + t\right)$$

и применяя к случайной величине $\widetilde{\xi}$ с учетом (7.4) неравенство Чебышева [4], получим, что вероятность события $\widetilde{\xi} \notin I$, то есть доля тех ФАЛ f из $P_2(n)$, для которых $|N_f| \notin I$, не больше, чем

$$\frac{\mathbb{D}\eta}{t^2} \leqslant \frac{1}{4n^2}$$

и, следовательно, стремится к 0 при n стремящемся к бесконечности. Это означает, в частности, что для почти всех ФАЛ f из $P_2(n)$, выполнено равенство

$$|N_f| = 2^{n-1}\left(1 \pm O\left(n \cdot 2^{-n/2}\right)\right) \tag{7.5}$$

то есть длина совершенной ДНФ у почти всех ФАЛ из $P_2(n)$ асимптотически равна 2^{n-1}.

Лемма 7.2. *Для почти всех ФАЛ f, $f \in P_2(n)$, выполняются неравенства*

$$\lambda(f) \leqslant \frac{3}{4}2^{n-1}\left(1 + O\left(n \cdot 2^{-n/2}\right)\right), \tag{7.6}$$

$$\lambda(f) \leqslant \frac{3}{4}n \cdot 2^{n-1}\left(1 + O\left(n \cdot 2^{-n/2}\right)\right), \tag{7.7}$$

Доказательство. Пусть ФАЛ f, $f \in P_2(n)$, является реализацией случайной величины ξ. Для каждого набора β, $\beta \in B^{n-1}$, рассмотрим случайную величину $\eta_\beta = \xi_{(0,\beta)} \vee \xi_{(1,\beta)}$. Заметим, что случайные величины η_β, $\beta \in B^{n-1}$, независимы, а математическое ожидание и дисперсия любой из них равны $\frac{3}{4}$ и $\frac{3}{16}$ соответственно. Заметим также, что равенство $\eta_\beta = 1$ выполняется тогда и только тогда, когда в ДНФ $\mathfrak{A}_f$, построенной по лемме 7.1 для ФАЛ f, входит слагаемое, соответствующее набору β. Из независимости случайных величин η_β, $\beta \in B^{n-1}$, следует, что для их суммы $\widetilde{\eta} = \widetilde{\eta}^{(n)}$ выполняются соотношения

$$\mathbb{E}\widetilde{\eta}^{(n)} = \frac{3}{4}2^{n-1}, \qquad \mathbb{D}\widetilde{\eta}^{(n)} = \frac{3}{16}2^{n-1}. \tag{7.8}$$

Полагая

$$t = \left\lceil n \cdot 2^{\frac{n}{2}} \right\rceil, \qquad I = \left(\frac{3}{4}2^{n-1} - t, \frac{3}{4}2^{n-1} + t\right)$$

и проводя на основе (7.8) рассуждения аналогичные тем, с помощью которых из соотношений (7.4) выводилось равенство (7.5), получим, что $\lambda(\mathfrak{A}_f) \in I$ у не менее, чем $2^{2^n}\left(1 - \frac{1}{n^2}\right)$ ФАЛ f из $P_2(n)$. Это означает, что для почти всех ФАЛ f, $f \in P_2(n)$, длина и ранг её ДНФ $\mathfrak{A}_f$, построенной в соответствии с леммой 7.1, удовлетворяет (7.6), (7.7).

Лемма доказана. □

§8 Алгоритмические трудности минимизации ДНФ и оценки максимальных значений некоторых связанных с ней параметров. Теорема Ю. И. Журавлева о ДНФ сумма минимальных

Решение задач минимизации ДНФ для заданной ФАЛ характеризуется различными параметрами этой ФАЛ и, в первую очередь, значениями исследуемых функционалов ее сложности (см. §7). Кроме того, как отмечалось выше, ряд параметров (длина сокращенной ДНФ, число тупиковых или минимальных ДНФ и др.) характеризуют трудоемкость задачи минимизации ДНФ для рассматриваемой ФАЛ. В связи с этим представляет интерес поведение при $n = 1, 2, \ldots$, максимального значения того или иного подобного параметра ψ для ФАЛ из $P_2(n)$:

$$\psi(n) = \max_{f \in P_2(n)} \psi(f),$$

которое,как и в случае функционалов сложности, называют, обычно, функцией Шеннона для параметра ψ в классе ДНФ.

Будем обозначать значение функции Шеннона для параметров, равных числу[1] тупиковых ДНФ, числу минималь-

[1]Все ДНФ рассматриваются с точностью до перестановки ЭК и букв в них.

ных ДНФ и длине сокращенной ДНФ у ФАЛ из $P_2(n)$, через $\tau(n)$, $\mu\,(n)$ и $\lambda_{\text{сокр.}}(n)$ соответственно.

Из монотонности функционала ψ для сложности ДНФ (см. §7) следует, что ψ-минимальную ДНФ всегда можно выбрать среди тупиковых ДНФ, алгоритм построения которых описан в §6. Однако, как показывает следующее утверждение, ФАЛ могут иметь очень много различных тупиковых ДНФ, и даже число различных минимальных ДНФ у них может быть очень велико.

Лемма 8.1. *Число тупиковых (минимальных) ДНФ у ФАЛ f из $P_2\,(n)$, $n \geqslant 4$, вида*

$$f\,(x_1, \ldots, x_n) = g(x_1, x_2, x_3) \cdot (x_4 \oplus \cdots \oplus x_n),$$

где $\overline{N}_g = \{(000),\,(111)\}$, равно $5^{2^{n-4}}$ (соответственно $2^{2^{n-4}}$).

Доказательство. Из свойств линейной ФАЛ и свойств ФАЛ g вытекает, что (см. §1 и §4) любая простая импликанта K ФАЛ f имеет вид

$$K = K_i\,(x_1, x_2, x_3) \cdot x_4^{\beta_4} \cdots x_n^{\beta_n},$$

где K_i, $i = 1, \ldots, 6$, — простая импликанта ФАЛ g (см. рис. 2.2а и (2.10)) и $\beta_4 \oplus \cdots \oplus \beta_n = 1$. Таким образом, сокращенная ДНФ ФАЛ f с «геометрической» точки зрения состоит из 2^{n-4} циклов длины 6 (см. §4). Следовательно, любая тупиковая (минимальная) ДНФ ФАЛ f включает в себя одно из пяти (соответственно двух) реберных покрытий, связанных с тупиковыми (соответственно минимальными) ДНФ ФАЛ g, приведенными в (4.1)–(4.2) (соответственно (4.1)), для каждого из 2^{n-4} указанных циклов. Поэтому число тупиковых (минимальных) ДНФ ФАЛ f равно $5^{2^{n-4}}$ (соответственно $2^{2^{n-4}}$).

Лемма доказана. □

Следствие.

$$\tau(n) \geqslant 5^{2^{n-4}}, \mu_n(n) \geqslant 2^{2^{n-4}}.$$

Важным параметром, влияющим на размер таблицы Квайна и, следовательно, на трудоемкость задачи минимизации, является длина сокращенной ДНФ. Установим некоторые нижние оценки длины сокращенной ДНФ у ФАЛ от n БП, показывающие, в частности, что длина сокращенной ДНФ может быть существенно больше длины совершенной ДНФ той же ФАЛ.

Для $I \subseteq [0, n]$ через $\mathfrak{s}_n^I(x_1, \ldots, x_n)$ обозначим ФАЛ из $P_2(n)$, которая является характеристической ФАЛ объединения всех слоев куба B^n с номерами из I. При этом числа из I считаются *рабочими числами* ФАЛ $\mathfrak{s}_n^I$. Заметим, что ФАЛ $\mathfrak{s}_n^I$ является *симметрической*, то есть не изменяет свое значение при любой перестановке аргументов, и наоборот, любая симметрическая функция алгебры логики совпадает с одной из ФАЛ вида $\mathfrak{s}_n^I$. Заметим также, что отличная от константы симметрическая ФАЛ является существенной ФАЛ. Легко видеть, что рабочими числами симметрических ФАЛ ℓ_n и $\overline{\ell}_n$ являются все нечетные и все четные числа отрезка $[0, n]$ соответственно.

Симметрическая ФАЛ называется *поясковой*, если ее рабочие числа образуют отрезок. Поясковой ФАЛ является, в частности, ФАЛ голосования $H(x_1, x_2, x_3) = \mathfrak{s}_3^{[2,3]}$, а также ФАЛ $g = \mathfrak{s}_3^{[1,2]}$, показанная на рис. 2.2а. Легко видеть, что сокращенная ДНФ поясковой ФАЛ $\mathfrak{s}_n^{[r,p]}(x_1, \ldots, x_n)$, где $0 \leqslant r \leqslant p \leqslant n$, состоит из всех ЭК ранга $(n + r - p)$, которые содержат r БП и $(n - p)$ отрицаний БП, то есть имеет вид

$$\mathfrak{s}_n^{[r,p]}(x_1, \ldots, x_n) = \bigvee_{\substack{1 \leqslant i_1 < \cdots < i_{n+r-p} \leqslant n \\ \sigma_1 + \cdots + \sigma_{n+r-p} = r}} x_{i_1}^{\sigma_1} \cdots x_{i_{n+r-p}}^{\sigma_{n+r-p}}. \qquad (8.1)$$

Из (8.1) следует, что длина сокращенной ДНФ ФАЛ $\mathbf{s}_n^{[r,p]}$ равна $\binom{n}{r} \cdot \binom{n-p}{n-r}$, и поэтому при $r = n - p = \left\lceil \frac{n}{3} \right\rceil$ она в соответствии с формулой Стирлинга (1.3) не меньше, чем $e_1 \frac{3^n}{n}$, где e_1 — некоторая константа. Таким образом, доказано следующее утверждение:

Лемма 8.2.

$$\lambda_{сокр.}(n) \geqslant e_1 \frac{3^n}{n},$$

где e_1 — некоторая константа.

Рассмотренные примеры показывают, что с алгоритмической точки зрения задача минимизации ДНФ является очень трудоемкой задачей. В теории сложности вычислений, где трудоемкость алгоритма определяется, обычно, числом битовых операций, необходимых для его выполнения в «худшем» случае, выделен целый класс так называемых NP-полных проблем, которые считаются алгоритмически трудными (см., например, [1, 23]). К NP-полным проблемам относится, в частности, проблема выполнимости КНФ, которая состоит в том, чтобы по заданной КНФ выяснить, равна тождественно нулю реализуемая ею ФАЛ или нет. Таким образом, даже построение сокращенной ДНФ из КНФ (см. §3) является алгоритмически трудной задачей.

С другой стороны, Ю.И. Журавлев [9, 6] предложил применительно к ДНФ модель так называемых локальных или окрестностных алгоритмов, когда преобразование рассматриваемой грани однозначно определяется «состоянием» ее «окрестности» заданного порядка (см. §4). Он же (см. теорему 8.1) доказал, что при построении минимальной ДНФ для ФАЛ из $P_2(n)$, $n \geqslant 3$, приходится, в общем случае, рассматривать окрестности порядка $(n-3)$ ее максимальных граней. Следовательно, задача минимизации ДНФ является трудной и с точки зрения уровня локальности используемых алгоритмов.

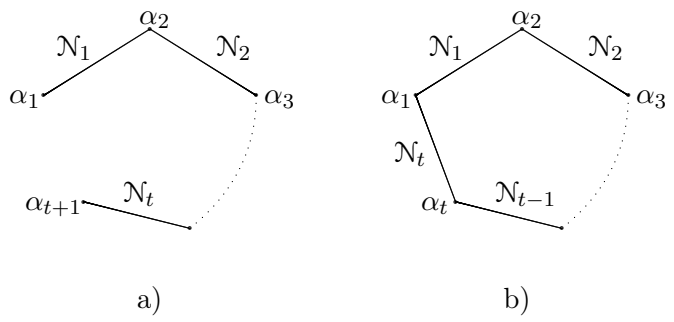

Рис. 8.1: множество N_f для цепной и циклической ФАЛ f

Определим ДНФ сумма минимальных ФАЛ f (ДНФ ΣM ФАЛ f) как дизъюнкцию всех тех её простых импликант, которые входят хотя бы в одну минимальную ДНФ ФАЛ f.

Функция $f(x_1, \ldots, x_n)$ называется *цепной* (*циклической*) *функцией длины* t, если ее сокращенная ДНФ с «геометрической» точки зрения представляет собой цепь (соответственно цикл) из t последовательно соединенных ребер $\mathcal{N}_1$, $\mathcal{N}_2$, $\ldots$, $\mathcal{N}_t$ куба B^n (см. рис. 8.1a и 8.1b). Заметим, что циклическая ФАЛ длины t существует тогда и только тогда, когда $t \geqslant 6$ — четное число, а цепная ФАЛ длины t — при любом $t \geqslant 1$. Пример цепной ФАЛ длины 3 дает ФАЛ g'', показанная на рис. 4.1, а ФАЛ g (см. рис. 2.1a) является циклической ФАЛ длины 6.

Из теоремы 4.1 следует, в частности, что для любой цепной ФАЛ длины не меньше 4 и любой циклической ФАЛ ДНФ ΣT совпадает с сокращенной ДНФ. При этом цепная ФАЛ f нечетной длины $t = 2k - 1 \geqslant 3$ имеет единственную минимальную ДНФ, которая совпадает с ее ДНФ ΣM и соответствует покрытию (см. рис. 8.1a) $\mathcal{N}_1 \cup \mathcal{N}_3 \cup \ldots \cup \mathcal{N}_t$ длины k. Действительно, множество N_f в данном случае состоит из $2k$ наборов и не может быть покрыто $(k-1)$ ребром. Кро-

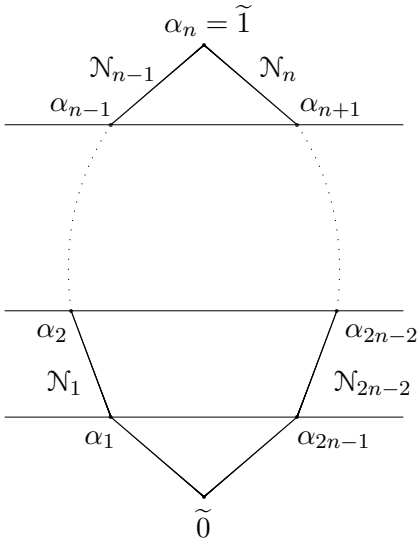

Рис. 8.2: цепная ФАЛ длины $(2n-2)$ в кубе B^n

ме того, покрытие множества N_f, состоящее из k ребер, не может включать в себя ребра с общими вершинами и должно содержать ядровые ребра $\mathcal{N}_1$ и $\mathcal{N}_t$ ФАЛ f. Легко видеть, что только покрытие $\mathcal{N}_1 \cup \mathcal{N}_3 \cup \ldots \cup \mathcal{N}_t$ обладает всеми этими свойствами. Таким образом, для цепной ФАЛ нечетной длины t, $t \geqslant 5$, ДНФ ΣT не совпадает с ДНФ ΣM.

Теорема 8.1 (ср. [6, 23, 10]). *При любом $n \in \mathbb{N}$, $n \geqslant 3$, в $P_2(n)$ существуют ФАЛ f' и f'', имеющие общую простую импликанту K, которая входит в ДНФ ΣM одной, но не входит в ДНФ ΣM другой из этих ФАЛ и для которой $S_{n-3}(N_K, f') = S_{n-3}(N_K, f'')$.*

Доказательство. Достаточно построить в $P_2(n)$ цепную функцию f четной длины $t = 2k \geqslant 2n-2 \geqslant 4$. Действительно, если указанная ФАЛ f найдена, а ее множество N_f соответ-

ствует рис. 8.1а, то, полагая

$$N_{f'} = N_f \setminus \{\alpha_1\} \quad \text{и} \quad N_{f''} = N_f \setminus \{\alpha_{t+1}\},$$

получим цепные ФАЛ f' и f'' нечетной длины $2k-1$ такие, что каждое ребро $\mathcal{N}_i$, где $i = 2, \ldots, t-1$, входит в ДНФ ΣM одной из них, но не входит в ДНФ ΣM другой. При этом, очевидно, $S_{k-2}(\mathcal{N}_k, f') = S_{k-2}(\mathcal{N}_k, f'')$ и, следовательно, искомая ЭК K соответствует ребру $\mathcal{N}_k$.

Для завершения доказательства возьмем в качестве f цепную ФАЛ длины $(2n-2)$, у которой множество N_f состоит из всех наборов $\alpha_i = (\underbrace{1, \ldots, 1}_{i}, \underbrace{0, \ldots, 0}_{n-i})$, где $i \in [1, n]$, и наборов $\alpha_{n+i} = \overline{\alpha}_i$, $i \in [1, n)$, а ребро с номером j, $j \in [1, 2n-2]$, имеет вид $\mathcal{N}_j = \{\alpha_j, \alpha_{j+1}\}$ (см. рис. 8.2) и применим к ней описанные выше построения.

Теорема доказана. □

Замечание 1. Из теоремы следует, что критерий вхождения ЭК в ДНФ ΣM не имеет такого локального характера, как критерий вхождения ЭК в ДНФ ΣT (сравните с теоремой 4.1).

Замечание 2. Известно [7], что при $n \geqslant 14$ в $P_2(n)$ имеется цепная ФАЛ четной длины t, $t \geqslant 2^{n-11} - 4$, на основе которой справедливость теоремы можно установить для окрестности порядка $\left(\frac{t}{2} - 2\right)$ (см. доказательство).

Литература

[1] *Алексеев В. Б.* Введение в теорию сложности алгоритмов. М.: Издательский отдел ф-та ВМиК МГУ, 2002.

[2] *Алексеев В. Б., Вороненко А. А., Ложкин С. А., Романов Д. С., Сапоженко А. А., Селезнева С. Н.* Задачи по курсу «Основы кибернетики». Издательский отдел ф-та ВМиК МГУ, 2002.

[3] *Алексеев В. Б., Ложкин С. А.* Элементы теории графов, схем и автоматов. М.: Издательский отдел ф-та ВМиК МГУ, 2000.

[4] *Боровков А. А.* Курс теории вероятностей. М.: Наука, 1976.

[5] *Гаврилов Г. П., Сапоженко А. А.* Задачи и упражнения по дискретной математике. 3-е изд., перераб. М.: ФИЗМАТЛИТ, 2004.

[6] Дискретная математика и математические вопросы кибернетики, под редакцией *С. В. Яблонского* и *О. Б. Лупанова.* Т. 1. М.: Наука, 1974.

[7] *Евдокимов А. А.* О максимальной длине цепи в единичном n-мерном кубе // Матем. заметки. 1969. 6. №3. С. 309–319.

[8] *Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И.* Лекции по теории графов. М.: Наука, 1977.

[9] *Журавлев Ю. И.* Локальные алгоритмы вычисления информации // Кибернетика. №1. 1965. С. 12–19.

[10] *Журавлев Ю. И.* Теоретико-множественные методы в алгебре логики // Проблемы кибернетики. Вып. 8. М.: Физматгиз, 1962. С. 5-44.

[11] *Кузъмин В. А.* Оценки сложности реализации функций алгебры логики простейшими видами бинарных программ // Сб. «Методы дискретного анализа в теории кодов и схем». Новосибирск, 1976. Вып. 29. С. 11–39

[12] *Ложкин С. А.* Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. М.: Наука, 1996. С. 189–214.

[13] *Ложкин С. А.* Структурное моделирование и декомпозиция для некоторых классов схем. М.: Издательский отдел ф-та ВМиК МГУ, 2001.

[14] *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.

[15] *Лупанов О. Б.* О сложности реализации функций алгебры логики релейно-контактными схемами // Проблемы кибернетики. Вып. 11. М.: Наука, 1964. С. 25–48.

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

[17] *Лупанов О. Б.* Об одном подходе к синтезу управляющих систем — принципе локального кодирования.

// Проблемы кибернетики. Вып. 14. М.: Наука, 1965. С. 31–110.

[18] *Мурога С.* Системы проектирования сверхбольших интегральных схем. М.: Мир, 1985.

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

[20] *Нигматуллин Р. Г.* Сложность булевых функций. М.: Наука, 1991.

[21] *Поваров Г. Н.* Метод синтеза вычислительных и управляющих контактных схем // Автоматика и телемеханика. 1957. Т. 18. №2. С. 145–162.

[22] *Сапоженко А. А.* Дизъюнктивные нормальные формы. М.: Изд-во МГУ, 1975.

[23] *Сапоженко А. А.* Некоторые вопросы сложности алгоритмов. Издательский отдел ф-та ВМиК МГУ, 2001.

[24] *Сапоженко А. А., Ложкин С. А.* Методы логического проектирования и оценки сложности схем на дополняющих МОП-транзисторах // Микроэлектроника. 1983. Т. 12. №1. С. 42–47.

[25] *Фихтенгольц Г. М.* Основы математического анализа, том 1. М.: Наука, 1968.

[26] *Фихтенгольц Г. М.* Основы математического анализа, том 2. М.: Наука, 1964.

[27] *Чегис И. А., Яблонский С. В.* Логические способы контроля работы электрических схем // Труды МИ АН СССР. Т. 51. М.: Изд-во АН СССР, 1958. С. 270–360.

[28] *Яблонский С. В.* Введение в дискретную математику. 2-е изд., перераб. и доп. М.: Наука, 1986.

[29] *Яблонский С. В.* Надежность управляющих систем. М.: Изд-во МГУ, 1991.

[30] *Яблонский С. В.* Некоторые вопросы надежности и контроля управляющих систем // Математические вопросы кибернетики. Вып. 1. М.: Наука, 1988. С. 5–25.

[31] *Яблонский С. В.* Элементы математической кибернетики. М.: Высшая школа, 2007.

[32] *Cardot C.* Quelques resultats sur l'application de l'algèbre de Boole à la synthèse des circuits a relais // Ann. Telecommunications. 1952. V.7. №2. P. 75–84.

[33] *Shannon C. E.* The syntesis of two-terminal switching circuits // Bell Syst. Techn. J. 1949. V. 28. №1. P. 59–98 (Русский перевод: *Шеннон К.* Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 59–101).

[34] *Wegener I.* Branching programs and binary decision diagrams. SIAM Publishers, 2000.