Московский Государственный Университет
имени М. В. Ломоносова
Факультет Вычислительной Математики и Кибернетики
Кафедра Математической Кибернетики

Основы кибернетики

С. А. Ложкин

Москва 2003

Оглавление

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, []). 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, []),

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

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 [] следует, что[1]

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

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[2]

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

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[3]

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

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 отношение эквивалентности τ, заданное на множестве A, порождает разбиение этого множества на классы τ-эквивалентности — максимальные

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

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

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

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

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 $a'\tau a''$.

По умолчанию все рассматриваемые далее множества считаются конечными. Для частично упорядоченного множества (A, τ) множество, состоящее из попарно сравнимых (несравнимых) элементов множества A, называется *цепью* (соответственно *антицепью*) этого частично упорядоченного множества. Заметим, что цепь $C \subseteq A$ в частично упорядоченном множестве (A, τ) представляет собой линейно упорядоченное множество вида (C, τ). Максимальная мощность цепей (антицепей) частично упорядоченного множества называется его *длиной* (соответственно *шириной*). Цепь или антицепь частично упорядоченного множества называется *неуплотняемой*, если она представляет собой максимальное по включению множество соответствующего типа.

Частично упорядоченное множество (A, τ) длины t называется *ранжированным частично упорядоченным множеством*, если все его неуплотняемые цепи имеют мощность t. При этом каждый элемент A имеет, очевидно, один и тот же номер в любой содержащей его неуплотняемой цепи, а все элементы из A, для которых указанный номер равен i, $i \in [0, t)$, образуют i-й *ярус* данного частично упорядоченного множества (A, τ). Заметим, что каждый ярус ранжированного частично упорядоченного множества является его неуплотняемой антицепью.

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 [], 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, $i \in [1, n]$, определена формула $\mathcal{F}_i$ глубины q_i над множеством Б, которая реализует функцию f_i из $\mathcal{P}_A$, то запись $\mathcal{F}$ вида

$$\mathcal{F} = \varphi(\mathcal{F}_1, \ldots, \mathcal{F}_k)$$

является *формулой глубины* $q = \max\{q_1, \ldots, q_k\} + 1$ *над* Б, которая реализует функцию f вида $f = \varphi(f_1, \ldots, f_k)$. Все записи, полученные в результате указанного индуктивного построения, и только они считаются *формулами над множеством* Б. Под *сложностью* (*рангом*) формулы $\mathcal{F}$ понимается число вхождений в нее ФС (соответственно символов переменных), которое обозначается $L(\mathcal{F})$ (соответственно, $R(\mathcal{F})$).

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 [], в Б могут присутствовать ФАЛ, при удалении которых оставшееся множество продолжает быть полным.

§2 Гиперкуб и функции алгебры логики. Дизъюнктивные нормальные формы и связанные с ними разложения функций

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 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 $\beta \leqslant \alpha$ ($\alpha \not\leqslant \beta$ и $\beta \not\leqslant \alpha$), называются *сравнимыми* (соответственно *несравнимыми*). Заметим, что пара $(B^n, \leqslant)$ задает ранжированное частично упорядоченное множество (см. §1) длины $n+1$, где при любом $i \in [0,n]$ множество B_i^n образует i-й ярус, а наборы

с номерами i и $i+1$, $i \in [0,n)$, в любой неуплотняемой цепи являются соседними наборами куба.

Лемма 2.1. *Ширина частично упорядоченного множества* $(B^n, \leqslant)$ *равна* $\binom{n}{\lceil \frac{n}{2} \rceil}$.

Доказательство. Легко видеть, что число неуплотняемых цепей частично упорядоченного множества $(B^n, \leqslant)$ равно $n!$ и что через каждый набор $\alpha \in B^n_i$ проходит $i!\,(n-i)!$ таких цепей. Пусть $A' \subseteq B^n$ — неуплотняемая антицепь частично упорядоченного множества $(B, \leqslant)$ и пусть $A'_i = B^i_n \cap A'$ для всех $i \in [0,n)$. Заметим, что каждая неуплотняемая цепь частично упорядоченного множества $(B, \leqslant)$ содержит не более одного элемента множества A' и поэтому, с учетом сказанного выше,

$$\sum_{i=0}^{n} |A'_i| \cdot (i!) \cdot (n-i)! \leqslant n!,$$

откуда следует, что

$$\sum_{i=0}^{n} |A'_i| = |A'| \leqslant \max_{i \in [0,n]} \binom{n}{i}.$$

Нетрудно убедиться в том, что неравенства

$$\binom{n}{i} < \binom{n}{i+1} \text{ и } 2i+1 < n$$

равносильны, если i изменяется на отрезке $[0,n]$. Таким образом, максимальное по i значение величины $\binom{n}{i}$ на отрезке $[0,n]$ достигается при $i = \lceil \frac{n}{2} \rceil$ и равно $\binom{n}{\lceil \frac{n}{2} \rceil}$. Следовательно, множество $B^n_{\lceil \frac{n}{2} \rceil}$ является максимальной по числу элементов антицепью куба B^n. Лемма доказана. □

Замечание 1. Аналогичным образом доказывается, что если в ранжированном частично упорядоченном множестве через каждые два элемента одного и того же яруса проходит одинаковое число неуплотняемых цепей, то ширина этого частично упорядоченного множества равна максимальной мощности его ярусов.

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 $i \in [1,n]$ 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 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 $\aleph_1, \ldots, \aleph_6$,

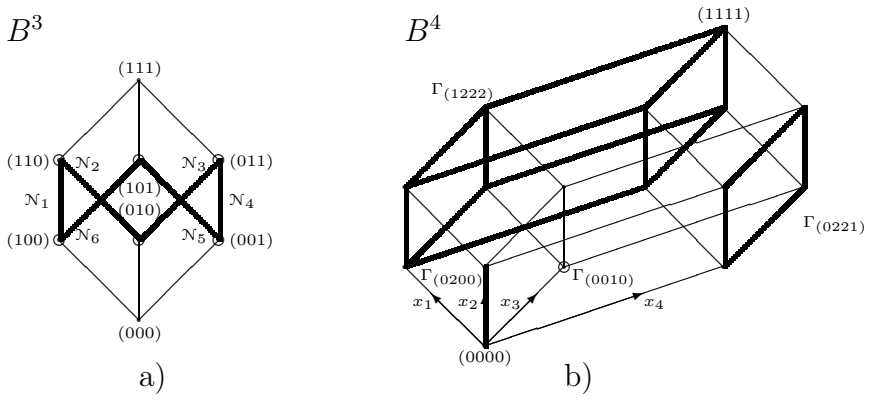


Рис. 2.1: B^3 и B^4, примеры граней

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 r в кубе B^n, где $\gamma = (\alpha, 2, \ldots, 2)$ и $\alpha \in B^r$, соответствует отрезку куба длины 2^{n-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) $\mathfrak{X} = \{x_1, x_2, \ldots, x_n, \ldots\}$ и будем рассматривать функции алгебры логики (ФАЛ) или, иначе, булевы функции от переменных из $\mathfrak{X}$, а множество всех таких функций будем обозначать через $P_2(\mathfrak{X})$ или P_2 Будем предполагать также, что каждый рассматриваемый n-мерный куб имеет вид $B^n = B^n(X)$, где множество переменных $X = \{x_{j_1}, \ldots, x_{j_n}\} \subset \mathfrak{X}$ 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 $\mathfrak{X}$ 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 $k \in [1, n)$

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 $P_2\,(2)$

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 $\oplus$. Заметим, также, что имеют место тождества[1]

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

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

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 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 $\overline{x}_1\overline{x}_2x_3\overline{x}_4$, $\overline{x}_1\overline{x}_3\overline{x}_4$, $x_1\overline{x}_4$ 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.

[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.

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_2 / x_3 / x_1	0 0	1 1
0	0	1
1	1	1

b)

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

c)

Рис. 2.3: функция голосования

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:

$$f(x_1,\ldots,x_n)=\bigvee_{(\alpha_1,\ldots,\alpha_n)\in N_f} x_1^{\alpha_1}\ldots x_n^{\alpha_n}=\bigwedge_{(\beta_1,\ldots,\beta_n)\in\overline{N}_f}\left(x_1^{\overline{\beta}_1}\vee\ldots\vee x_n^{\overline{\beta}_n}\right). \tag{2.3}$$

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 (2.3), 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.

Номер $\nu(\alpha)$ набора $\alpha=(\alpha_1,\ldots,\alpha_n)$ из B^n считается *номером* ЭК (ЭД) ранга n от БП $X(n)$ вида $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ (соответственно $x_1^{\overline{\alpha}_1}\vee\ldots\vee x_n^{\overline{\alpha}_n}$), а система из всех таких ФАЛ, упорядоченных по их номерам, называется *конъюнктивным* (соответственно *дизъюнктивным*) *дешифратором порядка* n от БП $x_1,\ldots,x_n$ и обозначается через Q_n (соответственно J_n). Функция вида

$$\mu(x_1,\ldots,x_n,y_0,\ldots,y_{2^n-1})=\bigvee_{\alpha=(\alpha_1,\ldots,\alpha_n)} x_1^{\alpha_1}\cdots x_n^{\alpha_n}y_{\nu(\alpha)}$$

называется *мультиплексорной функцией* или, иначе, *мультиплексором порядка* n. При этом переменные $x=(x_1,\ldots,x_n)$ $(y=(y_0,\ldots,y_{2^n-1}))$ считаются *адресными* (соответственно *информационными*) БП мультиплексора μ_n.

Мультиплексорную ФАЛ порядка $(n-q)$, $0\leqslant q<n$, от адресных БП $x''=$ $=(x_{q+1},\ldots,x_n)$ и информационных БП $y=(y_0,\ldots,y_{2^{n-q}-1})$ часто используют для разложения произвольной ФАЛ $f(x_1,\ldots,x_n)$ по БП x'', которое обобщает совершенную ДНФ (2.3) следующим образом:

$$f(x',x'')=\bigvee_{\sigma''=(\sigma_{q+1},\ldots,\sigma_n)} x_{q+1}^{\sigma_{q+1}}\cdots x_n^{\sigma_n}f_{\sigma''}(x')=\mu_{n-q}(x'',f_{\widetilde{0}}(x'),\ldots,f_{\widetilde{1}}(x')), \tag{2.4}$$

где $x'=(x_1,\ldots,x_q)$ и $f_{\sigma''}(x')=f(x',\sigma'')$. Заметим, что при $q=0$ все «остаточные» ФАЛ $f_{\sigma''}(x')$ являются константами.

Представление (2.4), в свою очередь, можно обобщить следующим образом. Пусть $\Delta = (\delta_1, \ldots, \delta_p)$ — разбиение куба B^n, а $\chi_i,\ i \in [1,p]$, — характеристическая ФАЛ компоненты δ_i и пусть

$$\mu_\Delta(x, y_1, \ldots, y_p) = \bigvee_{i=1}^{p} \chi_i(x)\, y_i = \bigwedge_{i=1}^{p} (\overline{\chi}_i(x) \vee y_i), \tag{2.5}$$

где $x = (x_1, \ldots, x_n)$, — так называемая *мультиплексорная функция разбиения* Δ. Тогда любую ФАЛ f из $P_2(n)$ можно представить в виде

$$f(x) = \bigvee_{i=1}^{p} g_i(x)\, \chi_i(x) = \mu_\Delta(x, g_1(x), \ldots, g_p(x)), \tag{2.6}$$

где $g_i,\ i \in [1,p]$, — произвольная ФАЛ из $P_2(n)$, совпадающая с f на δ_i. Заметим, что для разложения ФАЛ можно использовать как дизъюнктивные варианты представлений (2.4), (2.6), так и конъюнктивные варианты этих представлений, связанные с конъюнктивным разложением (2.5).

§3 Эквивалентные преобразования формул. Полнота системы основных тождеств для формул базиса $\{\&, \vee, \neg\}$

Рассмотрим вопросы, связанные с эквивалентными преобразованиями формул над базисом Б на основе тождеств. Для того, чтобы выделить набор $x = (x_{i_1}, \ldots, x_{i_n})$, который состоит из всех различных БП алфавита $\mathcal{X}$, встречающихся в формуле $\mathcal{F}$ и перечисленных в порядке возрастания их номеров, будем записывать ее в виде $\mathcal{F} = \mathcal{F}(x)$. При этом формулу, которая получается из $\mathcal{F}$ в результате замены каждого вхождения БП $x_{i_j},\ j = 1, \ldots, n$, формулой $\mathcal{F}_j$ будем считать *результатом подстановки формулы* $\mathcal{F}_j$ *вместо БП* $x_{i_j},\ j = 1, \ldots, n$, *в формулу* $\mathcal{F}$ и будем обозначать ее через $\mathcal{F}(\mathcal{F}_1, \ldots, \mathcal{F}_n)$. Заметим, что формула $\mathcal{F}(\mathcal{F}_1, \ldots, \mathcal{F}_n)$ реализует ФАЛ $f(f_1, \ldots, f_n)$, где ФАЛ f (ФАЛ f_j) — ФАЛ, реализуемая формулой $\mathcal{F}$ (соответственно $\mathcal{F}_j,\ j = 1, \ldots, n$). Отсюда следует, что если указанную подстановку применить к обеим частям тождества $t : \mathcal{F}' = \mathcal{F}''$, где $\mathcal{F}' = \mathcal{F}'(x)$ и $\mathcal{F}'' = \mathcal{F}''(x)$, мы получим тождество

$$\widehat{t} :\ \widehat{\mathcal{F}}' = \widehat{\mathcal{F}}'',$$

где $\widehat{\mathcal{F}}' = \mathcal{F}'(\mathcal{F}_1, \ldots, \mathcal{F}_n)$ и $\widehat{\mathcal{F}}'' = \mathcal{F}''(\mathcal{F}_1, \ldots, \mathcal{F}_n)$, которое называется *подстановкой для тождества* t.

Формулы, полученные в процессе индуктивного построения (см. §1) формулы $\mathcal{F}$, называются ее *подформулами*. При этом подформулы, из которых на последнем шаге

индуктивного построения получается $\mathcal{F}$, считаются ее *главными* подформулами. Из определений следует, что для формул имеет место так называемый принцип эквивалентной замены. Это означает, что если подформулу $\widehat{\mathcal{F}}'$ (подформулу $\widehat{\mathcal{F}}''$) формулы $\mathcal{F}$ заменить, учитывая тождество $\widehat{t}$ эквивалентной ей формулой $\widehat{\mathcal{F}}''$ (соответственно $\widehat{\mathcal{F}}'$), то полученная в результате такой замены формула $\check{\mathcal{F}}$ будет эквивалентна формуле $\mathcal{F}$, то есть будет справедливо тождество

$$\check{t}:\ \mathcal{F}=\check{\mathcal{F}}.$$

Указанный переход от $\mathcal{F}$ к $\check{\mathcal{F}}$ (от t к $\check{t}$) будем записывать в виде однократной выводимости вида $\mathcal{F}\underset{t}{\mapsto}\check{\mathcal{F}}$ (соответственно $t\mapsto\check{t}$). Аналогичный переход от $\mathcal{F}$ к $\widetilde{\mathcal{F}}$ в результате применения одного из тождеств системы τ (нескольких последовательных применений тождеств из τ) будем записывать в виде однократной (соответственно кратной) выводимости вида $\mathcal{F}\underset{\tau}{\mapsto}\widetilde{\mathcal{F}}$ (соответственно $\mathcal{F}\underset{\tau}{\models}\widetilde{\mathcal{F}}$). При этом считается, что тождество

$$\widetilde{t}:\ \mathcal{F}=\widetilde{\mathcal{F}}$$

выводится из системы тождеств τ, и этот факт записывается в виде выводимости $\tau\mapsto\widetilde{t}$ или $\tau\models\widetilde{t}$ в зависимости от числа использованных переходов. Переход вида $\mathcal{F}\underset{\tau}{\models}\widetilde{\mathcal{F}}$ будем называть также *эквивалентным преобразованием (ЭП) формулы* $\mathcal{F}$ *в формулу* $\widetilde{\mathcal{F}}$ *на основе системы тождеств* τ. Заметим, что в силу обратимости ЭП из выводимости $\mathcal{F}\underset{\tau}{\models}\widetilde{\mathcal{F}}$ следует обратная выводимость $\widetilde{\mathcal{F}}\underset{\tau}{\models}\mathcal{F}$. Система тождеств τ называется *полной* для ЭП формул над Б, если для любых двух эквивалентных формул $\mathcal{F}'$ и $\mathcal{F}''$ над Б имеет место выводимость $\mathcal{F}'\underset{\tau}{\models}\mathcal{F}''$.

Далее до конца главы будем рассматривать только формулы над базисом Б_0 и будем называть их просто формулами[1]. Заметим, что имеют место (см., в частности, §1) следующие тождества ассоциативности

$$t^{\text{А}}_{\circ}:\ x_1\circ(x_2\circ x_3)=(x_1\circ x_2)\circ x_3,$$

тождества коммутативности

$$t^{\text{К}}_{\circ}:\ x_1\circ x_2=x_2\circ x_2$$

и тождества отождествления БП

$$t^{\text{ОП}}_{\circ}:\ x\circ x=x,$$

[1]Эквивалентные преобразования формул в произвольном базисе будут рассмотрены во второй главе.

где $\circ \in \{\&, \vee\}$, тождества дистрибутивности «$\circ$» относительно «$\diamond$»

$$t^{\mathrm{D}}_{\circ,\diamond}:\ x_1 \circ (x_2 \diamond x_3) = (x_1 \circ x_2) \diamond (x_1 \circ x_3)$$

и тождества («правила») де Моргана

$$t^{\mathrm{M}}_{\neg}:\ \overline{(\overline{x}_1)} = x_1, \quad t^{\mathrm{M}}_{\circ}:\ \overline{(x_1 \circ x_2)} = (\overline{x}_1) \diamond (\overline{x}_2)\,,$$

где $(\circ, \diamond) \in \{(\&, \vee)\,, (\vee, \&)\}$, тождества подстановки констант[1]

$$t^{\text{ПК}}_{0,\&} : x_1\,(x_2 \cdot \overline{x}_2) = x_2 \cdot \overline{x}_2, \qquad t^{\text{ПК}}_{1,\&} : x_1\,(x_2 \vee \overline{x}_2) = x_1,$$
$$t^{\text{ПК}}_{0,\vee} : x_1 \vee x_2 \cdot \overline{x}_2 = x_1, \qquad t^{\text{ПК}}_{1,\vee} : x_1 \vee (x_2 \vee \overline{x}_2) = x_2 \vee \overline{x}_2,$$

а также тождество поглощения

$$t^{\text{П}}:\ x_1 \vee x_1 x_2 = x_1,$$

тождество обобщенного склеивания

$$t^{\text{ОС}}:\ x_1x_2 \vee \overline{x}_1x_3 = x_1x_2 \vee \overline{x}_1x_3 \vee x_2x_3$$

и другие.

Рассмотрим теперь примеры ЭП формул. Докажем, что

$$\left\{t^{\mathrm{M}}_{\&},\, t^{\mathrm{M}}_{\neg}\right\} \rightleftarrows \left\{t^{\mathrm{M}}_{\vee}\right\} \quad \text{и} \quad \left\{t^{\mathrm{K}}_{\&},\, \tau^{\mathrm{M}}\right\} \rightleftarrows \left\{t^{\mathrm{K}}_{\vee}\right\},$$

где $\tau^{\mathrm{M}} = \left\{t^{\mathrm{M}}_{\&},\, t^{\mathrm{M}}_{\neg},\, t^{\mathrm{M}}_{\vee}\right\}$. Действительно,

$$\overline{x_1 \vee x_2} \underset{t^{\mathrm{M}}_{\neg}}{\rightleftarrows} \overline{\left(\overline{\overline{x}}_1\right) \vee \left(\overline{\overline{x}}_2\right)} \underset{t^{\mathrm{M}}_{\&}}{\mapsto} \overline{\overline{(\overline{x}_1) \cdot (\overline{x}_2)}} \underset{t^{\mathrm{M}}_{\neg}}{\mapsto} \overline{x}_1 \cdot \overline{x}_2$$

и

$$x_1 \vee x_2 \underset{t^{\mathrm{M}}_{\neg}}{\mapsto} \overline{\overline{x_1 \vee x_2}} \underset{t^{\mathrm{M}}_{\vee}}{\mapsto} \overline{\overline{x}_1 \cdot \overline{x}_2} \underset{t^{\mathrm{K}}_{\&}}{\mapsto} \overline{\overline{x}_2 \cdot \overline{x}_1} \underset{t^{\mathrm{M}}_{\&},\, t^{\mathrm{M}}_{\neg}}{\rightleftarrows} x_2 \vee x_1.$$

Аналогичным образом доказывается, что

$$\left\{t^{\mathrm{A}}_{\&},\, \tau^{\mathrm{M}}\right\} \rightleftarrows \left\{t^{\mathrm{A}}_{\vee}\right\},\ \left\{t^{\text{ОП}}_{\&},\, \tau^{\mathrm{M}}\right\} \rightleftarrows \left\{t^{\text{ОП}}_{\vee}\right\},\ \left\{t^{\mathrm{D}}_{\&,\vee},\, \tau^{\mathrm{M}}\right\} \rightleftarrows \left\{t^{\mathrm{D}}_{\vee,\&}\right\} \text{ и } \left\{t^{\text{ПК}}_{\sigma,\&},\, \tau^{\mathrm{M}}\right\} \rightleftarrows \left\{t^{\text{ПК}}_{\overline{\sigma},\vee}\right\},$$

где $\sigma \in \{0, 1\}$. Завершая примеры выводимостей, докажем, что

$$\left\{t^{\text{ПК}}_{1,\&},\, t^{\mathrm{D}}_{\&,\vee},\, t^{\mathrm{A}}_{\vee},\, t^{\mathrm{K}}_{\vee},\, t^{\text{ОП}}_{\vee}\right\} \rightleftarrows t^{\text{П}}.$$

[1] В отличие от (2.1)–(2.2) тождества подстановки констант приведены для базиса Б_0, где роль константы 0 (константы 1) играет формула вида $x_i \cdot \overline{x}_i$ (соответственно $x_i \vee \overline{x}_i$).

Действительно,

$$x_1 \vee x_1x_2 \underset{t^{\text{ПК}}_{1,\&}}{\longmapsto} x_1\left(x_2 \vee \overline{x}_2\right) \vee x_1x_2 \underset{t^{\text{D}}_{\&,\vee}}{\longmapsto} x_1\left(\left(x_2 \vee \overline{x}_2\right) \vee x_2\right)$$
$$\underset{t^{\text{A}}_{\vee},t^{\text{K}}_{\vee}}{\models} x_1\left(\left(x_2 \vee x_2\right) \vee \overline{x}_2\right) \underset{t^{\text{ОП}}_{\vee}}{\longmapsto} x_1\left(x_2 \vee \overline{x}_2\right) \underset{t^{\text{ПК}}_{1,\&}}{\longmapsto} x_1.$$

Положим

$$\begin{aligned}
\tau^{\text{осн}} &= \left\{t^{\text{M}}_{\&},\, t^{\text{M}}_{\neg},\, t^{\text{A}}_{\&},\, t^{\text{K}}_{\&},\, t^{\text{ОП}}_{\&},\, t^{\text{D}}_{\&,\vee},\, t^{\text{ПК}}_{1,\&},\, t^{\text{ПК}}_{0,\&}\right\},\\
\tau^{\text{A}} &= \left\{t^{\text{A}}_{\&},\, t^{\text{A}}_{\vee}\right\},\\
\tau^{\text{K}} &= \left\{t^{\text{K}}_{\&},\, t^{\text{K}}_{\vee}\right\},\\
\tau^{\text{ОП}} &= \left\{t^{\text{ОП}}_{\&},\, t^{\text{ОП}}_{\vee}\right\},\\
\tau^{\text{D}} &= \left\{t^{\text{D}}_{\&,\vee},\, t^{\text{D}}_{\vee,\&}\right\},\\
\tau^{\text{ПК}} &= \left\{t^{\text{ПК}}_{0,\&},\, t^{\text{ПК}}_{1,\&},\, t^{\text{ПК}}_{0,\vee},\, t^{\text{ПК}}_{1,\vee}\right\},\\
\widetilde{\tau}^{\text{осн}} &= \left\{\tau^{\text{M}},\, \tau^{\text{A}},\, \tau^{\text{K}},\, \tau^{\text{ОП}},\, \tau^{\text{D}},\, \tau^{\text{ПК}},\, t^{\text{П}}\right\}.
\end{aligned}$$

Систему $\tau^{\text{осн}}$ будем называть *системой основных тождеств*, а систему $\widetilde{\tau}^{\text{осн}}$ — *расширенной системой основных тождеств*. Рассмотренные выше примеры выводимостей доказывают следующее утверждение.

Лемма 3.1. *Система $\widetilde{\tau}^{осн}$ выводима из системы $\tau^{осн}$.*

Покажем теперь, что с помощью ЭП на основе системы тождеств $\tau^{\text{осн}}$ из любой формулы можно получить совершенную ДНФ или формулу $x_1\overline{x}_1$. Введем для этого некоторые понятия, характеризующие формулы, появляющиеся на промежуточных этапах указанного ЭП. Произвольную конъюнкцию букв, содержащую, в общем случае, повторяющиеся или противоположные буквы, будем называть *обобщенной* ЭК (ОЭК), а дизъюнкцию таких конъюнкций, содержащую, в общем случае, повторяющиеся «слагаемые», — обобщенной ДНФ (ОДНФ). Обычную ЭК (ДНФ) и формулу $x_1 \cdot \overline{x}_1$ будем считать *канонической* ОЭК (соответственно *канонической* ОДНФ), а совершенную ДНФ и формулу $x_1 \cdot \overline{x}_1$ — *совершенными* ОДНФ. Формулу, в которой все ФС $\neg$ применяются только к БП и нет двух последовательно применяемых ФС $\neg$, будем называть *формулой с поднятыми отрицаниями*.

Пусть формула $\mathcal{F}\left(x_1, \ldots, x_n\right)$ реализует ФАЛ $f\left(x_1, \ldots, x_n\right)$. Докажем существование ЭП вида

$$\mathcal{F} \underset{\tau^{\text{M}}}{\models} \mathcal{F}' \underset{\left\{t^{\text{D}}_{\&,\vee},t^{\text{K}}_{\&}\right\}}{\models} \mathcal{F}'' \underset{\tau^{\text{ПП}}}{\models} \widehat{\mathcal{F}} \underset{\left\{t^{\text{D}}_{\&,\vee},\tau^{\text{ПП}}\right\}}{\models} \widetilde{\mathcal{F}}, \tag{3.1}$$

где $\tau^{\text{ПП}} = \left\{\tau^{\text{A}},\, \tau^{\text{K}},\, \tau^{\text{ПК}},\, \tau^{\text{ОП}},\, t^{\text{П}}\right\}$, $\mathcal{F}'$ — формула с поднятыми отрицаниями, $\mathcal{F}''$ — обобщенная ДНФ, а $\widehat{\mathcal{F}}$ и $\widetilde{\mathcal{F}}$ — каноническая и совершенная ОДНФ ФАЛ f соответственно. Действительно, *поднятие отрицаний*, то есть переход от $\mathcal{F}$ к $\mathcal{F}'$ в (3.1)

можно осуществить применением тождеств $t^{\mathrm{M}}_{\neg}$, $t^{\mathrm{M}}_{\&}$ и $t^{\mathrm{M}}_{\vee}$ к подформулам вида $\overline{\overline{(\mathcal{F}_1)}}$, $\overline{(\mathcal{F}_1 \cdot \mathcal{F}_2)}$ и $\overline{(\mathcal{F}_1 \vee \mathcal{F}_2)}$ соответственно до тех пор, пока все такие подформулы не будут «устранены». Переход от $\mathcal{F}'$ к $\mathcal{F}''$ в (3.1), который называется *раскрытием скобок*, осуществляется применением тождеств $\left\{t^{\mathrm{D}}_{\&,\vee},\, t^{\mathrm{K}}_{\&}\right\}$ к подформулам вида $\mathcal{F}_1 \cdot (\mathcal{F}_2 \vee \mathcal{F}_3)$ или $(\mathcal{F}_1 \vee \mathcal{F}_2) \cdot \mathcal{F}_3$ до тех пор, пока они встречаются в преобразуемой формуле.

Переход от $\mathcal{F}''$ к $\widehat{\mathcal{F}}$ в (3.1), который называется *приведением подобных*, выполняется в три этапа. На первом этапе каждая ОЭК K'' из ОДНФ $\mathcal{F}''$ преобразуется в каноническую ОЭК K с помощью тождеств $\left\{t^{\mathrm{OП}}_{\&},\, t^{\mathrm{ПК}}_{0,\&},\, t^{\mathrm{A}}_{\&},\, t^{\mathrm{K}}_{\&}\right\}$, а также тождества

$$x_i \cdot \overline{x}_i = x_1 \cdot \overline{x}_1, \tag{3.2}$$

которое выводится из них следующим образом:

$$x_i \cdot \overline{x}_i \underset{t^{\mathrm{ПК}}_{0,\&}}{\mapsto} (x_1 \cdot \overline{x}_1) \cdot (x_i \cdot \overline{x}_i) \underset{t^{\mathrm{K}}_{\&}}{\mapsto} (x_i \cdot \overline{x}_i) \cdot (x_1 \cdot \overline{x}_1) \underset{t^{\mathrm{ПК}}_{0,\&}}{\mapsto} x_1 \cdot \overline{x}_1.$$

На втором этапе полученная формула $\check{\mathcal{F}}$ преобразуется в $\widehat{\mathcal{F}}$ путем «устранения» повторных вхождений равных элементарных конъюнкций или подформул $x_1 \cdot \overline{x}_1$ с помощью тождеств $\left\{\tau^{\mathrm{A}},\, \tau^{\mathrm{K}},\, t^{\mathrm{OП}}_{\vee}\right\}$ и, в случае $f \not\equiv 0$, последующего «устранения» ОЭК $x_1 \cdot \overline{x}_1$ с помощью тождеств $\left\{t^{\mathrm{A}}_{\vee},\, t^{\mathrm{K}}_{\vee},\, t^{\mathrm{ПК}}_{0,\vee}\right\}$.

Заметим, что первые два этапа приведения подобных, на которых происходит приведение повторений БП в ОЭК и ЭК, уже дают нам искомую формулу $\widehat{\mathcal{F}}$. Однако, для уменьшения числа шагов в последующих ЭП можно выполнить третий этап приведения подобных — этап приведения поглощений ЭК. На каждом шаге этого этапа в полученной ДНФ с помощью тождеств $\left\{\tau^{\mathrm{A}},\, \tau^{\mathrm{K}}\right\}$ выделяется подформула вида $K'' \vee K'' \cdot K$, где K'' и K — некоторые ЭК, а затем ЭК $K'' \cdot K$ «устраняется» с помощью ЭП

$$K'' \vee K'' \cdot K \underset{t^{\mathrm{П}}}{\mapsto} K''. \tag{3.3}$$

Заметим также, что раскрытие скобок и различные этапы приведения подобных можно чередовать друг с другом при ЭП подформул формулы $\mathcal{F}'$ или формул $\mathcal{F}''$, $\widehat{\mathcal{F}}$.

Переход от $\widehat{\mathcal{F}}$ к $\widetilde{\mathcal{F}}$ в (3.1) выполняется в два этапа. Сначала каждая ЭК $\widehat{K}$ из $\widehat{\mathcal{F}}$, которая имеет ранг r, где $r = n - q < n$, и не содержит букв БП $x_{i_1}, \ldots, x_{i_q}$, приводится к ее совершенной ДНФ $\widetilde{K}$ от БП $X(n)$ в результате следующего ЭП:

$$\widehat{K} \underset{t^{\mathrm{ПК}}_{1,\&}}{\models} \widehat{K}\,(x_{i_1} \vee \overline{x}_{i_1}) \cdots \left(x_{i_q} \vee \overline{x}_{i_q}\right) \underset{t^{\mathrm{D}}_{\&,\vee}}{\models} \widetilde{K}.$$

Затем в полученной ОДНФ устраняются повторные вхождения слагаемых так, как это делалось ранее при переходе от $\check{\mathcal{F}}$ к $\widehat{\mathcal{F}}$, и в результате мы приходим к совершенной ОДНФ $\widetilde{\mathcal{F}}$. Таким образом, доказано следующее утверждение.

Лемма 3.2. *Любую формулу $\mathcal{F}(x_1, \ldots, x_n)$, реализующую ФАЛ f, с помощью ЭП на основе системы тождеств $\tau^{осн}$ можно преобразовать в совершенную ОДНФ ФАЛ f от БП $X(n)$.*

Рассмотрим описанные выше ЭП на примере формулы

$$\mathcal{F} = (x_1 \vee x_2) \cdot \overline{(x_1 \cdot x_3)} \cdot (x_2 \vee x_3),$$

для которой

$$\begin{aligned}
&\mathcal{F} \underset{t^{\mathrm{M}}_{\&}}{\mapsto} (x_1 \vee x_2) \cdot (\overline{x}_1 \vee \overline{x}_3) \cdot (x_2 \vee x_3) && = \mathcal{F}',\\
&\mathcal{F}' \underset{\left\{t^{\mathrm{D}}_{\&,\vee}, \tau^{\mathrm{ПП}} \setminus t^{\mathrm{П}}\right\}}{\models\!\!\models} x_1x_2\overline{x}_3 \vee \overline{x}_1x_2 \vee \overline{x}_1x_2x_3 \vee x_2\overline{x}_3 && = \check{\mathcal{F}} = \widehat{\mathcal{F}},\\
&\widehat{\mathcal{F}} \underset{\{\tau^{\mathrm{A}}, \tau^{\mathrm{K}}, t^{\mathrm{П}}\}}{\models\!\!\models} \overline{x}_1x_2 \vee x_2\overline{x}_3 && = \widehat{\mathcal{F}}',\\
&\widehat{\mathcal{F}}' \underset{\left\{t^{\mathrm{D}}_{\&,\vee}, \tau^{\mathrm{ПП}}\right\}}{\models\!\!\models} x_1x_2\overline{x}_3 \vee \overline{x}_1x_2\overline{x}_3 \vee \overline{x}_1x_2x_3 \vee \overline{x}_1x_2\overline{x}_3 && = \widetilde{\mathcal{F}}.
\end{aligned}$$

Теорема 3.1. *Система $\tau^{осн}$ — полная система тождеств.*

Доказательство. Пусть $\mathcal{F}'$ и $\mathcal{F}''$ — эквивалентные формулы, реализующие равные ФАЛ f' и f'' соответственно, а набор $x(n) = x$ содержит все различные БП, встречающиеся в $\mathcal{F}'$ и $\mathcal{F}''$. Пусть, далее, ФАЛ $f(x)$ равна f' и f'', а $\widetilde{\mathcal{F}}$ — совершенная ОДНФ ФАЛ f от БП $X(n)$. В силу леммы 3.2 имеет место ЭП

$$\mathcal{F}' \underset{\tau^{\mathrm{осн}}}{\models\!\!\models} \widetilde{\mathcal{F}} \underset{\tau^{\mathrm{осн}}}{\models\!\!\models} \mathcal{F}'',$$

которое доказывает теорему. □

Коснемся, в заключение, вопроса о наличии в системе $\tau^{\mathrm{осн}}$ тождеств, которые можно вывести из других тождеств этой системы. Рассмотрим сначала ЭП вида

$$x_1x_1 \underset{t^{\mathrm{ПК}}_{0,\vee}}{\mapsto} x_1x_1 \vee x_1\overline{x}_1 \underset{t^{\mathrm{D}}_{\&,\vee}}{\mapsto} x_1(x_1 \vee \overline{x}_1) \underset{t^{\mathrm{ПК}}_{1,\&}}{\underset{x}{\mapsto}} x_1,$$

которое, с учетом установленных ранее выводимостей, доказывает, что

$$\left\{\tau^{\mathrm{M}},\ t^{\mathrm{D}}_{\&,\vee},\ t^{\mathrm{ПК}}_{1,\&}\right\} \models\!\!\models t^{\mathrm{ОП}}_{\&}.$$

Заметим, далее, что тождество (3.2) можно вывести из системы $\tau' = \left\{\tau^{\mathrm{M}},\ t^{\mathrm{ПК}}_{1,\&},\ t^{\mathrm{K}}_{\&}\right\}$. Действительно,

$$x_1 \cdot \overline{x}_1 \underset{\tau^{\mathrm{M}}}{\models\!\!\models} \overline{(\overline{x}_1 \vee x_1)} \underset{t^{\mathrm{ПК}}_{1,\&}}{\mapsto} \overline{(\overline{x}_1 \vee x_1) \cdot (x_2 \vee \overline{x}_2)} \underset{t^{\mathrm{K}}_{\&}}{\mapsto} \overline{(x_2 \vee \overline{x}_2) \cdot (\overline{x}_1 \vee x_1)}$$
$$\underset{t^{\mathrm{ПК}}_{1,\&}}{\mapsto} \overline{(x_2 \vee \overline{x}_2)} \underset{\tau^{\mathrm{M}}}{\models\!\!\models} \overline{x}_2 \cdot x_2 \underset{t^{\mathrm{K}}_{\&}}{\mapsto} x_2 \cdot \overline{x}_2.$$

Отсюда следует, что из системы тождеств $\left\{\tau', t^{\text{А}}_{\&}, t^{\text{ОП}}_{\&}\right\}$ можно вывести тождество $t^{\text{ПК}}_{0,\&}$, так как

$$x_1 \cdot (x_2 \cdot \overline{x}_2) \underset{\tau'}{\rightleftarrows} x_1 \cdot (x_1 \cdot \overline{x}_1) \underset{t^{\text{А}}_{\&}}{\mapsto} (x_1 \cdot x_1) \cdot \overline{x}_1 \underset{t^{\text{ОП}}_{\&}}{\mapsto} x_1 \cdot \overline{x}_1 \underset{\tau'}{\rightleftarrows} x_2 \cdot \overline{x}_2.$$

Таким образом, тождества $t^{\text{ОП}}_{\&}$ и $t^{\text{ПК}}_{0,\&}$ выводятся из остальных тождеств системы $\tau^{\text{осн}}$.

§4 Сокращенная ДНФ и способы ее построения. Некоторые оценки длины сокращенной ДНФ

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

$$f(x_1, \ldots, x_n) = K_1 \vee \ldots \vee K_s = \mathfrak{A}, \tag{4.1}$$
$$f(x_1, \ldots, x_n) = J_1 \cdots J_t = \mathfrak{B}, \tag{4.2}$$

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 (4.1) и (4.2) эквивалентны следующим покрытиям множеств N_f и $\overline{N}_f$ гранями куба B^n

$$N_f = N_{K_1} \cup \ldots \cup N_{K_s}; \tag{4.3}$$
$$\overline{N}_f = \overline{N}_{J_1} \cup \ldots \cup \overline{N}_{J_t}. \tag{4.4}$$

Так, представление

$$g(x_1, x_2, x_3) = K_1 \vee \ldots \vee K_6, \tag{4.5}$$

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

$$K_1 = x_1\overline{x}_3, \quad K_2 = x_2\overline{x}_3, \quad K_3 = \overline{x}_1x_2, \quad K_4 = \overline{x}_1x_3, \quad K_5 = \overline{x}_2x_3, \quad K_6 = x_1\overline{x}_2,$$

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 (2.3) 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 (4.1) и соответствующим ей покрытием (4.3).

Рассмотрим теперь некоторые специальные виды ДНФ, их «геометрическую» интерпретацию и способы построения. 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 приведения поглощений ЭК (см. §3), т. е. путем ЭП вида (3.3).

Дизъюнктивную нормальную форму $\mathfrak{A}$ вида (4.1) будем называть *неприводимой*, если соответствующее ей покрытие является неприводимым (см. §1), то есть ни одна ни одна из граней $N_{K_1}, \ldots, N_{K_s}$ не содержится ни в одной из других граней покрытия. На «языке имплицируемости» это означает, что ни одна из ЭК K_i, $i \in [1, n]$, не является импликантой ЭК K_j, где $j \in [1, n]$ и $i \neq j$. Заметим, что с помощью приведения поглощений ЭК (см. §3), из любой ДНФ $\mathfrak{A}$ можно получить неприводимую ДНФ $\widehat{\mathfrak{A}}$.

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.

Дизъюнкция всех простых импликант ФАЛ f называется ее *сокращенной* ДНФ. Заметим, что сокращенная ДНФ ФАЛ f является неприводимой ДНФ, и что ей соответствует покрытие множества N_f всеми максимальными по включению гранями множества N_f этой ФАЛ, которые мы будем называть просто *максимальными гранями* ФАЛ f. Указанное соответствие позволяет строить сокращенную ДНФ на основе «геометрических» соображений. Так, в соответствии с рис. 2.1 правая часть (4.5) является сокращенной ДНФ ФАЛ g, а из рис. 4.1a 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

$$g' = K'_1 \vee \ldots \vee K'_7, \tag{4.6}$$

где $K'_1 = \overline{x}_1\overline{x}_4, K'_2 = \overline{x}_1\overline{x}_2, K'_3 = \overline{x}_2\overline{x}_3, K'_4 = \overline{x}_3\overline{x}_4, K'_5 = x_2\overline{x}_4, K'_6 = \overline{x}_1x_3, K'_7 = \overline{x}_2x_4$, причем ЭК K'_i, $i = 1, \ldots, 7$, соответствует грани $\mathcal{N}'_i = N_{K'_i}$ на рис. 4.1a. На рис. 4.1b 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.

Теорема 4.1. *Пусть $\mathfrak{A}'$ и $\mathfrak{A}''$ — сокращенные ДНФ ФАЛ f' и f'' соответственно, а неприводимая ДНФ $\mathfrak{A}$ получается из формулы $\mathfrak{A}' \cdot \mathfrak{A}''$ в результате раскрытия скобок и приведения подобных. Тогда $\mathfrak{A}$ — сокращенная ДНФ ФАЛ $f = f' \cdot f''$.*

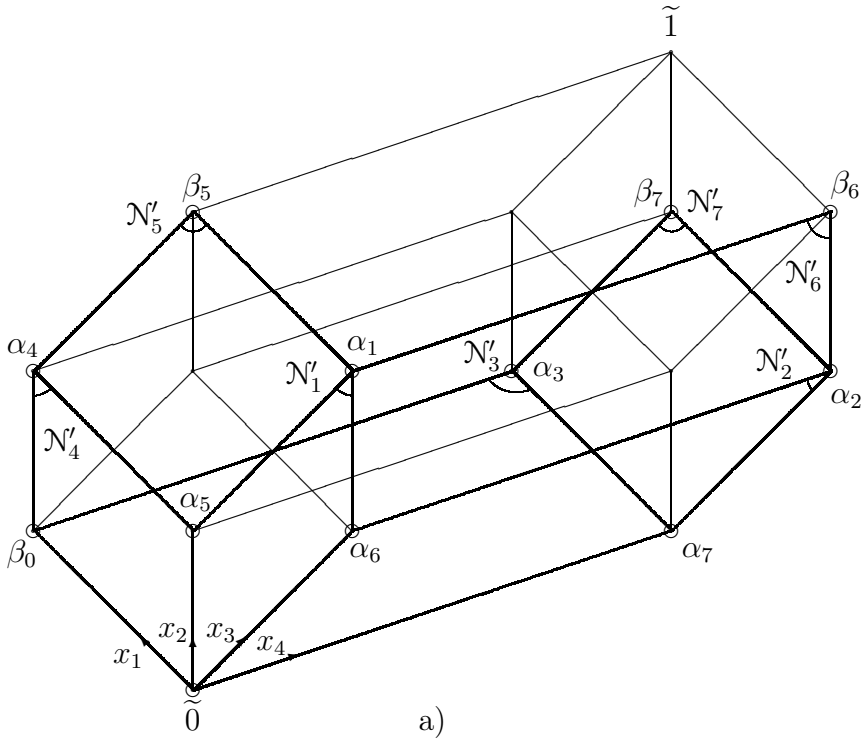


Рис. 4.1: «геометрия» сокращенной ДНФ ФАЛ g'

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 неприводимая ДНФ $\mathfrak{A}$ 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 4.1 к ФАЛ g', показанной на рис. 4.1, получим (сравните с (4.6))

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

Следующий метод (метод Блейка []) позволяет получать сокращенную ДНФ ФАЛ f из произвольной ДНФ этой ФАЛ с помощью эквивалентных преобразований на основе тождеств $\left\{\tau^{\text{ПП}},\, t^{\text{ОС}}\right\}$ (см. §3). Любая ДНФ $\mathfrak{A}'$, которую можно получить из ДНФ $\mathfrak{A}$ путем формирования в ней с помощью тождеств $\left\{\tau^{\text{А}},\, \tau^{\text{К}}\right\}$ подформул вида $x_i K' \vee \overline{x}_i K''$, проведения ЭП

$$x_i K' \vee \overline{x}_i K'' \underset{t^{\text{ОС}}}{\mapsto} x_i K' \vee \overline{x}_i K'' \vee K' K'' \tag{4.7}$$

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 неприводимую ДНФ, которая не имеет строгих расширений.

Теорема 4.2. *Неприводимая ДНФ является сокращенной ДНФ тогда и только тогда, когда она не имеет строгих расширений.*

Доказательство. Достаточно убедиться в том, что неприводимая ДНФ $\mathfrak{A}$, 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'' не содержат БП x_i. 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 $x_iK'\vee\overline{x}_iK''$ в результате ЭП (4.7). 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 неприводимой ДНФ, 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:

$$\begin{aligned}\mathfrak{A}\underset{\{\tau^{\mathrm{A}},\tau^{\mathrm{K}}\}}{\models}&(x_1x_2x_3\vee\overline{x}_1x_2x_3)\vee x_1\overline{x}_2x_3\vee x_1x_2\overline{x}_3\underset{\{t^{\mathrm{OC}},t^{\mathrm{П}}\}}{\models}(x_2x_3\vee x_1\overline{x}_2x_3\vee x_1x_2\overline{x}_3)\\ &\underset{\{\tau^{\mathrm{A}},\tau^{\mathrm{K}}\}}{\models}(x_2x_3\vee\overline{x}_2x_1x_3)\vee x_1x_2\overline{x}_3\underset{\{t^{\mathrm{OC}},t^{\mathrm{П}},t^{\mathrm{ОП}}_{\&}\}}{\models}x_2x_3\vee x_1x_3\vee x_1x_2\overline{x}_3\\ &\underset{\tau^{\mathrm{A}},\tau^{\mathrm{K}}}{\models}x_2x_3\vee(x_3x_1\vee\overline{x}_3x_1x_2)\underset{\{t^{\mathrm{OC}},t^{\mathrm{П}},t^{\mathrm{ОП}}_{\&}\}}{\models}x_2x_3\vee x_1x_3\vee x_1x_2.\end{aligned}\tag{4.8}$$

Приведем, в заключение параграфа, некоторые 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 $s_n^I(x_1,\ldots,x_n)$ 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 s_n^I. Заметим, что ФАЛ 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 s_n^I. Заметим также, что отличная от константы симметрическая ФАЛ является существенной ФАЛ. Легко видеть, что симметрические ФАЛ ℓ_n и $\overline{\ell}_n$, рабочими числами которых являются все нечетные и все четные числа отрезка $[0, n]$ соответственно, имеют вид

$$\ell_n = x_1 \oplus \cdots x_n, \qquad \overline{\ell}_n = x_1 \oplus \cdots \oplus x_n \oplus 1.$$

Симметрическая ФАЛ называется *поясковой*, если ее рабочие числа образуют отрезок. Поясковой ФАЛ является, в частности, ФАЛ голосования $H(x_1, x_2, x_3) = s_3^{[2,3]}$, а также ФАЛ $g = s_3^{[1,2]}$, показанная на рис. 2.1а. Легко видеть, что сокращенная ДНФ поясковой ФАЛ $s_n^{[r,p]}(x_1, \ldots, x_n)$, 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

$$s_n^{[r,p]}(x_1, \ldots, x_n) = \bigvee_{\substack{1 \leqslant i_1 < \cdots < i_{n+r-p} \leqslant n \\ \sigma_1 + \cdots + \sigma_{n+r-p} = r}} x_{i_1}^{\sigma_1} \cdots x_{i_{n+r-p}}^{\sigma_{n+r-p}}. \tag{4.9}$$

Из (4.9) следует, что длина сокращенной ДНФ ФАЛ $s_n^{[r,p]}$ 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.

С другой стороны, сокращенная ДНФ любой ФАЛ из $P_2(n)$ является неприводимой ДНФ, и поэтому соответствует антицепи в частично упорядоченном множестве из всех граней куба B^n с отношением вложения. Заметим, что это частично упорядоченное множество является ранжированным частично упорядоченным множеством длины $(n + 1)$, где i-й ярус, $i = 0, \ldots, n$, состоит из всех граней размерности i, число которых равно $\binom{n}{i} 2^{n-i}$. Заметим также, что через любую грань куба B^n размерности i, $i = 0, \ldots, n$, проходит $(n - i)! \cdot i! \cdot 2^i$ неуплотняемых цепей указанного частично упорядоченного множества, которое, следовательно, удовлетворяет условию замечания к лемме 2.1. Оценивая максимальное значение величины $\binom{n}{i} 2^{n-i}$ на отрезке $i \in [0, n]$ так, как это делалось при доказательстве леммы 2.1 для биномиальных коэффициентов $\binom{n}{i}$, можно показать, что оно достигается, когда $i = \left\lceil \frac{n-2}{3} \right\rceil$. В соответствии с формулой Стирлинга (1.3) отсюда следует, что мощность любой антицепи рассматриваемого частично упорядоченного множества, а значит и длина сокращенной ДНФ любой ФАЛ f из $P_2(n)$, не больше, чем $e_2 \frac{3^n}{\sqrt{n}}$, где e_2 — некоторая константа.

§5 Тупиковые и минимальные ДНФ. Ядро и ДНФ Квайна. Критерий вхождения импликант в тупиковые ДНФ, его локальность

Рассмотрим вопрос о построении тех ДНФ, в которых нет ничего «лишнего». 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, то есть $\mathfrak{A}$ получается из сокращенной ДНФ ФАЛ f путем удаления некоторых ЭК, и что $\mathfrak{A}$ является неприводимой ДНФ (см. §4). С «геометрической» точки зрения тупиковая ДНФ $\mathfrak{A}$ ФАЛ f задает тупиковое (см. §1) покрытие множества N_f максимальными гранями ФАЛ f и обратно. Исходя из этих «геометрических» соображений, можно находить все или некоторые тупиковые ДНФ для ФАЛ от небольшого числа БП. Так например, сокращенная ДНФ (4.8) для ФАЛ «голосования» $H(x_1, x_2, x_3)$ является единственной тупиковой ДНФ этой ФАЛ, ФАЛ $g(x_1, x_2, x_3) = s_3^{\{1,2\}}$ (см. рис. 2.1а и (4.5)) имеет пять тупиковых ДНФ —

$$\mathfrak{A}_1 = K_1 \vee K_3 \vee K_5, \quad \mathfrak{A}_2 = K_2 \vee K_4 \vee K_6 \tag{5.1}$$

$$\mathfrak{A}_3 = K_1 \vee K_2 \vee K_4 \vee K_5,\ \mathfrak{A}_4 = K_2 \vee K_3 \vee K_5 \vee K_6,\ \mathfrak{A}_5 = K_3 \vee K_4 \vee K_6 \vee K_1, \tag{5.2}$$

а у ФАЛ $g'(x_1, x_2, x_3, x_4)$ (см. рис. 4.1 и (4.6)) имеются две тупиковые ДНФ —

$$\mathfrak{A}'_1 = K'_5 \vee K'_6 \vee K'_7 \vee K'_3, \quad \mathfrak{A}'_2 = K'_5 \vee K'_6 \vee K'_7 \vee K'_4. \tag{5.3}$$

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. Так ДНФ $\mathfrak{A}_1$ и $\mathfrak{A}_2$ в (5.1) являются минимальными и, одновременно, кратчайшими ДНФ ФАЛ $g = s_3^{\{1,2\}}$, а для ФАЛ g', показанной на рис. 4.1, обе ее тупиковые ДНФ $\mathfrak{A}'_1$ и $\mathfrak{A}'_2$ в (5.3) являются минимальными и, одновременно, кратчайшими.

При построении тупиковых ДНФ ФАЛ f бывает полезно знать ДНФ *пересечение тупиковых* (*сумма тупиковых*) ФАЛ f, то есть дизъюнкцию всех тех различных простых импликант этой ФАЛ, которые входят в любую (соответственно хотя бы в одну) тупиковую ДНФ ФАЛ f. Заметим, что ДНФ пересечение тупиковых (ДНФ $\cap T$) ФАЛ f в общем случае не реализует саму ФАЛ f, а в некоторых случаях и, в частности, в случае $g = s_3^{\{1,2\}}$ (см. выше), может быть пустой. В тоже время ДНФ сумма тупиковых (ДНФ ΣT) ФАЛ f всегда реализует эту ФАЛ, содержится в ее

сокращенной и может с ней совпадать, как это имеет место в случае $g_3^{\{1,2\}}$ или в случае ФАЛ «голосования». Аналогичным образом определяется ДНФ сумма минимальных (ДНФ ΣM) ФАЛ f и т.п. Очевидно, что ДНФ ΣM ФАЛ f реализует эту ФАЛ и содержится в ее ДНФ ΣT, а для всех приведенных выше ФАЛ ДНФ ΣM совпадает с ДНФ ΣT.

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. Так, ядром ФАЛ g', показанной на рис. 4.1, являются грани $\mathcal{N}'_5$, $\mathcal{N}'_6$ и $\mathcal{N}'_7$, которые содержат ядровые точки β_5, β_6 и β_7 соответственно.

Лемма 5.1. *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. □

Будем называть ФАЛ *ядровой*, если все ее максимальные грани являются ядровыми. Из леммы 5.1 следует, что сокращенная ДНФ ядровой ФАЛ является ее единственной тупиковой ДНФ. Примером ядровой ФАЛ является ФАЛ голосования (4.8) (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. 5.1, ее сокращенная ДНФ имеет вид $g'' = x_2\overline{x}_3 \vee \overline{x}_1x_2 \vee \overline{x}_1x_3$, то есть отличается от ДНФ Квайна, которая является единственной тупиковой ДНФ этой ФАЛ и имеет вид $g'' = x_2\overline{x}_3 \vee \overline{x}_1x_3$. В то же время для ФАЛ g', показанной на рис. 4.1, ДНФ Квайна совпадает с сокращенной

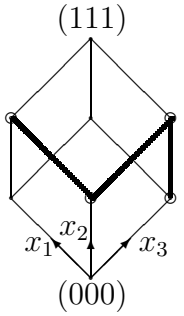


Рис. 5.1: «геометрия» сокращенной ДНФ ФАЛ g''

ДНФ этой ФАЛ и отличается от ее ДНФ ΣT, которая (см. выше) равна

$$K'_3 \vee K'_4 \vee K'_5 \vee K'_6 \vee K'_7.$$

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 будем называть *регулярной относительно грани N_K точкой ФАЛ f*, где $\alpha \in N_f$ и $N_K \in \Pi_\alpha(f)$, если найдется точка β, $\beta \in N_f \setminus N_K$, для которой $\Pi_\beta(f) \subseteq \Pi_\alpha(f)$. При этом, очевидно, $N_K \notin \Pi_\beta(f)$, так как $\beta \notin N_K$, и, следовательно, включение $\Pi_\beta(f) \subseteq \Pi_\alpha(f)$, которое означает, что любая максимальная грань ФАЛ f, проходящая через точку β, проходит и через точку α, может быть только строгим включением $\Pi_\beta(f) \subset \Pi_\alpha(f)$. Грань N_K ФАЛ f называется *регулярной гранью* этой ФАЛ, если все точки N_K регулярны относительно нее самой. Заметим, что грань, которая не входит в ядро, но покрывается им, является регулярной. Заметим также, что для ФАЛ g', показанной на рис. 4.1, грани $\mathcal{N}'_1$ и $\mathcal{N}'_2$, которые не входят в ДНФ ΣT, являются регулярными, так как

$$\Pi_{\beta_5}(g') \subset \Pi_{\alpha_1}(g'),\ \Pi_{\beta_6}(g') \subset \Pi_{\alpha_2}(g') \text{ и } \Pi_{\beta_i}(g') \subset \Pi_{\alpha_i}(g') \text{ для всех } i,\ i = 0, 5, 6, 7.$$

Теорема 5.1 ([]). *Простая импликанта K ФАЛ f входит в ДНФ ΣT тогда и только тогда, когда когда грань N_K не является регулярной гранью этой ФАЛ.*

Доказательство. Пусть $N_K = \{\alpha_1, \ldots, \alpha_s\}$ — регулярная грань ФАЛ f. Тогда для каждого j, $j = 1, \ldots, s$, в силу регулярности точки α_j относительно грани N_K найдется точка β_j, $\beta_j \in N_f \setminus N_K$, 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, не содержащая грань N_K и покрывающая не принадлежащие ей точки $\beta_1, \ldots, \beta_s$, «автоматически» покроет все точки $\alpha_1, \ldots, \alpha_s$ этой грани. Таким образом, грань N_K 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 относительно N_K точку α, и пусть $N_f \setminus N_K = \{\beta_1, \ldots, \beta_q\}$. Из нерегулярности точки α относительно грани N_K следует, что для любого $j,\ j = 1, \ldots, q$, пучок $\Pi_{\beta_j}(f)$ не вложен в пучок $\Pi_\alpha(f)$ и поэтому в $\Pi_{\beta_j}(\alpha)$ 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 тупиковое покрытие множества N_f, являющееся подпокрытием указанного покрытия, будет соответствовать тупиковой ДНФ, содержащей ЭК K.

Теорема доказана. □

Коснемся, в заключение, вопроса о локальном характере рассмотренных выше критериев вхождения простых импликант ФАЛ f в ее ДНФ $\cap T$ и ДНФ ΣT. 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 5.1 следует, что ЭК K входит в ДНФ ΣT ФАЛ f тогда и только тогда, когда для любой точки α из N_K найдется точка $\beta,\ \beta \in N_f \setminus N_K$, 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 грани ФАЛ f выделены и «помечены» (для этого, как уже говорилось, достаточно рассмотреть их окрестности порядка 1), то вхождение ЭК K в ДНФ Квайна ФАЛ f сводится к покрытию грани N_K отличными от нее «помеченными» гранями из окрестности $S_1(N_K, f)$.

§6 Особенности ДНФ для функций из некоторых классов. Теорема Ю. И. Журавлева о ДНФ сумма минимальных

Рассмотрим особенности «поведения» и связанные с ними особенности ДНФ для функций из некоторых классов. 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 ℓ_n и $\overline{\ell}_n$ (см. §4) являются единственными существенными линейными ФАЛ в $P_2(n)$. 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 разложение ФАЛ f по БП x_i (см. (2.4)) переходит в равенство

$$f(x_1, \ldots, x_n) = x_i \oplus f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \tag{6.1}$$

и обратно, а значит ФАЛ является линейной тогда и только тогда, когда она линейно зависит от всех своих существенных БП. На самом деле для линейности ФАЛ f достаточно, чтобы она линейно зависела от всех своих существенных БП, кроме одной. Это легко доказать индукцией по числу существенных БП ФАЛ f, используя тот факт, что все ФАЛ из $P_2(1)$ являются линейными, в качестве базиса индукции и применяя равенство (6.1) для обоснования индуктивного перехода.

Заметим, что если во множестве N_f ФАЛ $f(x_1, \ldots, x_n)$ нет соседних по некоторой БП x_i наборов, то в каждую импликанту K ФАЛ f обязательно входит одна из букв БП x_i. Действительно, если K не содержит букв БП x_i, то для любого набора α из N_K и соседнего с ним по БП x_i набора β будут выполняться равенства $K(\alpha) = K(\beta) = 1$. Следовательно, $f(\alpha) = f(\beta) = 1$, так как K — импликанта f, а это противоречит свойствам множества N_f. Указанное свойство выполняется, в частности, если ФАЛ f линейно зависит от БП x_i, так как при этом $f(\alpha) \neq f(\beta)$ для любых соседних по БП x_i наборов α и β.

Заметим, далее, что если во множестве N_f ФАЛ $f(x_1, \ldots, x_n)$ вообще нет соседних наборов, то она имеет единственную ДНФ от БП $X(n)$ — свою совершенную ДНФ. Действительно, ранг любой импликанты K ФАЛ f в этом случае равен n, а соответствующая ей грань N_K состоит из одного набора куба B^n. Следовательно, любая ДНФ $\mathfrak{A}$ ФАЛ f включает в себя $|N_f|$ ЭК ранга n, то есть является ее совершенной ДНФ. Очевидно, что если во множестве N_f есть соседние наборы, то совершенная ДНФ ФАЛ f уже не будет единственной ДНФ этой ФАЛ. Таким образом, доказано следующее утверждение.

Лемма 6.1. *Совершенная ДНФ ФАЛ f из $P_2(n)$ является ее единственной ДНФ от БП $X(n)$ тогда и только тогда, когда во множестве N_f нет соседних наборов.*

Следствие. *Совершенная ДНФ линейной существенной ФАЛ является единственной ДНФ этой ФАЛ от ее существенных БП.*

Рассмотрим теперь 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 простая импликанта K ФАЛ f имеет вид $K = \overline{x}_i \cdot K'$, где ЭК K' не содержит букв БП x_i. Заметим, что ЭК K' не является импликантой ФАЛ f, так как иначе ЭК K не была бы простой импликантой f, и, следовательно, существует набор β из B^n такой, что $K'(\beta) = 1$, но $K(\beta) = f(\beta) = 0$. Таким образом, $\beta\langle i\rangle = 1$ и поэтому для набора α соседнего с набором β по БП x_i выполняются равенства

$$K'(\alpha) = K'(\beta) = K(\alpha) = f(\alpha) = 1,$$

а также неравенство $\alpha \leqslant \beta$, из которого в силу монотонности ФАЛ f по БП x_i вытекает, что $f(\beta) = 1$. Полученное противоречие доказывает, что простая импликация 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 представленна в указанном виде. Легко видеть также, что $K_\beta^+(\gamma) = 1$ тогда и только тогда, когда $\gamma \geqslant \beta$, откуда следует, что ЭК $K_{\beta'}^+$ имплицирует ЭК $K_{\beta''}^+$ тогда и только тогда, когда $\beta' \geqslant \beta''$. 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^+.

Лемма 6.2. *Сокращенная ДНФ $\mathfrak{A}$ монотонной ФАЛ f, $f \in P_2(n)$, является единственной тупиковой ДНФ этой ФАЛ и имеет вид:*

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

Доказательство. Докажем сначала, что для любого набора β, $\beta \in N_f^+$, ЭК $K = K_\beta^+$ является простой импликантой ФАЛ f. Действительно, ЭК K является импликантой ФАЛ f так как $K(\beta) = 1$ и поэтому, в силу монотонности ФАЛ f, $K(\gamma) = 1$ для любого набора γ из B^n такого, что $\gamma \geqslant \beta$, то есть для любого набора γ из N_K. Более того, ЭК K является простой импликантой ФАЛ f, так как любая ЭК K', получающаяся из K удалением некоторых букв, имеет вид $K' = K_{\beta'}^+$, где $\beta' \leqslant \beta$ и $\beta' \neq \beta$, то есть не является импликантой ФАЛ f, поскольку обращается в 1 на наборе β' из $\overline{N}_f$.

Докажем теперь, что у ФАЛ f нет простых импликант, отличных от ЭК из $\mathfrak{A}$. Пусть монотонная ЭК K является простой импликантой ФАЛ f и имеет вид $K = K_\beta^+$, где $\beta \notin N_f^+$. При этом набор β входит в N_K и, следовательно, входит в N_f. Отсюда вытекает существование в N_f^+ набора β', для которого выполнены соотношения $\beta' \leqslant \beta$ и $\beta' \neq \beta$, то есть имеют место включения $N_f \supseteq N_{K'} \supset N_K$, где $K' = K_{\beta'}^+$, противоречащие простоте импликанты K. Совпадение ДНФ $\mathfrak{A}$ с сокращенной ДНФ ФАЛ f доказано.

Завершая доказательство, заметим, что в покрытии множества N_f, соответствующем ДНФ $\mathfrak{A}$, любой набор β, $\beta \in N_f^+$, покрывается только той максимальной гранью ФАЛ f, которая связана с ЭК K_β^+. Это означает, что все грани указанного покрытия являются ядровыми гранями ФАЛ f, а ДНФ $\mathfrak{A}$ совпадает с ДНФ $\cap T$ ФАЛ f.

Лемма доказана. □

Следствие. *Монотонная ФАЛ является ядровой ФАЛ.*

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 $\mathcal{N}_1$, $\mathcal{N}_2$, …, $\mathcal{N}_t$ куба B^n (см. рис. 6.1a и 6.1b). Заметим, что циклическая ФАЛ длины t существует тогда и только тогда, когда $t \geqslant 6$ — четное число, а цепная ФАЛ длины t — при любом

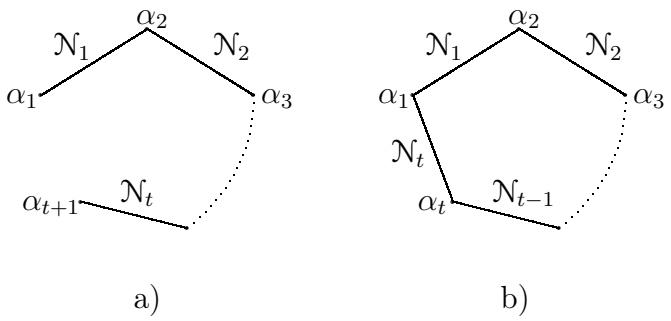


Рис. 6.1: множество N_f для цепной и циклической ФАЛ f

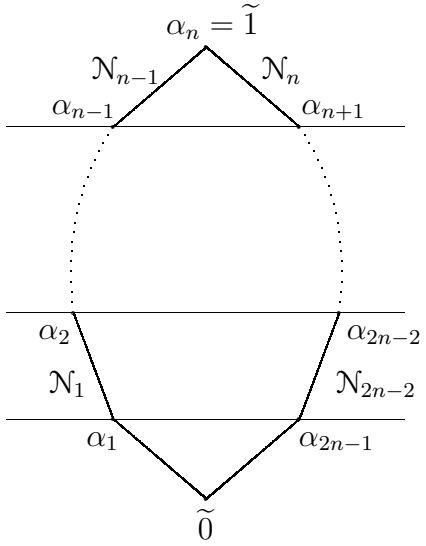


Рис. 6.2: цепная ФАЛ длины $(2n-2)$ в кубе B^n

$t \geqslant 1$. Пример цепной ФАЛ длины 3 дает ФАЛ g'', показанная на рис. 5.1, а ФАЛ $g = s_3^{\{1,2\}}$ (см. рис. 2.1а) является циклической ФАЛ длины 6.

Из теоремы 5.1 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. 6.1а) $\mathcal{N}_1 \cup \mathcal{N}_3 \cup \ldots \cup \mathcal{N}_t$ длины k. Действительно, множество N_f в данном случае состоит из $2k$ наборов и не может быть покрыто $(k-1)$ ребром. Кроме 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 6.1 (ср. []). *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 соответствует рис. 6.1а, 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. 6.2) 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 в ДНФ ΣT (сравните с теоремой 5.1).

Замечание 2. Известно [], 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).

§7 Функция покрытия и построение всех тупиковых ДНФ. Оценка длины градиентного покрытия

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 $\mathfrak{N}$. Будем считать, что i-я строка (j-й столбец) матрицы M соответствует подмножеству $\mathfrak{N}_i$ системы $\mathfrak{N}$ (элементу α_j множества $\mathfrak{N}$) 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 $\mathfrak{N}_i \ni \alpha_j$, 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 $\{\mathfrak{N}_i\}_{i\in I}$ задает покрытие множества $\mathfrak{N}$. 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 $\mathfrak{N}$ эквивалентна задаче построения всех тупиковых покрытий матрицы M, соответствующей паре $(\mathfrak{N},\mathfrak{N})$.

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 $y = (y_1,\dots,y_p)$, — 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 6.2 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 $I = \{i_1,\dots,i_r\}$, и обратно.

Лемма 7.1. *Функция покрытия $F(y_1,\dots,y_p)$ матрицы M, $M \in B^{p,s}$, без нулевых столбцов задается КНФ вида:*

$$F(y_1,\dots,y_p) = \bigwedge_{j=1}^{s}\Bigg(\bigvee_{\substack{1\leqslant i\leqslant p\\ M\langle i,j\rangle=1}} y_i\Bigg). \tag{7.1}$$

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 $y = (y_1,\dots,y_p)$. Легко видеть, что $J_j(\beta) = 1$ для произвольного набора β, $\beta \in$ $\in B^p$, 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 (7.1) обращается в 1 на наборе β тогда и только тогда, когда указанное выше множество строк 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* (7.1) *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 $\mathfrak{N}$ взять множество N_f, а в качестве его покрытия $\mathfrak{N}$ — систему всех максимальных граней ФАЛ f. Матрица M, соответствующая указанной паре $(\mathfrak{N}, \mathfrak{N})$, называется, обычно, *таблицей Квайна* ФАЛ f. Заметим, что по таблице Квайна можно построить ядро, ДНФ Квайна и ДНФ ΣT рассматриваемой ФАЛ. Действительно, столбец таблицы Квайна, покрываемый только одной строкой, соответствует ядровой точке ФАЛ, а покрывающая его «ядровая строка» — ядровой грани этой ФАЛ. Строка, покрываемая ядровыми строками, соответствует грани, покрываемой ядром и т. п.

Рассмотрим, для примера, задачу построения всех тупиковых ДНФ для ФАЛ $g(x_1, x_2, x_3) = s_3^{\{1,2\}}$ из ее сокращенной ДНФ, полагая (см. рис. 2.1а, (4.5), (5.1) и (5.2)), что

$$N_g = \{\alpha_1 = (100), \alpha_2 = (110), \alpha_3 = (010), \alpha_4 = (011), \alpha_5 = (001), \alpha_6 = (101)\},$$

$$\mathfrak{N} = \{\mathfrak{N}_1, \ldots, \mathfrak{N}_6\},$$

где $\mathfrak{N}_i = N_{K_i} = \{\alpha_i, \alpha_{i+1}\}$ 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 (7.1) 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. (5.1), (5.2)).

В общем случае при построении всех тупиковых ДНФ ФАЛ f, $f \in P_2(n)$, с помощью леммы 7.1 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 $N_{K_{t+1}}, \ldots, N_{K_q}$ — регулярными гранями ФАЛ f. Положим

$$\widehat{\mathcal{N}} = \bigcup_{i=p+1}^{t} N_{K_i}, \quad \mathcal{N} = N_f \setminus \widehat{\mathcal{N}} \quad \text{и} \quad \mathfrak{N} = \{\mathcal{N}_1, \ldots, \mathcal{N}_p\},$$

где $\mathcal{N}_i = N_{K_i} \setminus \widehat{\mathcal{N}}$ при всех i, $i \in [1, p]$. При этом 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. 4.1 (см. также (4.6) и (5.3)), получим тривиальную задачу о покрытии множества $\mathcal{N} = \{(1000)\}$ двумя совпадающими с ним подмножествами $\mathcal{N}_1 = \mathcal{N}'_3 \setminus \widehat{\mathcal{N}}$ и $\mathcal{N}_2 = \mathcal{N}'_4 \setminus \widehat{\mathcal{N}}$, где $\widehat{\mathcal{N}} = \mathcal{N}'_5 \cup \mathcal{N}'_6 \cup \mathcal{N}'_7$.

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 7.1 ([]). *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] $\left\lceil \frac{1}{\gamma} \ln^+(\gamma s) \right\rceil + \frac{1}{\gamma}$.

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

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 $\{i_1,\dots,i_t\}$, 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

$$q \leqslant t + \delta_t \cdot s, \tag{7.2}$$

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 $\gamma ps\delta_t$, 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 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

$$\delta_t \leqslant (1-\gamma)^t \leqslant e^{-\gamma t} \tag{7.3}$$

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 (7.2) и учитывая (7.3), 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 $\mathcal{N}_1, \mathcal{N}_2, \dots, \mathcal{N}_p$ множества $\mathcal{N} = \{\alpha_1,\dots,\alpha_s\}$ 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 $I_1,\ \dots,\ I_s$, где $I_i = \{j:\ \alpha_i \ni \mathcal{N}_j\}$

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 7.2 ([]). *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 7.1 и построения покрытия длины q, где

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

Лемма доказана. □

§8 Алгоритмические трудности минимизации ДНФ. Оценки максимальных и 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. 2). 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

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

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.

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, []). 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. §4) является алгоритмически трудной задачей.

С другой стороны, Ю.И. Журавлев [] предложил применительно к ДНФ модель так называемых локальных или окрестностных алгоритмов, когда преобразование рассматриваемой грани однозначно определяется «состоянием» ее «окрестности» заданного порядка (см. §6). Он же (см. теорему 6.1) 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.

Из монотонности функционала ψ для сложности ДНФ следует, что ψ-минимальную ДНФ всегда можно выбрать среди тупиковых ДНФ, алгоритм построения которых описан в §7. Однако, как показывает следующее утверждение, ФАЛ могут иметь очень много различных[1] тупиковых ДНФ и даже число различных минимальных ДНФ у них может быть очень велико.

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

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

$$f(x_1, \ldots, x_n) = s_3^{\{1,2\}}(x_1, x_2, x_3) \oplus x_4 \oplus \cdots \oplus x_n$$

равно $5^{2^{n-4}}$ (соответственно $2^{2^{n-4}}$).

Доказательство. Пусть

$$g(x_1, x_2, x_3) = s_3^{\{1,2\}}(x_1, x_2, x_3), \quad \ell'(x_4, \ldots, x_n) = x_4 \oplus \cdots \oplus x_n \oplus 1.$$

Из линейной зависимости ФАЛ f от БП $x_4, \ldots, x_n$ вытекает, что (см. §6) любая простая импликанта K ФАЛ f имеет вид

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

где либо K' — произвольная простая импликанта K_i, $i = 1, \ldots, 6$, ФАЛ g (см. рис. 2.1а и (4.5)) и $(\beta_4, \ldots, \beta_n) \in N_{\ell'}$, либо $K' \in \{x_1x_2x_3, \overline{x}_1\overline{x}_2\overline{x}_3\}$ и $(\beta_4, \ldots, \beta_n) \in \overline{N}_{\ell'}$. Таким образом, сокращенная ДНФ ФАЛ f с «геометрической» точки зрения состоит из 2^{n-3} изолированных точек — ядровых граней размерности 0, — и 2^{n-4} циклов длины 6 (см. §6). Следовательно, любая тупиковая (минимальная) ДНФ ФАЛ f включает в себя систему из 2^{n-3} точек и одно из пяти (соответственно двух) реберных покрытий, связанных с тупиковыми (соответственно минимальными) ДНФ ФАЛ g, приведенными в (5.1)–(5.2) (соответственно (5.1)), 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. □

Замечание 1. Поскольку длина тупиковой ДНФ у любой ФАЛ из $P_2(n)$ не больше, чем 2^n, а число различных граней куба B^n равно 3^n, то, следовательно, число тупиковых ДНФ у любой ФАЛ из $P_2(n)$ не больше, чем

$$2^n \binom{3^n}{2^n} \leqslant 2^n \cdot \frac{3^{n \cdot 2^n}}{(2^n)!} \leqslant 3^{n \cdot 2^n}.$$

Замечание 2. Оценку замечания 1 можно уточнить следующим образом. Установим между множеством всех ДНФ от БП $X(n)$ и кубом B^{3^n} изоморфизм, отображающий ДНФ $\mathfrak{A}$ в набор β, для которого $\beta\langle i \rangle = 1$ тогда и только тогда, когда грань куба B^n с номером i, $i \in [1, 3^n]$, входит в покрытие, связанное с $\mathfrak{A}$. При этом любая тупиковая ДНФ соответствует набору с не более, чем 2^n, единицами, а две различные тупиковые ДНФ одной и той же ФАЛ — попарно не сравнимым наборам. Следовательно, число тупиковых ДНФ у одной и той же ФАЛ из $P_2(n)$ не больше ширины частично упорядоченного множества $(A, \leqslant)$, где множество A состоит из всех слоев куба B^{3^n} с номерами $0, 1, \ldots, 2^n$, которая, в свою очередь, в силу замечания к лемме 2.1 не больше, чем $\binom{3^n}{2^n}$.

Рассмотрим, в заключение, поведение функций Шеннона для ранга и длины ДНФ, а также сравним их с «типичными», то есть характерными для почти всех ФАЛ, значениями соответствующих функционалов сложности.

Теорема 8.1. *Для любого n, $n \in \mathbb{N}$, и для почти всех ФАЛ f, $f \in P_2(n)$, имеют место соотношения*[1]*:*

$$\lambda(n) = 2^{n-1}, \qquad R(n) = n \cdot 2^{n-1}, \tag{8.1}$$

$$\lambda(f) \lesssim \frac{3}{4} 2^{n-1}, \qquad R(f) \lesssim \frac{3}{4} n \cdot 2^{n-1} \tag{8.2}$$

Доказательство. Нижняя оценка в (8.1) достигается на линейной функции алгебры логики $\ell_n = x_1 \oplus \cdots \oplus x_n$, для которой совершенная ДНФ длины 2^{n-1} от БП $X(n)$ является ее единственной ДНФ от этих БП (см. §6) и поэтому

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

Для получения требуемой в (8.1) верхней оценки возьмем произвольную ФАЛ f из $P_2(n)$ и в соответствии с (2.4) разложим ее по БП $x_2, \ldots, x_n$ следующим образом:

$$f(x_1, \ldots, x_n) = \bigvee_{\sigma'' = (\sigma_2, \ldots, \sigma_n)} x_2^{\sigma_2} \cdots x_n^{\sigma_n} \cdot f(x_1, \sigma'') \tag{8.3}$$

Легко видеть, что после замены в разложении (8.3) каждой ФАЛ $f(x_1, \sigma'')$ равной ей ФАЛ из множества $\{0,\ 1,\ x_1,\ \overline{x}_1\}$ и проведения необходимых ЭП (см. §3) мы получим ДНФ $\mathfrak{A}_f$ длины не больше, чем 2^{n-1}, что доказывает верхние оценки в (8.1).

Рассмотрим, далее, дискретную векторную случайную величину $\xi = (\xi_{\widetilde{0}}, \ldots, \xi_{\widetilde{1}})$, состоящую из 2^n независимых случайных величин ξ_α, $\alpha \in B^n$, принимающих значения 0 и 1 с вероятностью $\frac{1}{2}$, а также совокупность из 2^{n-1} случайных величин η_β, где $\beta \in B^{n-1}$, вида $\eta_\beta = \xi_{0,\beta} \vee \xi_{1,\beta}$, которые, очевидно, являются независимыми случайными величинами, принимающими значения 0 и 1 с вероятностью $\frac{1}{4}$ и $\frac{3}{4}$ соответственно. Заметим, что любая ФАЛ f из $P_2(n)$ является реализацией величины ξ, при которой $\xi_\alpha = f(\alpha)$ для любого α, $\alpha \in B^n$, и что вероятность такой реализации равна 2^{-2^n}. Отсюда следует, что для любого множества Q, $Q \subseteq P_2(n)$, отношение $|Q| / 2^{2^n}$, то есть доля тех ФАЛ f из $P_2(n)$, которые принадлежат Q, равна вероятности того, что реализация случайной величины ξ принадлежит Q. В частности, вероятность того, что случайная величина

$$\eta = \sum_{\beta \in B^{n-1}} \eta_\beta$$

[1] Асимптотическое неравенство $a(n) \lesssim b(n)$ означает, что $\overline{\lim\limits_{n \to \infty}} (a(n) / b(n)) \leqslant 1$, или, что то же самое, $a(n) \leqslant b(n)(1 + o(1))$.

принимает значение из отрезка $I,\ I \subseteq [0, 2^n]$, равна доле тех функций алгебры логики f из $P_2(n)$, для которых $\lambda(\mathfrak{A}_f) \in I$. Действительно, при указанной выше интерпретации $\eta_\beta = f(0, \beta) \vee f(1, \beta)$ и, следовательно, $\eta_\beta = 1$ тогда и только тогда, когда ФАЛ вида $x_2^{\beta_2} \cdots x_n^{\beta_n} f(x_1, \beta_2, \ldots, \beta_n)$ из (8.3) не равна тождественно 0, то есть входит в ДНФ $\mathfrak{A}_f$ в виде отдельной ЭК.

Из независимости случайных величин $\eta_\beta,\ \beta \in B^{n-1}$, вытекает (см., например, []), что

$$\mathbb{E}\eta = \sum_{\beta \in B^{n-1}} \mathbb{E}\eta_\beta, \qquad\qquad \mathbb{D}\eta = \sum_{\beta \in B^{n-1}} \mathbb{D}\eta_\beta,$$

где $\mathbb{E}\theta$ и $\mathbb{D}\theta$ — математическое ожидание и дисперсия случайной величины θ соответственно. Следовательно

$$\mathbb{E}\eta = \frac{3}{4}2^{n-1}, \qquad\qquad \mathbb{D}\eta = \frac{3}{16}2^{n-1}, \tag{8.4}$$

так как $\mathbb{E}\eta_\beta = \frac{1}{4}$ и $\mathbb{D}\eta_\beta = \frac{3}{16}$ при любом $\beta,\ \beta \in B^{n-1}$. Полагая

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

и применяя к случайной величине η с учетом (8.4) неравенство Чебышева [], получим, что вероятность события $\eta \notin I$, то есть доля тех ФАЛ f из $P_2(n)$, для которых $\lambda(\mathfrak{A}_f) \notin I$, не больше, чем

$$\frac{\mathbb{D}\eta}{t^2} \leqslant \frac{3}{32n^2}$$

и, следовательно, стремится к 0 при n стремящемся к бесконечности. Это означает, в частности, что для почти всех ФАЛ f из $P_2(n)$, выполнены соотношения (8.2).

Теорема доказана. □

§9 Задача контроля схем и тесты для таблиц. Построение всех тупиковых тестов, оценки длины диагностического теста

Для управляющей системы (схемы) без памяти, функционирование которой описывается дискретной функцией или, в общем случае, вектор-функцией, может быть сформулирована следующая модель (см. []), в рамках которой обычно рассматриваются вопросы ее надежности и контроля. Предполагается, что имеется некоторый «внешний» источник неисправностей (источник помех) И, под действием которого рассматриваемая схема Σ может переходить в одно из своих «неисправных состояний»

(схем), определяемых этим источником. Пусть схеме $\Sigma = \Sigma_1$, реализующей функцию $f = f_1$ от входных переменных $x = (x_1, \ldots, x_n)$, и источнику неисправностей И соответствуют «неисправные» состояния (схемы) $\Sigma_2, \ldots, \Sigma_s$, где схема Σ_i, $i = 2, \ldots, s$, реализует функцию f_i от переменных x. При этом все состояния (как исправное $\Sigma = \Sigma_1$, так и неисправные $\Sigma_2, \ldots, \Sigma_s$) разбиваются на классы (функционально) неотличимых состояний, то есть классы эквивалентности по отношению равенства реализуемых функций, и рассматриваются далее с точностью до неотличимости. В дальнейшем, говоря о ненадежной схеме Σ, будем иметь в виду пару $(\Sigma, \text{И})$ и (или) соответствующее ей множество схем вместе с теми функциями, которые они реализуют. Для простоты рассмотрения будем считать, что все переменные и функции являются булевскими, хотя многие излагаемые далее результаты без существенных изменений переносятся на случай многозначных функций, случай вектор-функций и другие более общие случаи.

Пусть $(\Sigma, \text{И})$ — указанная выше модель ненадежной схемы Σ с возможными состояниями $\Sigma = \Sigma_1, \Sigma_2, \ldots, \Sigma_s$ в которых реализуются ФАЛ $f = f_1, f_2, \ldots, f_s$ соответственно от БП $X(n)$, определенные на множестве наборов $A = \{\alpha_1, \ldots, \alpha_p\} \subseteq B^n$. Рассмотрим матрицу M, $M \in B^{p,s}$, где

$$M\langle i, j\rangle = f_j(\alpha_i),$$

считая, что i-й строке (j-му столбцу) этой таблицы соответствует набор α_i (соответственно функция f_j и состояние Σ_j). Матрица, состоящая из различных столбцов (строк) называется *отделимой по столбцам* (соответственно *строкам*) матрицей. Заметим, что каждому классу неотличимых состояний модели $(\Sigma, \text{И})$ соответствует группа одинаковых столбцов матрицы M и рассмотрим отделимую по столбцам матрицу $\widehat{M}$, состоящую из всех различных столбцов матрицы M. При этом будем считать, что каждый столбец матрицы $\widehat{M}$ связан с соответствующим классом неотличимости состояний модели $(\Sigma, \text{И})$ и будем называть $\widehat{M}$ *таблицей контроля* данной модели. Для простоты будем, как правило, предполагать, что все состояния модели $(\Sigma, \text{И})$ попарно отличимы, то есть, $M = \widehat{M}$. Это предположение, очевидно, не ограничивает общности рассуждений.

Пусть, далее, помимо таблицы контроля M для модели $(\Sigma, \text{И})$ задана цель контроля, то есть указано множество $\mathcal{N}$, состоящее из тех неупорядоченных пар различных чисел отрезка $[1, s]$, для которых пары состояний (столбцов матрицы M) с соответствующими номерами необходимо отличать друг от друга, сравнивая значения, расположенные в тех или иных строках данной пары столбцов. В частности, если $\mathcal{N}$ состоит из всех пар указанного вида, то целью контроля является *диагностика схемы*, а если $\mathcal{N} = \{(1,2), \ldots, (1,t)\}$, то — *проверка исправности схемы*. Множество строк матрицы M с номерами из T, $T \subseteq [1, p]$, называется *тестом для матрицы M относительно множества* $\mathcal{N}$, или, иначе, *тестом для* $(M, \mathcal{N})$, если для любой пары (i, j) из $\mathcal{N}$ существует t, $t \in T$, такое, что $M\langle t, i\rangle \neq M\langle t, j\rangle$. Мощность теста называется также его *длиной*.

Заметим, что множество, состоящее из всех строк таблицы контроля, всегда образует тест. Тест, который перестает быть тестом при удалении любой своей строки, называется *тупиковым*, а тест, который имеет минимальную мощность, — *минимальным*. В том случае, когда целью контроля является диагностика схемы (проверка исправности схемы), тест называется *диагностическим* (соответственно *проверяющим*).

Будем говорить, что множество наборов θ, $\theta \subseteq A$, образует *тест для модели* $(\Sigma, \text{И})$ *относительно цели контроля* $\mathcal{N}$ или, иначе, *тест для* $(\Sigma, \text{И}, \mathcal{N})$, если соответствующие наборам из θ строки матрицы M образуют тест для $(M, \mathcal{N})$. Все введенные выше понятия, которые касаются тестов для таблиц, без изменений переносятся на случай тестов для ненадежных схем.

Для описания тестов можно ввести функцию, аналогичную функции покрытия из §7. Пусть M, $M \in B^{p,s}$, — отделимая по столбцам матрица, а $\mathcal{N}$ — связанная с ней цель контроля. 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 тест для $(M, \mathcal{N})$, и будем называть эту ФАЛ *функцией теста* для $(M, \mathcal{N})$. Сопоставим паре $(M, \mathcal{N})$ матрицу $\mathcal{M}$ из множества $B^{p,S}$, $S = |\mathcal{N}|$, столбцы которой пронумерованы парами из $\mathcal{N}$, а ее столбец с номером $(i, j) \in \mathcal{N}$ получается в результате поразрядного сложения по модулю 2 столбцов с номерами i и j матрицы M. Заметим, что строки матрицы M с номерами из множества T, $T \subseteq [1, p]$, образуют тест (тупиковый тест, минимальный тест) для пары $(M, \mathcal{N})$ тогда и только тогда, когда строки матрицы $\mathcal{M}$ с номерами из T образуют покрытие (тупиковое покрытие, покрытие минимальной длины) матрицы $\mathcal{M}$. Отсюда вытекает, в частности, что ФАЛ теста F для пары $(M, \mathcal{N})$ является, одновременно, ФАЛ покрытия для матрицы $\mathcal{M}$ и обратно, а значит для нее в силу леммы 7.1 справедливо следующее утверждение.

Лемма 9.1. *Функция теста $f(y_1, \ldots, y_p)$ для отделимой по столбцам матрицы M, $M \in B^{p,s}$, и цели контроля $\mathcal{N}$ может быть задана с помощью КНФ*

$$f(y_1, \ldots, y_p) = \bigwedge_{(i,j) \in \mathcal{N}} \left(\bigvee_{\substack{1 \leqslant t \leqslant p \\ M\langle t,i \rangle \neq M\langle t,j \rangle}} y_t \right), \tag{9.1}$$

Следствие. *Каждая элементарная конъюнкция вида $y_{t_1}, \ldots, y_{t_r}$ сокращенной ДНФ функции $f(y_1, \ldots, y_p)$, получающаяся из КНФ (9.1) в результате раскрытия скобок и приведения подобных (см. §4), соответствует тупиковому тесту, связанному с множеством $T = \{t_1, \ldots, t_r\}$ и обратно.*

На данной лемме основан следующий алгоритм построения всех тупиковых тестов для матрицы M относительно цели контроля $\mathcal{N}$:

1. выписываем для функции теста КНФ вида (9.1);
2. раскрывая в ней скобки и приводя подобные, получаем сокращенную ДНФ функции теста;
3. сопоставляем каждой элементарной конъюнкции этой сокращенной ДНФ тупиковый тест.

Так, например, для построения всех тупиковых диагностических тестов матрицы M вида

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

выпишем соответствующую ей КНФ (9.1):

$$F(y_1, y_2, y_3, y_4) = (y_1 \vee y_2 \vee y_3) \cdot (y_2 \vee y_4) \cdot (y_1 \vee y_3 \vee y_4).$$

Раскрывая в этой КНФ скобки и приводя подобные, получим сокращенную ДНФ для функции теста:

$$F(y_1, y_2, y_3, y_4) = y_1y_2 \vee y_1y_4 \vee y_2y_3 \vee y_2y_4 \vee y_3y_4.$$

Следовательно, тупиковыми диагностическими тестами матрицы M являются множества ее строк с номерами

$$\{1, 2\},\ \{1, 4\},\ \{2, 3\},\ \{2, 4\},\ \{3, 4\}.$$

Для упрощения преобразований, связанных с применением описанного алгоритма, вместо исходной матрицы M можно рассматривать отделимую по строкам матрицу $\check{M}$, получающуюся из M удалением повторных вхождений одинаковых строк. При этом, очевидно, любой тупиковый тест матрицы M получается из тупикового теста той же длины матрицы $\check{M}$ в результате замены каждой его строки равной ей строкой матрицы M и обратно.

Рассмотрим, далее, некоторые оценки длины диагностических тестов для матриц с заданным числом столбцов.

Лемма 9.2. *Длина любого тупикового диагностического теста для отделимой по столбцам матрицы из множества $B^{p,s}$ заключена в пределах от $\lceil \log s \rceil$ до $(s-1)$.*

Доказательство. Пусть $M \in B^{p,s}$ и пусть, для определенности, первые t строк матрицы M образуют ее тупиковый диагностический тест. Очевидно, что в этом случае все столбцы матрицы $\widehat{M}$, состоящей из первых t строк матрицы M, различны

и, следовательно, $s \leqslant 2^t$, то есть $t \geqslant \lceil \log s \rceil$, поскольку число различных булевых столбцов высоты t равно 2^t. Требуемая нижняя оценка длины диагностического теста установлена.

Докажем теперь, что $t \leqslant (s-1)$. Для этого на множестве столбцов матрицы $\widehat{M}$ при любом q, $q \in [1,t]$, определим отношение эквивалентности $\underset{q}{\sim}$ так, что $m' \underset{q}{\sim} m''$ тогда и только тогда, когда столбцы m' и m'' матрицы $\widehat{M}$ совпадают в строках с номерами из отрезка $[1,q]$. Будем считать, по определению, что $\underset{0}{\sim}$ — тривиальное отношение с одним классом эквивалентности, а число классов эквивалентности по отношению $\underset{q}{\sim}$, где $q \in [1,t]$, будем обозначать через $\theta(q)$.

Из общих свойств отношений эквивалентности (см. §1) вытекает, что при любом q, $q \in [1,t)$, каждый класс эквивалентности по отношению $\underset{q}{\sim}$ либо является классом эквивалентности по отношению $\underset{q+1}{\sim}$, либо представляет собой объединение двух таких классов и, следовательно, $\theta(q) \leqslant \theta(q+1)$. В силу тупиковости теста полученное неравенство является строгим, так как равенство $\theta(q) = \theta(q+1)$ возможно тогда и только тогда, когда каждый класс эквивалентности отношения $\underset{q}{\sim}$ является классом эквивалентности отношения $\underset{q+1}{\sim}$ и обратно, то есть строка с номером q является «лишней» в рассматриваемом тесте.

Из диагностичности теста вытекает, что $\theta(t) = s$, и, таким образом, выполняются соотношения

$$1 = \theta(0) < \theta(1) < \cdots < \theta(t) = s,$$

из которых следует, что $t \leqslant (s-1)$.

Лемма доказана. □

Замечание. Указанные в лемме границы достигаются: нижняя — на любой отделимой по столбцам матрице из $B^{p,s}$, где $p = \lceil \log s \rceil$, а верхняя — на матрице из $B^{s-1,s}$, все столбцы которой различны и содержат не более одной единицы (обе матрицы имеют единственный диагностический тест, состоящий из всех строк).

Следующее утверждение характеризует «типичное» значение длины диагностического теста, то есть длину минимального диагностического теста у «почти всех» таблиц контроля.

Лемма 9.3. *Пусть $\varphi(s)$, $t(s)$ и $p(s)$ — целочисленные неотрицательные функции натурального аргумента s, для которых*

$$t(s) = \lceil 2 \log s \rceil + \varphi(s), \quad p(s) \geqslant t(s), \quad \varphi(s) \xrightarrow[s\to\infty]{} \infty.$$

Тогда у почти всех отделимых по столбцам матриц из $B^{p(s),s}$ первые $t(s)$ строк образуют диагностический тест.

Доказательство. Заметим, что все матрицы из $B^{p,s}$, где $p = p(s)$, у которых первые $t = t(s)$ строк образуют диагностический тест, отделимы по столбцам. Легко видеть также, что число таких матриц равно

$$2^t \left(2^t - 1\right) \cdots \left(2^t - s + 1\right) \cdot 2^{(p-t)s} = 2^{ps} \left(1 - \frac{1}{2^t}\right) \cdots \left(1 - \frac{(s-1)}{2^t}\right),$$

а их доля среди всех отделимых по столбцам матриц из $B^{p,s}$ не меньше, чем

$$\left(1 - \frac{1}{2^t}\right) \cdots \left(1 - \frac{(s-1)}{2^t}\right) \geqslant 1 - \frac{s^2}{2^t} \geqslant 1 - 2^{-2\varphi(s)},$$

и, следовательно, стремиться к 1 при s стремящемся к бесконечности.

Лемма доказана. □

Следствие. *Для любой неотрицательной и неограниченно возрастающей функции $\varphi(s)$ у почти всех отделимых по столбцам матриц из $B^{p,s}$ длина минимального диагностического теста не больше, чем* $2\log s + \varphi(s)$

Глава 2

Основные классы схем, их структурные представления и эквивалентные преобразования

§1 Основные понятия из теории графов, сетей, схем

Понятие графа, которое обобщает понятие бинарного отношения (см. §1 гл. 1), часто используется для описания структурных моделей, связанных с вычислениями, представлениями или реализациями дискретных функций. Напомним основные понятия и обозначения из теории графов, сетей и схем, а также сформулируем некоторые известные результаты (см., например, []).

Пару (V, E), где E — сочетание (с возможными повторениями) над множеством упорядоченных и неупорядоченных пар из V, будем, как обычно, называть *графом с множеством вершин* $V = V(G)$ *и множеством ребер* $E = E(G)$. При этом длина сочетания E считается числом ребер графа G и обозначается через $|E|$. Упорядоченные (неупорядоченные) пары вершин называются *ориентированными ребрами* или, иначе *дугами* (соответственно *неориентированными ребрами*), одинаковые пары — *параллельными ребрами* (*дугами*), дуги, отличающиеся порядком вершин, — *противоположными дугами*, а пары из совпадающих вершин — *петлями*. Граф из ориентированных (неориентированных) ребер считается *ориентированным* (соответственно *неориентированным*). Заметим, что бинарное отношение представляет собой ориентированный граф без параллельных дуг. При этом симметричное антирефлексивное отношение можно рассматривать как неориентированный граф без параллельных ребер и петель.

Будем говорить, что ориентированное (неориентированное) ребро *инцидентно* составляющим его вершинам, а дуга (u, v) *исходит* или, иначе, *выходит* из вершины u и *заходит* или, иначе, *входит* в вершину v. Число ребер, инцидентных вершине v

(входящих в v, выходящих из v) в графе G, называется *степенью* (соответственно *полустепенью захода*, *полустепенью исхода*) вершины v в графе G и обозначается через $d_G(v)$ (соответственно $d_G^+(v)$, $d_G^-(v)$). Заметим, что

$$\sum_{u \in V(G)} d_G(v) = 2\,|E(G)|\,, \tag{1.1}$$

и что $d_G(v) = d_G^+(v) + d_G^-(v)$ ($d_G(v) = d_G^+(v) = d_G^-(v)$) в случае ориентированного (соответственно неориентированного) графа G. Вершина v называется *изолированной вершиной* (*стоком*, *истоком*) графа G, если $d_G(v) = 0$ (соответственно $d_G^-(v) = 0$, $d_G^+(v) = 0$).

Граф $G' = (V', E')$ называется *подграфом* графа $G = (V, E)$, если $V' \subseteq V$ и $E' \subseteq E$. При этом G' считается *подграфом графа G, натянутым на множество вершин V'*, если E' включает в себя все входящие в E пары вершин из V'. Подграф, содержащий все вершины исходного графа, называется *остовным подграфом*. Легко видеть, что подграф всегда можно получить из исходного графа в результате (многократного) применения операций *удаления вершины* (*ребра*). При этом удаление вершины, как обычно, подразумевает удаление всех инцидентных ей ребер.

При определении понятий, связанных с «движениями» по графу, ограничимся случаем ориентированных графов, считая, как обычно, что неориентированное ребро эквивалентно двум противоположным дугам, связанным с той же парой вершин. Последовательность C, состоящая из ребер e_1, e_2, …, e_n, где $e_i = (v_i, v_{i+1}) \in E(G)$ при всех i, $i \in [1, n]$, называется $(v_1 - v_{n+1})$-*путем* графа G. При этом вершина v_1 (v_{n+1}) считается *начальной* (соответственно *конечной*) вершиной этого пути, вершины v_2, …, v_n — его *внутренними* вершинами, а число n — его *длиной*. Если все ребра пути различны (как элементы соответствующего сочетания), то он называется *цепью*, а если, кроме того, различны все его вершины, то — *простой цепью*. Если начальная и конечная вершины пути (цепи) C совпадают, то C считается *замкнутым путем* (соответственно *циклом*). Цикл, в котором все вершины, кроме начальной и конечной, различны, называется *простым циклом*.

Будем говорить, что *вершина u достижима из вершины v в графе G*, где $u, v \in V(G)$, если $u = v$, или в G существует $(v - u)$-цепь. Заметим, что отношение достижимости вершин графа G является рефлексивным и транзитивным, а если G — неориентированный граф, то и симметричным. Следовательно, множество вершин графа G распадается на классы эквивалентности по отношению их достижимости в графе $\widehat{G}$, который получается из графа G заменой каждой дуги на соответствующее неориентированное ребро ($G = \widehat{G}$, если G — неориентированный граф). При этом подграф графа G, натянутый на каждый такой класс вершин, называется *связной компонентой* графа G, а множество всех его связных компонент обозначается через $c(G)$. Граф G называется *связным*, если $|c(G)| = 1$.

Напомним, что

$$|E(G)| - |V(G)| + |c(G)| \geqslant 0 \tag{1.2}$$

и что левая часть (1.2) называется *цикломатическим числом* графа G. Напомним также, что это число равно максимальному числу линейно независимых относительно операции симметрической разности[1] подграфов графа G, состоящих из одного простого цикла и изолированных вершин.

Неориентированный (ориентированный) граф, не имеющий циклов (соответственно ориентированных циклов), называется *ациклическим*. Заметим, что в ориентированном ациклическом графе G всегда есть как стоки, так и истоки. При этом для каждой его вершины v можно определить ее *глубину* (соответственно *исходящую глубину*), как максимальную длину $(u-v)$- (соответственно $(v-u)$-) путей графа G, где u — один из истоков (соответственно, стоков) G. Легко видеть, что отношение достижимости является отношением частичного порядка на множестве вершин ориентированного ациклического графа и обратно.

Неориентированный связный ациклический граф называется *деревом*. Для дерева G, как известно, имеет место равенство

$$|E(G)| = |V(G)| - 1. \tag{1.3}$$

Дерево с выделенной вершиной (*корнем*) называется *корневым деревом*, а все отличные от корня вершины степени 1 этого дерева считаются его *листьями*. Ориентированный граф, который получается из корневого дерева заменой каждого его неориентированного ребра на соответствующую дугу, «направленную» к корню, называется *ориентированным деревом*.

Граф, вершинам и (или) ребрам которого сопоставлены определенные символы (пометки), считается *помеченным графом*. Примером такого графа является, в частности, корневое дерево. Другим примером помеченного графа является ациклический граф с *монотонной нумерацией вершин*, когда для любой дуги номер вершины, из которой она исходит, больше номера вершины, в которую эта дуга входит. Ориентированный граф G называется *упорядоченным*, если для любой его вершины v, $v \in V(G)$, все ребра, входящие в v, упорядочены и пронумерованы числами $1, 2, \ldots, d_G^+(v)$.

Графы $G' = (V', E')$ и $G'' = (V'', E'')$ называются *изоморфными*, если существуют такие взаимнооднозначные отображения $\varphi : V' \to V''$ и $\psi : E' \to E''$, при которых вершины и неориентированные ребра (дуги) G' переходят в вершины и неориентированные ребра (соответственно дуги) G'' с сохранением отношения инцидентности

[1] Под симметрической разностью графов G_1 и G_2 понимается граф G, для которого

$$V(G) = V(G_1) \cup V(G_2), \quad E(G) = (E(G_1) \cup E(G_2)) \setminus (E(G_1) \cap E(G_2)).$$

(соответственно, исхода, захода) вершин и ребер, а также всех пометок. Для (конечного) множества графов $\mathcal{G}$ через $|\mathcal{G}|$ будем обозначать число попарно неизоморфных графов в $\mathcal{G}$. Известно, что

$$|\mathfrak{D}(q)| \leqslant 4^q, \tag{1.4}$$

где $\mathfrak{D}(q)$ — множество упорядоченных ориентированных корневых деревьев с не более, чем q ребрами.

Введем теперь общие определения и обозначения, связанные с сетями и «абстрактными» схемами, а также с реализацией функций в различных классах дискретных управляющих систем (классах схем).

Набор вида $\mathcal{G} = (G; V'; V'')$, где G — граф, а V' и V'' — выборки из множества $V(G)$ длины p и q соответственно, причем выборка V' является выборкой без повторений, называется (p, q)-*сетью*. При этом выборка V' (выборка V'') считается *входной* (соответственно *выходной*) *выборкой*, а ее i-я вершина называется i-*м входным* (соответственно *выходным*) *полюсом* или, иначе, i-*м входом* (соответственно *выходом*) сети $\mathcal{G}$. Вершины, не участвующие в выборках сети, считаются ее *внутренними* вершинами.

Сеть, в которой входная и выходная выборки совпадают (не совпадают), называется *сетью с неразделенными* (соответственно *с разделенными*) *полюсами*. При этом в случае неразделенных полюсов сеть $\mathcal{G} = (G; V; V)$ будем записывать в виде $\mathcal{G} = (G; V)$. Как правило, входы и выходы (полюса) сети имеют специальные пометки, которые отличают эти вершины от других вершин сети и указываются вместо них в соответствующих выборках. Таким образом, сети можно считать специальным частным случаем помеченных графов.

Примером сети является корневое дерево, входами которого считаются его листья, а выходом — корень. При этом порядок листьев во входной выборке ориентированного упорядоченного корневого дерева $\mathcal{D}$ задается их «естественной» нумерацией τ, отображающей множество листьев дерева $\mathcal{D}$ в $\mathbb{N}$ так, что $\tau(v') < \tau(v'')$ тогда и только тогда, когда $k' < k''$, где k' и k'' — номера дуг, по которым цепи, соединяющие листья v' и v'' соответственно с корнем $\mathcal{D}$, входят в свою первую общую вершину.

Дерево (ориентированное дерево) D, являющееся остовным подграфом графа G, называется *остовным поддеревом*, а дерево D', которое получается из D в результате «подсоединения» всех не вошедших в него ребер G к своим «начальным» вершинам, — *остовным наддеревом* графа G. Очевидно, что при этом граф G может быть получен из дерева D' в результате присоединения некоторых вершин степени 1 (листьев) к другим его вершинам. Заметим, что любой неориентированный связный граф, а также любой ориентированный ациклический граф с 1 стоком всегда имеют остовные поддеревья и наддеревья соответствующего типа.

Будем считать, что ребра и вершины остовного поддерева, а также ребра связанного с ним остовного наддерева имеют те же самые пометки, которые они имели в исходном графе. Будем предполагать, в частности, что остовное наддерево ориен-

тированного ациклического упорядоченного графа является упорядоченным, и что выход связной $(p, 1)$-сети является корнем ее остовного наддерева.

Под «абстрактной» схемой понимается сеть, часть пометок которой составляют входные переменные и которая реализует систему (матрицу), состоящую из функций от этих переменных. Схему, которая реализует систему ФАЛ Q_n (J_n, μ_n) будем называть *дешифратором* (соответственно *дизъюнктивным дешифратором*, *мультиплексором*) *порядка* n. Схемы, реализующие равные системы функций, называются *эквивалентными*. Предполагается, что изоморфные схемы всегда эквивалентны, и поэтому для любого конечного множества схем $\mathcal{U}$ выполняется неравенство

$$\|\mathcal{U}\| \leqslant |\mathcal{U}|\,, \tag{1.5}$$

где $\|\mathcal{U}\|$ — число попарно не эквивалентных схем в $\mathcal{U}$.

Способы реализации функций могут быть различными для различных классов схем. Во многих случаях (см., например, §2–§5) реализация функций происходит в каждой вершине схемы, а сама схема реализует при этом систему функций, реализуемых на ее выходах. В других классах (см., например, §6) схема реализует матрицу функций, которая связана с отношениями достижимости для входов и выходов сетей, получающихся из данной схемы при различных подстановках констант вместо переменных и т. п.

§2 Представление формул с помощью деревьев. Оптимизация подобных формул по глубине

В §1 главы 1 дано индуктивное определение формулы и реализуемой ею функции. Рассмотрим способ представления формул алгебры логики с помощью ориентированных упорядоченных деревьев.

Пусть, по-прежнему, $\mathcal{X} = \{x_1, x_2, \dots, x_n, \dots\}$ — счетный упорядоченный алфавит входных БП и пусть $\text{Б} = \{\varphi_1, \varphi_2, \dots, \varphi_b\}$ — базис, где ФАЛ $\varphi_i,\ i = 1, \dots, b$, зависит от $k_i,\ k_i \geqslant 1$, БП и является существенной ФАЛ, если $k_i \geqslant 2$. Предполагается, что Б — полный базис (см. §2 главы 1) и допускается, в общем случае, наличие в нем равных ФАЛ. Чаще всего мы будем иметь дело с базисом $\text{Б}_0 = \{\&, \vee, \neg\}$.

Сопоставим каждому ФС $\varphi_i,\ i = 1, \dots, b$, функциональный элемент (ФЭ) $\mathcal{E}_i$, имеющий k_i входов, причем входу с номером j соответствует j-я БП x_j ФАЛ φ_i и один выход, на котором эта ФАЛ реализуется (см. рис. 2.1a). Упрощенный вариант изображения ФЭ $\mathcal{E}_i$ в виде вершины графа с пометкой φ_i, в которую входят k_i упорядоченных, то есть пронумерованных числами $1, \dots, k_i$ дуг, показан на рис. 2.1b. При этом предполагается, что дуга с номером $j,\ 1 \leqslant j \leqslant k_i$, соответствует j-му входу ФЭ $\mathcal{E}_i$. В дальнейшем мы, как правило, не будем делать различий между функциональным символом φ_i и функциональным элементом $\mathcal{E}_i$.

a) b)

Рис. 2.1: функциональный элемент $\mathcal{E}_i$

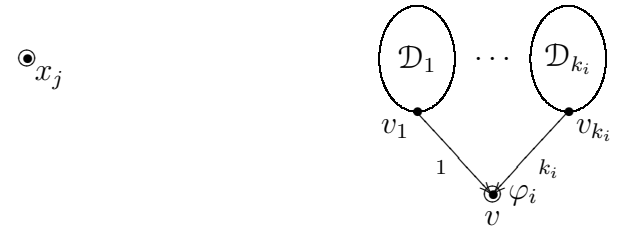
Множество всех формул над базисом Б будем обозначать через $\mathcal{U}_{\text{Б}}^{\Phi}$ и положим $\mathcal{U}_{\text{Б}_0}^{\Phi} = \mathcal{U}^{\Phi}$. Индукцией по глубине каждой формуле глубины q над Б можно сопоставить упорядоченное ориентированное корневое дерево глубины q, каждому листу которого приписана БП из $\mathcal{X}$, а каждой внутренней вершине — ФС из Б. Формуле x_j глубины 0 сопоставим «тривиальное» дерево с единственной вершиной, являющейся корнем и листом одновременно, которой приписана БП x_j (см. рис. 2.2a). Формуле $\mathcal{F}$ вида

$$\mathcal{F} = \varphi_i\left(\mathcal{F}_1, \ldots, \mathcal{F}_{k_i}\right), \tag{2.1}$$

которая является формулой глубины $(q+1)$ над Б, где

$$q = \max\left\{q_1, \ldots, q_{k_i}\right\}, \tag{2.2}$$

а $q_j,\ j = 1, \ldots, k_i$, — глубина главной подформулы $\mathcal{F}_j$ формулы $\mathcal{F}$, сопоставим дерево $\mathcal{D}$ глубины $(q+1)$ с корнем v, показанное на рис. 2.2b, где $\mathcal{D}_j,\ j = 1, \ldots, k_i$ — дерево глубины q_j с корнем v_j, которое соответствует формуле $\mathcal{F}_j$.



a) b)

Рис. 2.2: представление формулы деревом

Заметим, что формула $\mathcal{F}$ по сопоставленному ей дереву $\mathcal{D}$ восстанавливается однозначно, и что при этом поддеревья дерева $\mathcal{D}$ взаимнооднозначно сопоставляются подформулам формулы $\mathcal{F}$. На рис. 2.3a показано дерево, соответствующее формуле

$$\overline{\left((x_1 \vee x_2) \vee x_3\right)} \vee \left(x_3\left(x_1 \vee x_2\right) \vee x_1 x_2\right), \tag{2.3}$$

которая является формулой глубины 4 над базисом Б_0 и реализует ФАЛ $s_3^{\{0,2,3\}}$.

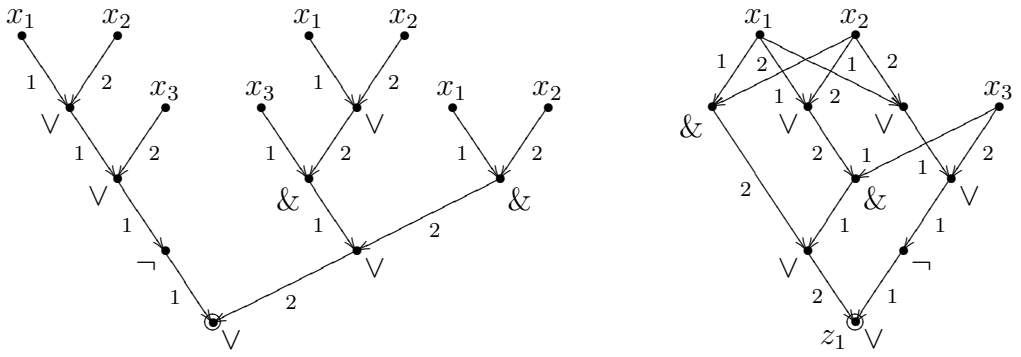


Рис. 2.3: представление формулы (2.3) деревом и квазидеревом

Для удобства будем считать, что в $\mathcal{U}^{\Phi}_{\text{Б}}$ входят не только отдельные формулы, но и упорядоченные системы (наборы) формул над базисом Б, что каждая такая система реализует набор, состоящий из ФАЛ, реализуемых ее формулами, и что этой системе формул соответствует система из деревьев, сопоставленных ее формулам.

Заметим, что ранг $R(\mathcal{F})$ формулы $\mathcal{F}$ равен числу листьев связанного с ней дерева $\mathcal{D}$, ее сложность $L(\mathcal{F})$ равна числу остальных вершин $\mathcal{D}$, а ее глубина $D(\mathcal{F})$ — глубине его корня. Заметим также, что порядок вхождения БП в запись формулы $\mathcal{F}$ при ее просмотре слева направо соответствует последовательности появления БП на листьях связанного с ней дерева,просматриваемых в «естественном» порядке (см. §1).

Рассмотрим теперь некоторые соотношения между параметрами формул над базисом Б_0. Заметим, что представляя формулы деревьями, такие соотношения можно доказывать более простым и наглядным способом. Так, индукцией по глубине формулы-дерева легко устанавливается справедливость следующего утверждения.

Лемма 2.1. *Для формулы $\mathcal{F}$, $\mathcal{F} \in \mathcal{U}^{\Phi}$, выполняются неравенства*

$$R(\mathcal{F}) \leqslant L(\mathcal{F}) + 1 \leqslant 2^{D(\mathcal{F})}. \tag{2.4}$$

Следствие.

$$D(\mathcal{F}) \geqslant \lceil \log(L(\mathcal{F}) + 1) \rceil. \tag{2.5}$$

Замечание. Ранг формулы $\mathcal{F}$ равен числу ФЭ $\&$, $\vee$ в ней, и поэтому первое из неравенств (2.4) переходит в равенство, если $\mathcal{F} \in \mathcal{U}^{\Phi}_{\{\&,\vee\}}$.

Формулы, получающиеся друг из друга эквивалентными преобразованиями на основе тождеств коммутативности и ассоциативности (см. §3 гл. 1), называются *подобными*. Легко видеть, что подобные формулы получаются друг из друга переста-

новкой аргументов и изменением порядка выполнения однотипных двуместных базисных операций, образующих соответствующую многоместную операцию, и поэтому могут отличаться друг от друга только глубиной.

Заметим, что сложность характеризует время вычисления формулы на одном процессоре, а глубина — время ее параллельного вычисления на неограниченном числе процессоров. Поэтому оптимизация подобных формул по глубине является частным случаем «распараллеливания» вычислений.

Лемма 2.2. *Пусть $\mathcal{F}$ — формула вида $x_1 \circ \cdots \circ x_t$, где $\circ \in \{\&, \vee\}$, и пусть для целых неотрицательных чисел $d, d_1, \ldots, d_t$ выполнено неравенство $2^{d_1} + \cdots + 2^{d_t} \leqslant \leqslant 2^d$. Тогда существует подобная $\mathcal{F}$ формула $\check{\mathcal{F}}$, в которой исходящая глубина входа x_i, $i = 1, \ldots, t$, не больше, чем $d - d_i$.*

Доказательство. Перестановкой и переименованием БП (аргументов) в формуле $\mathcal{F}$ можно добиться того, чтобы выполнялись неравенства:

$$d_1 \geqslant d_2 \geqslant \cdots \geqslant d_t. \tag{2.6}$$

Пусть теперь $\mathcal{F}'$ — формула вида $x_1 \circ \cdots \circ x_{2^d}$, которой соответствует полное двоичное d-ярусное дерево, а формула $\mathcal{F}''$ получается из $\mathcal{F}'$ удалением последних $\left(2^d - 2^{d_1} - \cdots - 2^{d_t}\right)$ вхождений БП вместе с теми ФС, которые с ними связаны. В силу (2.6) первые 2^{d_1} вхождений БП в $\mathcal{F}''$ составляют подформулу $\mathcal{F}_1$, которой соответствует полное двоичное d_1-ярусное дерево, содержащее 2^{d_1} вхождений БП в $\mathcal{F}''$, следующие 2^{d_2} вхождений БП в $\mathcal{F}''$ — подформулу $\mathcal{F}_2$, которой соответствует полное двоичное d_2-ярусное дерево, и так далее, вплоть до последних 2^{d_t} вхождений БП в $\mathcal{F}''$, составляющих подформулу $\mathcal{F}_t$, которой соответствует полное двоичное d_t-ярусное дерево. Обозначим через $\check{\mathcal{F}}$ формулу, которая получается из $\mathcal{F}''$ заменой подформулы $\mathcal{F}_i$ на БП x_i, $i = 1, \ldots, t$. Заметим, что $\check{\mathcal{F}}$ подобна $\mathcal{F}$ и что исходящая глубина БП x_i в $\check{\mathcal{F}}$ не больше чем $d - d_i$, то есть $\check{\mathcal{F}}$ является искомой формулой.

Лемма доказана. □

Следствие. *Для ЭК или ЭД $\mathcal{F}'$ существует подобная формула $\check{\mathcal{F}}'$ такая, что*

$$D\left(\check{\mathcal{F}}'\right) = \lceil \log\left(L\left(\mathcal{F}'\right) + 1\right) \rceil. \tag{2.7}$$

Действительно, если $\mathcal{F}' = x_1^{\sigma_1} \circ \ldots \circ x_t^{\sigma_t}$, где $\circ \in \{\&, \vee\}$, то искомая формула $\check{\mathcal{F}}'$ получается подстановкой $x_i^{\sigma_i}$ вместо x_i в формулу $\check{\mathcal{F}}$, которая строится по доказанной лемме для целых неотрицательных чисел:

$$d = \lceil \log\left(L\left(\mathcal{F}'\right) + 1\right) \rceil, \qquad d_i = \overline{\sigma}_i,$$

где $i = 1, \ldots, t$, так как

$$2^d \geqslant L\left(\mathcal{F}'\right) + 1 = \sum_{i=1}^{t} \left(1 + \overline{\sigma}_i\right) = \sum_{i=1}^{t} 2^{d_i}.$$

При этом нижняя оценка (2.7) вытекает из (2.5).

Для каждой формулы $\mathcal{F}$, $\mathcal{F} \in \mathcal{U}^{\Phi}$, индукцией по глубине определим величину $\mathrm{Alt}\,(\mathcal{F})$ так, что:

1. $\mathrm{Alt}\,(\mathcal{F}) = 0$, если $\mathcal{F}$ — ЭК или ЭД;
2. $\mathrm{Alt}\left(\overline{\mathcal{F}}\right) = \mathrm{Alt}\,(\mathcal{F}) + 1$, если $\mathcal{F}$ не является буквой;
3. $\mathrm{Alt}\,(\mathcal{F}_1 \circ \cdots \circ \mathcal{F}_t) = \max\{\mathrm{Alt}\,(\mathcal{F}_1), \ldots, \mathrm{Alt}\,(\mathcal{F}_t)\} + 1$, где $t \geqslant 2$ и $\circ \in \{\&, \vee\}$, если ни одна из формул $\mathcal{F}_1, \ldots, \mathcal{F}_t$ не является формулой вида $\mathcal{F}' \circ \mathcal{F}''$ и хотя бы одна из них не является буквой.

Величину $\mathrm{Alt}\,(\mathcal{F})$ будем называть *альтернированием* формулы $\mathcal{F}$. Легко видеть, что альтернирование формулы $\mathcal{F}$ с поднятыми отрицаниями равно максимальному числу изменений типов ФЭ $\&$ и $\vee$ в цепях дерева, соответствующего формуле $\mathcal{F}$. Очевидно также, что альтернирование любой (отличной от ЭК и ЭД) ДНФ или КНФ равно 1.

Лемма 2.3. *Для любой формулы $\mathcal{F}$ из $\mathcal{U}^{\Phi}$ существует подобная ей формула $\check{\mathcal{F}}$ такая, что*

$$D\left(\check{\mathcal{F}}\right) \leqslant \lceil \log\left(L\left(\mathcal{F}\right) + 1\right)\rceil + \mathrm{Alt}\,(\mathcal{F}). \tag{2.8}$$

Доказательство. Доказательство проведем индукцией по альтернированию формулы $\mathcal{F}$. Если $\mathrm{Alt}\,(\mathcal{F}) = 0$, то искомая формула $\check{\mathcal{F}}$ строится в соответствии со следствием из леммы 2.2 и удовлетворяет неравенству (2.8) в силу (2.7).

Пусть неравенство (2.8) справедливо для любой формулы $\mathcal{F}'$ такой, что $\mathrm{Alt}\,(\mathcal{F}') \leqslant (a-1)$, где $a \geqslant 1$, и пусть формула $\mathcal{F}$ имеет альтернирование a. Если $\mathcal{F} = \overline{\mathcal{F}'}$, то $\mathrm{Alt}\,(\mathcal{F}') \leqslant (a-1)$, а в качестве искомой формулы можно взять формулу $\check{\mathcal{F}} = \overline{\check{\mathcal{F}}'}$, где $\check{\mathcal{F}}'$ — подобная $\mathcal{F}'$ формула, которая удовлетворяет (2.8) и существует в силу индуктивного предположения. В остальных случаях представим формулу $\mathcal{F}$ в виде:

$$\mathcal{F} = \Phi\left(\mathcal{F}_1, \ldots, \mathcal{F}_t\right),$$

где $t \geqslant 2$, формула $\Phi\left(y_1, \ldots, y_t\right)$ при некотором $\circ$, $\circ \in \{\&, \vee\}$, имеет вид $y_1 \circ \ldots \circ y_t$, а альтернирование подформул $\mathcal{F}_1, \ldots, \mathcal{F}_t$ формулы $\mathcal{F}$ не больше, чем $(a-1)$. Положим

$$d = \lceil \log\left(L\left(\mathcal{F}\right) + 1\right)\rceil + 1 \quad \text{и} \quad d_i = \lceil \log\left(L\left(\mathcal{F}_i\right) + 1\right)\rceil,$$

где $i = 1, \ldots, t$, а затем для каждой формулы $\mathcal{F}_i$ построим по индуктивному предположению подобную ей формулу $\check{\mathcal{F}}_i$ такую, что

$$D\left(\check{\mathcal{F}}_i\right) \leqslant d_i + (a-1).$$

Так как при этом

$$2^d \geqslant 2\left(L\left(\mathcal{F}\right) + 1\right) = \sum_{i=1}^{t} 2\left(L\left(\mathcal{F}_i\right) + 1\right) \geqslant \sum_{i=1}^{t} 2^{d_i},$$

то построим по лемме 2.2 подобную формуле Φ формулу $\check{\Phi}$, в которой БП y_i, $i = 1, \ldots, t$, имеет исходящую глубину не больше, чем $d - d_i$. Следовательно, формула

$$\check{\mathcal{F}} = \check{\Phi}\left(\check{\mathcal{F}}_1, \ldots, \check{\mathcal{F}}_t\right),$$

подобна формуле $\mathcal{F}$, имеет глубину не больше, чем

$$d + (a - 2) = \lceil \log\left(L\left(\mathcal{F}\right) + 1\right)\rceil + a$$

и поэтому удовлетворяет неравенству (2.8).

Лемма доказана. □

Следствие. *Для любой ДНФ или КНФ* $\mathfrak{A}$ *существует подобная ей формула* $\check{\mathfrak{A}}$ *такая, что*

$$D\left(\check{\mathfrak{A}}\right) \leqslant \lceil \log\left(L\left(\mathfrak{A}\right) + 1\right)\rceil + 1.$$

Введенное выше понятие подобных формул без изменений переносится на любой базис, содержащий произвольный набор одноместных ФАЛ вместе с каким-либо набором двуместных ФАЛ из множества $\{x_1 \cdot x_2, x_1 \vee x_2, x_1 \oplus x_2, x_1 \sim x_2\}$, то есть множества двуместных ФАЛ, для которых выполнены тождества ассоциативности и коммутативности. Для каждого такого базиса Б аналогично базису $Б_0$ вводится понятие альтернирования формулы, в соответствии с которым пункт 2 определения альтернирования для базиса $Б_0$ распространяется на все одноместные ФАЛ из Б, пункт 3 — на все двуместные ФАЛ этого базиса, и пункт 1 — на все ФАЛ вида $\varphi_1\left(x_1\right) \circ \cdots \circ \varphi_t\left(x_t\right)$, где $\circ$ — двуместная, а $\varphi_1, \ldots, \varphi_t$ — одноместные ФАЛ из Б. Заметим, что при этом будут справедливы леммы 2.2 и 2.3. В частности, для полинома Жегалкина $\mathfrak{A}$ в силу того, что $\mathrm{Alt}\left(\mathfrak{P}\right) = 1$, будет справедливо следствие из леммы 2.3.

§3 Схемы из функциональных элементов и операции над ними. Оценка числа формул и схем в базисе $\{\&, \vee, \neg\}$

Рассмотрим теперь более общую по сравнению с формулами модель — модель схем из функциональных элементов (СФЭ), в которой последовательность операций суперпозиции базисных ФАЛ задается с помощью ориентированного ациклического графа, обобщающего дерево, и где возможно многократное использование промежуточных результатов. По существу СФЭ получается из системы деревьев (системы формул) в результате отождествления некоторых изоморфных поддеревьев (совпадающих подформул).

Пусть $\mathcal{Z}$ — счетный упорядоченный алфавит (выходных) БП, который не имеет общих БП с алфавитом $\mathcal{X}$.

Определение. *Схемой из функциональных элементов над базисом* Б называется ориентированная ациклическая упорядоченная сеть Σ, входная выборка которой состоит из всех истоков Σ, а вершины помечены следующим образом:

1. каждому входу (выходу) Σ сопоставлена БП из $\mathcal{X}$ (соответственно $\mathcal{Z}$), являющаяся пометкой связанной с ним вершины, причем различным входам (выходам) сопоставлены различные БП, а упорядоченность вершин во входной и выходной выборках Σ определяется упорядоченностью сопоставленных им БП;

2. каждая отличная от истока вершина v схемы Σ помечена ФС φ_i, где $k_i = d_\Sigma^+(v)$.

Заметим, что в общем случае вершины в выходной выборке СФЭ могут повторяться, то есть одной и той же выходной вершине может быть сопоставлено несколько БП из $\mathcal{Z}$. Если множество $X = \{x_{i_1}, \ldots, x_{i_n}\}$ ($Z = \{z_{j_1}, \ldots, z_{j_m}\}$) состоит из всех входных (соответственно выходных) БП СФЭ Σ, перечисленных в порядке возрастания их номеров в алфавите $\mathcal{X}$ (соответственно $\mathcal{Z}$), то, в соответствии с §1, будем записывать СФЭ Σ в виде $\Sigma = \Sigma(X; Z)$ или $\Sigma = \Sigma(x; z)$, где $x = (x_{i_1}, \ldots, x_{i_n})$ и $z = (z_{j_1}, \ldots, z_{j_m})$ — наборы БП, соответствующие множествам X и Z.

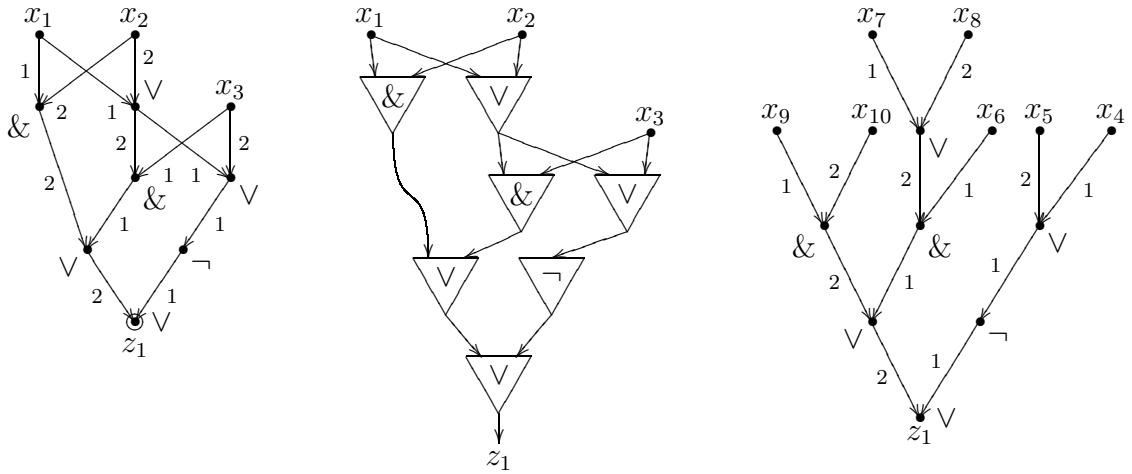


Рис. 3.1: СФЭ, полученная из квазидерева на рис. 2.3b, и ее каркас

Схема Σ, которая получается из дерева $\mathcal{D}$, связанного с формулой $\mathcal{F}$ из $\mathcal{U}_{\text{Б}}^{\Phi}$, в результате отождествления листьев с одинаковыми пометками и приписывания его корню выходной БП из $\mathcal{Z}$, называется *квазидеревом, соответствующим формуле* $\mathcal{F}$. Заметим, что указанное квазидерево Σ однозначно определяет формулу $\mathcal{F}$ и является СФЭ над базисом Б. Из этого квазидерева путем «отождествления» (наложения)

его изоморфных квазиподдеревьев можно получать и другие СФЭ, задающие формулу $\mathcal{F}$. На рис. 2.3b показано квазидерево над базисом $Б_0$ с входными БП x_1, x_2, x_3 и выходной БП z_1, которое получено из дерева, сопоставленного формуле (2.3) и изображенного на рис. 2.3a. На рис. 3.1a приведена СФЭ, полученная из данного квазидерева в результате отождествления двух его изоморфных квазиподдеревьев, а на рис. 3.1b дано более «наглядное» изображение этой СФЭ в виде системы соединенных соответствующим образом ФЭ.

Обозначим через $\mathcal{U}_Б^C$ множество всех СФЭ над базисом Б, и пусть $\mathcal{U}^C = \mathcal{U}_{Б_0}^C$. Заметим, что система квазидеревьев с общими входами, соответствующая системе формул над базисом Б, является СФЭ над Б, если выходам этих квазидеревьев приписаны различные выходные БП. В связи с этим формулы над Б и их системы будем считать частным случаем СФЭ над Б, полагая, что имеет место включение $\mathcal{U}_Б^Ф \subseteq \mathcal{U}_Б^C$. Заметим также, что СФЭ Σ, $\Sigma \in \mathcal{U}_Б^C$, входит в $\mathcal{U}_Б^Ф$ тогда и только тогда, когда все стоки Σ, и только они, являются ее выходами, а из каждой вершины Σ, отличной от ее входов и выходов, исходит одна дуга.

Определим теперь функционирование СФЭ $\Sigma = \Sigma(x_1, \ldots, x_n; z_1, \ldots, z_m)$ над базисом Б. Сначала индукцией по q, $q = 0, 1, \ldots$, определим для каждой вершины v глубины q в схеме Σ реализуемую в ней формулу $\mathcal{F}_v = \mathcal{F}_v(x_1, \ldots, x_n)$ глубины q над базисом Б. Если $q = 0$, то есть v — вход Σ, положим $\mathcal{F}_v = x_j$, где x_j — входная БП, сопоставленная вершине v. Пусть теперь v — вершина глубины $q+1$, $q \geqslant 0$, схемы Σ, которая имеет пометку φ_i, и в которую входит k_i дуг, причем дуга с номером j, $1 \leqslant j \leqslant k_i$, исходит из вершины v_j глубины q_j, где уже реализована формула $\mathcal{F}_j = \mathcal{F}_{v_j}$ глубины q_j, а для чисел q, q_1, …, q_{k_i} выполнено (2.2). Тогда в вершине v реализуется формула $\mathcal{F} = \mathcal{F}_v$ вида (2.1), которая имеет глубину $(q+1)$. При этом считается, что в вершине v СФЭ Σ *реализуется ФАЛ* $f(x_1, \ldots, x_n)$, если ФАЛ f реализуется формулой $\mathcal{F}_v$, и что СФЭ Σ *реализует систему ФАЛ* F, $F = (f_1, \ldots, f_m)$, или *реализует систему булевых уравнений* $z_1 = f_1, \ \ldots, \ z_m = f_m$, если f_j, $j = 1, \ldots, m$, — ФАЛ, реализованная в той выходной вершине СФЭ Σ, которой приписана БП z_j.

Заметим, что квазидерево, которое соответствует формуле $\mathcal{F}$, реализующей ФАЛ f, а также любая СФЭ, полученная из него отождествлением изоморфных квазиподдеревьев, реализует и формулу $\mathcal{F}$, и ФАЛ f. Так, СФЭ на рис. 3.1 реализует формулу (2.3) и ФАЛ $s_3^{\{0,2,3\}}(x_1, x_2, x_3)$, или уравнение $z_1 = s_3^{\{0,2,3\}}(x_1, x_2, x_3)$.

Также, как и для формул, для каждой СФЭ Σ, $\Sigma \in \mathcal{U}_Б^C$, определим следующие параметры (функционалы сложности):

1. $L(\Sigma)$ — *сложность* Σ, то есть число всех ее ФЭ;

2. $D(\Sigma)$ — *глубина* Σ, то есть максимальная глубина ее вершин.

Эти параметры имеют такой же содержательный смысл, что и в случае формул (см. §2).

В соответствии с §1 две СФЭ считаются изоморфными, если они изоморфны как помеченные графы, и эквивалентными, если они реализуют равные системы ФАЛ. Заметим, что СФЭ всегда эквивалентна системе формул, реализуемых ею на своих выходах. Заметим также, что изменение нумерации дуг, входящих в такую вершину v СФЭ Σ, которой сопоставлен ФЭ $\mathcal{E}_i$ с симметрической ФАЛ φ_i, не изменяет ФАЛ, реализуемую в вершине v, а значит, не влияет на функционирование Σ. В связи с этим в подобных случаях номера дуг, входящих в вершину v, могут не указываться. Легко видеть, что в соответствующих друг другу вершинах изоморфных СФЭ реализуются одинаковые формулы, а значит, и одинаковые ФАЛ. Следовательно, две изоморфные СФЭ эквивалентны, то есть для СФЭ справедливо неравенство (1.5).

Вершина СФЭ называется *висячей*, если она является стоком, но не является выходом схемы. Схема называется *приведенной*, если в ней нет висячих вершин. Заметим, что система формул является приведенной СФЭ, и что из любой СФЭ можно получить эквивалентную ей приведенную СФЭ с помощью операции *удаления висячих вершин*. Заметим также, что приведенные СФЭ, и только они, получаются из систем квазидеревьев в результате отождествления некоторых изоморфных квазиподдеревьев, и что в приведенных СФЭ все вершины лежат на цепях, идущих от входов схемы к ее выходам.

Удаление висячих вершин и отождествление изоморфных квазиподдеревьев являются примерами эквивалентных преобразований СФЭ, то есть преобразований, не изменяющих функционирование схем (см. §8–§10). Рассмотрим ряд таких структурных преобразований СФЭ, которые обобщают операцию суперпозиции ФАЛ и используются для построения сложных схем из более простых.

Также, как и в случае формул, простейшим видом суперпозиции СФЭ является операция *переименования входов схемы* с возможным их отождествлением. Определим, далее, операцию *снятия* (*дублирования*) *выхода схемы*, то есть удаления с него имеющейся (соответственно добавления к нему новой) выходной БП и другим частным случаем суперпозиции СФЭ будем считать операцию *переименования выходов схемы* с возможным их дублированием или снятием. Переименование входов и выходов СФЭ приводит к соответствующему переименованию (с возможным отождествлением) переменных у реализуемых ФАЛ и перестановке (с возможным повторением или удалением) этих ФАЛ.

Введем теперь операцию *объединения схем*, не имеющих общих вершин и переменных, как обычное объединение соответствующих графов. Заметим, что в результате объединения СФЭ $\Sigma'(x';z')$ и СФЭ $\Sigma''(x'';z'')$, реализующих системы ФАЛ F' и F'' соответственно, получается СФЭ $\Sigma=\Sigma'\cup\Sigma''$, которая имеет вид[1] $\Sigma=\Sigma((x',x'');(z',z''))$ и реализует систему ФАЛ (F',F'') (см. рис. 3.2а). При этом, очевидно, ФАЛ из набора F' (F'') не зависят существенно от БП из набора x'' (соответственно x')

[1]Предполагается, что номер любой БП из x' (z') меньше номера любой БП из x'' (соответственно z''). В остальных случаях происходит необходимая перестановка входных и выходных БП СФЭ Σ.

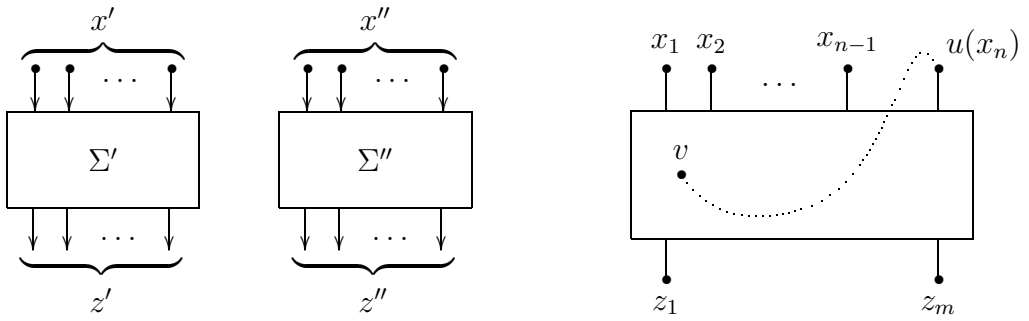


Рис. 3.2: к определению объединения схем и присоединения входа схемы к ее вершине

Определим, наконец, операцию *присоединения входа схемы к ее вершине*, которая из него не достижима. Пусть, для определенности, СФЭ Σ' получается из СФЭ $\Sigma(x_1, \ldots, x_n; z_1, \ldots, z_m)$ в результате присоединения входа x_n, связанного с вершиной u, к вершине v (см. рис. 3.2b)), то есть

$$\Sigma' = \Sigma'(x_1, \ldots, x_{n-1}; z_1, \ldots, z_m),\ V(\Sigma') = V(\Sigma) \setminus \{u\},$$

а множество дуг $E(\Sigma')$ является результатом замены вершины u вершиной v в дугах множества $E(\Sigma)$. Если при этом v — выходная вершина Σ, то СФЭ Σ'', которая получается в результате снятия с вершины v выходной БП z_i, считается результатом операции *присоединения входа* x_n *к выходу* z_i СФЭ Σ. Пусть, далее, $f_w(x_1, \ldots, x_n)$ — ФАЛ, реализуемая в вершине w СФЭ Σ, причем $f_w = g_w(x_1, \ldots, x_{n-1})$, если w не достижима из вершины u. Из определений следует, что в вершине w СФЭ Σ' реализуется ФАЛ $g_w(x_1, \ldots, x_{n-1})$, если w не достижима из вершины u в СФЭ Σ, и ФАЛ $f_w(x_1, \ldots, x_{n-1}, g_v(x_1, \ldots, x_{n-1}))$ в остальных случаях.

Будем говорить, что СФЭ Σ имеет вид $\Sigma = \Sigma''(\Sigma')$, то есть является *суперпозицией схем* Σ'' *и* Σ' без общих вершин и переменных, если она получается в результате объединения этих схем и присоединения (части) входов схемы Σ'' к (некоторым) выходам схемы Σ'. При этом (см. описание операции присоединения) схема Σ будет реализовать ФАЛ, получающиеся в результате соответствующей подстановки (некоторых) ФАЛ, реализованных схемой Σ' вместо (части) переменных ФАЛ, реализованных схемой Σ''. Заметим, что любое переименование выходов (входов) СФЭ Σ можно задать суперпозицией вида $\Sigma''_2(\Sigma''_1(\Sigma))$ (соответственно $\Sigma(\Sigma'_1(\Sigma'_2))$), где СФЭ Σ'_i и Σ''_i, $i = 1, 2$, состоят из изолированных вершин. Заметим также, что любая СФЭ может быть получена в результате многократного применения операции суперпозиции, на каждом шаге которой происходит присоединение одного ФЭ, к СФЭ, первоначально состоящей из изолированных вершин.

На рис. 3.3a) показана СФЭ $\Sigma_2^{\oplus}$, имеющая сложность 4 и реализующая ФАЛ $x_1 \oplus x_2$, а на рис. 3.3b) — СФЭ $\Sigma_q^{\oplus}$, $q \geqslant 3$, которая является результатом «последовательной» суперпозиции $(q-1)$ схем $\Sigma_2^{\oplus}$ и реализует ФАЛ $\ell_q(x_1, \ldots, x_q)$ со сложностью $4q - 4$.

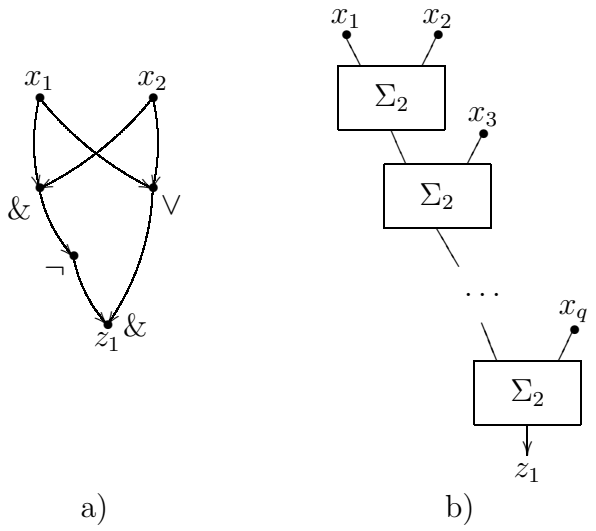


Рис. 3.3: пример суперпозиции СФЭ

Переменная, которая встречается в формуле только один раз, называется *бесповторной* переменной этой формулы. Формула называется *бесповторной*, если бесповторны все существенные БП реализуемой ею ФАЛ, и *абсолютной*, если бесповторны все ее БП. Заметим, что СФЭ вида $\Sigma = \Sigma''(\Sigma')$, где Σ' и Σ'' — системы формул, является системой формул тогда и только тогда, когда к каждому выходу Σ', участвующему в присоединениях к совпадающему с выходом ФЭ, присоединяется бесповторный вход Σ''.

Абсолютная формула $\mathcal{F}(x_{n+1}, \ldots, x_{n+p})$ называется *каркасом* приведенной СФЭ $\Sigma(x_1, \ldots, x_n; z_1)$, если вхождение БП x_{n+i}, $i \in [1, p]$, является i-м вхождением БП в $\mathcal{F}$, а дерево формулы $\mathcal{F}$ отличается от наддерева СФЭ Σ только пометками листьев. При этом, очевидно,

$$L(\Sigma) = L(\mathcal{F}), \quad D(\Sigma) \geqslant D(\mathcal{F}). \tag{3.1}$$

Из (3.1) следует, в частности, что соотношения (2.4)–(2.5) верны для любой приведенной СФЭ Σ, $\Sigma \in \mathcal{U}^{\mathrm{C}}$, с одним выходом. На рис. 3.1c) показан каркас СФЭ, изображенной на рис. 3.1a).

Легко видеть (см. рис. 3.4), что любая формула (приведенная СФЭ с одним выходом) Σ от БП $x_1, \ldots, x_n$ может быть получена из своего каркаса $\mathcal{F}$ в результате применения ряда операций присоединения входов $\mathcal{F}$ к входам $x_1, \ldots, x_n$ (соответственно к входам $x_1, \ldots, x_n$ и внутренним вершинам $\mathcal{F}$).

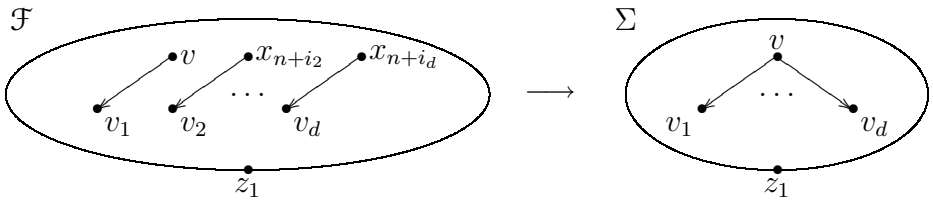


Рис. 3.4: получение схемы Σ из ее каркаса $\mathcal{F}$

Обозначим через $\mathcal{U}^{\mathrm{C}}_{\mathrm{Б}}(L,n)$ ($\mathcal{U}^{\Phi}_{\mathrm{Б}}(L,n)$ и $\mathcal{U}^{\Phi}_{\mathrm{Б}}[D,n]$) множество приведенных СФЭ $\Sigma=\Sigma(x_1,\ldots,x_n;z_1)$ (соответственно формул $\mathcal{F}=\mathcal{F}(x_1,\ldots,x_n)$) над базисом Б, для которых $L(\Sigma)\leqslant L$ (соответственно $L(\mathcal{F})\leqslant L$ и $D(\mathcal{F})\leqslant D$), причем индекс $\mathrm{Б}_0$ будем, как обычно, опускать. Заметим, что из неравенства (2.4) вытекает включение

$$\mathcal{U}^{\Phi}[D,n]\subseteq\mathcal{U}^{\Phi}\left(2^D-1,n\right). \tag{3.2}$$

Теорема 3.1. *Для любых натуральных n, L, D выполняются неравенства*

$$\left\|\mathcal{U}^{\mathrm{C}}(L,n)\right\|\leqslant(32(L+n))^{L+1},\qquad\left\|\mathcal{U}^{\Phi}(L,n)\right\|\leqslant(32n)^{L+1} \tag{3.3}$$

$$\left\|\mathcal{U}^{\Phi}[D,n]\right\|\leqslant(32n)^{2^D}. \tag{3.4}$$

Доказательство. Пусть $\Sigma\in\mathcal{U}^{\mathrm{C}}(L,n)$, а $\check{\mathcal{F}}$ — каркас Σ. В силу (3.1) и леммы 2.1 формула $\check{\mathcal{F}}$ удовлетворяет соотношениям

$$R\left(\check{\mathcal{F}}\right)\leqslant L+1,\quad\left|E\left(\check{\mathcal{F}}\right)\right|\leqslant 2L\left(\check{\mathcal{F}}\right)\leqslant 2L.$$

Заметим (см. (1.4)), что число попарно не изоморфных корневых ориентированных упорядоченных деревьев с не более, чем $2L$, ребрами не превосходит 4^{2L}, а число способов пометки внутренних вершин такого дерева символами ФЭ из $\mathrm{Б}_0$ с подходящим числом входов не больше, чем 2^L. Следовательно, число попарно не изоморфных каркасов для схем из $\mathcal{U}^{\mathrm{C}}(L,n)$ не превосходит 32^L.

Напомним, далее, что любая формула $\mathcal{F}$ (СФЭ Σ) из $\mathcal{U}^{\mathrm{C}}(L,n)$ может быть получена в результате присоединения каждого из $R\left(\check{\mathcal{F}}\right)\leqslant L+1$ входов формулы $\check{\mathcal{F}}$, являющейся ее каркасом, к входам x_1, …, x_n (соответственно к входам x_1, …, x_n и внутренним вершинам $\check{\mathcal{F}}$), которое можно осуществить не более, чем n^{L+1} (соответственно $(L+n)^{L+1}$) способами. Таким образом, в силу (1.5), (3.2)

$$\begin{aligned}
&\left\|\mathcal{U}^{\Phi}(L,n)\right\|\leqslant 32^L\cdot n^{L+1}\leqslant(32n)^{L+1},\\
&\left\|\mathcal{U}^{\mathrm{C}}(L,n)\right\|\leqslant 32^L\cdot(L+n)^{L+1}\leqslant(32(L+n))^{L+1},\\
&\left\|\mathcal{U}^{\Phi}[D,n]\right\|\leqslant\left\|\mathcal{U}^{\Phi}\left(2^D-1,n\right)\right\|\leqslant(32n)^{2^D}.
\end{aligned}$$

Теорема доказана. □

Следствие. *Число попарно не эквивалентных формул* $\mathcal{F}(x_1, \ldots, x_n)$ *с поднятыми отрицаниями над базисом* Б_0*, для которых* $R(\mathcal{F}) \leqslant R$*, не превосходит* $(64n)^R$.

Действительно, сопоставим формуле $\mathcal{F}$ указанного вида формулу $\mathcal{F}'$ из $\mathcal{U}^{\Phi}_{\{\&,\vee\}}$ от БП $x_1, \ldots, x_{2n}$, которая получается из $\mathcal{F}$ заменой каждой ее подформулы $\overline{x}_i$, $i \in \in [1, n]$, формулой x_{i+n} и для которой в силу замечания к лемме 2.1

$$L(\mathcal{F}') = R(\mathcal{F}) - 1 \leqslant R - 1.$$

Очевидно, что при таком сопоставлении неэквивалентные формулы переходят в неэквивалентные, и поэтому число попарно не эквивалентных формул рассматриваемого вида не больше, чем $\left\|\mathcal{U}^{\Phi}(R-1, 2n)\right\|$.

§4 Некоторые модификации схем из функциональных элементов. Оценка числа схем в произвольном базисе

Схема Σ, $\Sigma \in \mathcal{U}^{\text{С}}_{\text{Б}}$, с монотонной нумерацией вершин (см. §1), называется *вычисляющей программой (ВП) над базисом* Б (см., например, []). Пусть $\Sigma = \Sigma(x_1, \ldots, x_n; z_1, \ldots, z_m)$, и пусть, для определенности, v_i, $i \in [1, p]$, где $p = |V(\Sigma)|$, — вершина с номером i, причем вершины $v_1, \ldots, v_n$ имеют пометки $x_1, \ldots, x_n$, а вершины $v_{j_1}, \ldots, v_{j_m}$ — пометки $z_1, \ldots, z_m$ соответственно. Сопоставим вершине v_i, $i \in [1, p]$, «внутреннюю» БП u_i и будем считать, что v_i выполняет команду с номером i, которая является:

a) командой ввода $u_i = x_i$, если $i \in [1, n]$;

b) вычисляющей командой $u_i = \varphi^{(i)}\left(u^{(i)}_1, \ldots, u^{(i)}_{k^{(i)}}\right)$, где $\varphi^{(i)}$ — ФС от $k^{(i)}$ БП, приписанный вершине v_i в Σ, а $u^{(i)}_j$, $j = 1, \ldots, k^{(i)}$, — БП, сопоставленная начальной вершине дуги с номером j, входящей в v_i, если $i \in (n, p]$.

Кроме того, будем считать, что каждой вершине v_{j_i}, $i \in [1, m]$, соответствует команда с номером $(p + i)$, являющаяся командой вывода $z_i = u_{j_i}$.

Предполагается, что команды ВП Σ выполняются последовательно в соответствии с их номерами в моменты времени $1, 2, \ldots, p + m$ и что значение БП u_i, вычисленное момент времени i, $i \in [n, p]$, занимает отдельную битовую ячейку памяти на отрезке времени $[i, a_i)$, где a_i — максимальный номер команды, в которой встречается u_i. Максимальное число отрезков вида $[i, a_i)$, где $i \in (n, p]$, имеющих непустое пересечение, называется *шириной* ВП Σ, и определяет минимальное число ячеек памяти, необходимых для ее работы. Заметим, что число ФЭ ВП Σ характеризует время выполнения ее вычисляющих команд на одном процессоре, а максимальная глубина вершин Σ — время выполнения ее вычисляющих команд на параллельных процессорах.

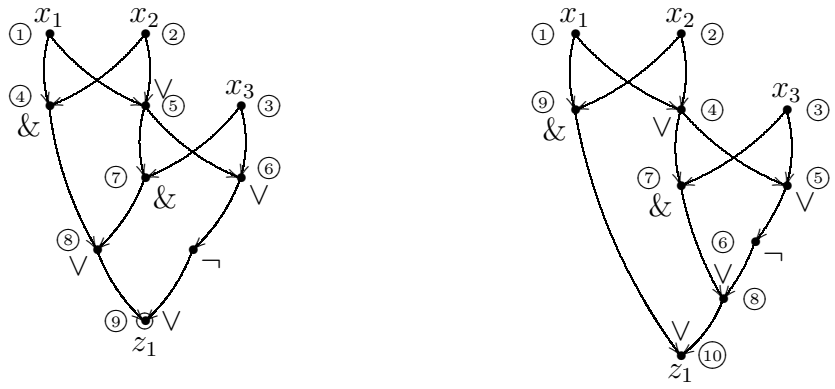


Рис. 4.1: эквивалентные СФЭ ширины 3 и 2

Так, на рис. 4.1a) приведена монотонная нумерация вершин для СФЭ, показанной на рис. 3.1a), которая задает ВП ширины 3, а на рис. 4.1b) — эквивалентная ей ВП ширины 2. Заметим также, что любая ДНФ или КНФ при подходящей монотонной нумерации вершин переходит в ВП ширины 2.

Будем рассматривать формулы и СФЭ с различными ограничениями на соединения ФЭ. Так, для базисов Б, имеющих одновходовые неконстантные ФЭ, введем понятие *усилительной* СФЭ — СФЭ, в которой «ветвятся» выходы только одновходовых ФЭ. Заметим, что указанное ограничение выполняется во многих классах электронных схем, причем в соответствующих базисах имеются специальные «усилительные» ФЭ, реализующие тождественную ФАЛ.

Введем теперь «взвешенные» функционалы сложности и глубины СФЭ. Будем считать, что каждому функциональному элементу $\mathcal{E}_i,\ i = 1, \ldots, b$, сопоставлены положительные действительные числа $\mathcal{L}_i$ и T_i, называемые его «весом» и «задержкой», которые характеризуют сложность («размер») и время срабатывания $\mathcal{E}_i$ соответственно. Предполагается, что «вес» и «задержка» любого ФЭ стандартного базиса $\text{Б}_0 = \{\&, \vee, \neg\}$ равны 1. Если (v_0, v_t)-цепь C длины t в СФЭ Σ проходит через вершины $v_1, \ldots, v_{t-1}$, и вершине $v_j,\ j = 1, \ldots, t$, при этом соответствует ФЭ $\mathcal{E}_{i_j}$ базиса Б, то число $T(C) = T_{i_1} + \cdots + T_{i_t}$ будем называть *задержкой* этой цепи.

По аналогии с глубиной (см. §1) определим *задержку* вершины v СФЭ Σ как максимальную задержку тех цепей Σ, которые начинаются в одной из ее входных вершин и заканчиваются в вершине v. Для каждой СФЭ Σ, $\Sigma \in \mathcal{U}_{\text{Б}}^{\text{C}}$, помимо сложности $L(\Sigma)$, глубины $D(\Sigma)$ и ранга $R(\Sigma)$ определим следующие параметры (функционалы сложности):

1. $\mathcal{L}(\Sigma)$ — *размер* Σ, то есть сумма «весов» всех ее ФЭ;
2. $T(\Sigma)$ — *задержка* Σ, то есть максимальная задержка ее вершин;

Заметим, что функционал L (D) является частным случаем функционала $\mathcal{L}$ (соответственно, T), когда веса (соответственно, задержки) всех ФЭ базиса Б равны 1. Введем также «частичный» размер $\mathcal{L}_{\text{Б}'}(\Sigma)$ (задержку $T_{\text{Б}'}(\Sigma)$), который равен сумме весов ФЭ Σ типа $\mathcal{E}_i$, где $\mathcal{E}_i \in \text{Б}'$, в СФЭ Σ (соответственно, максимальной сумме задержек ФЭ указанного вида, лежащих на одной цепи Σ). Аналогичным образом вводится «частичная» сложность $L_{\text{Б}'}(\Sigma)$ и «частичная» глубина $D_{\text{Б}'}(\Sigma)$ для СФЭ Σ.

Для некоторых типов СФЭ можно рассматривать и другие функционалы сложности. Так, например, для ДНФ мы уже рассматривали их длину, то есть число ЭК, а для СФЭ с монотонной нумерацией вершин — их ширину. С содержательной точки зрения различные меры сложности отражают различные параметры моделируемых схем или программ. Так, например, сложность может характеризовать стоимость, размеры или потребляемую мощность СБИС, а также время выполнения программы на одном процессоре. При этом глубина схемы характеризует время срабатывания СБИС или время выполнения программы на параллельных процессорах, ширина программы — число ячеек памяти, необходимых для хранения ее внутренних БП, и т. д.

Обобщим лемму 2.1 и теорему 3.1 на случай произвольного базиса $\text{Б} = \{\mathcal{E}_i\}_{i=1}^{b}$. Положим $\widehat{\text{Б}} = \{\mathcal{E}_i : k_i \geqslant 2\}$ и заметим, что множество $\widehat{\text{Б}}$ не пусто в силу полноты базиса Б. Для ФЭ $\mathcal{E}_i$, $\mathcal{E}_i \in \widehat{\text{Б}}$, определим его *приведенный вес* ρ_i и *приведенную задержку* τ_i следующим образом:

$$\rho_i = \frac{\mathcal{L}_i}{k_i - 1}, \qquad \tau_i = \frac{T_i}{\log k_i}.$$

Введем, далее, величины

$$\rho_{\text{Б}} = \min_{\mathcal{E}_i \in \widehat{\text{Б}}} \rho_i \quad \text{и} \quad \tau_{\text{Б}} = \min_{\mathcal{E}_i \in \widehat{\text{Б}}} \tau_i,$$

которые назовем *приведенным весом* и *приведенной задержкой базиса* Б соответственно. Для базиса Б_0, очевидно,

$$\widehat{\text{Б}}_0 = \{\&, \vee\}, \quad \rho_{\text{Б}_0} = \tau_{\text{Б}_0} = 1.$$

Для функционала сложности ψ типа L, $\mathcal{L}$, D, T через $\widehat{\psi}(\Sigma)$ будем обозначать величину $\psi_{\widehat{\text{Б}}}(\Sigma)$.

Лемма 4.1. *Для любой формулы $\mathcal{F}$, $\mathcal{F} \in \mathcal{U}_{\text{Б}}^{\Phi}$, выполняются неравенства*

$$R(\mathcal{F}) \leqslant \frac{1}{\rho_{\text{Б}}} \widehat{\mathcal{L}}(\mathcal{F}) + 1, \qquad R(\mathcal{F}) \leqslant 2^{\frac{\widehat{T}(\mathcal{F})}{\tau_{\text{Б}}}}. \tag{4.1}$$

Доказательство. Пусть для каждого i, $i = 1, \ldots, b$, формула $\mathcal{F}$ содержит s_i ФЭ $\mathcal{E}_i$. При этом для числа ребер квазидерева $\mathcal{F}$ будут выполняться равенства

$$|E(\mathcal{F})| = \sum_{i=1}^{b} s_i \cdot k_i = R(\mathcal{F}) + \sum_{i=1}^{b} s_i - 1.$$

Следовательно,

$$R(\mathcal{F}) = \sum_{i=1}^{b} s_i (k_i - 1) + 1 = \sum_{k_i \geqslant 2} \frac{k_i - 1}{\mathcal{L}_i} \cdot \mathcal{L}_i s_i + 1 \leqslant \frac{1}{\rho_{\text{Б}}} \sum_{k_i \geqslant 2} \mathcal{L}_i s_i + 1 = \frac{1}{\rho_{\text{Б}}} \widehat{\mathcal{L}}(\mathcal{F}) + 1$$

и первое неравенство (4.1) доказано.

Второе неравенство (4.1) доказывается индукцией по $D(\mathcal{F})$. Действительно, при $D(\mathcal{F}) = 0$, когда $\mathcal{F} = x_j$ для некоторого $j \in [1, n]$, оно, очевидно, выполняется. Пусть теперь второе неравенство (4.1) верно для любой формулы глубины не больше, чем d, и пусть $\mathcal{F} = \varphi_i(\mathcal{F}_1, \ldots, \mathcal{F}_{k_i})$, где $D(\mathcal{F}) = d$ и $D(\mathcal{F}_j) < d$, $\widehat{T}(\mathcal{F}_j) = t_j$ при всех $j = 1, \ldots, k_i$. Тогда

$$R(\mathcal{F}) = \sum_{j=1}^{k_i} R(\mathcal{F}_j) \leqslant k_i \cdot 2^{\frac{t}{\tau_{\text{Б}}}},$$

где $t = \max_{1 \leqslant j \leqslant k_i} t_j$. Следовательно, при $k_i = 1$ формула $\mathcal{F}$ удовлетворяет второму неравенству (4.1), так как в этом случае $\widehat{T}(\mathcal{F}) = t$. При $k_i \geqslant 2$ в соответствии с определением $\tau_{\text{Б}}$ выполняется неравенство

$$k_i \leqslant 2^{\frac{T_i}{\tau_{\text{Б}}}},$$

используя которое и учитывая, что в данном случае $\widehat{T}(\mathcal{F}) = t + T_i$, получим

$$R(\mathcal{F}) \leqslant k_i \cdot 2^{\frac{t}{\tau_{\text{Б}}}} \leqslant 2^{\frac{t+T_i}{\tau_{\text{Б}}}} = 2^{\frac{\widehat{T}(\mathcal{F})}{\tau_{\text{Б}}}}.$$

Лемма доказана. □

Замечание. Аналогично первому неравенству (4.1) доказывается, что число ребер квазидерева, соответствующего формуле $\mathcal{F}$, в которой нет трех и более последовательно соединенных одновходовых ФЭ, удовлетворяет неравенству

$$|E(\mathcal{F})| \leqslant 6(R(\mathcal{F}) - 1). \tag{4.2}$$

Действительно, если $\mathcal{F}$ содержит s_i ФЭ $\mathcal{E}_i$, $i = 1, \ldots, b$, то

$$R(\mathcal{F}) = \sum_{i=1}^{b} s_i (k_i - 1) + 1 \geqslant \widehat{S}(\mathcal{F}) + 1,$$

$$|E(\mathcal{F})| \leqslant 3\left(R(\mathcal{F}) + \widehat{S}(\mathcal{F}) - 1\right) \leqslant 3(2R(\mathcal{F}) - 2) = 6(R(\mathcal{F}) - 1).$$

Пусть $\mathcal{U}_{\text{Б}}^{\text{С}}\langle\mathcal{L}, n\rangle$ ($\mathcal{U}_{\text{Б}}^{\Phi}\langle\mathcal{L}, n\rangle$, $\mathcal{U}_{\text{Б}}^{\Phi}\{T, n\}$) — множество всех приведенных схем из функциональных элементов $\Sigma(x_1, \ldots, x_n; z_1)$ (соответственно формул $\mathcal{F}(x_1, \ldots, x_n)$) над базисом Б, для которых $\mathcal{L}(\Sigma) \leqslant \mathcal{L}$ (соответственно $\mathcal{L}(\mathcal{F}) \leqslant \mathcal{L}$, $T(\mathcal{F}) \leqslant T$). Следующее утверждение доказывается аналогично теореме 3.1 с использованием (1.4), (4.1), (4.2) и с учетом того, что в любом введенном выше множестве схем $\mathcal{U}$ для любой схемы Σ, $\Sigma \in \mathcal{U}$, найдется эквивалентная схема, в которой нет трех и более последовательно соединенных одновходовых ФЭ.

Теорема 4.1. *Для любых $\mathcal{L} \geqslant 0$, $T \geqslant 0$ и любого натурального n справедливы неравенства*

$$\left\|\mathcal{U}_{\text{Б}}^{\text{С}}\langle L, n\rangle\right\| \leqslant (c(L+n))^{\frac{1}{\rho_{\text{Б}}}L+1}, \tag{4.3}$$

$$\left\|\mathcal{U}_{\text{Б}}^{\Phi}\langle L, n\rangle\right\| \leqslant (cn)^{\frac{1}{\rho_{\text{Б}}}L+1}, \tag{4.4}$$

$$\left\|\mathcal{U}_{\text{Б}}^{\Phi}\{T, n\}\right\| \leqslant (cn)^{2^{\frac{T}{\tau_{\text{Б}}}}}, \tag{4.5}$$

где c — некоторая константа, зависящая от базиса Б.

Замечание. Для любого $\mathcal{L} \geqslant 0$ и любого натурального n выполняется неравенство

$$\left\|\mathcal{U}_{\text{Б}}^{\text{УС}}\langle\mathcal{L}, n\rangle\right\| \leqslant \max_{0\leqslant\widehat{\mathcal{L}}\leqslant\mathcal{L}} \left(c\left(\mathcal{L}-\widehat{\mathcal{L}}+n\right)\right)^{\frac{1}{\rho_{\text{Б}}}\widehat{\mathcal{L}}+1}, \tag{4.6}$$

где $\mathcal{U}_{\text{Б}}^{\text{УС}}\langle\mathcal{L}, n\rangle$ — множество всех усилительных СФЭ из $\mathcal{U}_{\text{Б}}^{\text{С}}\langle\mathcal{L}, n\rangle$, а c — некоторая константа, зависящая от базиса.

Действительно, для любой усилительной СФЭ Σ' существует эквивалентная ей усилительная СФЭ Σ такая, что $\mathcal{L}(\Sigma) \leqslant \mathcal{L}(\Sigma')$, которая является приведенной СФЭ и в которой нет трех и более последовательно соединенных одновходовых ФЭ. Следовательно, для каркаса $\mathcal{F}$ СФЭ Σ указанного вида будут выполняться неравенства (4.1)–(4.2), а число рассматриваемых СФЭ Σ, имеющих один и тот же каркас $\mathcal{F}$, при условии $\mathcal{L}(\Sigma) \leqslant \mathcal{L}$ не больше, чем (ср. с доказательством теоремы 3.1)

$$\left(L(\mathcal{F}) - \widehat{L}(\mathcal{F}) + n\right)^{R(\mathcal{F})} \leqslant c_1\left(\mathcal{L}-\widehat{\mathcal{L}}+n\right)^{\frac{1}{\rho_{\text{Б}}}+1}.$$

Перемножая полученную оценку с оценкой числа каркасов рассматриваемых СФЭ и максимизируя их произведение как функцию параметра $\widehat{\mathcal{L}}$, принимающего значения из действительного отрезка $[0, \mathcal{L}]$, придем к (4.6).

§5 Контактные схемы с одним входом и π-схемы, оценка их числа

Рассмотрим класс контактных схем, в которых реализация ФАЛ осуществляется не с помощью преобразования входных значений в выходные, как это происходит, например, в схемах из функциональных элементов (см. §3), а в результате передачи значений по ребрам графа, проводимостью которого «управляют» входные БП. Ребро или дуга графа с пометкой x_i ($\overline{x}_i$) называется *замыкающим* (соответственно *размыкающим*) контактом БП x_i (см. рис. 5.1).

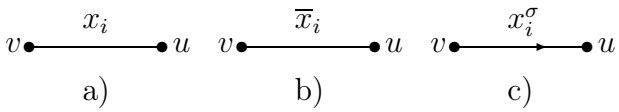


Рис. 5.1: типы контактов

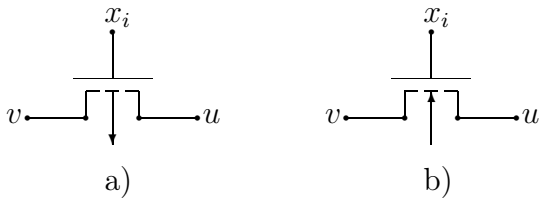


Рис. 5.2: физическая интерпретация контактов

Считается, что контакт вида x_i^σ, $\sigma \in \{0,1\}$, проводит тогда и только тогда, когда $x_i = \sigma$, причем ориентированный контакт, то есть контакт, связанный с дугой, проводит только в соответствующем направлении.

С точки зрения управления проводимостью неориентированный размыкающий (замыкающий) контакт БП x_i функционирует как p-МОП (соответственно n-МОП) транзистор, на затвор которого поступает БП x_i (см. рис. 5.2a и 5.2b), а аналогичный ориентированный контакт — как МОП-транзистор соответствующего типа с диодом Шоттки [4]. Кроме того, ориентированный контакт вида x_i^σ, идущий из вершины v в вершину u (см. рис. 5.1c), часто рассматривают как команду условного перехода из v в u, который выполняется, если $x_i = \sigma$ (см. также §7).

Сеть Σ с входами $a'_1, \ldots, a'_{m'}$ и выходами $a''_1, \ldots, a''_{m''}$, в которой все ребра (дуги) помечены БП $x_1, \ldots, x_n$ или их отрицаниями $\overline{x}_1, \ldots, \overline{x}_n$, называется (m', m'')-*контактной схемой* (КС) *от БП* $x_1, \ldots, x_n$ и обозначается $\Sigma = \Sigma(x_1, \ldots, x_n)$ или $\Sigma = \Sigma(x_1, \ldots, x_n; a'_1, \ldots, a'_{m'}; a''_1, \ldots, a''_{m''})$. При этом число контактов называется *сложностью* КС Σ и обозначается через $L(\Sigma)$. На рис. 5.3a–c показаны некоторые конкретные КС от БП x_1, x_2, x_3 с входом a_1 и выходами a_2, a_3.

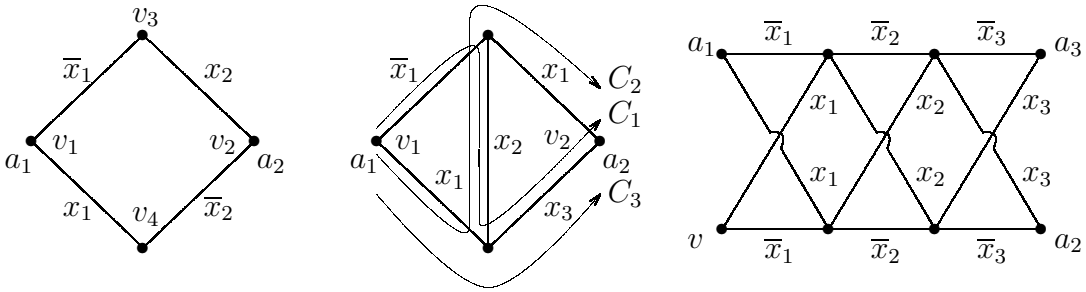


Рис. 5.3: некоторые КС от БП x_1, x_2, x_3

Пусть $\Sigma = \Sigma(x_1, \ldots, x_n)$ — КС от БП $X(n)$. Определим $\Sigma(\alpha)$ как сеть, получающуюся из Σ в результате удаления всех ребер (дуг) с пометками $x_1^{\overline{\alpha}_1}, \ldots, x_n^{\overline{\alpha}_n}$, то есть ребер, которые не проводят на наборе α, и снятия пометок с остальных ребер Σ. Для вершин v и u КС Σ введем *функцию проводимости от вершины v к вершине u* как ФАЛ $g_{v,u}(x_1, \ldots, x_n)$, которая равна 1 на наборе $\alpha = (\alpha_1, \ldots, \alpha_n) \in B^n$ тогда и только тогда, когда в сети $\Sigma(\alpha)$ существует $(v-u)$-цепь, то есть тогда и только тогда, когда в Σ имеется цепь из проводящих на наборе α контактов вида $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$, идущая из v в u. Будем говорить также, что ФАЛ $g_{v,u}$ является *функцией достижимости вершины u из вершины v* или, иначе, *реализуется* между вершинами v и u. Из определения следует, что для нахождения ФАЛ $g_{v,u}(x_1, \ldots, x_n)$ достаточно просмотреть все наборы α, $\alpha \in B^n$, и для каждого из них выяснить наличие или отсутствие в Σ цепи, состоящей из проводящих на наборе α контактов, которая идет из v в u. Так, просматривая все наборы значений БП x_1, x_2, можно убедиться в том, что ФАЛ проводимости $g_{v_1,v_2}(x_1, x_2)$ в КС Σ, показанной на рис. 5.3a, равна $x_1 \oplus x_2$, а ФАЛ проводимости g_{v_3,v_4} равна 0.

Будем считать, что в каждой вершине $(1,m)$-КС $\Sigma(x_1, \ldots, x_n; a'; a_1, \ldots, a_m)$ реализуется ФАЛ проводимости от входа a' к этой вершине и что Σ реализует систему ФАЛ $F = (f_1, \ldots, f_m)$, где f_j — ФАЛ проводимости от a' к выходу с пометкой a_j, $j \in [1,m]$. Так, КС, изображенные на рис. 5.3a, 5.3b и 5.3c, реализуют ФАЛ $x_1 \oplus x_2$, $H(x_1, x_2, x_3)$ и набор ФАЛ $(x_1 \oplus x_2 \oplus x_3,\ x_1 \oplus x_2 \oplus x_3 \oplus 1)$ соответственно. На рис. 5.4 показана $(1, 2^n)$-КС $\mathcal{D}(x_1, \ldots, x_n; a'; a_0, \ldots, a_{2^n-1})$, которая называется *контактным деревом порядка n* от БП $X(n)$. Легко видеть, что между входом и выходной вершиной a_i, $i = 0, \ldots, 2^n - 1$, контактного дерева (КД) порядка n от БП $X(n)$ реализуется ЭК вида $x_1^{\sigma_1} \cdots x_n^{\sigma_n}$, где $\nu(\sigma_1, \ldots, \sigma_n) = (i-1)$, и что ФАЛ проводимости между любыми его выходами равна 0. Таким образом, КД порядка n является дешифратором порядка n, то есть схемой, реализующей систему Q_n из всех ЭК ранга n от БП $X(n)$.

Схемы Σ' и Σ'' считаются, как обычно, *изоморфными*, если изоморфны соответствующие им графы, и *эквивалентными*, если они реализуют равные системы ФАЛ. Изоморфные КС, очевидно, эквивалентны.

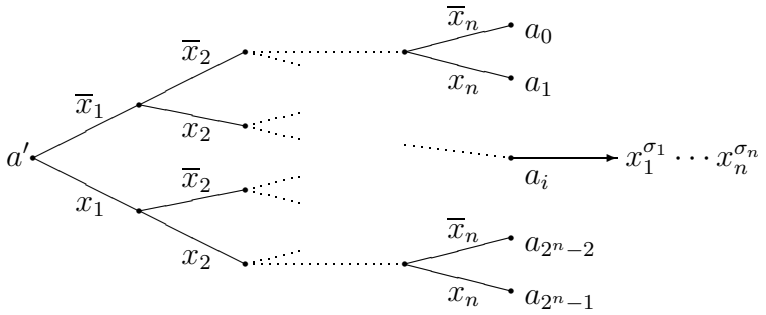


Рис. 5.4: контактное дерево

Для множества C, состоящего из контактов вида $x_{i_1}^{\sigma_1}, \ldots, x_{i_r}^{\sigma_r}$ в КС Σ, определим его *функцию проводимости* $K(C)$ и *функцию отделимости* $J(C)$ как ФАЛ вида $x_{i_1}^{\sigma_1} \cdots x_{i_r}^{\sigma_r}$ и $x_{i_1}^{\overline{\sigma}_1} \vee \ldots \vee x_{i_r}^{\overline{\sigma}_r}$ соответственно. При этом множество C называется *проводящим* (*отделимым*), если $K(C) \neq 0$ ($J(C) \neq 1$), и *нулевым* (соответственно, *единичным*) в противном случае. Заметим, что в результате приведения подобных (см. §3 гл. 1) отличная от 0 ФАЛ $K(C)$ и отличная от 1 ФАЛ $J(C)$ могут быть преобразованы в ЭК и ЭД соответственно. Очевидно, также, что

$$K(C') \geqslant K(C) \quad \text{и} \quad J(C') \leqslant J(C),$$

если $C' \subseteq C$.

Множество S, которое состоит из ребер графа $G = (V, E)$ и обладает тем свойством, что вершина u, $u \in V$, достижима из вершины v, $v \in V$, в графе G, но не достижима из нее в графе $(V, E \setminus S)$, называется $(u|v)$-*сечением* графа G. Легко видеть, что любая $(u - v)$-цепь графа G имеет хотя бы одно общее ребро с любым $(u|v)$-сечением этого графа. Сечение, которое не имеет собственных подмножеств, являющихся сечением, называется *тупиковым*.

Из введенных определений (см. также §1) следует, что ФАЛ g, реализуемая КС $\Sigma(x_1, \ldots, x_n; a_1; a_2)$, обращается в 1 (обращается в 0) на наборе α, $\alpha \in B^n$, тогда и только тогда, когда в Σ существует множество контактов C, образующее простую проводящую $(a_1 - a_2)$-цепь (соответственно, тупиковое отделимое $(a_1|a_2)$)-сечение), для которого $K(C) = 1$ (соответственно, $J(C) = 0$) на наборе α. Таким образом,

$$g(x_1, \ldots, x_n) = K(C_1) \vee \ldots \vee K(C_t) = J(S_1) \,\&\, \ldots \,\&\, J(S_p), \tag{5.1}$$

где $C_1, \ldots, C_t$ и $S_1, \ldots, S_p$ — все простые проводящие $(a_1 - a_2)$-цепи и все тупиковые отделимые $(a_1|a_2)$-сечения КС Σ.

Заметим, что первая из формул (5.1) может быть преобразована в ДНФ, а вторая — в КНФ, в результате приведения подобных (см. §3 главы 1), если $g \not\equiv 0$ и $g \not\equiv 1$ соответственно. Так, в КС, показанной на рис. 5.3b, имеются три простые

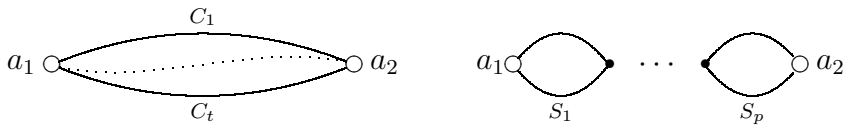


Рис. 5.5: КС, моделирующая ДНФ и КНФ

проводящие цепи C_1, C_2 и C_3, которые идут из a_1 в a_2. При этом

$$K(C_1) = \overline{x}_1 x_2 x_3, \quad K(C_2) = x_1 x_2 x_1 = x_1 x_2, \quad K(C_3) = x_1 x_3$$

и, следовательно,

$$g(x_1, x_2, x_3) = \overline{x}_1 x_2 x_3 \vee x_1 x_2 \vee x_1 x_3 = x_1 x_2 \vee x_2 x_3 \vee x_3 x_1 = H(x_1, x_2, x_3).$$

Первое соотношение (5.1) можно использовать для построения$(1,1)$-КС Σ', в которой ФАЛ проводимости от входа a_1 к выходу a_2 описывается заданной ДНФ вида

$$\mathfrak{A} = K_1 \vee \ldots \vee K_t,$$

где $K_1, \ldots, K_t$ — различные ЭК, и которая «моделирует» ДНФ $\mathfrak{A}$. Указанная контактная схема Σ' получается в результате проведения из a_1 в a_2 цепей $C_1, \ldots, C_t$ без общих контактов и внутренних вершин так, что $K(C_i) = K_i,\ i = 1, \ldots, t$ (см. рис. 5.5a). Заметим, что при этом $L(\Sigma') = R(\mathfrak{A})$. Схема, моделирующая совершенную ДНФ ФАЛ f, называется *канонической* КС для этой ФАЛ.

Аналогичным образом на основе второго соотношения (5.1) строится $(1,1)$-КС Σ'', которая «моделирует» КНФ

$$\mathfrak{B} = J_1 \& \ldots \& J_p$$

и для которой по-прежнему $L(\Sigma'') = R(\mathfrak{B})$. Эта КС с входом a_1 и выходом a_2 получается (см. рис. 5.5b) в результате последовательного соединения КС $S_1, \ldots, S_p$, где КС $S_j,\ j = 1, \ldots, p$, реализует ЭД J_j и состоит из параллельно соединенных контактов, соответствующих буквам ЭД J_j.

Схемы, моделирующие ДНФ или КНФ, являются частным случаем т. н. параллельно-последовательных КС или, иначе, π-схем.

Простейшей π-схемой считается любая $(1,1)$-КС, которая состоит из одного контакта, соединяющего полюса (см. рис. 5.6a). Если π-схемы Σ_1 и Σ_2 уже определены, то $(1,1)$-КС Σ' (Σ''), которая получается в результате их параллельного (соответственно последовательного) соединения (см. рис. 5.6b и 5.6c) тоже является π-схемой. Заметим, что при этом вход (выход) Σ' является результатом отождествления входов (соответственно выходов) Σ_1 и Σ_2, тогда как входом Σ'' является вход Σ_1, выходом

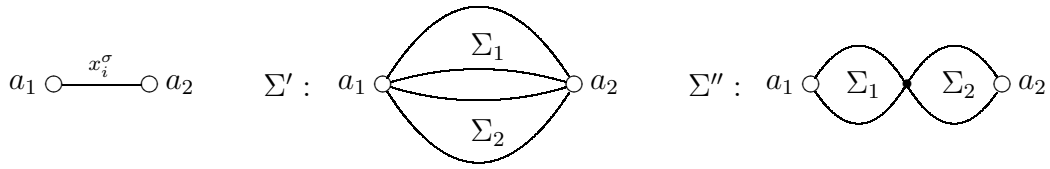


Рис. 5.6: к определению π-схемы

Σ'' — выход Σ_2 отождествляется с входом Σ_2 и становится внутренней вершиной Σ''. Легко видеть, что π-схема, показанная на рис. 5.6a, реализует ФАЛ x_i^σ, а π-схемы Σ' и Σ'' (см. рис. 5.6b и 5.6c) — ФАЛ $f_1 \vee f_2$ и $f_1 \& f_2$ соответственно, где f_1 и f_2 — ФАЛ, реализуемые π-схемами Σ_1 и Σ_2 соответственно.

Лемма 5.1. *Любой π-схеме Σ можно сопоставить эквивалентную ей формулу F из $\mathfrak{U}^\Phi$ с поднятыми отрицаниями такую, что $R(F) = L(\Sigma)$ и обратно.*

Доказательство. Построим формулу F индукцией по строению π-схемы Σ. Если Σ — простейшая π-схема вида x_i^σ, то положим $F = x_i^\sigma$. Если π-схемам Σ_1 и Σ_2 уже сопоставлены формулы F_1 и F_2 с поднятыми отрицаниями, то π-схеме Σ' (Σ''), получающейся в результате параллельного (соответственно последовательного) соединения Σ_1 и Σ_2 сопоставим формулу $F' = F_1 \vee F_2$ (соответственно $F'' = F_1 \& F_2$). При этом

$$R(F') = R(F'') = R(F_1) + R(F_2)$$

и, следовательно, по индуктивному предположению,

$$R(F') = R(F'') = L(\Sigma_1) + L(\Sigma_2) = L(\Sigma).$$

Аналогичным образом, индукцией по строению формулы F с поднятыми отрицаниями можно сопоставить ей эквивалентную π-схему Σ такую, что $L(\Sigma) = R(F)$.

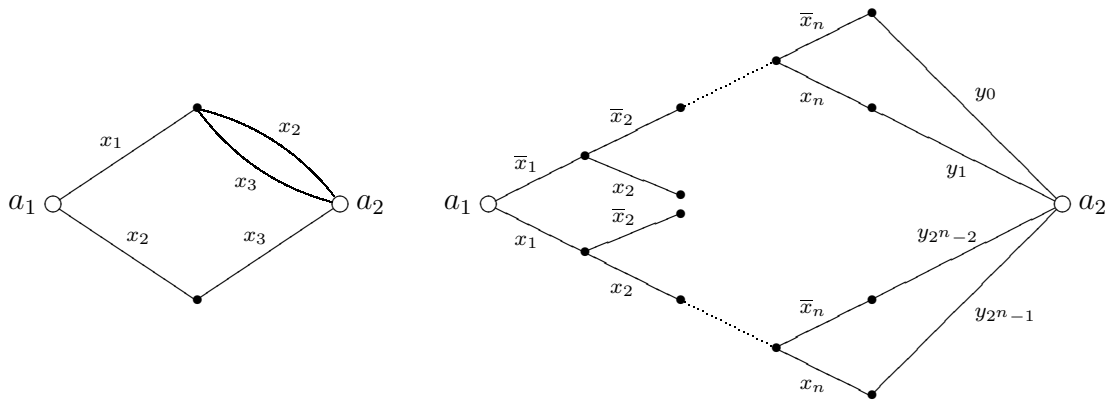
Лемма доказана. □

На рис 5.7a показана π-схема, которая реализует ФАЛ $H(x_1, x_2, x_3)$ и соответствует формуле:

$$H(x_1, x_2, x_3) = x_1(x_2 \vee x_3) \vee x_2 x_3,$$

а на рис. 5.7b — π-схема, которая построена на основе контактного дерева и реализует ФАЛ μ_n — мультиплексорную ФАЛ порядка n, — в соответствии с формулой

$$\mu_n(x_1, \ldots, x_n, y_0, \ldots, y_{2^n-1}) = \bigvee_{\sigma_1 \in B} x_1^{\sigma_1} \left(\bigvee_{\sigma_2 \in B} x_2^{\sigma_2} \left(\cdots \left(\bigvee_{\sigma_n \in B} x_n^{\sigma_n} y_{\nu(\sigma_1, \ldots, \sigma_n)} \right) \cdots \right) \right).$$



a) b)

Рис. 5.7: примеры π-схем

Будем называть $(1, m)$-КС *приведенной*, если все изолированные вершины Σ являются ее полюсами, а все контакты и остальные вершины Σ принадлежат простым проводящим цепям, соединяющим ее вход и выходы. При этом КС $\widehat{\Sigma}$, которая получается из КС Σ удалением «лишних», то есть не принадлежащих цепям указанного вида, неполюсных вершин и контактов, является эквивалентной Σ приведенной КС такой, что $L(\widehat{\Sigma}) \leqslant L(\Sigma)$. Заметим, что приведенная КС не содержит петель, а приведенная КС, не реализующая нулевых ФАЛ, является связным графом. Так, КС, показанная на рис. 5.3c, не является приведенной, а соответствующая ей приведенная КС получается из нее удалением вершины v.

Рассмотрим, в заключение, некоторые оценки числа контактных схем различных типов. Пусть $\mathcal{U}^{\mathrm{K}}$, $\mathcal{U}^{\overrightarrow{\mathrm{K}}}$ и $\mathcal{U}^{\pi}$ — множество всех КС из неориентированных контактов, множество всех КС из ориентированных контактов и множество всех π-схем соответственно. Если $\mathcal{U}^{\mathrm{A}}$ — один из указанных классов схем, то через $\mathcal{U}^{\mathrm{A}}(L, n)$ будем обозначать множество приведенных $(1, 1)$-КС Σ из $\mathcal{U}^{\mathrm{A}}$ от БП $X(n)$, для которых $L(\Sigma) \leqslant L$. Для любого множества схем $\mathcal{U}$ в соответствии с §1 через $|\mathcal{U}|$ и $\|\mathcal{U}\|$ будем по-прежнему обозначать число попарно не изоморфных и попарно не эквивалентных схем в $\mathcal{U}$ соответственно. При этом для любого из введенных выше множеств схем неравенство (1.5) будет выполняться.

Из леммы 5.1 в силу следствия из теоремы 3.1 вытекает справедливость следующего утверждения.

Лемма 5.2. *При любых натуральных L и n выполняется неравенство*

$$\|\mathcal{U}^{\pi}(L, n)\| \leqslant (64n)^{L}.$$

Лемма 5.3. *При любых натуральных L и n выполняются неравенства*

$$\left\|\mathfrak{U}^{\mathrm{K}}(L,n)\right\| \leqslant (8nL)^L, \qquad \left\|\mathfrak{U}^{\overrightarrow{\mathrm{K}}}(L,n)\right\| \leqslant (6nL)^L.$$

Доказательство. Возьмем произвольную КС $\Sigma = \Sigma(x_1,\ldots,x_n;a_1,a_2)$, $\Sigma \in \mathfrak{U}^{\mathrm{K}}(L,n)$ и выделим в ней остовное дерево $\mathcal{D}$ с корнем a_2 так, чтобы вершина a_1 была листом $\mathcal{D}$. Пусть, далее, $\mathcal{D}'$ — связанное с $\mathcal{D}$ остовное наддерево КС Σ, которое получается путем присоединения каждого из не вошедших в $\mathcal{D}$ ребер Σ к одной из своих концевых вершин, отличной от a_1 (см. §1). Рассмотрим ориентированное упорядоченное дерево $\mathcal{D}''$, получающееся из $\mathcal{D}'$ введением (условной) ориентации всех его ребер по направлению к корню и таким их упорядочением, при котором вершина a_1 становится первым листом $\mathcal{D}''$ (см. §1).

Заметим, что число ребер (вершин, листьев) дерева $\mathcal{D}''$ не больше, чем L (соответственно $L+1$, L), и поэтому в силу (1.4) число таких деревьев с учетом пометок их ребер символами $x_1,\ldots,x_n,\overline{x}_1,\ldots,\overline{x}_n$ не больше, чем $(8n)^L$. Заметим также, что КС Σ может быть получена в результате присоединения каждого листа дерева $\mathcal{D}''$ к одной из его вершин, отличной от a_2. Следовательно,

$$\left\|\mathfrak{U}^{\mathrm{K}}(L,n)\right\| \leqslant \left|\mathfrak{U}^{\mathrm{K}}(L,n)\right| \leqslant (8nL)^L.$$

Второе неравенство леммы устанавливается аналогично.

Лемма доказана. □

§6 Многополюсные контактные схемы и их суперпозиции. Разделительные схемы, лемма Шеннона

Рассмотрим сначала особенности функционирования КС с несколькими входами.

Для произвольных выборок $V' = \left(v'_1,\ldots,v'_p\right)$ и $V'' = \left(v''_1,\ldots,v''_q\right)$ из множества $V(G)$ графа G определим *матрицу достижимости выборки V' из выборки V''* как матрицу M, $M \in B^{p,q}$, для которой

$$M\langle i,j\rangle = \begin{cases} 1, & \text{если } v''_j \text{ достижима из } v'_i, \\ 0, & \text{в остальных случаях.} \end{cases}$$

Заметим, что в случае $V' = V''$ матрица M является рефлексивной и транзитивной[1],

[1]Матрица M, $M \in B^{m,m}$, считается рефлексивной (транзитивной) тогда и только тогда, когда она задает рефлексивное (соответственно транзитивное) отношение на множестве $[1,m]$, то есть

$$M\langle i,i\rangle = 1 \quad (\text{соответственно } M\langle i,t\rangle \cdot M\langle t,j\rangle \geqslant M\langle i,j\rangle)$$

для любого i (соответственно любых i,j и t) из отрезка $[1,m]$.

а если, кроме того, G — неориентированный граф, то и симметричной матрицей. Заметим также, что транзитивность рефлексивной матрицы M, $M \in B^{m,m}$, имеет место тогда и только тогда, когда[2]

$$M^2 = M. \tag{6.1}$$

Действительно, полагая $\widehat{M} = M^2$, получим

$$\widehat{M}\langle i,j\rangle = \bigvee_{t=1}^{m} M\langle i,t\rangle \cdot M\langle t,j\rangle \tag{6.2}$$

и, следовательно, в случае $\widehat{M} = M$ неравенства транзитивности

$$\widehat{M}\langle i,j\rangle = M\langle i,j\rangle \geqslant M\langle i,t\rangle \cdot M\langle t,j\rangle$$

будут выполнены при любых i, j, t из отрезка $[1, m]$. С другой стороны, из транзитивности рефлексивной матрицы M в силу (6.2) следует, что

$$\widehat{M}\langle i,j\rangle = M\langle i,j\rangle \vee \left(\bigvee_{\substack{1\leqslant t\leqslant m \\ t\neq i,j}} M\langle i,j\rangle \cdot M\langle t,j\rangle \right) = M\langle i,j\rangle .$$

Матрица достижимости выходной выборки сети из ее входной выборки называется *матрицей достижимости* этой сети.

Определим функционирование КС $\Sigma = \Sigma(x_1,\ldots,x_n; a'_1,\ldots,a'_{m'}; a''_1,\ldots,a''_{m''})$ как матрицу $F = F(x_1,\ldots,x_n)$ с m' строками, m'' столбцами и элементами из $P_2(n)$, для которой $F\langle i,j\rangle$ — ФАЛ, реализуемая между a'_i и a''_j, где $i \in [1, m']$ и $j \in [1, m'']$. Заметим, что при любом α, $\alpha \in B^n$, матрица $F(\alpha)$ является матрицей достижимости сети $\Sigma(\alpha)$. В соответствии с общими правилами из §1 функционирование КС $\Sigma = \Sigma(x_1,\ldots,x_n; a_1,\ldots,a_m)$ с неразделенными полюсами определяется как функционирование КС с разделенными полюсами вида $\Sigma(x_1,\ldots,x_n; a_1,\ldots,a_m; a_1,\ldots,a_m)$. В этом случае матрица F является рефлексивной и транзитивной матрицей, а если, кроме того, Σ — неориентированная сеть, то и — симметричной матрицей.

Так, КС $\Sigma(x_1,x_2,x_3; a_1,v; a_2,a_3)$, показанная на рисунке 5.3с реализует матрицу $\begin{bmatrix} l_3 & \bar{l}_3 \\ \bar{l}_3 & l_3 \end{bmatrix}$ от БП $X(3)$, а соответствующая ей КС с неразделенными полюсами a_1, a_2, a_3 — матрицу $\begin{bmatrix} 1 & l_3 & \bar{l}_3 \\ l_3 & 1 & 0 \\ \bar{l}_3 & 0 & 1 \end{bmatrix}$.

Заметим также, что функционирование $(1,1)$-КС из неориентированных контактов по существу не отличается от функционирования соответствующей двухполюсной КС с неразделенными полюсами, функционирование $(1, m'')$-КС представляет

[2]Считаем, что при умножении матриц из 0 и 1 вместо операции сложения используется операция дизъюнкции.

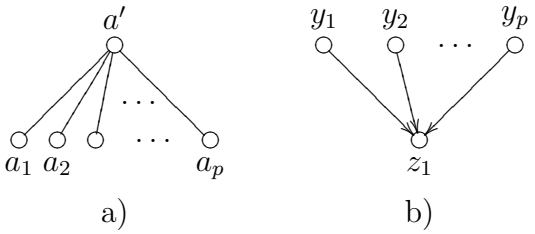


Рис. 6.1: проводящая и вентильная звезды порядка p

собой набор (строку) из m'' ФАЛ проводимости от ее входа к выходам, а функционирование $(m', 1)$-КС — столбец из m' ФАЛ проводимости от ее входов к выходу.

В дальнейшем будем считать, что в каждой вершине (p, q)-КС Σ реализуется столбец, составленный из p ФАЛ проводимости от входов Σ к этой вершине, и, следовательно, матрица, реализуемая КС Σ, состоит из q столбцов, реализуемых на ее выходах.

Рассмотрим теперь вопросы, связанные с нахождением матриц достижимости для суперпозиции сетей или КС. Из соображений удобства будем допускать наличие в КС неориентированных (ориентированных) ребер без пометок, которые проводят при любых значениях управляющих входных БП и называются *проводниками* (соответственно *вентилями*). Это позволяет считать, что сети являются частным случаем КС и реализуют свои матрицы достижимости, состоящие из константных ФАЛ.

Операция суперпозиции КС Σ'' и Σ', результатом которой является КС вида $\Sigma = \Sigma''(\Sigma')$, определяется аналогично тому, как это делалось для СФЭ (см. §3), с той лишь разницей, что пометками входов и выходов не обязательно являются переменные. Дополняя введенные в §3 специальные виды суперпозиции, определим *стыковку* схем Σ'' и Σ', как их суперпозицию вида $\Sigma''(\Sigma')$, при которой все входы Σ'' присоединяются к различным выходным вершинам Σ'. Стыковка вида $\Sigma''(\Sigma')$ называется *полной*, если в ней участвуют все выходы схемы Σ', и каждый вход схемы Σ'' присоединяется к выходу схемы Σ' с тем же номером.

Заметим (ср. с §3), что (однократная) операция суперпозиции общего вида $\Sigma = \Sigma''(\Sigma')$ всегда может быть сведена к последовательному выполнению операций переименования входов Σ'', переименования выходов Σ', объединения каждой из полученных схем с некоторой схемой, состоящей из изолированных вершин, и полной стыковки объединенных схем. Заметим также, что результат отождествления p каких-либо входов у КС Σ эквивалентен результату стыковки вида $\Sigma(\Sigma')$, при которой эти входы присоединяются к выходам $(1, p)$-проводящей звезды $\Sigma' = \Sigma'(a'; a_1, \ldots, a_p)$ — схемы, состоящей из p проводников, соединяющих ее вход со всеми выходами (см. рис. 6.1a).

Схема называется *разделительной по входам(выходам)*, если ФАЛ проводимости между любыми ее различными входами (соответственно выходами) равна 0.

Так $(p,1)$-схема $\Sigma'' = \Sigma''(y_1,\ldots,y_p;z_1)$, показанная на рисунке 6.1b, является разделительной по входам схемой, которая называется *вентильной звездой порядка* p. Примером разделительной по выходам КС может служить $(1,2^n)$-контактное дерево порядка n (см. рис. 5.4). Будем говорить, что КС Σ от БП $x_1,\ldots,x_n$ *разделительна на наборе* $\alpha=(\alpha_1,\ldots,\alpha_n)$ значений этих БП, если соответствующей разделительностью обладает сеть $\Sigma(\alpha)$.

Лемма 6.1. *Пусть КС Σ вида $\Sigma=\Sigma''(\Sigma')$ является результатом полной стыковки (p,q)-КС Σ' и (q,s)-КС Σ'' от БП $x_1,\ldots,x_n$. Пусть, кроме того, v' (v'') — произвольная вершина КС Σ' (соответственно Σ''), а ФАЛ f'_j (соответственно f''_j), $j\in[1,q]$, — ФАЛ проводимости от вершины v' к j-му выходу в КС Σ' (соответственно от j-го входа к вершине v'' в КС Σ''). Тогда для ФАЛ f – ФАЛ проводимости от вершины v' к вершине v'' в КС Σ, – справедливо неравенство*

$$f(x_1,\ldots,x_n)\geqslant f'_1\cdot f''_1\vee\cdots\vee f'_q\cdot f''_q, \tag{6.3}$$

которое переходит в равенство

$$f(x_1,\ldots,x_n)= f'_1\cdot f''_1\vee\cdots\vee f'_q\cdot f''_q, \tag{6.4}$$

если КС Σ' разделительна по выходам или КС Σ'' разделительна по входам.

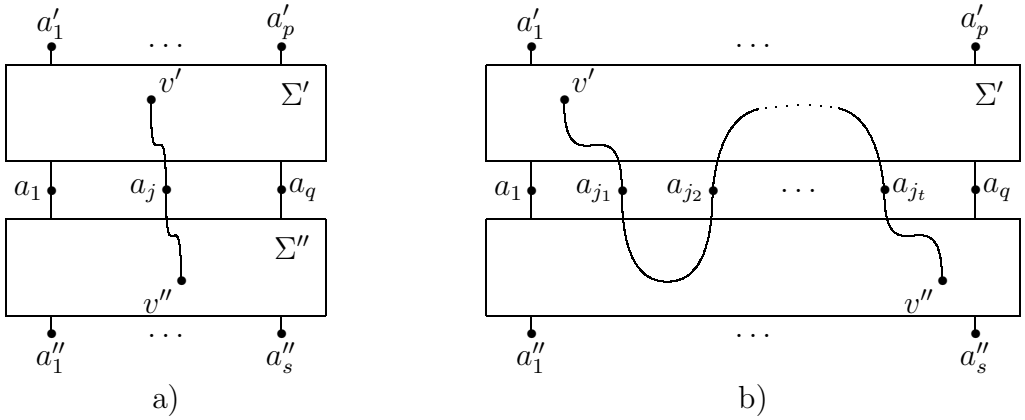


Рис. 6.2: к доказательству леммы 6.1

Доказательство. Пусть a_j, $j\in[1,q]$, – вершина КС Σ, которая получается в результате присоединения j-го входа КС Σ'' к j-му выходу КС Σ' (см. рис. 6.2a). Справедливость неравенства (6.3) следует из того, что его правая часть задает ту часть ФАЛ проводимости от v' к v'' в КС Σ, которая задается проводимостями $(v'-v'')$-цепей КС Σ, проходящих через вершины $a_1,\ldots,a_q$ ровно один раз (см. рис. 6.2a). Любая другая $(v'-v'')$-цепь КС Σ проходит через указанные вершины t, $t\geqslant 2$, раз (см. рис. 6.2b) и в случае разделительности КС Σ' по выходам или разделительности КС Σ'' по входам имеет нулевую проводимость.

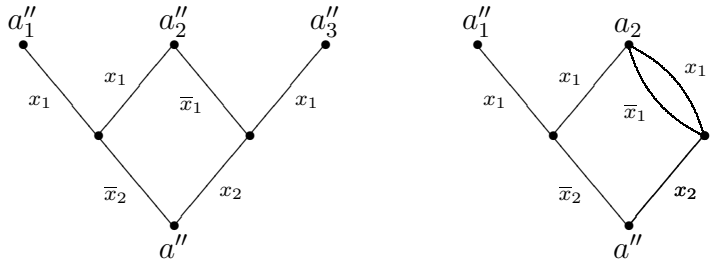
Лемма доказана. □

Следствие 1. *В условиях леммы для матриц F, F' и F'', реализуемых КС Σ, Σ' и Σ'' соответственно, справедливо неравенство $F \geqslant F' \cdot F''$, которое переходит в равенство, если КС Σ' разделительна по выходам или КС Σ'' разделительна по входам.*

Следствие 2. *При отождествлении входов разделительная по входам КС Σ'' переходит в разделительную по входам КС Σ, которая реализует матрицу, получающуюся из матрицы КС Σ'' в результате поразрядной дизъюнкции строк, соответствующих отождествляемым выходам.*

Действительно, схема Σ эквивалентна некоторой схеме являющейся результатом полной стыковки вида $\Sigma''(\Sigma)'$, где схема Σ' состоит из изолированных входов-выходов и проводящей звезды (см. рис. 6.1а), и в силу следствия 1 реализует указанную матрицу ФАЛ. При этом разделительность КС Σ вытекает из аналогичных соображений связанных с КС $\widehat{\Sigma}$, которая получается из КС Σ в результате объявления входов КС Σ входами и, одновременно, выходами КС $\widehat{\Sigma}$.

Замечание. Равенство (6.4) и матричное равенство из следствия 1 выполняются на наборе $\alpha = (\alpha_1, \ldots, \alpha_n)$ значений БП $x_1, \ldots, x_n$, если КС Σ' разделительна по выходам на наборе α или КС Σ'' разделительна по входам на этом наборе.



a) b)

Рис. 6.3: отождествление входов у $(3,1)$-КС Σ''

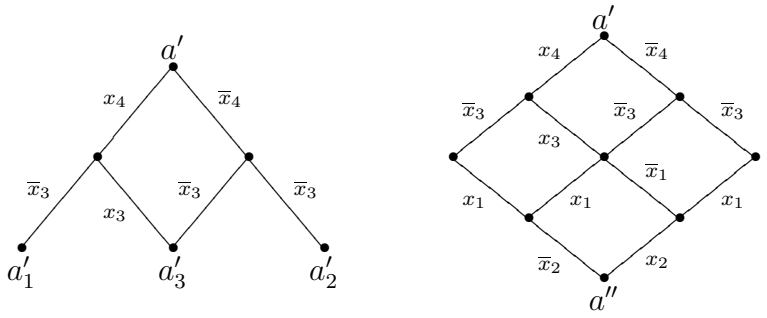
Из леммы 6.1 и следствия 2 из нее вытекает, что неравенства типа (6.3) будут выполняться для любой суперпозиции общего вида $\Sigma = \Sigma''(\Sigma')$, а равенства типа (6.4) — для суперпозиции вида $\Sigma = \Sigma''(\Sigma')$ с разделительной по входам КС Σ''. Суперпозиция вида $\Sigma = \Sigma''(\Sigma')$ называется *корректной*, если связанные с ней равенства типа (6.4) выполняются для любой входной вершины v' КС Σ' и любой выходной вершины v'' КС Σ''. В силу вышесказанного, суперпозиция $\Sigma = \Sigma''(\Sigma')$ является корректной, если КС Σ'' разделительна по входам. Аналогичным образом определяется понятие корректности суперпозиции $\Sigma = \Sigma''(\Sigma')$ на наборе $\alpha = (\alpha_1, \ldots, \alpha_n)$ значений входных БП $x_1, \ldots, x_n$, которая вытекает из разделительности КС Σ'' по входам на наборе α.

Заметим, что операции переименования входов без отождествления, переименования выходов и объединения корректны в любом случае. В то же время операции отождествления входов, а также операции стыковки не всегда являются корректными. Так на рис. 6.3a изображена $(3,1)$-КС $\Sigma''(x_1,x_2;a_1'',a_2'',a_3'';a'')$, которая реализует столбец f'' из ФАЛ

$$f_1''=x_1\overline{x}_2,\ f_2''=x_1\oplus x_2 \text{ и } f_3''=x_1x_2,$$

а на рисунке 6.3b — $(2,1)$-КС $\widehat{\Sigma}''(x_1,x_2;a_1'',a_2;a'')$, которая получается из Σ'' в результате отождествления входов $a_2''=a_3''=a_2$ и реализует столбец $\widehat{f}''$ из ФАЛ

$$\widehat{f}_1''=x_1\neq f_1'',\ \widehat{f}_2''=x_1\vee x_2.$$



a) b)

Рис. 6.4: $(1,3)$-КС Σ' и $\Sigma=\Sigma''(\Sigma')$

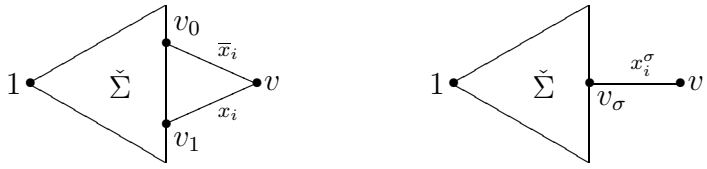
На рис. 6.4a показана $(1,3)$-КС $\Sigma'(x_3,x_4;a';a_1',a_2',a_3')$, которая реализует набор f' из ФАЛ

$$f_1'=\overline{x}_3x_4,\ f_2'=x_3\sim x_3,\ f_3'=\overline{x}_3\overline{x}_4,$$

а на рис. 6.4b — $(1,1)$-КС $\Sigma(x_1,x_2,x_3,x_4;a';a'')$, которая является результатом полной стыковки вида $\Sigma''(\Sigma)'$ и реализует ФАЛ $f(x_1,x_2,x_3,x_4)$ такую, что

$$f(x_1,x_2,x_3,x_4)=\overline{x}_3x_4x_1\vee(x_3\sim x_4)\cdot(x_1\oplus x_2)\vee\overline{x}_3\overline{x}_4x_1x_2\neq f_1'\cdot f_1''\vee f_2'\cdot f_2''\vee f_3'\cdot f_3''$$

Примером корректной суперпозиции является операция присоединения одного или двух противоположных контактов, которая лежит в основе метода каскадов (см. §2 гл. 3) и заключается в следующем. Пусть $(1,m)$-КС Σ получается из $(1,\check{m})$-КС $\check{\Sigma}$ в результате добавления новой выходной вершины v, которая соединяется с выходными вершинами v_0 и v_1 КС $\check{\Sigma}$ контактами $\overline{x}_i$ и x_i соответственно (см. рис. 6.5a).



a) b)

Рис. 6.5: присоединение одного или двух противоположных контактов

Тогда в вершинах v_0 и v_1 КС Σ в силу разделительности по входам присоединяемой $(2,1)$-КС реализуются те же самые ФАЛ g_0 и g_1, что и в КС $\check{\Sigma}$, а в вершине v — ФАЛ g вида

$$g = \mu\left(x_i, g_0, g_1\right) = \overline{x}_i g_0 \vee x_i g_1. \tag{6.5}$$

Аналогичные соотношения будут справедливы и тогда, когда вершина v КС Σ связана с КС $\check{\Sigma}$ только одним контактом вида $x_i^\sigma,\ \sigma \in \{0,1\}$, соединяющим ее с вершиной v_σ (см. рис. 6.5b). В этом случае в вершине v КС Σ реализуется ФАЛ

$$g = x_i^\sigma g_\sigma. \tag{6.6}$$

Естественным обобщением операции присоединения двух противоположных контактов является операция суперпозиции вида $\Sigma = \Sigma''(\Sigma')$, где Σ' — $(1,m)$-КС, а Σ'' — $(2^n,1)$-КД от БП $X(n)$, показанное на рис. 7.3a, которая лежит в основе метода Шеннона (см. §2 гл. 3). При этом в силу разделительности КС Σ'' по входам указанная суперпозиция является корректной и в выходной вершине Σ, соответствующей выходу, то есть корню, КД Σ'', реализуется ФАЛ вида

$$f = \mu_n(x_1, \ldots, x_n, g_0, g_1, \ldots, g_{2^n-1}), \tag{6.7}$$

где g_i — ФАЛ, реализуемая на том выходе Σ', к которому присоединяется i-й вход (лист) Σ'', $i \in [0, 2^n)$.

§7 Некоторые модификации и частные случаи контактных схем. Оценка числа схем различных типов

Для того, чтобы приблизить функционирование КС с несколькими входами к функционированию СФЭ, рассмотрим следующую модификацию КС. Будем считать, что БП из алфавита X являются управляющими (адресными) входными БП и введем еще один алфавит входных БП — алфавит $Y = \{y_1, y_2, \dots\}$, который состоит из информационных (преобразуемых) БП. Контактную (p, q)-схему, входам(выходам) которой сопоставлены в качестве пометок БП из Y (соответственно Z), причем вход (соответственно выход) с большим номером помечен БП с большим номером, будем называть *преобразующей* контактной схемой (ПКС).

Будем считать, что в вершине v ПКС $\Sigma(x_1, \dots, x_n; y_1, \dots, y_p; z_1, \dots, z_q)$ реализуется ФАЛ вида

$$f_v(x, y) = y_1 \cdot g_v^{(1)}(x) \vee \dots \vee y_p \cdot g_v^{(p)}(x) \tag{7.1}$$

где $x = x(n)$, $y = (y_1, \dots, y_p)$, а $g_v^{(i)}(x)$ – ФАЛ проводимости от i-го входа Σ к вершине v, $i \in [1, p]$, и что КС Σ реализует систему $\mathcal{F}$, состоящую из q ФАЛ, реализуемых на ее выходах, или, иначе, систему уравнений $z = \mathcal{F}(x, y)$, где $z = (z_1, \dots, z_q)$. Заметим, что при этом

$$f_v(x, y) = y \cdot g_v(x) \text{ и } \mathcal{F}(x, y) = y \cdot F(x) \tag{7.2}$$

где $g_v(x)$ – столбец, а $F(x)$ – матрица из ФАЛ, которые реализуются «обычным» способом в вершине v и на выходах КС Σ соответственно.

Соотношение (7.1) имеет следующий содержательный смысл: ФАЛ f_v обращается в 1 при $x = \alpha$ и $y = \beta = (\beta_1, \dots, \beta_p)$ тогда и только тогда, когда из некоторой выходной вершины v_i с сопоставленной БП y_i такой, что $\beta_i = 1$, в вершину v идет проводящая при $x = \alpha$ цепь C (см. рис. 7.1). В соответствии с (7.1) в каждой входной вершине v_i, $i = 1, \dots, p$, тоже реализуется ФАЛ $f_{v_i}(x, y)$, для которой $f_{v_i}(x, y) \geqslant y_i$.

Так, вентильная звезда Σ'' порядка p, приведенная на рис. 6.1b, является ПКС, реализующей ФАЛ $y_1 \vee \dots \vee y_p$. На рис. 7.2a показана ПКС Σ от БП $(x_1, \dots, x_p; y_1, \dots, y_p; z_1)$, которая называется *неоднородной звездой порядка* p, имеет степень $(\sigma_1, \dots, \sigma_p)$ и реализует ФАЛ $x_1^{\sigma_1} y_1 \vee \dots \vee x_p^{\sigma_p} y_p$. На рис. 7.2b изображена преобразующая контактная схема $\widehat{\Sigma}$, которая получается из указанной ПКС Σ, где $\sigma_1 = \sigma_2 = \dots = \sigma_p = \sigma$, в результате отождествления БП $x_1 = x_2 = \dots = x_p = x$, называется *однородной звездой порядка* p, имеет степень σ и реализует ФАЛ $x^\sigma (y_1 \vee \dots \vee y_p)$. На рис. 7.3a приведена $(2^n, 1)$-ПКС $\mathcal{D}(x_1, \dots, x_n; y_0, \dots, y_{2^n-1}; z)$, которая получается из $(1, 2^n)$-КС, являющейся контактным деревом порядка n (см. рис. 5.4), в результате

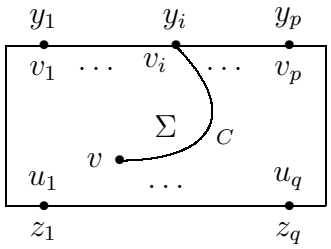


Рис. 7.1: к определению преобразующей контактной схемы

объявления его листьев информационными входами,а корня дерева – выходом. Легко видеть, что указанная схема является ПКС-мультиплексором порядка n, то есть реализует ФАЛ $\mu_n(x_1, \ldots, x_m, ; y_0, \ldots, y_{2^n-1})$.

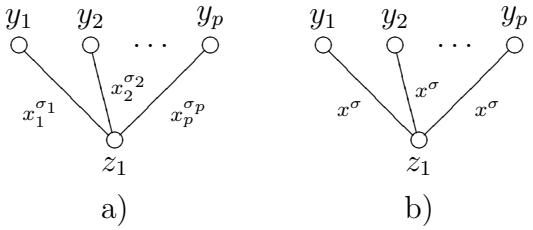


Рис. 7.2: неоднородная и однородная звезды порядка p

Суперпозиция ПКС понимается как суперпозиция связанных с ними КС и считается корректной в случае корректности последней. Отметим, что корректная суперпозиция ПКС реализует соответствующую ей суперпозицию ФАЛ. Действительно, пусть, для определенности, ПКС $\Sigma\,(x; y; z)$ является результатом корректной полной стыковки вида $\Sigma = \Sigma''\,(\Sigma')$, где ПКС $\Sigma'\,(x; y; z')$ и $\Sigma''\,(x; y''; z)$ реализуют системы ФАЛ

$$\mathcal{F}'\,(x, y) = y \cdot F'(x) \text{ и } \mathcal{F}''\,(x, y'') = y'' \cdot F(x)$$

соответственно (см. (7.2)). Тогда в силу корректности рассматриваемой суперпозиции система ФАЛ $\mathcal{F}\,(x, y)$, реализуемая ПКС Σ, имеет вид (см. следствие 1 из леммы 6.1)

$$\mathcal{F}\,(x, y) = y \cdot F'(x) \cdot F''(x) = \mathcal{F}''\,(x, \mathcal{F}'\,(x, y))\,,$$

то есть задается соответствующей суперпозицией систем ФАЛ $\mathcal{F}'$ и $\mathcal{F}''$. Аналогичным образом рассматривается и корректная суперпозиция общего вида.

В случае ПКС будем рассматривать и еще один тип суперпозиции — подстановку константы 1 вместо информационных БП. Схему Σ', которая получается из ПКС

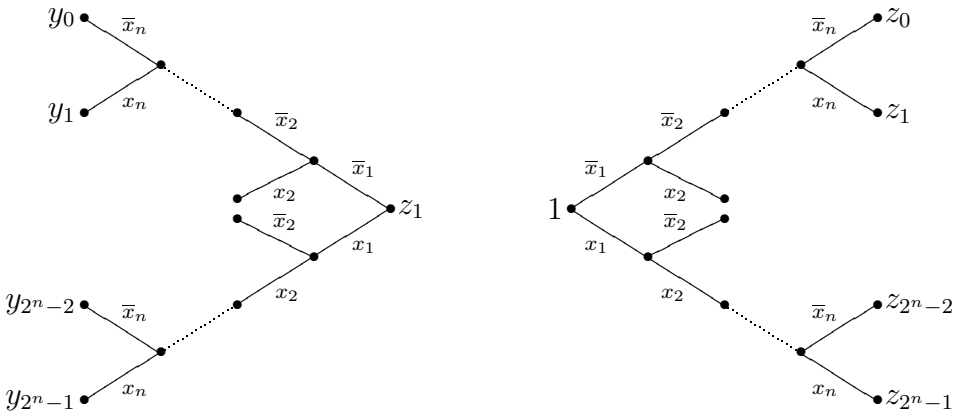


Рис. 7.3: ПКС-мультиплексор и ПКС1-дешифратор на основе контактного дерева

$\Sigma(x_1,\ldots,x_n;y_1,\ldots,y_p;z_1,\ldots,z_q)$ в результате замены пометок $y_{i_1},\ldots,y_{i_s}$, где $1 \leqslant i_1 < \cdots < i_s \leqslant p$ на пометку 1 будем называть *преобразующей контактной схемой с* 1*-входами* (ПКС1). При этом считается, что информационными входными БП Σ' являются БП из набора y', который получается удалением БП $y_{i_1},\ldots,y_{i_s}$ из набора $y_1,\ldots,y_p$, что вершины, соответствующие БП $y_{i_1},\ldots,y_{i_s}$ в Σ, становятся 1-входами Σ', и что ФАЛ $f'_v(x,y')$, реализуемая в вершине v схемы Σ', задается формулой, которая получается из правой части (7.1) в результате подстановки константы 1 вместо БП $y_{i_1},\ldots,y_{i_s}$.

Легко видеть, что подстановка константы 1 является корректной операцией суперпозиции, и что любая ПКС1 эквивалентна ПКС1, которая получается из нее в результате «склейки» всех 1-входов в один такой вход. Заметим также, что функционирование $(1,m)$-ПКС1 с 1-входом совпадает с функционированием соответствующей ей $(1,m)$-КС. Так, на рис. 7.3b показана $(1,2^n)$-ПКС1, которая соответствует $(1,2^n)$-контактному дереву порядка n и является ПКС1-дешифратором порядка n.

Рассмотрим теперь следующий класс контактных схем, который является удобной математической моделью интегральных схем на дополняющих МОП-транзисторах (см., например, [4]). Пусть $(2,m)$-КС вида $\Sigma(x_1,\ldots,x_n;a',a'';a_1,\ldots,a_m)$ получается из $(1,m)$-КС вида $\Sigma'(x_1,\ldots,x_n;a';a'_1,\ldots,a'_m)$, которая реализует набор функций алгебры логики $F=(f_1,\ldots,f_m)$, и $(1,m)$-КС вида $\Sigma''(x_1,\ldots,x_n;a'';a''_1,\ldots,a''_m)$, которая реализует набор ФАЛ $\overline{F}=\left(\overline{f}_1,\ldots,\overline{f}_m\right)$, в результате следующего отождествления вершин: $a'_i=a''_i=a_i$, где $i=1,\ldots,m$ (см. рис. 7.4a). Заметим, что на любом наборе $\alpha=(\alpha_1,\ldots,\alpha_n)$ значений БП $x_1,\ldots,x_n$ и при любом j, $j=1,\ldots,m$ в КС Σ имеется проводящая цепь либо из a', если $f_j(\alpha)=1$, либо из a'', если $f_j(\alpha)=0$, в a_j. Заметим также, что ФАЛ проводимости между входами a' и a'' в КС Σ равна 0. Действитель-

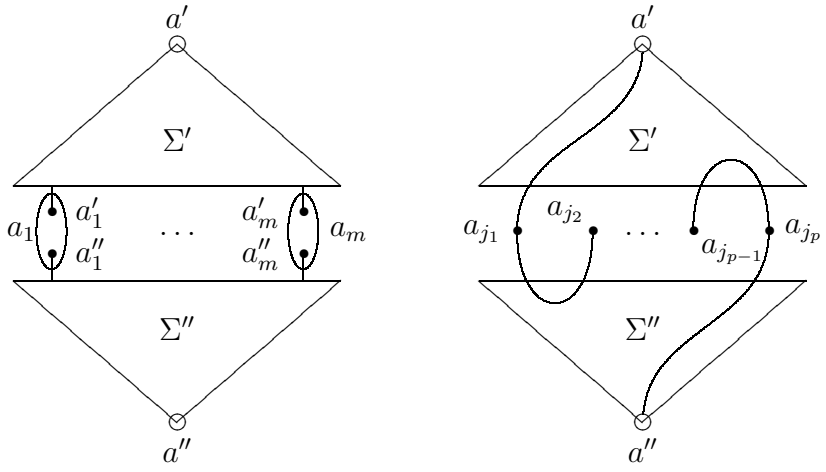


Рис. 7.4: к построению модели ИС на дополняющих МОП-транзисторах

но, пусть на наборе $x = \alpha$ в Σ имеется проводящая цепь C из a' в a'' последовательно переходящая из Σ' в Σ'' и обратно в вершинах $a_{j_1}, \ldots, a_{j_p}$ (см. рис. 7.4b). Тогда, в силу специфики структуры КС Σ, будут справедливы равенства:

$$f_{j_1}(\alpha) = 1, \quad \overline{f}_{j_1}(\alpha) = \overline{f}_{j_2}(\alpha), \quad f_{j_2}(\alpha) = f_{j_3}(\alpha), \ldots$$
$$\ldots, \quad f_{j_{p-1}}(\alpha) = f_{j_p}(\alpha), \quad f_{j_p}(\alpha)) = 1,$$

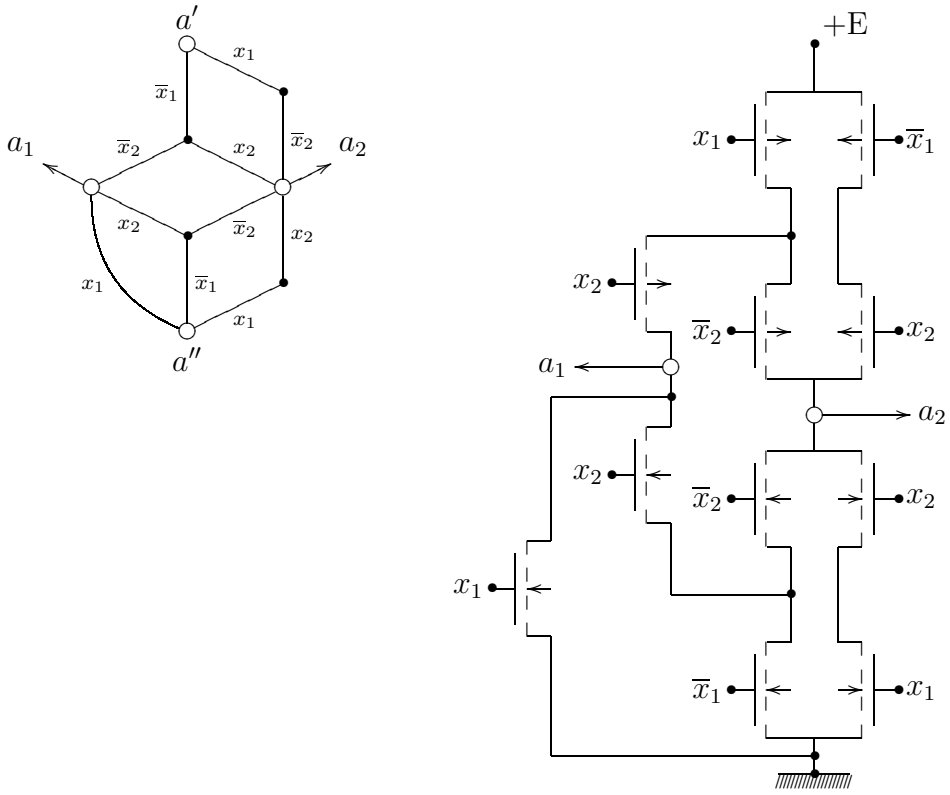
из которых вытекает, что, с одной стороны,

$$f_{j_1}(\alpha) = f_{j_2}(\alpha) = \cdots = f_{j_p}(\alpha) = 1,$$

а, с другой стороны,

$$f_{j_p}(\alpha) = f_{j_{p-1}}(\alpha) = \cdots = f_{j_1}(\alpha) = 0.$$

Отмеченные выше особенности КС Σ позволяют использовать ее для построения схемы на дополняющих МОП-транзисторах, реализующей набор ФАЛ F. Для этого достаточно подключить ее вход a' (a'') к источнику высокого (соответственно низкого) потенциала, а каждый контакт вида x_i^σ КС Σ' (Σ'') заменить p-МОП (соответственно n-МОП) транзистором, на затвор которого подана ФАЛ $x_i^{\overline{\sigma}}$ (соответственно x_i^σ). На рис. 7.5a показана КС Σ указанного вида, а на рис. 7.5b — соответствующая ей схема на дополняющих МОП-транзисторах, реализующая набор ФАЛ $F = (\overline{x}_1 \cdot \overline{x}_2, x_1 \oplus x_2)$.



a) b)

Рис. 7.5: модель интегральной схемы на дополняющих МОП-транзисторах

В последние годы активно изучается один специальный класс КС — т.н. двоичные решающие диаграммы (BDD), которые представляют собой, по существу, адресующие бинарные программы (см., например, [2, 8]). Схема Σ с одним входом a' и двумя выходами a_0, a_1, называется *двоичной решающей диаграммой*, если она состоит из ориентированных контактов и не имеет (ориентированных) циклов, а из каждой ее вершины v, отличной от выходов, исходят две дуги с противоположными пометками вида $x_i, \overline{x}_i$ (см. рис. 7.6a). При этом вершине v (a_0, a_1), обычно, сопоставляют пометку x_i (соответственно $0, 1$), а пометки $\overline{x}_i$ и x_i у исходящих из v ребер заменяют пометками 0 и 1 соответственно (см. рис. 7.6b). Заметим, что BDD Σ указанного вида от БП $x_1, \ldots, x_n$ реализует между входом a' и выходом a_1 некоторую ФАЛ $f(x_1, \ldots, x_n)$, между входом a' и выходом a_0 — ФАЛ $\overline{f}(x_1, \ldots, x_n)$, а ФАЛ проводимости между a_0 и a_1 равна 0. В таком случае, обычно, считается что Σ реализует ФАЛ f. Так, например, BDD Σ, показанная на рис. 7.7 (ср. с рис. 5.3c), реализует ФАЛ $x_1 \oplus x_2 \oplus x_3$.

Наряду со сложностью $L(\Sigma)$ BDD Σ введем также ее *размер* $\mathcal{L}(\Sigma)$, равный числу вершин Σ, отличных от выходов, и заметим, что $L(\Sigma) = 2\mathcal{L}(\Sigma)$. Пусть, как обычно, $\mathcal{U}^{\mathrm{BDD}}(\mathcal{L}, n)$ — множество тех BDD Σ от БП $X(n)$, размер которых не больше, чем $\mathcal{L}$.

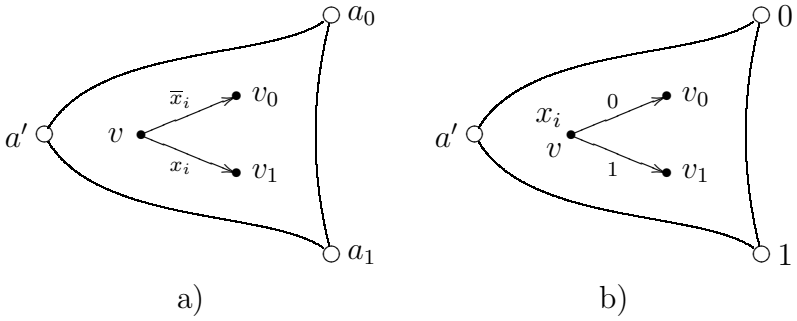


Рис. 7.6: к определению BDD

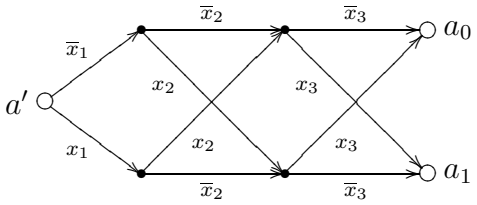


Рис. 7.7: BDD для ℓ_3

Лемма 7.1. *Для любых натуральных* $\mathfrak{L}$, n *справедливо неравенство:*

$$\left\|\mathcal{U}^{\mathrm{BDD}}(\mathfrak{L}, n)\right\| \leqslant (16n(\mathfrak{L}+2))^{\mathfrak{L}+1}.$$

Доказательство. Легко видеть, что любая BDD рассматриваемого вида эквивалентна некоторой BDD Σ от БП $x_1, \ldots, x_n$, которая содержит ровно $\mathfrak{L}$ вершин, отличных от выходов. Сопоставим BDD Σ граф $\widehat{\Sigma}$, получающийся из нее изменением ориентации всех дуг. Заметим, что указанное сопоставление является взаимно однозначным с точностью до изоморфизма, а $\widehat{\Sigma}$ — ориентированный ациклический граф с одним стоком и двумя истоками, помеченными символами $0, 1$, в котором каждая отличная от истока вершина имеет две входящие дуги и помечена одной из БП $x_1, \ldots, x_n$. Используя рассуждения из доказательства теоремы 3.1, число попарно не изоморфных графов $\widehat{\Sigma}$ указанного вида можно оценить сверху числом $(16n\,(\mathfrak{L}+2))^{\mathfrak{L}+1}$.

Лемма доказана. □

§8 Эквивалентные преобразования схем. Основные тождества для контактных схем, вывод вспомогательных и обобщенных тождеств

В §3 главы 1 были даны основные определения и введены обозначения, связанные с эквивалентными преобразованиями (ЭП) формул. Распространим эти понятия и обозначения на случай реализации ФАЛ с помощью сетей и, в частности, на класс контактных схем.

Пусть $\mathcal{U}$ — один из введенных выше классов схем. В соответствии с определениями из §2, §3, §5–§7 эквивалентность схем Σ' и Σ'' из $\mathcal{U}$ имеет место тогда и только тогда, когда Σ' и Σ'' реализуют равные системы (матрицы) ФАЛ. При этом, обычно, предполагается, что соответствующие друг другу полюса (выходы, входы) в Σ' и Σ'' имеют одинаковые пометки, а эквивалентность Σ' и Σ'' записывается в виде тождества

$$t:\ \Sigma' \sim \Sigma''.$$

Для схем из $\mathcal{U}$, как правило, определяется ряд «простейших» преобразований, сохраняющих эквивалентность схем, которые называются *подстановками*. Тождество

$$\widehat{t}:\ \widehat{\Sigma}' \sim \widehat{\Sigma}'',$$

которое получается в результате применения одной и той же подстановки к обеим частям тождества $t:\ \Sigma' \sim \Sigma''$, называется *подстановкой тождества* t. Схема Σ' называется *подсхемой схемы* Σ, если

$$V(\Sigma') \subseteq V(\Sigma), \qquad E(\Sigma') \subseteq E(\Sigma)$$

и любая вершина v, $v \in V(\Sigma')$, которая либо относится к множеству входов (выходов) Σ, либо служит конечной (соответственно, начальной) вершиной некоторого ребра из $E(\Sigma) \setminus E(\Sigma')$, является входом (соответственно, выходом) Σ'. Из определений следует, что для СФЭ и КС с неразделенными полюсами, как и для формул (см. §3 главы 1), имеет место принцип эквивалентной замены. При этом все введенные в §3 главы 1 для случая элементарных преобразований формул понятия (однократная и кратная выводимость, обратимость ЭП, полнота системы тождеств), а также связанные с ними обозначения переносятся на случай ЭП указанных классов схем без изменений.

Рассмотрим теперь вопросы ЭП для КС из $\mathcal{U}^{\mathrm{K}}$ с неразделенными (бесповторными) полюсами. В соответствии с §6 эквивалентность КС $\Sigma' = \Sigma'(x_1, \ldots, x_n; a_1, \ldots, a_m)$ и $\Sigma'' = \Sigma''(x_1, \ldots, x_n; a_1, \ldots, a_m)$ означает, что для любых i и j из отрезка $[1, m]$ ФАЛ проводимости от a_i к a_j в КС Σ' равна ФАЛ проводимости от a_i к a_j в КС Σ''. На рис. 8.1a–8.1e и 8.1f приведены пары эквивалентных КС, образующие тождества

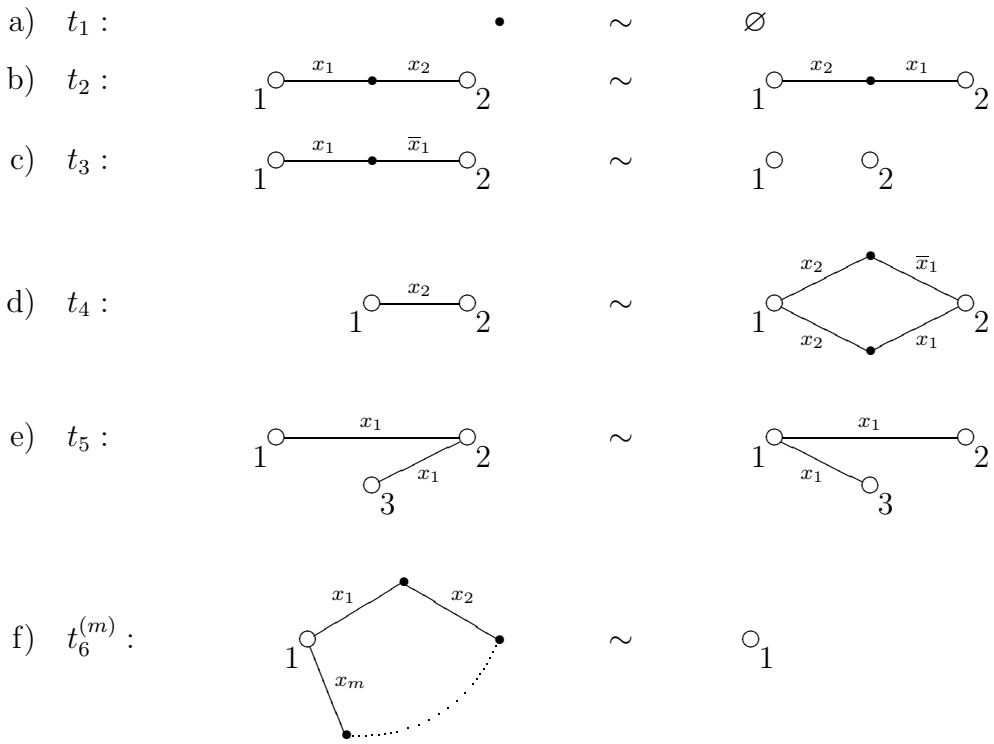


Рис. 8.1: основные тождества для КС

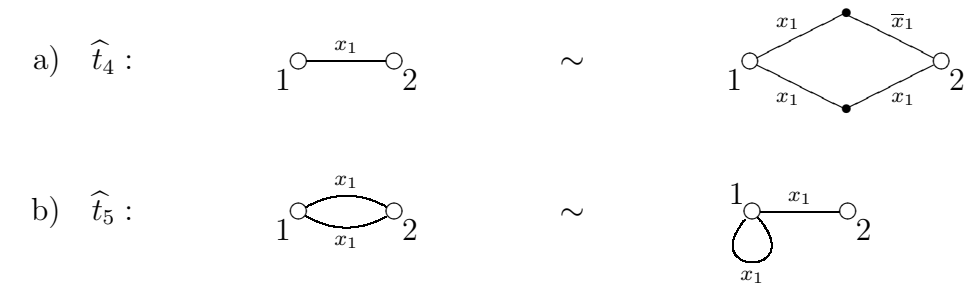


Рис. 8.2: подстановки для основных тождеств

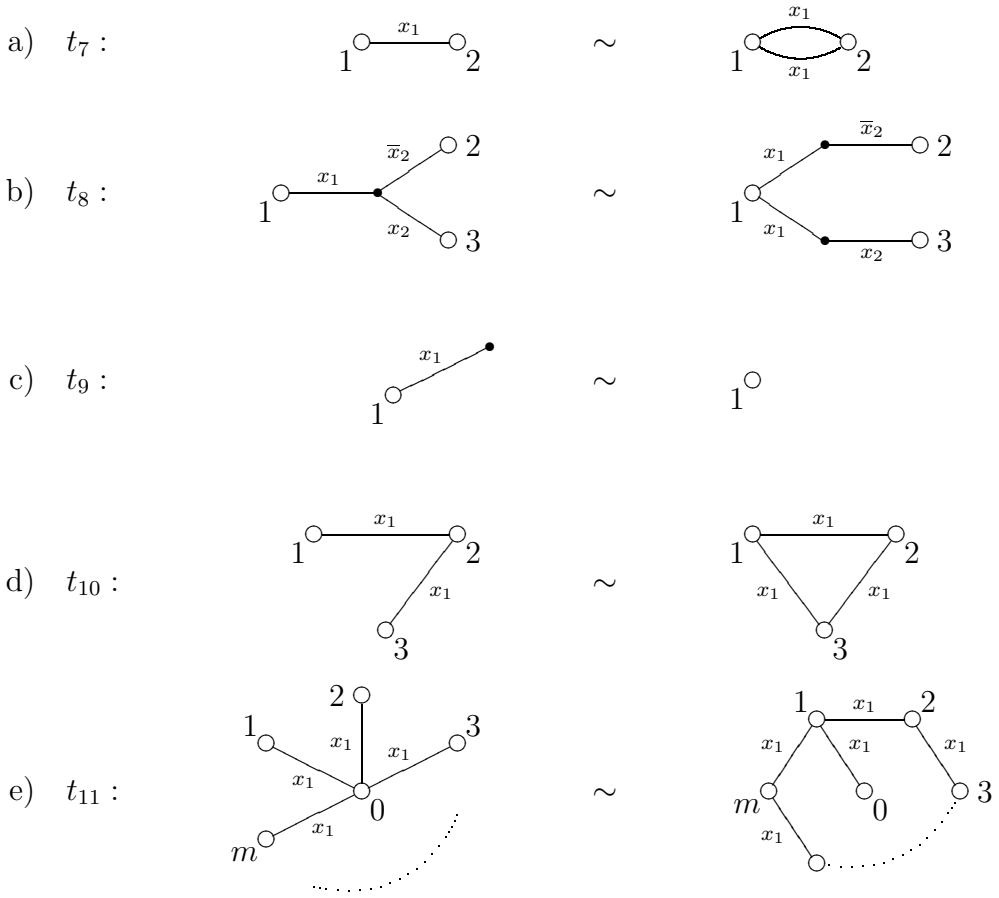


Рис. 8.3: вспомогательные тождества для КС

t_1–t_5 и $t_6^{(m)}$, $m = 1, 2, \ldots$, соответственно, которые мы будем называть *основными тождествами* для ЭП КС.

Определим подстановку для КС как переименование (с возможным отождествлением и инвертированием) БП, а также переименование (с возможным отождествлением и снятием) полюсов. Заметим, что применяя одну и ту же подстановку к двум эквивалентным КС мы получим эквивалентные КС. Действительно, для переименования БП и переименования без отождествления полюсов это очевидно, а в случае отождествления полюсов эквивалентность получаемых КС вытекает из того, что матрица достижимости КС, являющейся результатом отждествления, однозначно определяется матрицей достижимости исходной КС. На рис. 8.2a (8.2b) показана подстановка $\widehat{t}_4$ тождества t_4 (соответственно $\widehat{t}_5$ тождества t_5), связанная с переименованием БП x_2 в x_1 (соответственно полюсов $1 = 3$ в 1).

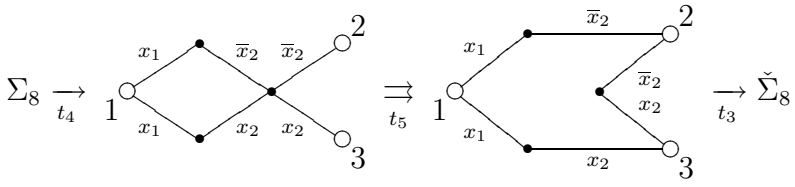


Рис. 8.4: вывод t_8

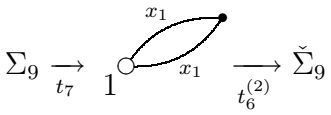


Рис. 8.5: вывод t_9

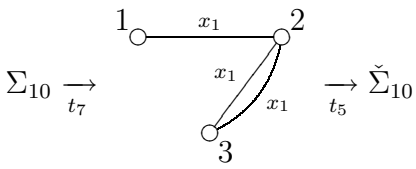


Рис. 8.6: вывод t_{10}

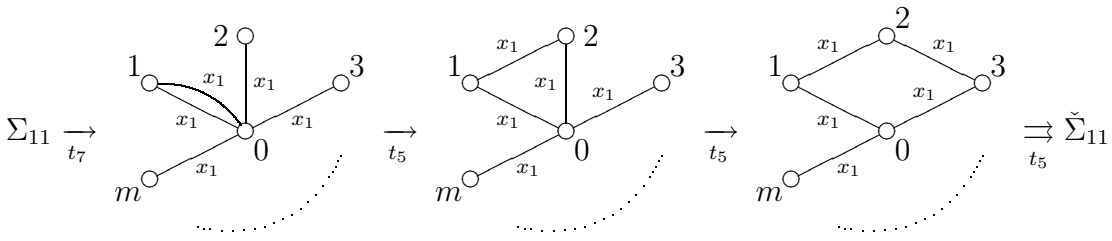


Рис. 8.7: вывод t_{11}

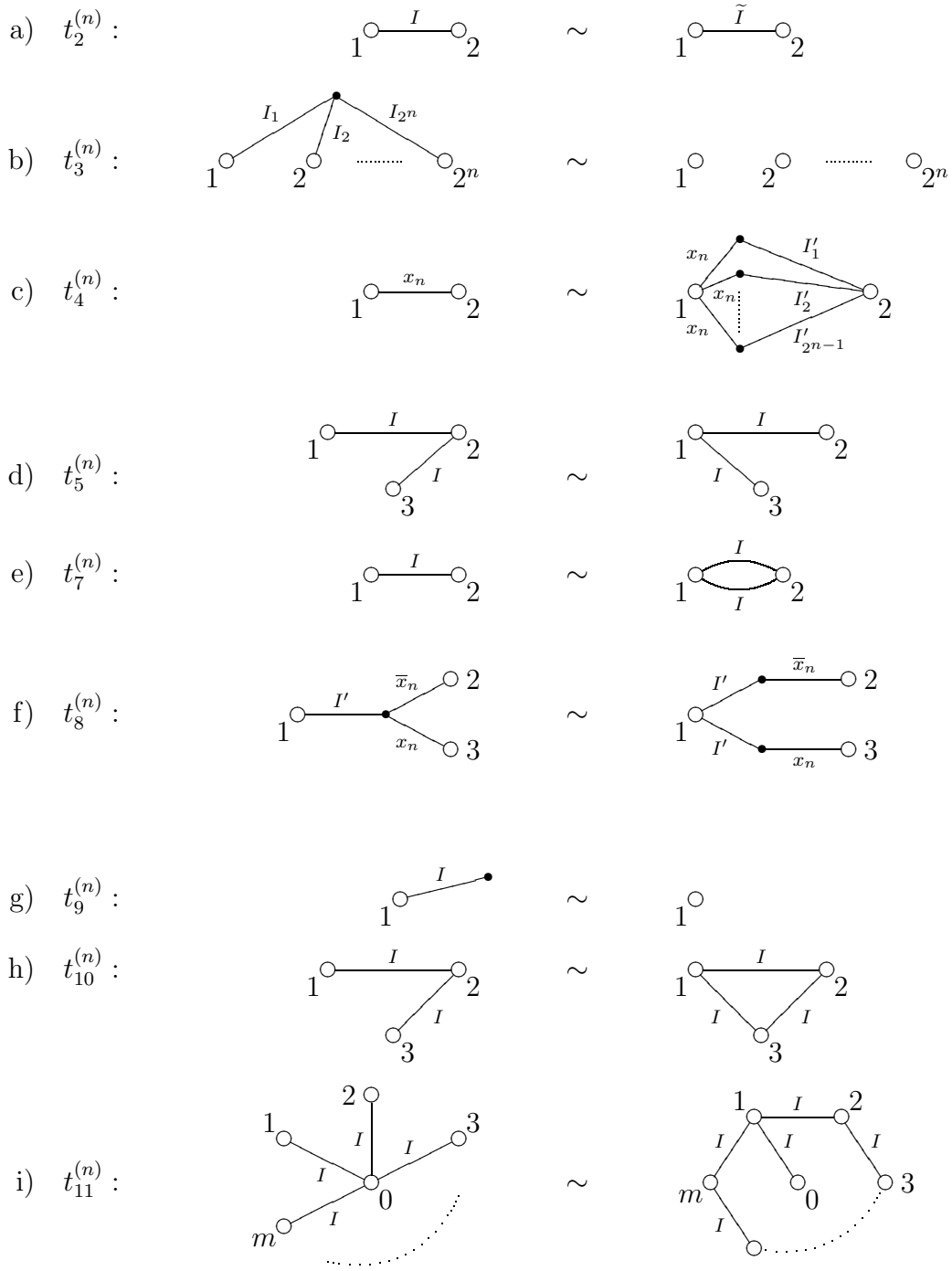


Рис. 8.8: обобщенные тождества порядка n для КС

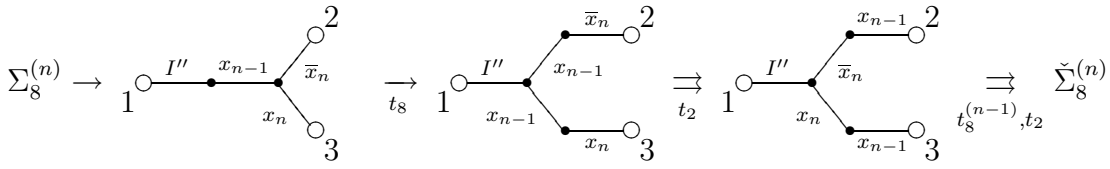


Рис. 8.9: вывод $t_8^{(n)}$

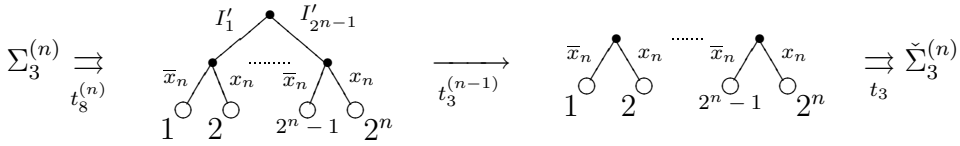


Рис. 8.10: вывод $t_3^{(n)}$

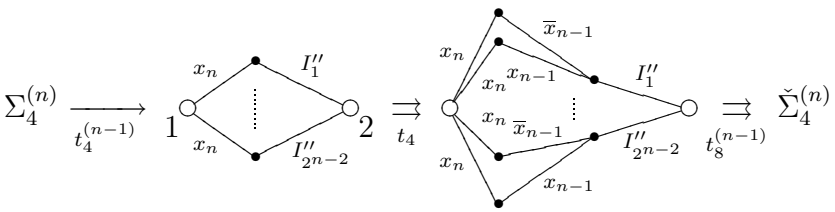


Рис. 8.11: вывод $t_4^{(n)}$

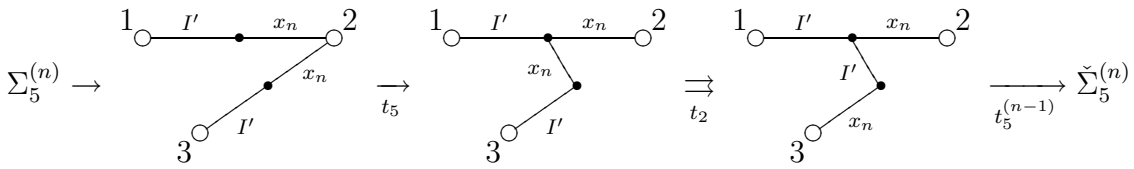


Рис. 8.12: вывод $t_5^{(n)}$

Рассмотрим примеры ЭП контактных схем с помощью системы основных тождеств. На рис. 8.3a–8.3e приведены тождества t_7–t_{11}, которые мы будем называть *вспомогательными*. Заметим, что выводимость $\{t_5, t_6^{(1)}\} \rightrightarrows t_7$ доказывается применением тождества $t_6^{(1)}$ к правой части тождества $\widehat{t_5}$ (см. рис. 8.2a) для удаления из нее «висячего» цикла длины 1. Выводимость тождеств t_8–t_{11} из основных тождеств $\{t_1 - t_5, t_6^{(1)}, t_6^{(2)}\}$ показана на рис. 8.4–8.7 соответственно, где Σ_i и $\check{\Sigma}_i$ — левая и правая части тождества t_i, $i \in [8, 11]$. Тождество t_{10} называют иногда тождеством замыкания по транзитивности, а тождество t_{11} — «леммой» о звезде.

Обобщим тождества t_1–t_{11} на случай КС от БП $X(n)$, где $n \geqslant 2$. Сопоставим ЭК $K_i^{(n)}$, $i \in [1, 2^n]$, вида $K_i^{(n)} = x_1^{\sigma_1} \cdots x_n^{\sigma_n}$, где $\nu(\sigma_1, \ldots, \sigma_n) = i - 1$, моделирующую цепочку $I_i^{(n)}$ (см. §5), и пусть

$$\begin{aligned} I_i^{(n)} &= I_i, \quad i \in [1, 2^n], & I &= I_{2^n}; \\ I_i^{(n-1)} &= I'_i, \quad i \in \left[1, 2^{n-1}\right], & I' &= I'_{2^{n-1}}; \\ I_i^{(n-2)} &= I''_i, \quad i \in \left[1, 2^{n-2}\right], & I'' &= I''_{2^{n-2}}. \end{aligned}$$

Систему тождеств $\tau^{(n)} = \left\{t_1^{(n)}, \ldots, t_{11}^{(n)}\right\}$, где $t_1^{(n)} = t_1$, $t_6^{(n)}$ — соответствующее основное тождество (см. рис. 8.1f), $t_2^{(n)}$ — система, состоящая из тождеств, показанных на рис. 8.8a, где $\widetilde{I}$ — произвольная перестановка цепочки I, а остальные тождества приведены на рис. 8.8b—8.8i, будем называть системой *обобщенных тождеств порядка* n. При этом система $\tau_n = \left\{t_1, \ldots, t_5, t_6^{(1)}, \ldots, t_6^{(n)}\right\}$ считается системой основных тождеств порядка n, а система всех основных тождеств обозначается через τ_∞.

Лемма 8.1. *При $n \geqslant 2$ имеет место выводимость $\tau_n \rightrightarrows \tau^{(n)}$.*

Доказательство. Отметим сначала следующие очевидные выводимости:

$$\{t_2\} \rightrightarrows t_2^{(n)}, \qquad \{t_9\} \rightrightarrows t_9^{(n)}.$$

Выводимость $\tau_n \rightrightarrows t_i^{(n)}$, $i = 8, 3, 4, 5$ докажем индукцией по n, $n \geqslant n_i$, где $n_3 = n_5 = 1$ и $n_8 = n_4 = 2$. Базис этой индукции составляет тождество $t_i = t_i^{(n_i)}$, $i = 8, 3, 4, 5$, а обоснование индуктивного перехода дает выводимость правой части $\check{\Sigma}_i^{(n)}$ тождества $t_i^{(n)}$, $n > n_i$, из его левой части $\Sigma_i^{(n)}$, показанная на рис. 8.9–8.12.

Легко видеть, что выводимости

$$\left\{t_2^{(n)}, t_5^{(n)}\right\} \rightrightarrows t_7^{(n)}, \qquad \left\{t_7^{(n)}, t_5^{(n)}\right\} \rightrightarrows \left\{t_{10}^{(n)}, t_{11}^{(n)}\right\}$$

при $n \geqslant 2$ доказываются аналогично тому, как это делалось для случая $n = 1$ (см. рис. 8.6, 8.7).

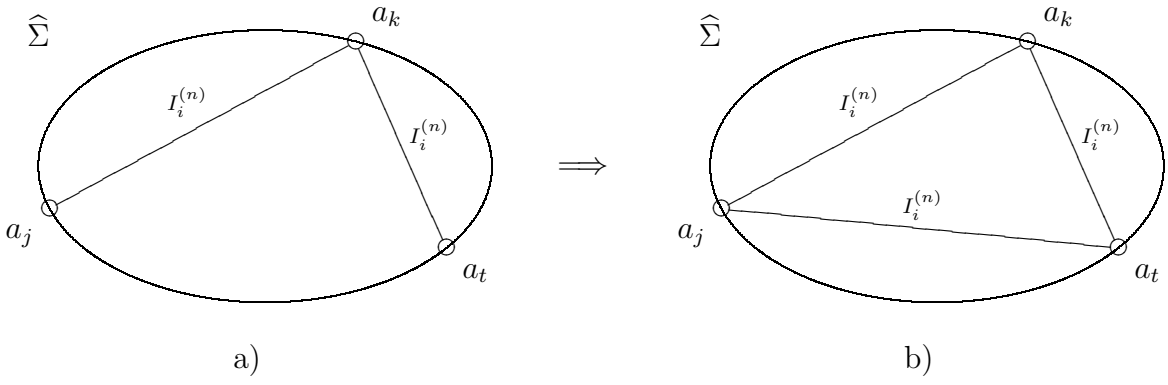
Лемма доказана. □

§9 Полнота системы основных тождеств и отсутствие конечной полной системы тождеств в классе контактных схем

Докажем сначала полноту системы основных тождеств τ_∞ для ЭП КС. Для этого, как обычно, достаточно доказать, что с помощью ЭП на основе системы τ_∞ произвольную КС из $\mathcal{U}^{\mathrm{K}}$ можно привести к каноническому виду.

Будем говорить, что КС $\widehat{\Sigma}(x_1,\ldots,x_n;a_1,\ldots,a_m)$ является *канонической КС от БП* $X(n)$ или, иначе, *канонической КС порядка* n, если она представляет собой объединение канонических $(1,1)$-КС (см. §5) вида $\widehat{\Sigma}_{i_j}(x_1,\ldots,x_n;a_i,a_j)$. Любую цепь $I_i^{(n)}$ (см. §8), где $i\in[1,2^n]$, а также любую цепь, которая получается из $I_i^{(n)}$ перестановкой контактов, будем называть *канонической цепью порядка* n. Заметим, что КС $\widehat{\Sigma}\,(x_1,\ldots,x_n;a_1,\ldots,a_m)$ является канонической КС порядка n тогда и только тогда, когда она обладает следующими свойствами:

1. любой контакт $\widehat{\Sigma}$ принадлежит некоторой канонической цепи порядка n, являющейся подсхемой схемы $\widehat{\Sigma}$, причем полюсами этой подсхемы служат только концевые вершины данной цепи;
2. любая внутренняя вершина $\widehat{\Sigma}$ является внутренней вершиной некоторой цепи из пункта 1;
3. в КС $\widehat{\Sigma}$ отсутствуют «висячие циклы» (см. тождество $t_6^{(n)}$) и «параллельные» цепи, то есть канонические цепи порядка n из пункта 1, которые соединяют одни и те же полюса и реализуют равные ЭК;
4. в КС $\widehat{\Sigma}$ нет существенных транзитных проводимостей, то есть наличие цепей вида $I_i^{(n)}$, соединяющих полюс a_j с полюсом a_k и полюс a_k с полюсом a_t (см. рис. 9.1a), влечет наличие цепи такого же вида, соединяющей полюс a_j с полюсом a_t (см. рис. 9.1b).



a) b)

Рис. 9.1: к свойству 4 КС канонического вида

Лемма 9.1. *Для любой КС* Σ*, где* $\Sigma \in \mathfrak{U}^{\mathrm{K}}$ *и* $\Sigma = \Sigma(x_1, \ldots, x_n; a_1, \ldots, a_m)$*, и любой эквивалентной* Σ *КС* $\widehat{\Sigma}(x_1, \ldots, x_n; a_1, \ldots, a_m)$ *канонического вида существует ЭП* $\Sigma \underset{\tau_n}{\rightrightarrows} \widehat{\Sigma}$.

Доказательство. Построим ЭП вида

$$\Sigma \underset{\tau_n}{\rightrightarrows} \Sigma_1 \underset{\tau_n}{\rightrightarrows} \Sigma_2 \underset{\tau_n}{\rightrightarrows} \Sigma_3 \underset{\tau_n}{\rightrightarrows} \Sigma_4 = \widehat{\Sigma},$$

где КС Σ_i, $i = 1, 2, 3, 4$, обладает отмеченными выше свойствами $1, \ldots, i$, отличающими канонические КС. Первое из этих ЭП имеет вид

$$\Sigma \underset{t_4^{(n)}}{\rightrightarrows} \Sigma_1$$

и связано с применением к каждому контакту тождества $t_4^{(n)}$.

Существование ЭП

$$\Sigma_1 \underset{\left\{t_6^{(n)}, t_{11}^{(n)}, t_9^{(n)}, t_3^{(n)}, t_1^{(n)}\right\}}{\rightrightarrows} \Sigma_2 \tag{9.1}$$

докажем индукцией по числу тех внутренних вершин КС Σ_1, которые не являются внутренними вершинами ее канонических цепей. Базис индукции составляют схемы Σ_1, которые не имеют указанных вершин и для которых, следовательно, $\Sigma_2 = \Sigma_1$. Пусть теперь КС Σ_1 имеет хотя бы одну вершину указанного вида и пусть v — одна из таких вершин. Удалим с помощью тождества $t_6^{(n)}$ все присоединенные к v «висячие» циклы и рассмотрим все остальные цепи $J_1, \ldots, J_q$, концевой вершиной которых она является (см. рис. 9.2a). Не ограничивая общности рассуждений, будем считать, что для некоторых натуральных чисел

$$a_1 = 1 < a_2 < \cdots < a_p < a_{p+1} = q + 1$$

и любого j, $j \in [1, p]$, цепи $J_{a_j}, \ldots, J_{a_{j+1}-1}$ являются цепями типа $I_{i_j}^{(n)} = I_{i_j}$, где $i_1, \ldots, i_p$ — различные числа отрезка $[1, 2^n]$. Применяя к каждой из этих p групп цепей одного типа тождество $t_{11}^{(n)}$, получим КС Σ_1', в которой из вершины v выходит по одной цепи каждого типа I_{i_j}, $j \in [1, p]$ (см. рис. 9.2b). Пусть, далее, КС Σ_1'' получается из КС Σ_1' присоединением к вершине v с помощью тождества $t_9^{(n)}$ «висячих» цепей $J_{p+1}, \ldots, J_{2^n}$ всех отсутствующих среди $I_{i_1}, \ldots, I_{i_p}$ типов (см. рис. 9.2c), а КС Σ_1''' получается из КС Σ_1'' в результате удаления с помощью тождества $t_3^{(n)}$ вершины v вместе со всеми «инцидентными» ей цепями и устранения с помощью тождества t_1 образовавшихся при этом изолированных вершин — концевых вершин цепей $J_{p+1}, \ldots, J_{2^n}$ (см. рис. 9.2d). По индуктивному предположению для КС Σ''' существует ЭП вида

$$\Sigma''' \underset{\left\{t_6^{(n)}, t_{11}^{(n)}, t_9^{(n)}, t_3^{(n)}, t_1^{(n)}\right\}}{\rightrightarrows} \Sigma_2$$

и, следовательно, для КС Σ_1 существует ЭП (9.1).

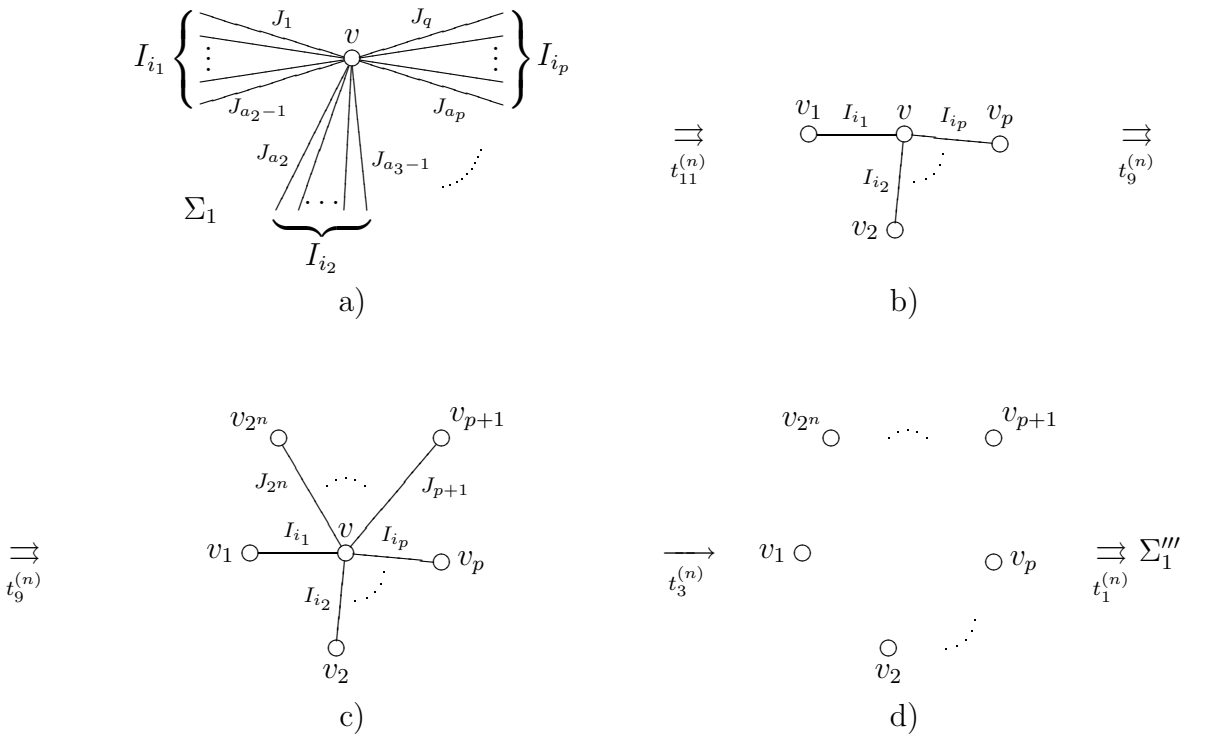


Рис. 9.2: к доказательству леммы 9.1

Переход от КС Σ_2 к КС Σ_3 осуществляется с помощью тождеств $t_6^{(n)}$ и $t_7^{(n)}$, а от КС Σ_2 к КС Σ_3 — с помощью тождеств $t_{10}^{(n)}$.

Лемма доказана. □

Теорема 9.1. *Для любых двух эквивалентных КС Σ' и Σ'' от БП $x_1, \ldots, x_n$ существует ЭП вида $\Sigma' \underset{\tau_n}{\rightrightarrows} \Sigma''$.*

Доказательство. Пусть $\widehat{\Sigma}'$ и $\widehat{\Sigma}''$ — канонические КС от БП $x_1, \ldots, x_n$, эквивалентные КС Σ' и Σ'' соответственно. Из определений следует, что $\widehat{\Sigma}' \underset{t_2^{(n)}}{\rightrightarrows} \widehat{\Sigma}''$, и поэтому в силу леммы 9.1 существует ЭП вида

$$\Sigma' \underset{\tau_n}{\rightrightarrows} \widehat{\Sigma}' \underset{t_2^{(n)}}{\rightrightarrows} \widehat{\Sigma}'' \underset{\tau_n}{\rightrightarrows} \Sigma''.$$

Теорема доказана. □

Следствие 1. *Система τ_n является КПСТ для ЭП КС из $\mathfrak{U}^{\mathrm{K}}$ от БП $x_1, \ldots, x_n$.*

Следствие 2. *Система τ_∞ является ПСТ для ЭП КС из $\mathfrak{U}^{\mathrm{K}}$.*

Докажем теперь отсутствие КПСТ в классе $\mathcal{U}^{\mathrm{K}}$. Для КС Σ от БП $x_1, \ldots, x_n$ и набора $\alpha,\ \alpha \in B^n$, определим величину

$$\Theta(\Sigma, \alpha) = |E(\Sigma(\alpha))| - |V(\Sigma(\alpha))| + c(\Sigma(\alpha)),$$

которая (см. §1) задает цикломатическое число графа $\Sigma(\alpha)$. Положим, далее,

$$\Theta(\Sigma) = \sum_{\alpha \in B^n} \Theta(\Sigma, \alpha).$$

Лемма 9.2. *Если* $\Sigma'(x_1, \ldots, x_n) \underset{\{t_1 - t_5\}}{\rightrightarrows} \Sigma''(x_1, \ldots, x_n)$, *то* $\Theta(\Sigma') = \Theta(\Sigma'')$, *а если* $\Sigma' \underset{\tau_k}{\rightrightarrows} \Sigma''$, *где* $k < n$, *то* $\Theta(\Sigma') - \Theta(\Sigma'')$ *делится на* 2^{n-k}.

Доказательство. Докажем, что $\Theta(\Sigma') = \Theta(\Sigma'')$, если $\Sigma' \underset{t_i}{\rightarrow} \Sigma''$ для любого i из отрезка $[1, 5]$. Действительно, пусть КС Σ'' получается из КС Σ' заменой ее подсхемы $\widehat{\Sigma}'_i$, которая имеет вид левой части тождества t_i, на соответствующую ей правую часть $\widehat{\Sigma}''_i$ этого тождества. Нетрудно проверить, что для любого i, $i \in [1, 5]$, число циклов графа $\Sigma(\alpha)$ для любого $\alpha \in B^n$ сохранится, и, следовательно, $\Theta(\Sigma') = \Theta(\Sigma'')$.

Пусть теперь $\Sigma' \underset{\tau_k}{\rightrightarrows} \Sigma''$, причем $k < n$. Если КС Σ' содержит в качестве подсхемы цикл из k контактов с одним полюсом, то КС Σ'' содержит вместо него один лишь полюс. Рассмотрим цикломатическое число сети $\Sigma'(\alpha)$ для различных $\alpha, \alpha \in B^n$. Если цикл указанного вида в КС Σ' содержит контакты, помеченные различными буквами одной и той же БП, то, очевидно, для любого α, $\alpha \in B^n$, $\Theta(\Sigma') - \Theta(\Sigma'') = 0$. В противном случае пусть $x_{j_1}, \ldots, x_{j_m}$ — все различные БП, встречающиеся среди пометок указанного цикла, причем $m \leqslant k$. Заметим, что если цикл проводит на наборе α, $\alpha \in B^n$, то он проводит и на всех 2^{n-m} наборах, в которых значения переменных с индексами $j_1, \ldots, j_m$ совпадают со значениями соответствующих переменных набора α. Таким образом,

$$\Theta(\Sigma') - \Theta(\Sigma'') = \sum_{\alpha = (\alpha_1, \ldots, \alpha_n)} (\Theta(\Sigma'(\alpha)) - \Theta(\Sigma''(\alpha))).$$

Отсюда получаем, что $\Theta(\Sigma') - \Theta(\Sigma'')$ делится на 2^{n-m} и, следовательно, на 2^{n-k}.

Лемма доказана. □

Теорема 9.2. *В классе* $\mathcal{U}^{\mathrm{K}}$ *не существует конечной полной системы тождеств.*

Доказательство. Проведем доказательство от противного: пусть τ — КПСТ для ЭП КС $\mathcal{U}^{\mathrm{K}}$, и пусть n — максимальное число БП, встречающихся в тождествах системы τ. Тогда $\tau_n \rightrightarrows \tau$ и τ_n — КПСТ для $\mathcal{U}^{\mathrm{K}}$. Докажем, что $\tau_n \not\rightrightarrows t_6^{(n+1)}$. Для этого рассмотрим КС Σ', состоящую из простого цикла длины $(n+1)$, содержащего контакты с

пометками $x_i,\ i \in [1, n+1]$, и имеющую единственный полюс с пометкой 1. Очевидно, что ей эквивалентна КС Σ'', содержащая изолированный полюс 1. Если $\tau_n \rightrightarrows t_6^{(n+1)}$, то $\Sigma' \rightrightarrows \Sigma''$. Согласно данным выше определениям, $\Theta(\Sigma') = 1,\ \Theta(\Sigma'') = 0$ и разность $\Theta(\Sigma') \overset{\tau_n}{-} \Theta(\Sigma'') = 1$ не делится на 2, что противоречит утверждению леммы 9.2. Таким образом, $t_6^{(n+1)}$ не выводится из τ_n, а значит, и из τ. Отсюда следует, что τ не может являться КПСТ для ЭП КС $\mathcal{U}^{\mathrm{K}}$.

Теорема доказана. □

§10 Эквивалентные преобразования схем из функциональных элементов, полнота системы основных тождеств для базиса $\{\&, \vee, \neg\}$. Структурное моделирование и эквивалентные преобразования формул и схем в различных базисах

Рассмотрим сначала вопросы ЭП СФЭ. Мы будем использовать введенные в §8 общие понятия и определения, касающиеся ЭП схем, считая подстановкой СФЭ переименование (с возможным отождествлением) ее входных БП и переименование (с возможным дублированием и снятием) ее выходных БП. Напомним, что формулы представляют собой частный случай СФЭ, и для определенности будем считать, что любая формула $\mathcal{F}$ из $\mathcal{U}_{\mathrm{Б}}^{\Phi}$ является формулой-словом (см. §1 главы 1), а соответствующую ей формулу-граф, т. е. квазидерево (см. §3), будем обозначать через $\underline{\mathcal{F}}$. При этом тождеству $t:\ \mathcal{F}' = \mathcal{F}''$, где $\mathcal{F}', \mathcal{F}'' \in \mathcal{U}_{\mathrm{Б}}^{\Phi}$, будет соответствовать тождество $\underline{t} : \underline{\mathcal{F}'} \sim \underline{\mathcal{F}''}$, где $\underline{\mathcal{F}'}, \underline{\mathcal{F}''} \in \mathcal{U}_{\mathrm{Б}}^{\mathrm{C}}$, являющееся «схемным» аналогом тождества t. Множество СФЭ вида $\underline{\mathcal{F}}$, где $\mathcal{F} \in \mathfrak{F} \subseteq \mathcal{U}_{\mathrm{Б}}^{\Phi}$, будем обозначать через $\underline{\mathfrak{F}}$, а систему тождеств вида $\underline{t}$, где $t \in \tau$, а τ — система тождеств для $\mathcal{U}_{\mathrm{Б}}^{\Phi}$, — через $\underline{\tau}$. Так, на рис. 10.1a и 10.1b приведены тождества $\underline{t_{\&}^{\mathrm{M}}}$ и $\underline{t_{1,\&}^{\mathrm{ПК}}}$ из системы $\underline{\tau^{\mathrm{осн}}}$ (см. §3 главы 1).

На рис. 10.2a и 10.2b показаны тождество *ветвления* $t_{\mathcal{E}_i}^{\mathrm{B}}$ и тождество *снятия* $t_{\mathcal{E}_i}^{\mathrm{C}}$ *для функционального элемента* $\mathcal{E}_i,\ i \in [1, b]$, соответственно, а на рис. 10.2c — тождество *снятия входа* $t_{\mathrm{вх}}^{\mathrm{C}}$. Заметим, что эти тождества не являются аналогами формульных тождеств и положим

$$\tau_{\mathrm{Б}}^{\mathrm{B}} = \left\{t_{\mathcal{E}_i}^{\mathrm{B}}\right\}_{i=1}^{b}, \qquad \tau_{\mathrm{Б}}^{\mathrm{C}} = \left\{t_{\mathcal{E}_i}^{\mathrm{C}}\right\}_{i=1}^{b} \cup \left\{t_{\mathrm{вх}}^{\mathrm{C}}\right\}.$$

Очевидно, что с помощью этих тождеств можно избавиться от всех висячих вершин и всех внутренних ветвлений, имеющихся в СФЭ. Следовательно, для любой СФЭ $\Sigma,\ \Sigma \in \mathcal{U}_{\mathrm{Б}}^{\mathrm{C}}$, существует ЭП вида $\Sigma \underset{\{\tau^{\mathrm{C}}, \tau^{\mathrm{B}}\}}{\rightrightarrows} \underline{\mathcal{F}}$, где $\mathcal{F}$ — формула (система формул) из $\mathcal{U}_{\mathrm{Б}}^{\Phi}$.

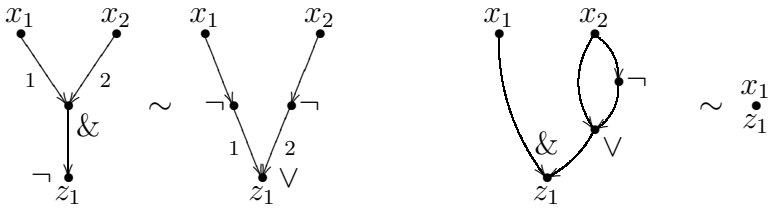


Рис. 10.1: тождества $\underline{t^{\text{М}}_{\&}}$ и $\underline{t^{\text{ПК}}_{1,\&}}$

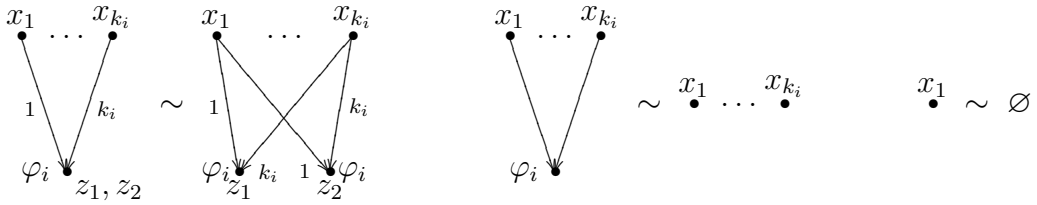


Рис. 10.2: тождества ветвления, снятия ФЭ и снятия входа

Пусть, далее, $\mathcal{F} \underset{t}{\rightarrow} \widehat{\mathcal{F}}$ — однократное ЭП для формул из $\mathcal{U}^{\Phi}_{\text{Б}}$, где тождество t имеет вид

$$t:\ \mathcal{F}'(x_1,\ldots,x_n) = \mathcal{F}''(x_1,\ldots,x_n),$$

а формула $\widehat{\mathcal{F}}$ получается из формулы $\mathcal{F}$ заменой подформулы $\mathcal{F}'(\mathcal{F}_1,\ldots,\mathcal{F}_n)$ формулой $\mathcal{F}''(\mathcal{F}_1,\ldots,\mathcal{F}_n)$. Сопоставим этому ЭП «моделирующее» его однократное ЭП СФЭ вида $\underline{\mathcal{F}} \underset{\underline{t}}{\rightarrow} \widehat{\Sigma}$ (см. рис. 10.3). Заметим, что в том случае, когда формулы $\mathcal{F}'$ и $\mathcal{F}''$ являются абсолютными формулами, а БП $x_1,\ldots,x_n$ — их существенными БП, СФЭ $\widehat{\Sigma}$ совпадает с СФЭ $\underline{\mathcal{F}''}$. В остальных случаях из подформулы вида $\mathcal{F}'(\mathcal{F}_1,\ldots,\mathcal{F}_n)$ формулы $\mathcal{F}$ необходимо с помощью тождеств $\tau^{\text{В}}_{\text{Б}}$ сформировать сначала подсхему $\underline{\mathcal{F}'}(\underline{\mathcal{F}}_1,\ldots,\underline{\mathcal{F}}_n)$, а затем применить тождество $\underline{t}$. При этом в СФЭ $\widehat{\Sigma}$ могут появиться висячие вершины или внутренние «ветвления» и для перехода от $\widehat{\Sigma}$ к $\widehat{\mathcal{F}}$ необходимо провести ЭП вида $\widehat{\Sigma} \underset{\{\tau^{\text{С}},\tau^{\text{В}}\}}{\rightrightarrows} \widehat{\mathcal{F}}$. Следовательно, для любого ЭП вида $\mathcal{F} \underset{\tau}{\rightrightarrows} \widehat{\mathcal{F}}$, где $\mathcal{F}, \widehat{\mathcal{F}} \in \mathcal{U}^{\Phi}_{\text{Б}}$, существует моделирующее его ЭП вида

$$\underline{\mathcal{F}} \underset{\{\underline{\tau},\tau^{\text{В}}_{\text{Б}},\tau^{\text{С}}_{\text{Б}}\}}{\rightrightarrows} \underline{\widehat{\mathcal{F}}}.$$

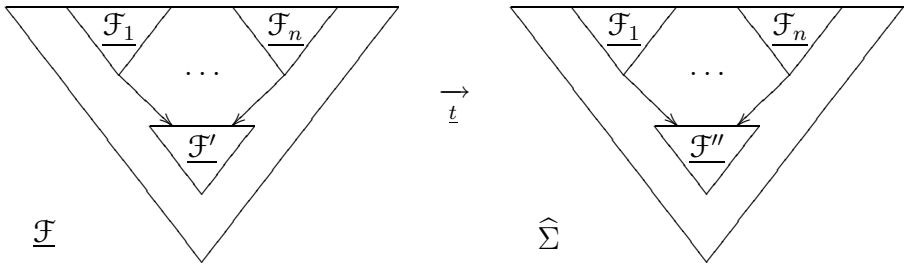


Рис. 10.3: моделирование ЭП формул с помощью ЭП СФЭ

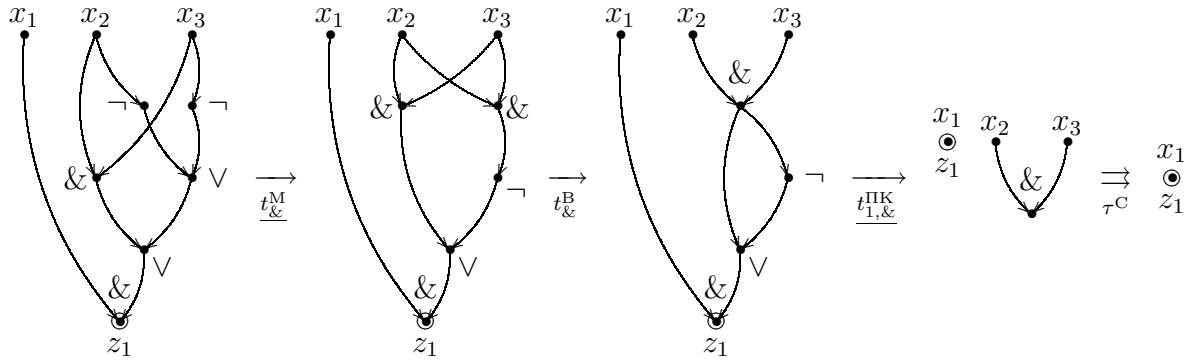


Рис. 10.4: пример моделирования ЭП формул с помощью ЭП СФЭ

На рис. 10.4 показано ЭП СФЭ из $\mathcal{U}^{\mathrm{C}}$, которое моделирует следующее ЭП для формул из $\mathcal{U}^{\Phi}$

$$x_1\left(x_2x_3 \vee \overline{x}_2 \vee \overline{x}_3\right) \underset{t^{\mathrm{M}}_{\&}}{\mapsto} x_1\left(x_2x_3 \vee \overline{x_2 \cdot x_3}\right) \underset{t^{\mathrm{ПК}}_{1,\&}}{\mapsto} x_1.$$

Из описанного выше способа «моделирования» ЭП формул с помощью ЭП СФЭ, а также способа перехода от формул к СФЭ и обратно на основе ЭП с помощью тождеств τ^{B}, τ^{C} вытекает справедливость следующего утверждения.

Теорема 10.1. *Если τ — КПСТ для ЭП формул из $\mathcal{U}^{\Phi}_{\mathrm{Б}}$, то $\left\{\underline{\tau}, \tau^{\mathrm{C}}, \tau^{\mathrm{B}}\right\}$ — КПСТ для ЭП СФЭ из $\mathcal{U}^{\mathrm{C}}_{\mathrm{Б}}$.*

Следствие. *Система тождеств $\left\{\underline{\tau^{\text{осн}}}, \tau^{\mathrm{C}}, \tau^{\mathrm{B}}\right\}$ — КПСТ для ЭП СФЭ из $\mathcal{U}^{\mathrm{C}}$.*

Рассмотрим теперь вопросы структурного моделирования формул в различных базисах. Пусть помимо базиса $\mathrm{Б} = \{\varphi_i\}_{i=1}^{b}$ у нас имеется другой конечный полный базис $\mathrm{Б}' = \{\varphi'_i\}_{i=1}^{b'}$, и пусть формула $\Phi'_i\left(x_1, \ldots, x_{k'_i}\right)$ из $\mathcal{U}^{\Phi}_{\mathrm{Б}'}$, где $k'_i \geqslant k_i$, реализует ФАЛ φ_i, $i = 1, \ldots, b$. Заметим, что в случае $k'_i > k_i$ БП $x_{k_i+1}, \ldots, x_{k'_i}$ являются фиктивными БП формулы Φ'_i и будем считать, что в случае, когда φ_i — константа

и, следовательно, $k_i = 1$, имеет место равенство $k'_i = 2$, а формула Φ'_i зависит только от БП x_2. Положим

$$\Phi' = (\Phi'_1, \ldots, \Phi'_b), \qquad \Pi' = (\Pi'_1, \ldots, \Pi'_b),$$

где Π'_i — тождество вида $\varphi_i = \Phi'_i$, $i = 1, \ldots, b$, и формулы из Φ' (тождества из Π') будем называть *формулами* (соответственно *тождествами*) *перехода от базиса* Б *к базису* Б′.

Для формулы $\mathcal{F}$, $\mathcal{F} \in \mathcal{U}^{\Phi}_{\text{Б}}$, обозначим через $\Pi'(\mathcal{F})$ формулу над базисом Б′, которая получается из $\mathcal{F}$ заменой каждой ее подформулы вида $\varphi_i(\mathcal{F}_1, \ldots, \mathcal{F}_{k_i})$ формулой $\Phi'_i\left(\mathcal{F}_1, \ldots, \mathcal{F}_{k_i}, x_{k_i+1}, \ldots, x_{k'_i}\right)$, то есть является результатом подстановки формулы $\mathcal{F}_j$ вместо БП x_j в формулу Φ'_i (см. §3 главы 1) для всех j, $j = 1, \ldots, k_i$. Переход от формулы $\mathcal{F}$ к формуле $\Pi'(\mathcal{F})$ будем называть *структурным моделированием формулы* $\mathcal{F}$ *в базисе* Б′ *на основе формул перехода* Φ' или, иначе, *на основе тождеств перехода* Π'. Заметим, что этот переход является специальным ЭП вида

$$\mathcal{F} \underset{\Pi'}{\rightrightarrows} \Pi'(\mathcal{F})$$

для формул над базисом Б∪Б′. Отсюда следует, в частности, что в результате указанного структурного моделирования обеих частей тождества t, являющихся формулами из $\mathcal{U}^{\Phi}_{\text{Б}}$, получается тождество t' для формул из $\mathcal{U}^{\Phi}_{\text{Б}'}$, которое мы будем обозначать через $\Pi'(t)$. Множество формул вида $\Pi'(\mathcal{F})$, где $\mathcal{F} \in \mathfrak{F} \subseteq \mathcal{U}^{\Phi}_{\text{Б}}$, будем обозначать через $\Pi'(\mathfrak{F})$, а множество тождеств вида $\Pi'(t)$, где $t \in \tau$ — тождество над $\mathcal{U}^{\Phi}_{\text{Б}}$, — через $\Pi'(\tau)$.

Переменная, входящая в запись формулы ровно один раз, называется *бесповторной* БП этой формулы. Формула $\mathcal{F}$ называется *бесповторной*, если все существенные БП реализуемой ею ФАЛ являются бесповторными для $\mathcal{F}$. Заметим, что абсолютная формула является бесповторной, а другие примеры бесповторных формул дают, в частности, формулы $x_1 \cdot \overline{x}_1$ и $x_2(x_1 \vee \overline{x}_1)$. Будем говорить, что базис Б допускает *бесповторное моделирование* в базисе Б′, если в $\mathcal{U}^{\Phi}_{\text{Б}'}$ существуют бесповторные формулы $\Phi'_1, \ldots, \Phi'_b$, реализующие ФАЛ $\varphi_1, \ldots, \varphi_b$ соответственно.

Лемма 10.1. *Если базис* Б *допускает бесповторное моделирование в базисе* Б′*, то для любой формулы* $\mathcal{F}$ *из* $\mathcal{U}^{\Phi}_{\text{Б}}$ *существует эквивалентная ей формула* $\mathcal{F}'$ *из* $\mathcal{U}^{\Phi}_{\text{Б}'}$*, такая, что*

$$S(\mathcal{F}') \leqslant c_1 S(\mathcal{F}), \qquad R(\mathcal{F}') \leqslant c_2 R(\mathcal{F}), \qquad D(\mathcal{F}') \leqslant c_3 D(\mathcal{F}), \tag{10.1}$$

где c_1, c_2, c_3 *— некоторые константы, зависящие только от базисов* Б, Б′.

Доказательство. Пусть $\Phi' = (\Phi'_1, \ldots, \Phi'_b)$ — система из бесповторных формул перехода от базиса Б к базису Б′, а Π' — связанная с ней система тождеств перехода, и пусть $\mathcal{F}' = \Pi'(\mathcal{F})$. Справедливость для $\mathcal{F}'$ неравенств (10.1), где c_1 и c_3 — максимальный размер и максимальная глубина формул Φ'_i соответственно, а c_2 — максимальное

отношение $k_i'/_{k_i}$, $i \in [1, b]$, докажем индукцией по $D(\mathcal{F})$. Действительно, для формул глубины 1 эти неравенства выполняются в силу выбора констант. Пусть, далее, неравенства (10.1) выполняются для любой формулы глубины не больше, чем $(d-1)$, где $d \geqslant 1$, и пусть формула $\mathcal{F}$ глубины d имеет вид

$$\mathcal{F} = \varphi_i(\mathcal{F}_1, \ldots, \mathcal{F}_{k_i}),$$

где $D(\mathcal{F}_j) \leqslant d-1$ для всех j, $j \in [1, k_i]$. Тогда

$$\mathcal{F}' = \Pi'(\mathcal{F}) = \Phi_i'\left(\mathcal{F}_1', \ldots, \mathcal{F}_{k_i}', x_{k_i+1}, \ldots, x_{k_i'}\right),$$

где $\mathcal{F}_j' = \Pi'(\mathcal{F}_j)$, $j = 1, \ldots, k_i$, и, следовательно,

$$D(\mathcal{F}') \leqslant D(\Phi_i') + c_3 \max_{1 \leqslant j \leqslant k_i} D(\mathcal{F}_j) \leqslant c_3 D(\mathcal{F}).$$

Аналогичным образом, но уже с учетом бесповторности формул перехода, доказываются неравенства (10.1) с константами c_1 и c_2 для размера и ранга формулы $\mathcal{F}'$ соответственно.

Лемма доказана. □

Замечание. Неравенство (10.1) для глубины $\mathcal{F}'$ выполняется с определенной выше константой c_3 для произвольных базисов Б′, Б.

Пусть $\text{Б}_+ = \{x_1 \oplus x_2, x_1 \cdot x_2, 1\}$, а базис Б″ получается из базиса Б_+ заменой функционального элемента, реализующего ФАЛ $x_1 \cdot x_2$, на ФЭ, реализующий функцию «голосования» $H(x_1, x_2, x_3) = x_1x_2 \vee x_2x_3 \vee x_3x_1$. Заметим, что базис Б_0 допускает бесповторное моделирование в базисе Б″. Действительно, формулы $H(x_1, x_2, y \oplus y)$, $H(x_1, x_2, 1)$ и $x \oplus 1$ являются бесповторными формулами над Б″, которые реализуют ФАЛ $x_1 \cdot x_2$, $x_1 \vee x_2$ и $\overline{x}$ соответственно. Базис Б_0 допускает бесповторное моделирование и в базисе Б_+, поскольку бесповторные формулы $x_1 \oplus 1$ и $((x_1 \oplus 1) \cdot (x_2 \oplus 1) \oplus 1)$ над Б_+ реализуют ФАЛ $\overline{x}_1$ и $x_1 \vee x_2$ соответственно. Оказывается, что базис Б_0 допускает бесповторное моделирование в любом базисе Б. Именно это означает следующее утверждение, которое вытекает, по существу, из полноты системы базисных ФАЛ $\{\varphi_i\}_{i=1}^b$ и из лемм о немонотонной и нелинейной ФАЛ (см. [6]).

Лемма 10.2. *Существуют бесповторные формулы $\mathcal{F}_\neg$, $\mathcal{F}_\&$ и $\mathcal{F}_\vee$ над базисом* Б, *которые реализуют ФАЛ $\overline{x}_1$, $x_1 \cdot x_2$ и $x_1 \vee x_2$ соответственно.*

Доказательство. В силу полноты системы ФАЛ $\{\varphi_i\}_{i=1}^b$ можно построить формулы $\mathcal{F}_0$, $\mathcal{F}_1$ от БП y над Б, которые реализуют константы 0, 1 и являются бесповторными в связи с отсутствием существенных БП. Из полноты следует также, что среди базисных ФАЛ есть немонотонная ФАЛ $\varphi'(x_1, \ldots, x_{k'})$ и нелинейная ФАЛ $\varphi''(x_1, \ldots, x_{k''})$.

В силу леммы о немонотонной ФАЛ найдется набор $(\alpha_1, \alpha_2, \ldots, \alpha_{k'})$ из $B^{k'}$ и число i, $1 \leqslant i \leqslant k'$, такие, что

$$\varphi'(\alpha_1, \ldots, \alpha_{i-1}, x_i, \alpha_{i+1}, \ldots, \alpha_{k'}) = \overline{x}_i.$$

Следовательно, формула

$$\mathcal{F}_\neg(x) = \mathcal{F}_\neg(x, y) = \varphi'\left(\mathcal{F}_{\alpha_1}, \ldots, \mathcal{F}_{\alpha_{i-1}}, x, \mathcal{F}_{\alpha_{i+1}}, \ldots, \mathcal{F}_{\alpha_{k'}}\right)$$

является бесповторной формулой над Б, реализующей ФАЛ $\overline{x}$. Положим:

$$\mathcal{F}^{(1)}_\neg(x, y) = \mathcal{F}_\neg(x) \quad \text{и} \quad \mathcal{F}^{(0)}_\neg(x, y) = x.$$

Из доказательства леммы о нелинейной ФАЛ следует, что найдется такой набор $\beta = (\beta_1, \ldots, \beta_{k''})$ из $B^{k''}$, натуральные числа i и j, $1 \leqslant i < j \leqslant k''$, а также константа γ, $\gamma \in B$, для которых

$$\varphi''(\beta_1, \ldots, \beta_{i-1}, x_i \oplus \beta_i, \beta_{i+1}, \ldots, \beta_{j-1}, x_j \oplus \beta_j, \beta_{j+1}, \ldots, \beta_{k''}) = x_i \cdot x_j \oplus \gamma.$$

Тогда формула $\mathcal{F}_\&$ вида

$$\mathcal{F}_\&(x_1, x_2, y) = \mathcal{F}^{(\gamma)}_\neg\Big(\varphi''\big(\mathcal{F}_{\beta_1}, \ldots, \mathcal{F}_{\beta_{i-1}}, \mathcal{F}^{(\beta_i)}_\neg(x_1, y), \mathcal{F}_{\beta_{i+1}}, \ldots \\ \ldots, \mathcal{F}_{\beta_{j-1}}, \mathcal{F}^{(\beta_j)}_\neg(x_2, y), \mathcal{F}_{\beta_{j+1}}, \ldots, \mathcal{F}_{\beta_{k''}}\big), y\Big)$$

является бесповторной формулой над Б и реализует ФАЛ $x_1 \cdot x_2$. Бесповторная формула $\mathcal{F}_\vee(x_1, x_2, y)$, которая реализует ФАЛ $x_1 \vee x_2$, получается из формулы

$$\mathcal{F}_\neg(\mathcal{F}_\&(\mathcal{F}_\neg(x_1, y), \mathcal{F}_\neg(x_2, y), y), y)$$

«удалением» всех вхождений двух последовательных формул $\mathcal{F}_\neg$.

Лемма доказана. □

Заметим, что базис Б_+ не допускает бесповторного моделирования в базисе Б_0, поскольку ФАЛ $x_1 \oplus x_2$ не может быть реализована в нем бесповторной формулой.

Рассмотрим теперь вопросы моделирования ЭП формул в базисе Б с помощью ЭП формул базиса Б′. Пусть $\Phi' = (\Phi'_1, \ldots, \Phi'_b)$ — система формул перехода от базиса Б к базису Б′, а $\Pi' = (\Pi'_1, \ldots, \Pi'_b)$ — система тождеств перехода, связанная с Φ'. Заметим, что любое ЭП для формул из $\mathcal{U}^\Phi_\text{Б}$, имеющее вид

$$\mathcal{F} \underset{\tau}{\rightrightarrows} \widehat{\mathcal{F}}, \tag{10.2}$$

может быть «промоделировано» с помощью ЭП для формул из $\mathcal{U}^\Phi_{\text{Б}'}$ вида

$$\mathcal{F}' \underset{\tau'}{\rightrightarrows} \widehat{\mathcal{F}}', \tag{10.3}$$

где $\mathcal{F}' = \Pi'(\mathcal{F})$, $\widehat{\mathcal{F}}' = \Pi'(\widehat{\mathcal{F}})$ и $\tau' = \Pi'(\tau)$. Действительно, пусть ЭП (10.2) является однократным ЭП на основе тождества $t,\ t \in \tau$, которое имеет вид

$$t:\ \mathfrak{A}(x_1, \ldots, x_q) = \mathfrak{B}(x_1, \ldots, x_q),$$

и пусть формула $\widehat{\mathcal{F}}$ получается в результате замены подформулы $\mathfrak{A}(\mathcal{F}_1, \ldots, \mathcal{F}_q)$ формулы $\mathcal{F}$ формулой $\mathfrak{B}(\mathcal{F}_1, \ldots, \mathcal{F}_q)$. Тогда тождество $t' = \Pi'(t)$ имеет вид

$$t':\ \mathfrak{A}'(x_1, \ldots, x_1) = \mathfrak{B}(x_1, \ldots, x_q),$$

где $\mathfrak{A}' = \Pi'(\mathfrak{A})$ и $\mathfrak{B}' = \Pi'(\mathfrak{B})$, а формула $\widehat{\mathcal{F}}'$ может быть получена из формулы $\mathcal{F}'$ в результате замены ее подформулы $\mathfrak{A}'\left(\mathcal{F}'_1, \ldots, \mathcal{F}'_q\right)$, где $\mathcal{F}'_j = \Pi'(\mathcal{F}_j)$ для всех $j,\ j \in [1, q]$, формулой $\mathfrak{B}'\left(\mathcal{F}'_1, \ldots, \mathcal{F}'_q\right)$. Моделирование кратного ЭП вида (10.2) с помощью кратного ЭП вида (10.3) осуществляется путем последовательного моделирования однократных ЭП, составляющих ЭП (10.2).

Описанное выше моделирование позволяет выполнять ЭП для тех эквивалентных формул из $\mathcal{U}^{\Phi}_{\text{Б}'}$, которые принадлежат множеству $\Pi'\left(\mathcal{U}^{\Phi}_{\text{Б}}\right)$, то есть являются «моделями» формул из $\mathcal{U}^{\Phi}_{\text{Б}}$, на основе системы тождеств $\Pi'(\tau)$, являющихся «моделями» тождеств из τ. Для того, чтобы проводить ЭП для произвольных формул из $\mathcal{U}^{\Phi}_{\text{Б}'}$ с использованием системы тождеств $\Pi'(\tau)$, выберем какую-либо систему формул перехода $\Phi = (\Phi_1, \ldots, \Phi_{b'})$ от базиса Б′ к базису Б и рассмотрим связанную с ней систему тождеств перехода $\Pi = (\Pi_1, \ldots, \Pi_{b'})$. Пусть $\check{\Pi}$ — система тождеств вида $\check{\Pi} = \Pi'(\Pi)$ для ЭП формул из $\mathcal{U}^{\Phi}_{\text{Б}'}$, которая получается в результате структурного моделирования правых чатей тождеств из Π на основе системы тождеств Π'. Для произвольной формулы $\mathcal{F}',\ \mathcal{F}' \in \mathcal{U}^{\Phi}_{\text{Б}'}$, положим

$$\check{\Pi}(\mathcal{F}') = \Pi'(\Pi(\mathcal{F}))$$

и заметим, что

$$\mathcal{F}' \underset{\check{\Pi}}{\rightrightarrows} \check{\mathcal{F}}' = \check{\Pi}(\mathcal{F}'), \quad \check{\mathcal{F}}' \in \Pi'\left(\mathcal{U}^{\Phi}_{\text{Б}}\right).$$

В силу сказанного выше отсюда вытекает справедливость следующего утверждения.

Теорема 10.2 (теорема перехода). *Пусть τ — КПСТ для ЭП формул из $\mathcal{U}^{\Phi}_{\text{Б}}$, а Π' и Π — системы тождеств для перехода от базиса* Б *к базису* Б′ *и от базиса* Б′ *к базису* Б *соответственно. Тогда система тождеств $\{\Pi'(\tau), \Pi'(\Pi)\}$ является КПСТ для ЭП формул из $\mathcal{U}^{\Phi}_{\text{Б}}$.*

Следствие. *Из системы тождеств $\tau^{\text{осн}}$ для ЭП формул из $\mathcal{U}^{\Phi}$ (см. §3 главы 1) указанным в теореме способом можно получить КПСТ для ЭП формул в любом базисе* Б.

Глава 3

Синтез и сложность управляющих систем

§1 Задача синтеза. Простейшие методы синтеза схем и оценки сложности функций

В общем виде задача синтеза состоит в построении по заданной системе функций реализующей ее схемы, которая принадлежит заданному классу и на которой достигается минимальное значение заданного функционала сложности. частным случаем этой задачи является рассмотренная в §8 главы 1 задача минимизации ДНФ. Дадим основные определения, связанные с задачей синтеза схем, и введем необходимые обозначения.

Пусть $\mathcal{U}$ — один из введенных в главе 2 классов схем, который является полным в том смысле, что каждую систему ФАЛ F можно реализовать некоторой его схемой Σ, а Ψ — какой-либо функционал сложности схем класса $\mathcal{U}$, то есть отображение $\mathcal{U}$ во множество неотрицательных действительных чисел. Будем считать, что функционал сложности Ψ обладает свойством *монотонности*, то есть $\Psi(\Sigma) \geqslant \Psi(\Sigma')$, если $\Sigma, \Sigma' \in \mathcal{U}$, и Σ' получается из Σ в результате удаления вершин или ребер (ср. с §8 гл. 1). Все введенные в главе 2 функционалы сложности этим свойством обладают. Определим сложность $\Psi(F)$ системы ФАЛ F относительно функционала Ψ в классе $\mathcal{U}$ как минимальное значение величины $\Psi(\Sigma)$ на множестве тех схем Σ из $\mathcal{U}$, которые реализуют F. При этом схема Σ, принадлежащая классу $\mathcal{U}$, которая реализует F и для которой $\Psi(\Sigma) = \Psi(F)$, называется *минимальной схемой* в классе $\mathcal{U}$ относительно функционала Ψ. Величину $\Psi(F)$ в том случае, когда функционал Ψ совпадает с введенным в главе 2 функционалом L ($\mathfrak{L}$, D, T, R, и т. д.) будем называть *сложностью* (соответственно, *размером*, *глубиной*, *задержкой*, *рангом*, и т. д.)

системы ФАЛ F. Введем функцию

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

которая, обычно, называется *функцией Шеннона для класса* $\mathcal{U}$ *относительно функционала сложности* Ψ. В дальнейшем сложность системы ФАЛ F относительно функционала Ψ для любого из введенных классов вида $\mathcal{U}_{\text{Б}}^{\text{A}}$ ($\mathcal{U}^{\text{A}}$) будем обозначать через $\Psi_{\text{Б}}^{\text{A}}(F)$ (соответственно, $\Psi^{\text{A}}(F)$), а функцию Шеннона для этого класса относительно Ψ — через $\Psi_{\text{Б}}^{\text{A}}(n)$ (соответственно, $\Psi^{\text{A}}(n)$). В обозначениях классов $\mathcal{U}_{\text{Б}}^{\text{C}}$, $\mathcal{U}_{\text{Б}}^{\Phi}$, а также связанных с ними функционалов сложности и функций Шеннона, нижний индекс Б вида Б_0 будем, как обычно, опускать.

Отметим некоторые простейшие соотношения между введенными функциями. Очевидно, что для сложностей $\Psi'(F)$ и $\Psi''(F)$ системы ФАЛ F относительно функционала Ψ в классах схем $\mathcal{U}'$ и $\mathcal{U}''$ соответственно выполняется неравенство

$$\Psi'(F) \leqslant \Psi''(F),$$

если $\mathcal{U}' \supseteq \mathcal{U}''$. В частности,

$$\Psi_{\text{Б}}^{\text{C}}(F) \leqslant \Psi_{\text{Б}}^{\Phi}(F), \qquad \Psi^{\text{K}}(F) \leqslant \Psi^{\pi}(F),$$

и т. д. Для любой СФЭ Σ, $\Sigma \in \mathcal{U}_{\text{Б}}^{\text{C}}$, которая реализует систему ФАЛ F, существует эквивалентная формула (система формул) $\mathcal{F}$, $\mathcal{F} \in \mathcal{U}_{\text{Б}}^{\Phi}$, которая состоит из формул, реализуемых на выходах Σ, и получается из Σ с помощью эквивалентных преобразований на основе тождеств τ^B в результате «поднятия» ветвлений к входам (см. §10 гл. 2). Следовательно,

$$D(\Sigma) = D(F), \qquad T(\Sigma) = T(\mathcal{F}),$$

и поэтому

$$D_{\text{Б}}^{\text{C}}(F) = D_{\text{Б}}^{\Phi}(F), \qquad T_{\text{Б}}^{\text{C}}(F) = T_{\text{Б}}^{\Phi}(F).$$

Положим:

$$D_{\text{Б}}(F) = D_{\text{Б}}^{\text{C}}(F) = D_{\text{Б}}^{\Phi}(F),$$
$$T_{\text{Б}}(F) = T_{\text{Б}}^{\text{C}}(F) = T_{\text{Б}}^{\Phi}(F),$$

и введем функции Шеннона

$$D_{\text{Б}}(n) = D_{\text{Б}}^{\text{C}}(n) = D_{\text{Б}}^{\Phi}(n),$$
$$T_{\text{Б}}(n) = T_{\text{Б}}^{\text{C}}(n) = T_{\text{Б}}^{\Phi}(n).$$

При этом для системы ФАЛ $F = (f_1, \ldots, f_m)$ будут справедливы равенства

$$D_{\text{Б}}(F) = \max_{1 \leqslant i \leqslant m} D_{\text{Б}}(f_i), \qquad T_{\text{Б}}(F) = \max_{1 \leqslant i \leqslant m} T_{\text{Б}}(f_i).$$

Заметим также, что для сложности $L(F)$ системы ФАЛ $F = (f_1, \ldots, f_m)$ в любом из рассматриваемых классов схем выполняются неравенства

$$\max_{1 \leqslant i \leqslant m} L(f_i) \leqslant L(F) \leqslant \sum_{i=1}^{m} L(f)_i.$$

Задача синтеза допускает тривиальное решение, связанное с использованием переборного алгоритма (см. §8 главы 1), который, однако, имеет большую трудоемкость и практически не применим, если число БП больше 5.

Для реализации ФАЛ и получения верхних оценок их сложности можно использовать другой простейший метод синтеза схем, основанный на моделировании совершенной ДНФ. На основе этого моделирования с учетом результатов §2 главы 2 доказывается следующее утверждение.

Лемма 1.1. *Для любой функции алгебры логики $f(x_1, \ldots, x_n)$, $f \neq 0$, существует формула $\mathcal{F}$, $\mathcal{F} \in \mathfrak{U}^{\Phi}$, и π-схема Σ, которые реализуют f, и для которых справедливы неравенства:*

$$L(\mathcal{F}) \leqslant 2n \cdot |N_f| - 1, \qquad L(\Sigma) \leqslant n\,|N_f|. \tag{1.1}$$

Следствие 1. *В соответствии с леммой 2.3 из §2 главы 2 формулу $\mathcal{F}$ можно выбрать так, что*

$$T(\mathcal{F}) \leqslant \lceil \log n + \log |N_f| \rceil + 1. \tag{1.2}$$

Следствие 2. *В силу* (1.1), (1.2) *с учетом того, что ФАЛ* 0 *можно реализовать π-схемой сложности* 2, *а также формулой из $\mathfrak{U}^{\Phi}$, имеющей сложность* 2 *и глубину* 2 *выполняются неравенства*

$$\begin{aligned} L^{\text{C}}(n) \leqslant L^{\Phi}(n) &\leqslant n \cdot 2^{n+1}, \\ D(n) &\leqslant n + \lceil \log n \rceil + 1, \\ L^{\text{K}}(n) \leqslant L^{\pi}(n) &\leqslant n \cdot 2^{n}. \end{aligned}$$

Довольно часто задачу синтеза приходится решать для следующих ФАЛ и систем ФАЛ:

1. линейной ФАЛ порядка n, то есть ФАЛ ℓ_n или ФАЛ $\overline{\ell}_n$;

2. мультиплексорной ФАЛ μ_n порядка n;

3. дешифратора Q_n (дизъюнктивного дешифратора J_n) порядка n;

4. универсальной системы $\overrightarrow{P}_2(n)$ порядка n, состоящей из всех различных ФАЛ множества $P_2(n)$, упорядоченных в соответствии с номерами их столбцов значений.

Следуя §1 главы 2, будем называть (схемным) мультиплексором, дешифратором, дизъюнктивным дешифратором и универсальным многополюсником любую схему, которая реализует соответствующую систему ФАЛ.

Примером контактного дешифратора порядка n является $(2^n, 1)$-контактное дерево, показанное на рисунке 5.4, а пример контактного мультиплексора порядка n дает π-схема, приведенная на рис. 5.7б. Заметим, что сложность схем, показанных на рис. 5.4 и 5.7б, равна $2^{n+1}-2$ и $3\cdot 2^n-2$ соответственно, причем число размыкающих контактов в каждой из них равно 2^n-1.

В результате моделирования π-схемы, показанной на 5.7б, можно построить бесповторную по информационным БП формулу (см. §5 главы 2)

$$\widetilde{\mathcal{F}}_n(x_1,\ldots,x_n,y_0,\ldots,y_{2^n-1}) = \bigvee_{\sigma_1\in B} x_1^{\sigma_1}\left(\bigvee_{\sigma_2\in B} x_2^{\sigma_2}\left(\cdots\left(\bigvee_{\sigma_n\in B} x_n^{\sigma_n} y_{\nu(\sigma_1,\ldots,\sigma_n)}\right)\cdots\right)\right),$$

которая реализует ФАЛ μ_n, имеет сложность $4\cdot 2^n-3$ и альтернирование $2n-1$. Наряду с этой формулой будем использовать для реализации мультиплексорной ФАЛ μ_n бесповторную по информационным БП формулу

$$\widehat{\mathcal{F}}_n(x_1,\ldots,x_n,y_0,\ldots,y_{2^n-1}) =$$

$$= \bigvee_{(\sigma_1,\ldots,\sigma_{n-t})\in B^{n-t}} x_1^{\sigma_1}\cdots x_{n-t}^{\sigma_{n-t}}\left(\bigvee_{(\sigma_{n-t+1},\ldots,\sigma_n)\in B^t} x_{n-t+1}^{\sigma_{n-t+1}}\cdots x_n^{\sigma_n} y_{\nu(\sigma_1,\ldots,\sigma_n)}\right),$$

где $t=\lfloor \log n\rfloor$. Заметим что альтернирование формулы $\widehat{\mathcal{F}}_n$ равно 3 и что

$$L\left(\widehat{\mathcal{F}}_n\right) \leqslant 2^n + \frac{3}{2}\left(R\left(\widehat{\mathcal{F}}_n\right) - 2^n\right) \leqslant 2^{n+2} + 3\log n\cdot 2^{n-1}, \tag{1.3}$$

поскольку вхождения адресных БП в формулу $\widehat{\mathcal{F}}_n$ с отрицаниями составляют ровно половину всех вхождений в нее этих БП.

Лемма 1.2. *Для любой ФАЛ f, $f\in P_2(n)$ и $f\neq 0$, существует π-схема Σ и формула $\mathcal{F}$, $\mathcal{F}\in\mathfrak{U}^{\Phi}$, которые реализуют f, и для которых справедливы неравенства:*

$$L(\Sigma) \leqslant 2^n + |N_f| - 2, \qquad L(\mathcal{F}) \leqslant 2^{n+1} + |N_f| - 4.$$

Доказательство. В качестве Σ можно взять π-схему, которая получается из $(1, 2^n)$-КД порядка n от БП $x_1, \ldots, x_n$, в результате удаления тех его выходов, где реализуются ЭК, не входящие в совершенную ДНФ ФАЛ f, и отождествления остальных выходов КД. Так как при удалении вершины удаляются и все инцидентные ей контакты, то

$$L(\Sigma) \leqslant 2(2^n - 1) - (2^n - |N_f|) = 2^n + |N_f| - 2.$$

Формула $\mathcal{F}$ получается в результате моделирования построенной π-схемы Σ в классе формул с поднятыми отрицаниями (см. §5 гл. 2), и поэтому

$$R(\mathcal{F}) = L(\Sigma), \qquad L(\mathcal{F}) = R(\mathcal{F}) + L^{-}(\Sigma) - 1,$$

где $L^{-}(\Sigma)$ — число размыкающих контактов в схеме Σ. Следовательно,

$$L(\mathcal{F}) \leqslant L(\Sigma) + 2^n - 2 \leqslant 2^{n+1} + |N_f| - 4,$$

так как число размыкающих контактов в КД порядка n равно $2^n - 1$.

Лемма доказана. □

Следствие.

$$L^{\pi}(n) \leqslant 2^{n+1} - 2, \tag{1.4}$$

$$L^{\Phi}(n) \leqslant 3 \cdot 2^n - 4. \tag{1.5}$$

Рассмотрим, в заключение, простейшие нижние оценки сложности ФАЛ.

Лемма 1.3. *Если ФАЛ $f(x_1, \ldots, x_n)$ существенно зависит от всех своих БП, то*

$$L^{\mathrm{C}}(f) \geqslant n - 1, \qquad L^{\mathrm{K}}(f) \geqslant n. \tag{1.6}$$

Если при этом ФАЛ f не является монотонной ФАЛ (каждая БП x_i, $i \in [1, k]$, не является ни монотонной ни инмонотонной БП ФАЛ f), то

$$L^{\mathrm{C}}(f) \geqslant n, \qquad (\textit{соответственно } L^{\mathrm{K}}(f) \geqslant n + k) \tag{1.7}$$

Доказательство. Пусть Σ — минимальная по сложности СФЭ из $\mathfrak{U}^C$ реализующая ФАЛ f и пусть $\mathcal{F}$ — каркас Σ. Из существенной зависимости ФАЛ f от БП $x_1, \ldots, x_n$ следует, что $R(\mathcal{F}) \geqslant n$, и поэтому в силу соотношений (2.4), (3.1) главы 2

$$L^{\mathrm{C}}(f) = L(\Sigma) = L(\mathcal{F}) \geqslant n - 1.$$

Если же, кроме того, ФАЛ f не является монотонной ФАЛ, то формула $\mathcal{F}$ должна содержать хотя бы один ФЭ $\neg$ и, следовательно, в силу замечания к лемме 2.1 главы 2 в указанном случае

$$L^{\mathrm{C}}(f) = L(\Sigma) = L(\mathcal{F}) \geqslant n.$$

Таким образом первые из неравенств (1.6) и (1.7) доказаны.

Пусть теперь Σ — минимальная по сложности $(1,1)$-КС, реализующая ФАЛ f. Из существенной зависимости ФАЛ f от БП x_i, $i \in [1,n]$, следует, что либо контакт вида x_i, либо контакт вида $\overline{x}_i$ встречается в КС Σ, и поэтому

$$L^{\mathrm{K}}(f) = L(\Sigma) \geqslant n.$$

Если же, кроме того, БП x_i, $i \in [1,k]$, не является ни монотонной, ни инмонотонной БП ФАЛ f, то как контакт вида x_i, так и контакт вида $\overline{x}_i$, входят в Σ и, следовательно, в данном случае

$$L^{\mathrm{K}}(f) = L(\Sigma) \geqslant n + k.$$

Лемма доказана. □

Лемма 1.4. *Для системы $F = (f_1, \ldots, f_m)$, состоящей из попарно различных ФАЛ отличных от констант (от переменных), справедливо неравенство*

$$L^{\mathrm{K}}(F) \geqslant m, \qquad (\textit{соответственно } L^{\mathrm{C}}(F) \geqslant m). \tag{1.8}$$

Доказательство. Первое из неравенств (1.8) вытекает из того, что все ФАЛ f_i, $i = 1, \ldots, m$, реализуются на попарно различных выходах СФЭ отличных от ее входов.

Пусть теперь Σ — приведенная $(1,m)$-КС, реализующая систему ФАЛ F. Из приведенности Σ и условий леммы вытекает, что Σ — связный граф с не менее чем $(m+1)$ вершиной, и поэтому

$$L(\Sigma) \geqslant |V(\Sigma)| - 1 \geqslant m.$$

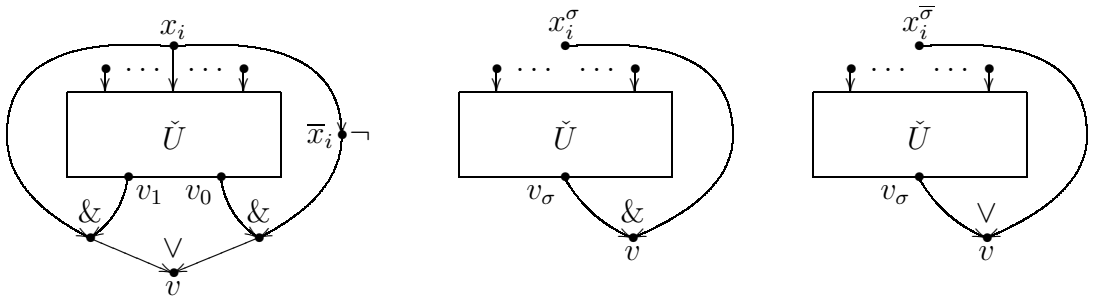
Лемма доказана. □

Следствие.

$$L^{\mathrm{C}}(Q_n) \geqslant 2^n, \qquad L^{\mathrm{K}}(Q_n) \geqslant 2^n,$$
$$L^{\mathrm{C}}(\mathfrak{J}_n) \geqslant 2^n, \qquad L^{\mathrm{K}}(\mathfrak{J}_n) \geqslant 2^n,$$
$$L^{\mathrm{C}}\left(\overrightarrow{P}_2(n)\right) \geqslant 2^{2^n} - n, \qquad L^{\mathrm{K}}\left(\overrightarrow{P}_2(n)\right) \geqslant 2^{2^n} - 2.$$

§2 Метод каскадов для контактных схем и схем из функциональных элементов. Метод Шеннона

Приведенные в §1 простейшие методы синтеза позволяют строить формулы и π-схемы, специфика которых не допускает многократного использования «промежуточных результатов». Метод каскадов [10, 9] является достаточно простым и в то же время довольно эффективным методом синтеза как КС, так и СФЭ, который позволяет это делать. Он связан с последовательным разложением заданных ФАЛ по БП и рекурсивным построением схемы, реализующей эти ФАЛ.



a) b) c)

Рис. 2.1: к описанию метода каскадов для СФЭ

Для построения соответствующей контактной схемы используется (см. §6 главы 2) операция присоединения двух противоположных контактов, которая позволяет реализовать разложение вида

$$g = \mu(x_i, g_0, g_1) = \overline{x}_i g_0 \vee x_i g_1, \tag{2.1}$$

(см. рис. 6.5a), и операция присоединения одного контакта (см. рис. 6.5b), если необходимо реализовать разложение

$$g = x_i^\sigma g_\sigma. \tag{2.2}$$

Переход от СФЭ $\check{U}$, $\check{U} \in \mathcal{U}^{\mathrm{C}}$, которая реализует в выходных вершинах v_0 и v_1 ФАЛ g_0 и g_1 соответственно, к СФЭ U, $U \in \mathcal{U}^{\mathrm{C}}$, которая реализует ФАЛ g, удовлетворяющую (2.1) ((2.2)), показан на рис. 2.1a (соответственно 2.1b).

Метод каскадов позволяет по произвольной заданной системе функций алгебры логики $F = (f_1, \ldots, f_m)$, $F \in P_2^m(n)$, строить $(1,m)$-КС Σ_F, $\Sigma_F \in \mathcal{U}^{\mathrm{K}}$, и СФЭ U_F, $U_F \in \mathcal{U}^{\mathrm{C}}$, которые реализуют F. Будем считать, что все ФАЛ $f_1, f_2, \ldots, f_m$ системы F различны, отличны от констант, и для каждой БП x_i, $1 \leqslant i \leqslant n$, среди них есть ФАЛ, существенно зависящая от x_i.

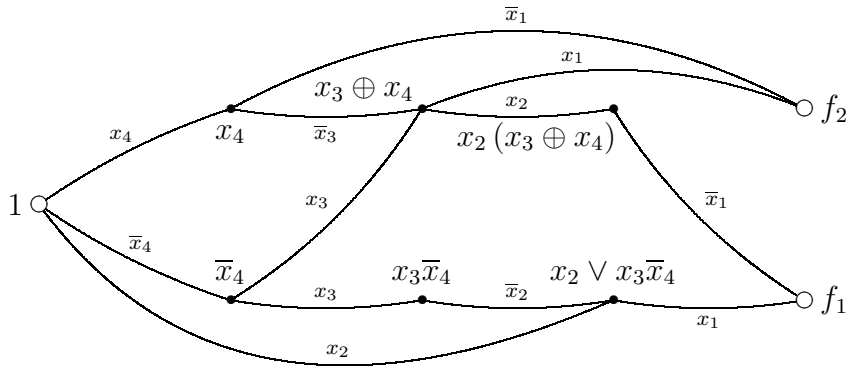


Рис. 2.2: КС для F, построенная методом каскадов, с помеченными вершинами

Разложим ФАЛ $f_1, f_2, \ldots, f_m$ сначала по БП x_1, потом по БП x_2, и так далее. При этом построим последовательности множеств G_i и $\widehat{G}_i$, состоящих из ФАЛ от БП $x_i, x_{i+1}, \ldots, x_n$, где $i = 1, 2, \ldots, n$, такие, что

1. G_i состоит из всех различных ФАЛ $g\,(x_i, \ldots, x_n)$ вида

$$g = f_j\,(\sigma_1, \ldots, \sigma_{i-1}, x_i, x_{i+1}, \ldots, x_n)\,,$$

   где $1 \leqslant j \leqslant m,\ (\sigma_1, \ldots, \sigma_{i-1}) \in B^{i-1}$;

2. $\widehat{G}_i$ состоит из всех различных функций $g,\ g \in G_i$, которые существенно зависят от x_i.

Легко видеть, что

$$G_1 = \{f_1, \ldots, f_m\}\,, \qquad \widehat{G}_n \subseteq \{x_n, \overline{x}_n\}\,,$$

а множества ФАЛ $\widehat{G}_1, \ldots, \widehat{G}_n$ не пусты и попарно не пересекаются. Положим, далее,

$$\check{G}_i = \bigcup_{j=i}^{n} \widehat{G}_j, \qquad \check{m}_i = \left|\check{G}_i\right| + 1,$$

где $i = 1, 2, \ldots, n$, и пусть

$$\widehat{G}_{n+1} = \check{G}_{n+1} = \varnothing, \qquad \check{m}_{n+1} = 1.$$

Заметим, что любую ФАЛ $g,\ g \in \widehat{G}_i$, где $1 \leqslant i \leqslant n$, можно представить в виде (2.1), где $g_\sigma = g\,(\sigma, x_{i+1}, \ldots, x_n)$, и, следовательно, $g_\sigma \in \check{G}_{i+1} \cup \{0, 1\}$ для всех $\sigma,\ \sigma \in B$. Если при этом для некоторого $\sigma,\ \sigma \in B$, ФАЛ g_σ равна 0, то вместо (2.1) будем использовать разложение (2.2), где $g_\sigma \in \check{G}_{i+1} \cup \{1\}$.

Пусть $(1,1)$-КС $\check{\Sigma}_{n+1}$ представляет собой изолированный вход, который одновременно является выходом, и реализует константу 1. Пусть, далее, для некоторого

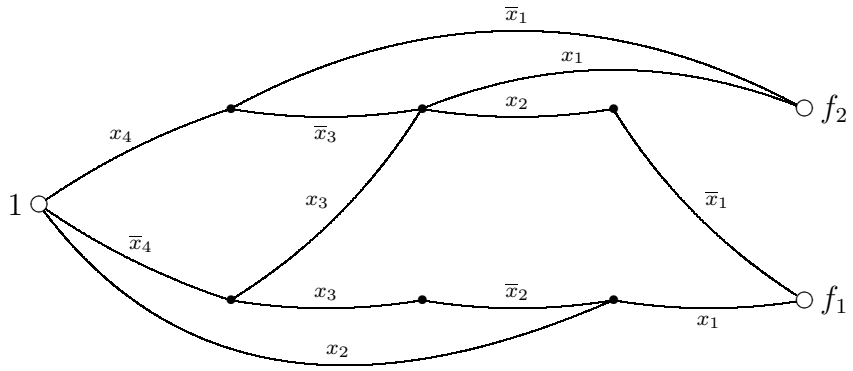


Рис. 2.3: КС для системы ФАЛ F, построенная методом каскадов

$i,\ 1 \leqslant i \leqslant n$, уже построена $(1, \check{m}_{i+1})$-КС $\check{\Sigma}_{i+1}$, реализующая систему ФАЛ $\check{G}_{i+1} \cup \{1\}$. Построим тогда $(1, \check{m}_i)$-КС $\check{\Sigma}_i$, которая реализует систему ФАЛ $\check{G}_i \bigcup \{1\}$ следующим образом:

1. КС $\check{\Sigma}_i$ содержит КС $\check{\Sigma}_{i+1}$ в качестве подсхемы, на выходах которой (они одновременно являются выходами $\check{\Sigma}_i$) реализуются ФАЛ из множества $\check{G}_{i+1} \bigcup \{1\}$;

2. Каждая ФАЛ $g,\ g \in \widehat{G}_i$, реализуется согласно (2.1) ((2.2)) на выходе v КС $\check{\Sigma}_i$, который при $\alpha = 0, 1$ (соответственно $\alpha = \sigma$) соединен контактом вида x_i^α с тем выходом v_α подсхемы $\check{\Sigma}_{i+1}$, где реализуется ФАЛ $g_\alpha = g(\alpha, x_{i+1}, \ldots, x_n)$ так, как это показано на рис. 6.5a (соответственно рис. 6.5b).

Таким образом, построенная указанным выше способом КС $\check{\Sigma}_1$ реализует систему ФАЛ $\check{G}_1 \cup \{1\}$, и для получения искомой КС Σ_F достаточно «снять» пометки с тех выходных вершин КС $\check{\Sigma}_1$, в которых реализуются ФАЛ, отличные от $f_1, \ldots, f_m$. При этом константа 1 всегда реализуется КС $\check{\Sigma}_1$, а константа 0 может быть реализована в изолированной вершине, и поэтому их включение в систему ФАЛ F не влияет на построение КС Σ_F и ее сложность. Заметим также, что если при построении КС Σ_F все контакты ориентировать по направлению от вершины v_α к вершине v (см. второй этап построения КС $\check{\Sigma}_i$), мы получим ориентированную ациклическую $(1, m)$-КС $\overrightarrow{\Sigma}_F$, которая реализует систему ФАЛ F.

Аналогичным образом по методу каскадов строится и СФЭ U_F, реализующая систему ФАЛ F, с той лишь разницей, что:

1. СФЭ $\check{U}_n$ реализует систему ФАЛ I, состоящую из БП $x_1, \ldots, x_n$, а также ФАЛ вида $\overline{x}_i,\ 1 \leqslant i \leqslant n$, которые встречаются в КС Σ_F;

2. для всех $i,\ i = (n-1), \ldots, 1$, при переходе от СФЭ $\check{U}_{i+1}$, реализующей систему ФАЛ $\check{G}_{i+1} \cup I$, к СФЭ $\check{U}_i$, реализующей систему ФАЛ $\check{G}_i \cup I$, разложение (2.1), где

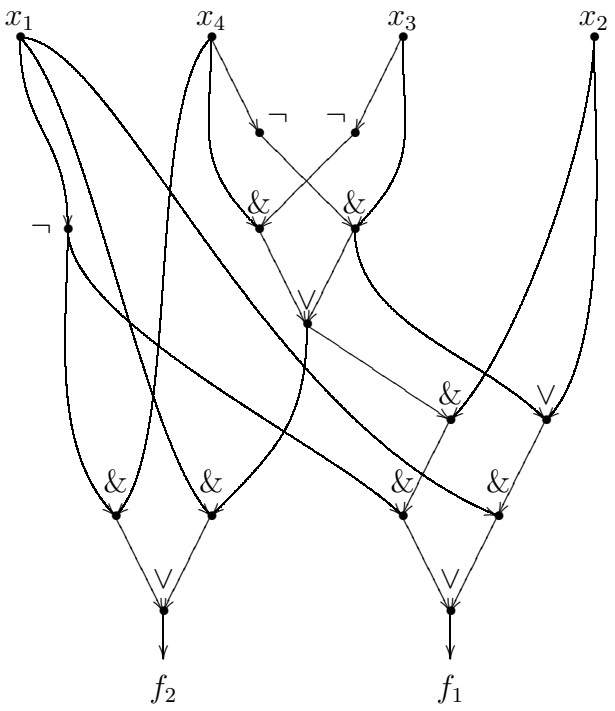


Рис. 2.4: СФЭ для системы ФАЛ F, построенная методом каскадов

$g \in \widehat{G}_i$ и $g_0, g_1 \in \check{G}_{i+1}$, реализуется так, как показано на рис. 2.1a, а разложение (2.2), применяемое в случае $g_{\overline{\sigma}} = 0$ (разложение $g = x_i^{\overline{\sigma}} \vee g_\sigma x_i^\sigma = x_i^{\overline{\sigma}} \vee g_\sigma$ в случае $g_{\overline{\sigma}} = 1$), — так, как показано на рис. 2.1b (соответственно, 2.1c);

3. каждая ФАЛ вида $g_\sigma x_i^\sigma$, используемая в предыдущем пункте при реализации разложений вида (2.1) или (2.2) для различных ФАЛ g, реализуется только один раз.

Как и в случае КС, СФЭ U_F, реализующая систему ФАЛ F и построенная по методу каскадов, получается из СФЭ $\check{U}_1$ в результате «снятия» тех выходов, в которых реализуются ФАЛ, отличные от ФАЛ из F.

Пусть теперь Σ_f — $(1,1)$-КС, построенная по методу каскадов для функции алгебры логики f, $f \in P_2(n)$, a_1 и a' — вход и выход Σ_f соответственно, а a_0 — дополнительная изолированная вершина. Рассмотрим $(1,2)$-КС $\widetilde{\Sigma}_f$ с входом a' и выходами a_0, a_1, которая строится аналогично Σ_f с той лишь разницей, что контакты ориентированы от вершины v к вершине v_α (см. второй этап построения КС $\check{\Sigma}_i$), и что при их проведении используется только разложение (2.1), а в случае, когда $g_\sigma = 0$, контакт x_i^σ идет из вершины v в вершину a_0. Нетрудно убедиться в том, что КС $\widetilde{\Sigma}_f$ является BDD (см. §7 главы 2) и реализует ФАЛ f.

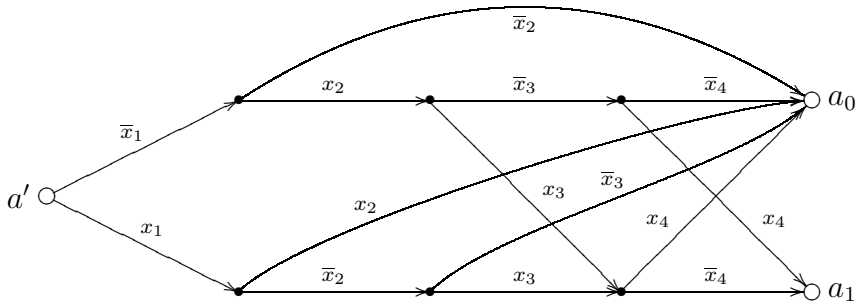


Рис. 2.5: BDD для f_1, построенная методом каскадов

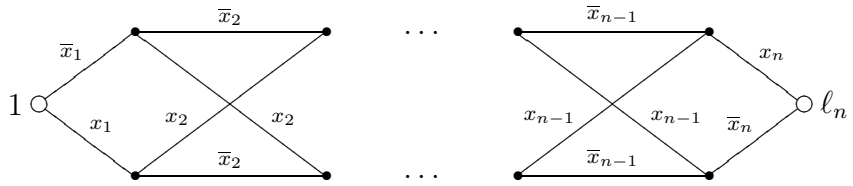


Рис. 2.6: схема Кардо для линейной функции ℓ_n

Пусть, например, $F = (f_1, f_2)$, где

$$f_1 = \overline{x}_1 x_2 (x_3 \oplus x_4) \vee x_1 (x_2 \vee x_3 \overline{x}_4),$$
$$f_2 = x_1 (x_3 \oplus x_4) \vee \overline{x}_1 x_4.$$

Тогда:

$$\widehat{G}_1 = G_1 = \{f_1, f_2\};$$
$$\widehat{G}_2 = \{x_2 (x_3 \oplus x_4), x_2 \vee x_3 \overline{x}_4\}, \qquad G_2 = \widehat{G}_2 \cup \{x_3 \oplus x_4, x_4\};$$
$$\widehat{G}_3 = \{x_3 \oplus x_4, x_3 \overline{x}_4\}, \qquad G_3 = \widehat{G}_3 \cup \{x_4\};$$
$$\widehat{G}_4 = \{x_4, \overline{x}_4\}.$$

На рис. 2.2 показана построенная для данной системы ФАЛ КС $\check{\Sigma}_1$, вершины которой помечены сопоставленными им ФАЛ, на рис. 2.3 — соответствующая ей КС Σ_F, на рис. 2.4 — строго приведенная СФЭ U_F, а на рис. 2.5 — BDD, реализующая ФАЛ f_1.

Другим примером КС, построенной по методу каскадов для линейной ФАЛ ℓ_n, где $n \geqslant 2$, является известная схема Кардо [11], показанная на рис. 2.6. Заметим, что эта КС имеет сложность $4n - 4$ и является минимальной. При построении по методу каскадов $(1, 2^n)$-КС, реализующей систему функций алгебры логики Q_n (J_n), мы получим контактное дерево (соответственно дизъюнктивное контактное дерево) порядка n, показанное на рис. 5.4 из §5 главы 2 (соответственно на рис. 2.7, где

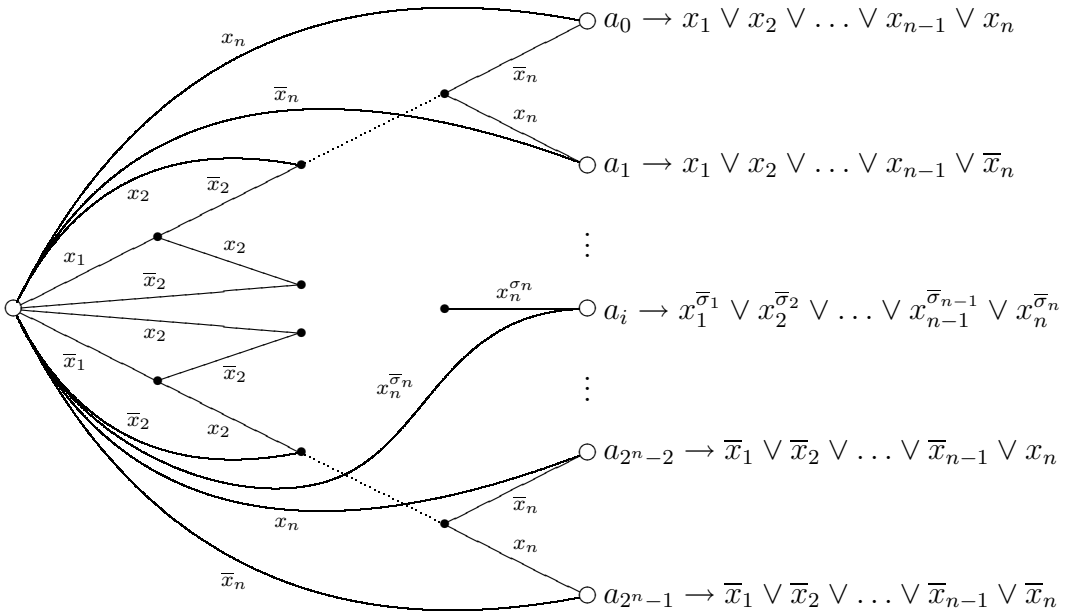


Рис. 2.7: дизъюнктное контактное дерево

$i = \nu((\sigma_1, \ldots, \sigma_n))$, $0 \leqslant i \leqslant 2^n - 1$). Как будет показано в §8, КД не является минимальным контактным дешифратором.

Аналогичным образом с помощью метода каскадов можно построить дешифратор порядка n в классе $\mathcal{U}^{\mathrm{C}}$ со сложностью $(2^{n+1} + n - 4)$, а также универсальный многополюсник в классе $\mathcal{U}^{\mathrm{C}}$ ($\mathcal{U}^{\mathrm{K}}$) сложности $2^{2^n} - n$ (соответственно не больше, чем $2 \cdot 2^{2^n}$). Суммируя все вышесказанное, приходим к следующему утверждению.

Лемма 2.1. *Для любого натурального n выполняются соотношения:*

$$L^{\mathrm{K}}(Q_n) \leqslant 2^{n+1} - 2, \qquad L^{\mathrm{C}}(Q_n) \leqslant 2^{n+1} + n - 4;$$
$$L^{\pi}(\mu_n) \leqslant 3 \cdot 2^n - 2, \qquad L^{\Phi}(\mu_n) \leqslant 2^{n+2} - 4;$$
$$L^{\mathrm{K}}\big(\overrightarrow{P}_2(n)\big) \leqslant 2 \cdot 2^{2^n}, \qquad L^{\mathrm{C}}\big(\overrightarrow{P}_2(n)\big) \leqslant 2^{2^n} - n.$$

Следствие. $L^{\mathrm{C}}\big(\overrightarrow{P}_2(n)\big) = 2^{2^n} - n.$

Рассмотрим, в заключение, метод Шеннона для синтеза КС и СФЭ (см. [12, §?], [1, §7]), который позволяет установить порядок роста функций Шеннона $L^{\mathrm{K}}(n)$ и $L^{\mathrm{C}}(n)$ (см. §3).

Метод Шеннона заключается в выборе некоторого параметра q, $1 \leqslant q \leqslant n$, и построении схемы Σ_f, реализующей произвольную ФАЛ $f(x_1, \ldots, x_n)$ на основе раз-

ложения:

$$f(x', x'') = \bigvee_{\sigma''=(\sigma_{q+1},\ldots,\sigma_n)} x_{q+1}^{\sigma_{q+1}} \cdots x_n^{\sigma_n} \cdot f_{\sigma''}(x'), \tag{2.3}$$

где $x' = (x_1, \ldots, x_q)$, $x'' = (x_{q+1}, \ldots, x_n)$, и $f_{\sigma''}(x') = f(x', \sigma'')$ при всех σ'', $\sigma'' \in B^{n-q}$. При этом схема Σ_f представляет собой корректную суперпозицию вида $\Sigma''(\Sigma')$, где Σ'' — мультиплексор порядка $(n-q)$ от адресных БП x'', информационные входы которого при выполнении указанной суперпозиции присоединяются к выходам универсального многополюсника Σ' порядка q от БП x' в соответствии с (2.3).

Полагая

$$q = \lfloor \log(n - 2\log n) \rfloor,$$

построим для ФАЛ $f(x_1, \ldots, x_n)$ указанным выше способом КС (СФЭ) Σ_f, где Σ'' — $(2^n, 1)$-КД порядка $(n-q)$ из §6 главы 2 (соответственно, формула $\mathcal{F}_{n-q}$ из §1), а Σ' — универсальный многополюсник из леммы 2.1. Корректность построенной суперпозиции в случае КС обеспечивается разделительностью КД, которая влечет за собой соотношение (6.7) из §6 главы 2. Для сложности полученной схемы Σ_f будут справедливы оценки

$$L(\Sigma_f) \leqslant 2 \cdot 2^{2^q} + 2 \cdot 2^{n-q} \leqslant \frac{2^{n+2}}{n - 2\log n} + O\left(\frac{2^n}{n^2}\right),$$

если $\Sigma_f \in \mathcal{U}^{\mathrm{K}}$, и

$$L(\Sigma_f) \leqslant 2^{2^q} + 4 \cdot 2^{n-q} \leqslant \frac{8 \cdot 2^n}{n - 2\log n} + O\left(\frac{2^n}{n^2}\right),$$

если $\Sigma_f \in \mathcal{U}^{\mathrm{C}}$. Таким образом, доказано следующее утверждение.

Теорема 2.1. *Для функций Шеннона $L^{\mathrm{K}}(n)$ и $L^{\mathrm{C}}(n)$ выполнены соотношения:*

$$L^{\mathrm{K}}(n) \lesssim 4\frac{2^n}{n}, \qquad L^{\mathrm{C}}(n) \lesssim 8\frac{2^n}{n}.$$

§3 Нижние мощностные оценки функций Шеннона

Установим ряд нижних оценок для введенных в §1 функций Шеннона. Все эти оценки получены с помощью мощностного метода, предложенного Шенноном [13], который основан на том, что число ФАЛ от БП $x_1, \ldots, x_n$ не может быть меньше числа тех попарно не эквивалентных схем, сложность которых не превосходит значения соответствующей функции Шеннона от аргумента n.

Пусть $\mathcal{U}$ — один из рассмотренных в главе 2 классов схем, L — введенный там функционал сложности, а $L(n)$ — функция Шеннона для класса $\mathcal{U}$ относительно L. Пусть, далее, $\mathcal{Q}(n)$ — некоторое множество ФАЛ из $P_2(n)$, $n = 1, 2, \ldots$, и пусть

$$L(\mathcal{Q}(n)) = \max_{f \in \mathcal{Q}(n)} L(f).$$

При этом последовательность $\mathcal{Q} = \mathcal{Q}(1), \mathcal{Q}(2), \ldots, \mathcal{Q}(n), \ldots$ будем называть *классом* ФАЛ, а функцию $L(\mathcal{Q}(n))$ — *функцией Шеннона* (для класса схем $\mathcal{U}$ относительно функционала сложности L), *связанной с классом ФАЛ* $\mathcal{Q}$. Заметим, что

$$L(\mathcal{Q}(n)) \leqslant L(n) = L(P_2(n)).$$

Обозначим через $\mathcal{U}(L, n)$ множество тех схем Σ, $\Sigma \in \mathcal{U}$ которые реализуют одну ФАЛ из $P_2(n)$, и для которых $L(\Sigma) \leqslant L$. Следующее «мощностное» неравенство вытекает непосредственно из определений:

$$\|\mathcal{U}(L(\mathcal{Q}(n)), n)\| \geqslant |\mathcal{Q}(n)|. \tag{3.1}$$

Оно позволяет получить нижнюю оценку функции Шеннона $L(\mathcal{Q}(n))$ на основе известной верхней оценки величины $\|\mathcal{U}(L, n)\|$. Заметим, что мощностные неравенства, аналогичные (3.1), имеют место и для других функционалов сложности. В частности, для функции Шеннона $D(\mathcal{Q}(n))$, связанной с реализацией ФАЛ из класса $\mathcal{Q}$ в классе схем $\mathcal{U}$ вида $\mathcal{U}_{\text{Б}}^{\text{C}}$ или $\mathcal{U}_{\text{Б}}^{\Phi}$ с оптимизацией функционала сложности D, справедливо неравенство

$$\|\mathcal{U}[T(\mathcal{Q}(n)), n]\| \geqslant |\mathcal{Q}(n)|, \tag{3.2}$$

где $\mathcal{U}[D, n]$ — множество тех схем Σ из $\mathcal{U}$, которые реализуют одну ФАЛ из $P_2(n)$ и для которых $D(\Sigma) \leqslant D$. Для множеств $\mathcal{U}(L, n)$, $\mathcal{U}[D, n]$, $\mathcal{U}\langle\mathcal{L}, n\rangle$, $\mathcal{U}\{T, n\}$, связанных с различными классами схем $\mathcal{U}$ вида $\mathcal{U}^{\text{A}}$ и $\mathcal{U}_{\text{Б}}^{\text{A}}$ будем использовать соответствующие обозначения из гл. 2

Из результатов главы 2 вытекает следующее утверждение.

Лемма 3.1. *Для каждого натурального n справедливы неравенства:*

$$\left|\mathcal{U}^{\mathrm{C}}(L,n)\right| \leqslant (32(L+n))^{L+1}, \tag{3.3}$$

$$\left|\mathcal{U}^{\Phi}(L,n)\right| \leqslant (64n)^{L+1}, \tag{3.4}$$

$$\left|\mathcal{U}^{\mathrm{K}}(L,n)\right| \leqslant (8nL)^{L}, \tag{3.5}$$

$$\left|\mathcal{U}^{\vec{\mathrm{K}}}(L,n)\right| \leqslant (16nL)^{L}, \tag{3.6}$$

$$\left|\mathcal{U}^{\mathrm{BDD}}(\mathcal{L},n)\right| \leqslant (16n(\mathcal{L}+2))^{\mathcal{L}+1}, \tag{3.7}$$

$$\left|\mathcal{U}^{\Phi}[T,n]\right| \leqslant (64n)^{2^T}. \tag{3.8}$$

Лемма 3.2. *Для $\gamma \in \{0,1\}$ и положительных действительных чисел a, α, y, q, таких, что*

$$(ay^{\gamma})^{\alpha y} \geqslant q, \tag{3.9}$$

в случае $\gamma = 1$ и $\frac{a}{\alpha}\log q > 2$ выполняется неравенство

$$y \geqslant \frac{\log q}{\alpha \log\left(\frac{a}{\alpha}\log q\right)}\left(1 + \frac{\log\log\left(\frac{a}{\alpha}\log q\right)}{\log\left(\frac{ae}{\alpha}\log q\right)}\right), \tag{3.10}$$

где e — основание натуральных логарифмов, а в случае $\gamma = 0$ и $a > 1$ — неравенство

$$y \geqslant \frac{\log q}{\alpha \log a}. \tag{3.11}$$

Доказательство. В случае $\gamma = 0$ и $a > 1$ неравенство (3.11) получается в результате логарифмирования (3.9) и деления обеих частей полученного неравенства на $\alpha \log a$.

Рассмотрим теперь случай, когда $\gamma = \alpha = a = 1$ и $\log q > 2$. В этом случае (3.10) следует из того, что левая часть (3.9) монотонно возрастает по y, и для

$$y' = (1+\varepsilon)\frac{\log q}{\log\log q}, \quad \text{где } \varepsilon = \frac{\log\log\log q}{\log(e\log q)},$$

справедливы соотношения

$$\begin{aligned} y'\log y' &= (1+\varepsilon)\frac{\log q}{\log\log q}\left(\log\log q - \log\log\log q + \log e \ln(1+\varepsilon)\right) \\ &\leqslant \log q\,(1+\varepsilon)\left(1 - \frac{\log\log\log q}{\log\log q} + \frac{\varepsilon \log e}{\log\log q}\right) \\ &= \log q\,(1+\varepsilon)(1-\varepsilon) = \log q\left(1-\varepsilon^2\right) \leqslant \log q. \end{aligned}$$

Заметим, что в случае $\gamma = 1,\ \alpha > 0,\ a > 0$ неравенство (3.9) эквивалентно неравенству

$$(ay)^{ay} \geqslant q^{\frac{a}{\alpha}},$$

и поэтому неравенство (3.10) получается из неравенства $y \geqslant y'$ в результате замены y на ay и $\log q$ на $\frac{a}{\alpha}\log q$, если выполнено условие $\frac{a}{\alpha}\log q > 2$.

Лемма доказана. □

Теорема 3.1. *Для некоторой последовательности $\varepsilon = \varepsilon(n)$, $n = 1, 2, \ldots$, такой, что $\varepsilon(n) \geqslant 0$ при $n \geqslant n_0$ и $\varepsilon(n)$ стремится к 0 при n стремящемся к бесконечности, для почти всех ФАЛ f, $f \in P_2(n)$, выполняются неравенства*

$$L^{\mathrm{C}}(f) \geqslant (1+\varepsilon(n))\frac{2^n}{n}, \tag{3.12}$$

$$L^{\Phi}(f) \geqslant (1-\varepsilon(n))\frac{2^n}{\log n}, \tag{3.13}$$

$$L^{\mathrm{K}}(f) \geqslant (1-\varepsilon(n))\frac{2^n}{n}, \tag{3.14}$$

$$L^{\vec{\mathrm{K}}}(f) \geqslant (1-\varepsilon(n))\frac{2^n}{n}, \tag{3.15}$$

$$\mathcal{L}^{\mathrm{BDD}}(f) \geqslant (1-\varepsilon(n))\frac{2^n}{n}, \tag{3.16}$$

$$D(f) \geqslant n - \log\log n - \varepsilon(n). \tag{3.17}$$

Доказательство. Пусть $\mathfrak{U}$ — один из рассматриваемых в лемме класс схем с функционалом сложности L, а $\mathfrak{Q}(n)$, $n = 1, 2, \ldots$, — такое множество ФАЛ, что

$$\mathfrak{Q}(n) \subseteq P_2(n), \qquad |\mathfrak{Q}(n)| = \left\lceil \frac{2^{2^n}}{n} \right\rceil,$$

и для любых ФАЛ g, f, где $g \in \mathfrak{Q}(n)$, $f \in P_2(n) \setminus \mathfrak{Q}(n)$, выполняется неравенство $L(g) \leqslant L(f)$. Заметим, что при этом множество ФАЛ $P_2(n) \setminus \mathfrak{Q}(n)$ содержит почти все ФАЛ из $P_2(n)$, и что для любой ФАЛ f, $f \in P_2(n) \setminus \mathfrak{Q}(n)$, справедливо неравенство

$$L(f) \geqslant L(\mathfrak{Q}(n)). \tag{3.18}$$

Связанные с классом $\mathfrak{U}$ неравенства (3.12)–(3.16) для произвольной функции алгебры логики f, $f \in P_2(n) \setminus \mathfrak{Q}(n)$, выводятся из соответствующих классу $\mathfrak{U}$ неравенств (3.3)–(3.7) на основе (3.18) и мощностной нижней оценки (3.1) для введенного класса ФАЛ $\mathfrak{Q}(n)$ с использованием леммы 3.2, где $q = |\mathfrak{Q}(n)|$, и

1) $\gamma = 1$, $\alpha = 1$, $a = 32$, $y = L + n$, если $\mathfrak{U} = \mathfrak{U}^{\mathrm{C}}$;
2) $\gamma = 0$, $\alpha = 1$, $a = 64n$, $y = L + 1$, если $\mathfrak{U} = \mathfrak{U}^{\Phi}$;
3) $\gamma = 1$, $\alpha = 1$, $a = 8n$, $y = L$, если $\mathfrak{U} = \mathfrak{U}^{\mathrm{K}}$;
4) $\gamma = 1$, $\alpha = 1$, $a = 16n$, $y = L$, если $\mathfrak{U} = \mathfrak{U}^{\vec{\mathrm{K}}}$;
5) $\gamma = 1$, $\alpha = \frac{1}{2}$, $a = 16n$, $y = \mathcal{L} + 2$, если $\mathfrak{U} = \mathfrak{U}^{\mathrm{BDD}}$.

Действительно, подставляя указанные значения в (3.10) и (3.11), получим

$$L(f) \geqslant \frac{2^n - \log n}{\alpha\left(n + \log\frac{a}{\alpha}\right)}\left(1 + \frac{\log\left(\log\left(2^n - \log n\right) + \log\frac{a}{\alpha}\right)}{n + \log\frac{a}{\alpha} + \log e}\right),$$

если $\gamma = 1$, и

$$L(f) \geqslant \frac{2^n - \log n}{\alpha \log a}$$

в остальных случаях. Следовательно, неравенство (3.12) ((3.13), (3.14), (3.15), (3.16)) будет справедливо для достаточно больших n при $\varepsilon(n) = \frac{\log n - 6}{n}$ (соответственно $\varepsilon(n) = \frac{7}{\log n}$, $\varepsilon(n) = \frac{4}{n}$, $\varepsilon(n) = \frac{8}{n}$, $\varepsilon(n) = \frac{12}{n}$).

Для доказательства неравенства (3.17) аналогичным образом вводится функциональный класс $\mathfrak{Q}(n)$, состоящий из $\left\lceil \frac{2^{2^n}}{n} \right\rceil$ функций алгебры логики множества $P_2(n)$ с наименьшей глубиной , а затем на основе (3.8) с использованием леммы 3.2, где $q = |\mathfrak{Q}(n)|$, $y = 2^T$, $\gamma = 0$, $\alpha = 1$, и $a = 64n$, устанавливается справедливость (3.17) при $\varepsilon(n) = \frac{12}{\log n}$.

Теорема доказана. □

Следствие.

$$L^{\mathrm{C}}(n) \gtrsim \frac{2^n}{n}, \qquad L^{\Phi}(n) \gtrsim \frac{2^n}{\log n}, \qquad L^{\mathrm{K}}(n) \gtrsim \frac{2^n}{n},$$
$$L^{\overrightarrow{\mathrm{K}}}(n) \gtrsim \frac{2^n}{n}, \qquad L^{\mathrm{BDD}}(n) \gtrsim \frac{2^{n+1}}{n}, \qquad T(n) \geqslant n - \log\log n - o(1).$$

Рассмотрим теперь аналогичные нижние оценки для СФЭ и формул в произвольном базисе Б. Следующее утверждение доказывается на основе леммы 4.1 и теоремы 4.1 из §4 главы 2 и мощностных неравенств (3.1), (3.2) аналогично тому, как доказывалась теорема 3.1.

Теорема 3.2. *Для некоторой последовательности $\varepsilon = \varepsilon(n)$, $n = 1, 2, \ldots$, такой, что $\varepsilon(n) \geqslant 0$ при $n \geqslant n_0$ и $\varepsilon(n)$ стремится к 0 при n стремящемся к бесконечности, для почти всех ФАЛ f, $f \in P_2(n)$, выполняются неравенства*

$$L^{\mathrm{C}}_{\mathrm{Б}}(f) \geqslant \rho_{\mathrm{Б}} \frac{2^n}{n}(1 + \varepsilon(n)), \tag{3.19}$$

$$L^{\Phi}_{\mathrm{Б}}(f) \geqslant \rho_{\mathrm{Б}} \frac{2^n}{\log n}(1 - \varepsilon(n)), \tag{3.20}$$

$$T_{\mathrm{Б}}(f) \geqslant \tau_{\mathrm{Б}}(n - \log\log n - \varepsilon(n)). \tag{3.21}$$

Следствие.

$$L^{\mathrm{C}}_{\mathrm{Б}}(n) \gtrsim \rho_{\mathrm{Б}} \frac{2^n}{n}, \qquad L^{\Phi}_{\mathrm{Б}}(n) \gtrsim \rho_{\mathrm{Б}} \frac{2^n}{\log n}, \qquad T_{\mathrm{Б}}(n) \geqslant \tau_{\mathrm{Б}}(n - \log\log n - o(1)).$$

§4 Дизъюнктивно-универсальные множества функций. Асимптотически наилучший метод О. Б. Лупанова для синтеза схем из функциональных элементов в базисе $\{\&, \vee, \neg\}$

Рассмотрим метод синтеза схем из класса $\mathcal{U}^{\mathrm{C}}$, который был предложен О.Б. Лупановым [] и позволил впервые установить асимптотику функции Шеннона $L^{\mathrm{C}}(n)$. Этот метод, как и метод Шеннона (см. §2), основан на представлении реализуемой ФАЛ $f,\ f \in P_2(n)$, в виде (2.3) и построении искомой СФЭ Σ_f, реализующей ФАЛ f, как суперпозиции схем вида $\Sigma_f = \Sigma''(\Sigma')$. При этом схема Σ'' по-прежнему является мультиплексором порядка $(n-q)$ от адресных БП $x'' = (x_{q+1}, \ldots, x_n)$, а схема Σ' реализует все ФАЛ вида $f_{\sigma''}(x')$, где $x' = (x_1, \ldots, x_q)$, $\sigma'' \in B^{n-q}$, и $f_{\sigma''}(x') = f(x', \sigma'')$. Однако, в отличие от метода Шеннона, каждая ФАЛ $f_{\sigma''}(x')$ берется не с выхода универсального многополюсника от БП x', а реализуется на выходе Σ' как дизъюнкция некоторых ФАЛ, выбранных из специального множества $G,\ G \subseteq P_2(q)$, реализованного на выходах соответствующей подсхемы схемы Σ'.

Множество ФАЛ $G,\ G \subseteq P_2(m)$, называется *дизъюнктивно-универсальным множеством (ДУМ) порядка m и ранга p*, если любая ФАЛ $g,\ g \in P_2(m)$, может быть представлена в виде

$$g = g_1 \vee \ldots \vee g_p,$$

где $g_i \in G$ при всех $i,\ i = 1, \ldots, p$. Стандартный способ построения таких множеств связан с разбиениями единичного куба.

Пусть $\Pi = (\pi_1, \ldots, \pi_p)$ — разбиение куба B^m, и пусть для всех $i,\ i = 1, \ldots, p$, ФАЛ $\chi_i(x_1, \ldots, x_m)$ — характеристическая ФАЛ множества π_i, а $G^{(i)}$ — множество всех тех ФАЛ $g,\ g \in P_2(m)$, которые обращаются в 0 вне π_i. Заметим, что множество ФАЛ G вида

$$G = G^{(1)} \cup \ldots \cup G^{(p)}$$

является ДУМ порядка m и ранга p. Действительно, любая ФАЛ $g,\ g \in P_2(m)$, может быть представлена в виде

$$g = g_1 \vee \ldots \vee g_p, \tag{4.1}$$

где $g_i = \chi_i g$ и, следовательно, $g_i \in G^{(i)}$ для всех $i,\ i = 1, \ldots, p$. Заметим также, что мощность множества $G^{(i)},\ i = 1, \ldots, p$, равна 2^{s_i}, где $s_i = |\pi_i|$, и что множество $G^{(i)} \cap G^{(j)}$ состоит из ФАЛ, тождественно равной 0, если $1 \leqslant i < j \leqslant p$. Следовательно,

$$\lambda = |G| = \sum_{i=1}^{p} \left|G^{(i)}\right| - (p-1) \leqslant \sum_{i=1}^{p} 2^{s_i} \leqslant p2^s, \tag{4.2}$$

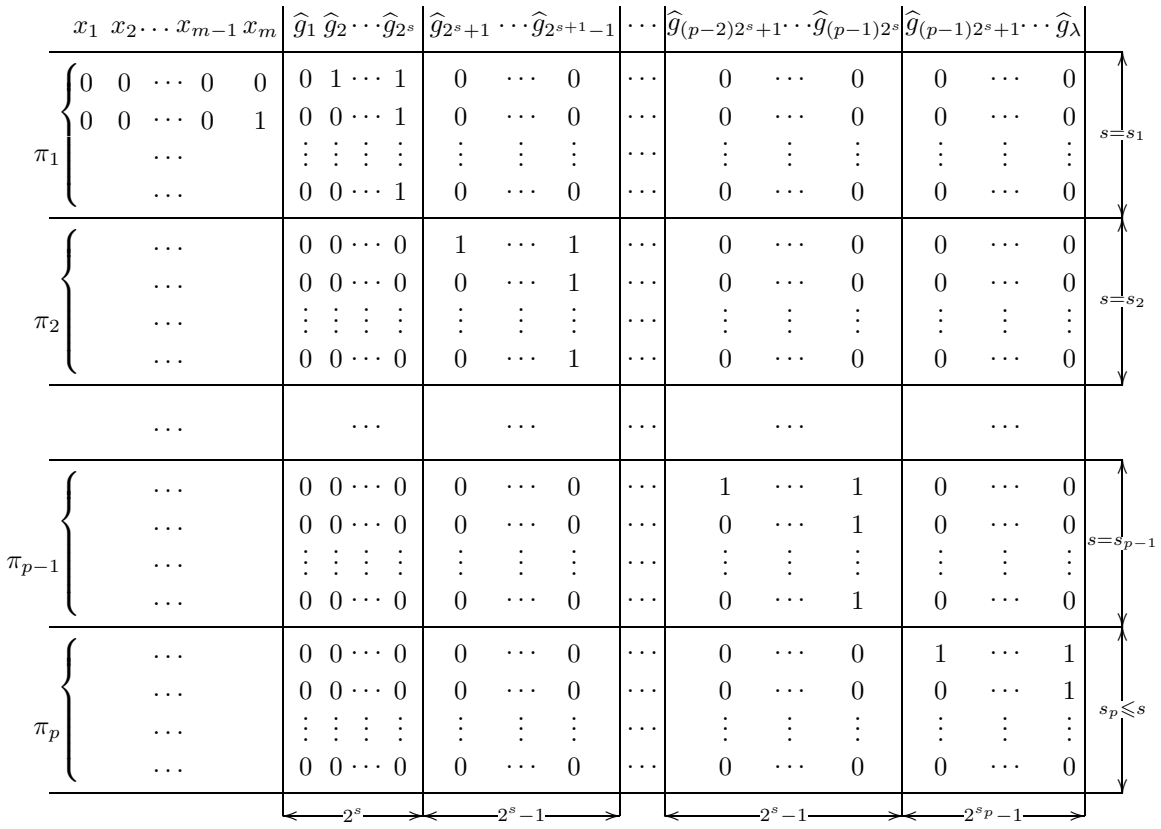


Рис. 4.1: к определению дизъюнктивно-универсального множества

где

$$s = \max_{1 \leqslant i \leqslant p} s_i.$$

В дальнейшем, на протяжении §4–§7, будем считать, что для произвольного разбиения $\Pi = (\pi_1, \dots, \pi_p)$ куба B^m, где $p \geqslant m$, от БП $(x_1, \dots, x_m)$ номер любого набора из множества π_i меньше номера любого набора из множества π_j, если $i < j$. Компоненты разбиения Π будем при этом называть *полосами* куба B^m. Кроме того, будем предполагать, что для

$$s \leqslant 2^m, \qquad p = \left\lceil \frac{2^m}{s} \right\rceil \tag{4.3}$$

выполнены соотношения

$$s_1 = s_2 = \dots = s_{p-1} = s, \quad s_p = 2^m - (p-1)\, s \leqslant s. \tag{4.4}$$

С этим разбиением будем связывать введенные выше обозначения $G,\ \lambda$ и $G^{(i)},\ \chi_i,\ s_i$, где $i = 1, \ldots, p$, а через $\overrightarrow{G}$ будем обозначать набор $(\widehat{g}_1, \ldots, \widehat{g}_\lambda)$ из $P_2^\lambda(q)$, который состоит из всех различных ФАЛ множества G, упорядоченных в соответствии с номерами их столбцов значений (см. рис. 4.1).

Заметим, что значения параметров s и m, которые однозначно определяют все введенные выше величины, будут выбираться в каждом параграфе по-своему.

Теорема 4.1. *Для функции Шеннона $L^{\mathrm{C}}(n)$ выполнено неравенство*

$$L^{\mathrm{C}}(n) \leqslant \frac{2^n}{n}\left(1 + \frac{5\log n + O(1)}{n}\right). \tag{4.5}$$

Доказательство. Возьмем произвольную функцию алгебры логики $f,\ f \in P_2(n)$, и построим СФЭ $\Sigma_f,\ \Sigma_f \in \mathcal{U}^{\mathrm{C}}$, которая реализует f и удовлетворяет (4.5). Пусть $m = q$, и пусть $x' = (x_1, \ldots, x_q),\ x'' = (x_{q+1}, \ldots, x_n)$, и $f_{\sigma''}(x') = f(x', \sigma'')$ для всех σ'' из B^{n-q}. Пусть, далее, Σ'' — мультиплексор порядка $(n-q)$ от адресных БП x'' и информационных БП $y = (y_0, \ldots, y_{2^{n-q}-1})$, который построен в соответствии с леммой 2.1 и реализует мультиплексорную ФАЛ $\mu_{n-q}(x'', y)$. Обозначим через Σ_G СФЭ, которая реализует систему ФАЛ $\overrightarrow{G}$ и представляет собой объединение схем, построенной для каждой из них в соответствии с леммой 1.2. Заметим, что в силу леммы 2.1, (1.5) и (4.2) выполнены неравенства

$$L(\Sigma'') \leqslant 4 \cdot 2^{n-q}, \qquad L(\Sigma_G) \leqslant 3p2^{s+q}. \tag{4.6}$$

Схема Σ' содержит СФЭ Σ_G в качестве подсхемы и реализует каждую ФАЛ $f_{\sigma''}(x')$, где $\sigma'' \in B^{n-q}$, на одном из своих выходов как ФАЛ $g(x')$ вида (4.1) с помощью СФЭ из $(p-1)$ ФЭ $\vee$, входы которой присоединены к соответствующим выходам Σ_G. Искомая СФЭ Σ_f имеет вид $\Sigma_f = \Sigma''(\Sigma')$ и реализует ФАЛ f в соответствии с разложением (2.3). Для нее в силу (4.6) будут выполняться неравенства

$$L(\Sigma_f) \leqslant 2^{n-q}(p-1) + L(\Sigma'') + L(\Sigma_G) \leqslant 2^{n-q}(p-1) + 4 \cdot 2^{n-q} + 3p2^{s+q},$$

и, следовательно, при

$$s = \lceil n - 5\log n \rceil, \qquad q = \lceil 2\log n \rceil$$

в соответствии с (4.3) будет справедливо соотношение

$$L(\Sigma_f) \leqslant \frac{2^n}{n - 5\log n} + O\left(\frac{2^n}{n^2}\right), \tag{4.7}$$

из которого вытекает (4.5).

Теорема доказана. □

Следствие. *Из* (4.5) *и* (3.12) *(см. также следствие из теоремы 3.1) вытекает, что*

$$L^{\mathrm{C}}(n) \sim \frac{2^n}{n}.$$

Замечание. При разложении ФАЛ из G по БП x_q получится не более, чем $2p2^{\frac{s+1}{2}}$, различных ФАЛ из $P_2(q-1)$, каждую из которых можно реализовать по методу каскадов (см. §2) со сложностью не больше, чем $3 \cdot 2^{q-1}$. Следовательно, сложность СФЭ, реализующей систему ФАЛ $\overrightarrow{G}$ по методу каскадов при их разложении по БП $x_q, x_{q-1}, \ldots, x_1$, не больше, чем

$$3p \cdot 2^s + O\left(p2^{q+\frac{s}{2}}\right).$$

Используя эту схему вместо СФЭ Σ_G и выбирая значения параметров так, что

$$s = \lceil n - 3\log n \rceil, \qquad q = \lceil 2\log n \rceil,$$

можно получить СФЭ $\check{\Sigma}_f$, которая реализует f со сложностью

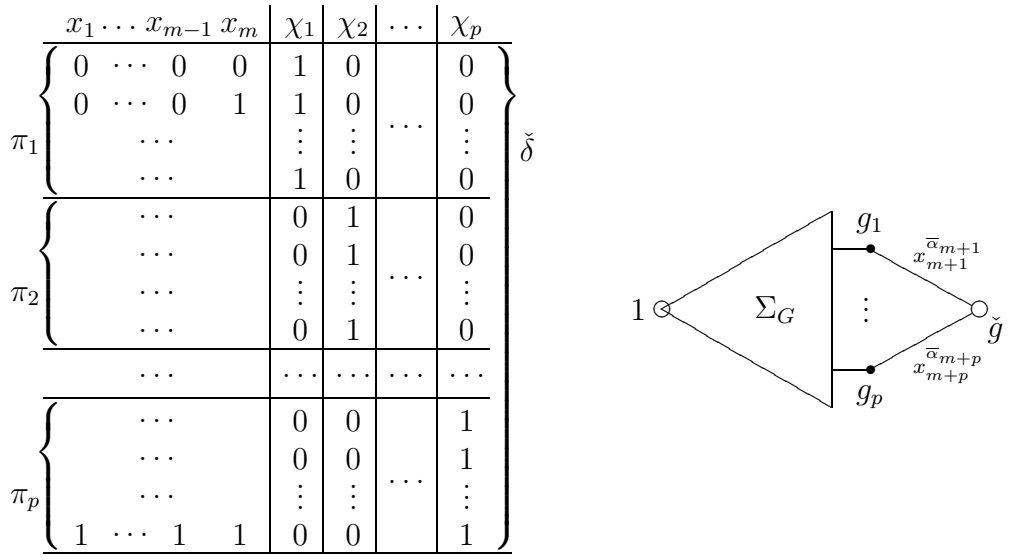
$$L\left(\check{\Sigma}_f\right) \leqslant \frac{2^n}{n}\left(1 + \frac{3\log n + O(1)}{n}\right).$$

§5 Регулярные сдвиговые разбиения единичного куба и связанные с ними разложения функций

Построенное в §4 для синтеза СФЭ ДУМ G будем использовать и далее (см. §6), хотя прямая реализация представления (4.1) в других классах схем не всегда возможна. Так, при синтезе КС (формул) часть ФАЛ (соответственно все ФАЛ) множества G должны быть «промоделированы» переменными или их отрицаниями. Для реализации такого моделирования в данном параграфе строятся специальные разбиения единичного куба, а затем рассматриваются связанные с ними разложения ФАЛ.

Множество δ, $\delta \subseteq B^q$, называется *m-регулярным* множеством наборов куба B^q, если $m < q$, $|\delta| = 2^m$, и все префиксы[1] длины m наборов из δ различны. Заметим, что m-регулярному множеству δ, $\delta \subseteq B^q$, можно взаимнооднозначно сопоставить систему ФАЛ $\psi = (\psi_1, \ldots, \psi_{q-m})$ из $P_2^{q-m}(m)$ так, что набор $\alpha = (\beta, \gamma)$, где $\beta \in B^m$ и $\gamma \in B^{q-m}$, принадлежит δ тогда и только тогда, когда $\psi(\beta) = \gamma$. Так, строки таблицы, показанной на рис. 4.1, образуют m-регулярное множество $\widehat{\delta}$ наборов куба $B^{m+\lambda}$, которое соответствует системе ФАЛ $\overrightarrow{G}$, а строки таблицы, показанной на

[1] Для слова (набора) α вида $\alpha = \beta\gamma$ слово β (γ) считается его *префиксом* (соответственно, *суффиксом*).



a) b)

Рис. 5.1: m-регулярное множество и связанная с ним суперпозиция

рис. 5.1a, — m-регулярное множество наборов $\check{\delta},\ \check{\delta} \subseteq B^{m+p}$, соответствующее системе ФАЛ $\overrightarrow{\chi} = (\chi_1, \dots, \chi_p)$. Заметим также, что любая ФАЛ $g,\ g \in P_2(q)$, совпадает на m-регулярном множестве наборов $\delta,\ \delta \subseteq B^m$, с некоторой ФАЛ из $P_2(m)$, если рассматривать $P_2(m)$ как множество всех ФАЛ из $P_2(q)$ с несущественными БП $x_{m+1}, \dots, x_q$. При этом любая ФАЛ из связанной с δ системы функций совпадает на δ с соответствующей БП куба B^q.

Для наборов $\beta = (\beta_1, \dots, \beta_q)$ и $\alpha = (\alpha_1, \dots, \alpha_q)$ через $\beta \oplus \alpha$ будем обозначать набор вида $(\beta_1 \oplus \alpha_1, \dots, \beta_q \oplus \alpha_q)$. Для множества $\delta,\ \delta \subseteq B^q$, и набора $\alpha,\ \alpha \in B^q$, определим множество $\delta \oplus \alpha$ как множество различных наборов вида $\beta \oplus \alpha$, где $\beta \in \delta$, то есть множество, получающееся из множества δ сдвигом (параллельным переносом) на набор α. Заметим, что для m-регулярного множества $\delta,\ \delta \subseteq B^q$, и любого набора $\alpha,\ \alpha \in B^q$, множество $\delta \oplus \alpha$ также является m-регулярным. Если при этом $\nu(\alpha) < 2^{q-m}$, то есть

$$\alpha = \left(\underbrace{0, ..., 0}_{m}, \gamma \right),$$

где $\gamma = (\gamma_1, \dots, \gamma_{q-m})$, и $\nu(\gamma) = \nu(\alpha)$, а множество наборов δ соответствует системе ФАЛ $\psi = (\psi_1, \dots, \psi_{q-m})$, то множество наборов $\delta \oplus \alpha$ будет соответствовать системе ФАЛ $(\psi_1 \oplus \gamma_1, \dots, \psi_{q-m} \oplus \gamma_{q-m})$, получающейся из системы ψ инвертированием некоторых ФАЛ.

В частности, для определенного выше множества $\widehat{\delta},\ \widehat{\delta} \subseteq B^{m+\lambda}$, из свойств ДУМ G и m-регулярности $\widehat{\delta}$ следует, что любая ФАЛ из $P_2(m+\lambda)$ совпадает на любом множестве $\widehat{\delta} \oplus \alpha$, где $\alpha \in B^{m+\lambda}$ и $\nu(\alpha) < 2^{\lambda}$, с некоторой ЭД ранга p от БП $x_{m+1}, \ldots, x_q$.

Аналогичным образом, любая ФАЛ $g,\ g \in P_2(m+p)$, на любом множестве наборов $\check{\delta} \oplus \alpha$, где

$$\alpha = \left(\underbrace{0, \ldots, 0}_{m}, \alpha_{m+1}, \ldots, \alpha_{m+p} \right),$$

совпадает с ФАЛ вида

$$\check{g} = x_{m+1}^{\overline{\alpha}_{m+1}} \cdot g_1 \vee \ldots \vee x_{m+p}^{\overline{\alpha}_{m+p}} \cdot g_p, \tag{5.1}$$

где $g_i = g\chi_i \in G^{(i)},\ i = 1, \ldots, p$. При этом ФАЛ $\check{g}$ может быть реализована в результате операции присоединения звезды из контактов вида $x_{m+1}^{\overline{\alpha}_{m+1}}, \ldots, x_{m+p}^{\overline{\alpha}_{m+p}}$ к выходам $(1, \lambda)$-КС Σ_G, реализующей систему ФАЛ $\overrightarrow{G}$, так, как это показано на рис. 5.1b. Заметим, что указанная операция суперпозиции является корректной на множестве наборов $\check{\delta} \oplus \alpha$ в силу разделительности присоединяемой $(p, 1)$-КС на этом множестве.

Лемма 5.1. *Для любого m-регулярного множества наборов $\delta,\ \delta \subseteq B^q$, система множеств $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$, где $\delta_i = \delta \oplus \alpha$ и $\nu(\alpha) = i-1$ при всех $i,\ i = 1, \ldots, 2^{q-m}$, образует разбиение куба B^q.*

Доказательство. Докажем сначала, что Δ — покрытие куба B^q. Для этого возьмем произвольный набор из B^q вида (β, γ), где $\beta \in B^m$ и $\gamma \in B^{q-m}$, а по нему найдем во множестве δ набор вида $(\beta, \widehat{\gamma})$, который имеется в δ в силу m-регулярности этого множества. Следовательно,

$$(\beta, \gamma) = (\beta, \widehat{\gamma}) \oplus \left(\underbrace{0, \ldots, 0}_{m}, \widehat{\gamma} \oplus \gamma \right) = (\beta, \widehat{\gamma}) \oplus \alpha,$$

где $\nu(\alpha) < 2^{q-m}$. Таким образом, система Δ образует покрытие куба B^m.

С другой стороны, из m-регулярности δ следует m-регулярность любого из множеств $\delta_i,\ i = 1, \ldots, 2^{q-m}$, и поэтому

$$\sum_{i=1}^{2^{q-m}} |\delta_i| = 2^m 2^{q-m} = 2^q.$$

Следовательно, система Δ образует разбиение куба B^q.

Лемма доказана. □

Замечание. Если $q \geqslant m + ar$, и множество δ соответствует системе ФАЛ

$$\left(\underbrace{\psi, \ldots, \psi}_{a}\right),$$

где $\psi = (\psi_1, \ldots, \psi_r) \in P_2^r(q)$, то число тех компонент разбиения Δ, на которых каждая ФАЛ системы ψ совпадает с некоторой БП куба B^q, не меньше, чем

$$\left(1 - \frac{r}{2^a}\right) 2^{q-m}.$$

Действительно, для любого фиксированного j, $1 \leqslant j \leqslant r$, доля тех компонент δ_i, $1 \leqslant i \leqslant 2^{q-m}$, разбиения Δ, на которых ФАЛ ψ_j не совпадает ни с одной из БП куба B^q, не больше, чем $\frac{1}{2^a}$. Следовательно, доля тех компонент разбиения Δ, на которых хотя бы одна из ФАЛ системы ψ не совпадает ни с одной из БП куба B^q, не больше, чем $\frac{r}{2^a}$.

В §6 мы будем выбирать параметр m так, что

$$m < q \leqslant n, \tag{5.2}$$

и будем рассматривать разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q от БП $x' = (x_1, \ldots, x_q)$, построенное по лемме 5.1 для некоторого m-регулярного множества наборов $\delta = \delta_0$. При этом для произвольной ФАЛ $f(x)$ из $P_2(n)$, где $x = (x_1, \ldots, x_n)$, вместо разложения f по БП набора $x'' = (x_{q+1}, \ldots, x_n)$ (см. (2.3)) будем рассматривать ее представление в виде

$$f(x) = \bigvee_{\sigma''=(\sigma_{q+1},\ldots,\sigma_n)} x_{q+1}^{\sigma_{q+1}} \cdots x_n^{\sigma_n} \left(\bigvee_{i=1}^{2^{q-m}} \chi_i'(x') f_{\sigma'',i}(x')\right)$$
$$= \bigvee_{i=1}^{2^{q-m}} \chi_i'(x') \left(\bigvee_{\sigma''=(\sigma_{q+1},\ldots,\sigma_n)} x_{q+1}^{\sigma_{q+1}} \cdots x_n^{\sigma_n} f_{\sigma'',i}(x')\right) = \bigvee_{i=1}^{2^{q-m}} f_i, \tag{5.3}$$

где $\chi_i'(x')$ — характеристическая ФАЛ множества δ_i, $i = 1, \ldots, 2^{q-m}$, $f_{\sigma'',i}(x')$ — произвольная ФАЛ, совпадающая на δ_i с ФАЛ $f_{\sigma''}(x') = f(x', \sigma'')$, и

$$f_i(x', x'') = \chi_i(x') \left(\bigvee_{\sigma''=(\sigma_{q+1},\ldots,\sigma_n)} x_{q+1}^{\sigma_{q+1}} \cdots x_n^{\sigma_n} f_{\sigma''}(x')\right). \tag{5.4}$$

§6 Асимптотически наилучший метод синтеза контактных схем и формул в базисе $\&, \vee, \neg$

Для синтеза КС (формул) будем использовать представления (5.3)–(5.4), где $q = m + \lambda$ (соответственно $q = m + p$), а разбиение Δ куба B^q построено по лемме 5.1 для определенного выше множества наборов $\check{\delta}$ (соответственно $\widehat{\delta}$), и, следовательно, ФАЛ $f_{\sigma'',i}(x')$ представляет собой ФАЛ $\check{g}_{\sigma'',i}$ вида (5.1) (соответственно ЭД $J_{\sigma'',i}$ от БП $x_{m+1}, \ldots, x_q$).

Теорема 6.1. *Для функции Шеннона $L^{\mathrm{K}}(n)$ выполнено неравенство*

$$L^{\mathrm{K}}(n) \leqslant \frac{2^n}{n}\left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right). \tag{6.1}$$

Доказательство. Для произвольной ФАЛ f, $f \in P_2(n)$, построим $(1,1)$-КС Σ_f, которая реализует f со сложностью, удовлетворяющей (6.1). Пусть $q = m + p$, $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ — описанное выше разбиение куба B^q, а Σ_G — $(1,\lambda)$-КС, которая реализует систему ФАЛ $\overrightarrow{G}$ по их совершенным ДНФ на основе контактного дерева (см. лемму 1.2 и оценку (1.4)). Для каждого i, $i = 1, \ldots, 2^{q-m}$, построим $(1, 2^{n-q})$-КС Σ'_i, которая содержит КС Σ_G в качестве подсхемы и реализует каждую ФАЛ $f_{\sigma'',i}(x')$, $\sigma'' \in B^{n-q}$, из разложений (5.4) как ФАЛ $\check{g}_{\sigma'',i}$ вида (5.1) в соответствии с рис. 5.1b. Заметим, что при этом

$$L(\Sigma_G) \leqslant \lambda 2^{m+1}, \tag{6.2}$$

$$L(\Sigma'_i) \leqslant L(\Sigma_G) + p2^{n-q}. \tag{6.3}$$

Пусть, далее, КС Σ_i, $i = 1, \ldots, 2^{q-m}$, реализует ФАЛ f_i (см. (5.4)) в результате корректной суперпозиции, показанной на рис. 6.1a, где $\check{\Sigma}_i$ — $(1,1)$-КС, реализующая ФАЛ χ'_i по ее совершенной ДНФ, а входы $(2^{n-q}, 1)$-КД Σ'' от управляющих БП набора x'' присоединены к выходам Σ'_i в соответствии с (5.4). Заметим, что при этом

$$L(\Sigma_i) \leqslant L(\Sigma'_i) + 2^{n-q+1} + q2^m. \tag{6.4}$$

Пусть, наконец, Σ_f — $(1,1)$-КС, которая получается в результате параллельного соединения схем $\Sigma_1, \ldots, \Sigma_{2^{q-m}}$, которая реализует f в соответствии с (5.3), и для которой в силу (6.2)–(6.4) будет выполнено неравенство

$$L(\Sigma_f) \leqslant \left((p+2)\,2^{n-q} + (\lambda+q)\,2^{m+1}\right)2^{q-m}. \tag{6.5}$$

Из этого неравенства при $q = m + p$ и

$$m = \left\lfloor \frac{3}{2}\log n \right\rfloor, \qquad s = \lceil n - 2\sqrt{n} \rceil$$

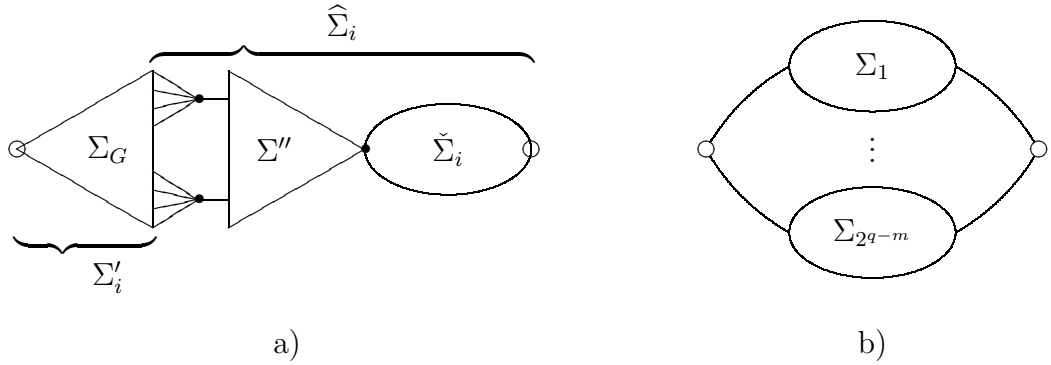


Рис. 6.1: к доказательству теоремы 6.1

в силу (4.2), (4.3) вытекает неравенство (6.1) для сложности Σ_f, так как

$$(p+2)\,2^{n-m} \leqslant \frac{2^n}{s} + 32^{n-m} = \frac{2^n}{n}\left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right),$$

$$(\lambda+q)\,2^{q+1} = (p2^s + m + p)\,2^{m+p+1} \leqslant ((2^s+1)p+m)\,2^{m+p+1} \leqslant$$
$$\leqslant \left(\frac{2^{m+s+2}}{s} + m\right)2^{m+p+1} \leqslant \frac{2^{2m+s+p+4}}{s} \leqslant \frac{32}{s}2^{n-\sqrt{n}+3\log n} = o\left(\frac{2^n}{n\sqrt{n}}\right).$$

Теорема доказана. □

Замечание 1. Построенную КС Σ_f можно разбить на не более, чем

$$\left(\lambda p + \lambda 2^{m+1} + 2^{n-q+1} + q2^m\right)2^p = O\left(\frac{2^n}{n\sqrt{n}}\right)$$

«звезд», каждая из которых состоит из контактов одного и того же типа. Для этого достаточно контакты всех звезд, показанных на рис. 5.1b, перераспределить в звезды из однотипных контактов, «центрами» которых являются выходы подсхем Σ_G схем Σ'_i, $i = 1, \ldots, 2^{q-m}$, а любой из остальных контактов КС Σ_f считать отдельной звездой.

Замечание 2. При построении КС $\overrightarrow{\Sigma}_f$, $\overrightarrow{\Sigma}_f \in \mathfrak{U}^{\overrightarrow{\mathrm{K}}}$, которая реализует ФАЛ f указанным выше способом, вместо звезды, показанной на рис. 5.1b, необходимо использовать звезду из соответствующих ориентированных контактов вида $x_{m+1}^{\sigma_{i,1}}, \ldots, x_{m+p}^{\sigma_{i,m+p}}$, которая является разделительной $(p,1)$-КС и обеспечивает корректность операции суперпозиции. Следовательно, используя для всех КС Σ'_i одну и ту же подсхему Σ_G, при

$$m = \lfloor 2\log n \rfloor - 1, \qquad s = \lceil n - 5\log n \rceil$$

получим

$$L^{\overrightarrow{\mathrm{K}}}(n) \leqslant \frac{2^n}{n}\left(1+\frac{5\log n + O(1)}{n}\right).$$

Аналогичная оценка справедлива и в классе контактно-вентильных схем.

Следствие. $L^{\mathrm{K}}(n) \sim L^{\overrightarrow{\mathrm{K}}}(n) \sim \frac{2^n}{n}$.

Теорема 6.2. *Для функции Шеннона $L^{\Phi}(n)$ выполнено неравенство*

$$L^{\Phi}(n) \leqslant \frac{2^n}{\log n}\left(1+\frac{4\log\log n + o(1)}{\log n}\right). \tag{6.6}$$

Доказательство. Для произвольной ФАЛ f, $f \in P_2(n)$, построим формулу $\mathfrak{F}_f$, которая реализует f и удовлетворяет (6.6).

Пусть $q = m + \lambda$, а $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ — разбиение куба B^q, построенное по лемме 5.1 для описанного выше множества наборов $\widehat{\delta}$. Рассмотрим π-схему $\widetilde{\Sigma}_f$, которая реализует f и строится аналогично КС Σ_f из доказательства теоремы 6.1 с той лишь разницей, что $(1, 2^{n-q})$-КС Σ'_i реализует каждую ЭД $J_{\sigma'',i}$, $\sigma'' \in B^{n-q}$, с помощью пучка из p параллельных контактов от БП $x_{m+1}, \ldots, x_q$. При этом, очевидно, для сложности π-схемы $\widetilde{\Sigma}_f$ неравенство (6.5) будет справедливо при $\lambda = 0$. Искомая формула $\widetilde{\mathfrak{F}}_f$ получается из формулы с поднятыми отрицаниями, моделирующей π-схему Σ_f, заменой каждой ЭД $J_{\sigma'',i}$ вида $x_{j_1} \vee \ldots \vee x_{j_t} \vee \overline{x}_{j_{t+1}} \vee \ldots \vee \overline{x}_{j_p}$, где $t \leqslant p$, формулой $\widetilde{J}_{\sigma'',i}$ вида $x_{j_1} \vee \ldots \vee x_{j_t} \vee \overline{x_{j_{t+1}} \cdots x_{j_p}}$.

Заметим, что в формуле $\widetilde{\mathfrak{F}}_f$ на каждую подформулу $\widetilde{J}_{\sigma'',i}$ приходится не более одного ФЭ $\neg$, а число остальных ФЭ $\neg$ не больше, чем число размыкающих контактов во всех подсхемах вида $\check{\Sigma}_i$ и Σ'' (см. рис. 6.1) π-схемы $\widetilde{\Sigma}_f$, которое равно половине суммарной сложности этих схем. Следовательно,

$$L\left(\widetilde{\mathfrak{F}}_f\right) \leqslant L\left(\widetilde{\Sigma}_f\right) + 2^{n-m} + q2^q. \tag{6.7}$$

Выбирая значения параметров m и s так, что

$$m = \lfloor 3\log\log n \rfloor, \qquad s = \lfloor \log n - 4\log\log n \rfloor,$$

получим

$$p \leqslant \frac{2^m}{s} + 1, \qquad \lambda \leqslant p2^s \leqslant \frac{2^{m+s+1}}{s} \lesssim \frac{2n}{\log^2 n}, \qquad q = m + \lambda \lesssim \frac{2n}{\log^2 n},$$

и, следовательно, в силу (6.5), (6.7) выполняется неравенство

$$L\left(\widetilde{\Sigma}_f\right) \leqslant L\left(\widetilde{\mathfrak{F}}_f\right) \leqslant \frac{2^n}{\log n - 4\log\log n} + O\left(\frac{2^n}{\log^3 n}\right),$$

из которого для сложности формулы $\widetilde{\mathfrak{F}}_f$ вытекает (6.6).

Теорема доказана. □

Следствие. $L^{\Phi}(n) \sim L^{\pi}(n) \sim \frac{2^n}{\log n}$.

Теорема 6.3. *Для любой ФАЛ f, $f \in P_2(n)$ в $\mathfrak{U}^{\Phi}$ существует реализующая ее формула $\mathfrak{F}_f$, для которой*

$$L(\mathfrak{F}_f) \lesssim \frac{2^n}{\log n}, \qquad D(\mathfrak{F}_f) \leqslant n - \log\log n + 6 + o(1)$$

Доказательство. Заметим, что в формуле $\widetilde{\mathfrak{F}}_f$ из теоремы 6.2 мультиплексорная ФАЛ μ_{n-q} от адресных БП x', участвующая в разложении (5.4), реализуется с помощью формулы $\widetilde{\mathfrak{F}}_{n-q}$ из §1. Построим формулу $\widehat{\mathfrak{F}}_f$ аналогично формуле $\widetilde{\mathfrak{F}}_f$ из теоремы 6.2 с той лишь разницей, что вместо формулы $\widetilde{\mathfrak{F}}_{n-q}$ используется формула $\widehat{\mathfrak{F}}_{n-q}$ из §1.

Искомая формула $\mathfrak{F}_f$ подобна формуле $\widehat{\mathfrak{F}}_f$ и получается из нее с помощью леммы 2.3 из §3 главы 2. При этом учитывая то, что

$$\operatorname{Alt}\left(\widehat{\mathfrak{F}}_f\right) \leqslant 6,$$

а также принимая во внимание оценки сложности формул $\widetilde{\mathfrak{F}}_{n-q}$ из §1 и оценки сложности других подформул формулы $\widehat{\mathfrak{F}}_f$ (см. теорему 6.2), при тех же значениях параметров m и s, что и в теореме 6.2, получим

$$L(\mathfrak{F}_f) \lesssim \frac{2^n}{\log n}, \qquad D(\mathfrak{F}_f) \leqslant n - \log\log n + 6 + o(1).$$

□

Следствие. $D(n) = n - \log\log n \pm O(1)$.

§7 Асимптотически наилучший метод синтеза схем из функциональных элементов и формул в произвольном базисе

Обобщим понятие ДУМ ФАЛ следующим образом. Пусть $\varphi(y_1, \ldots, y_p)$ — существенная ФАЛ, то есть ФАЛ, существенно зависящая от всех своих БП. Множество ФАЛ G, $G \in P_2(m)$, называется *φ-универсальным множеством (φ-УМ) порядка m*, если любая ФАЛ g, $g \in P_2(m)$, может быть представлена в виде

$$g = \varphi(g_1, \ldots, g_p), \tag{7.1}$$

где $g_i \in G$ при всех i, $i = 1, \ldots, p$. Заметим, что в случае $\varphi(y_1, \ldots, y_p) = y_1 \vee \ldots \vee y_p$ понятие φ-УМ совпадает с введенным в §4 понятие ДУМ ранга p. Так же, как и в

§4, будем строить φ-УМ порядка m на основе разбиения $\Delta = (\delta_1, \ldots, \delta_p)$ единичного куба B^m. Для каждого $i,\ i = 1, \ldots, p$, в силу существенной зависимости ФАЛ φ от БП y_i найдется набор двоичных констант $\alpha_{i,1}, \ldots, \alpha_{i,p}$ такой, что

$$\varphi(\alpha_{i,1}, \ldots, \alpha_{i,i-1}, y_i, \alpha_{i,i+1}, \ldots, \alpha_{i,p}) = y_i \oplus \alpha_{i,i}. \tag{7.2}$$

Обозначим через $G^{(i)},\ i = 1, \ldots, p$, множество всех тех ФАЛ из $P_2(m)$, которые при любом $j,\ 1 \leqslant j \leqslant p$ и $j \neq i$, равны $\alpha_{i,j}$ на множестве наборов δ_j, и пусть

$$G = G^{(1)} \cup \ldots \cup G^{(p)}.$$

Нетрудно убедиться в том, что равенство (7.1) имеет место для любой функции $g,\ g \in P_2(m)$, если $g_i,\ i = 1, \ldots, p$, — ФАЛ из $G^{(i)}$, совпадающая на δ_i с ФАЛ $g \oplus \alpha_{i,i}$. Действительно, для любого $i,\ i = 1, \ldots, p$, и любого набора $\alpha,\ \alpha \in \delta_i$, в силу (7.2) получим:

$$\varphi(g_1(\alpha), \ldots, g_p(\alpha)) = \varphi(\alpha_{i,1}, \ldots, \alpha_{i,i-1}, g(\alpha) \oplus \alpha_{i,i}, \alpha_{i,i+1}, \ldots, \alpha_{i,p}) = g(\alpha).$$

Следовательно, множество G является φ-УМ порядка m.

Найдем среди ФЭ базиса Б, Б $= \{\mathcal{E}_i\}_{i=1}^{b}$, элемент $\mathcal{E}_j$, на котором достигается приведенный вес $\rho_j = \rho_{\text{Б}}$ (см. §4 главы 2), то есть

$$\rho_j = \frac{\mathcal{L}_j}{k_j - 1} = \min_{k_i \geqslant 2} \rho_i = \rho_{\text{Б}}. \tag{7.3}$$

Пусть, далее, m, s, t, p — натуральные числа, такие, что

$$p = t(k_j - 1) + 1, \tag{7.4}$$

$$k_j \leqslant \frac{2^m}{s} \leqslant p < \frac{2^m}{s} + (k_j - 1), \tag{7.5}$$

а $\Pi = (\pi_1, \ldots, \pi_p)$ — такое разбиение куба B^m на последовательные отрезки (см. §4), что

$$|\pi_i| = s_i \leqslant s \tag{7.6}$$

для всех $i,\ i = 1, \ldots, p$ (ср. с (4.4)). Рассмотрим абсолютную формулу $\mathcal{F}$, построенную из t ФЭ $\mathcal{E}_j$, которая с учетом (7.4) и в соответствии с леммой 1.1 из [2, §1] имеет p входов и реализует существенную ФАЛ $\varphi(y_1, \ldots, y_p)$. Построим φ-УМ G порядка m на основе разбиения Π. Пусть $\overrightarrow{G} = (\widehat{g}_1, \ldots, \widehat{g}_\lambda)$ — система, состоящая из всех различных ФАЛ множества G, для которой в силу (7.6) по-прежнему выполняется неравенство (см. §4)

$$\lambda \leqslant p2^s. \tag{7.7}$$

Теорема 7.1. *Для функции Шеннона* $L^{\mathrm{C}}_{\mathrm{Б}}(n)$ *выполняется неравенство*

$$L^{\mathrm{C}}_{\mathrm{Б}}(n) \leqslant \rho_{\mathrm{Б}} \frac{2^n}{n} \left(1 + \frac{4\log n + O(1)}{n}\right). \tag{7.8}$$

Доказательство. Возьмем произвольную функцию $f,\ f \in P_2(n)$, и построим схему $\Sigma_f,\ \Sigma_f \in \mathcal{U}^{\mathrm{C}}_{\mathrm{Б}}$, которая реализует f со сложностью, удовлетворяющей (7.8). Искомая СФЭ Σ_f строится аналогично тому, как это делалось при доказательстве теоремы 4.1, с той лишь разницей, что:

1. G — указанное выше φ-УМ порядка m от БП x';
2. в схемах Σ'' и Σ_G вместо ФЭ $\&, \vee, \neg$ используются моделирующие их СФЭ из $\mathcal{U}^{\mathrm{C}}_{\mathrm{Б}}$ (см. §10 главы 2);
3. схема Σ' реализует каждую ФАЛ $f_{\sigma''}(x')$ на выходе формулы $\mathcal{F}$, входы которой присоединены к выходам схемы Σ_G в соответствии с представлением

$$f_{\sigma''}(x') = \varphi(g_{\sigma'',1}, \ldots, g_{\sigma'',p})$$

(см. (7.1)), где $g_{\sigma'',i} \in G$ при всех $i,\ i = 1, \ldots, p$.

Сложность построенной СФЭ Σ_f с учетом (7.7) и по аналогии с (4.7) будет удовлетворять неравенству

$$L(\Sigma_f) \leqslant \mathcal{L}_j t 2^{n-m} + O\left(2^{n-m} + p2^{s+m}\right),$$

из которого при тех же значениях параметров s, m, что и в §4, в силу (7.3)–(7.5) следует (7.8).

Теорема доказана. □

Следствие.

$$L^{\mathrm{C}}_{\mathrm{Б}}(n) \sim \rho_{\mathrm{Б}} \frac{2^n}{n}.$$

Теорема 7.2. *Для функции Шеннона* $L^{\Phi}_{\mathrm{Б}}(n)$ *выполняется неравенство*

$$L^{\Phi}_{\mathrm{Б}}(n) \leqslant \rho_{\mathrm{Б}} \frac{2^n}{\log n} \left(1 + \frac{4\log\log n + O(1)}{\log n}\right). \tag{7.9}$$

Доказательство. Возьмем произвольную ФАЛ $f,\ f \in P_2(n)$, и построим формулу $\mathcal{F}_f,\ \mathcal{F}_f \in \mathcal{U}^{\Phi}_{\mathrm{Б}}$, которая реализует f со сложностью, удовлетворяющей (7.9). Искомая формула $\mathcal{F}_f$ строится аналогично тому, как это делалось при доказательстве теоремы 6.2, с той лишь разницей, что:

1. разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q, где $q = m + \lambda a$, выбирается для указанной выше системы ФАЛ $\overrightarrow{G}$ на основе замечания к лемме 5.1;

2. каждая ФАЛ $f_{\sigma'',i}(x')$, где $\sigma'' \in B^{n-q}$, $i = 1, 2, \ldots, 2^{q-m}$, представляет собой ФАЛ вида $\varphi\left(x_{j_1}, \ldots, x_{j_p}\right)$, где $m+1 \leqslant j_1 < \ldots < j_p \leqslant q$, если на компоненте δ_i любая ФАЛ из $\overrightarrow{G}$ совпадает с некоторой БП (см. замечание к лемме 5.1), и ФАЛ вида $\varphi\left(x_{j_1}^{\sigma_1}, \ldots, x_{j_p}^{\sigma_p}\right)$ в остальных случаях;

3. вместо ФЭ $\&, \vee, \neg$ используются моделирующие их бесповторные формулы базиса Б (см. §10 главы 2)), а каждая ФАЛ $f_{\sigma'',i}(x')$ реализуется с помощью построенной выше формулы $\mathcal{F}$.

Сложность построенной формулы $\mathcal{F}_f$ с учетом замечания к лемме 5.1 и по аналогии с (6.6) будет удовлетворять неравенству

$$L(\mathcal{F}_f) \leqslant \mathcal{L}_j t 2^{n-m} + O\left(2^{n-m}\left(1 + \frac{t\lambda}{2^a}\right)\right),$$

из которого при тех же значениях параметров s, m, что и в теореме 6.2 и $a = \lceil \log n \rceil$ следует (7.9).

Теорема доказана. □

§8 Синтез схем для функций из специальных классов. Асимптотика сложности контактного дешифратора, минимальность контактного дерева в классе разделительных схем

Будем использовать введенные в §3 определения и обозначения для функций Шеннона, связанных с реализацией ФАЛ из класса $\mathfrak{Q}$, $\mathfrak{Q} = \mathfrak{Q}(1), \mathfrak{Q}(2), \ldots, \mathfrak{Q}(n), \ldots$, где

$$\mathfrak{Q} \subseteq P_2 \text{ и } \mathfrak{Q}(n) = \mathfrak{Q} \cap P_2(n), \quad n = 1, 2, \ldots .$$

При этом, как правило, будем рассматривать реализацию ФАЛ из класса $\mathfrak{Q}$ схемами из классов $\mathfrak{U}^{\mathrm{C}}$ и $\mathfrak{U}^{\mathrm{K}}$, а функции Шеннона для их сложности будем обозначать через $L^{\mathrm{C}}(\mathfrak{Q}(n))$ и $L^{\mathrm{K}}(\mathfrak{Q}(n))$ соответственно.

На основе мощностных соображений аналогично тому, как это было сделано в §3 для случая $\mathfrak{Q} = P_2$, доказывается следующее утверждение.

Лемма 8.1. *Для произвольного класса ФАЛ $\mathfrak{Q}$ выполняются следующие асимптотические неравенства*

$$L^{\mathrm{K}}(\mathfrak{Q}(n)) \gtrsim \frac{\log|\mathfrak{Q}(n)|}{n}, \qquad L^{\mathrm{C}}(\mathfrak{Q}(n)) \gtrsim \frac{\log|\mathfrak{Q}(n)|}{n} - 1.$$

Доказательство. Из неравенства (3.1), а также леммы 5.3 главы 2 следует, что

$$\left(8nL^{\mathrm{K}}\left(\mathfrak{Q}\left(n\right)\right)\right)^{L^{\mathrm{K}}(\mathfrak{Q}(n))} \geqslant \left|Q\left(n\right)\right|.$$

Логарифмируя это неравенство и учитывая, что в силу следствия из теоремы 6.1

$$\log L^{\mathrm{K}}\left(\mathfrak{Q}\left(n\right)\right) \leqslant \log L^{\mathrm{K}}\left(n\right) \leqslant n - \log n + o\left(1\right),$$

получим неравенства

$$L^{\mathrm{K}}\left(\mathfrak{Q}\left(n\right)\right)\left(3 + \log n + \log L^{\mathrm{K}}\left(\mathfrak{Q}\left(n\right)\right)\right) \geqslant L^{\mathrm{K}}\left(\mathfrak{Q}\left(n\right)\right)\left(3 + n + o\left(1\right)\right) \geqslant \log\left|\mathfrak{Q}\left(n\right)\right|,$$

из которых следует первое неравенство леммы.

Второе неравенство леммы доказывается аналогично с использованием результатов теоремы 4.1, а также теоремы 3.1 главы 2.

Лемма доказана. □

С помощью модификации асимптотически наилучших методов синтеза для многих классов ФАЛ $\mathfrak{Q}$ можно получать такие верхние оценки функций Шеннона $L^{\mathrm{C}}\left(\mathfrak{Q}\left(n\right)\right)$ и $L^{K}\left(\mathfrak{Q}\left(n\right)\right)$, которые асимптотически совпадают с нижними оценками из леммы 8.1.

Пусть, например, класс $\mathfrak{Q}$ состоит из всех ФАЛ симметричных по первым двум БП. Легко видеть, что при этом $\left|\mathfrak{Q}\left(n\right)\right| = 2^{\frac{3}{4}2^n}$ и что $f \in \mathfrak{Q}(n)$ тогда и только тогда, когда вторая и третья четверти столбца значений $\widetilde{\alpha}_f$ совпадают. Следовательно, в силу леммы 8.1 отсюда вытекает, что

$$L^{\mathrm{K}}\left(\mathfrak{Q}\left(n\right)\right) \gtrsim \frac{3}{4} \cdot \frac{2^n}{n}.$$

Докажем теперь, что

$$L^{\mathrm{K}}\left(\mathfrak{Q}\left(n\right)\right) \lesssim \frac{3}{4} \cdot \frac{2^n}{n}, \text{ то есть } L^{\mathrm{K}}\left(\mathfrak{Q}\left(n\right)\right) \sim \frac{3}{4} \cdot \frac{2^n}{n}.$$

Действительно разлагая ФАЛ $f\left(x_1, \ldots, x_n\right)$ из $\mathfrak{Q}\left(n\right)$ по БП x_1, x_2, получим

$$f\left(x_1, x_2, x'\right) = \bigvee_{(\sigma_1,\sigma_2)\in B^2} x_1^{\sigma_1} x_2^{\sigma_2} f_{\sigma_1,\sigma_2}\left(x'\right), \tag{8.1}$$

где $x' = \left(x_3, \ldots, x_n\right)$ и $f_{\sigma_1,\sigma_2}\left(x'\right) = f_{\sigma_1,\sigma_2}\left(\sigma_1, \sigma_2, x'\right)$, причем $f_{01} = f_{10}$ в силу симметричности ФАЛ f по БП x_1, x_2. Искомая КС Σ_f реализует ФАЛ f в соответствии с (8.1) и имеет вид $\Sigma_f = \Sigma''\left(\Sigma'\right)$, где Σ'' — $(4,1)$-КД от БП x_1, x_2, а $(1,3)$-КС Σ' от БП x' реализует асимптотически наилучшим способом ФАЛ f_{00}, $f_{01} = f_{10}$ и f_{11} от БП x'. Легко видеть, что сложность построенной схемы асимптотически не больше, чем $\frac{3}{4}\frac{2^n}{n}$.

Важным частным случаем задачи синтеза схем для ФАЛ из специальных классов является задача построения минимальных или близких к ним схем для конкретных ФАЛ (систем ФАЛ), встречающихся в приложениях. Рассмотрим эту задачу на примере контактного дешифратора порядка n.

Лемма 8.2. $L^{\mathrm{K}}(Q_n) \leqslant 2^n + O\left(\frac{2^n}{\sqrt{n}}\right)$.

Доказательство. Заметим что в $(1, p2^{n-q})$-КС $\widehat{\Sigma}_i,\ i = 1, \ldots, 2^{q-m}$, которая получается из КС Σ_i, построенной при доказательстве теоремы 6.1 в результате удаления подсхемы Σ_G и разъединения всех присоединенных к ее выходам концевых вершин звезд (см. рис. 6.1а), система ФАЛ проводимости от входа $\widehat{\Sigma}_i$, совпадающего с выходом Σ_i, к выходам $\widehat{\Sigma}_i$ — концевым вершинам звезд, – состоит из всех ФАЛ вида $\chi'_i x_{q+1}^{\sigma_{q+1}} \cdots x_n^{\sigma_n}$. Следовательно, при $s = 1$ и $m = \left\lfloor \frac{1}{2} \log n \right\rfloor$ схема Σ_n, которая получается в результате отождествления входов у всех указанных выше схем $\widehat{\Sigma}_i,\ i = 1, \cdots, 2^{q-m}$, реализует систему ФАЛ Q_n со сложностью

$$L(\Sigma_n) \leqslant 2^n + 2^{n-m+1} + q2^{m+p} = 2^n \left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right).$$

Лемма доказана. □

Легко видеть, что в отличие от контактного дерева контактный дешифратор, построенный при доказательстве леммы 8.2, не является разделительной КС. Докажем, в заключение, что $(1, 2^n)$-контактное дерево — минимальный контактный дешифратор порядка n в классе разделительных (по выходам) КС.

Лемма 8.3. *Если разделительная по выходам* $(1, m)$*-КС* Σ *реализует* m *различных ФАЛ отличных от* 0*, то*

$$L(\Sigma) \geqslant 2m - 2.$$

Доказательство. Пусть Σ — приведенная и, следовательно, связная КС от БП $x_1, \ldots, x_n$. Из разделительности Σ следует, что при любом α, $\alpha \in B^n$, сеть $\Sigma(\alpha)$ состоит не менее, чем из m, связных компонент. Заметим, что удаление всякого ребра увеличивает число связных компонент графа не более, чем на единицу, и поэтому число $|\Sigma(\overline{\alpha})|$ — число контактов не проводящих на наборе α, — удовлетворяет неравенству

$$|E(\Sigma(\overline{\alpha}))| \geqslant m - 1. \tag{8.2}$$

Суммируя (8.2) по всем α, $\alpha \in B^n$, и учитывая, что каждый контакт КС Σ не проводит ровно на половине всех наборов куба B^n, получим

$$2^{n-1} L(\Sigma) \geqslant 2^n (m - 1), \qquad L(\Sigma) \geqslant 2m - 2.$$

Лемма доказана. □

Следствие. *Контактное дерево порядка n является минимальной разделительной $(1, 2^n)$-КС, реализующей систему ФАЛ Q_n.*

Действительно, в соответствии с леммой 8.3 сложность разделительной $(1, 2^n)$-КС не меньше чем $2^{n+1} - 2$, то есть не меньше сложности $(1, 2^n)$-контактного дерева порядка n.