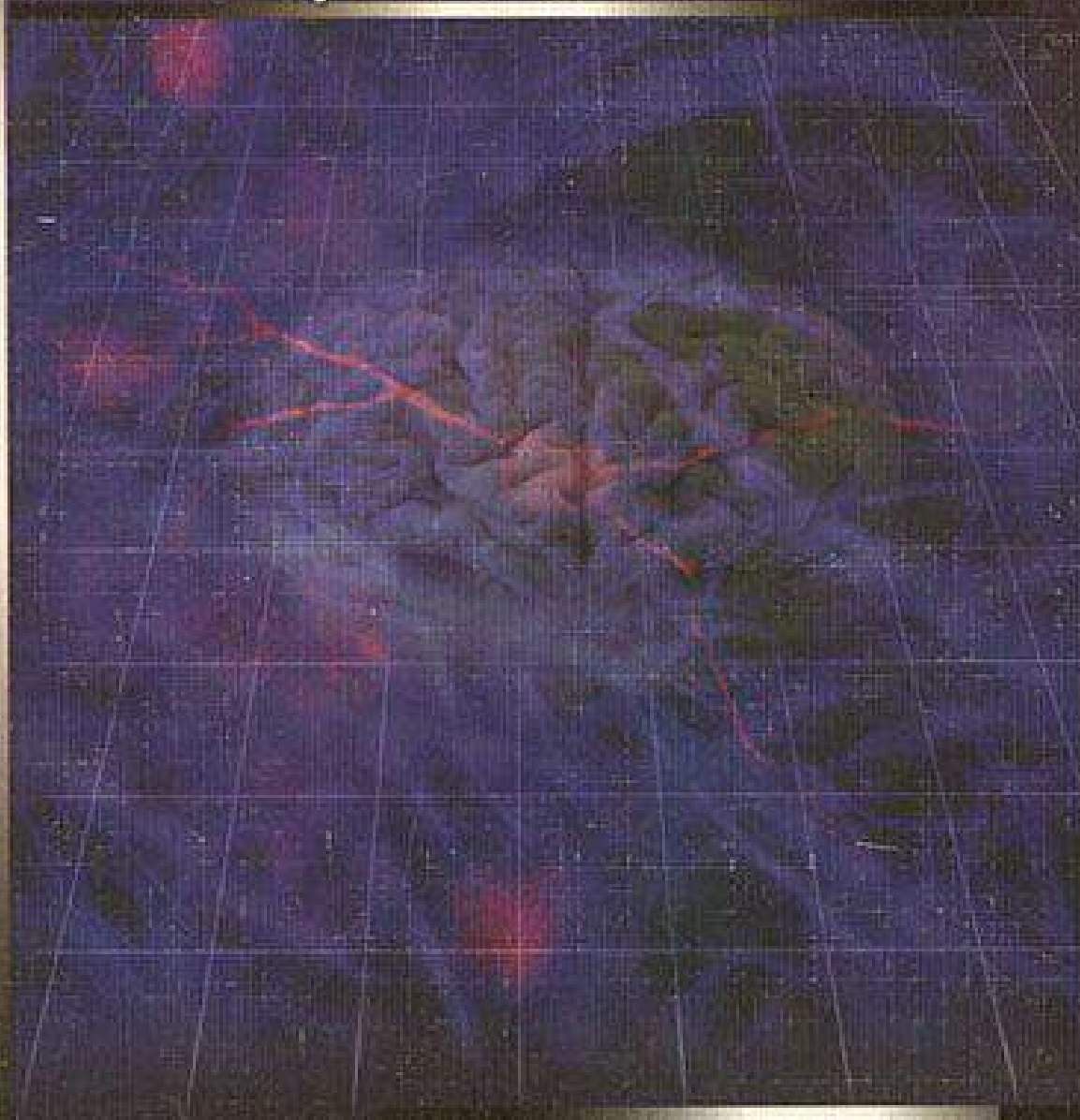


ДЛЯ ВЫСШИХ
УЧЕБНЫХ ЗАВЕДЕНИЙ

С.В. Яблонский

Элементы математической кибернетики



МАТЕМАТИКА

ozon.ru



УДК 519.7
ББК 22.18
Я 14

Рецензенты: кафедра дискретной математики механико-математического факультета МГУ (зав. кафедрой академик РАН О.Б. Лупанов); д-р физ.-мат. наук Ю.Н. Янов (Институт прикладной математики им. М.В. Келдыша)

Научная библиотека МГУ



62009760

Яблонский С.В.

Я 14 Элементы математической кибернетики: Учебник/С.В. Яблонский — М.: Высш. школа, 2007. — 188 с.: ил.

ISBN 978-5-06-004760-8

В книге представлены четыре базовых раздела математической теории управляющих систем: синтез и сложность; эквивалентные преобразования; надежность; контроль исправности и диагностика неисправностей. Даны: описание изучаемых объектов, постановка основных задач, описание методов решения этих задач и получаемых результатов.

Для студентов и аспирантов, специализирующихся в области математической кибернетики. Будет полезно научным работникам и инженерам, интересующимся кибернетикой, вычислительной техникой и устройствами управления.

УДК 519.7
ББК 22.18

ISBN 978-5-06-004760-8

© ОАО «Издательство «Высшая школа», 2007

Оригинал-макет данного издания является собственностью издательства «Высшая школа», и его репродуцирование (воспроизведение) любым способом без согласия издательства запрещается.

НАУЧНАЯ БИБЛИОТЕКА МГУ

28

Предисловие редактора

Данная книга естественным образом возникла на основе различных специальных, а затем и обязательных курсов лекций, читавшихся Сергеем Всеволодовичем Яблонским на протяжении более чем тридцати лет в Московском государственном университете им. М. В. Ломоносова. Весь материал книги естественным образом разбивается на четыре части: синтез и сложность управляющих систем; эквивалентные преобразования управляющих систем; надежность управляющих систем; контроль управляющих систем. Каждая из этих частей достаточно полно и последовательно освещает соответствующий базовый раздел математической кибернетики.

В первой части вводится понятие управляющей системы и дается типичная постановка задачи синтеза. Последовательно, от наиболее простых до асимптотически оптимальных излагаются универсальные методы синтеза контактных схем, а затем схем из функциональных элементов. Демонстрируется использование так называемых мощностных соображений (предложенных Шенноном) для получения нижних оценок сложности схем; сложность схемы чаще всего отождествляется с числом элементов, т. е. контактов или функциональных элементов в ней.

Исследуется задача синтеза схем для отдельных важных классов функций: линейных, симметрических и выделенных автором функций из инвариантных классов, сыгравших значительную роль в развитии теории синтеза и сложности управляющих систем. Достаточно кратко, но все-таки затрагивается обширная и выдвигающаяся в настоящее время на передний план проблема получения нижних оценок сложности для управляющих систем, реализующих конкретные функции.

Во второй части весьма компактно и вместе с тем с исчерпывающей полнотой изложены все основные имеющиеся к настоящему времени принципиальные результаты, касающиеся эквивалентных преобразований формул в P_2 , формул в P_k , схем из функциональных элементов, контактных схем, автоматов (т. е. фактически всех наиболее важных классов управляющих систем).

В третьей части достаточно подробно и последовательно рассматривается построение надежных схем из ненадежных элементов: излагаются основные способы вероятностного описания источников помех и повреждений схем; приводится предложенный автором частный (для некоторого конкретного базиса), но весьма изящный и поучительный способ построения сколь угодно надежных схем с использованием преимущественно ненадежных элементов; представлен и другой асимптотически оптимальный метод построения надежных схем также преимущественно из ненадежных элементов.

Эффективное использование предложенного автором принципа самокорректирования демонстрируется на примере самокорректирующихся контактных схем и самокорректирующихся схем их функциональных элементов.

В четвертой части излагается принадлежащая автору и ставшая общепринятой постановка задачи контроля исправности и диагностики неисправностей управляющих систем логическими способами, т. е. без вмешательства в схему, с использованием соответствующих экспериментов. Приводятся методы построения таблиц функций неисправностей, методы построения тупиковых и минимальных тестов для таблиц. Рассматриваются условные и безусловные тесты, демонстрируется возможность построения простых тестов с учетом структуры схемы.

При редактировании и подготовке текста книги к печати, к сожалению, уже не было возможности обсудить некоторые вопросы, касающиеся изложения материала, с самим автором. В этой ситуации редактор стремился вносить в первоначальный рукописный текст как можно меньше изменений, и редактирование свелось к устранению имевшихся отдельных погрешностей.

В книге собран и хорошо представлен весьма богатый материал, до сих пор разбросанный по многочисленным, порой уже малодоступным источникам, и ранее не собранный воедино. Многие приведенные в книге результаты стали классическими. Четкие, ясные определения основных математических объектов исследования успешно используются на протяжении десятилетий вплоть до настоящего времени. Основные изложенные в книге подходы к решению поставленных задач являются, по существу, основой того математического аппарата, который используется и развивается далее в современных научных исследованиях по главным направлениям математической кибернетики, в становлении и развитии которой С. В. Яблонский принимал активное участие.

Сам автор справедливо считал, что хорошая теория должна содержать, по крайней мере, три компоненты: а) описание объектов теории; б) постановку ее основных задач; в) описание (характеристику) методов их решения и получаемых результатов. Эти компоненты присутствуют во всех представленных в книге направлениях и поэтому книга имеет большую методологическую ценность, особенно с учетом проникновения дискретной математики и математической кибернетики в учебные программы уже многих высших учебных заведений.

Ясно, что данная книга окажется востребованной и полезной как для студентов и аспирантов, так и для научных сотрудников, специализирующихся в области математической кибернетики.

Н. П. Редькин

ВВЕДЕНИЕ

Пусть $\mathcal{U}$ — класс управляющих систем (У.С.) U таких, что $U = (\Sigma, \Phi)$. Во многих случаях $\Phi = \varphi(\Sigma)$ и более того, отображение $\Sigma \rightarrow \Phi$ задается алгоритмом (см. алгоритмический подход). Часто при рассмотрении У.С. важна не сама функция Φ , а некоторая производная величина f , называемая функциональной характеристикой, определяемая соотношением

$$f = \psi(\Phi).$$

Здесь f можно рассматривать как интерпретацию работы Φ У.С. U , а пару (Σ, f) как вспомогательную У.С., как обобщение У.С. (Σ, Φ) — поскольку при $\psi(Z) = Z$, $f \equiv \Phi$. Положим $\mathfrak{S} = \{\Sigma\}$, $\mathfrak{F} = \{\Phi\}$ и $\mathfrak{f} = \{f\}$. В таблице 1¹ приведены множества $\mathfrak{S}$, $\mathfrak{F}$ и $\mathfrak{f}$ для основных классов модельных объектов. Для указанных классов функции φ и ψ вычислимы и потому отображение $\Sigma \rightarrow f$ может быть задано алгоритмом A .

Т а б л и ц а 1

$\mathcal{U}$	$\mathfrak{S}$	$\mathfrak{F}$	$\mathfrak{f}$
p -полюсные контактные схемы	p -полюсные контактные схемы	класс булевых матриц порядка p специального вида	класс булевых матриц порядка p специального вида
двухполюсные контактные схемы	двухполюсные контактные схемы	класс булевых матриц порядка 2 специального вида	множество булевых функций
схемы из функциональных элементов	схемы из функциональных элементов в данном базисе B	системы булевых уравнений	системы булевых функций
автоматы	автоматные схемы в базисе B	системы канонических уравнений	• множество о.-д. функций • множество регулярных событий
машины Тьюринга	автоматы с головкой над бесконечной лентой	преобразования, осуществляемые машиной	класс частично рекурсивных функций
программы	программы (графы специального вида в базисе B)	преобразования памяти и программ	класс частично рекурсивных функций

Теперь перейдем к содержательному описанию постановки задачи синтеза У.С. в достаточно общем виде для того, чтобы избежать повторений

¹В данной таблице название классов У.С. совпадает с названием классов схем, так как последние полностью определяют эти классы. Функциональные характеристики для более простых классов совпадают с функциями. Для более богатых классов возможности для их выбора значительно увеличиваются

Ряд определений (булевой функции, контактной схемы, схемы из функциональных элементов, совершенной д.н.ф., сети и др.) здесь и далее не приводится — их можно найти, например, в [15, 34].

при рассмотрении конкретных классов У.С. Выделяя общую часть для этих классов, мы вынуждены оставаться на наивной позиции, и уточнение отдельных моментов отодвинуть до рассмотрения индивидуальных классов.

В постановке задачи синтеза следует выделить три этапа.

I. Тривиальная подстановка: для каждой функции $f \in \mathfrak{F}$ построить схему $\Sigma \in \mathfrak{S}$, реализующую f , т. е. такую, что (Σ, f) — есть обобщенная У.С.

Как мы видим, для модельных объектов такое решение существует и притом при помощи простых алгоритмов. Обозначим через Σ_0 результат работы такого алгоритма для функции f .

Главная особенность данной задачи — наличие многих решений (даже бесконечного числа). В этом случае мы не можем оценить качество решения Σ_0 .

II. Постановка с учетом сложности схем. Это уточнение связано с рассмотрением функционала $L(\Sigma)$, где $\Sigma \in \mathfrak{S}$, выражающего сложность схемы, который может иметь различный смысл:

обозначать число элементов схемы Σ ;

задавать площадь (или объем), занимаемую схемой Σ ;

указывать вероятность отказа схемы Σ ;

задавать время вычисления Σ на каждом входном наборе и т. п.

О п р е д е л е н и е. Схема Σ_m , реализующая f , называется минимальной (относительно L), если существует $\min L(\Sigma) = L(f)$, где минимум берется по всем схемам Σ , $\Sigma \in \mathfrak{S}$, реализующим f , и $L(\Sigma_m) = L(f)$, т. е. минимум достигается на Σ_m .

Легко видеть, что если число схем Σ , реализующих f и имеющих сложность меньшую или равную $L(\Sigma_0)$, конечно, то минимальная схема Σ_m для f существует.

Данная ситуация выполнена для классов контактных схем, схем из функциональных элементов и автоматов и ряда других объектов. Минимальные схемы существуют также при $L(\Sigma)$ неотрицательном и целочисленном. Теперь проблема синтеза — проблема построения минимальных схем.

Для только что упомянутых классов данная задача имеет положительное решение, основанное на просмотре всех схем сложности не более $L(\Sigma_0)$, так называемый алгоритм полного перебора.

Основной недостаток переборного алгоритма — большая трудоемкость — означает практическую невозможность построения минимальных схем даже с применением современных ЭВМ у же при небольших значениях параметров.

III. Дальнейшее уточнение задачи синтеза связано прежде всего с отказом от оптимального решения для каждой функции и с рассмотрением задачи сразу для целого класса функций $\mathfrak{F}_i$, $\mathfrak{F}_i \subseteq \mathfrak{F}$ и $\mathfrak{F} = \bigcup_i \mathfrak{F}_i$ при условии, что $|\mathfrak{F}_i| < +\infty$ для каждого i .

При указанном ограничении положим

$$L(i) = \max_{f, f \in \mathfrak{F}_i} L(f).$$

Функция $L(i)$ называется функцией Шеннона. Она, очевидно, характеризует величину сложности, достаточную при реализации функции из класса $\mathfrak{F}_i$.

В данных условия существует два подхода.

Первый подход:

а) требование нахождения минимальной схемы для каждой функции заменяется на требование достижения оптимума для всего класса $\mathfrak{F}_i$ ($i = 1, \dots$), что может быть аналитически задано условием — $L(\Sigma) \leq L(i)$ для любой $f \in \mathfrak{F}_i$ и Σ , реализующей f , или чаще условием $L(\Sigma) \lesssim L(i)$ (асимптотическая постановка);

б) при указанном ограничении (см. а) пытаются найти более простой алгоритм синтеза, чем полный перебор (последнее в конкретных случаях бывает ясно²).

Второй подход:

а) заранее накладывается ограничение на сложность допустимых алгоритмов;

б) в рамках указанного класса алгоритмов ищется такой, который в определенном смысле дает более простые схемы.

Проблематика синтеза У.С. развивается при рассмотрении отдельных классов У.С., для которых строятся алгоритмы синтеза, находятся оценки сложности получаемых схем и алгоритмов синтеза.

Данная часть делится на три больших раздела:

1. Изучение универсальных методов синтеза.
2. Построение классов функций и изучение методов синтеза схем для функций, принадлежащих этим классам.
3. Исследование нижних оценок для просто задаваемых функций.

²Более точно: например, в классе полиномиальных алгоритмов.

РАЗДЕЛ 1. УНИВЕРСАЛЬНЫЕ МЕТОДЫ СИНТЕЗА

Здесь речь идет о разработке методов синтеза и соответствующих им алгоритмов A для случая, когда рассматривается весь класс управляющих систем $\mathcal{U}$. Изучение этих вопросов развивается на отдельных классах.

ГЛАВА 1. КЛАСС КОНТАКТНЫХ СХЕМ

Дадим расшифровку абстрактной схемы. Мы имеем для рассматриваемого случая:

$\mathfrak{S}$ — множество всех p -полюсных контактных схем Σ ;

$\mathfrak{F}$ — множество булевых матриц специального вида, имеющих порядок p (для $p = 2$ множество $\mathfrak{F}$ совпадает с множеством булевых функций P_2);

$L(\Sigma)$ — число контактов в Σ ;

$L(f) = \operatorname{opt}_{\Sigma} L(\Sigma) = \min_{\Sigma_{\text{реал. } f}} L(\Sigma)$ — минимальная сложность схемы,

реализующей f (здесь $\min$ всегда существует);

$\mathfrak{F}_{n,p}$ — множество матриц специального вида порядка p , содержащих булевы функции от переменных $x_1, \dots, x_n$; очевидно, $\mathfrak{F} = \bigcup_n \mathfrak{F}_{n,p}$ и $|\mathfrak{F}_{n,p}| < +\infty$;

$L(n, p)$ — функция Шеннона, которая в силу конечности $\mathfrak{F}_{n,p}$ определена для любых p и n ; при $p = 2$ для краткости будем писать $L(n, 2) = L(n)$.

Универсальные методы синтеза начнем рассматривать со случая двухполюсных контактных схем и прежде всего опишем два простейших метода синтеза.

§ 1. Простейшие методы синтеза

1. Синтез схемы по совершенной д.н.ф. (алгоритм A_1). Мы видели, что для этого надо для функции $f(x_1, \dots, x_n) \not\equiv 0$ взять ее разложение в совершенную д.н.ф.

$$f(x_1, \dots, x_n) = \bigvee_{\substack{j=1 \\ (\sigma_1(j), \dots, \sigma_n(j)) \\ f(\sigma_1, \dots, \sigma_n)=1}}^s x_1^{\sigma_1(j)} \& \dots \& x_n^{\sigma_n(j)}$$

и по ней строить схему Σ (рис. 1), реализующую f . При $f \equiv 0$ можно взять, например, схему, изображенную на рис. 2. Мы имеем $L(\Sigma) \leq n2^n$, т. е. $L_{A_1}(n) = n2^n$.

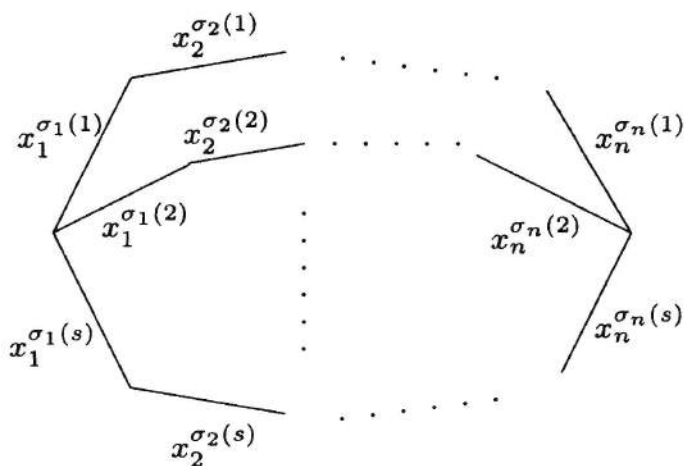


Рис. 1



Рис. 2

2. Синтез схемы по дереву (алгоритм A_2). В случае $f(x_1, \dots, x_n) \neq 0$ берем разложение f в совершенную д.н.ф. и рассмотрим контактное дерево D_n с одним входом и 2^n выходами (рис. 3).

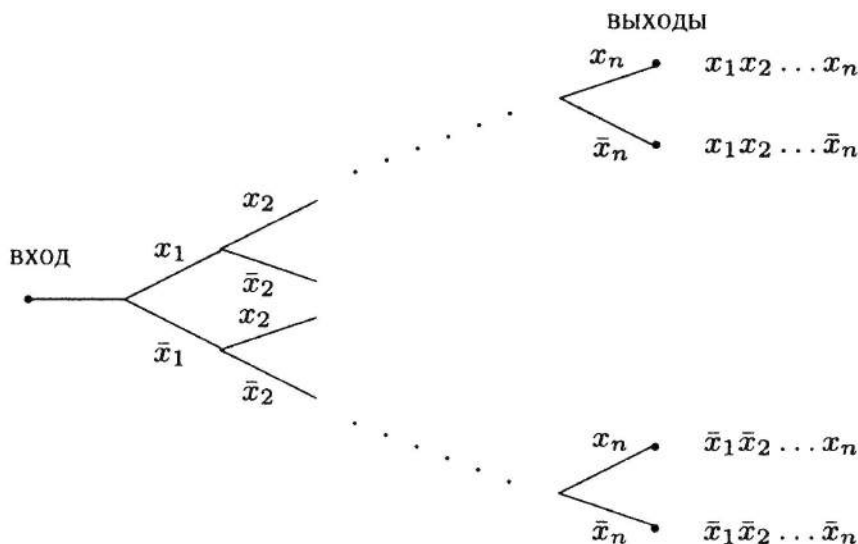


Рис. 3

Очевидно, что на его выходах реализуются все 2^n конъюнкций вида

$$x_1 x_2 \dots x_n, \dots, x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n}, \dots, \bar{x}_1 \bar{x}_2 \dots \bar{x}_n.$$

Если все выходы дерева D_n , соответствующие членам совершенной д.н.ф. функции f , объединить, а поддеревья, содержащие только неиспользованные выходы, отбросить, то получим схему Σ , реализующую f . Для $f \equiv 0$ действуем как в 1. Мы имеем

$$L(\Sigma) \leq 2 \cdot 2^n - 2 < 2 \cdot 2^n, \text{ т. е. } L_{A_2}(n) < 2 \cdot 2^n.$$

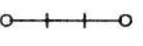
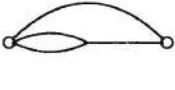
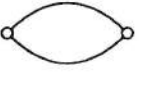
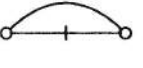
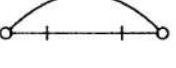
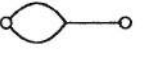
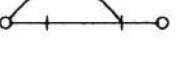
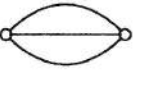
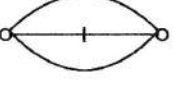
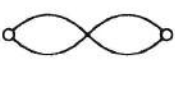
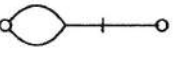
§ 2. Алгоритм полного перебора (A_0)

Для двухполюсных контактных схем можно предложить достаточно просто формулируемый алгоритм построения минимальных схем (алгоритм полного перебора A_0), опирающийся на то, что для каждой булевой функции $f(x_1, \dots, x_n)$ существует двухполюсная контактная схема, ее реализующая.

Указанный алгоритм основан на следующих шагах.

1. Постепенный просмотр двухполюсных сетей, состоящих из ребер со свойством сильной связности (указанные сети с числом ребер $h = 0, 1, 2, 3, 4$ приведены в табл. 2). Этот просмотр идет по нарастанию числа ребер, начиная с $h = 0$.

Т а б л и ц а 2

0	1	2	3	4	
					
					
					
					
					

2. Построение всех контактных схем из данной сети над контактами $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$.

3. Анализ функции, реализуемой рассматриваемой схемой: если она совпадает с f , то данная схема будет искомой минимальной схемой, если не совпадает с f , то переходят к следующей схеме. Этот процесс обязательно заканчивается построением минимальной схемы.

Главной особенностью алгоритма полного перебора всех схем является то, что он обладает колоссальной трудоемкостью. В силу этого он не пригоден для целей синтеза схем даже при $n = 4$, например, вычислить значение $L(4)$.

§ 3. Метод Шеннона

В 1949 г. К. Шенноном [43] был предложен оригинальный метод синтеза контактных схем, позволивший установить порядок функций Шеннона.

Пусть $\{f_1(x_1, \dots, x_n), \dots, f_s(x_1, \dots, x_n)\}$ — множество булевых функций ($f_i \neq f_j$ при $i \neq j$).

О п р е д е л е н и е. Контактный многополюсник, имеющий один вход и s выходов, называется универсальным для данного множества функций $\{f_1, \dots, f_s\}$, если для каждого i ($1 \leq i \leq s$) в многополюснике найдется выход $\tau(i)$ такой, что между входом и этим выходом реализуется функция $f_i(x_1, \dots, x_n)$.

Пример. В качестве множества булевых функций взято множество всех конъюнкций вида

$$K_{i(\tilde{\sigma})} = x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n}, \quad i(\tilde{\sigma}) = 1, \dots, 2^n.$$

Универсальным многополюсником для него будет контактное дерево D_n с n ярусами (см. рис. 3).

Очевидно $L(D_n) < 2 \cdot 2^n$.

Пусть Q — произвольное подмножество булевых функций и $P_Q(n)$ — число булевых функций из Q , зависящих от переменных $x_1, \dots, x_n$.

Лемма 1. Если класс Q замкнут относительно операции подстановки констант вместо некоторых переменных, операции добавления и изъятия несущественных переменных, то для любого n можно построить универсальный многополюсник U_Q^n для множества всех функций из Q , зависящих от переменных $x_1, \dots, x_n$, и такой, что

$$L(U_Q^n) \leq 2 \cdot P_Q(n). \quad (*)$$

Доказательство. Если Q не содержит функций, существенно зависящих от переменных, утверждение очевидно, так как $L(U_Q^n) = 0$, а $0 \leq P_Q(0) \leq 2$. Пусть Q содержит хотя бы одну функцию, имеющую существенно переменное. Тогда $P_Q(0) = 2$ в силу свойств класса Q . В этом случае утверждение доказываем по индукции.

а) Базис индукции: $n = 0$. На рис. 4 приведен универсальный многополюсник U_Q^0 , реализующий обе константы. Для него $L(U_Q^0) = 0$, а $P_Q(0) = 2$ и неравенство (*) выполнено.

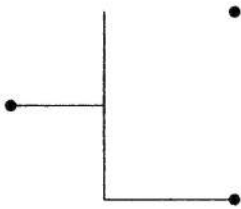


Рис. 4

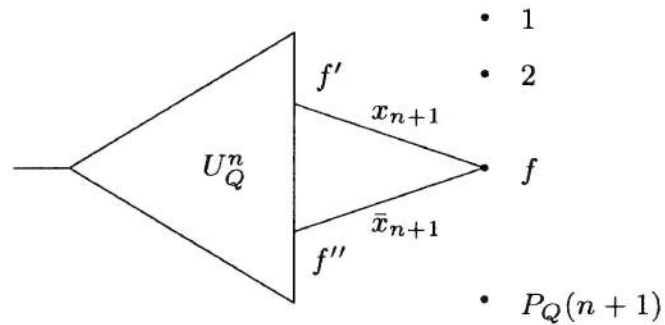


Рис. 5

б) Индуктивный переход от n к $n + 1$. Пусть построен универсальный многополюсник U_Q^n так, что

$$L(U_Q^n) \leq 2P_Q(n).$$

Выбираем $P_Q(n + 1)$ вершин в качестве выходов многополюсника U_Q^{n+1} (рис. 5) и каждой вершине сопоставим взаимно однозначным образом функцию из Q , зависящую от переменных $x_1, \dots, x_{n+1}$. Пусть $f(x_1, \dots, x_{n+1}) \in Q$. Рассмотрим ее разложение по переменному x_{n+1}

$$f(x_1, \dots, x_{n+1}) = x_{n+1}f'(x_1, \dots, x_n) \vee \bar{x}_{n+1}f''(x_1, \dots, x_n).$$

В силу замкнутости Q относительно подстановки констант f' и $f'' \in Q$ зависят от переменных $x_1, \dots, x_n$, поэтому существуют выходы многополюсника U_Q^n , на которых они реализуются.

1) Если $f' \equiv f''$ (вырожденный случай), соответствующий выход многополюсника U_Q^n соединяем ребром с вершиной, соответствующей f .

2) Если $f' \not\equiv f''$ (основной случай), производим соединение ненулевых вершин f' и f'' с f через контакты x_{n+1} и $\bar{x}_{n+1}$ так, как указано на рис. 5 в соответствии с разложением функции f .

Полученный многополюсник и возьмем в качестве U_Q^{n+1} .

В силу замкнутости класса Q относительно добавления несущественных переменных вырожденная ситуация повторится ровно $P_Q(n)$ раз и

$$L(U_Q^{n+1}) \leq L(U_Q^n) + 2(P_Q(n+1) - P_Q(n)) \leq 2P_Q(n+1).$$

Лемма доказана.

С л е д с т в и е. Если $Q = P_2$ — множество всех булевых функций, то $L(U_Q^n) \leq 2 \cdot 2^{2^n}$.

Обозначим через $\langle i, j \rangle$ проводимость между i и j вершинами.

О п р е д е л е н и е. Многополюсник с одним входом и s выходами называется разделительным, если проводимость $\langle i, j \rangle$ между любыми его выходами i и j ($i \neq j$) равна 0, т. е. $\langle i, j \rangle = 0$. Очевидно, контактное дерево D будет разделительным многополюсником.

Л е м м а 2 (Шеннон). Пусть имеются два многополюсника U_1 и U_2 , из которых U_1 имеет один вход a и некоторое число выходов, а U_2 какое-то число входов и один выход b . Предположим, что многополюсник U_1 — разделительный и каждый выход многополюсника U_1 соединен не более, чем с одним входом многополюсника U_2 . Тогда полученная контактная схема с входом a и выходом b (рис. 6) реализует функцию $\langle a, b \rangle$ и

$$\langle a, b \rangle = \bigvee_{i=1}^s \langle a, i \rangle \langle \tau(i), b \rangle,$$

где, если для i нет входа $\tau(i)$, с которым он соединен, слагаемое принимается равным 0.

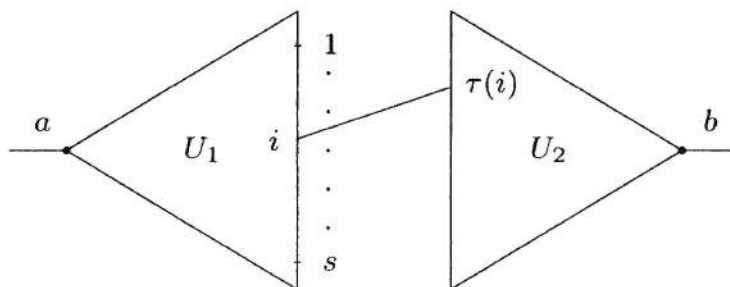


Рис. 6

Доказательство. Очевидно, что данная формула учитывает вклад всех цепей от a до b , которые не возвращаются из U_2 в U_1 . Прочие цепи (имеющие возврат; см. рис. 7), либо невозможны (случай а) в силу условия соединения многополюсников, либо дает нулевой вклад (случай б) из-за разделительности U_1 .

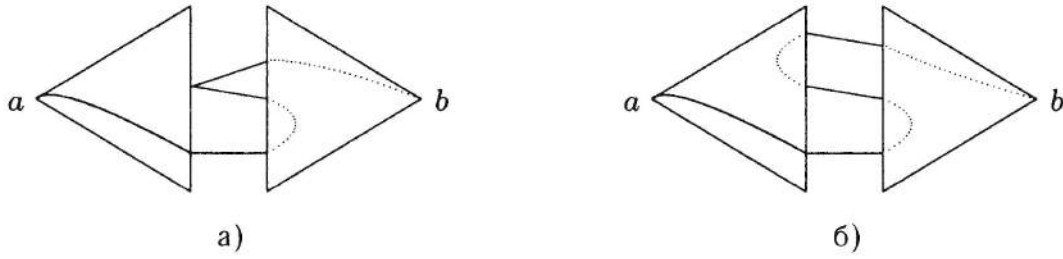


Рис. 7

Лемма доказана.

Теорема 1. Существует метод синтеза A_3 (метод Шеннона) такой, что для каждой булевой функции f он дает контактную схему Σ_f , реализующую f , такую, что

$$L_{A_3}(\Sigma_f) \lesssim 4 \frac{2^n}{n}.$$

Доказательство. Для функции $f(x_1, \dots, x_n)$ возьмем разложение

$$f(x_1, \dots, x_n) = \bigvee_{(\sigma_1, \dots, \sigma_{n-m})} x_1^{\sigma_1} \& \dots \& x_{n-m}^{\sigma_{n-m}} f(\sigma_1, \dots, \sigma_{n-m}, x_{n-m+1}, \dots, x_n).$$

Возьмем, далее, контактное дерево D_{n-m} по переменным $x_1, \dots, x_{n-m}$ и универсальный многополюсник U_Q^m с 2^{2^m} входами и одним выходом

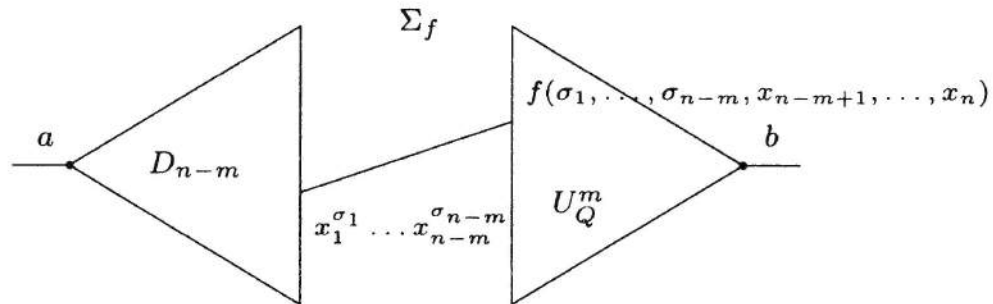


Рис. 8

для всех функций от m переменных $x_{n-m+1}, \dots, x_n$ (рис. 8) и для каждого $(\sigma_1, \dots, \sigma_{n-m})$ выход дерева $x_1^{\sigma_1} \dots x_{n-m}^{\sigma_{n-m}}$ соединим со входом $f(\sigma_1, \dots, \sigma_{n-m}, x_{n-m+1}, \dots, x_n)$ многополюсника U_Q^m ; полученную схему обозначим через Σ_f . В силу леммы 2 имеем

$$\begin{aligned} \langle a, b \rangle &= \bigvee_{(\sigma_1, \dots, \sigma_{n-m})} \langle a, x_1^{\sigma_1} \dots x_{n-m}^{\sigma_{n-m}} \rangle \langle f(\sigma_1, \dots, \sigma_{n-m}, x_{n-m+1}, \dots, x_n), b \rangle = \\ &= \bigvee_{(\sigma_1, \dots, \sigma_{n-m})} x_1^{\sigma_1} \dots x_{n-m}^{\sigma_{n-m}} f(\sigma_1, \dots, \sigma_{n-m}, x_{n-m+1}, \dots, x_n) = f(x_1, \dots, x_n), \end{aligned}$$

т. е. двухполюсник Σ_f реализует функцию f . Очевидно,

$$L(\Sigma_f) = L(D_{n-m}) + L(U_Q^m) \leq 2 \cdot 2^{n-m} + 2 \cdot 2^{2^m}.$$

Возьмем $m = \lfloor \log(n - \log n) \rfloor$; здесь и далее $\log a$ означает двоичный логарифм a . Мы имеем

$$\begin{aligned} \log(n - 2 \log n) - 1 < m \leq \log(n - 2 \log n) \\ \frac{1}{2}(n - 2 \log n) < 2^m \leq n - 2 \log n. \end{aligned}$$

Отсюда

$$L(\Sigma_f) \leq \frac{2 \cdot 2^n}{\frac{1}{2}(n - 2 \log n)} + \frac{2 \cdot 2^n}{n^2} = 4 \frac{2^n}{n} (1 + o(1)).$$

Теорема доказана.

§ 4. Нижняя оценка

Сравнивая оценки, полученные для трех методов A_1, A_2, A_3 , мы видим, что переходя от A_1 к A_2 и от A_2 к A_3 , оценки улучшились в $\frac{n}{2}$ раз. Естественно, возникает вопрос, возможно ли дальнейшее совершенствование методов синтеза и, если возможно, то насколько. Для того чтобы ответить на этот вопрос, надо получить нижнюю оценку для функции Шеннона $L(n)$.

Т е о р е м а 2. $L(n) \geq \frac{2^n}{n}$.

Д о к а з а т е л ь с т в о. Как известно из курса «Дискретная математика», число $s(h, 2)$ двухполюсных сетей, состоящих из h ребер, не превосходит $(ch)^h$. Та же оценка сохраняется, если оценивать число сетей указанного типа, но содержащих не более h ребер (надо несколько увеличить константу c).

Очевидно, что число $|\mathfrak{S}(h, n)|$ контактных схем, содержащих не более h контактов, над алфавитом $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$ не превосходит

$$(ch)^h (2n)^h.$$

Возьмем произвольное $\varepsilon > 0$ и оценим величину

$$\log \frac{|\mathfrak{S}(h, n)|}{2^{2^n}} \quad \text{при} \quad h = \left\lceil (1 - \varepsilon) \frac{2^n}{n} \right\rceil.$$

Мы имеем

$$\begin{aligned} \log \frac{|\mathfrak{S}(h, n)|}{2^{2^n}} &\leq (1 - \varepsilon) \frac{2^n}{n} \log (2c(1 - \varepsilon)2^n) - 2^n = \\ &= (1 - \varepsilon) \frac{2^n}{n} \log (2c(1 - \varepsilon)) - \varepsilon 2^n \rightarrow -\infty \quad (n \rightarrow \infty). \end{aligned}$$

Отсюда следует, что при $n > N$ логарифм отношения становится отрицательным, а само отношение будет меньше 1. Значит $|\mathfrak{S}(h, n)| < 2^{2^n}$, т. е.

найдутся функции, которые невозможно реализовать контактными схемами сложности, не превосходящей $\lceil (1 - \varepsilon) \frac{2^n}{n} \rceil$. Поэтому

$$L(n) > \left\lceil (1 - \varepsilon) \frac{2^n}{n} \right\rceil \quad \text{при } n > N,$$

что и доказывает теорему.

Следствие из доказательства. Доля тех функций, которые требуют более $(1 - \varepsilon) \frac{2^n}{n}$ контактов, стремится к 1 при $n \rightarrow \infty$ или, как говорят, почти для всех булевых функций от n переменных $L(f) \gtrsim \frac{2^n}{n}$.

Непосредственно к данному результату примыкает теорема, установленная фактически Шенноном, о порядке функций $L(n)$.

Т е о р е м а 3. $L(n) \asymp \frac{2^n}{n}$.

§ 5. Асимптотически наилучший метод синтеза контактных схем

Данный метод был предложен в 1958 г. О. Б. Лупановым и использует две весьма существенные идеи. Первая из них связана с асимптотически в два раза более простой реализацией множества всех конъюнкций $y_1^{\sigma_1} \& \dots \& y_k^{\sigma_k}$, чем это дает контактное дерево с k ярусами. Вторая идея появилась из анализа конструкции Шеннона, сделанного самим Шенноном. Оказалось, что множитель при $\frac{2^n}{n}$ имеет форму «пилы», так как при $n \rightarrow \infty$ колеблется между 2 и 4. Упомянутая идея связана с идеей сглаживания этой пилы.

Изложению метода предпослём два вспомогательных построения.

1. Правильное представление булевой функции $f(x_1, \dots, x_n)$ с параметрами k и s .

Рассмотрим прямоугольную таблицу, строки которой занумерованы наборами $(\sigma_1, \dots, \sigma_k)$, где k — заданный параметр, а столбцы — наборами $(\sigma_{k+1}, \dots, \sigma_n)$ (см. табл. 3).

Т а б л и ц а 3

	0	σ_{k+1}	1	x_{k+1}
	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$x_1 \dots x_k$	0	σ_n	1	x_n
0 ... 0				s
				s
				$f(\sigma_1, \dots, \sigma_k, \sigma_{k+1}, \dots, \sigma_n)$
$\sigma_1 \dots \sigma_k$				s
1 ... 1				s'

В клетку на пересечении строки с номером $(\sigma_1, \dots, \sigma_k)$ и столбца с номером $(\sigma_{k+1}, \dots, \sigma_n)$ вписывается значение $f(\sigma_1, \dots, \sigma_k, \sigma_{k+1}, \dots, \sigma_n)$. Таким образом, получается таблица, заполненная числами 0 и 1. Нетрудно видеть, что она однозначным образом определяет булеву функцию.

Выберем второй параметр s и разрежем эту таблицу (сверху вниз) на горизонтальные полосы шириной s (по s строчек). При этом последняя полоса может оказаться не полной и будет содержать s' ($s' \leq s$) строк. Занумеруем полосы числами (сверху вниз) $1, 2, \dots, p$, где $p = \lceil \frac{2^k}{s} \rceil$.

Обозначим через $f_i(x_1, \dots, x_n)$ функцию, определяемую следующим образом:

$$f_i(\sigma_1, \dots, \sigma_n) = \begin{cases} f(\sigma_1, \dots, \sigma_n), & \text{если } (\sigma_1, \dots, \sigma_k) \text{ принадлежит } i\text{-й полосе,} \\ 0 & \text{в остальных случаях.} \end{cases}$$

Очевидно,

$$f(x_1, \dots, x_n) = \bigvee_{i=1}^p f_i(x_1, \dots, x_n).$$

Далее, возьмем i -ю полосу и в ней столбцы разобьем на группы так, что каждая группа содержит столбцы одного сорта, а разные группы — столбцы разных сортов. Произведем, далее, нумерацию групп числами $1, 2, \dots, t(i)$, где, очевидно, $t(i) \leq 2^s$.

Обозначим через $f_{i,j}(x_1, \dots, x_n)$ функцию, определенную следующим образом

$$f_{i,j}(\sigma_1, \dots, \sigma_n) = \begin{cases} f_i(\sigma_1, \dots, \sigma_n), & \text{если } (\sigma_{k+1}, \dots, \sigma_n) \text{ определяет} \\ & \text{столбец из } j\text{-й группы,} \\ 0 & \text{в остальных случаях.} \end{cases}$$

Поскольку на наборе $(\sigma_1, \dots, \sigma_k)$, принадлежащем i -й полосе, в пределах j -й группы значение $f_{i,j}$ постоянно, то

$$f_{i,j}(x_1, \dots, x_n) = f_{i,j}^{(1)}(x_1, \dots, x_k) \& f_{i,j}^{(2)}(x_{k+1}, \dots, x_n),$$

где $f_{i,j}^{(1)}(x_1, \dots, x_k)$ — характеристическая³ функция номеров $(\sigma_1, \dots, \sigma_k)$ тех строк i -й полосы, на которых $f_{i,j}(\sigma_1, \dots, \sigma_k) = 1$, а $f_{i,j}^{(2)}(x_{k+1}, \dots, x_n)$ — характеристическая функция номеров столбцов $(\sigma_{k+1}, \dots, \sigma_n)$, определяющих j -ю группу i -й полосы.

Мы получаем правильное представление функции f с параметрами k, s

$$f(x_1, \dots, x_n) = \bigvee_{i=1}^p \bigvee_{j=1}^{t(i)} f_{i,j}^{(1)}(x_1, \dots, x_k) \& f_{i,j}^{(2)}(x_{k+1}, \dots, x_n).$$

³Функция называется характеристической для данного множества, если она на нем равна 1, а вне его — 0.

2. Разбиение куба на сферы. Как известно из дискретной математики, при $r = 2^p$ единичный r -мерный куб разбивается в прямую сумму единичных сфер. Рассмотрим какое-нибудь конкретное разбиение множества точек $(\beta_1, \dots, \beta_r)$ единичного r -мерного куба в прямую сумму единичных сфер. Пусть центрами этих сфер являются вершины $(\beta_1^h, \dots, \beta_r^h)$, где $h = 1, 2, \dots, \frac{2^r}{r}$. Обозначим через $\varphi_h(z_1, \dots, z_r)$ характеристическую функцию сферы с центром $(\beta_1^h, \dots, \beta_r^h)$. Очевидно,

$$\varphi_h(z_1, \dots, z_r) = z_1^{\beta_1^h} z_2^{\beta_2^h} \dots z_r^{\beta_r^h} \vee z_1^{\beta_1^h} z_2^{\bar{\beta}_2^h} \dots z_r^{\beta_r^h} \vee \dots \vee z_1^{\beta_1^h} z_2^{\beta_2^h} \dots z_r^{\bar{\beta}_r^h}.$$

Легко видеть, что $\bigvee_{h=1}^{2^r/r} \varphi_h = 1$,

$$\varphi_h \cdot z_\nu^{\bar{\beta}_\nu^h} = z_1^{\beta_1^h} \dots z_\nu^{\bar{\beta}_\nu^h} \dots z_r^{\beta_r^h} \quad \text{и} \quad \varphi_h z_\nu^{\bar{\beta}_\nu^h} \cdot z_\mu^{\bar{\beta}_\mu^h} \equiv 0 \quad \text{при} \quad \nu \neq \mu.$$

Положим далее, взяв $z_1 = x_{k+1}, \dots, z_r = x_{k+r}$,

$$f_{i,j,h}(x_{k+1}, \dots, x_n) = f_{i,j}^{(2)}(x_{k+1}, \dots, x_n) \varphi_h(x_{k+1}, \dots, x_{k+r}).$$

Тогда

$$\begin{aligned} f(x_1, \dots, x_n) &= \bigvee_{i=1}^p \bigvee_{j=1}^{t(i)} f_{i,j}^{(1)} f_{i,j}^{(2)} = \bigvee_{i=1}^p \bigvee_{j=1}^{t(i)} f_{i,j}^{(1)} f_{i,j}^{(2)} \bigvee_{h=1}^{2^r/r} \varphi_h = \\ &= \bigvee_{i=1}^p \bigvee_{j=1}^{t(i)} \bigvee_{h=1}^{2^r/r} f_{i,j}^{(1)} f_{i,j,h}. \end{aligned} \quad (*)$$

Теорема 4 (Лупанов [13]). *Существует метод синтеза A_4 такой, что для каждой булевой функции f он дает контактную схему Σ_f , реализующую f , такую, что*

$$L_{A_4}(\Sigma_f) \leq \frac{2^n}{n} \left(1 + O\left(\frac{1}{\sqrt{n}}\right) \right) \quad \text{при} \quad n \geq N.$$

Доказательство. Возьмем разложение (*) произвольной булевой функции $f = f(x_1, \dots, x_n)$. Схему Σ_f будем строить как параллельное соединение схем Σ_f^i , реализующих функции f_i ($i = 1, \dots, p$). В свою очередь, схема Σ_f^i будет строиться в виде системы многополюсников $M_1^i, \dots, M_6^i$, каждый из которых является продолжением предыдущего (при $i > 1$) (рис. 9) так, что $\Sigma_f^i = M_6^i$.

Перейдем к описанию многополюсников $M_1^i, \dots, M_6^i$ и оценке их сложности (см. также рис. 10).

M_1^i — контактное дерево по переменным $x_{k+1}, \dots, x_{k+r}$,

$$L(M_1^i) < 2 \cdot 2^r.$$

62002760

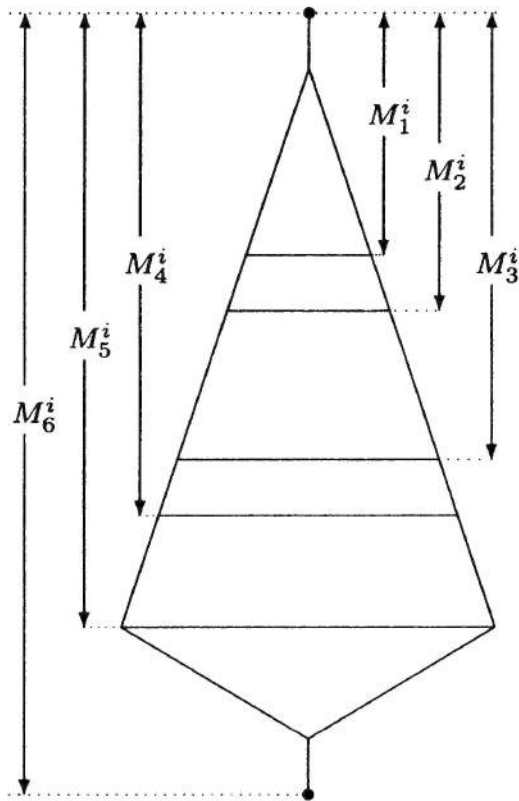


Рис. 9

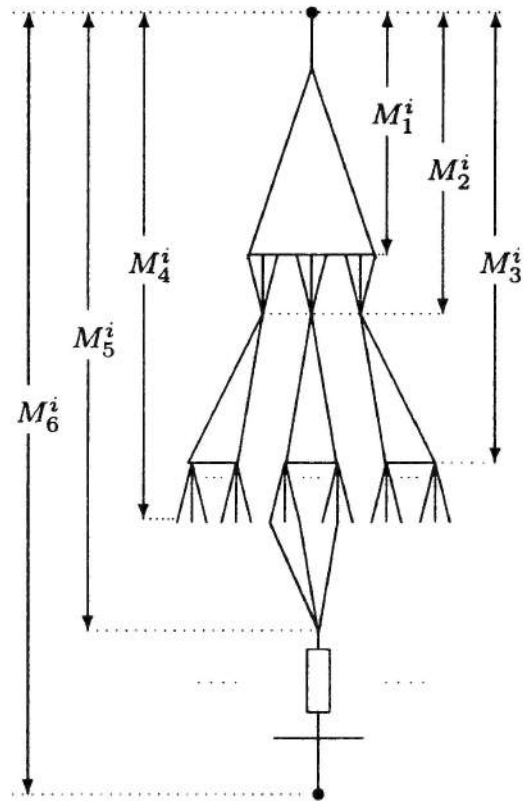


Рис. 10

M_2^i — получается из M_1^i . Выходам M_1^i соответствуют вершины r -мерного единичного куба. Выходы, отвечающие одной и той же сфере (их r штук), склеиваются вместе и дают выход многополюсника M_2^i . Очевидно, M_2^i реализует все характеристические функции $\varphi_1, \dots, \varphi_{2^r/r}$ и

$$L(M_2^i \setminus M_1^i) = 0.$$

M_3^i — получается из M_2^i подвешиванием к его выходам контактных деревьев по переменным $x_{k+r+1}, \dots, x_n$. На выходах M_3^i реализуются функции вида

$$x_{k+r+1}^{\sigma_{k+r+1}} \& \dots \& x_n^{\sigma_n} \varphi_h$$

и

$$L(M_3^i \setminus M_2^i) < 2 \cdot 2^{n-k-r} \frac{2^r}{r} = \frac{2 \cdot 2^{n-k}}{r}.$$

M_4^i — получается из M_3^i подвешиванием к его выходам пучков из r контактов (метелок). Если выход принадлежит дереву, подвешенному к h -й сфере, то метелка состоит из контактов

$$x_{k+1}^{\bar{\beta}_{k+1}^h}, \dots, x_{k+r}^{\bar{\beta}_{k+r}^h}$$

(рис. 11). На выходах M_4^i реализуются $x_{k+1}^{\sigma_{k+1}} \& \dots \& x_n^{\sigma_n}$ и

$$L(M_4^i \setminus M_3^i) = 2^{n-k}.$$

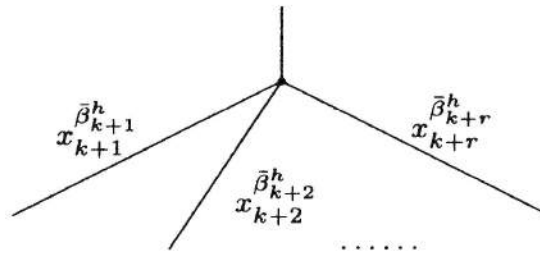


Рис. 11

M_5^i — получается из M_4^i : для каждого j и h функция $f_{i,j,h}$ разлагается в совершенную д.н.ф. и выходы M_4^i , соответствующие членам этой д.н.ф., объединяются и образуют новый выход — выход M_5^i . Тогда на выходах M_5^i реализуются функции $f_{i,j,h}$ и

$$L(M_5^i \setminus M_4^i) = 0.$$

M_6^i — получается из M_5^i подвешиванием к выходам, реализующим $f_{i,j,h}$, схем, реализующих по совершенным д.н.ф. функции $f_{i,j}^{(1)}$, и последующим объединением их выходов;

$$L(M_6^i \setminus M_5^i) \leq 2^s \cdot \frac{2^r}{r} \cdot k \cdot s.$$

Утверждается, что M_6^i реализует функцию f_i , а также и то, что M_5^i реализует функцию $f_{i,j,h}$. Необходимость доказательства этого факта связана с тем, что при объединении выходов метелок могут возникнуть незапланированные, ложные цепи вида, как указано на рис. 12.

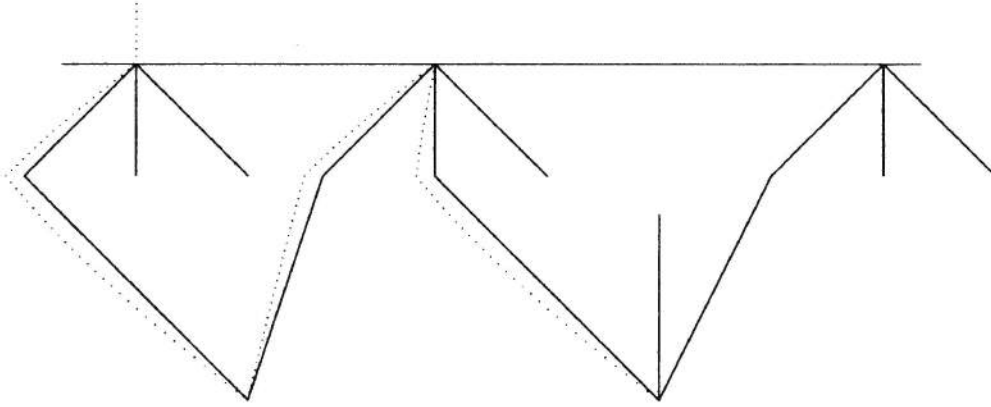


Рис. 12

В силу того, что подобные переплетения соединений происходят в пределах одной и той же h -й сферы, в этой цепи обязательно встретятся два различных контакта вида $x_{k+\nu}^{\bar{\beta}_{k+\nu}^h}$ и $x_{k+\mu}^{\bar{\beta}_{k+\mu}^h}$ ($\nu \neq \mu$) и тогда

$$x_{k+\nu}^{\bar{\beta}_{k+\nu}^h} \& x_{k+\mu}^{\bar{\beta}_{k+\mu}^h} \& \varphi_h \equiv 0.$$

Поэтому такие цепи имеют нулевую проводимость и никак не влияют на проводимость всей схемы.

Продолжим оценку сложности схемы Σ_f :

$$L(\Sigma_f) \leq \left(\frac{2^k}{s} + 1 \right) \left(2 \cdot 2^r + \frac{2^{n-k+1}}{r} + 2^{n-k} + \frac{2^{r+s} \cdot k \cdot s}{r} \right).$$

Положим $r = 2^{\lceil 1/2 \log n \rceil}$, $k = \lfloor 2 \log n \rfloor$, и $s = \lfloor n - 2\sqrt{n} \rfloor$. Тогда $\frac{2^k}{s} + 1 \sim \frac{2^k}{s}$ и

$$L(\Sigma_f) \lesssim \frac{2 \cdot 2^{k+r}}{s} + \frac{2^{n+1}}{s \cdot r} + \frac{2^n}{s} + \frac{2^{k+r+s} k}{r}.$$

Поскольку $\frac{1}{2}\sqrt{n} < r \leq \sqrt{n}$, $2^k \leq n^2$, то

$$2 \frac{2^{k+r}}{s} \lesssim 2n2^{\sqrt{n}} = o\left(\frac{2^n}{n\sqrt{n}}\right),$$

$$\frac{2^{n+1}}{s \cdot r} \lesssim \frac{4 \cdot 2^n}{n\sqrt{n}} = O\left(\frac{2^n}{n\sqrt{n}}\right),$$

$$\frac{2^n}{s} \sim \frac{2^n}{n},$$

$$\frac{2^{k+r+s} \cdot k}{r} \leq \frac{2^{2 \log n + n - \sqrt{n}} 2 \log n}{\frac{1}{2}\sqrt{n}} = 4n^{3/2} \log n \frac{2^n}{2^{\sqrt{n}}} = o\left(\frac{2^n}{n\sqrt{n}}\right).$$

Значит

$$L(\Sigma_f) \lesssim \frac{2^n}{n} \left(1 + O\left(\frac{1}{\sqrt{n}}\right) \right).$$

Теорема доказана.

Из доказательства видно, что основная часть схемы Σ_f сосредоточена в метелках, а все остальное составляет малую долю от $\frac{2^n}{n}$. Из данной теоремы и нижней оценки для $L(n)$ (теоремы 2) вытекает

Т е о р е м а 5. $L(n) \sim \frac{2^n}{n}$.

§ 6. Синтез p -полюсных ($p \geq 2$) контактных схем

Мы видели, что p -полюсная контактная схема реализует матрицу $\Phi = M$ из булевых функций специального вида, т. е.

$$M = \|f_{i,j}(x_1, \dots, x_n)\|$$

и выполнены 3 свойства. Каждый набор $(\alpha_1, \dots, \alpha_n)$ приводит в схеме Σ к разбиению $R_{\alpha_1, \dots, \alpha_n}$ ее полюсов в прямую сумму множеств, в каждом из

которых при $x_1 = \alpha_1, \dots, x_n = \alpha_n$ полюса соединены друг с другом. Таким образом, функционирование схемы Σ можно характеризовать таблицей разбиений (см. табл. 4).

Т а б л и ц а 4

$x_1 \ x_2 \ \dots \ x_n$	
0 0 ... 0	$R_{00 \dots 0}$
0 0 ... 1	$R_{00 \dots 1}$
.....	
.....	
$\alpha_1 \ \alpha_2 \ \dots \ \alpha_n$	$R_{\alpha_1 \ \alpha_2 \ \dots \ \alpha_n}$
.....	
.....	
1 1 ... 1	$R_{11 \dots 1}$

Легко видеть, что произвольной таблице такого вида соответствует p -полюсная схема ее реализующая: нужно вершины каждой компоненты разбиения $R_{\alpha_1, \dots, \alpha_n}$ соединить друг с другом цепочками последовательно соединенных контактов $x_1^{\alpha_1}, \dots, x_n^{\alpha_n}$. Отсюда следует, что число попарно неэквивалентных матриц порядка p из булевых функций $f_{i,j}(x_1, \dots, x_n)$, удовлетворяющих перечисленным свойствам, равно $\Phi(p)^{2^n}$, где $\Phi(p)$ — число разбиений множества из p элементов.

Разбиению $R_{\alpha_1, \dots, \alpha_n}$ соответствует матрица $M_{\alpha_1, \dots, \alpha_n}$ из 0 и 1 порядка p , получаемая из M при $x_1 = \alpha_1, \dots, x_n = \alpha_n$. Эта матрица состоит из попарно непересекающихся ящиков, сплошь заполненных 1 и расположенных по диагонали. Обозначим через $M_{\sigma_{i_1}, \dots, \sigma_{i_s}}^{x_{i_1}, \dots, x_{i_s}}$ значение матрицы при $x_{i_1} = \sigma_{i_1}, \dots, x_{i_s} = \sigma_{i_s}$. Используя эти обозначения, мы получаем аналог разложения булевой функции по переменным $x_1, \dots, x_k$

$$\begin{aligned}
 M &= \|f_{i,j}(x_1, \dots, x_n)\| = \left\| \bigvee_{(\sigma_1, \dots, \sigma_k)} x_1^{\sigma_1} \dots x_k^{\sigma_k} f_{i,j}(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n) \right\| = \\
 &= \bigvee_{(\sigma_1, \dots, \sigma_k)} x_1^{\sigma_1} \dots x_k^{\sigma_k} M_{\sigma_1, \dots, \sigma_k}^{x_1, \dots, x_k}.
 \end{aligned}$$

В частности, для $k = 1$ и $k = n$ имеет аналог разложения по переменному и в совершенную д.н.ф.

$$\begin{aligned}
 M &= x_n M_1^{x_n} \vee \bar{x}_n M_0^{x_n}, \\
 M &= \bigvee_{(\sigma_1, \dots, \sigma_n)} x_1^{\sigma_1} \dots x_n^{\sigma_n} M_{\sigma_1, \dots, \sigma_n}^{x_1, \dots, x_n} = \bigvee_{(\sigma_1, \dots, \sigma_n)} x_1^{\sigma_1} \dots x_n^{\sigma_n} M_{\sigma_1, \dots, \sigma_n}.
 \end{aligned}$$

На основе этих разложений можно предложить соответствующие обобщения методов синтеза для двухполюсных контактных схем. Например, аналог разложения в совершенную д.н.ф. дает схему, изображенную на рис. 13.

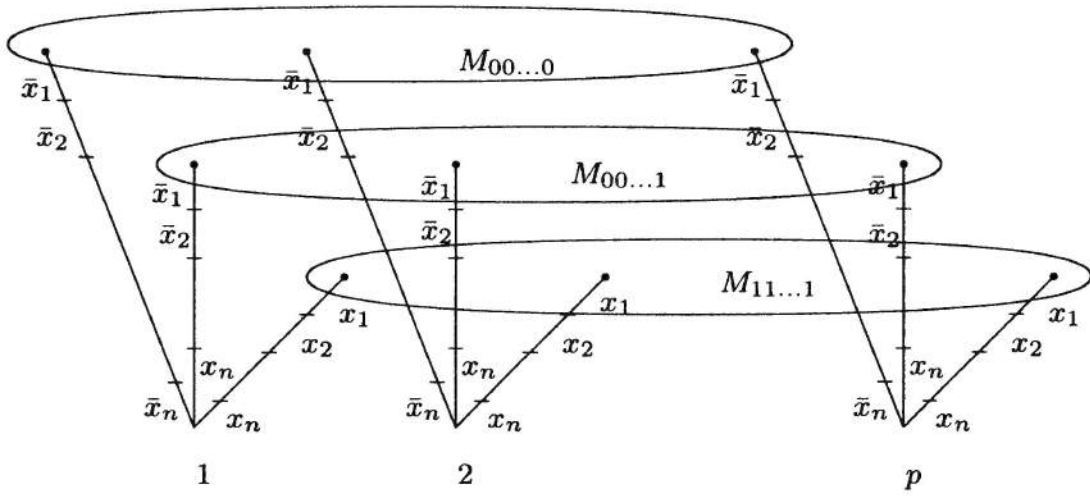


Рис. 13

Здесь из каждого полюса исходящие ветви $x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n}$ идут к разбиению, определяемому матрицей $M_{\sigma_1 \sigma_2 \dots \sigma_n}$, и таким образом, объединяются там в группы, соответствующие компонентам разбиения. Поскольку в каждой группе одну из цепочек $x_1^{\sigma_1} \dots x_n^{\sigma_n}$ можно заменить на ребро без нарушения свойств проводимости многополюсника, то

$$L(\Sigma) \leq (p-1)n2^n.$$

Если воспользоваться методом Лупанова при реализации каждой функции $f_{i,j}(x_1, \dots, x_n)$ ($1 \leq i < j \leq p$), то получим для $L(n, p)$ более сильную асимптотическую оценку

$$L(n, p) \lesssim \frac{p(p-1)}{2} \frac{2^n}{n}.$$

В то же время, так как число p -полюсных сетей, имеющих не более h ребер⁴, не превосходит $(ch)^h$ (отличается от оценки числа соответствующих графов не более, чем в $(2h)^p$ раз) и логарифм числа булевых матриц порядка p , удовлетворяющих специальным свойствам, равен $2^n \log \Phi(p)$, то, повторяя в точности таким же образом вывод нижней оценки функции Шеннона для контактных схем, получаем

$$L(n, p) \gtrsim \frac{2^n \log \Phi(p)}{n}.$$

⁴Поскольку $(ch)^h$ дает верхнюю оценку для числа графов с занумерованными вершинами, в которых полюсными вершинами можно считать вершины с концами $1, 2, \dots, p$.

ГЛАВА 2. КЛАСС СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

Дадим расшифровку абстрактной схемы. Здесь мы имеем:

$\mathfrak{S}_B$ — множество всех схем из функциональных элементов (Ф.Э.) в базисе B ;

$\mathfrak{F} = \Phi$ — множество булевых уравнений Φ (или систем $(f_1, \dots, f_p)$ булевых функций);

$L_B(\Sigma) \sum_{j=1}^h L(F_{i_j})$, где $F_{i_1}, \dots, F_{i_h}$ — совокупность всех элементов, встречающихся в Σ (полагаем $L_B(F_i) > 0$, $i = 1, \dots, r$).

В частности, может быть $L_B(F_i) \equiv 1$ для всех $i = 1, \dots, r$, тогда $L(\Sigma) = h$ — число элементов в схеме Σ .

Далее имеем $L_B(\Phi) = \min_{\Sigma \text{ реал. } \Phi} L_B(\Sigma) = \min_{\Sigma} L_B(\Sigma)$ — минимальная сложность схемы, реализующей Φ (здесь $\min$ всегда существует);

$\mathfrak{F}_{n,p}$ — множество булевых уравнений вида

$$\begin{cases} z_1 = f_1(x_1, \dots, x_n), \\ \dots\dots\dots \\ z_p = f_p(x_1, \dots, x_n) \end{cases}$$

(очевидно $|\mathfrak{F}_{n,p}| < +\infty$);

$L_B(n, p)$ — функция Шеннона — определена для любых p и n ; при $p = 1$ для краткости будем писать $L_B(n, 1) = L_B(n)$.

В этом разделе речь будет идти о синтезе схем в следующем базисе:

$B_0 = \left\{ \begin{array}{c} \downarrow \\ \nabla \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ - \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ \nabla \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \& \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ \nabla \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \vee \\ \downarrow \end{array} \right\}$, где $L_{B_0}(F_i) \equiv 1$ и $p = 1$. В этом случае функцию Шеннона обозначим через $L(n)$.

§ 1. Простейшие методы синтеза

1. Синтез схем по совершенной д.н.ф. (алгоритм A_1):

а) если $f \equiv \text{const}$, то в качестве Σ_f берем схему, изображенную на рис. 14;

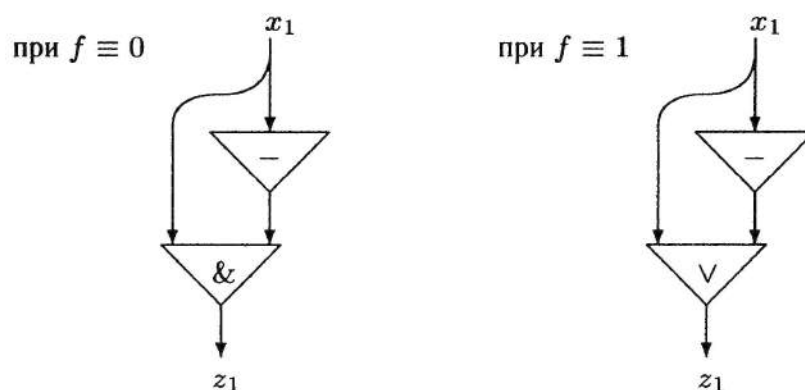


Рис. 14

б) если $f \neq \text{const}$, то разлагаем ее в совершенную д.н.ф.,

$$f(x_1, \dots, x_n) = \bigvee_{i=1}^s K_i \quad \text{где} \quad K_i = x_1^{\sigma_1^{(i)}} \& \dots \& x_n^{\sigma_n^{(i)}}.$$

Для удобства изображения схем введем вспомогательный «элемент» σ (рис. 15). На рис. 16 изображена схема Σ_{K_i} , реализующая отдельную конъюнкцию K_i , а на рис. 17 — схема, реализующая набор конъюнкций $K_1, \dots, K_s$, в ней инверторы обслуживают одновременно несколько схем Σ_{K_i} . Наконец, на рис. 18 изображена схема, реализующая Σ_f . Очевидно $L_{A_1}(\Sigma_f) \leq n + s(n - 1) + s - 1 < n(s + 1) \leq n2^n$, так как $f \neq 1$.

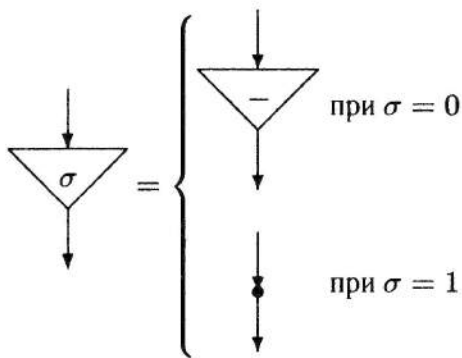


Рис. 15

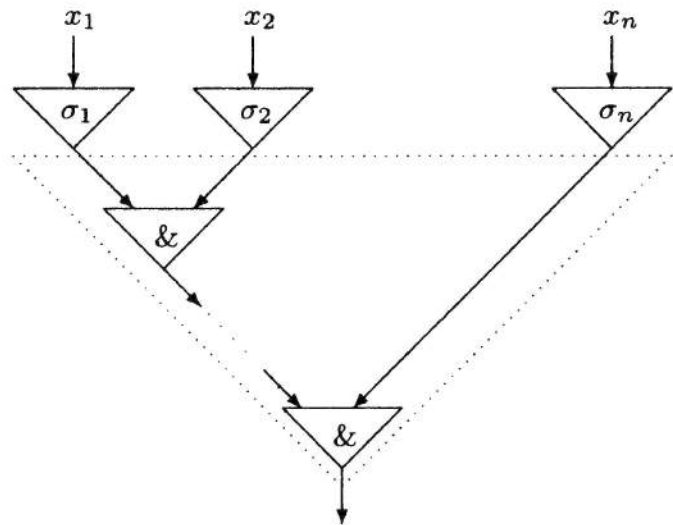


Рис. 16

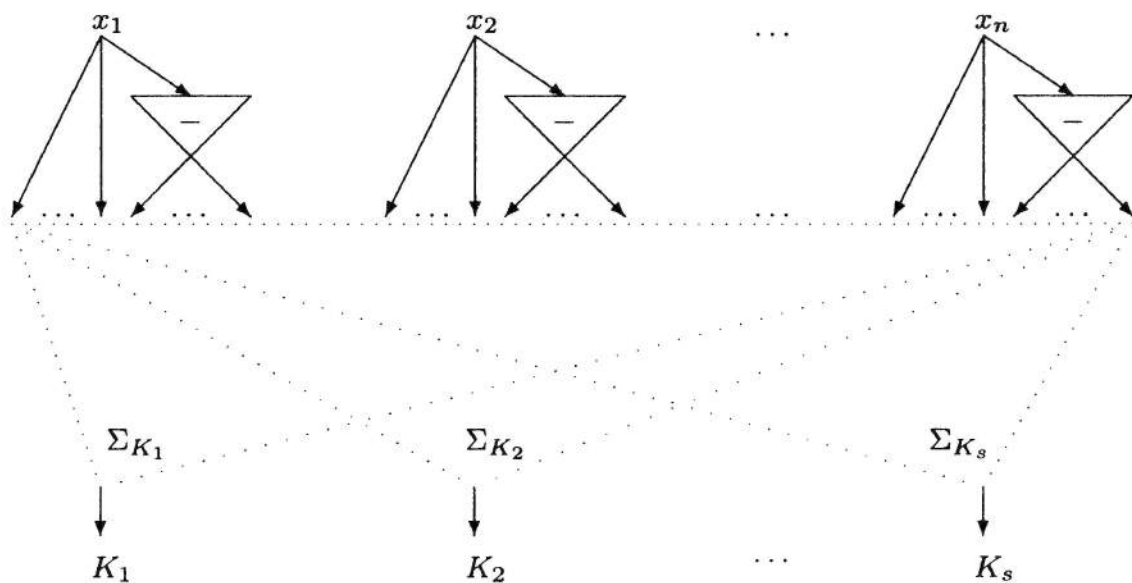


Рис. 17

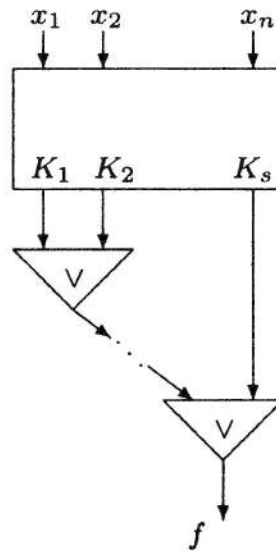


Рис. 18

2. Метод, основанный на разложении функции f по переменному x_n (алгоритм A_2).

Рассмотрим разложение

$$f(x_1, \dots, x_n) = x_n \& f' \vee \bar{x}_n \& f'',$$

где $f' = f(x_1, \dots, x_{n-1}, 1)$, $f'' = f(x_1, \dots, x_{n-1}, 0)$.

На рис. 19 представлена индуктивная процедура построения схемы Σ_f . Мы имеем

$$L_{A_2}(1) = 2;$$

$$L_{A_2}(n) \leq 2L_{A_2}(n-1) + 4 \quad \text{или} \quad L_{A_2}(n) \leq 3 \cdot 2^n - 4.$$

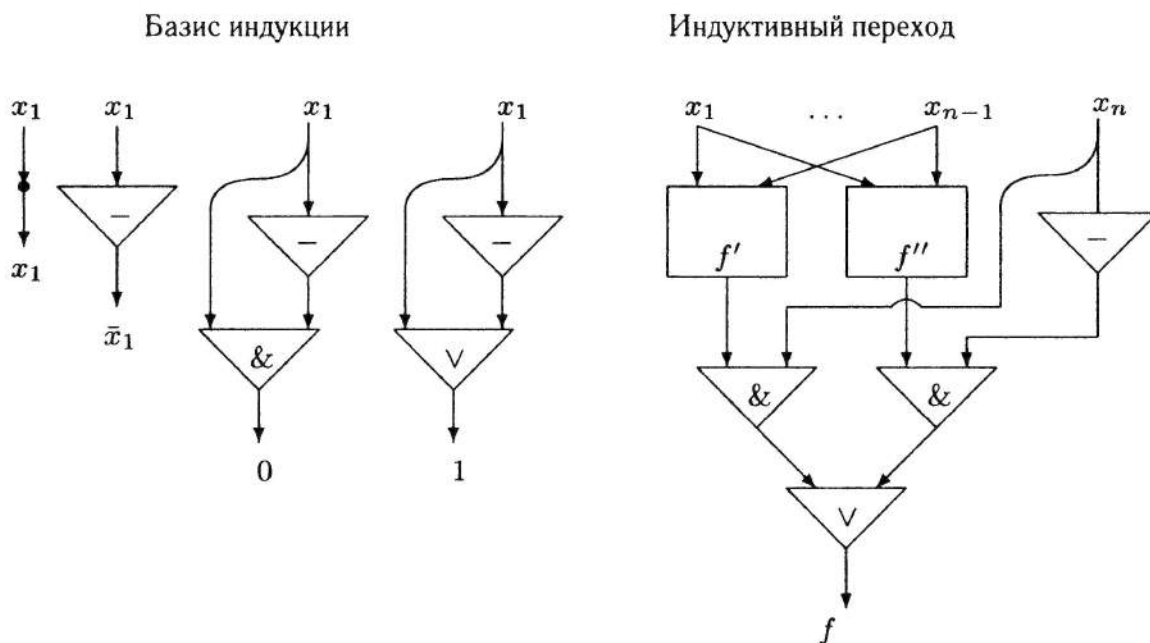


Рис. 19

§ 2. Алгоритм полного перебора

Здесь покажем, что существует алгоритм (A_2) , который для каждой системы $\{\Phi\}$ булевых уравнений

[illegible]

строит минимальную схему $\Sigma_{\{F\}}$ из функциональных элементов (Ф.Э.) в базисе B_0 .

Для этого последовательно просматриваем все схемы со входами $x_1, \dots, x_n$ и выходами $z_1, \dots, z_p$ в данном базисе с числом элементов h .

Берем $h = 0$. Мы имеем конечное число схем, не содержащих элементов — это схемы, у которых каждый выход соединен не более, чем с одним входом, а входы могут соединяться с несколькими выходами. Для каждой схемы проверим, реализует она данную систему уравнений или нет. Таким образом, либо мы найдем требуемую схему (она, очевидно, будет минимальной, так как $L(\Sigma_{\{\Phi\}}) = 0$), либо среди схем сложности $h = 0$ искомой схемы нет. В последнем случае минимальная схема имеет сложность $L(\Sigma) > 0$.

Берем $h = 1$. Мы имеем конечное число схем, содержащих один элемент. Для каждой схемы проверяем, реализует она данную систему уравнений или нет. В результате этого, мы либо найдем требуемую схему, и она будет минимальной, либо среди схем сложности $h = 0$ и $h = 1$ искомой схемы нет. В последнем случае минимальная схема Σ имеет сложность $L(\Sigma) > 1$ и т. д. В силу того, что данная система может быть реализована, например, каждая строчка по совершенной д.н.ф., то приведенный выше процесс должен окончиться, и в результате мы получим минимальную схему.

§ 3. Метод Шеннона

В случае схем из Ф.Э. может быть использован метод Шеннона.

Пусть $\{f_1(x_1, \dots, x_n), \dots, f_s(x_1, \dots, x_n)\}$ — множество булевых функций ($f_i \neq f_j$ при $i \neq j$).

О п р е д е л е н и е. Многополюсник из Ф.Э., имеющий n входов $x_1, \dots, x_n$ и s выходов, называется универсальным для данного множества функций, если для каждого i ($1 \leq i \leq s$) найдется в многополюснике выход $\tau(i)$ такой, что на нем реализуется функция $f_i(x_1, \dots, x_n)$.

Лемма 3. Для любого n ($n \geq 1$) можно построить универсальный многополюсник U_n для множества всех булевых функций от n переменных $x_1, \dots, x_n$ и

$$L(U_n) \leq 2 \cdot 2^{2^n}.$$

Доказательство. Построение многополюсника U_n будем осуществлять индуктивным образом.

Базис индукции ($n = 1$). В качестве U_1 возьмем многополюсник, изображенный на рис. 20. Мы имеем $L(U_1) = 3 < 2 \cdot 2^1$.

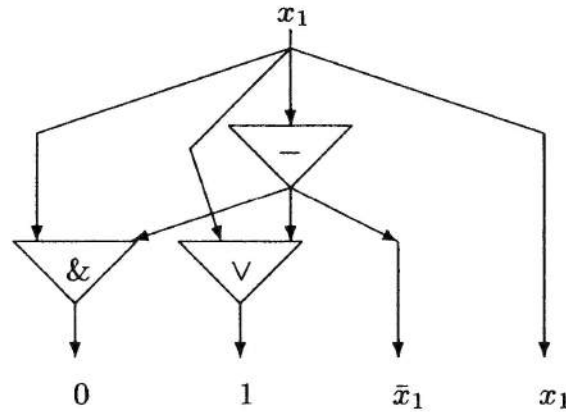


Рис. 20

Индуктивный переход. Предположим, что построен универсальный многополюсник U_{n-1} для множества всех булевых функций, зависящих от переменных $x_1, \dots, x_{n-1}$ и $L(U_{n-1}) \leq 2 \cdot 2^{2^{n-1}}$. Рассмотрим разложение

$$f(x_1, \dots, x_n) = x_n f'(x_1, \dots, x_{n-1}) \vee \bar{x}_n f''(x_1, \dots, x_{n-1}).$$

В зависимости от вида функций f' и f'' множество всех булевых функций от переменных $x_1, \dots, x_n$ разобьем на три непересекающихся класса.

I. При $f' \equiv f'' \equiv 0$ класс содержит одну функцию $f \equiv 0$.

II. Ровно одна из функций f' и f'' тождественно равна 0. В этом случае f имеет вид

$$f = x_n f'(x_1, \dots, x_{n-1}) \quad \text{при } f'' \equiv 0$$

или

$$f = \bar{x}_n f''(x_1, \dots, x_{n-1}) \quad \text{при } f' \equiv 0.$$

В этом классе имеется $2(2^{2^{n-1}} - 1)$ функций.

III. Все остальные функции, т. е. функции f , у которых $f' \not\equiv 0$ и $f'' \not\equiv 0$. В этом классе содержится

$$2^{2^n} - 2(2^{2^{n-1}} - 1) - 1$$

функций.

На рис. 21 изображен многополюсник U_n . Здесь выходы многополюсника U_{n-1} занумерованы числами $1, \dots, 2^{2^{n-1}}$, причем считается, что на выходе 1 реализуется константа 0.

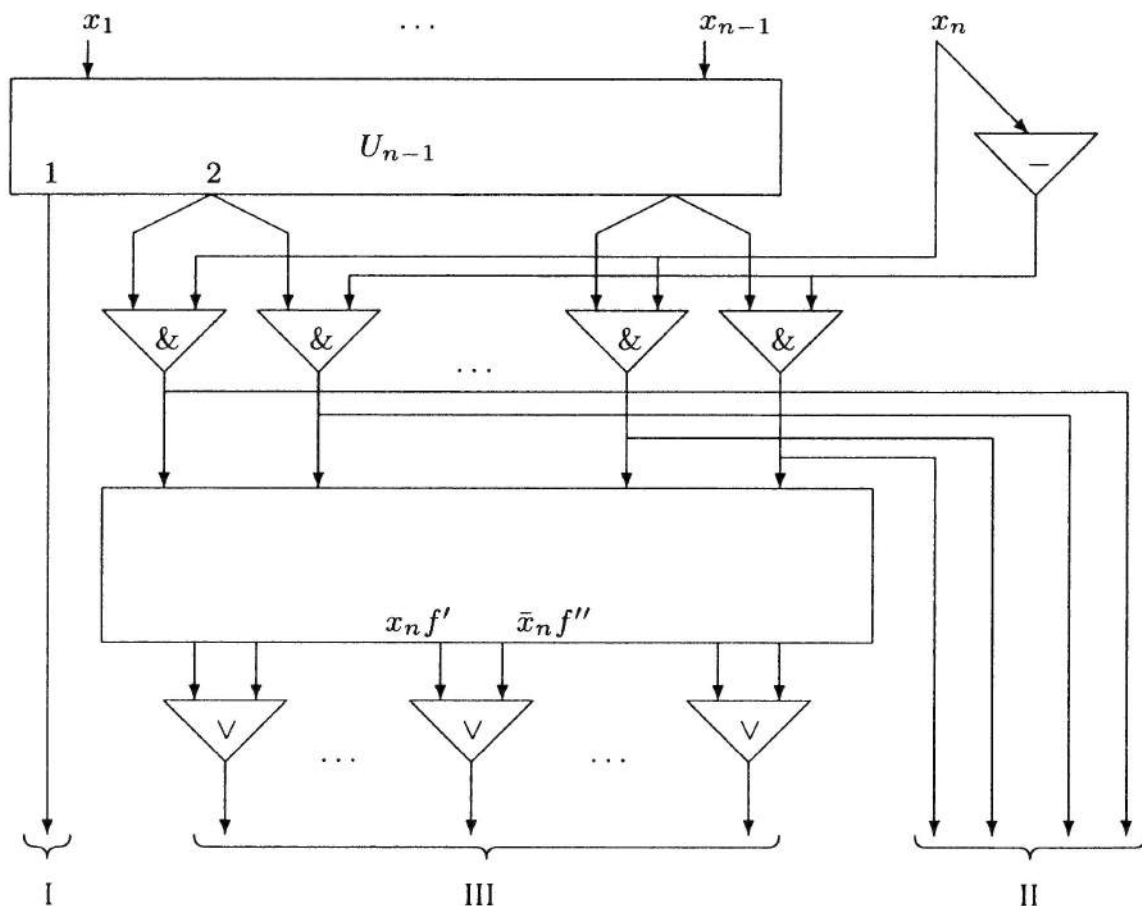


Рис. 21

Выходы многополюсника U_n разбиты на три класса в соответствии с разбиением множества всех булевых функций, зависящих от переменных $x_1, \dots, x_n$.

Данный многополюсник содержит:

- а) подсхему U_{n-1} и вне ее еще
- б) один инвертор,
- в) $2(2^{2^{n-1}} - 1)$ конъюнкторов,
- г) $2^{2^n} - 2(2^{2^{n-1}} - 1) - 1$ дизъюнкторов.

Таким образом,

$$L(U_n) = L(U_{n-1}) + 1 + 2(2^{2^{n-1}} - 1) + 2^{2^n} - 2(2^{2^{n-1}} - 1) - 1 \leq 2 \cdot 2^{2^{n-1}} + 1 + 2^{2^n} \leq 2 \cdot 2^{2^n}.$$

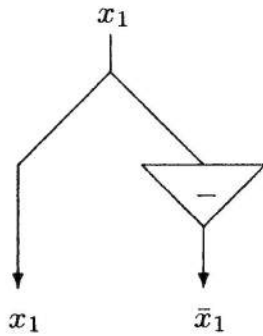
Лемма доказана.

Л е м м а 4 (о реализации множества всех конъюнкций). *Можно построить для любого $n > 0$ из Ф.Э. многополюсник V_n с n входами $x_1, \dots, x_n$ и 2^n выходами, реализующий все конъюнкции вида $x_1^{\sigma_1}, \dots, x_n^{\sigma_n}$ и*

$$L(V_n) = 2 \cdot 2^n + n - 4.$$

Доказательство. На рис. 22 представлено индуктивное построение указанного многополюсника.

Базис индукции



Индуктивный переход

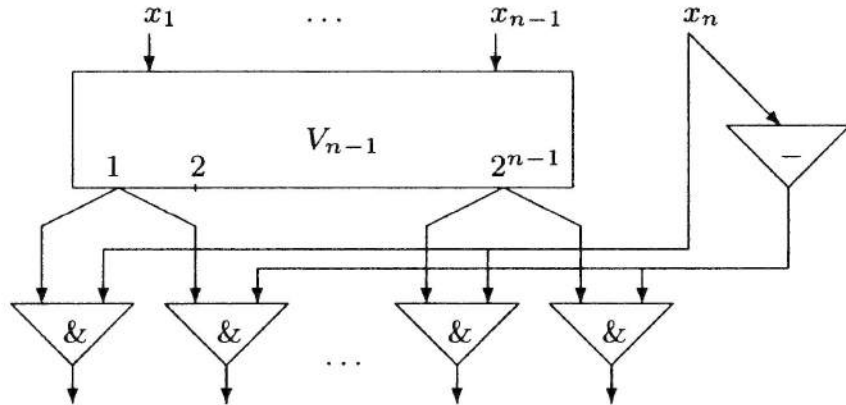


Рис. 22

Мы имеем

$$L(V_1) = 1,$$

$$L(V_n) = L(V_{n-1}) + 1 + 2^n = 2 \cdot 2^{n-1} + n - 5 + 1 + 2^n = 2 \cdot 2^n + n - 4.$$

Лемма доказана.

Теорема 6 (см. К. Э. Шеннон [43]). Существует метод синтеза (алгоритм A_3), который для булевой функции $f(x_1, \dots, x_n)$ позволяет построить схему из Ф.Э. Σ_f и $L_{A_3}(\Sigma_f) \lesssim 8 \frac{2^n}{n}$.

Доказательство. Возьмем разложение

$$f(x_1, \dots, x_n) = \bigvee_{(\sigma_1, \dots, \sigma_{n-k})} x_1^{\sigma_1} \& \dots \& x_{n-k}^{\sigma_{n-k}} f(\sigma_1, \dots, \sigma_{n-k}, x_{n-k+1}, \dots, x_n).$$

Рассмотрим схему Σ_f , изображенную на рис. 23. В этой схеме выделены:

V_{n-k} — многополюсник универсальный для всех конъюнкций

$$K_{\sigma_1, \dots, \sigma_{n-k}} = x_1^{\sigma_1} \& \dots \& x_{n-k}^{\sigma_{n-k}}$$

(k — фиксированное число);

U_k — многополюсник универсальный для множества всех булевых функций, которые зависят от переменных $x_{n-k+1}, \dots, x_n$, где через $\tau(\sigma_1, \dots, \sigma_{n-k})$ обозначен его выход, на котором реализуется функция

$$f(\sigma_1, \dots, \sigma_{n-k}, x_{n-k+1}, \dots, x_n).$$

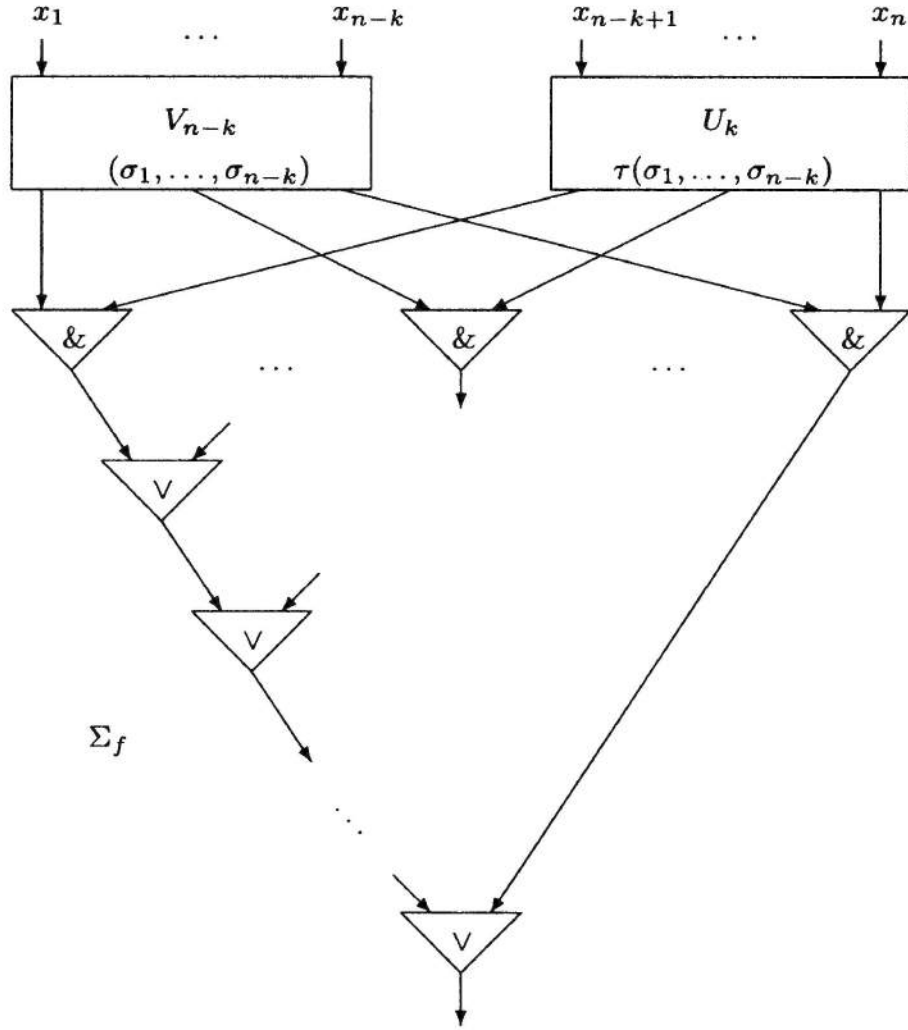


Рис. 23

Легко видеть, что данная схема Σ_f реализует функцию $f(x_1, \dots, x_n)$ в соответствии с приведенным выше разложением. Оценим сложность Σ_f

$$\begin{aligned}
 L(\Sigma_f) &\leq L(V_{n-k}) + L(U_k) + 2 \cdot 2^{n-k} - 1 \leq \\
 &\leq 2 \cdot 2^{n-k} + n - k - 4 + 2 \cdot 2^{2^k} + 2 \cdot 2^{n-k} - 1 = \\
 &= 4 \cdot 2^{n-k} + 2 \cdot 2^{2^k} + n - k - 5.
 \end{aligned}$$

Подберем параметр k так, чтобы правая часть этого неравенства стала возможно меньше. Так как нас интересует порядок величины $L_{A_3}(\Sigma_f)$, то вместо минимума правой части, который в дискретном случае вычисляется сложно, мы возьмем значение правой части при $k = \lceil \log(n - 2 \log n) \rceil$.

Мы имеем

$$\begin{aligned}
 \frac{1}{2}(n - 2 \log n) &< 2^k \leq n - 2 \log n, \\
 L_{A_3}(\Sigma_f) &\lesssim 4 \frac{2^n}{2^k} + 2 \cdot 2^{2^k} \lesssim \frac{4 \cdot 2^n}{\frac{1}{2}(n - 2 \log n)} + 2 \cdot \frac{2^n}{n^2} \lesssim 8 \frac{2^n}{n}.
 \end{aligned}$$

Теорема доказана.

Учитывая полученную нижнюю оценку (см. § 5), мы получаем

$$L(n) \asymp \frac{2^n}{n}$$

и значит, алгоритм A_3 является наилучшим по порядку.

§ 4. Асимптотически наилучший метод синтеза схем из функциональных элементов в базисе $\{\&, \vee, -\}$

Здесь мы несколько отступаем от того плана, которому мы следовали при рассмотрении синтеза контактных схем. Нам удобнее, чтобы не нарушить целостности изложения, сначала завершить изложение универсальных методов синтеза схем из Ф.Э., а затем перейти к рассмотрению нижних оценок.

Асимптотически наилучший метод синтеза для схем из Ф.Э. был предложен О.Б. Лупановым вслед за решением аналогичного вопроса для контактных схем. При этом оказалось, что для синтеза схем из Ф.Э. в базисе B_0 конструкция выглядит значительно проще.

Теорема 7 (О.Б. Лупанов [15]). *Существует метод синтеза A_4 такой, что для любой булевой функции f он дает схему Σ_f из Ф.Э. в базисе B_0 , реализующую f , такую, что*

$$L(\Sigma_f) \lesssim \frac{2^n}{n}.$$

Доказательство. Зададим функцию f в виде прямоугольной таблицы размера $2^k \times 2^{n-k}$ (см. табл. 3). Легко видеть, что столбец с номером $\sigma_{k+1}, \dots, \sigma_n$ задает функцию $f(x_1, \dots, x_k, \sigma_{k+1}, \dots, \sigma_n)$ и $f(x_1, \dots, x_n) = \bigvee x_{k+1}^{\sigma_{k+1}} \& \dots \& x_n^{\sigma_n} f(x_1, \dots, x_k, \sigma_{k+1}, \dots, \sigma_n)$. Далее, разрезая эту таблицу на полосы шириной s и действуя также, как и в случае контактных схем, мы получаем разбиение столбцов каждой полосы i на $t(i)$ сортов.

Т а б л и ц а 5

$\sigma_1(1), \dots, \sigma_k(1)$		γ_1	
.....			
.....			
$\sigma_1(s), \dots, \sigma_k(s)$		γ_s	

j

Пусть $((\sigma_1(1), \dots, \sigma_k(1)), \dots, (\sigma_1(s), \dots, \sigma_k(s)))$ — строки i -й полосы и $(\gamma_1, \dots, \gamma_s)$ — столбец сорта j (см. табл. 5). Обозначим через $f_{i,j}(x_1, \dots, x_k)$ булеву функцию, определяемую следующим способом:

$$f_{i,j}(x_1, \dots, x_k) = \begin{cases} \gamma_l, & \text{если } (x_1, \dots, x_k) = (\sigma_1(l), \dots, \sigma_k(l)), l = 1, \dots, s, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Столбец с номером $\sigma_{k+1}, \dots, \sigma_n$ разрезается полосами на $p = \lceil \frac{2^k}{s} \rceil$ коротких столбцов. Поэтому

$$f(x_1, \dots, x_k, \sigma_{k+1}, \dots, \sigma_n) = f_{i,j_1}(x_1, \dots, x_k) \vee \dots \vee f_{i,j_p}(x_1, \dots, x_k), \quad (*)$$

где j_ν — номер сорта соответствующего короткого столбца, принадлежащего ν -й полосе.

Теперь перейдем к описанию схемы Σ_f . Ее мы получим в виде соединения отдельных блоков (рис. 24). Попутно будем оценивать сложность блоков.

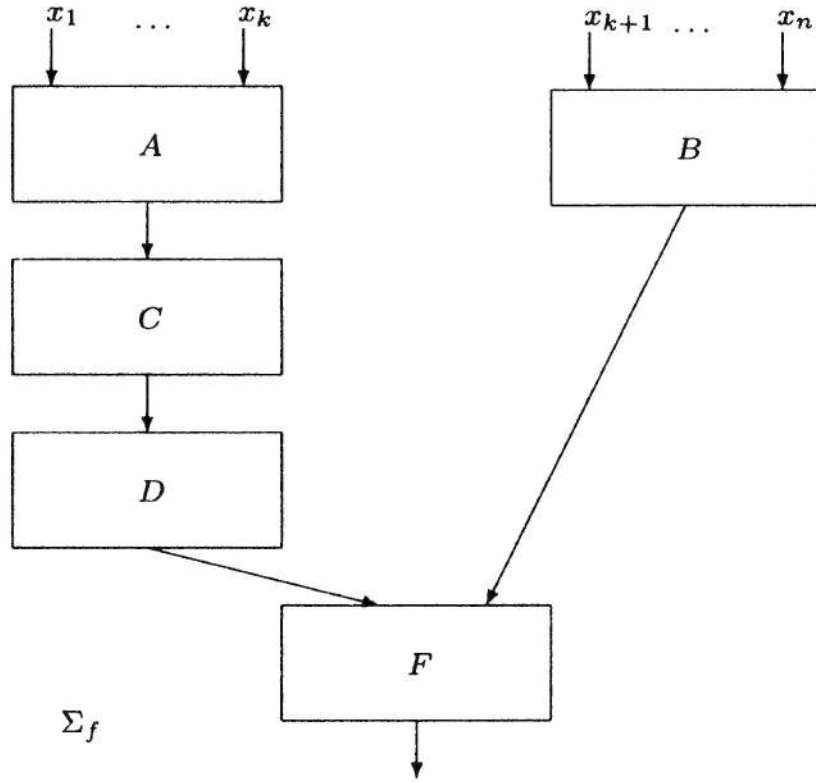


Рис. 24

1. Блок A реализует тривиальным образом все конъюнкции вида $x_1^{\sigma_1} \& \dots \& x_k^{\sigma_k}$,

$$L(A) \leq k2^k.$$

2. Блок B реализует все конъюнкции $x_{k+1}^{\sigma_{k+1}} \& \dots \& x_n^{\sigma_n}$,

$$L(B) \leq (n - k)2^{n-k}.$$

3. Блок C реализует по совершенной д.н.ф. функции $f_{i,j}(x_1, \dots, x_k)$,

$$L(C) \leq (s - 1)(t(1) + \dots + t(p)) \leq sp2^s.$$

4. Блок D реализует функции $f(x_1, \dots, x_k, \sigma_{k+1}, \dots, \sigma_n)$ на основе формулы (*),

$$L(D) \leq (p - 1)2^{n-k} < p2^{n-k}.$$

5. Блок F реализует функцию $f(x_1, \dots, x_n)$, исходя из разложения $f(x_1, \dots, x_n)$,

$$L(F) \leq 2^{n-k} + 2^{n-k} - 1 < 2 \cdot 2^{n-k}.$$

Суммируя полученные оценки, имеем

$$L(\Sigma_f) \leq k2^k + (n-k)2^{n-k} + sp2^s + p2^{n-k} + 2 \cdot 2^{n-k}.$$

Положим $k = \lceil 3 \log n \rceil$, $s = \lceil n - 5 \log n \rceil$. Тогда

$$p = \left\lceil \frac{2^k}{s} \right\rceil \sim \frac{2^k}{s} \quad \text{и} \quad L(\Sigma_f) \lesssim k2^k + n2^{n-k} + 2^{k+s} + \frac{2^n}{s},$$

причем

$$k2^k = o\left(\frac{2^n}{n}\right), \quad n2^{n-k} = o\left(\frac{2^n}{n}\right), \quad 2^{k+s} = o\left(\frac{2^n}{n}\right), \quad \frac{2^n}{s} \sim \frac{2^n}{n}.$$

Поэтому

$$L(\Sigma_f) \lesssim \frac{2^n}{n}.$$

Учитывая (см. §5) нижнюю оценку для $L(n)$, получаем

Т е о р е м а 8. $L(n) \sim \frac{2^n}{n}$.

Таким образом, алгоритм A_4 является асимптотически наилучшим.

В заключение этого параграфа обсудим вопрос о синтезе схем из Ф.Э.

в произвольном полном конечном базисе $B = \left\{ \begin{array}{c} \downarrow n_i \downarrow \\ \nabla \\ F_i \\ \downarrow \end{array} \right\} \quad (i = 1, \dots, r)$ с

$$L_B(\Sigma) = \sum_{i=1}^h l_i h_i,$$

где $l_i = L_B(F_i) > 0$ и h_i — число вхождений элементов F_i в схему Σ .

Пусть далее

$$\rho = \min_{n_i > 1} \frac{l_i}{n_i - 1}.$$

Тогда имеет место следующая

Т е о р е м а 9 (О. Б. Лупанов [12]). *Для любого класса схем из Ф.Э. над конечным базисом B и $l_i > 0$ ($i = 1, \dots, r$) существует асимптотически наилучший метод синтеза A , который для каждой булевой функции строит схему Σ_f такую, что*

$$L_A(\Sigma_f) \lesssim \rho \frac{2^n}{n} \quad \text{и} \quad L_A(n) \sim \rho \frac{2^n}{n}.$$

Доказательство теоремы распадается на две части.

Одна — построение метода синтеза, что выходит за рамки данного курса, и другая — получение нижних оценок сложности для $L_A(n)$, которое излагается в следующем параграфе.

§ 5. Нижние мощностные оценки

В этом параграфе сначала мы будем рассматривать верхние оценки для различных вариантов схем из Ф.Э. При этом в подсчете приходится учитывать более общие объекты, которые мы называем соединениями.

В самом деле, пусть Σ — схема из Ф.Э. в базисе $B = \left\{ \begin{array}{c} \downarrow \dots \downarrow \\ n_i \\ \nabla F_i \\ \downarrow \end{array} \right\}$ ($i = 1, \dots, r$). Ее можно рассматривать как соединение трех типов объектов: входов, выходов и элементов, изображение которых дано на рис. 25.



Рис. 25



Рис. 26

В этом соединении свободные концы стрелок идентифицируются с входами $x_{i_1}, \dots, x_{i_m}$ или с выходами $z_1, \dots, z_p$ элементов. Тривиальную схему, у которой вход совпадает с выходом, будем изображать так, как указано на рис. 26.

Теперь перейдем к анализу произвольной схемы Σ . Обозначим через Γ_Σ ориентированный граф, соответствующий схеме Σ . В Γ_Σ входы помечены символами $x_{i_1}, \dots, x_{i_m}$, выходы — $z_1, \dots, z_p$, и внутренние вершины — F_i . На рис. 27 изображена схема Σ над базисом B_0 и соответствующий граф.

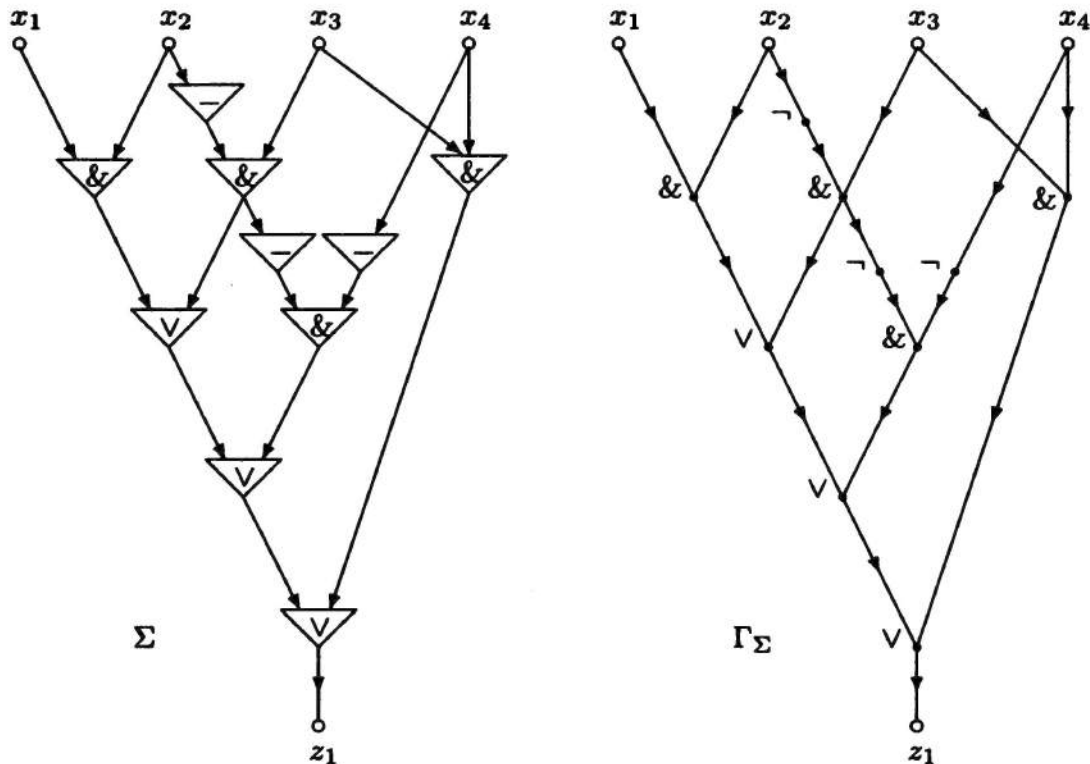


Рис. 27

Возьмем в каждом входе и каждом выходе элемента ровно по одной исходящей стрелке. Получим систему $\mathcal{D}_\Sigma = \{\mathcal{D}_1, \dots, \mathcal{D}_p\}$ ориентированных деревьев с корнями $z_1, \dots, z_p$. При этом некоторые из деревьев (их q штук, $q \leq p - 1$) могут быть вырожденными, т. е. состоять из одного корня. На рис. 28 показана система $\mathcal{D}_\Sigma$, состоящая из одного дерева $\mathcal{D}$, для графа Γ_Σ из предыдущего примера. Очевидно, что система $\mathcal{D}_\Sigma$ содержит все вершины графа Γ_Σ , т. е. $h_0 + m + p$ вершин (где h_0 — число функциональных элементов в Σ) и $h_0 + m$ ребер.

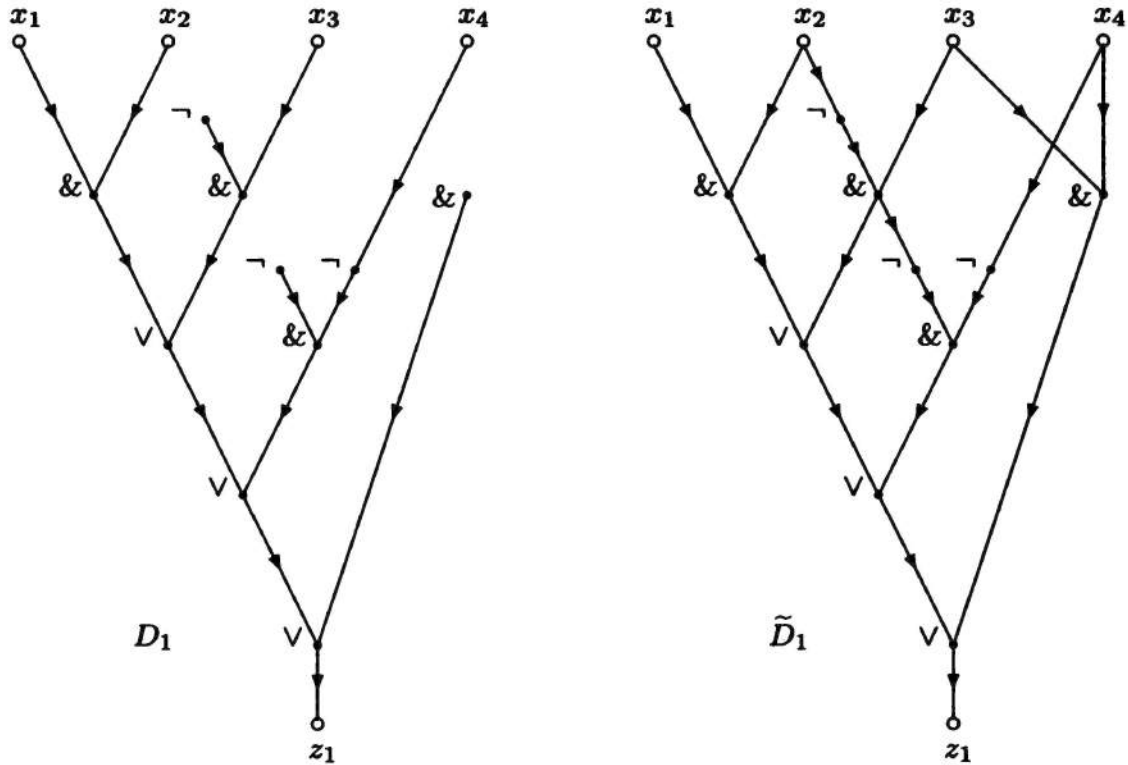


Рис. 28

Функциональные символы F_i , которые приписаны вершинам деревьев $\mathcal{D}_1, \dots, \mathcal{D}_p$, и изолированные корневые вершины из $\mathcal{D}_1, \dots, \mathcal{D}_p$ позволяют «восстановить» однозначным образом ребра из Γ_Σ , не попавшие в деревья. В результате этого мы получим систему «расширенных» деревьев $\tilde{\mathcal{D}}_\Sigma = \{\tilde{\mathcal{D}}_1, \dots, \tilde{\mathcal{D}}_p\}$. В них, очевидно, появятся новые вершины и ребра.

Общее число ребер в этой системе равно $\sum_{i=1}^r n_i h_i + p$, т. е. числу ребер в Γ_Σ . С другой стороны, каждый «элемент» прикреплен в $\tilde{\mathcal{D}}_\Sigma$ либо к другому «элементу», либо к выходу, поэтому суммарное число концевых вершин в этой же системе равно $\sum_{i=1}^r n_i h_i + p - h_0 = \sum_{i=1}^r (n_i - 1) h_i + p$, так как $h_0 = \sum_{i=1}^r h_i$. Таким образом, число Δ восстанавливаемых ребер равно

$$\Delta = \left(\sum_{i=1}^r n_i h_i + p \right) - (h_0 + m) = \sum_{i=1}^r (n_i - 1) h_i + p - m.$$

На рис. 28 представлено дерево $\tilde{\mathcal{D}}_1$, содержащее дополнительно $\Delta = 4$

ребер. Для того чтобы от системы $(\tilde{\mathcal{D}}_1, \dots, \tilde{\mathcal{D}}_p)$ перейти к Γ_Σ необходимо концевые вершины, непомеченные символами $x_{i_1}, \dots, x_{i_m}$ отождествить либо с внутренними вершинами, либо со входами $x_{i_1}, \dots, x_{i_m}$, т. е. для каждой такой вершины имеем $\leq h_0 + m$ возможностей.

Ниже в табл. 6 приведены значения основных параметров для Γ_Σ , $\{\mathcal{D}_1, \dots, \mathcal{D}_p\}$ и $\{\tilde{\mathcal{D}}_1, \dots, \tilde{\mathcal{D}}_p\}$.

Т а б л и ц а 6

	Γ_Σ	$\{\mathcal{D}_1, \dots, \mathcal{D}_p\}$	$\{\tilde{\mathcal{D}}_1, \dots, \tilde{\mathcal{D}}_p\}$
Число вершин	$h_0 + m + p$	$h_0 + m + p$	
Число концевых вершин			$\sum_{i=1}^r (n_i - 1)h_i + p$
Число ребер	$\sum_{i=1}^r n_i h_i + p$	$h_0 + m$	$\sum_{i=1}^r n_i h_i + p$

Теперь перейдем к рассмотрению конкретных классов схем из Ф.Э.

I. Класс $\mathfrak{S}(n, h)$ всех схем из Ф.Э. над базисом

$$B_0 = \left\{ \begin{array}{c} \downarrow \\ \nabla \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \downarrow \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \downarrow \\ \downarrow \end{array} \right\}$$

со входами, помеченными символами из алфавита $X_n = \{x_1, \dots, x_n\}$, имеющими один выход z , и содержащими не более h элементов. Пусть $S(n, h) = |\mathfrak{S}(n, h)|$ — число схем в $\mathfrak{S}(n, h)$.

Возьмем произвольную схему Σ из $\mathfrak{S}(n, h)$. Пусть $x_{i_1}, \dots, x_{i_m} \subseteq X_n$ ($m \leq n$) — символы переменных, приписанные входам Σ . Обозначим через h_1 — число инверторов, а через h_2 — число конъюнкторов и дизъюнкторов в Σ . В таком случае $h_0 = h_1 + h_2$ и $h_0 \leq h$. Производя анализ схемы Σ , мы получим Γ_Σ , $\mathcal{D}_\Sigma$ и $\tilde{\mathcal{D}}_\Sigma$ (см. рис. 27, 28). Системы деревьев $\mathcal{D}_\Sigma$ и $\tilde{\mathcal{D}}_\Sigma$ здесь состоят из одного дерева. Их параметры легко находятся при помощи табл. 6, в частности,

$$\Delta = h_2 - m + 1 \quad (\text{число недостающих ребер}).$$

На основе анализа докажем следующую лемму.

Л е м м а 5. При $h_0 \geq c_0 n$ существует константа c , не зависящая от n и h , такая, что

$$S(n, h) < (ch)^h.$$

Д о к а з а т е л ь с т в о. Опишем процесс построения произвольной схемы $\Sigma \in \mathfrak{S}(n, h)$. Этот процесс дает все указанные схемы и некоторые соединения, не являющиеся схемами. Таким образом, число $S(n, h)$ оценивается сверху числом получаемых соединений.

Итак, схема Σ из $\mathfrak{S}(n, h)$ определяется

1. Указанием числа h_0 ($h_0 \leq h$) и выбором разбиения $h_0 = h_1 + h_2$; имеем $\leq (h+1)^2$ способов.
2. Выбором переменных $x_{i_1}, \dots, x_{i_m} \in X_n$; $\leq 2^n$ способов.
3. Фиксацией дерева с $h_0 + m$ ребрами; $\leq 4^{h_0+m} \leq 4^{h+m}$ способов.
4. Приписыванием некоторым входам⁵ дерева символов $x_{i_1}, \dots, x_{i_m}$; $\leq (h_0 + m)^m \leq (h + m)^m$ способов.
5. Приписыванием оставшимся (кроме выходной) вершинам символов $\neg$ (h_1 штук) и $\&$, $\vee$ (h_2 штук); $\leq C_{h_0}^{h_1} 2^{h_2} \leq 3^{h_0} \leq 3^h$ способов.
6. Восстановлением «недостающих» ребер и их присоединением к вершинам, не являющимся выходом; $\leq (h_0 + m)^{h_2-m+1} \leq (h + m)^{h_2-m+1}$ способов.

Объединяя эти оценки, получим

$$S(n, h) \leq (h+1)^2 8^n 12^h (h+m)^{h_2+1} \leq (ch)^h, \text{ так как } m \leq n \leq \frac{h}{c_0}.$$

Лемма доказана.

II. Класс $\mathfrak{S}_B(n, L)$ всех схем Σ из Ф.Э. над базисом $B = \left\{ \begin{array}{c} \downarrow n_i \downarrow \\ \triangle F_i \\ \downarrow \end{array} \right\}$

($i = 1, \dots, r$) со входами, помеченными символами из алфавита X_n , имеющих один выход z_1 и сложность $L_B(\Sigma) = \sum_{i=1}^r \lambda_i h_i \leq L$, где $\lambda_i = L_B(F_i)$, а h_i — число элементов F_i в Σ ($i = 1, \dots, r$). Пусть $S(n, L) = |\mathfrak{S}_B(n, L)|$ — число схем в $\mathfrak{S}_B(n, L)$.

Анализ схемы $\Sigma \in \mathfrak{S}_B(n, L)$ со входами $x_{i_1}, \dots, x_{i_m}$ ($m \leq n$) осуществляется так же, как и в предыдущем случае. Здесь, поскольку $n_i - 1 \leq \frac{\lambda_i}{\rho}$,

$$\Delta = \sum_{i=1}^r (n_i - 1) h_i - m + 1 \leq \frac{L}{\rho} - m + 1.$$

Л е м м а 6. При $L \geq c_0 h$ существует константа c , не зависящая от h и L такая, что

$$S(n, L) \leq (cL)^{\frac{L}{\rho}}.$$

Д о к а з а т е л ь с т в о. Схема $\Sigma \in \mathfrak{S}_B(n, L)$ определяется

1. Указанием набора $(h_1, \dots, h_r)$, удовлетворяющего неравенству

$$\lambda_1 h_1 + \dots + \lambda_r h_r \leq L.$$

Пусть

$$\lambda_{\min} = \min_{1 \leq i \leq r} \lambda_i, \quad h_0 = \sum_{i=1}^r h_i.$$

Тогда $h < \frac{L}{\lambda_{\min}}$ и число выборов $\leq \left\lceil \frac{L}{\lambda_1} \right\rceil \dots \left\lceil \frac{L}{\lambda_r} \right\rceil \leq \left(\frac{L}{\lambda_{\min}} \right)^r$.

⁵Если у дерева входов меньше, чем m , то берутся произвольные вершины.

2. Выбором переменных $\{x_{i_1}, \dots, x_{i_m}\} \subseteq X_n$; имеем 2^n способов.
 3. Фиксацией дерева с $h_0 + m$ ребрами; $\leq 4^{h_0+m}$ способов.
 4. Приписыванием некоторым входам дерева символов $x_{i_1}, \dots, x_{i_m}$; имеем $\leq (h_0 + m)^m$ способов.
 5. Приписыванием оставшимся (кроме выходной) вершинам символов F_i ($i = 1, \dots, r$); имеем $\leq r^{h_0}$ способов.
 6. Восстановлением «недостающих» ребер и их присоединением к вершинам, не являющихся выходом; $\leq (h_0 + m)^{\frac{L}{\rho} - m + 1}$ способов.
- Объединяя оценки, получаем

$$S(n, L) \leq \left(\frac{L}{\lambda_{\min}} \right)^r 8^n (4r)^{h_0} (h_0 + m)^{\frac{L}{\rho} + 1}.$$

Учитывая $\frac{L}{c_0} \geq n \geq m$ и $h_0 + m \leq L(\frac{1}{\lambda_{\min}} + \frac{1}{c_0})$, имеем

$$S(n, L) < (cL)^{\frac{L}{\rho}}.$$

Лемма доказана.

III. Класс $\mathfrak{S}_B(n, p, L)$ всех схем Σ из Ф.Э. над базисом $B = \left\{ \begin{array}{c} \downarrow n_i \downarrow \\ F_i \\ \downarrow \end{array} \right\}$

($i = 1, \dots, r$) со входами, помеченными символами из алфавита X_n , с p выходами, помеченными символами $z_1, \dots, z_p$ и имеющими сложность $L_B(\Sigma) \leq L$. Пусть $S(n, p, L)$ — число схем в $\mathfrak{S}_B(n, p, L)$.

Анализ схемы $\Sigma \in \mathfrak{S}_B(n, p, L)$ со входами $x_{i_1}, \dots, x_{i_m}$ ($m \leq n$) осуществляется так же, как и в предыдущих случаях. Здесь появляется система $\mathcal{D}_\Sigma$ деревьев $\mathcal{D}_1, \dots, \mathcal{D}_p$ и расширенных деревьев $\tilde{\mathcal{D}}_1, \dots, \tilde{\mathcal{D}}_p$. Параметры их указаны в табл. 6, $\Delta \leq \frac{L}{\rho} - m + 1$ (см. случай II), а число систем из p деревьев, содержащих данное число ребер $h_0 + m$, сводится к оценке числа деревьев из $h_0 + m + p$ ребер (нужно к корням деревьев $\mathcal{D}_1, \dots, \mathcal{D}_p$ добавить по одному ребру и концы их склеить; рис. 29).

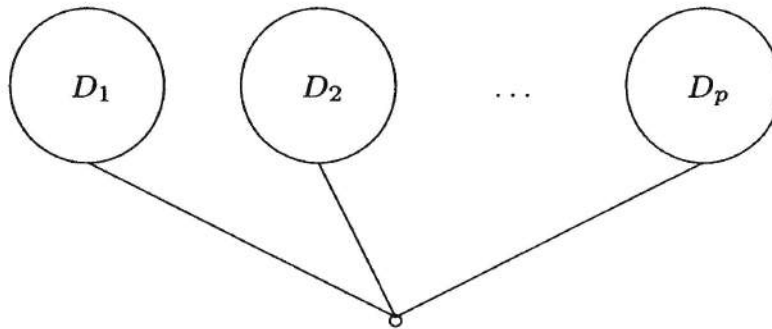


Рис. 29

Л е м м а 7. При $L \geq c_0 n$ существует константа c , не зависящая от n, p, L , такая, что

$$S(n, p, L) < (cL)^{\frac{L}{\rho} + p}.$$

Доказательство. Почти полностью совпадает со случаем II. Схема $\Sigma \in \mathfrak{S}_B(n, p, L)$ определяется

1. Указанием набора $(h_1, \dots, h_r)$, который удовлетворяет неравенству $\lambda_1 h_1 + \dots + \lambda_r h_r \leq L$; имеем $\leq \left\lfloor \frac{L}{\lambda_1} \right\rfloor \dots \left\lfloor \frac{L}{\lambda_r} \right\rfloor \leq \left(\frac{L}{\lambda_{\min}} \right)^r$ вариантов.

2. Выбором переменных $\{x_{i_1}, \dots, x_{i_m}\} \subseteq X_n$; имеем 2^n способов.

3. Фиксацией системы деревьев $\mathcal{D}_1, \dots, \mathcal{D}_p$; имеем $\leq 4^{h_0+m+p}$ вариантов.

4. Приписыванием некоторым входам деревьев символов $x_{i_1}, \dots, x_{i_m}$; имеем $\leq (h_0 + m)^m$ способов.

5. Приписыванием оставшимся (кроме выходных) вершинам символов F_i ($i = 1, \dots, r$); $\leq r^h$ способов.

6. Восстановлением «недостающих» ребер и их присоединением к вершинам, не являющимся выходными; $\leq (h_0 + m)^{\frac{L}{\rho} - m + p}$ способов.

Объединяя оценки, получим при $L \geq c_0 n$

$$S(n, p, L) \leq \left(\frac{L}{\lambda_{\min}} \right)^r 8^n (4r)^h 4^p (h_0 + m)^{\frac{L}{\rho} - m + p} < (cL)^{\frac{L}{\rho} + p}.$$

Лемма доказана.

Сформулируем следствие, которое будет использовано в дальнейшем.

Следствие. При $p = o(L)$ и $L \geq c_0 n$ для любого $\varepsilon > 0$ существует N такое, что при $n > N$

$$S(n, p, L) < (cL)^{\frac{L}{\rho}(1+\varepsilon)}.$$

В леммах 5–7 фигурируют классы $\mathfrak{S}(n, h)$, $\mathfrak{S}_B(n, L)$, $\mathfrak{S}_B(n, p, L)$. При чем класс $\mathfrak{S}_B(n, p, L)$ является самым широким, а оценка для $S(n, p, L)$ содержит, как частный случай, оценки для $S(n, h)$ и $S(n, L)$.

IV. Класс $\mathfrak{S}_B^k(n, p, L)$ всех схем Σ из Ф.Э. над k -значным базисом

$B = \left\{ \begin{array}{c} \downarrow n_i \downarrow \\ \nabla F_i \\ \downarrow \end{array} \right\} \quad (i = 1, \dots, r)$ со входами, помеченными символами из алфавита $X_n = \{x_1, \dots, x_n\}$, с p выходами, помеченными символами $z_1, \dots, z_p$, и имеющих сложность $L_B(\Sigma) \leq L$, где $L_B(\Sigma)$ определяется так же, как и в пункте II.

Схема Σ называется неприводимой, если существует такой выбор деревьев $\mathcal{D}_1, \dots, \mathcal{D}_p$, что все несущественные входы соответствующих расширенных деревьев $\tilde{\mathcal{D}}_1, \dots, \tilde{\mathcal{D}}_p$ (т. е. полученных из $\mathcal{D}_1, \dots, \mathcal{D}_p$ добавлением недостающих ребер), которые принадлежат множеству недостающих ребер, подключены в Σ ко входу x_{i_1} , имеющему наименьший номер i_1 .

Замечание. Очевидно, что всякую схему Σ можно преобразовать в неприводимую схему, имеющую то же функционирование и ту же сложность.

Полезно иметь в виду, что каждой схеме Σ с одним выходом соответствует дерево $\tilde{\mathcal{D}}_\Sigma$ (в силу нашего анализа) и $L_B(\Sigma) = L_B(\tilde{\mathcal{D}}_\Sigma)$, а число существенных входов m и $\tilde{m}$ соответственно для Σ и $\tilde{\mathcal{D}}_\Sigma$ удовлетворяют неравенству $m \leq \tilde{m}$, поэтому

$$\frac{L_B(\Sigma)}{m} \geq \frac{L_B(\tilde{\mathcal{D}}_\Sigma)}{\tilde{m}}.$$

Следовательно, для вычисления ρ^* можно ограничиться множеством всех деревьев над B .

Теперь мы можем оценить величину $\tilde{\Delta}$ — число тех входов деревьев $\tilde{\mathcal{D}}_1, \dots, \tilde{\mathcal{D}}_p$, т. е. концевых ребер, которые необходимо присоединить к вершинам. Очевидно

$$\tilde{\Delta} \leq \sum_{i=1}^p \tilde{m}_i,$$

где $\tilde{m}_i$ — число существенных входов дерева $\tilde{\mathcal{D}}_i$. Отсюда

$$\begin{aligned} \tilde{\Delta} &\leq \sum_{\substack{i \\ \tilde{m}_i > N_1}} \tilde{m}_i + \sum_{\substack{i \\ \tilde{m}_i \leq N_1}} \tilde{m}_i \leq \sum_{\substack{i \\ \tilde{m}_i > N_1}} \frac{L_B(\tilde{\mathcal{D}}_i)}{\rho^*} (1 + \varepsilon/3) + pN_1 \leq \\ &\leq \frac{(1+\varepsilon/3)}{\rho^*} \sum_{i=1}^p L_B(\tilde{\mathcal{D}}_i) + pN_1 \leq \frac{(1+\varepsilon/3)}{\rho^*} L_B(\Sigma) + pN_1 \leq \frac{L}{\rho^*} (1+\varepsilon/3) + pN_1. \end{aligned}$$

Л е м м а 8. При $L \geq c_0 n$ существует константа c , не зависящая от n , p и L , при которой для любого $\varepsilon > 0$ найдется $N_1(\varepsilon)$ такое, что при $n > N_1$

$$S^k(n, p, L) \leq (cL)^{\frac{L}{\rho^*} (1+\varepsilon/3) + N_1 p + n}.$$

Д о к а з а т е л ь с т в о. Является дальнейшим развитием доказательства для случая III. Схема $\Sigma \in \tilde{\mathfrak{S}}_B^k(n, p, L)$ определяется:

1. Указанием набора $(h_1, \dots, h_r)$, который удовлетворяет неравенству $\lambda_1 h_1 + \dots + \lambda_r h_r \leq L$; имеем $\leq \left\lfloor \frac{L}{\lambda_1} \right\rfloor \dots \left\lfloor \frac{L}{\lambda_r} \right\rfloor \leq \left(\frac{L}{\lambda_{\min}} \right)^r$ способов.

2. Выбором переменных $\{x_{i_1}, \dots, x_{i_m}\} \subseteq X_n$; 2^n способов.

3. Фиксацией системы деревьев $\mathcal{D}_1, \dots, \mathcal{D}_p$; имеем $\leq 4^{h_0 + m + p}$ способов.

4. Приписыванием некоторым входам деревьев символов $x_{i_1}, \dots, x_{i_m}$; имеем $\leq (h_0 + m)^m$ способов.

5. Приписыванием оставшимся (кроме выходных) вершинам символов F_i ($i = 1, \dots, r$); $\leq r^h$ способов.

6. Восстановлением «недостающих» ребер, присоединением несущественных входов к x_{i_1} и остальных $\tilde{\Delta}$ входов к вершинам, отличным от выходных; $\leq (h_0 + m)^{\tilde{\Delta}}$ способов.

Объединяя оценки, получим

$$S^k(n, p, L) \leq \left(\frac{L}{\lambda_{\min}} \right)^r 8^n (4r)^h 4^p (h+n)^{\tilde{\Delta}+n}.$$

Если взять $n > N_1$ и учесть неравенства

$$n \leq \frac{L}{c_0}, \quad h \leq \frac{L}{\lambda_{\min}}, \quad \text{и} \quad \tilde{\Delta} \leq \frac{L}{\rho^*} (1 + \varepsilon/3) + N_1 p,$$

то получим

$$S^k(n, p, L) \leq (cL)^{(1+\varepsilon/3)\frac{L}{\rho^*} + N_1 p + n}.$$

С л е д с т в и е. Пусть $n = o(L)$ и $p = o(L)$. Тогда найдется L_0 такое, что при $L \geq L_0$

$$\frac{n}{L} < \frac{\varepsilon}{3} \frac{1}{\rho^*} \quad \text{и} \quad \frac{p}{L} < \frac{\varepsilon}{3} \frac{1}{N_1 \rho^*}.$$

Поскольку $L \geq c_0 n$, то последние неравенства имеют место при $n \geq N_2$, где $c_0 N_2 \geq L_0$.

Пусть $N = \max(N_1, N_2)$, тогда при $n > N$

$$S^k(n, p, L) \leq (cL)^{\frac{L}{\rho^*}(1+\varepsilon)}.$$

Теперь мы перейдем к формулировке и доказательству теоремы о нижней оценке функции Шеннона справедливой не только для различных классов схем из Ф.Э., но и имеющей место для очень широкого семейства классов У.С., включая классы контактных схем, классы автоматов и т. д.

Пусть $\mathfrak{S}(n, p)$ — класс многополюсников с n входами и p выходами, а $\mathfrak{F}(n, p)$ — множество отображений, реализуемое ими.

Рассмотрим подмножество $\tilde{\mathfrak{F}}(n, p) \subseteq \mathfrak{F}(n, p)$ и пусть

$$P(n, p) = |\tilde{\mathfrak{F}}(n, p)| < +\infty.$$

Обозначим через $L(n, p)$ функцию Шеннона для реализации отображений из класса $\tilde{\mathfrak{F}}(n, p)$, а через $S(n, p, L)$ число схем из $\mathfrak{S}(n, p)$ с не более, чем n входами, p выходами и имеющими сложность не более, чем L .

Т е о р е м а 10. Если для любого $\varepsilon > 0$ существует N такое, что при $n > N$ и $L \geq c_0 n$ (где $c_0 > 0$) выполнены условия

- (1) $S(n, p, L) \leq (\varphi(n, p)L)^{\frac{L}{\omega}(1+\varepsilon)} \quad (\varphi(n, p) > 0, \omega > 0),$
- (2) $(1 - \varepsilon)\omega \frac{\log P(n, p)}{\log \log P(n, p)} > c_0 n,$
- (3) $\log \varphi(n, p) = o(\log \log P(n, p)),$

то

$$L(n, p) \gtrsim \omega \frac{\log P(n, p)}{\log \log P(n, p)}.$$

Доказательство. Берем $\varepsilon > 0$ и полагаем

$$L = \left[(1 - \varepsilon) \omega \frac{\log P(n, p)}{\log \log P(n, p)} \right].$$

Очевидно, в силу (2) при $n > N$ получим $L \geq c_0(n)$. На основании (1) при этих условиях

$$S(n, p, L) \leq (\varphi(n, p) L)^{\frac{L}{\omega(1+\varepsilon)}}.$$

Оценим величину $\log \frac{S(n, p, L)}{P(n, p)}$ при данном L . Имеем

$$\begin{aligned} \log \frac{S(n, p, L)}{P(n, p)} &\leq (1 - \varepsilon^2) \frac{\log P(n, p)}{\log \log P(n, p)} \left\{ \log \frac{(1 - \varepsilon) \varphi(n, p) \omega}{\log \log P(n, p)} + \log \log P(n, p) \right\} - \\ &- \log P(n, p) = -\varepsilon^2 \log P(n, p) + (1 - \varepsilon^2) \frac{\log P(n, p)}{\log \log P(n, p)} \log \frac{(1 - \varepsilon) \omega}{\log \log P(n, p)} + \\ &+ (1 - \varepsilon^2) \frac{\log P(n, p)}{\log \log P(n, p)} \log \varphi(n, p). \end{aligned}$$

Главным здесь является член $-\varepsilon^2 \log P(n, p)$, поэтому

$$\log \frac{S(n, p, L)}{P(n, p)} \rightarrow -\infty \quad (n \rightarrow \infty).$$

Тогда найдется $N_1 \geq N$ такое, что при $n \geq N_1$

$$\log \frac{S(n, p, L)}{P(n, p)} < 0, \quad \text{т. е.} \quad S(n, p, L) \leq P(n, p)$$

и число схем сложности L будет меньше, чем число отображений. В таком случае найдется отображение, которое будет при любой реализации иметь сложность большую, чем L и тогда

$$L(n, p) \geq (1 - \varepsilon) \omega \frac{\log P(n, p)}{\log \log P(n, p)} \quad \text{или} \quad L(n, p) \gtrsim \omega \frac{\log P(n, p)}{\log \log P(n, p)}.$$

Теорема доказана.

З а м е ч а н и е. Условие (2) дает ограничения на величину $P(n, p)$, которая не может расти слишком медленно. Ограничение $p = o(L)$ выполняется при $p = o\left(\frac{\log P(n, p)}{\log \log P(n, p)}\right)$.

С л е д с т в и е. Нижняя оценка верна для $n \cdot p$ отображений из $\tilde{\mathfrak{F}}(n, p)$, поскольку в доказательстве теоремы оценивается доля тех отображений, которые реализуются схемами со сложностью не превосходящей $L = \left[(1 - \varepsilon) \omega \frac{\log P(n, p)}{\log \log P(n, p)} \right]$, и устанавливается, что она стремится к 0.

Рассмотрим применение теоремы о нижней оценке для различных случаев.

I. Класс схем из Ф.Э. в базисе $B_0 = \left\{ \begin{array}{c} \downarrow \\ \triangle \\ \downarrow \end{array} \begin{array}{c} - \\ & \\ & \end{array}, \begin{array}{c} \downarrow \downarrow \\ \triangle \\ \downarrow \end{array} \begin{array}{c} \& \\ & \\ & \end{array}, \begin{array}{c} \downarrow \downarrow \\ \triangle \\ \downarrow \end{array} \begin{array}{c} \vee \\ & \\ & \end{array} \right\}$ с n входами и одним выходом ($p = 1$); $L(\Sigma) = h$ — число элементов, $\omega = \rho = 1$, $\varphi(n, p) \equiv c$.

Здесь, согласно лемме 5, имеем $S(n, h) < (ch)^h$, $\mathfrak{F} = P_2$ и $\log P(n) = 2^n$. Все условия теоремы 10 выполнены. Поэтому

$$L(n) \gtrsim \frac{2^n}{n}.$$

II. Класс схем из Ф.Э. в произвольном базисе $B = \left\{ \begin{array}{c} \downarrow \dots \downarrow \\ \triangle \\ \downarrow \end{array} \begin{array}{c} n_i \\ F_i \\ n_i \end{array} \right\}$ ($i = 1, \dots, r$) с n входами и одним выходом ($p = 1$); $L_B(\Sigma) = \sum_{i=1}^r \lambda_i h_i$, $\omega = \rho = \min_{n_i \geq 2} \frac{\lambda_i}{n_i - 1}$, $\varphi(n, p) \equiv c$.

Здесь, согласно лемме 6, имеем $S(n, L) \leq (cL)^{\frac{L}{\rho}}$, $\mathfrak{F} = P_2$ и $\log P(n) = 2^n$. Все условия теоремы 10 выполнены. Поэтому

$$L_B(n) \gtrsim \rho \frac{2^n}{n}.$$

III. Класс схем из Ф.Э. в произвольном базисе B с n входами и p выходами; $L_B(\Sigma) = \sum_{i=1}^r \lambda_i h_i$, $\omega = \rho$, $\varphi(n, p) \equiv c$.

Здесь (см. следствие из леммы 7) $S(n, p, L) \leq (cL)^{\frac{L}{\rho}} (1 + \varepsilon)$ при $p = o(L)$, а $\mathfrak{F} = P_2^p$ и $\log_2 P(n, p) = p 2^n$. Все условия теоремы 10 при этом выполнены. Поэтому

$$L_B(n, p) \gtrsim \frac{\rho p 2^n}{n + \log p}.$$

Ограничение $p = o(L)$ выполняется (см. замечание к теореме 10), если

$$\frac{p \log \log P(n, p)}{\log P(n, p)} = \frac{n + \log p}{2^n} \rightarrow 0,$$

что эквивалентно $\log p = o(2^n)$. При p — постоянном

$$L_B(n, p) \gtrsim \frac{\rho p 2^n}{n}.$$

IV. Класс двухполюсных контактных схем над элементами $\{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$; L — число контактов, $\omega = 1$, $\varphi(n, p) = 2nc$.

Здесь $S(n, 2, L) \leq (2ncL)^L$ (см. доказательство теоремы 2), $\mathfrak{F} = P_2$ и $\log P(n, p) = 2^n$. Все условия теоремы 10 выполнены. Поэтому

$$L(n) \gtrsim \frac{2^n}{n}.$$

V. Класс p -полюсных контактных схем над элементами $\{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$; L — число контактов, $\omega = 1$, $\varphi(n, p) = 2nc$.

Здесь $S(n, p, L) \leq (2ncL)^L$ (см. § 6 из предыдущей главы), $\mathfrak{F}$ — множество матриц порядка p , имеющих специальный вид, $\log P(n, p) = 2^n \log \Phi(p)$. Условия теоремы 10 выполнены. Поэтому

$$L(n, p) \gtrsim \frac{\log \Phi(p) 2^n}{n}.$$

VI. Класс схем из Ф.Э. в произвольном многозначном базисе B с n входами и p выходами; $L_B(\Sigma) = \sum_{i=1}^r \lambda_i h_i$, $\omega = \rho^*$, $\varphi(n, p) \equiv c$.

Здесь, согласно лемме 8, $S(n, p, L) \leq (cL)^{\frac{L}{\rho^*}} (1 + \varepsilon)$ при $p = o(L)$, $n = o(L)$; $\mathfrak{F} = P_k^p$ и $\log_k P(n, p) = pk^n$. Все условия теоремы 10 при этом выполнены. Поэтому

$$L_B^k(n, p) \gtrsim \frac{\rho^* pk^n}{n + \log_k p}.$$

Ограничение $n = o(L)$ выполнено автоматически, а ограничение $p = o(L)$ выполняется (см. замечание к теореме 10), если $\frac{n + \log_k p}{\rho^* k^n} \rightarrow 0$, что имеет место при $\log p = o(k^n)$. При постоянном p

$$L_B^k(n, p) \gtrsim \frac{\rho^* pk^n}{n}.$$

Другие приложения теоремы 10 будут рассмотрены ниже.

ГЛАВА 3. КЛАСС АВТОМАТНЫХ СХЕМ

Дадим расшифровку понятий для случая автоматных схем. Здесь

$\mathfrak{S}$ — множество автоматных схем в базисе $B = \left\{ \begin{array}{c} \downarrow \\ \neg \\ \downarrow \end{array}, \begin{array}{c} \downarrow \downarrow \\ \& \\ \downarrow \end{array}, \begin{array}{c} \downarrow \downarrow \\ \vee \\ \downarrow \end{array}, \begin{array}{c} \downarrow \\ 3 \\ \downarrow \end{array} \right\};$

Φ — системы канонических уравнений;

$\mathfrak{F}$ — множество систем ограниченно-детерминированных (о.-д.) функций;

$L_B(\Sigma) = \sum_{i=1}^r \lambda_i h_i$, где в основном $r = 4$, $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ — соответственно сложность элемента задержки, инвертора, конъюнктора и дизъюнктора, а h_1, h_2, h_3, h_4 — их число в Σ ;

$L_B(f)$ — минимальная сложность реализации о.-д. функции f в базисе B ;

$\mathfrak{F}_{n,p,r}$ — множество систем о.-д. функций, содержащих p о.-д. функций от переменных из $X_n = \{x_1, \dots, x_n\}$ и имеющих вес не более чем r (очевидно, $|\mathfrak{F}_{n,p,r}| < +\infty$);

$L_B(n, p, r)$ — функция Шеннона.

§ 1. Асимптотика для числа о.-д. функций

Рассмотрим множество о.-д. функций от одного переменного, переводящих последовательности значности N в последовательности значности M и имеющих вес r . Каждую такую функцию можно задать при помощи диа-

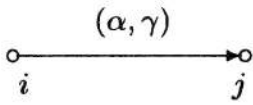


Рис. 30

граммы Мура, содержащей r вершин. В этой диаграмме все вершины занумерованы числами $0, 1, \dots, r-1$ так, что начальная вершина имеет номер 0. Из каждой вершины исходит N ребер, нумеруемых числами $0, 1, \dots, N-1$ и имеющих пометки из множества $\{0, 1, \dots, M-1\}$. На рис. 30 изображено ребро, идущее из вершины i в вершину j , пара (α, γ) указывает номер ребра — α и пометку — γ .

Определение. Вершины i и j называются различимыми, если можно указать слово $a = \alpha_1, \dots, \alpha_s$ в алфавите $\{0, 1, \dots, N-1\}$ такое, что слова $b_1 = \gamma_1^1, \dots, \gamma_s^1$ и $b_2 = \gamma_1^2, \dots, \gamma_s^2$, получаемые по a при движении из вершин соответственно i и j , различны. В противном случае вершины i и j называются неразличимыми.

Легко видеть, что в диаграмме Мура, содержащей r вершин и соответствующей о.-д. функции веса r , все вершины попарно различимы.

Определение. Вершины i и j называются сходными, если исходящим из этих вершин ребрам, имеющим одинаковые номера, приписаны равные значения, и они идут в одну и ту же вершину (для разных номеров ребер вершины могут быть разными).

Очевидно, что сходные вершины можно естественным образом склеить, и мы получим диаграмму Мура с меньшим числом состояний и реализующую ту же о.-д. функцию.

Замечание. Из этого рассуждения следует, что в диаграмме Мура с r вершинами, соответствующей о.-д. функции веса r , все вершины попарно не являются сходными.

Лемма 9. Если вершины i и j сходные, то они эквивалентны.

Доказательство очевидно.

Обозначим через $P(N, M, r)$ число о.-д. функций в алфавитах мощности N и M , имеющих вес r .

Теорема 11. При $N \rightarrow \infty$, постоянном r и любом M

$$P(N, M, r) \sim \frac{(Mr)^{Nr}}{(r-1)!}.$$

Доказательство.

А) Верхняя оценка. Очевидно, что число диаграмм Мура с данными параметрами N , M и r , у которых вершины занумерованы числами $0, 1, \dots, r-1$, причем вершина 0 — начальная, равно

$$(Mr)^{Nr}.$$

При этом каждая о.-д. функция веса r реализуется ровно $(r-1)!$ раз, поскольку, в силу замечания, все диаграммы Мура, получаемые из данной,

путем любого переименования вершин $1, \dots, r-1$ (а их $(r-1)!$), попарно различны. В силу этого

$$(r-1)! P(N, M, r) \leq (Mr)^{Nr} \quad (*)$$

или

$$P(N, M, r) \leq \frac{(Mr)^{Nr}}{(r-1)!}. \quad (**)$$

Б) Нижняя оценка. Неравенство (*) обусловлено тем, что правая часть учитывает диаграммы, в которых возможны:

- 1) недостижимые вершины из начальной вершины;
- 2) эквивалентные состояния.

Введем следующие обозначения:

$\xi(N, M, r)$ — число занумерованных диаграмм Мура, в каждой из которых найдется хотя бы одна вершина, недостижимая из начальной;

$\eta(N, M, r)$ — число занумерованных диаграмм Мура, в каждой из которых имеется по крайней мере два эквивалентных состояния.

Очевидно,

$$(r-1)!P(N, M, r) \geq (Mr)^{Nr} - \xi(N, M, r) - \eta(N, M, r).$$

Таким образом, для получения искомой нижней оценки достаточно оценить сверху величины ξ и η .

Оценка ξ . Пусть начальная вершина (помечена 0) попадает в компоненту мощности i , а остальные $r-i$ вершин — недостижимы.

Приведем подсчет таких диаграмм:

- а) имеем C_{r-1}^{i-1} выборов компоненты, содержащей начальную вершину и состоящей из i вершин;
- б) имеем не более $i^{Ni} M^{Ni}$ фрагментов связной компоненты мощности i ;
- в) имеем $r^{N(r-i)} M^{N(r-i)}$ остатков.

Итак,

$$\xi(N, M, r) \leq \sum_{i=1}^{r-1} C_{r-1}^{i-1} (Mr)^{Nr} \left(\frac{i}{r}\right)^{Ni} = (Mr)^{Nr} \sum_{i=1}^{r-1} C_{r-1}^{i-1} \left(\frac{i}{r}\right)^{Ni}.$$

Оценка η . Очевидно, что две эквивалентные вершины (состояния) характеризуются тем, что исходящим из этих вершин ребрам с одинаковыми номерами приписаны одинаковые значения. Таким образом, η не превосходит числа занумерованных диаграмм Мура, в каждой из которых встречается хотя бы одна пара различных вершин, исходящим ребрам которых, имеющим одинаковые номера, приписаны одинаковые значения (ср. с понятием сходных вершин). С учетом этого обстоятельства произведем оценку η . Итак, число диаграмм, имеющих хотя бы две

одинаковые полустары (совокупности исходящих ребер), подсчитывается так:

а) одна из указанных вершин отлична от начальной и может быть выбрана $r - 1$ способами;

б) тогда вторая вершина (она может совпадать и с начальной, но отлична от первой) выбирается $r - 1$ способами;

в) мы имеем r^{Nr} способов подключения ребер и $M^{N(r-1)}$ способов приписывания значений ребрам (нумерация ребер для второй вершины автоматически следует из нумерации первой).

Следовательно,

$$\eta(N, M, r) \leq (r - 1)^2 (Mr)^{Nr} \frac{1}{M^N}.$$

Объединяя оценки, получаем

$$(r - 1)! P(N, M, r) \geq (Mr)^{Nr} \left(1 - \sum_{i=1}^{r-1} C_{r-1}^{i-1} \left(\frac{i}{r} \right)^{Ni} - \frac{(r - 1)^2}{M^N} \right).$$

Так как

$$\sum_{i=1}^{r-1} C_{r-1}^{i-1} \left(\frac{i}{r} \right)^{Ni} \leq \sum_{i=1}^{r-1} C_{r-1}^{i-1} \left(\frac{r-1}{r} \right)^N \leq 2^{r-1} \left(\frac{r-1}{r} \right)^N$$

и r постоянно, то

$$(r - 1)! P(N, M, r) \geq (Mr)^{Nr} (1 - o(1)). \quad (***)$$

Из неравенств (**) и (***) следует результат теоремы.

Данная теорема может быть усилена.

Т е о р е м а 12. При $N \rightarrow \infty$, $\log r = o(N)$ и любом M

$$P(N, M, r) \sim \frac{(Mr)^{Nr}}{(r - 1)!}.$$

Д о к а з а т е л ь с т в о. Для $r = \text{const}$ теорема доказана, поэтому достаточно ее установить для случая $r \rightarrow \infty$, $\log r = o(N)$. Последнее требует более точной оценки суммы

$$\sum_{i=1}^{r-1} C_{r-1}^{i-1} \left(\frac{i}{r} \right)^{Ni} \leq \sum_{i=1}^{r-1} C_r^i \left(\frac{i}{r} \right)^{Ni} = \sum_{i=1}^{r-1} A_i,$$

где $A_i = C_r^i \left(\frac{i}{r} \right)^{Ni}$, $1 \leq i \leq r - 1$.

Компоненты A_i — функции C_r^i и $\left(\frac{i}{r} \right)^{Ni}$ являются унимодальными функциями по i . Функция C_r^i — выпукла кверху и имеет максимум в точке $\left[\frac{r+1}{2} \right]$ (и нечетном r еще при $\left[\frac{r+1}{2} \right] - 1$), а функция $\left(\frac{i}{r} \right)^{Ni}$ выпукла книзу

с минимумом, принадлежащем множеству $\left\{\left[\frac{r}{e}\right], \left[\frac{r}{e} + 1\right]\right\}$, так как соответствующая функция действительного переменного $\left(\frac{x}{r}\right)^{Nx}$ на $\left[1, \frac{r}{e}\right]$ имеет минимум при $x = \frac{r}{e}$ и на $\left[1, \frac{r}{e}\right]$ убывает, а на $\left[\frac{r}{e}, r-1\right]$ возрастает. Отрезок $[1, r-1]$ разбиваем на части (стремясь выделить участки, на которых обе компоненты монотонны) $1 \leq i \leq \frac{r}{3}$, $\frac{r}{3} \leq i \leq \left[\frac{r}{2}\right]$, $\left[\frac{r}{2}\right] + 1 \leq i \leq r-1$, которые при достаточно большом r не пусты. Произведем разбиение суммы на три слагаемых

$$\sum_{i=1}^{r-1} A_i = \sum_{1 \leq i < \frac{r}{3}} A_i + \sum_{\frac{r}{3} \leq i \leq \left[\frac{r}{2}\right]} A_i + \sum_{\left[\frac{r}{2}\right] + 1 \leq i \leq r-1} A_i.$$

Будем изучать поведение $\{A_i\}$ на указанных частях. С этой целью рассмотрим величины

$$B_i = \frac{A_i}{A_{i+1}} = \frac{i+1}{r-i} \left(\frac{r}{i+1}\right)^N \left(\frac{1}{\left(1 + \frac{1}{i}\right)^i}\right)^N.$$

1. Оценка $\sum_{1 \leq i < \frac{r}{3}} A_i$. Имеем

$$B_i > \frac{r}{r-i} \left(\frac{r}{i+1}\right)^{N-1} e^{-N} > \frac{1}{e} \left(\frac{3}{e\left(1 + \frac{3}{r}\right)}\right)^{N-1}.$$

Так как при больших r получим $e\left(1 + \frac{3}{r}\right) < 3$, то найдется N_1 такое, что при $N \geq N_1$ будет $B_i > 1$ ($1 \leq i < \frac{r}{3}$). При этих условиях наибольшим слагаемым при $1 \leq i < \frac{r}{3}$ будет A_1 . Мы получаем при $N \geq N_1$:

$$\sum_{1 \leq i < \frac{r}{3}} A_i \leq \frac{r}{3} A_1 = \frac{1}{3} \left(\frac{1}{r}\right)^{N-2} \rightarrow 0 \quad \text{при } N \rightarrow \infty.$$

2. Оценка $\sum_{\left[\frac{r}{2}\right] + 1 \leq i \leq r-1} A_i$. Поскольку $i+1 \geq \left[\frac{r}{2}\right] + 2 > \frac{r}{2}$ и при $i \geq 2$

имеем $\left(1 + \frac{1}{i}\right)^i \geq 2.25$, то

$$B_i \leq r \left(\frac{2}{2.25}\right)^N = \left(\frac{2 \cdot 2^{\frac{\log r}{N}}}{2.25}\right)^N.$$

Так как $\frac{\log r}{N} \rightarrow 0$ при $N \rightarrow \infty$, то $B_i \rightarrow 0$ (при $N \rightarrow \infty$) и поэтому существует N_2 такое, что при $N \geq N_2$ будет $B_i < \frac{1}{2}$ ($i = \left[\frac{r}{2}\right] + 1, \dots, r-1$), а

$$\begin{aligned} \sum_{i \leq r-1} A_i &= A_{r-1} (1 + B_{r-2} + B_{r-2} B_{r-3} + \dots) \leq \\ &\leq A_{r-1} \left(1 + \frac{1}{2} + \frac{1}{4} + \dots\right) < 2re^{-N} = 2e^{(-1 + \frac{\ln r}{N})N} \rightarrow 0. \end{aligned}$$

3. Оценка $\sum_{\frac{r}{3} \leq i \leq [\frac{r}{2}]} A_i$. При $N \rightarrow \infty$

$$\sum_{\frac{r}{3} \leq i \leq [\frac{r}{2}]} A_i \leq \max_{\frac{r}{3} \leq i \leq [\frac{r}{2}]} \left(\frac{i}{r}\right)^{Ni} 2^r.$$

В силу унимодальности и выпуклости книзу функции $\left(\frac{x}{r}\right)^{Nx}$ ее максимальное значение принимается на концах отрезка, т. е.

$$\max_{\frac{r}{3} \leq i \leq [\frac{r}{2}]} \left(\frac{i}{r}\right)^{Ni} \leq \max \left\{ \left(\frac{1}{3}\right)^{\frac{Nr}{3}}, \left(\frac{1}{2}\right)^{\frac{Nr}{2}} \right\} = \left(\frac{1}{\sqrt{2}}\right)^{Nr} < \frac{1}{4^r}$$

при $N \geq 4$. Отсюда

$$\sum_{\frac{r}{3} \leq i \leq [\frac{r}{2}]} A_i \leq \frac{1}{2^r} \rightarrow 0 \quad \text{при} \quad r \rightarrow \infty.$$

Следовательно,

$$\sum_{i=1}^{r-1} A_i = o(1).$$

Далее,

$$\frac{(r-1)^2}{M^N} = \left(1 - \frac{1}{r}\right)^2 \left(\frac{2^{2 \frac{\log r}{N}}}{M}\right)^N = o(1).$$

Мы получаем

$$P(N, M, r) \gtrsim \frac{(Mr)^{Nr}}{(r-1)!} (1 - o(1)).$$

Теорема доказана.

§ 2. Нижняя мощностная оценка

Здесь рассматривается класс $\mathfrak{S}^a(n, p, l, L)$ автоматных схем в базисе

$B = \left\{ \begin{array}{c} \downarrow n_i \downarrow \\ \nabla \\ F_i \end{array}, \begin{array}{c} \downarrow \\ \boxed{3} \\ \downarrow \end{array}, (i = 1, \dots, r) \right\}$ со входами из алфавита X_n , имеющими p выходов $z_1, \dots, z_p$, $l_0 \leq l$ задержек и со сложностью $L(\Sigma) = \sum_{i=0}^r \lambda_i h_i \leq L$. Обозначим $|\mathfrak{S}^a(n, p, l, L)|$ через $S^a(n, p, l, L)$.

Л е м м а 10. При $L \geq c_0(n + l)$, $p + l = o(L)$ для любого $\varepsilon > 0$ существует $N(\varepsilon)$ такое, что при $n > N$

$$S^a(n, p, l, L) \leq (cL)^{\frac{L}{p}(1+\varepsilon)}.$$

Д о к а з а т е л ь с т в о. Возьмем $\Sigma \in \mathfrak{S}^a(n, p, l, L)$. Пусть l_0 — число задержек в Σ . Удалим в Σ задержки и образовавшиеся дополнительные

входы и выходы занумеруем соответственно числами $1, \dots, l_0$. Мы получим схему $\tilde{\Sigma} \in \mathfrak{S}(n + l_0, p + l_0, L)$ со входами $x_{i_1}, \dots, x_{i_m}, 1, \dots, l_0$ и выходами $z_1, \dots, z_p, 1, \dots, l_0$, имеющую сложность $L(\tilde{\Sigma}) = L(\Sigma) - \lambda_0 l_0 \leq L - \lambda_0 l_0 \leq L$. По схеме $\tilde{\Sigma}$ однозначно восстанавливается Σ . Отсюда

$$S^a(n, p, l, L) \leq \sum_{l_0=0}^{\left\lfloor \frac{L}{\lambda_0} \right\rfloor} S(n + l_0, p + l_0, L) \leq \left(\left\lfloor \frac{L}{\lambda_0} \right\rfloor + 1 \right) S(n + l_0, p + l_0, L).$$

С другой стороны, в силу следствия из леммы 7 при $L \geq c_0 n$ и $p + l = o(L)$ для любого $\varepsilon > 0$ существует $N_1(\varepsilon)$ такое, что при $n > N_1$

$$S(n + l_0, p + l_0, L) \leq (c_1 L)^{\frac{L}{\rho}(1+\varepsilon)}.$$

Таким образом, при указанных ограничениях и $n > N_1$

$$S^a(n, p, l, L) \leq \left(\frac{L}{\lambda_0} + 1 \right) (c_1 L)^{\frac{L}{\rho}(1+\varepsilon)}.$$

Беря $n > N$ ($N > N_1$), мы получим

$$S^a(n, p, l, L) \leq (cL)^{\frac{L}{\rho}(1+\varepsilon)}.$$

Лемма доказана.

Теперь воспользуемся теоремой 10 о нижней оценке и докажем следующую теорему.

Т е о р е м а 13. При r постоянном и $\log p = o(2^n)$

$$L(n, p, r) \gtrsim \rho \frac{r 2^n (p + \log r)}{n + \log p}.$$

Д о к а з а т е л ь с т в о. Беря $l_0 \geq \lceil \log r \rceil$, мы можем каждую о.-д. функцию из $\mathfrak{F}(n, p, r)$ реализовать автоматной схемой при некотором L .

Полагая $L = \left\lceil \rho \frac{\log P(n, p, r)}{\log \log P(n, p, r)} \right\rceil$, мы удовлетворим условию леммы 10 при $p = o(L)$, что равносильно (с учетом теоремы 11) условию $\log p = o(2^n)$. В этом случае выполнены предпосылки теоремы 10 о нижней оценке.

Теперь нам остается выписать явный вид асимптотической оценки снизу, зная (из теоремы 11), что $P(n, p, r) \sim \frac{(Mr)^{Nr}}{(r-1)!}$ (при постоянном r). Мы имеем

$$\log P(n, p, r) \sim Nr(\log M + \log r) - \log(r-1)! \sim Nr(\log M + \log r)$$

и

$$\log \log P(n, p, r) \sim \log N + \log r + \log(\log M + \log r) \sim \log N + \log \log M.$$

Мы получаем

$$\frac{\log P(n, p, r)}{\log \log P(n, p, r)} \sim \frac{Nr(\log M + \log r)}{\log N + \log M},$$

где $N = 2^n$, $M = 2^p$. Следовательно⁶,

$$\frac{\log P(n, p, r)}{\log \log P(n, p, r)} \sim \frac{r2^n(p + \log r)}{n + \log p}.$$

Окончательно мы получаем

$$L(n, p, r) \gtrsim \rho \frac{r2^n(p + \log r)}{n + \log p}.$$

§ 3. Синтез автоматов и условия, при которых метод является асимптотически наилучшим

Каждую о.-д. функцию веса не большего чем r (r — постоянно), можно записать при помощи канонических уравнений

$$\begin{cases} z_1(t) = f_1(x_1(t), \dots, x_n(t), q_1(t-1), \dots, q_l(t-1)), \\ \dots \\ z_p(t) = f_p(x_1(t), \dots, x_n(t), q_1(t-1), \dots, q_l(t-1)), \\ q_1(t) = g_1(x_1(t), \dots, x_n(t), q_1(t-1), \dots, q_l(t-1)), \\ \dots \\ q_l(t) = g_l(x_1(t), \dots, x_n(t), q_1(t-1), \dots, q_l(t-1)), \end{cases}$$

$$q_1(0) = \dots = q_l(0) = 0 \quad \text{при} \quad l = \lceil \log r \rceil.$$

Реализуя систему булевых функций $\{f_1, \dots, f_p, g_1, \dots, g_l\}$ по методу Лупанова и соединяя входы $q_1, \dots, q_l$ с выходами $g_1, \dots, g_l$ через задержки, получим схему Σ^a (рис. 31).

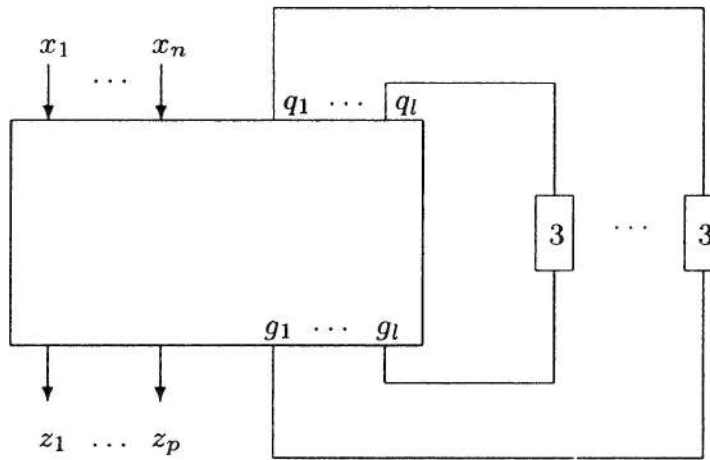


Рис. 31

⁶Отсюда видна и эквивалентность условия $p = o(L)$ и $\log p = o(2^n)$.

Для этой схемы выполняются (теорема 9) соотношения

$$L(\Sigma^a) \gtrsim \rho \frac{(p+l)2^{n+l}}{n+l} + \lambda_0 l \sim \rho \frac{(p+l)2^{n+l}}{n}.$$

Если $r = 2^l$ и $\log p = o(n)$, то верхняя оценка асимптотически совпадает с нижней и имеет вид

$$L(n, p, r) \sim \rho \frac{r(p + \log r)2^n}{n}.$$

Очевидно, условие $\log p = o(n)$ поглощает условие $\log p = o(2^n)$.

Данный результат справедлив для любого r , но для этого надо воспользоваться методом синтеза для частичных булевых функций.

ГЛАВА 4. МЕТОД КАСКАДОВ

Асимптотически наилучшие методы синтеза дают хорошие результаты для синтеза почти всех булевых функций («плохих функций»). В то же время они плохо приспособлены для реализации функций, допускающих существенно более простые минимальные схемы, чем плохие функции. Кроме того, эти методы мало эффективны для небольшого числа переменных.

Ввиду этого, представляет интерес поиск методов синтеза, которые, может быть, на всем классе функций работают хуже асимптотически наилучших, но для функций, встречающихся в приложениях (входящих в множество «хороших функций»), давали бы сравнительно хорошие схемы и притом достаточно простым алгоритмом.

Одним из таких методов является метод каскадов, который в своей простейшей форме извлекается естественно из метода Шеннона. Для случая двухполюсных контактных схем был предложен американскими учеными Захедом и Кейвудом в 1955 г. и независимо, но в более общей форме для многополюсных контактных схем — Г.Н. Поваровым [20] в 1955 г. Здесь излагается этот метод еще в более общей форме, охватывающей не только контактные схемы, но и схемы из функциональных элементов, применительно к различным базисам.

Указанный метод складывается из следующих этапов:

I. Выбор разложения (декомпозиции) для булевой функции

$$f(x_1, \dots, x_n) = g(h_1(X_1), \dots, h_m(X_m)),$$

где m не зависит от n и каждая из функций $h_1, \dots, h_m$ зависит менее, чем от n переменных.

II. Построение схемы разложения.

III. Получение реализации в данном классе управляющих систем.

IV. Упрощение схемы.

Дадим характеристику этих этапов.

I. В качестве разложений можно взять:

$$1) f(x_1, \dots, x_n) = x_n f(x_1, \dots, x_{n-1}, 1) \vee \bar{x}_n f(x_1, \dots, x_{n-1}, 0);$$

$$2) f(x_1, \dots, x_n) = x_n f_1(x_1, \dots, x_{n-1}) + f_2(x_1, \dots, x_{n-1}) \pmod{2};$$

3) $f(x_1, \dots, x_n) = x_n f_1(x_1, \dots, x_{n-1}) \vee f_2(x_1, \dots, x_{n-1})$ — для монотонных функций.

Выбор разложения естественно связывается с базисом для изучаемого класса управляющих систем. В частности, внешняя функция $g(y_1, \dots, y_m)$ должна достаточно просто выражаться через базисные функции и операции.

Предпочтительно выбирать такие разложения, у которых при фиксированной внешней функции внутренние функции $h_1, \dots, h_m$ определяются однозначно по f .

В качестве основного разложения возьмем разложение

$$f(x_1, \dots, x_n) = x_n f'(x_1, \dots, x_{n-1}) \vee \bar{x}_n f''(x_1, \dots, x_{n-1})$$

и дальнейшие этапы подробно разберем для этого случая.

II. Построение схемы разложения.

Пусть задана система попарно различных булевых функций

$$\mathfrak{B}_n = \{f_1(x_1, \dots, x_n), \dots, f_p(x_1, \dots, x_n)\} \quad \text{и} \quad f_i \not\equiv \text{const}^7 \quad (i = 1, \dots, p).$$

а) Выберем порядок следования переменных

$$x_{i_1} \prec x_{i_2} \prec \dots \prec x_{i_n}.$$

Поскольку можно осуществить перенумерацию переменных, то можно считать, что выбранным порядком будет

$$x_1 \prec x_2 \prec \dots \prec x_n.$$

б) Индуктивным образом строим последовательность множеств

$$\mathfrak{B}_n, \mathfrak{B}_{n-1}, \dots, \mathfrak{B}_0,$$

в которой множество $\mathfrak{B}_i$ будет состоять из некоторых функций, зависящих от переменных $x_1, x_2, \dots, x_i$. Множество $\mathfrak{B}_n$ определено. Пусть построены множества

$$\mathfrak{B}_n, \dots, \mathfrak{B}_i, \quad i \geq 0.$$

Если $i = 0$, процесс закончен. Если $i > 0$, то для каждой функции $f \in \mathfrak{B}_i$ рассматриваем разложение

$$f(x_1, \dots, x_i) = x_i f'(x_1, \dots, x_{i-1}) \vee \bar{x}_i f''(x_1, \dots, x_{i-1})$$

и функции f' , f'' включаем в множество $\mathfrak{B}_{i-1}$. Множество $\mathfrak{B}_{i-1}$ будет состоять из некоторых функций, зависящих от переменных $x_1, \dots, x_{i-1}$. Очевидно, что множество $\mathfrak{B}_0$, так как $\mathfrak{B}_n$ не содержит констант, содержит константы 0 и 1.

⁷Поскольку реализация констант не вызывает трудностей.

в) От последовательности множеств $\mathfrak{B}_n, \mathfrak{B}_{n-1}, \dots, \mathfrak{B}_0$ перейдем к последовательности $\mathfrak{C}_n, \mathfrak{C}_{n-1}, \dots, \mathfrak{C}_0$, где $\mathfrak{C}_i$ состоит из всех функций множества $\mathfrak{B}_i$, которые существенно зависят от переменного x_i ($n \leq i \leq 1$), и $\mathfrak{C}_0 = \{1\}$. Очевидно, что $\mathfrak{C}_i \subseteq \mathfrak{B}_i$ и $\bigcup_{i=0}^n \mathfrak{C}_i = \bigcup_{i=0}^n \mathfrak{B}_i \setminus \{0\}$. Положим $c_i = |\mathfrak{C}_i|$. Тогда

$$\mathfrak{C}_i = \{f_{i,1}(x_1, \dots, x_i), \dots, f_{i,c_i}(x_1, \dots, x_i)\}.$$

г) Построение схемы разложения. Для каждого множества $\mathfrak{C}_i$, где $i = 0, 1, \dots, n$, выбираем на плоскости c_i точек и взаимно однозначным образом помечаем их символами $f_{i,1}, \dots, f_{i,c_i}$. Далее, вершину, помеченную символом f , где

$$f(x_1, \dots, x_i) = x_i f' \vee \bar{x}_i f'',$$

соединяем с вершинами, помеченными символами f' и f'' , так, как указано на рис. 32.

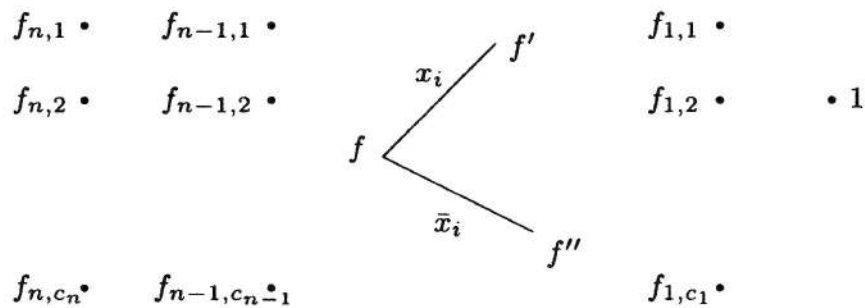


Рис. 32

Полученный рисунок дает искомую схему разложения.

Пример 1.

а) Полагаем $\mathfrak{B}_n = \{x_1 + \dots + x_n \pmod{2}\}$.

б) Строим последовательность $\mathfrak{B}_n, \mathfrak{B}_{n-1}, \dots, \mathfrak{B}_0$:

$$\mathfrak{B}_n = \{x_1 + \dots + x_n\},$$

$$\mathfrak{B}_{n-1} = \{x_1 + \dots + x_{n-1}, x_1 + \dots + x_{n-1} + 1\},$$

...

$$\mathfrak{B}_i = \{x_1 + \dots + x_i, x_1 + \dots + x_i + 1\},$$

...

$$\mathfrak{B}_1 = \{x_1, x_1 + 1\},$$

$$\mathfrak{B}_0 = \{0, 1\}.$$

в) Находим последовательность $\mathfrak{C}_n, \mathfrak{C}_{n-1}, \dots, \mathfrak{C}_0$. Очевидно, что здесь $\mathfrak{C}_n = \mathfrak{B}_n, \dots, \mathfrak{C}_1 = \mathfrak{B}_1, \mathfrak{C}_0 = \{1\}$.

г) Учитывая разложения

$$x_1 + \dots + x_i = x_i(x_1 + \dots + x_{i-1} + 1) \vee \bar{x}_i(x_1 + \dots + x_{i-1}),$$

$$x_1 + \dots + x_i + 1 = x_i(x_1 + \dots + x_{i-1}) \vee \bar{x}_i(x_1 + \dots + x_{i-1} + 1),$$

получаем схему разложения (рис. 33). Здесь $c_n = c_0 = 1$ и $c_i = 2, 1 \leq i \leq n-1$.

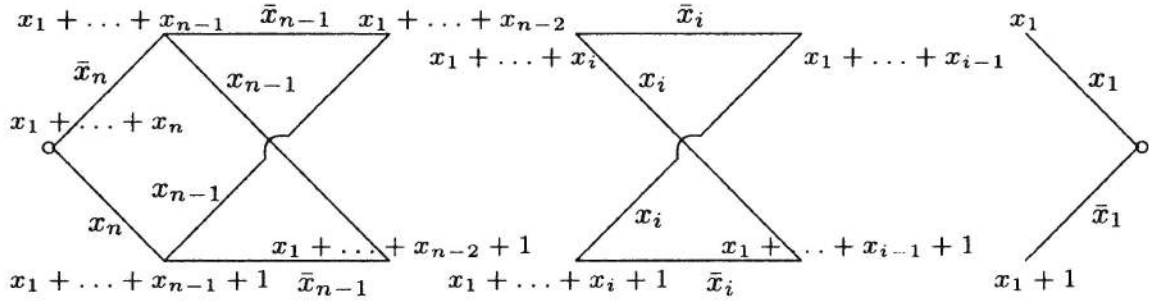


Рис. 33

Для практических целей процедуру построения схемы разложения удобнее видоизменить, чтобы избежать двойного рассмотрения разложения функций (пункты (б) и (г)), так.

- а) Выбор порядка следования переменных.
- б) Выписывание разложений по переменным.
- в) Построение множеств $\mathfrak{C}_n, \dots, \mathfrak{C}_0$. Здесь $f(x_1, \dots, x_m) \in \mathfrak{C}_i$ ($i \leq m \leq n$) тогда и только тогда, когда: 1) f является компонентой разложения системы; 2) максимальный номер существенного переменного равен i ($i \leq m$); при этом считается, что $i = 0$, если существенных переменных нет.
- г) Построение схемы разложений.

Пример 2. Возьмем $\mathfrak{B}_4 = \{f(x_1, x_2, x_3, x_4)\}$, где

$$f(x_1, x_2, x_3, x_4) = \bar{x}_1 \bar{x}_2 \bar{x}_3 x_4 \vee \bar{x}_1 \bar{x}_2 x_3 \bar{x}_4 \vee \bar{x}_1 x_2 \bar{x}_3 \bar{x}_4 \vee \bar{x}_1 x_2 x_3 x_4 \vee \\ \vee x_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \vee x_1 \bar{x}_2 x_3 x_4 \vee x_1 x_2 \bar{x}_3 x_4 \vee x_1 x_2 x_3 \bar{x}_4 \vee x_1 x_2 x_3 x_4.$$

Исходя из естественного порядка следования переменных, строим разложения по переменным:

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_4(\bar{x}_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3 \vee x_1 x_2 x_3) \vee \\ &\quad \vee \bar{x}_4(\bar{x}_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 \bar{x}_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee x_1 x_2 x_3), \\ \bar{x}_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3 \vee x_1 x_2 x_3 &= \\ &= x_3(\bar{x}_1 x_2 \vee x_1 \bar{x}_2 \vee x_1 x_2) \vee \bar{x}_3(\bar{x}_1 \bar{x}_2 \vee x_1 x_2), \\ \bar{x}_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 \bar{x}_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee x_1 x_2 x_3 &= x_3(\bar{x}_1 \bar{x}_2 \vee x_1 x_2) \vee \bar{x}_3(\bar{x}_1 x_2 \vee x_1 \bar{x}_2), \\ \bar{x}_1 x_2 \vee x_1 \bar{x}_2 \vee x_1 x_2 &= x_2 \vee \bar{x}_2 x_1, \\ \bar{x}_1 \bar{x}_2 \vee x_1 x_2 &= x_2 x_1 \vee \bar{x}_2 \bar{x}_1, \\ \bar{x}_1 x_2 \vee x_1 \bar{x}_2 &= x_2 \bar{x}_1 \vee \bar{x}_2 x_1. \end{aligned}$$

Строим множества $\mathfrak{C}_4, \mathfrak{C}_3, \mathfrak{C}_2, \mathfrak{C}_1, \mathfrak{C}_0$:

$$\begin{aligned} \mathfrak{C}_4 &= \{f(x_1, x_2, x_3, x_4)\}, \\ \mathfrak{C}_3 &= \{\bar{x}_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3 \vee x_1 x_2 x_3, \\ &\quad \bar{x}_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 \bar{x}_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee x_1 x_2 x_3\}, \\ \mathfrak{C}_2 &= \{\bar{x}_1 x_2 \vee x_1 \bar{x}_2 \vee x_1 x_2, \bar{x}_1 \bar{x}_2 \vee x_1 x_2, \bar{x}_1 x_2 \vee x_1 \bar{x}_2\}, \\ \mathfrak{C}_1 &= \{x_1, \bar{x}_1\}, \\ \mathfrak{C}_0 &= \{1\}. \end{aligned}$$

Получаем следующую схему разложения (рис. 34).

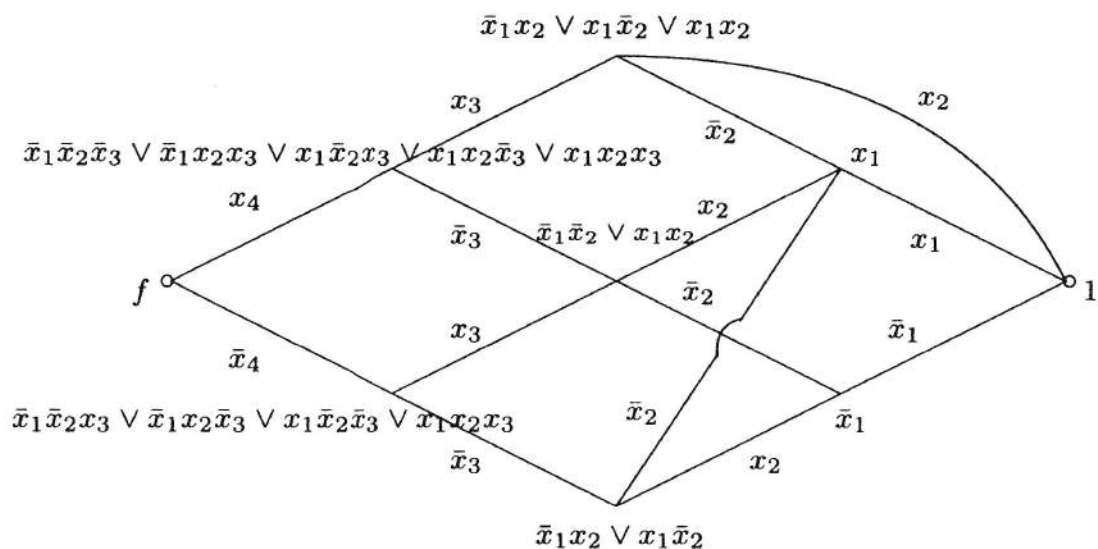


Рис. 34

Как видно из примеров, схема разложения содержит полную информацию о компонентах разложения (подфункциях) и их связях.

III. Получение реализации.

1. В классе контактных схем. В построенной нами схеме разложения удаляем пометки подфункций, стоящие при вершинах. Получаем искомую контактную схему.

Для примеров 1 и 2 эти схемы изображены на рис. 35.

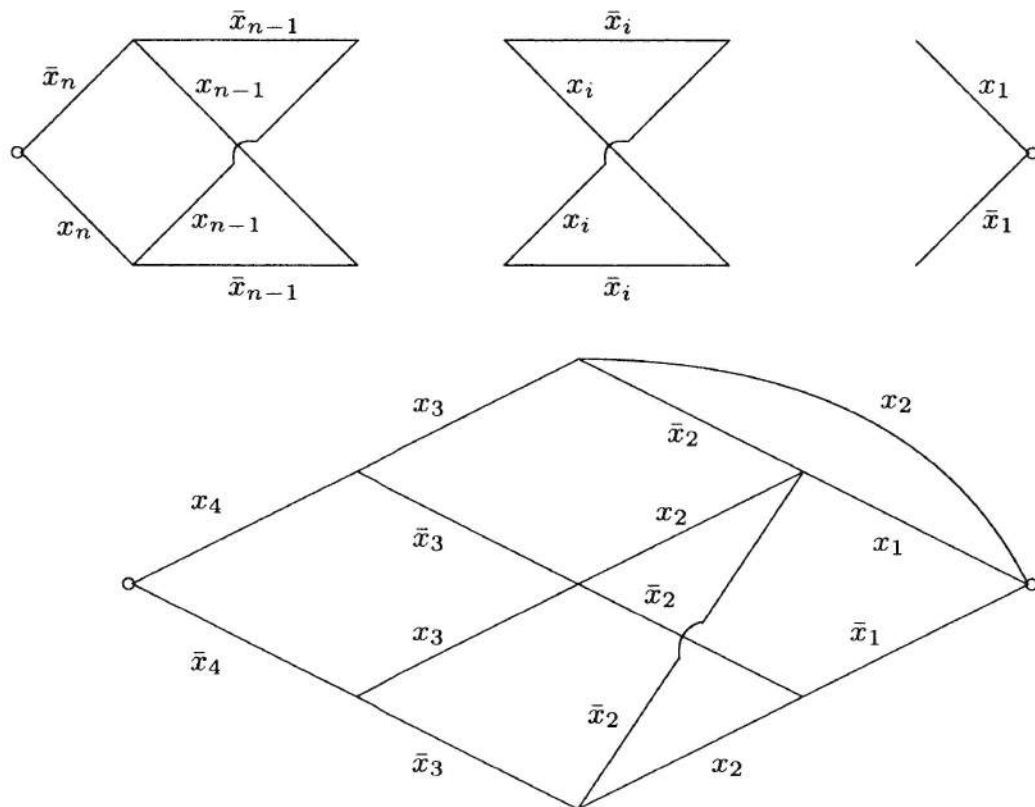


Рис. 35

Данные схемы весьма компактны. Первая из них содержит $4n - 4$ контакта и является минимальной для $x_1 + \dots + x_n$, вторая имеет сложность 14 и близка к минимальной. Цепи этих схем сильно переплетены, что затрудняет их получение путем «случайного» склеивания цепей.

2. В классе схем из Ф.Э. с базисом B_0 . Пусть $B_0 = \left\{ \begin{array}{c} \downarrow \\ \neg \\ \downarrow \end{array}, \begin{array}{c} \downarrow \downarrow \\ \& \\ \downarrow \end{array}, \begin{array}{c} \downarrow \downarrow \\ \vee \\ \downarrow \end{array} \right\}$.

Искомая схема из Ф.Э. получается из схемы разложения путем замены фрагментов (рис. 36) соответственно на подсхемы (рис. 37), присоединения к вершине с пометкой 1 схемы (рис. 38) и склейкой всех входов с пометкой x_i ($i = 1, \dots, n$).

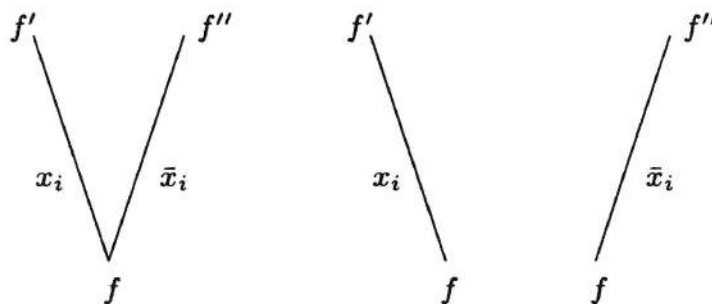


Рис. 36

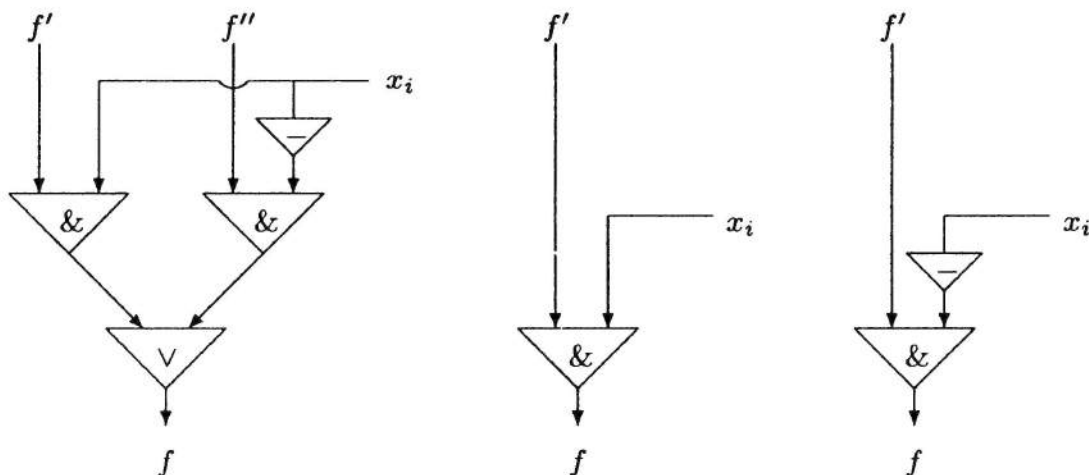


Рис. 37

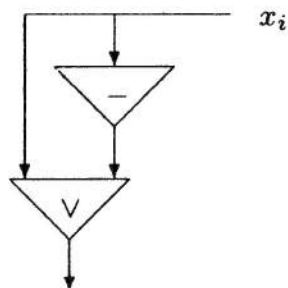


Рис. 38

На рис. 39 приведена схема из Ф.Э., реализующая

$$x_1 + x_2 + x_3 \pmod{2}$$

(она по сравнению со схемой разложения развернута на 90°).

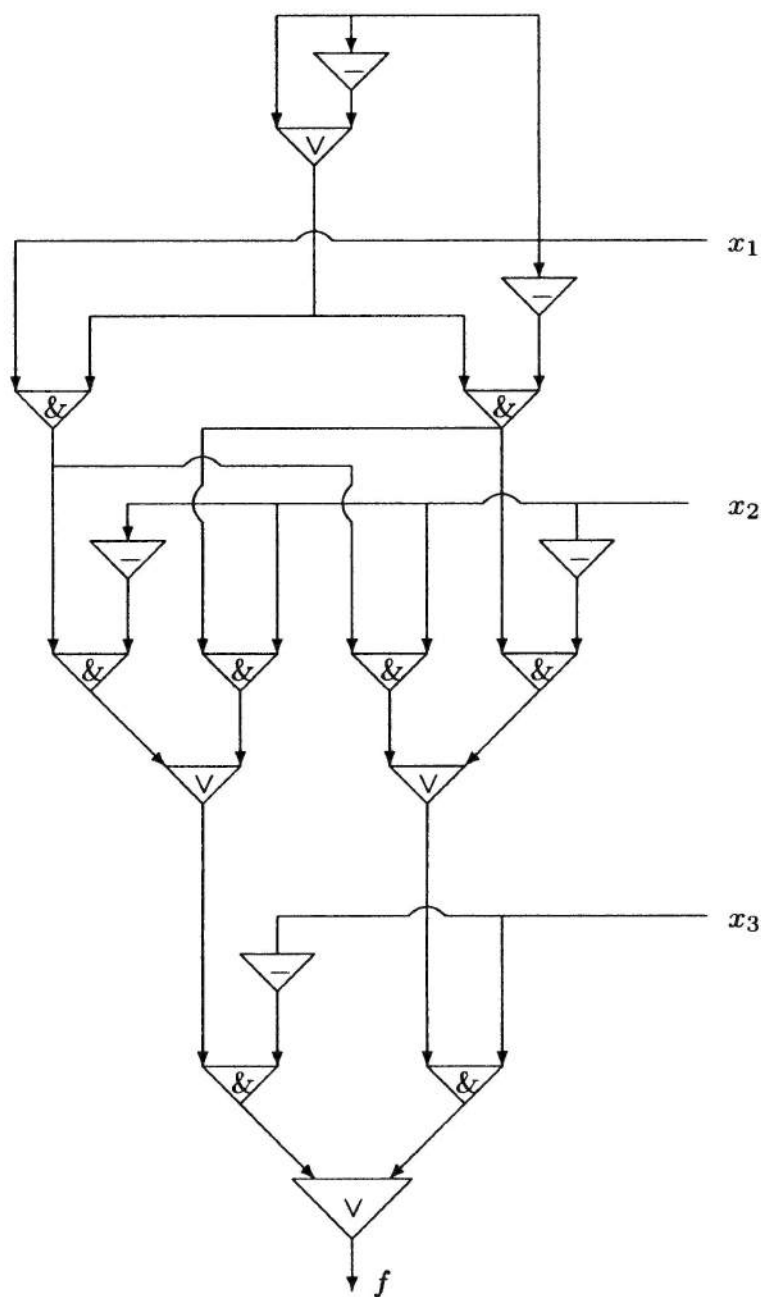


Рис. 39

Далее на рис. 40 приводится схема из Ф.Э., реализующая функцию из второго примера.

IV. Упрощение схемы.

В случае схем из Ф.Э. построенная схема допускает иногда значительные упрощения. Они сводятся:

- а) к объединению инверторов, стоящих на входах x_i ($i = 1, \dots, n$);
- б) удалению схемы, реализующей 1, и конъюнкторов, на входы которых подается 1;

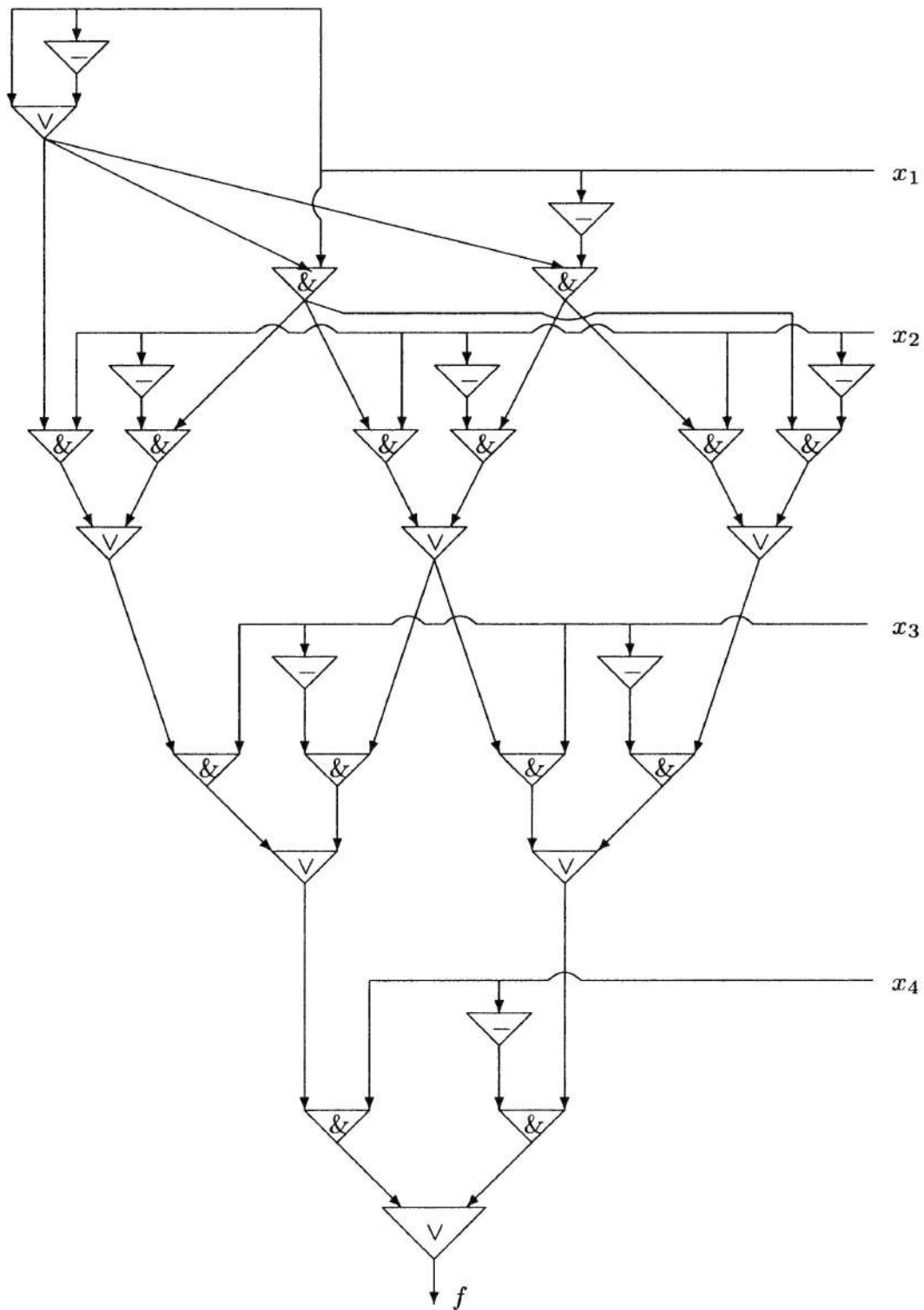


Рис. 40

в) если имеются подфункции f и $\tilde{f}$ вида

$$\begin{aligned} f &= x_i f' \vee \bar{x}_i f'', & \text{или} & & f &= x_i f' \vee \bar{x}_i f'', \\ \tilde{f} &= x_i f' \vee \bar{x}_i \tilde{f}'', & & & \tilde{f} &= x_i \tilde{f}' \vee \bar{x}_i f'', \end{aligned}$$

то при их реализации член $x_i f'$ (или $\bar{x}_i f''$) нужно реализовывать один раз.

Поясним эти моменты для упрощения схемы (рис. 40). Заметим, что подфункции $\bar{x}_1 x_2 \vee x_1 \bar{x}_2 \vee x_1 x_2$ и $x_1 \bar{x}_2 \vee \bar{x}_1 x_2$ имеют совпадающие части

в разложениях по x_2 :

$$\bar{x}_1 x_2 \vee x_1 \bar{x}_2 \vee x_1 x_2 = x_2 \vee \bar{x}_2 x_1, \quad x_1 \bar{x}_2 \vee \bar{x}_1 x_2 = x_2 \bar{x}_1 \vee \bar{x}_2 x_1,$$

поэтому подсхемы, реализующие $\bar{x}_2 x_1$, можно объединить. Мы приходим к схеме (рис. 41), содержащей 20 функциональных элементов против 29 в исходной. Следует обратить внимание на то, что перечисленные преобразования схем для схем из Ф.Э. ввиду ориентированности элементов проходят без всяких оговорок. Для контактных схем склеивание цепей может привести к потере свойства разделительности и поэтому давать новые дополнительные цепи.

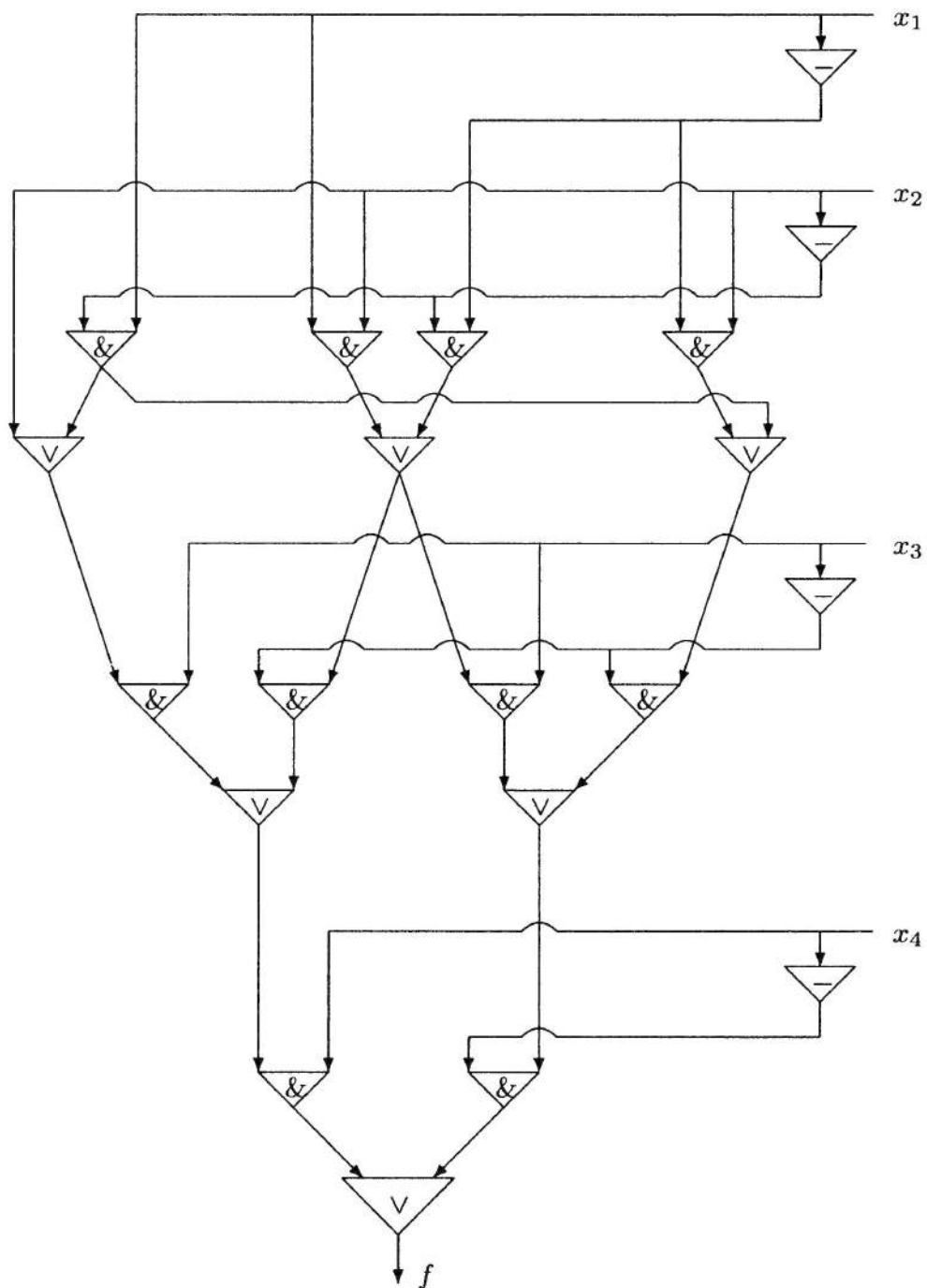


Рис. 41

Рассмотрим качественно вопрос о сложности схем, получаемых методом каскадов.

а) Случай контактных схем. Здесь сложность построенной контактной схемы совпадает с числом ребер в схеме разложения. Для схемы разложения (см. также примеры 1 и 2) характерно то, что при построении множеств $\mathfrak{B}$ ($\mathfrak{C}$) сначала появляются различные компоненты в разложении — этому этапу в схеме соответствует дерево, затем компоненты начинают повторяться — дерево начинает склеиваться и возникает неправильная часть схемы, подобная части универсального многополюсника. Более подробный анализ показывает, что схема, полученная методом каскадов, получается из схемы, построенной по методу Шеннона, путем частичной склейки цепей. Это позволяет заключить, что ее сложность $\lesssim 4\frac{2^n}{n}$ и для почти всех булевых функций сложности соответствующих этим методам схем асимптотически эквивалентны.

б) Случай из Ф.Э. в классическом базисе. Рассмотрим сначала схему, получаемую непосредственно по схеме разложения с объединением инверторов на входах. Число конъюнкторов и дизъюнкторов в ней не превосходит суммы числа вершин плюс числа ребер схемы разложения. Отсюда сложность схемы из Ф.Э. $\lesssim 6\frac{2^n}{n}$ (ибо число ребер не более, чем в два раза больше числа вершин и число вершин $\lesssim 2\frac{2^n}{n}$ (см. пункт а)).

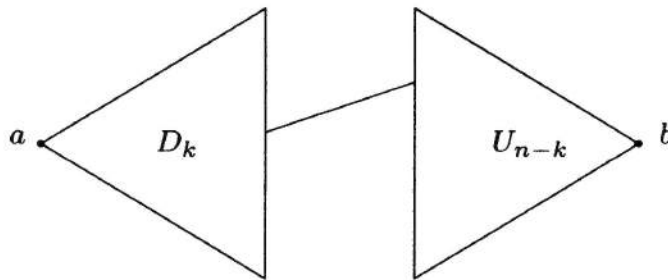


Рис. 42

Если учесть, что в методе Шеннона при $m = n - k = \lceil \log(n - 2 \log n) \rceil$ (рис. 42) число контактов в k -м ярусе дерева D_k равно $2^k \asymp \frac{2^n}{n}$, а число входов универсального многополюсника U_{n-k} есть $2^{2^{n-k}} \lesssim \frac{2^n}{n^2}$, то в соответствующей этому многополюснику схеме из Ф.Э. можно осуществить склейку компонент $x_k^\sigma \tilde{f}$. В результате этого число конъюнкторов может быть значительно уменьшено: верхняя оценка числа конъюнкторов уменьшается асимптотически на 2^k и составляет вместо $4\frac{2^n}{n}$ величину $2\frac{2^n}{n}$. Таким образом, сложность схем из Ф.Э., построенных по методу каскадов, будет $\lesssim 4\frac{2^n}{n}$. Можно показать, что нижняя оценка для наихудшего случая будет равна

$$\delta(n) \frac{2^n}{n}, \quad \text{где } 2 \leq \delta(n) \leq 4.$$

В заключение заметим, что сложность схемы, получаемой по методу каскадов, зависит от выбора порядка разложения.

РАЗДЕЛ 2. СИНТЕЗ СХЕМ ДЛЯ ОТДЕЛЬНЫХ КЛАССОВ ФУНКЦИЙ

Универсальные методы синтеза (т. е. методы, пригодные для всего класса $\mathfrak{F}$) показывают, что для основных классов У.С. возможно построение для почти всех функций из $\mathfrak{F}_n$ схем, сложность которых близка к минимальной и асимптотически равна $\rho \frac{2^n}{n}$, т. е. является при сравнительно небольших n весьма большой. Это означает, что практический интерес представляет реализация функций, принадлежащих малой доле из $\mathfrak{F}_n$. Поэтому с самого начала развития теории синтеза появился интерес к выявлению классов функций из $\mathfrak{F}$, допускающих простую реализацию, и к разработке соответствующих методов синтеза. В дальнейшем данные вопросы будем рассматривать, когда $\mathfrak{F} = P_2$, для реализаций контактными схемами.

§ 1. Примеры синтеза для некоторых простейших классов функций

1. Класс L линейных функций l_n^σ , где

$$l_n^\sigma(x_1, \dots, x_n) = x_1 + \dots + x_n + \sigma.$$

а) Реализация контактными схемами. Как мы видели, метод каскадов для l_n^σ дает схему Σ_n^σ и

$$L(\Sigma_n^\sigma) = 4n - 4.$$

Из последующего будет вытекать, что схема Σ_n^σ минимальна.

б) Реализация контактными π -схемами.

З а м е ч а н и е. Если Σ_n^σ реализует функцию l_n^σ , то схема $\Sigma_n^{\bar{\sigma}}$, получающаяся из Σ_n^σ путем замены всех контактов x_1 на $\bar{x}_1$ и $\bar{x}_1$ на x_1 , будет реализовывать $l_n^{\bar{\sigma}}$ и

$$L(\Sigma_n^{\bar{\sigma}}) = L(\Sigma_n^\sigma).$$

Поэтому достаточно уметь реализовывать функцию l_n^0 .

О п р е д е л е н и е контактной π -схемы (индуктивное).

Б а з и с индукции. Простейшая двухполюсная контактная схема, содержащая один контакт x^σ , является π -схемой.

И н д у к т и в н ы й п е р е х о д. Если Σ_1 и Σ_2 -контактные π -схемы, то их последовательное и параллельное соединение будут контактными π -схемами (рис. 43).

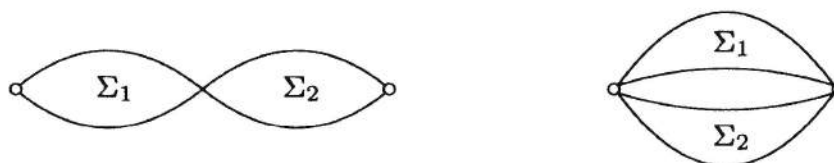


Рис. 43

Легко видеть, что класс контактных π -схем уже класса всех двух-полюсных контактных схем. Однако, каждая булева функция может быть реализована двухполюсной контактной π -схемой. Так, $f(x_1, \dots, x_n) \equiv 0$ может быть реализована схемой, указанной на рис. 44, а функции, отличные от константы 0, реализуем, используя совершенную д.н.ф. Пусть $n \geq 1$, т. е. $l_n^0 \neq \text{const}$.

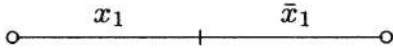


Рис. 44

Теорема 14. Существует метод синтеза для линейных функций в классе контактных π -схем такой, что

$$L_\pi(l_n^\sigma) \leq 4n^2,$$

а при $n = 2^m$

$$L_\pi(l_n^\sigma) \leq n^2.$$

Доказательство. Рассмотрим сначала случай, когда $n = 2^m$. По индукции сначала устанавливаем, что при $m = 0$ имеем $n = 1$, и линейная функция от одного переменного x^σ , может быть реализована π -схемой из одного контакта x^σ . Здесь $L_\pi(\Sigma_1^\sigma) = 1 = 1^2$. Индуктивный переход основан на тождестве

$$\begin{aligned} x_1 + \dots + x_{2^m} &= (x_1 + \dots + x_{2^{m-1}}) + (x_{2^{m-1}+1} + \dots + x_{2^m}) = \\ &= (x_1 + \dots + x_{2^{m-1}}) \overline{(x_{2^{m-1}+1} + \dots + x_{2^m})} \vee \\ &\vee \overline{(x_1 + \dots + x_{2^{m-1}})} (x_{2^{m-1}+1} + \dots + x_{2^m}), \end{aligned}$$

в котором по предположению индукции компоненты $x_1 + \dots + x_{2^{m-1}}$ и $x_{2^{m-1}+1} + \dots + x_{2^m}$, а, следовательно, и их отрицания могут быть реализованы π -схемами $\Sigma_{2^{m-1}}^0$, $\tilde{\Sigma}_{2^{m-1}}^0$, $\Sigma_{2^{m-1}}^1$, $\tilde{\Sigma}_{2^{m-1}}^1$. Тогда функция l_n^0 может быть реализована π -схемой $\Sigma_{2^m}^0$ (рис. 45).

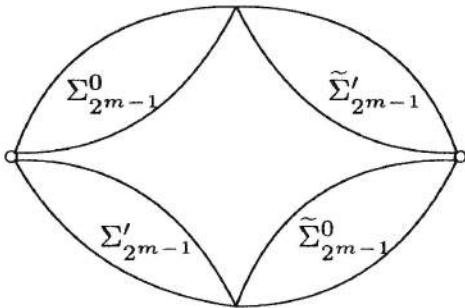


Рис. 45

Получаем $L_\pi(\Sigma_{2^m}^0) = 4L(\Sigma_{2^{m-1}}^0) \leq 4(2^{m-1})^2 = (2^m)^2$. Таким образом, при $n = 2^m$ имеем $L_\pi(l_n^\sigma) \leq n^2$.

В общем случае $2^m \leq n < 2^{m+1}$. Функция l_n^σ получается из функции $l_{2^{m+1}}^\sigma$, если положить $x_{n+1} = \dots = x_{2^{m+1}} = 0$. В таком случае схема для l_n^σ может быть получена из $\Sigma_{2^{m+1}}^\sigma$ при соответствующей подстановке. Поэтому

$$L_\pi(l_n^\sigma) \leq L_\pi(l_{2^{m+1}}^\sigma) \leq (2^{m+1})^2 = 4(2^m)^2 \leq 4n^2.$$

Теорема доказана⁸.

⁸При более точном рассуждении для произвольного n , беря разбиение $x_1 + \dots + x_n$ на два почти равных слагаемых, можно получить оценку $L_\pi(l_n^\sigma) \leq \frac{9}{8}n^2$.

2. Класс S симметрических функций.

Определение. Функция $f(x_1, \dots, x_n) \in P_2$ называется симметрической, если она не меняет своего значения при любой перестановке ее существенных переменных.

Легко видеть, что линейная функция является симметрической. Поэтому $L \subseteq S$. Однако класс S существенно шире, чем класс L , так как он содержит такие функции, как $x_1 \& x_2$, $x_1 \vee x_2$ и др., которые не являются линейными.

Пусть все переменные симметрической функции $f(x_1, \dots, x_n)$ являются существенными. Тогда, если $f(\alpha_1, \dots, \alpha_n) = 1$, то $f(\alpha_{i_1}, \dots, \alpha_{i_n}) = 1$, где $(\alpha_{i_1}, \dots, \alpha_{i_n})$ — перестановка значений $(\alpha_1, \dots, \alpha_n)$. Отсюда следует, что если набор $(\alpha_1, \dots, \alpha_n)$ содержит r единиц, то на любом наборе, содержащем r единиц, $f = 1$. Таким образом, множество единичных значений функции f содержит целиком некоторое множество слоев куба. Обозначим их через $r_1, \dots, r_s$ (слой r_ν содержит все наборы с r_ν единицами). Эти числа иногда называют рабочими числами, и функцию записывают так:

$$f(x_1, \dots, x_n) = S_{r_1, \dots, r_s}(x_1, \dots, x_n).$$

Симметрическая функция, которая имеет ровно одно рабочее число r , называется элементарной симметрической функцией. Ее обозначают через $\sigma_r(x_1, \dots, x_n)$.

Для симметрической функции $S_{r_1, \dots, r_s}(x_1, \dots, x_n)$ имеет место разложение

$$S_{r_1, \dots, r_s}(x_1, \dots, x_n) = \bigvee_{\nu=1}^s \sigma_{r_\nu}(x_1, \dots, x_n).$$

На рис. 46 приведены реализации элементарной симметрической функции $\sigma_r(x_1, \dots, x_n)$ и множества всех элементарных симметрических функций в классе контактных схем.

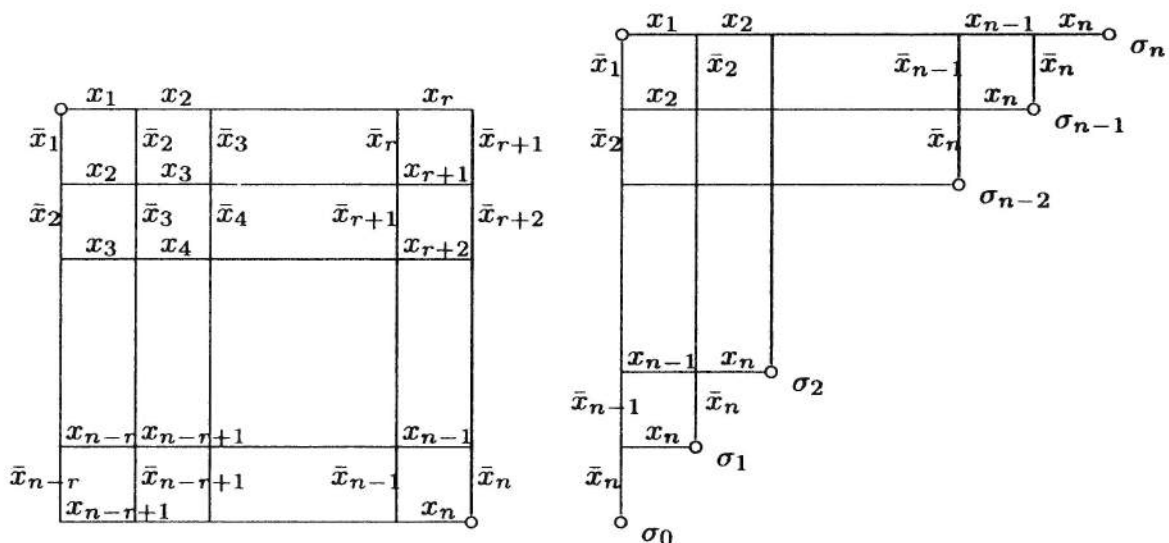


Рис. 46

Теорема 15. Существует метод синтеза для симметрических функций $S_{r_1, \dots, r_s}(x_1, \dots, x_n)$ в классе контактных схем такой, что

$$L(S_{r_1, \dots, r_s}(x_1, \dots, x_n)) \leq n(n+1).$$

Доказательство. Для функции $S_{r_1, \dots, r_s}(x_1, \dots, x_n)$ рассмотрим ее разложение через элементарные симметрические функции и в многополюснике (рис. 46) выходы, соответствующие функциям $\sigma_{r_1}, \dots, \sigma_{r_s}$, объединим в общий выход схемы. Полученная двухполюсная схема будет, очевидно, реализовывать $S_{r_1, \dots, r_s}$. Ее сложность, очевидно, не превышает сложность многополюсника, т. е. величины $n(n+1)$.

Теорема доказана.

Указанные примеры свидетельствуют о том, что для отдельных классов возможно развивать методы синтеза, дающие схемы с невысокой сложностью.

Далее мы переходим к построению общей теории построения достаточно богатой системы классов и развития методов синтеза схем для этих классов.

§ 2. Инвариантные классы и их дескриптивные свойства

Определение. Множество Q функций алгебры логики называется инвариантным классом, если для каждой функции $f(x_1, \dots, x_n) \in Q$ классу Q принадлежат

- 1) все равные ей функции (получающиеся из f путем добавления и изъятий несущественных переменных),
- 2) все функции, получающиеся из f путем переименований (без отождествлений) переменных,
- 3) все функции, получающиеся из f путем любой подстановки констант на места (не обязательно всех) переменных.

Замечание. Если $f(x_1, \dots, x_n) \neq \text{const}$ и принадлежит инвариантному классу Q , то Q содержит обе константы 0 и 1.

Это определение естественно тем, что, если построен некоторый класс преобразователей, класс схем, то мы фактически располагаем всеми преобразователями, схемами, получаемыми из данных при помощи операций (1), (2) и (3), т. е. инвариантным классом.

Приведем примеры инвариантных классов.

1. Класс L всех линейных функций, т. е. функций $f(x_1, \dots, x_n)$, представимых в виде линейного выражения, т. е.

$$f(x_1, \dots, x_n) = c_0 + c_1x_1 + \dots + c_nx_n \pmod{2}.$$

2. Класс M всех монотонных функций.

3. Класс S всех симметрических функций, т. е. функций, значения которых не меняются при любой перестановке существенных переменных.

4. Класс P^N всех функций алгебры логики, зависящих существенно не более, чем от N переменных.

Доказательство их инвариантности очевидно.

Теперь перейдем к выяснению дескриптивных свойств инвариантных классов.

О п р е д е л е н и е. Функция $g(x_1, \dots, x_n)$ называется порождающим элементом для инвариантного класса Q , если $g \in Q$ и либо $g(x_1, \dots, x_n) = \text{const}$ с $n = 0$, либо при любой подстановке констант мы получаем функцию $g' \in Q$.

С л е д с т в и е. Если $g(x_1, \dots, x_n)$ — порождающий элемент для инвариантного класса Q , то все переменные $x_1, \dots, x_n$ являются существенными.

Из данного определения непосредственно вытекает и существование порождающего элемента для всякого инвариантного класса Q такого, что $Q \neq P_2$. В самом деле, в этом случае найдется функция $g(x_1, \dots, x_n) \in Q$. Либо g — порождающий элемент и тогда процесс закончен, либо существует такая подстановка констант, что из функции g получается функция g' , т. е. $g \xrightarrow{\text{п.к.}} g'$ и $g' \in Q$, причем g' зависит от меньшего числа переменных, чем функция g . Здесь возможны опять два случая: либо g' — порождающий элемент и процесс закончен, либо существует подстановка констант, которая из функции g' позволяет получить функцию g'' , т. е. $g' \xrightarrow{\text{п.к.}} g''$ и $g'' \in Q$, и т. д.

Поскольку на каждом шаге число переменных уменьшается, то процесс завершится и мы построим порождающий элемент.

П р и м е р. $Q = M$ — класс монотонных функций.

Пусть $g(x_1, \dots, x_n)$ — немонотонная функция. Тогда, как известно, (см. [34]) из нее при помощи подстановки констант можно получить $\bar{x}_i$ — немонотонную функцию одного переменного, которая, в силу того, что $0, 1 \in M$, будет порождающим элементом.

О п р е д е л е н и е. Две функции g_1 и g_2 будем называть подобными, если при помощи операции переименования переменных можно перейти от одной функции к другой.

В дальнейшем, как мы увидим, нас будут интересовать для инвариантного класса системы попарно неподобных порождающих элементов.

О п р е д е л е н и е. Система порождающих элементов для инвариантного класса Q называется неприводимой, если

- 1) каждые два различных порождающих элемента не подобны,
- 2) к ней невозможно присоединить ни одного порождающего элемента, отличного от взятых так, чтобы сохранилось свойство (1) (т. е. система максимальна).

Поскольку отношение подобия разбивает множество всех порождающих элементов для Q на классы эквивалентности, то для построения неприводимой системы достаточно из каждого класса эквивалентности выбрать по одному элементу.

Рассмотрим вопрос о построении неприводимых систем для ряда инвариантных классов.

1. Класс L . Поскольку из всякой нелинейной функции при помощи операций (1), (2) и (3) можно построить [1] нелинейную функцию от двух

переменных и любая функция от одного переменного является линейной, то порождающими элементами для класса L будут с точностью до подобия лишь функции вида

$$x_1x_2 + Ax_1 + Bx_2 + C \pmod{2}.$$

Мы получаем следующую неприводимую систему

$$\{g_1 = x_1x_2, g_2 = \bar{x}_1x_2, g_3 = \bar{x}_1\bar{x}_2, g_4 = x_1 \vee x_2, g_5 = \bar{x}_1 \vee x_2, g_6 = \bar{x}_1 \vee \bar{x}_2\}.$$

2. Класс M . Из предыдущего примера видно, что неприводимая система содержит одну функцию $g_1 = \bar{x}_1$.

3. Класс S . В этом случае процесс построения неприводимой системы оказывается более сложным. Приведем лишь бесконечную систему попарно не подобных порождающих элементов⁹. Таковой является система

$$\{g_n(x_1, \dots, x_n) = x_1x_2 \dots x_n \vee \bar{x}_2 \dots \bar{x}_n \ (n = 2, 3, \dots)\}.$$

Очевидно, $g_n \in S$, а при подстановке констант получаются функции

$$\begin{aligned} & x_2 \dots x_n \vee \bar{x}_2 \dots \bar{x}_n, & \bar{x}_2 \dots \bar{x}_n, \\ & x_1x_2 \dots x_{i-1}x_{i+1} \dots x_n, & \bar{x}_2 \dots \bar{x}_{i-1}\bar{x}_{i+1}\bar{x}_n \quad (i = 2, \dots, n), \end{aligned}$$

являющиеся симметрическими.

4. Класс P^N . Нетрудно видеть, что неприводимая система порождающих элементов для P^N содержится в множестве функций, существенно зависящих от $N + 1$ переменных.

Определение. Пусть $g(x_1, \dots, x_n) \in P_2$. Множество Π_g всех функций $h(y_1, \dots, y_m)$, каждую из которых путем подстановки констант и переименований переменных можно перевести в функцию g , называется пучком, порожденным функцией g .

З а м е ч а н и я.

1. Если g — порождающий элемент для инвариантного класса Q , то $\Pi_g \subseteq CQ$ (CQ означает дополнение Q до P_2).

2. Если g_1 и g_2 подобные функции, то $\Pi_{g_1} = \Pi_{g_2}$.

3. Если g_1 и g_2 не подобные порождающие элементы для инвариантного класса Q , то $g_1 \notin \Pi_{g_2}$ и $g_2 \notin \Pi_{g_1}$, т. е. пучки не вложены друг в друга.

Опираясь на эти понятия и их свойства, докажем ряд утверждений, выясняющих строение инвариантных классов.

Теорема 16. Пусть Q — произвольный инвариантный класс и $G = \{g_i\}$ — неприводимая система порождающих элементов для Q . Тогда¹⁰

$$Q = C \bigcup_i \Pi_{g_i}.$$

⁹В работе автора [31] при разборе класса S допущена ошибка.

¹⁰При $Q = P_2$ множество $\bigcup \Pi_{g_i}$ — пусто и утверждение верно.

Доказательство. Пусть $h \in Q$. Тогда $h \in \Pi_{g_i}$ ($i = 1, \dots$) и, значит, $h \in \bigcup_i \Pi_{g_i}$, т. е. $h \in C \bigcup_i \Pi_{g_i}$.

Пусть теперь $h \notin Q$. Покажем, что $h \in C \bigcup_i \Pi_{g_i}$ или $h \in \bigcup_i \Pi_{g_i}$. Как установлено выше, из $h \notin Q$ путем операции подстановки констант можно перейти к порождающему элементу g_i для Q , т. е. $h \xrightarrow{\text{п.к.}} g_i$ и, значит, $h \in \Pi_{g_i}$.

Теорема доказана.

Данная теорема позволяет выразить известные инвариантные классы через пучки, соответствующие построенным выше неприводимым системам порождающих элементов. Например,

$$L = C(\Pi_{x_1 x_2} \cup \Pi_{\bar{x}_1 x_2} \cup \Pi_{\bar{x}_1 \bar{x}_2} \cup \Pi_{x_1 \vee x_2} \cup \Pi_{\bar{x}_1 \cup x_2} \vee \Pi_{\bar{x}_1 \vee \bar{x}_2}),$$

$$M = C \Pi_{\bar{x}_i}.$$

Очевидно, что имеет место предложение в некотором смысле обратное к предыдущему.

Теорема 17. Пусть $G = \{g_i\}$ — произвольное подмножество функций алгебры логики. Тогда класс $Q = C \bigcup_i \Pi_{g_i}$ является инвариантным и некоторая его неприводимая система порождающих элементов содержится в G .

Данная теорема позволяет строить неограниченное число примеров инвариантных классов. Ответ на этот вопрос дает следующая теорема.

Теорема 18. Мощность множества всех инвариантных классов равна $\aleph$.

Доказательство. В силу того, что каждый инвариантный класс Q может быть задан в виде $C \bigcup_i \Pi_{g_i}$, то мощность множества всех инвариантных классов не превосходит мощности множества всех подмножеств $\{g_i\}$, т. е. $\aleph$.

С другой стороны, покажем, что эта мощность не менее $\aleph$. Для этого построим континуальное семейство попарно различных инвариантных классов.

Положим

$$f_i = x_1 \dots x_{i+1} \vee \bar{x}_1 \dots \bar{x}_{i+1} \quad (i \geq 1).$$

Легко видеть, что $f_i \notin \Pi_{f_j}$ при $i \neq j$ и, значит, они не получаются друг из друга при помощи операций (1), (2) и (3).

Введем обозначения: $\mathcal{E}_\alpha = \{f_{i_1}, f_{i_2}, \dots\}$ и $\mathcal{E}_\beta = \{f_{j_1}, f_{j_2}, \dots\}$. Очевидно, что классы Q^α и Q^β , получающиеся из $\mathcal{E}_\alpha$ и $\mathcal{E}_\beta$ путем их замыканий относительно операций (1), (2) и (3), будут различными инвариантными классами при $\mathcal{E}_\alpha \neq \mathcal{E}_\beta$. Таким образом, построенное семейство инвариантных классов Q^α континуально.

Теорема доказана.

§ 3. Метрические свойства инвариантных классов

Теперь перейдем к изучению метрических свойств инвариантных классов.

Обозначим через $P_Q(n)$ число функций из класса Q , зависящих от переменных $x_1, \dots, x_n$.

Теорема 19. Для каждого непустого инвариантного класса Q последовательность $\{ \sqrt[n]{P_Q(n)} \}$ сходится и

$$1 \leq \lim_{n \rightarrow \infty} \sqrt[n]{P_Q(n)} \leq 2.$$

Доказательство. Пусть $f(x_1, \dots, x_n) \in Q$. Рассмотрим разложение по переменному x_{n+1}

$$f(x_1, \dots, x_n, x_{n+1}) = x_{n+1} f(x_1, \dots, x_n, 1) \vee \bar{x}_{n+1} f(x_1, \dots, x_n, 0).$$

Очевидно, компоненты $f(x_1, \dots, x_n, 1)$, $f(x_1, \dots, x_n, 0)$ принадлежат также Q . Поэтому

$$P_Q(n+1) \leq P_Q^2(n)$$

или

$$\sqrt[n+1]{P_Q(n+1)} \leq \sqrt[n]{P_Q(n)}.$$

Таким образом,

$$\sqrt[2]{P_Q(1)} \geq \dots \geq \sqrt[n]{P_Q(n)} \geq \sqrt[n+1]{P_Q(n+1)} \geq \dots$$

и

$$1 \leq \sqrt[n]{P_Q(n)} \leq \sqrt[n]{2^{2^n}} = 2.$$

Следовательно, последовательность $\{ \sqrt[n]{P_Q(n)} \}$ не возрастает и ограничена снизу. Значит, она сходится к пределу $\lim_{n \rightarrow \infty} \sqrt[n]{P_Q(n)}$, заключенному в сегменте $[1, 2]$.

Теорема доказана.

Замечание. Из доказательства вытекает, что если $Q \neq P_2$, то $\lim_{n \rightarrow \infty} \sqrt[n]{P_Q(n)} < 2$. В самом деле, найдется $g(x_1, \dots, x_m) \in Q$ и потому

$$\lim_{n \rightarrow \infty} \sqrt[n]{P_Q(n)} \leq \sqrt[m]{P_Q(m)} < 2.$$

Для непустого инвариантного класса Q обозначим

$$\log_2 \lim_{n \rightarrow \infty} \sqrt[n]{P_Q(n)} = \sigma.$$

Очевидно, $0 \leq \sigma \leq 1$. Класс Q с параметром σ будем называть классом характеристики σ и писать $Q = Q_\sigma$.

Приведем подсчет σ для некоторых инвариантных классов.

1. Класс P_2 . $P_Q(n) = 2^{2^n}$ и $\sqrt[2^n]{P_Q(n)} = 2$, поэтому $\sigma = 1$.

2. Класс L . $P_Q(n) = 2^{n+1}$ и

$$\lim_{n \rightarrow \infty} \sqrt[2^n]{P_Q(n)} = \lim_{n \rightarrow \infty} \sqrt[2^n]{2^{n+1}} = 1, \quad \sigma = 0.$$

3. Класс Q^α . $P_Q(n) \leq 2^n - n + 1 + 2 \cdot 2^n \leq 3 \cdot 2^n$ и

$$1 \leq \lim_{n \rightarrow \infty} \sqrt[2^n]{P_Q(n)} \leq \lim_{n \rightarrow \infty} \sqrt[2^n]{3 \cdot 2^n} = 1, \quad \sigma = 0.$$

4. Класс $Q_{\frac{1}{2}}$ определяется как множество всех функций $f(x_1, \dots, x_n)$, представимых в виде

$$f(x_1, \dots, x_n) = f'(x_1, \dots, x_n) \& f''(x_1, \dots, x_n),$$

где f' — линейная функция, имеющая существенными переменными $x_{i_1}, \dots, x_{i_r}$, где $1 \leq i_1 < \dots < i_r \leq n$, т. е. $f' = x_{i_1} + \dots + x_{i_r} + c$, а функция f'' содержит все свои существенные переменные в множестве $\{x_{i_1}, \dots, x_{i_r}\}$.

Если зафиксировать функцию $f' = x_{i_1} + \dots + x_{i_r} + c$, то функция f полностью определяется значениями функции f'' на наборах $(\alpha_{i_1}, \dots, \alpha_{i_r})$ таких, что $\alpha_{i_1} + \dots + \alpha_{i_r} + c = 1 \pmod{2}$, и поэтому имеем ровно $2^{2^{r-1}}$ функций.

Нижняя оценка для $P_{Q_{\frac{1}{2}}}(n)$ получается, если зафиксировать f' , положив $f' = x_1 + \dots + x_n$ ($r = n$). Тогда $P_{Q_{\frac{1}{2}}}(n) \geq 2^{2^{n-1}}$.

Для установления верхней оценки заметим, что число функций f' равно 2^{n+1} и $2^{2^{r-1}} \leq 2^{2^{n-1}}$, поэтому

$$P_{Q_{\frac{1}{2}}}(n) \leq 2^{n+1} \cdot 2^{2^{n-1}}.$$

Следовательно,

$$\sqrt{2} \leq \lim_{n \rightarrow \infty} \sqrt[2^n]{P_{Q_{\frac{1}{2}}}(n)} \leq \sqrt{2} \lim_{n \rightarrow \infty} \sqrt[2^n]{2^{n+1}} = \sqrt{2}, \quad \text{т. е. } \sigma = \frac{1}{2}.$$

Примеры показывают, что инвариантные классы могут иметь характеристику 0, 1 и промежуточную характеристику $\frac{1}{2}$. Более подробные рассмотрения показывают [31], что для любого σ ($0 \leq \sigma \leq 1$) существует континуум попарно различных инвариантных классов характеристики σ . В то же время, как вытекает из замечания к теореме 19, существует только один инвариантный класс характеристики 1, а именно P_2 .

§ 4. Синтез схем для инвариантных классов

Теорема 20 (обобщение метода Шеннона). Если Q — инвариантный класс характеристики σ ($\sigma \neq 0$), то существует метод синтеза A' такой, что для каждой булевой функции f из Q он дает контактную схему Σ_f такую, что

$$L_{A'}(\Sigma_f) \lesssim 4\sigma \frac{2^n}{n}.$$

Доказательство. Берем для функции разложение

$$f(x_1, \dots, x_n) = \bigvee_{(\sigma_1, \dots, \sigma_{n-m})} x_1^{\sigma_1} \& \dots \& x_{n-m}^{\sigma_{n-m}} f(\sigma_1, \dots, \sigma_{n-m}, x_{n-m+1}, \dots, x_n).$$

Так как $f \in Q$, то для компонент разложения имеем

$$f(\sigma_1, \dots, \sigma_{n-m}, x_{n-m+1}, \dots, x_n) \in Q.$$

Возьмем контактное дерево $\mathcal{D}_{n-m}$ по переменным $x_1, \dots, x_{n-m}$ и универсальный многополюсник U_Q^m с $P_Q(m)$ входами и одним выходом для всех функций из Q , зависящих от m переменных $x_{n-m+1}, \dots, x_n$, и для каждого $\sigma_1, \dots, \sigma_{n-m}$ выход дерева $x_1^{\sigma_1} \& \dots \& x_{n-m}^{\sigma_{n-m}}$ соединим со входом $f(\sigma_1, \dots, \sigma_{n-m}, x_{n-m+1}, \dots, x_n)$ многополюсника U_Q^m (рис. 47).

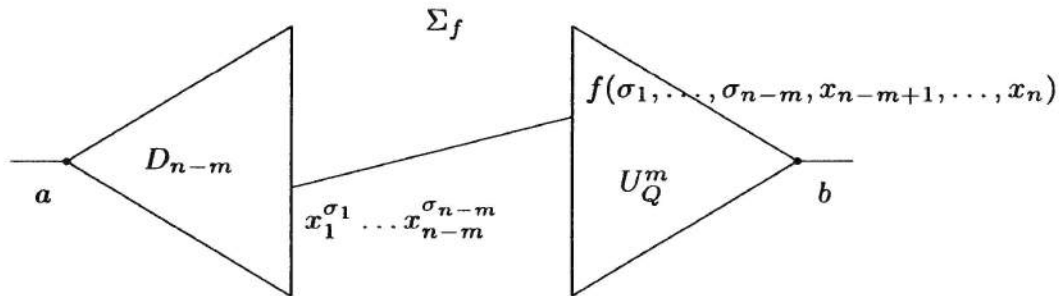


Рис. 47

В силу леммы 2 (Шеннона)

$$\langle a, b \rangle = f(x_1, \dots, x_n),$$

т. е. двухполюсник Σ_f реализует функцию f . Из леммы 1, учитывая также оценку для $L(\mathcal{D}_{n-m})$, имеем

$$L_Q(\Sigma_f) = L(\mathcal{D}_{n-m}) + L(U_Q^m) \leq 2 \cdot 2^{n-m} + 2P_Q(m).$$

Возьмем произвольное $\varepsilon > 0$ и пусть $\sqrt[m]{P_Q(m)} \leq 2^{\sigma+\varepsilon}$ при $m \geq m_0$. Пусть, далее, $m = \left\lceil \log \left(\frac{n-2 \log n}{\sigma+\varepsilon} \right) \right\rceil$. Мы имеем

$$\log \left(\frac{n-2 \log n}{\sigma+\varepsilon} \right) - 1 < m \leq \log \frac{n-2 \log n}{\sigma+\varepsilon}$$

и, следовательно,

$$\frac{n - 2 \log n}{2(\sigma + \varepsilon)} < 2^m \leq \frac{n - 2 \log n}{\sigma + \varepsilon}.$$

Отсюда

$$L_Q(\Sigma_f) \leq \frac{2 \cdot 2^n}{\left(\frac{n-2 \log n}{2(\sigma+\varepsilon)}\right)} + 2 \cdot 2^{(\sigma+\varepsilon) \frac{n-2 \log n}{\sigma+\varepsilon}} \lesssim 4(\sigma+\varepsilon) \frac{2^n}{n} + \frac{2 \cdot 2^n}{n^2} \lesssim 4(\sigma+\varepsilon) \frac{2^n}{n}.$$

Данное неравенство верно при любом ε , значит,

$$L_Q(\Sigma_f) \lesssim 4\sigma \frac{2^n}{n}.$$

Теорема доказана.

С л е д с т в и е.

1. $\frac{L_{Q_\sigma}(n)}{L(n)} \lesssim 4\sigma$ при любом σ , значит,

$$\lim_{n \rightarrow \infty} \frac{L_{Q_0}(n)}{L(n)} = 0.$$

2. При $\sigma < \frac{1}{4}$ получим $\frac{L_{Q_\sigma}(n)}{L(n)} \lesssim 1$, значит, функции из инвариантного класса Q_σ реализуются проще, чем в общем случае.

Так как $\log P_Q(n) \sim \sigma 2^n$, то нижняя оценка (см. теорему 10 и ее применение для класса контактных схем) для инвариантного класса Q_σ имеет вид $L_{Q_\sigma}(n) \gtrsim \sigma \frac{2^n}{n}$.

РАЗДЕЛ 3. ПРОБЛЕМА НИЖНИХ ОЦЕНОК СЛОЖНОСТИ УПРАВЛЯЮЩИХ СИСТЕМ

Всякий раз, когда для функции $f \in \mathfrak{F}$ мы находим схему Σ , реализующую f , мы получаем верхнюю оценку для $L(f)$, ибо

$$L(f) \leq L(\Sigma).$$

Чтобы судить о том, насколько найденное решение Σ близко к оптимуму, надо либо знать $L(f)$, либо иметь хорошую нижнюю оценку для $L(f)$.

Аналогичная ситуация возникает, если речь идет о задаче синтеза схем для класса функций $Q_n \subseteq \mathfrak{F}_n$. Здесь каждый метод синтеза дает верхнюю оценку для $L_{Q_n}(n)$ и для понимания качества этой оценки необходимо иметь хорошую нижнюю оценку для $L_{Q_n}(n)$.

Таким образом, возникает проблема нижних оценок сложности У.С.

Здесь можно выделить следующие основные направления.

1. Разработка нижних мощностных оценок, т. е. оценок, зависящих главным образом от $P(n)$ — числа функциональных объектов из $\mathfrak{F}_n$ и в слабой степени от базиса.

Данным вопросом мы много занимались, когда изучали универсальные методы синтеза схем для важнейших классов У.С. Мы установили, что

$$L(n) \gtrsim \rho \frac{\log P(n)}{\log \log P(n)}$$

для указанных классов и для почти всех функций из $\mathfrak{F}_n$ сложность минимальной схемы, т. е. $L(f)$, асимптотически не менее величины

$$\rho \frac{\log P(n)}{\log \log P(n)}.$$

Для многих классов функций эта оценка оказывается асимптотически неулучшаемой. Однако здесь не удалось найти ни одной конкретной функции (просто определяемой) со сложностью минимальной схемы, близкой к величине $L(n)$.

2. Нахождение нижних оценок для реализации функции от малого числа переменных.

Это направление связано с построением каталогов минимальных схем для функций, зависящих от малого числа переменных. Такие каталоги создавались во Франции, Японии и СССР [2, 5, 6, 37, 41] для реализации булевых функций $f(x_1, \dots, x_n)$ с $n = 1, 2, 3, 4$ в классе контактных схем и схем из функциональных элементов.

3. Получение нижних оценок для конкретных последовательностей функций и нижних оценок для узких классов функций.

Это направление мы проиллюстрируем двумя задачами: получение нижних нетривиальных линейных оценок и получение нижних квадратичных оценок в классе контактных π -схем.

§ 1. Линейные нижние оценки для реализации булевых функций контактными схемами

Мы начнем с некоторых тривиальных соображений.

1. Если $f(x_1, \dots, x_n)$ существенно зависит от x_i , то любая контактная схема, реализующая f , содержит хотя бы один из контактов $x_i, \bar{x}_i$. В силу этого, если все переменные функции f существенные, то

$$L(f) \geq n.$$

2. Говорят, что $f(x_1, \dots, x_i, \dots, x_n)$ возрастает (соответственно, убывает) по переменному x_i , если для любых значений $\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_n$ выполнено неравенство

$$f(\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n) \leq f(\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n)$$

(или, соответственно,

$$f(\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n) \geq f(\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n)).$$

В случае, если f возрастает по x_i (убывает по x_i), то существует реализация, не содержащая контактов $\bar{x}_i$ (контактов x_i).

Справедливо и обратное утверждение. Например, если схема Σ реализует f и не содержит контактов $\bar{x}_i$, то

$$f(\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n) \leq f(\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n),$$

т. е. функция возрастает. Аналогично рассматривается и случай, когда Σ не содержит контактов x_i .

Отсюда следует, что если f не возрастает и не убывает по x_i , то любая ее реализация содержит и контакты x_i , и контакты $\bar{x}_i$. В частности, если f не возрастает и не убывает по каждому своему переменному, то

$$L(f) \geq 2n.$$

Пример. Функция $l_n^0(x_1, \dots, x_n) = x_1 + \dots + x_n$ не возрастает и не убывает по каждому переменному при $n \geq 2$. Поэтому

$$L(l_n^0) \geq 2n \quad (n \geq 2).$$

Из вышесказанного вытекает, что схемы Σ_1^σ и Σ_2^σ (рис. 48) являются минимальными для $l_1^\sigma(x_1)$ и $l_2^\sigma(x_1, x_2) = x_1 + x_2 + \sigma$, так как $L(l_1^\sigma) \geq 1$ и $L(l_2^\sigma) \geq 4$.

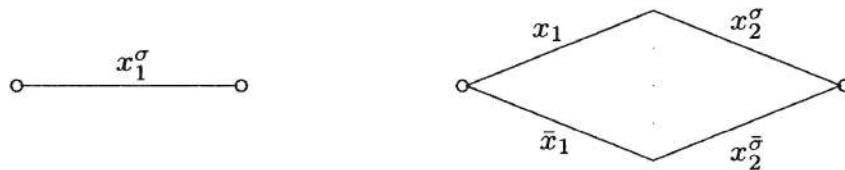


Рис. 48

Теорема 21 (Кардо [37]). Для линейной функции $l_n^\sigma(x_1, \dots, x_n)$ при $n \geq 2$

$$L(l_n^\sigma) \geq 4n - 4.$$

Доказательство.¹¹ Очевидно, можно предполагать, что $n \geq 3$.

Возьмем функцию $l'_n(x_1, \dots, x_n) = x_1 + \dots + x_n + 1$. Она, в частности, равна 1 на всех наборах, содержащих ровно две единицы.

Пусть Σ'_n — произвольная контактная схема, реализующая l'_n . Рассмотрим в ней множество всех ненулевых цепей $\{\Pi_\nu\}$ ¹² таких, что Π_ν для двух значений i и j ($i \leq j$, $j \leq n$, $i \neq j$) содержит только контакты x_i и x_j , а для остальных значений k ($k \neq i$, $k \neq j$, $1 \leq k \leq n$) — исключительно контакты $\bar{x}_k$. Двигаясь от полюса 1 к полюсу 2 по цепи Π_ν , первый (замыкающий) контакт пометим числом 1, а последний — 2 (рис. 49).

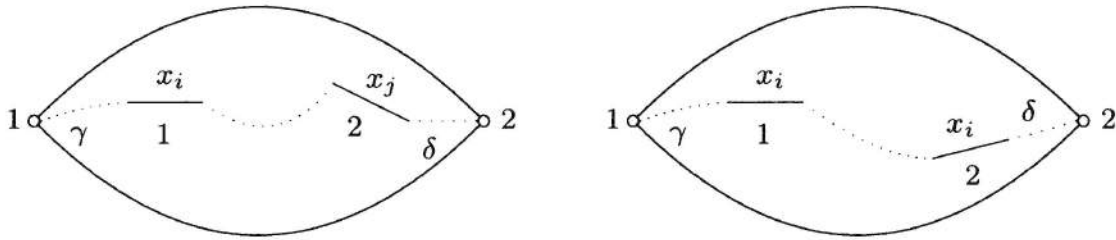


Рис. 49

На рис. 49 представлены обе возможности:

- 1) помеченные контакты разных сортов;
- 2) помеченные контакты одного сорта.

Очевидно также, что начальный участок γ и конечный участок δ состоят только из размыкающих контактов.

Сначала покажем, что если контакт x_i — общий для двух цепей Π_ν и Π_μ ($\nu \neq \mu$), то он не может иметь пометку 1 для цепи Π_ν и пометку 2 для цепи Π_μ (рис. 50).

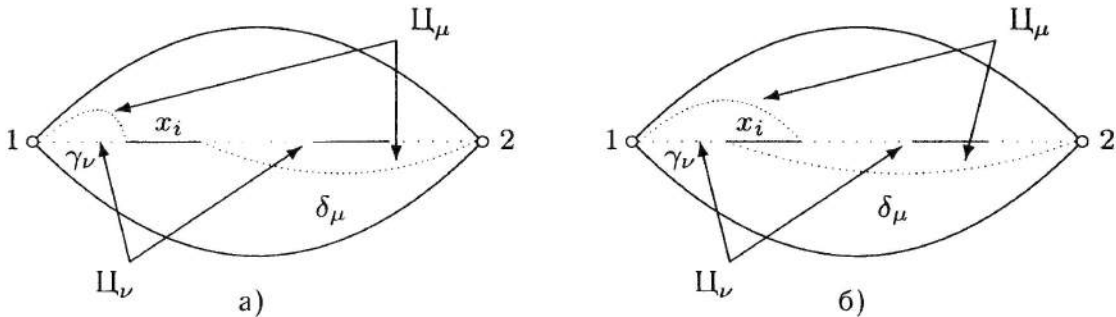


Рис. 50

Как видно из чертежей, возможны две конфигурации:

а) в этом случае $\gamma_\nu - x_i - \delta_\mu$ будет ненулевой цепью; тогда на наборе $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ с $\alpha_i = 1$, $\alpha_t = 0$ ($t \neq i$) эта цепь проводит, а $l'_n(\tilde{\alpha}) = 0$.

б) в этом случае $\gamma_\nu - \delta_\mu$ будет ненулевой цепью, не содержащей контактов $x_i, \bar{x}_i$; поэтому на наборе $\tilde{\alpha}$ эта цепь проводит, а $l'_n(\tilde{\alpha}) = 0$.

¹¹ Этот вариант доказательства найден С. А. Ложкиным [11]

¹² Очевидно, в схеме Σ'_n каждая ненулевая цепь содержит контакты для каждого x_i .

В обоих случаях имеем противоречие. Таким образом, нумерация (пометка) некоторых замыкающих контактов не зависит от выбора цепей.

Пусть $\mathfrak{M}_1$ и $\mathfrak{M}_2$ — множества всех контактов, помеченных соответственно числами 1 и 2. Докажем, что каждое из этих множеств содержит замыкающие контакты для всех переменных, кроме, быть может, одного.

Пусть $\mathfrak{M}_1$ не содержит контактов x_i и x_j ($i \neq j$). Рассмотрим ненулевую цепь $\mathcal{C}_\nu$, которая содержит из замыкающих контактов только контакты x_i и x_j (такая цепь существует, так как $l'_n(\tilde{\alpha}) = 1$, где набор $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ имеет только две единичные компоненты $\alpha_i = \alpha_j = 1$, остальные равны нулю). В цепи $\mathcal{C}_\nu$ один из контактов типа x_i или x_j встретится первым — он и будет помечен цифрой 1. Тогда он войдет в $\mathfrak{M}_1$. Мы получим противоречие. Аналогично разбирается и второе утверждение.

Определение. Контакт x_i^σ называется особым в Σ_n , если схема Σ_n содержит ровно один контакт типа x_i^σ .

Пример. На рис. 51 представлены схемы Σ'_3 и Σ''_3 , реализующие l'_3 с четырьмя и тремя особыми контактами.

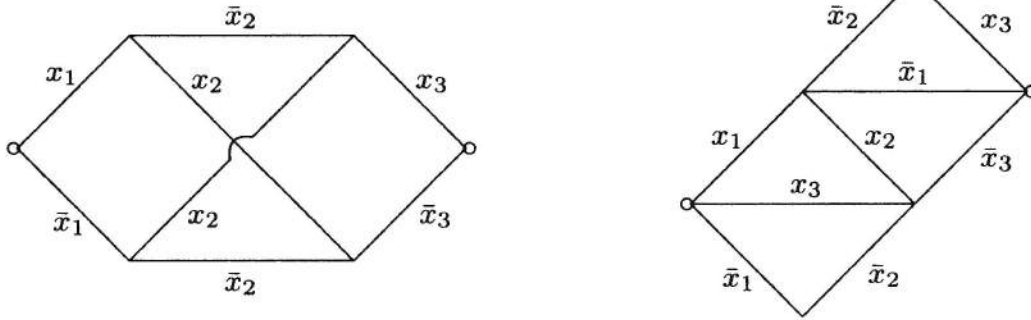


Рис. 51

Замечание. Схема Σ'_n не может содержать более двух особых замыкающих контактов. В самом деле, если это не так, то в ней найдутся три особых попарно различных контакта x_i, x_j, x_k ($i \neq j, i \neq k, j \neq k$). Тогда в множестве рассматриваемых цепей они обязательно получают пометки и, очевидно, два из них получают одну и ту же пометку σ . Эти контакты войдут в множество $\mathfrak{M}_\sigma$ и не будут принадлежать второму множеству, что противоречит предыдущему утверждению.

Обозначим через s число особых контактов в Σ'_n . Покажем, что $s \leq 4$. Допустим $s \geq 5$. Особые контакты в этом случае принадлежат не менее, чем трем переменным. Достаточно рассмотреть два случая.

1. Существует четыре особых контакта, принадлежащих четырем переменным. Например, $x_1^{\sigma_1}, x_2^{\sigma_2}, x_3^{\sigma_3}, x_4^{\sigma_4}$. Так как

$$l'_n(x_1 + \sigma_1, x_2 + \sigma_2, x_3 + \sigma_3, x_4 + \sigma_1 + \sigma_2 + \sigma_3, \dots) = l'_n(x_1, x_2, x_3, x_4, \dots),$$

то схема $\tilde{\Sigma}'_n$, полученная из Σ'_n заменой переменных

$$\begin{aligned} x_1 &\rightarrow x_1 + \sigma_1, & x_2 &\rightarrow x_2 + \sigma_2, & x_3 &\rightarrow x_3 + \sigma_3, \\ x_4 &\rightarrow x_4 + \sigma_1 + \sigma_2 + \sigma_3, & x_i &\rightarrow x_i \quad (i \geq 5), \end{aligned}$$

будет реализовывать функцию l'_n , содержать то же число контактов и иметь особые контакты x_1, x_2, x_3 , что противоречит вышесказанному.

2. Все особые контакты принадлежат трем переменным. Этот случай сводится к ситуации, когда особыми контактами будут

$$x_1, \bar{x}_1, x_2, \bar{x}_2, x_3^{\sigma_3}.$$

Здесь $l'_n(x_1 + \sigma_3, x_2, x_3 + \sigma_3, \dots) = l'_n(x_1, x_2, x_3, \dots)$ и схема $\tilde{\Sigma}'_n$, получаемая из Σ_n заменой переменных

$$x_1 \rightarrow x_1 + \sigma_3, \quad x_2 \rightarrow x_2, \quad x_3 \rightarrow x_3 + \sigma_3, \quad x_i \rightarrow x_i \quad (i \geq 4),$$

будет реализовывать l'_n , иметь ту же сложность, что и Σ'_n и иметь особыми контактами x_1, x_2, x_3 . Пришли по тем же причинам к противоречию.

Теперь оценим сложность схемы Σ'_n :

$$L(\Sigma'_n) \geq 2(2n - s) + s = 4n - s \geq 4n - 4.$$

Теорема доказана.

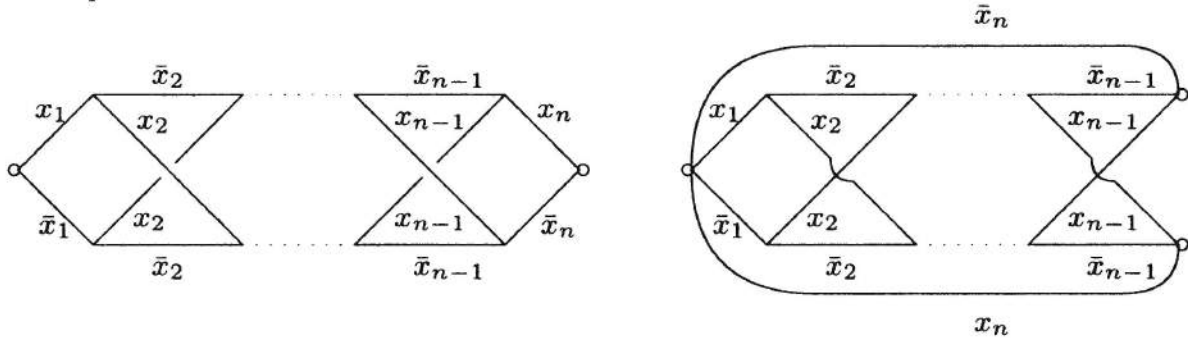


Рис. 52

Поскольку для l'_n существует реализация сложности $4n - 4$, то она является минимальной. На рис. 52 представлены две минимальные схемы для l'_n .

§ 2. Квадратичные нижние оценки для контактных π -схем

Некоторые вспомогательные факты.

Как известно из теории двухполюсных сетей, в случае, если сеть связна, то между ее полюсами имеются пути и их бесконечно много. Поэтому рассматривают специальные пути, называемые цепями. Оказывается, что число цепей, соединяющих полюса, конечно. Наряду с понятием пути естественно рассматривать двойственное понятие — понятие сечения.

О п р е д е л е н и е. Множество ребер двухполюсной связной сети называется сечением, если при выбрасывании этих ребер получающаяся сеть не будет связной и ее полюса попадают в разные компоненты связности.

Из определения вытекает, что сечение имеет с каждым путем по крайней мере одно общее ребро.

Очевидно, что множество всех ребер двухполюсной сети образует сечение. Однако, легко видеть, что это сечение может быть сильно избыточным. Поэтому естественно ввести специальный тип сечений, так называемые тупиковые сечения.

Определение. Сечение $\tilde{C}$ данной связной двухполюсной сети называется тупиковым, если всякое его собственное подмножество ребер $\tilde{C}'$ ($\tilde{C}' \subset \tilde{C}$) не будет сечением.

Пример. На рис. 53 изображена двухполюсная связная сеть, ребра которой для удобства занумерованы.

Рассмотрим следующие множества ребер:

$$\tilde{C}_1 = \{1, 2, 7\}, \quad \tilde{C}_2 = \{1, 2, 4, 5, 7\}, \quad \tilde{C}_3 = \{1, 5, 7\}.$$

Очевидно, что $\tilde{C}_2$ и $\tilde{C}_3$ будут сечениями, а $\tilde{C}_1$ сечением не является. В то же время сечение $\tilde{C}_2$ не является тупиковым сечением, так как $\tilde{C}_2 \supset \tilde{C}_3$, а $\tilde{C}_3$ является тупиковым сечением.

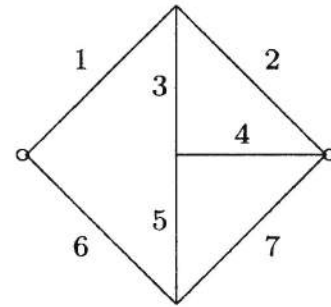


Рис. 53

Лемма 11. В каждой π -сети Γ любая цепь $\tilde{C}$ и тупиковое сечение $\tilde{C}$ имеют общими ровно одно ребро.

Доказательство. По индукции.

Базис индукции. Простейшая π -сеть есть ребро и она содержит единственную цепь и единственное тупиковое сечение, совпадающее с этим ребром. Поэтому утверждение леммы справедливо.

Индуктивный переход. Сеть Γ является либо последовательным соединением, либо параллельным соединением сетей Γ_1 и Γ_2 , для которых утверждение леммы справедливо (рис. 54).

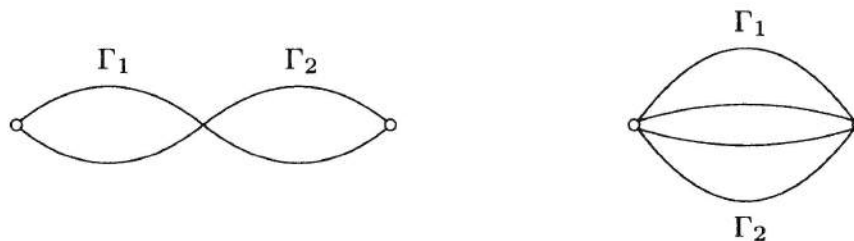


Рис. 54

Возьмем в Γ произвольную цепь $\tilde{C}$ и тупиковое сечение $\tilde{C}$ и рассмотрим случай, когда Γ — последовательное соединение Γ_1 и Γ_2 . Тогда цепь $\tilde{C}$ разбивается вершиной, в которой соединяются сети Γ_1 и Γ_2 , на две части $\tilde{C}_1$ и $\tilde{C}_2$, являющиеся цепями сетей Γ_1 и Γ_2 соответственно. Тупиковое сечение $\tilde{C}$ будет сечением (и притом тупиковым) одной из сетей (и потому не будет иметь ребер из другой сети). Пусть, например, сети Γ_1 . По предположению индукции $\tilde{C}_1$ и $\tilde{C}$ имеют общими ровно одно ребро.

Второй случай разбирается аналогичным образом: здесь цепь $\tilde{C}$ будет лежать целиком в одной из сетей Γ_1, Γ_2 , а тупиковое сечение $\tilde{C}$ разбивается на две части $\tilde{C}_1$ и $\tilde{C}_2$, которые будут сечениями (и притом тупиковыми) для сетей Γ_1 и Γ_2 соответственно.

Лемма доказана.

Следующий пример (рис. 55) показывает, что в классе всех связных двухполюсных сетей лемма 11 уже не верна. В самом деле, приведенная в данном примере сеть имеет совпадающую цепь $\tilde{C} = (1, 3, 5)$ и тупиковое сечение $\tilde{C} = (1, 3, 5)$.

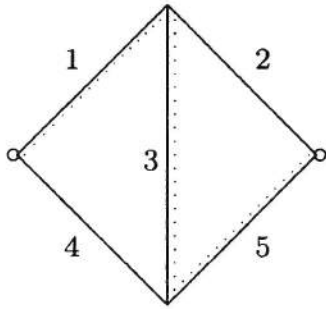


Рис. 55

Пусть Σ — двухполюсная контактная π -схема, а Γ — соответствующая ей π -сеть. Каждой цепи $\tilde{C}$ и тупиковому сечению $\tilde{C}$ сети Γ естественным образом соответствуют цепь C и тупиковое сечение C схемы Σ , которые определяются некоторым множеством контактов. Пусть

$$C = \{x_{i_1}^{\sigma_1}, \dots, x_{i_m}^{\sigma_m}\}, \quad C = \{x_{j_1}^{\tau_1}, \dots, x_{j_p}^{\tau_p}\}.$$

Определение. Цепь $C = \{x_{i_1}^{\sigma_1}, \dots, x_{i_m}^{\sigma_m}\}$ называется нулевой, если существует переменное x_i такое, что в цепи C одновременно встречаются x_i и $\bar{x}_i$. Тупиковое сечение $C = \{x_{j_1}^{\tau_1}, \dots, x_{j_p}^{\tau_p}\}$ называется единичным, если существует переменное x_j такое, что в сечении C одновременно встречаются x_j и $\bar{x}_j$.

Таким образом, множество всех цепей схемы Σ разбивается на две части: множество нулевых цепей и множество, состоящее из ненулевых цепей, а множество всех тупиковых сечений — на множество единичных тупиковых сечений и множество, состоящее из неединичных тупиковых сечений.

Определение. Говорят, что ненулевая цепь $C = \{x_{i_1}^{\sigma_1}, \dots, x_{i_m}^{\sigma_m}\}$ соответствует набору $(\beta_1, \dots, \beta_n)$, а неединичное тупиковое сечение $C = \{x_{j_1}^{\tau_1}, \dots, x_{j_p}^{\tau_p}\}$ — набору $(\alpha_1, \dots, \alpha_n)$, если

$$\beta_{i_1} = \sigma_1, \quad \dots, \quad \beta_{i_m} = \sigma_m,$$

а

$$\alpha_{j_1} = \bar{\tau}_1, \quad \dots, \quad \alpha_{j_p} = \bar{\tau}_p.$$

Очевидно, что в этом случае на наборе $(\beta_1, \dots, \beta_n)$ все константы цепи C будут замкнуты и поэтому

$$f(\beta_1, \dots, \beta_n) = 1,$$

а на наборе $(\alpha_1, \dots, \alpha_n)$ контакты, принадлежащие тупиковому сечению C , будут разомкнуты и поэтому

$$f(\alpha_1, \dots, \alpha_n) = 0.$$

Легко видеть, что каждой ненулевой цепи C (соответственно, неединичному тупиковому сечению C) отвечает хотя бы один набор $(\beta_1, \dots, \beta_n)$ (соответственно, $(\alpha_1, \dots, \alpha_n)$).

Следующая лемма показывает, что верно и обратное.

Лемма 12. Для каждого набора $(\beta_1, \dots, \beta_n)$ и $(\alpha_1, \dots, \alpha_n)$ таких, что

$$f(\beta_1, \dots, \beta_n) = 1 \quad \text{и} \quad f(\alpha_1, \dots, \alpha_n) = 0,$$

существуют цепь $\tilde{C}$ и тупиковое сечение C , которые соответствуют этим наборам.

Доказательство.

1. Рассмотрим в схеме Σ все контакты вида $x_1^{\beta_1}, \dots, x_n^{\beta_n}$. Если $x_1 = \beta_1, \dots, x_n = \beta_n$, то они все будут замкнуты и, так как

$$f(\beta_1, \dots, \beta_n) = 1,$$

то соответствующее подмножество ребер в Γ содержит цепь $\tilde{C}$, которая и определяет искомую цепь C .

2. Рассмотрим в схеме Σ все контакты вида $x_1^{\alpha_1}, \dots, x_n^{\alpha_n}$. Если $x_1 = \alpha_1, \dots, x_n = \alpha_n$, то они все будут разомкнуты. Покажем, что соответствующее им множество ребер из Γ образует сечение Γ . Рассмотрим произвольную цепь $\tilde{C}$ сети Γ . По определению ей соответствует цепь C схемы Σ .

а) Пусть C — ненулевая цепь. Так как $f(\alpha_1, \dots, \alpha_n) = 0$, то $\tilde{C}$ проходит через данное множество.

б) Пусть C — нулевая цепь. В ней встречается пара противоположных контактов, например, x_j и $\bar{x}_j$. Один из них обязательно принадлежит множеству $\{\{x_1^{\alpha_1}\}, \dots, \{x_n^{\alpha_n}\}\}$, поэтому $\tilde{C}$ проходит через это множество.

Для завершения доказательства остается в данном сечении сети Γ выбрать тупиковое сечение $\tilde{C}$. Очевидно, соответствующее тупиковое сечение C схемы Σ и будет искомым.

Лемма доказана.

Лемма 13 (Неравенство Коши–Буняковского). Пусть $a_1, \dots, a_n, b_1, \dots, b_n$ — произвольные действительные числа. Тогда

$$\left(\sum_{j=1}^n a_j b_j \right)^2 \leq \left(\sum_{j=1}^n a_j^2 \right) \left(\sum_{j=1}^n b_j^2 \right).$$

Доказательство. Рассмотрим выражение $\sum_{j=1}^n (a_j - \lambda b_j)^2$. Очевидно, при любом действительном λ

$$\sum_{j=1}^n (a_j - \lambda b_j)^2 \geq 0, \quad \text{т. е.} \quad \sum_{j=1}^n a_j^2 - 2\lambda \sum_{j=1}^n a_j b_j + \lambda^2 \sum_{j=1}^n b_j^2 \geq 0.$$

Это возможно, если дискриминант данного выражения меньше или равен нулю. Отсюда

$$D = \left(\sum_{j=1}^n a_j b_j \right)^2 - \left(\sum_{j=1}^n a_j^2 \right) \left(\sum_{j=1}^n b_j^2 \right) \leq 0.$$

Лемма доказана.

Пусть $f(x_1, \dots, x_n)$ — произвольная булева функция и $f \neq \text{const}$. Пусть, далее, Σ — какая-то контактная π -схема, реализующая f . Для каждого j ($1 \leq j \leq n$) занумеруем в схеме Σ контакты j -го реле числами $1, 2, \dots, m_j$. Очевидно, $\sum_{j=1}^n m_j = L_\pi(\Sigma)$. Введем следующие обозначения:

M^0 — подмножество вершин $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ n -мерного куба таких, что $f(\alpha_1, \dots, \alpha_n) = 0$ и $M^0 \neq \Lambda$;

M^1 — подмножество вершин $\tilde{\beta} = (\beta_1, \dots, \beta_n)$ n -мерного куба таких, что $f(\beta_1, \dots, \beta_n) = 1$ и $M^1 \neq \Lambda$;

R — подмножество ребер $(\tilde{\alpha}, \tilde{\beta})$ n -мерного куба таких, что $\tilde{\alpha} \in M^0$, $\tilde{\beta} \in M^1$ (см. рис. 56).

Т е о р е м а 22 (Храпченко [26]).

$$L_\pi(\Sigma) \geq \frac{|R|^2}{|M^0| \cdot |M^1|}.$$

(Здесь $|F|$ обозначает мощность множества $\mathfrak{F}$.)

Доказательство. Пусть $\tilde{\alpha} \in M^0$. Сопоставим этой вершине тупиковое сечение $C_{\tilde{\alpha}}$, соответствующее набору $\tilde{\alpha}$ (лемма 12).

Пусть $\tilde{\beta} \in M^1$. Сопоставим вершине $\tilde{\beta}$ цепь $\Pi_{\tilde{\beta}}$, соответствующую набору $\tilde{\beta}$ (лемма 12).

Обозначим через a_{ij}^0 число вершин $\tilde{\alpha}$ из M^0 , которым приписаны тупиковые сечения, проходящие через i -ый контакт j -го реле, а через a_{ij}^1 — число вершин $\tilde{\beta}$ из M^1 , которым приписаны цепи, проходящие через i -ый контакт j -го реле.

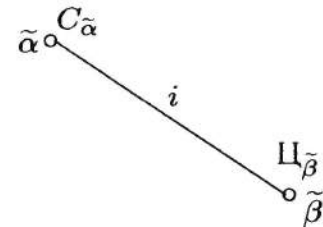


Рис. 56

Если пара $(\tilde{\alpha}, \tilde{\beta})$ такова, что $\alpha \in M^0$ и $\tilde{\beta} \in M^1$, то ей сопоставлена пара $(C_{\tilde{\alpha}}, \Pi_{\tilde{\beta}})$. В силу леммы 11 $C_{\tilde{\alpha}}$ и $\Pi_{\tilde{\beta}}$ имеют общими ровно один контакт. Пусть это будет i -ый контакт j -го реле.

В случае, когда $(\tilde{\alpha}, \tilde{\beta}) \in R$, наборы $\tilde{\alpha}$ и $\tilde{\beta}$ являются соседними и, как это вытекает из доказательства леммы 11, их соседство происходит по j -й компоненте, т. е.

$$\tilde{\alpha} = (\alpha_1, \dots, \alpha_j, \dots, \alpha_n) \quad \text{и} \quad \tilde{\beta} = (\alpha_1, \dots, \bar{\alpha}_j, \dots, \alpha_n).$$

Припишем данному ребру $(\tilde{\alpha}, \tilde{\beta})$ (оно параллельно оси j) номер i (рис. 56).

Очевидно, ребрам из R , имеющим одно и то же направление (параллельное оси j), могут быть приписаны одинаковые числа.

Обозначим через a_{ij} число ребер из R , которым приписан номер i и которые параллельны оси j .

Если ребру $(\tilde{\alpha}, \tilde{\beta})$, параллельному оси j , приписан номер i , то $C_{\tilde{\alpha}}$ и $\Pi_{\tilde{\beta}}$ проходят через i -ый контакт j -го реле. Кроме того, два различных ребра,

которым соответствует i -ый контакт j -го реле, параллельны и, значит, не имеют общих концевых вершин. Отсюда

$$a_{ij}^0, a_{ij}^1 \geq a_{ij}.$$

Теперь произведем подсчет пар $(\tilde{\alpha}, \tilde{\beta})$, где $\tilde{\alpha} \in M^0$, $\tilde{\beta} \in M^1$. С одной стороны, эта величина равна $|M^0| \cdot |M^1|$; с другой стороны, она равна числу пар $(C_{\tilde{\alpha}}, \Pi_{\tilde{\beta}})$.

Каждой паре $(C_{\tilde{\alpha}}, \Pi_{\tilde{\beta}})$ соответствует ровно один контакт схемы Σ , являющийся общим для $C_{\tilde{\alpha}}$ и $\Pi_{\tilde{\beta}}$. Поэтому подсчет пар $(C_{\tilde{\alpha}}, \Pi_{\tilde{\beta}})$ (с учетом кратности) можно осуществлять путем подсчета тех пар $(C_{\tilde{\alpha}}, \Pi_{\tilde{\beta}})$, для которых $C_{\tilde{\alpha}}$ и $\Pi_{\tilde{\beta}}$ имеют общими i -ый контакт j -го реле. Данная величина равна $a_{ij}^0 \cdot a_{ij}^1$, а общее число пар $(C_{\tilde{\alpha}}, \Pi_{\tilde{\beta}})$ равно

$$\sum_{j=1}^n \sum_{i=1}^{m_j} a_{ij}^0 a_{ij}^1.$$

Мы имеем

$$|M^0| \cdot |M^1| = \sum_{j=1}^n \sum_{i=1}^{m_j} a_{ij}^0 a_{ij}^1 \geq \sum_{j=1}^n \sum_{i=1}^{m_j} a_{ij}^2.$$

Используя неравенство Коши–Буняковского, получаем

$$\sum_{j=1}^n \sum_{i=1}^{m_j} a_{ij}^2 L_{\pi}(\Sigma) = \sum_{j=1}^n \sum_{i=1}^{m_j} a_{ij}^2 \sum_{j=1}^n \sum_{i=1}^{m_j} 1^2 \geq \left(\sum_{j=1}^n \sum_{i=1}^{m_j} a_{ij} \right)^2 = |R|^2.$$

Таким образом,

$$L_{\pi}(\Sigma) \geq \frac{|R|^2}{|M^0| \cdot |M^1|}.$$

Теорема доказана.

В качестве следствия получаем теорему о нижней оценке сложности реализации линейной функции $l_n(x) = x_1 + \dots + x_n \pmod{2}$ в классе контактных π -схем. Обозначим через Σ_n минимальную контактную π -схему для l_n .

Т е о р е м а 23 (Храпченко [25]).

$$L_{\pi}(\Sigma_n) \geq n^2.$$

Д о к а з а т е л ь с т в о. Пусть M^0 (соответственно, M^1) — множество всех вершин n -мерного куба, для которых $l_n = 0$ (соответственно, $l_n = 1$). Очевидно, $|M^0| = |M^1| = 2^{n-1}$. Пусть R — множество всех ребер, у которых одна вершина принадлежит M^0 , а другая M^1 . Очевидно,

R содержит все ребра n -мерного куба, и потому $|R| = n \cdot 2^{n-1}$. В силу предыдущей теоремы

$$L_{\pi}(\Sigma_n) \geq \frac{|R|^2}{|M^0| \cdot |M^1|} = \frac{n^2(2^{n-1})^2}{2^{n-1}2^{n-1}} = n^2.$$

Теорема доказана.

З а м е ч а н и е. Как мы видели ранее при $n = 2^m$, верхняя оценка для сложности минимальных схем этого класса имеет вид

$$L_{\pi}(\Sigma_n) \leq n^2.$$

Отсюда, построенные схемы для l_n при $n = 2^m$ являются минимальными.

Ч А С Т Ь II. ЭКВИВАЛЕНТНЫЕ ПРЕОБРАЗОВАНИЯ УПРАВЛЯЮЩИХ СИСТЕМ

ВВЕДЕНИЕ

При проектировании схем дискретных преобразователей часто используют следующий подход: на основе предыдущего опыта и различных теоретических соображений разрабатывается первоначальный вариант схемы, который дает схему с требуемым функционированием, но может быть далеким от оптимального варианта. Затем осуществляется этап усовершенствования схемы, элементарный шаг которого состоит в замене фрагментов схемы (подсхемы) на более простой фрагмент с таким же функционированием. В результате получают схему с тем же функционированием, но более простого вида. Эти усовершенствования продолжают до тех пор, пока это практически возможно. На этом процесс заканчивают и получают окончательный вариант схемы. Разумеется, данный эвристический подход не гарантирует оптимального результата, но может дать определенный эффект. Приведенное рассуждение является исходным пунктом в проблеме эквивалентных преобразований алгоритмов и управляющих систем [1, 9, 10, 17, 18].

Рассматривается класс управляющих систем $\mathcal{U} = \{U\}$, каждая из которых характеризуется парой (Σ, Φ) .

Предполагается, что этот класс удовлетворяет требованию регулярности, т. е.

$$\Phi = \varphi(\Sigma),$$

что всегда имеет место для так называемых алгоритмизированных У.С.

Пусть $f = \psi(\Phi)$ — функциональная характеристика U , выражающая определенную сторону функционирования У.С.

Например, если $\mathcal{U}$ — класс автоматов, то Φ — его канонические уравнения, а f — о.-д. функция, определяемая этими уравнениями.

В нашем случае f однозначно определяется схемой Σ .

1. У.С. U' и U'' называются эквивалентными, если при определенном соответствии полюсов $f' = f''$.

Поскольку сами У.С. однозначно определены своими схемами, то можно говорить также об эквивалентности схем.

2. Пусть Σ_1 — часть схемы Σ' , включающая в себя некоторое подмножество элементов и связей между ними. Эта часть Σ_1 задает подсхему, если в ней

(а) определена совокупность полюсов (иногда обладает спецификой, например, разбивается на входные и выходные полюса) так, что к ней относятся:

- все вершины из Σ_1 , являющиеся полюсами Σ' ;
- все вершины, по которым Σ_1 соприкасается с остальной частью Σ' ;
- может быть, еще какие-то вершины Σ_1 ;

(b) полюса определенным образом занумерованы (с учетом нумерации в Σ') и при этих уточнениях эта часть является схемой.

Предположим, что класс $\mathcal{U}$ является правильным, т. е. для каждой схемы Σ найдется управляющая система U , обладающая этой схемой, т. е. $U = (\Sigma, \Phi)$.

В этом предположении подсхема Σ_1 схемы Σ' определяет, и, в силу регулярности, однозначным образом, подуправляющую систему $U_1 = (\Sigma_1, \Phi_1)$ У.С. U' .

3. Пусть У.С. U_2 имеет такое же количество и ту же специфику полюсов, как У.С. U_1 . Тогда можно определить подстановку У.С. U_2 вместо У.С. U_1 , входящей в U' . Для этого удаляют из U' У.С. U_1 , сохраняя только полюса из U_1 . Затем к ним «присоединяют» с учетом специфики полюса У.С. U_2 . В результате мы получим из У.С. U' У.С. U'' . Очевидно, процесс присоединения можно осуществить многими способами. В случае, если U_2 имеет нумерацию полюсов, подобную U_1 , существует естественный способ присоединения U_2 : присоединение соответствует нумерациям полюсов U_1 и U_2 .

Например, У.С. U_1 — электронная лампа, U_2 — другая электронная лампа (не обязательно того же типа, что и U_1). Подстановка вместо U_1 состоит в удалении U_1 и замене ее на U_2 . Правильность подключения лампы U_2 обеспечивается за счет направляющей ножки, обеспечивающей соответствие полюсов.

4. Если U_2 эквивалентна U_1 , то операция подстановки называется эквивалентной подстановкой в случае, когда подстановка согласована с соответствием полюсов U_1 и U_2 , обеспечивающим их эквивалентность.

В примере с электронными лампами, если U_2 одного типа с U_1 , то замена будет эквивалентной.

Говорят также, что если при любой эквивалентной подстановке в произвольную У.С. из $\mathcal{U}$ она переходит в эквивалентную У.С., то для класса $\mathcal{U}$ выполнен принцип эквивалентной замены. В этом случае из $U_1 \sim U_2$ следует $U' \sim U''$.

5. Подмножество пар $\{(U_1 \sim U_2)\}$, эквивалентных У.С., называется системой тождеств. В дальнейшем тождества

$$U_1 \sim U_2$$

тракуются в разных смыслах.

(a) Считается, что тождество $U_1 \sim U_2$ задает одну эквивалентность, именно $U_1 \sim U_2$.

(b) Считается, что тождество $U_1 \sim U_2$ задает все эквивалентности, получающиеся из данной путем согласованных, изоморфных преобразований левой и правой части.

(c) Считается, что тождество $U_1 \sim U_2$ задает все эквивалентности, получающиеся из данной специальными преобразованиями, включающими изоморфные преобразования и согласованные подстановки в левую и правую части.

В дальнейшем в каждом случае фиксируется трактовка смысла тождества.

6. Пусть задана система множеств $\{(U_1 \sim U_2)\}$ в определенном смысле. Тогда последовательность

$$U' \rightarrow U'' \rightarrow \dots \rightarrow U^{(p)},$$

где $U^{(i+1)}$ получается из $U^{(i)}$ ($i = 1, \dots, p-1$) путем эквивалентной подстановки с использованием тождества из данной системы, называется эквивалентным преобразованием при помощи системы тождеств $\{(U_1 \sim U_2)\}$.

Будем обозначать через

$$U^1 \Rightarrow U^{(p)}$$

эквивалентное преобразование U^1 в $U^{(p)}$.

Очевидно, что эквивалентное преобразование обладает свойством взаимности, т. е. если $U^1 \Rightarrow U^{(p)}$, то $U^{(p)} \Rightarrow U^1$.

В случае, когда выполнен принцип эквивалентной замены, мы имеем

$$U^{(p)} \sim U^1.$$

7. Система тождеств $\{(U_1 \sim U_2)\}$ из $\mathfrak{M}$ называется полной, если каковы бы ни были У.С. U' и U'' из $\mathfrak{M}$ такие, что $U' \sim U''$, существует эквивалентное преобразование при помощи данной системы тождеств U' в U'' .

8. Основная проблематика теории эквивалентных преобразований группируется вокруг следующих задач.

Задача построений полных систем тождеств.

Поскольку всегда существует тривиальное решение задачи, которое в качестве системы тождеств имеет систему всех пар (U_1, U_2) из $\mathfrak{M}$ эквивалентных У.С., то данная задача требует уточнения. Под построением полной системы тождеств подразумевают построение нетривиальной полной системы, например, минимальной мощности.

Возвращаясь к рассуждению о проектировании схем, мы видим, что этап усовершенствования схем зависит от того, владеет ли инженер полной системой правил эквивалентных преобразований. Наличие полной системы правил преобразований принципиально позволяет получить оптимальную схему. Математически более точную иллюстрацию дает задача об упрощении д.н.ф. [1]. Как мы видели, там имеются два правила преобразований:

- 1) удаление множителя;
- 2) удаление слагаемого.

Оказывается, что при помощи этих правил (а они являются эквивалентными заменами при тех условиях, когда они применимы) можно построить любую тупиковую д.н.ф., исходя из некоторой записи совершенной д.н.ф. Если к этим правилам добавить ассоциативные и коммутативные законы для $\&$ и $\vee$, то окажется возможным переходить от одной записи совершенной д.н.ф. к любой другой. Отсюда следует, что при помощи этих правил можно преобразовать эквивалентным образом произвольную

д.н.ф. $\mathcal{A}_1$ в любую ей эквивалентную д.н.ф. $\mathcal{A}_2$:

$$\begin{aligned}\text{д.н.ф. } \mathcal{A}_1 &\Rightarrow \text{тупиковая д.н.ф. } \mathcal{A}'_1 \Rightarrow \\ &\Rightarrow \text{запись совершенной д.н.ф. } \mathcal{A}''_1 \Rightarrow \\ &\Rightarrow \text{запись совершенной д.н.ф. } \mathcal{A}''_2 \Rightarrow \\ &\Rightarrow \text{тупиковая д.н.ф. } \mathcal{A}'_2 \Rightarrow \text{д.н.ф. } \mathcal{A}_2.\end{aligned}$$

Задача построения алгоритмов для осуществления эквивалентных преобразований при помощи заданной системы тождеств.

Основной вопрос здесь состоит в том, чтобы иметь возможность производить эквивалентные преобразования экономным образом, например, с употреблением наименьшего числа эквивалентных подстановок. Эта задача лучше всего разработана для родственной проблемы — проблемы логического вывода.

Следует далее заметить, что можно обобщить задачу об эквивалентных преобразованиях, отказавшись от требования эквивалентности при подстановках, т. е. не предполагать, что $U_1 \sim U_2$, и рассматривать направление преобразования (подстановки), т. е. рассматривать подстановки вида

$$U_1 \rightarrow U_2.$$

При таких обобщениях данная тематика охватит ряд задач теории эволюции, теории построения сложных систем (из области химии, биологии, техники) и т. п.

§ 1. Эквивалентные преобразования формул в P_2

Изучение эквивалентных преобразований У.С. мы начинаем с простейшего класса У.С. — формул алгебры логики в классическом базисе — $\{ \neg, \&, \vee \}$ [34]. Это делается потому, что в нем эквивалентные преобразования имеют привычный алгебраический подход. Кроме того, на этом примере выявляются основные идеи и методы, связанные с построением полных систем тождеств.

Сначала проследим, как выглядит система понятий для формул в P_2 .

1. Формулы $\mathcal{A}'$ и $\mathcal{A}''$ называются равными (эквивалентными), если соответствующие им функции $f_{\mathcal{A}'}$ и $f_{\mathcal{A}''}$ равны. Например, $x_1 \& x_2 = \bar{x}_1 \vee \bar{x}_2$ или $x_1 \& \bar{x}_1 = x_2 \& \bar{x}_2$.

2. Если $\mathcal{A}_1$ — часть формулы $\mathcal{A}'$ и является формулой, то она называется подформулой формулы $\mathcal{A}'$.

3. Пусть $\mathcal{A}_1$ — подформула формулы $\mathcal{A}'$ и $\mathcal{A}_2$ — произвольная формула. Замена подформулы $\mathcal{A}_1$ на $\mathcal{A}_2$ в формуле $\mathcal{A}'$ называется подстановкой $\mathcal{A}_2$ вместо $\mathcal{A}_1$.

4. В случае, если $\mathcal{A}_2 = \mathcal{A}_1$, подстановка $\mathcal{A}_2$ вместо $\mathcal{A}_1$ называется эквивалентной подстановкой. Очевидно, для формул справедлив принцип эквивалентной замены: если обозначить через $\mathcal{A}''$ формулу, получающуюся из $\mathcal{A}'$ путем эквивалентной подстановки $\mathcal{A}_2$ вместо $\mathcal{A}_1$, то, очевидно, $\mathcal{A}'' = \mathcal{A}'$, или иначе, если $\mathcal{A}_2 = \mathcal{A}_1$, то $\mathcal{A}'' = \mathcal{A}'$.

5. Тожество $\mathfrak{A}_1(x_1, \dots, x_n) = \mathfrak{A}_2(x_1, \dots, x_n)$ в случае формул трактуется весьма широко: считается, что оно задает все тождества вида

$$\mathfrak{A}_1(\mathfrak{C}_1, \dots, \mathfrak{C}_n) = \mathfrak{A}_2(\mathfrak{C}_1, \dots, \mathfrak{C}_n),$$

где $\mathfrak{C}_1, \dots, \mathfrak{C}_n$ — произвольные формулы в данном базисе.

6. Затем определяется понятие эквивалентного преобразования одной формулы в другую при помощи заданной системы тождеств $\{\mathfrak{A}_1 = \mathfrak{A}_2\}$ как последовательность

$$\mathfrak{A}^{(1)} \rightarrow \mathfrak{A}^{(2)} \rightarrow \dots \rightarrow \mathfrak{A}^{(p)}$$

формул, в которой каждая последующая получается из предыдущей путем эквивалентной подстановки с использованием тождеств системы $\{\mathfrak{A}_1 = \mathfrak{A}_2\}$.

7. Наконец, формулируется понятие полной системы тождеств. Система тождеств $\{\mathfrak{A}_1 = \mathfrak{A}_2\}$ называется полной, если для любых двух эквивалентных формул $\mathfrak{A}'$ и $\mathfrak{A}''$ существует эквивалентное преобразование при помощи тождеств системы $\{\mathfrak{A}_1 = \mathfrak{A}_2\}$, переводящее формулу $\mathfrak{A}'$ в формулу $\mathfrak{A}''$. Очевидно, что для данного объекта тривиальная полная система тождеств имеет счетную мощность. Возникает вопрос о том, можно ли построить существенно более простую полную систему тождеств. Оказывается, что имеет место следующий факт.

Теорема 24. *Для системы формул алгебры логики в базисе $\{\neg, \&, \vee\}$ существует конечная полная система тождеств.*

Доказательство. Построение системы тождеств и доказательство ее полноты делается одновременно. Для этого в каждом классе эквивалентных формул выбирают некоторое подмножество формул, имеющих простое строение (формулы канонического вида). Далее подбирают систему тождеств, которая позволяет:

- 1) «приводить» произвольную формулу к каноническому виду,
- 2) две любые эквивалентные формулы, имеющие канонический вид, переводить друг в друга.

Этот подход, как мы увидим ниже, оказывается весьма плодотворным и, фактически, эффективно работает и в случае других классов У.С.

Пусть f — функция, соответствующая формуле $\mathfrak{A}$. Определим канонический вид формулы $\mathfrak{A}$ следующим образом:

а) если $f \equiv 0$, то каноническим видом формулы $\mathfrak{A}$ является формула вида $x_i \& \bar{x}_i$ ($i = 1, 2, \dots$);

б) если $f \not\equiv 0$ и алфавит $x_1, \dots, x_n$ содержит все существенные переменные функции f , то каноническим видом формулы $\mathfrak{A}$ является совершенная д.н.ф.

$$\bigvee_{\substack{(\sigma_1, \dots, \sigma_n): \\ f(\sigma_1, \dots, \sigma_n)=1}} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n}$$

(разумеется, с какой-то расстановкой скобок).

Заметим, что канонический вид формулы $\mathcal{A}$ неоднозначен и зависит от фиксации несущественных переменных, порядка следования слагаемых и порядков следований множителей в слагаемых, а также от расстановки скобок.

1. Приведение формулы $\mathcal{A}$ к каноническому виду. Этот этап распадается на ряд шагов.

(а) Спуск отрицаний вглубь формулы.

Достигается с использованием следующих тождеств

$$\overline{x_1 \& x_2} = \bar{x}_1 \vee \bar{x}_2, \quad (1)$$

$$\overline{x_1 \vee x_2} = \bar{x}_1 \& \bar{x}_2, \quad (2)$$

$$\bar{\bar{x}}_1 = x_1. \quad (3)$$

В результате формула преобразуется к виду, где отрицания могут быть только над символами переменных, а операции $\&$ и $\vee$ чередуются хаотически.

(b) Приведение к виду $\vee\&$.

При помощи тождеств

$$(x_1 \vee x_2)x_3 = (x_1x_3) \vee (x_2x_3), \quad (4)$$

$$x_1 \& x_2 = x_2 \& x_1 \quad (5)$$

формула далее приводится к виду, в котором сначала выполняются операции $\&$, а затем $\vee$.

(с) Группировка множителей, зависящих от одного и того же переменного.

Используя ассоциативный закон (тождество (6)) для умножения

$$(x_1 \& x_2) \& x_3 = x_1 \& (x_2 \& x_3), \quad (6)$$

а также коммутативный закон (5) в произведении, можно добиться, чтобы два множителя вида $x_i^{\sigma_1}$ и $x_i^{\sigma_2}$ были рядом внутри скобок, т. е. осуществить преобразование

$$\dots x_i^{\sigma_1} \& \dots \& x_i^{\sigma_2} \dots \implies \dots (x_i^{\sigma_1} \& x_i^{\sigma_2}) \dots$$

(d) Уничтожение повторений одинаковых множителей.

Осуществляется при помощи тождества

$$x_1 \& x_1 = x_1. \quad (7)$$

(е) Преобразование членов, содержащих x и $\bar{x}$.

Тождества

$$(x_1 \& \bar{x}_1) \& x_2 = x_1 \& \bar{x}_1, \quad (8)$$

$$(x_1 \& \bar{x}_1) \vee x_2 = x_2, \quad (9)$$

$$x_1 \vee x_2 = x_2 \vee x_1 \quad (10)$$

позволяют привести выражение к виду $x_1 \& \bar{x}_1$ или уничтожить вхождение $x_1 \& \bar{x}_1$.

Теперь исходная формула приведена к виду $\vee \&$, и в каждом слагаемом каждое переменное встречается не более одного раза, и может оказаться, что в отдельных слагаемых встречаются не все символы переменных из алфавита $x_1, \dots, x_n$ (отсутствие однородности).

(f) Введение однородности.

Если конъюнкция не содержит переменного x_1 , то при помощи тождества

$$x_2 = (x_1 \vee \bar{x}_1) \& x_2 \quad (11)$$

и последующего раскрытия скобок данная конъюнкция заменится на две, но уже содержащие переменное x_1 . Полученное на этом этапе выражение может содержать повторяющиеся слагаемые. Для их устранения используются

(g) Группировка одинаковых слагаемых.

Закон ассоциативности

$$x_1 \vee (x_2 \vee x_3) = (x_1 \vee x_2) \vee x_3 \quad (12)$$

и закон коммутативности (тождество (10)) позволяют осуществить преобразование

$$\dots \vee x_1 \vee \dots \vee x_1 \vee \dots \Rightarrow \dots (x_1 \vee x_1) \dots$$

(h) Приведение подобных.

Осуществляется при помощи тождества

$$x_1 \vee x_1 = x_1. \quad (13)$$

После всех этих преобразований мы преобразуем, очевидно, исходную формулу к каноническому виду.

2. Переход от одного канонического вида к любому ему эквивалентному каноническому виду над тем же алфавитом $x_1, \dots, x_n$:

(a) если $f \equiv 0$, то добавляем тождество

$$x_1 \& \bar{x}_1 = x_2 \& \bar{x}_2 \quad (14)$$

(равенство нулей); оно позволяет переходить от одного канонического вида к другому, ему эквивалентному;

(b) если $f \neq 0$, то каноническим видом является совершенная д.н.ф., определяемая с точностью до порядка слагаемых, порядка множителей внутри слагаемых и расстановки скобок. Поскольку у нас имеются ассоциативные и коммутативные законы, то искомое преобразование легко осуществляется.

3. Завершение доказательства.

Пусть $\mathfrak{A}'$ и $\mathfrak{A}''$ — произвольные эквивалентные формулы. Возьмем в качестве $\{x_1, \dots, x_n\}$ — алфавит, содержащий все переменные из $\mathfrak{A}'$ и $\mathfrak{A}''$. Обозначим через $\mathfrak{F}'$ и $\mathfrak{F}''$ канонические формулы, к которым они приводятся:

$$\mathfrak{A}' \Rightarrow \mathfrak{F}' \quad \text{и} \quad \mathfrak{A}'' \Rightarrow \mathfrak{F}''.$$

С другой стороны, из $\mathfrak{A}' = \mathfrak{A}''$ следует, что $\mathfrak{F}' = \mathfrak{F}''$ и в силу пункта 2 существует эквивалентное преобразование $\mathfrak{F}' \Rightarrow \mathfrak{F}''$. Тогда

$$\mathfrak{A}' \Rightarrow \mathfrak{F}' \Rightarrow \mathfrak{F}'' \Rightarrow \mathfrak{A}''$$

и дает эквивалентное преобразование $\mathfrak{A}'$ в $\mathfrak{A}''$ при помощи построенной системы тождеств (1)–(14).

Теорема доказана.

Построенная система тождеств избыточна и может быть сокращена. В самом деле, тождество (2) вытекает из (1) и (3):

$$\overline{x_1 \vee x_2} = \overline{\bar{x}_1 \vee \bar{x}_2} = \overline{\bar{x}_1 \& \bar{x}_2} = \bar{x}_1 \& \bar{x}_2;$$

тождество (10) следует из (3), (1) и (5):

$$x_1 \vee x_2 = \overline{\bar{x}_1 \vee \bar{x}_2} = \overline{\bar{x}_1 \& \bar{x}_2} = \overline{\bar{x}_2 \& \bar{x}_1} = \bar{x}_2 \vee \bar{x}_1 = x_2 \vee x_1;$$

тождество (11) является следствием тождеств (3), (1) и (9):

$$(x_1 \vee \bar{x}_1) \& x_2 = \overline{(x_1 \vee \bar{x}_1) \& x_2} = \overline{(\bar{x}_1 \& x_1) \vee \bar{x}_2} = \bar{x}_2 = x_2;$$

тождество (12) вытекает из (3), (1) и (6):

$$\begin{aligned} x_1 \vee (x_2 \vee x_3) &= \overline{\bar{x}_1 \vee (\bar{x}_2 \vee \bar{x}_3)} = \overline{\bar{x}_1 \& (\bar{x}_2 \& \bar{x}_3)} = \\ &= \overline{(\bar{x}_1 \& \bar{x}_2) \& \bar{x}_3} = (\bar{x}_1 \vee \bar{x}_2) \vee \bar{x}_3 = (x_1 \vee x_2) \vee x_3; \end{aligned}$$

тождество (13) следует из (3), (1) и (7):

$$x_1 \vee x_1 = \overline{\bar{x}_1 \vee \bar{x}_1} = \overline{\bar{x}_1 \& \bar{x}_1} = \bar{x}_1 = x_1;$$

тождество (14) получается из (8) и (5):

$$x_1 \& \bar{x}_1 = (x_1 \& \bar{x}_1) \& (x_2 \& \bar{x}_2) = (x_2 \& \bar{x}_2) \& (x_1 \& \bar{x}_1) = x_2 \& \bar{x}_2.$$

Все эти доказательства связаны с так называемым принципом двойственности для формул. Итак, окончательно мы получаем следующие тождества:

$$\overline{x_1 \& x_2} = \bar{x}_1 \vee \bar{x}_2, \quad (\text{I})$$

$$\bar{\bar{x}}_1 = x_1, \quad (\text{II})$$

$$(x_1 \vee x_2)x_3 = (x_1x_3) \vee (x_2x_3), \quad (\text{III})$$

$$x_1 \& x_2 = x_2 \& x_1, \quad (\text{IV})$$

$$(x_1 \& x_2) \& x_3 = x_1 \& (x_2 \& x_3), \quad (\text{V})$$

$$(x_1 \& \bar{x}_1) \& x_2 = x_1 \& \bar{x}_1, \quad (\text{VI})$$

$$(x_1 \& \bar{x}_1) \vee x_2 = x_2, \quad (\text{VII})$$

$$x_1 \& x_1 = x_1. \quad (\text{VIII})$$

В силу известной теоремы Поста [42] о том, что каждый замкнутый класс $\mathcal{P}$ из P_2 имеет конечный базис, можно задавать функции из $\mathcal{P}$ формулами в этом конечном базисе. Возникает вопрос о мощности полной системы тождеств для указанных классов формул. Ответ на это дает теорема Линдона (приводится без доказательства).

Т е о р е м а 25 (Линдон [9]). *Для каждого замкнутого класса $\mathcal{P}$ из P_2 система формул в его специальном базисе имеет конечную полную систему тождеств.*

§ 2. Эквивалентные преобразования формул в P_k

Сначала рассмотрим множество формул в P_k , которые построены из $0, 1, \dots, k-1, \mathcal{J}_i(x)$ ($i = 0, 1, \dots, k-1$), $\min(x_1, x_2)$ и $\max(x_1, x_2)$.

Основные понятия, связанные с эквивалентными преобразованиями, для P_k выглядят почти так же, как и для P_2 .

Т е о р е м а 26. *Для множества всех формул, построенных из $0, 1, \dots, k-1, \mathcal{J}_i(x)$ ($i = 0, 1, \dots, k-1$), $\min(x_1, x_2)$ и $\max(x_1, x_2)$, существует конечная полная система тождеств.*

Д о к а з а т е л ь с т в о. Основано на той же идее, что и для случая формул в P_2 . В качестве канонического вида для формулы $\mathcal{A}(x_1, \dots, x_n)$ берем аналог совершенной д.н.ф.

$$\bigvee_{(\sigma_1, \dots, \sigma_n)} \mathcal{J}_{\sigma_1}(x_1) \& \mathcal{J}_{\sigma_2}(x_2) \& \dots \& \mathcal{J}_{\sigma_n}(x_n) \& f(\sigma_1, \dots, \sigma_n),$$

где $\&$ и $\vee$ обозначают соответственно $\min(x_1, x_2)$ и $\max(x_1, x_2)$.

1. Преобразование формулы $\mathcal{A}$ к каноническому виду.

(а) Спуск функции $\mathcal{J}_\sigma$ вглубь формулы.

Пусть $\mathcal{J}_\sigma(\mathcal{B})$ — подформула формулы $\mathcal{A}$, где $\mathcal{B}$ — некоторая подформула. Возможны следующие случаи:

$\mathcal{B} = c$ (константа),

$\mathcal{B} = \mathcal{J}_\tau(\mathcal{C})$, где $\mathcal{C}$ некоторая подформула ($\tau = 0, \dots, k-1$),

$\mathcal{B} = \min(\mathcal{C}_1, \mathcal{C}_2)$,

$\mathcal{B} = \max(\mathcal{C}_1, \mathcal{C}_2)$, где $\mathcal{C}_1, \mathcal{C}_2$ — некоторые подформулы.

Для осуществления спуска необходимы следующие тождества:

$$\mathcal{J}_\sigma(c) = \begin{cases} 0, & \text{при } \sigma \neq c, \\ k-1, & \text{при } \sigma = c, \end{cases} \quad (1)$$

$$\mathcal{J}_\sigma(\mathcal{J}_\tau(x)) = \begin{cases} \mathcal{J}_0(x) \vee \dots \vee \mathcal{J}_{\tau-1}(x) \vee \\ \vee \mathcal{J}_{\tau+1}(x) \vee \dots \vee \mathcal{J}_{k-1}(x), & \text{при } \sigma = 0, \\ 0, & \text{при } 0 < \sigma < k-1, \\ \mathcal{J}_\tau(x), & \text{при } \sigma = k-1, \end{cases} \quad (2)$$

$$\begin{aligned} \mathcal{J}_\sigma(\min(x_1, x_2)) &= \mathcal{J}_\sigma(x_1)(\mathcal{J}_\sigma(x_2) \vee \dots \vee \mathcal{J}_{k-1}(x_2)) \vee \\ &\vee \mathcal{J}_\sigma(x_2)(\mathcal{J}_\sigma(x_1) \vee \dots \vee \mathcal{J}_{k-1}(x_1)), \end{aligned} \quad (3)$$

$$\begin{aligned} \mathcal{J}_\sigma(\max(x_1, x_2)) &= \mathcal{J}_\sigma(x_1)(\mathcal{J}_0(x_2) \vee \dots \vee \mathcal{J}_\sigma(x_2)) \vee \\ &\vee \mathcal{J}_\sigma(x_2)(\mathcal{J}_0(x_1) \vee \dots \vee \mathcal{J}_\sigma(x_1)). \end{aligned} \quad (4)$$

Заметим, что в процессе спуска функций $\mathcal{J}_\sigma$ вглубь, структура исходной формулы может значительно усложниться. В двухзначном случае при спуске отрицаний суммарное число операций $\&$ и $\vee$ сохраняется.

(b) Приведение к виду $\vee \&$.

Здесь используются тождества, выражающие закон дистрибутивности, коммутативности

$$(x_1 \vee x_2) \& x_3 = (x_1 \& x_3) \vee (x_2 \& x_3), \quad (5)$$

$$x_1 \& x_2 = x_2 \& x_1. \quad (6)$$

(c) Группировка множителей, зависящих от одного и того же переменного, а также констант.

В каждом произведении любые члены можно сгруппировать вместе, используя закон ассоциативности для умножения

$$(x_1 \& x_2) \& x_3 = x_1 \& (x_2 \& x_3) \quad (7)$$

и закон коммутативности (6).

(d) Уничтожение вхождений переменных в произведениях.

Осуществляется при помощи тождеств

$$x_1 \& x_1 = x_1, \quad (8)$$

$$x_1 = 1 \cdot \mathcal{J}_1(x_1) \vee 2 \cdot \mathcal{J}_2(x_1) \vee \dots \vee (k-1) \mathcal{J}_{k-1}(x_1). \quad (9)$$

После этого используют тождества пункта (b).

(e) Уничтожение повторений в произведениях констант и символов $\mathcal{J}$ для одного и того же переменного x .

Здесь используются тождества

$$c_1 \cdot c_2 = \min(c_1, c_2), \quad (10)$$

$$\mathcal{J}_\sigma(x) \& \mathcal{J}_\tau(x) = \begin{cases} 0, & \text{при } \sigma \neq \tau, \\ \mathcal{J}_\sigma(x), & \text{при } \sigma = \tau. \end{cases} \quad (11)$$

(f) Достижение однородности произведений.

Производится путем применения тождеств

$$x_1 = (k-1) \& x_1, \quad (12)$$

$$k-1 = \mathcal{J}_0(x_2) \vee \dots \vee \mathcal{J}_{k-1}(x_2), \quad (13)$$

а также последующего раскрытия скобок.

(g) Группировка слагаемых.
Для этого берем тождества

$$(x_1 \vee x_2) \vee x_3 = x_1 \vee (x_2 \vee x_3), \quad (14)$$

$$x_1 \vee x_2 = x_2 \vee x_1. \quad (15)$$

(h) Уничтожение повторений слагаемых.
Используется тождество

$$c_1 x_1 \vee x_1 = x_1. \quad (16)$$

Легко видеть, что эти тождества позволяют любую формулу привести к каноническому виду, и два эквивалентных канонических вида могут быть этими же тождествами преобразованы друг в друга.

Таким образом, и в P_2 , и в P_k в конкретных базисах существуют конечные полные системы тождеств. Здесь естественно возникает вопрос: что можно сказать об эквивалентных преобразованиях формул, если взять другие базисы? Например, для P_2 — базис

$$\{0, 1, x_1 x_2, x_1 + x_2\}$$

или для P_k — базис

$$\{x_1 + 1 \pmod k, \min(x_1, x_2)\}.$$

К этому вопросу примыкает непосредственно и другой вопрос: можно ли построить полную систему тождеств для данного базиса, если известна полная система тождеств для некоторого базиса того же замкнутого класса функций?

Ответы на эти вопросы дает теорема, которая справедлива для произвольных функциональных систем с операцией суперпозиции и имеющих конечный базис, и тем самым может быть применена к классам из P_2 и классам с конечным базисом из P_k .

Пусть $\mathcal{P}$ — класс функций, порожденный множеством F функций $f_1, \dots, f_r$. Будем рассматривать формулы в этом базисе и обозначать их так: $\mathfrak{A} = \mathfrak{A}[f_1, \dots, f_r]$ (где $f_1, \dots, f_r$ — не аргументы, а указатели функций из F) или кратко $\mathfrak{A} = \mathfrak{A}[F]$.

Рассмотрим другой базис $g_1, \dots, g_s$ этого класса $\mathcal{P}$. Формулы в этом базисе будем обозначать через $\mathfrak{B} = \mathfrak{B}[g_1, \dots, g_s] = \mathfrak{B}[G]$.

Пусть $\mathfrak{P} = \{\mathfrak{A}\}$ и $\mathfrak{Q} = \{\mathfrak{B}\}$.

Теорема 27. *Если система $\mathfrak{P}$ имеет конечную полную систему тождеств, то система $\mathfrak{Q}$ имеет также конечную полную систему тождеств.*

Доказательство. По условию система $\mathfrak{P}$ имеет конечную полную систему тождеств

$$\mathfrak{A}'_1[F] = \mathfrak{A}''_1[F], \quad \dots, \quad \mathfrak{A}'_m[F] = \mathfrak{A}''_m[F].$$

С другой стороны, так как F и G — базисы, то

$$\left. \begin{array}{c} f_1 = \mathfrak{C}_1[G], \\ \dots\dots\dots \\ f_r = \mathfrak{C}_r[G] \end{array} \right\} \quad \text{или} \quad F = \mathfrak{C}[G]$$

и

$$\left. \begin{array}{c} g_1 = \mathfrak{D}_1[F], \\ \dots\dots\dots \\ g_s = \mathfrak{D}_s[F] \end{array} \right\} \quad \text{или} \quad G = \mathfrak{D}[F].$$

Рассмотрим систему тождеств

$$\begin{array}{c} \mathfrak{A}'_1[\mathfrak{C}[G]] = \mathfrak{A}''_1[\mathfrak{C}[G]], \\ \dots\dots\dots \\ \mathfrak{A}'_m[\mathfrak{C}[G]] = \mathfrak{A}''_m[\mathfrak{C}[G]], \\ \\ \left. \begin{array}{c} g_1 = \mathfrak{D}_1[\mathfrak{C}[G]], \\ \dots\dots\dots \\ g_s = \mathfrak{D}_s[\mathfrak{C}[G]] \end{array} \right\} \quad \text{или} \quad G = \mathfrak{D}[\mathfrak{C}[G]]; \end{array}$$

покажем, что эта система является полной для Ω .

Рассмотрим произвольную пару эквивалентных формул для Ω

$$\mathfrak{B}'[G] = \mathfrak{B}''[G].$$

Если в этих формулах выразить базисные функции G через F , то получим

$$\mathfrak{A}'[F] = \mathfrak{B}'[\mathfrak{D}[F]] \quad \text{и} \quad \mathfrak{A}''[F] = \mathfrak{B}''[\mathfrak{D}[F]].$$

Очевидно, что

$$\mathfrak{A}'[F] = \mathfrak{A}''[F].$$

В силу того, что для $\mathfrak{P}$ имеется конечная полная система тождеств, мы имеем эквивалентное преобразование

$$\mathfrak{A}'[F] \rightarrow \mathfrak{A}'''[F] \rightarrow \dots \rightarrow \mathfrak{A}^p[F] \rightarrow \mathfrak{A}''[F].$$

По этому преобразованию построим другое эквивалентное преобразование

$$\begin{aligned} \mathfrak{B}'[G] &\Rightarrow \mathfrak{B}'[\mathfrak{D}[\mathfrak{C}[G]]] \equiv \mathfrak{A}'[\mathfrak{C}[G]] \rightarrow \mathfrak{A}'''[\mathfrak{C}[G]] \rightarrow \dots \\ &\dots \rightarrow \mathfrak{A}^p[\mathfrak{C}[G]] \rightarrow \mathfrak{A}''[\mathfrak{C}[G]] \equiv \mathfrak{B}''[\mathfrak{D}[\mathfrak{C}[G]]] \Rightarrow \mathfrak{B}''[G] \end{aligned}$$

для Ω .

Теорема доказана.

З а м е ч а н и я.

1. Теорема дает способ построения конечной полной системы в произвольном базисе.

2. Свойство иметь конечную полную систему тождеств зависит только от класса $\mathcal{P}$ и не зависит от базиса.

П р и м е р. Возьмем систему функций $\{\bar{x}_1, x_1 \& x_2, x_1 \vee x_2\}$ в качестве базиса F , а в качестве базиса G — систему функций $\{x_1 \rightarrow x_2, 0\}$. Эти базисы могут быть выражены друг через друга следующим образом:

$$\begin{aligned}\bar{x}_1 &= x_1 \rightarrow 0, \\ x_1 \& x_2 &= (x_1 \rightarrow (x_2 \rightarrow 0)) \rightarrow 0, \\ x_1 \vee x_2 &= (x_1 \rightarrow 0) \rightarrow x_2, \\ x_1 \rightarrow x_2 &= \bar{x}_1 \vee x_2, \\ 0 &= x_1 \& \bar{x}_1.\end{aligned}$$

Кроме того, мы имеем конечную полную систему тождеств для F :

$$\overline{x_1 \& x_2} = \bar{x}_1 \vee \bar{x}_2, \quad (\text{I})$$

$$\bar{\bar{x}}_1 = x_1, \quad (\text{II})$$

$$(x_1 \vee x_2)x_3 = x_1x_3 \vee x_2x_3, \quad (\text{III})$$

$$x_1x_2 = x_2x_1, \quad (\text{IV})$$

$$(x_1x_2)x_3 = x_1(x_2x_3), \quad (\text{V})$$

$$(x_1 \& \bar{x}_1) \& x_2 = x_1 \& \bar{x}_1, \quad (\text{VI})$$

$$(x_1 \& \bar{x}_1) \vee x_2 = x_2, \quad (\text{VII})$$

$$x_1 \& x_1 = x_1. \quad (\text{VIII})$$

В соответствии с доказанной выше теоремой мы получаем для G следующую полную систему тождеств:

$$[(x_1 \rightarrow (x_2 \rightarrow 0)) \rightarrow 0] \rightarrow 0 = ([x_1 \rightarrow 0] \rightarrow 0) \rightarrow [x_2 \rightarrow 0], \quad (1)$$

$$[x_1 \rightarrow 0] \rightarrow 0 = x_1, \quad (2)$$

$$\begin{aligned}& ([(x_1 \rightarrow 0) \rightarrow x_2] \rightarrow (x_3 \rightarrow 0)) \rightarrow 0 = \\ & = ([(x_1 \rightarrow (x_3 \rightarrow 0)) \rightarrow 0] \rightarrow 0) \rightarrow [(x_2 \rightarrow (x_3 \rightarrow 0)) \rightarrow 0],\end{aligned} \quad (3)$$

$$(x_1 \rightarrow (x_2 \rightarrow 0)) \rightarrow 0 = (x_2 \rightarrow (x_1 \rightarrow 0)) \rightarrow 0, \quad (4)$$

$$\begin{aligned}& ([(x_1 \rightarrow (x_2 \rightarrow 0)) \rightarrow 0] \rightarrow (x_3 \rightarrow 0)) \rightarrow 0 = \\ & = (x_1 \rightarrow ([(x_2 \rightarrow (x_3 \rightarrow 0)) \rightarrow 0] \rightarrow 0)) \rightarrow 0,\end{aligned} \quad (5)$$

$$\begin{aligned}& ([(x_1 \rightarrow ([x_1 \rightarrow 0] \rightarrow 0)) \rightarrow 0] \rightarrow (x_2 \rightarrow 0)) \rightarrow 0 = \\ & = (x_1 \rightarrow ([x_1 \rightarrow 0] \rightarrow 0)) \rightarrow 0,\end{aligned} \quad (6)$$

$$([(x_1 \rightarrow ([x_1 \rightarrow 0] \rightarrow 0)) \rightarrow 0] \rightarrow 0) \rightarrow x_2 = x_2, \quad (7)$$

$$(x_1 \rightarrow (x_1 \rightarrow 0)) \rightarrow 0 = x_1, \quad (8)$$

$$x_1 \rightarrow x_2 = ([x_1 \rightarrow 0] \rightarrow 0) \rightarrow x_2, \quad (9)$$

$$0 = (x_1 \rightarrow ([x_1 \rightarrow 0] \rightarrow 0)) \rightarrow 0. \quad (10)$$

Рассмотрим две эквивалентные формулы во втором базисе

$$0 \rightarrow 0 \quad \text{и} \quad x \rightarrow x.$$

Этим формулам в первом базисе соответствуют формулы

$$\overline{x \& \bar{x}} \vee (x \& \bar{x}) \quad \text{и} \quad \bar{x} \vee x.$$

Построим цепочку эквивалентных преобразований, переводящих их друг в друга:

$$\begin{aligned} \overline{x \& \bar{x}} \vee (x \& \bar{x}) &\xrightarrow{\Pi} \overline{x \& \bar{x}} \vee \overline{\overline{x \& \bar{x}}} \xrightarrow{\text{I}} \overline{(x \& \bar{x}) \& x \& \bar{x}} \xrightarrow{\text{VI}} \\ &\xrightarrow{\text{VI}} \overline{x \& \bar{x}} \xrightarrow{\text{I}} \bar{x} \vee \bar{x} \xrightarrow{\Pi} \bar{x} \vee x. \end{aligned} \quad (*)$$

В этой цепочке сконструируем цепочку эквивалентных преобразований для исходных формул. В формуле

$$0^* \xrightarrow{*} 0^*$$

заменяем 0^* , пользуясь (10):

$$[(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0] \xrightarrow{*} [(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0].$$

Далее заменяем $\xrightarrow{*}$ (для удобства помечена звездочкой)¹³:

$$\underbrace{([[(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0] \rightarrow 0] \rightarrow 0)}_{\overline{x \& \bar{x}}} \rightarrow \underbrace{[(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0]}_{x \& \bar{x}}.$$

Полученная формула соответствует формуле $\overline{x \& \bar{x}} \vee (x \& \bar{x})$, если в ней заменить $\rightarrow$, $\&$, $\vee$ через 0 и $\rightarrow$. Теперь начинаем использовать цепочку (*). Применяем к $x \& \bar{x}$ правило (2):

$$\underbrace{([[(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0] \rightarrow 0] \rightarrow 0)}_{\overline{x \& \bar{x}}} \rightarrow \underbrace{\{([[(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0] \rightarrow 0) \rightarrow 0\}}_{\overline{\overline{x \& \bar{x}}}}.$$

Затем используем тождество (1) и переводим выражение в конъюнктивную форму

$$\begin{aligned} &([[(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0] \rightarrow \{([[(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0] \rightarrow 0) \rightarrow 0\}} \rightarrow 0) \rightarrow 0 = \\ &= \overline{(x \& \bar{x}) \& x \& \bar{x}}. \end{aligned}$$

¹³Можно делать и в другом порядке.

После этого совершаем «умножение» на 0 (6):

$$\underbrace{[(x \rightarrow ([x \rightarrow 0] \rightarrow 0)) \rightarrow 0]}_{x \& \bar{x}} \rightarrow 0.$$

Затем переводим с помощью (1) в дизъюнктивную форму:

$$([x \rightarrow 0] \rightarrow 0) \rightarrow [(x \rightarrow 0) \rightarrow 0].$$

Далее «убираем» двойное отрицание (2):

$$\underbrace{([x \rightarrow 0] \rightarrow 0) \rightarrow x}_{\bar{x} \vee x}.$$

Наконец, при помощи (9) получаем

$$x \rightarrow x.$$

Этот пример иллюстрирует доказательство теоремы. Мы видим на нем, как находится конечная полная система тождеств в новом базисе, если она известна в исходном базисе. Кроме того, он иллюстрирует и технику эквивалентных преобразований в новом базисе.

Как мы видели в P_2 для любого замкнутого класса можно выбрать конечный базис (теорема Поста [42]) и для него указать конечную полную систему тождеств (теорема Линдона [9]). Только что доказанная теорема означает, что для любого замкнутого класса из P_2 в любом конечном базисе существует конечная полная система тождеств, и тем самым с этими классами можно обращаться, как с традиционными алгебро-логическими объектами.

При переходе к P_k оказывается, что ситуация становится более сложной, если $k \geq 3$. Именно: не каждый замкнутый класс имеет конечный базис, и, как мы покажем, не для каждого замкнутого класса с конечным базисом возможно построить конечную полную систему тождеств.

Первый такой пример в P_7 был построен Линдоном [10], впоследствии удалось снизить значность сначала до $k = 4$ (Вишин [3]) и затем до минимума $k = 3$ (Мурский [19]). Здесь мы изложим результат Линдона, который с методической точки зрения является пока самым простым.

Возьмем функцию $\varphi(x_1, x_2)$ (см. табл. 7). Очевидно, $\varphi \in P_7$. В дальнейшем введем для нее более простое обозначение $\varphi(x_1, x_2) = x_1 \cdot x_2$.

Обозначим $x \cdot x$ через 0, так как функция $x \cdot x \equiv 0$.

Рассмотрим совокупность формул $\mathfrak{P}$, построенных над $x_1 \cdot x_2$, и соответствующий ей замкнутый класс функций $\mathcal{P}$.

Т а б л и ц а 7

$x_1 \backslash x_2$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	0	1	5	6	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	5	5	5	0	0
6	0	0	6	6	6	0	0

Покажем, что следующие равенства являются в P_7 тождествами:

$$A_{1,2,3} : 0 \cdot x_1 = 0, \quad x_1 \cdot 0 = 0, \quad x_1 \cdot (x_2 \cdot x_3) = 0,$$

$$B_m : ((\dots(x_1 \cdot x_2) \cdot x_3 \dots) \cdot x_m) \cdot x_1 = 0 \quad (m = 1, 2, \dots),$$

$$C_m : ((\dots(x_1 \cdot x_2) \cdot x_3 \dots) \cdot x_m) \cdot x_2 = (\dots(x_1 \cdot x_2) \cdot x_3 \dots) \cdot x_m \quad (m = 2, 3, \dots).$$

Для $A_{1,2,3}$ утверждение следует из табл. 7.

Для B_m утверждение очевидно при $m = 1$. При $m > 1$, очевидно, $x_1 \cdot x_2$ либо равно 0, и тогда левая часть тоже равна 0, либо $\neq 0$ и в этом случае принимает одно из значений 1, 5, 6, что возможно, если $x_1 \in \{1, 5, 6\}$, но тогда левая часть также равна 0.

Для C_m рассмотрим следующие варианты для правой части:

1. $(\dots(x_1 \cdot x_2) \dots) \cdot x_m = 0$, тогда и левая часть равна 0;

2. $(\dots(x_1 \cdot x_2) \dots) \cdot x_m = 1$, тогда $x_1 = 1$, а $x_2 = 2$ и, значит, левая часть есть $1 \cdot 2 \cdot \dots \cdot 2 = 1$;

3. $(\dots(x_1 \cdot x_2) \dots) \cdot x_m = 5, 6$, тогда $x_2 \in \{2, 3, 4\}$ и левая часть есть $5 \cdot x_2 = 5$ или $6 \cdot x_2 = 6$.

Теорема 28. Пусть $\mathfrak{A}(x_1, \dots, x_n)$ и $\mathfrak{B}(x_1, \dots, x_n)$ — произвольные эквивалентные формулы из $\mathfrak{P}$. Тогда существует эквивалентное преобразование $\mathfrak{A}$ в $\mathfrak{B}$ при помощи тождеств $A_{1,2,3}$, B_m , C_m , где $m \leq n$.

Доказательство. Покажем, что при указанных ограничениях возможно любую формулу над $x_1, \dots, x_n$ привести к каноническому виду, в качестве которого мы берем либо выражение $x_1 \cdot x_1$, если $f_{\mathfrak{A}} \equiv 0$, либо выражение $(\dots(x_{i_1} \cdot x_{i_2}) \dots) \cdot x_{i_\mu}$, где каждый символ из алфавита $x_1, \dots, x_n$ встречается не более одного раза. Последнее имеет место, если $f_{\mathfrak{A}} \not\equiv 0$.

Далее показывается, что при помощи тех же правил (при $m \leq n$) можно от одного канонического вида перейти к любому ему эквивалентному.

Пусть $\mathfrak{A}(x_1, \dots, x_n)$ — произвольная формула. Возможны следующие случаи.

(1) $\mathfrak{A}$ содержит 0, т. е. подформулу вида $u \cdot u$. Тогда, используя $A_{1,2}$, преобразуем $\mathfrak{A}$ в 0.

(2) $\mathfrak{A}$ содержит умножение слева некоторой нетривиальной подформулы (отличной от символа переменного), т. е. имеет фрагмент вида $u \cdot (v \cdot w)$. Тогда, используя A_3 , этот фрагмент переведем в 0, и мы переходим к пункту (1).

Теперь можно предполагать, что формула $\mathfrak{A}$ не содержит нулей и умножений слева, т. е. имеет вид

$$(\dots(x_{i_1} \cdot x_{i_2}) \cdot x_{i_3} \dots) \cdot x_{i_\mu}.$$

Далее рассматриваются формулы, в которых умножение совершается только справа. В этом случае, если опустить скобки, то запись принимает следующий вид:

$$x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_\mu}.$$

Допустим, что в формуле имеются повторные вхождения переменных и x_{i_s}, x_{i_r} — пара повторяющихся переменных, т. е. $x_{i_r} = x_{i_s}$ (где $s < r$),

такая, что между переменными x_{i_r} и x_{i_s} встречаются переменные из множества $\{x_1, \dots, x_n\} \setminus \{x_{i_s}\}$ не более одного раза каждая.

(3) $x_{i_s} = x_{i_1}$. Тогда применимо правило B_m с $m \leq n$, и мы приходим к случаю (1).

(4) $x_{i_s} \neq x_{i_1}$. Тогда, обозначив через u начальный кусок произведения $x_{i_1} \cdot \dots \cdot x_{i_{s-1}}$, получим

$$u \cdot x_{i_s} \cdot x_{i_{s+1}} \cdot \dots \cdot x_{i_r} \cdot \dots, \quad \text{где } x_{i_s} = x_{i_r},$$

и мы можем к этой подформуле применить правило C_m , где $m \leq n$. В результате исчезнет вхождение x_{i_r} .

Совершая указанные преобразования, мы получим либо $x_i \cdot x_i$, либо $x_{i_1} \cdot \dots \cdot x_{i_\mu}$, где множители не повторяются. Теперь остается показать, что при помощи тех же тождеств возможно осуществить эквивалентное преобразование одной канонической формулы в любую другую каноническую формулу, ей эквивалентную. Здесь мы имеем два случая.

(1) $f_{\mathfrak{A}} \equiv 0$. Пусть формула $\mathfrak{A}$ имеет два канонических вида: $x_i \cdot x_i$ и $x_j \cdot x_j$. Очевидно, используя A_1 и A_2 , получим

$$x_i \cdot x_i = (x_i \cdot x_i) \cdot (x_j \cdot x_j) = x_j \cdot x_j.$$

(2) $f_{\mathfrak{A}} \neq 0$. Докажем, что каноническая форма имеет единственный вид. Пусть формула $\mathfrak{A}$ допускает два канонических представления

$$x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_\mu}, \quad (\text{I})$$

$$x_{j_1} \cdot x_{j_2} \cdot \dots \cdot x_{j_\nu}. \quad (\text{II})$$

(а) Оба произведения состоят из одних и тех же множителей. Допустим, что это не так и $x_{j_s} \notin I$. Тогда полагаем

$$x_{i_1} = 1, \quad x_{i_2} = \dots = x_{i_\mu} = 2,$$

а остальные переменные равны 0. В этом случае первое произведение равно $1 \cdot 2 \cdot \dots \cdot 2 = 1$, а второе равно 0, так как содержит $x_{j_s} = 0$. Это противоречит эквивалентности (I) и (II). Таким образом, $\nu = \mu$ и состав множителей в (I) и (II) одинаков.

(б) $x_{j_1} = x_{i_1}$. Если это не так, то полагаем опять

$$x_{i_1} = 1, \quad x_{i_2} = \dots = x_{i_\mu} = 2.$$

Тогда (I) = $1 \cdot 2 \cdot \dots \cdot 2 = 1$ и (II) = $2 \cdot \dots \cdot 1 \cdot \dots \cdot 2 = 0$. Получаем противоречие.

(с) Порядок множителей в (I) и (II) одинаковый. Допустим, что это не так. Тогда найдутся такие множители x_{i_s} и x_{i_r} , что $s < r$, а во втором произведении множитель x_{i_r} предшествует множителю x_{i_s} . В этом случае полагаем $x_{i_1} = 1$, $x_{i_s} = 3$, $x_{i_r} = 4$, а остальные переменные равными 2. Тогда

$$(I) = 1 \cdot \dots \cdot 2 \cdot 3 \cdot 2 \cdot \dots \cdot 2 \cdot 4 \cdot 2 \cdot \dots \cdot 2 = 5,$$

$$(II) = 1 \cdot \dots \cdot 2 \cdot 4 \cdot 2 \cdot \dots \cdot 2 \cdot 3 \cdot 2 \cdot \dots \cdot 2 = 6,$$

что противоречит эквивалентности (I) и (II).

Теорема доказана.

С л е д с т в и е. Система тождеств $A_{1,2,3}, B_m, C_m$ ($m = 1, 2, \dots$) является полной системой тождеств для $\mathfrak{P}$.

Теперь перейдем к изучению полных систем тождеств для $\mathfrak{P}$.

О п р е д е л е н и е. Формула $\mathfrak{A}$ из $\mathfrak{P}$ обладает свойством C^n , если:

- 1) $\mathfrak{A}$ содержит символы $x_1, x_2, \dots, x_n$;
- 2) $\mathfrak{A}$ не имеет подформулы вида $u \cdot u$ и $u \cdot (v \cdot w)$;
- 3) пусть $\mathfrak{A} = x_{i_1} \cdot \dots \cdot x_{i_\mu}$ и имеется второе (считая слева) вхождение символа x_{i_1} ; тогда левее этого второго вхождения встречаются все символы переменных $x_1, \dots, x_n$.

В остальных случаях $\mathfrak{A}$ не удовлетворяет свойству C^n .

П р и м е р. Левая часть тождества B_n удовлетворяет свойству C^n .

Л е м м а 14. Если формула $\mathfrak{A}$ удовлетворяет свойству C^n и $\mathfrak{B}$ получена из $\mathfrak{A}$ при помощи тождеств $A_{1,2,3}, B_m$ и C_m , где $m < n$, то формула $\mathfrak{B}$ также удовлетворяет свойству C^n .

Д о к а з а т е л ь с т в о. Очевидно, для установления леммы достаточно рассмотреть случай, когда $\mathfrak{B}$ получается из $\mathfrak{A}$ одной эквивалентной подстановкой. Легко видеть, что тождества $A_{1,2,3}$ применить к $\mathfrak{A}$ нельзя, так как $\mathfrak{A}$ удовлетворяет п. 2 определения свойства C^n и

$$\mathfrak{A} = x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_\mu}.$$

С другой стороны, к $\mathfrak{A}$ нельзя применить правило B_m ($m < n$) из-за того, что левее второго вхождения символа x_{i_1} встречаются все символы переменных $x_1, \dots, x_n$. Таким образом, к $\mathfrak{A}$ можно применить только тождества C_m ($m < n$), которые уничтожают только повторные вхождения переменных. Поэтому формула $\mathfrak{B}$ будет удовлетворять свойству C^n .

Лемма доказана.

С л е д с т в и е. Эквивалентность B_n

$$((\dots(x_1 \cdot x_2) \cdot x_3 \dots) \cdot x_n) \cdot x_1 = 0$$

нельзя получить при помощи тождеств $A_{1,2,3}, B_m, C_m$ ($m < n$).

В самом деле, левая часть B_n удовлетворяет свойству C^n , а правая нет, а если бы правая часть получалась из левой при помощи указанных тождеств, то по предыдущей лемме она удовлетворяла бы также свойству C^n .

Т е о р е м а 29. Для системы формул $\mathfrak{P}$ не существует конечной полной системы тождеств.

Д о к а з а т е л ь с т в о. Допустим, что система $\mathfrak{P}$ имеет конечную полную систему тождеств

$$\mathfrak{A}'_1 = \mathfrak{A}''_1, \quad \dots, \quad \mathfrak{A}'_r = \mathfrak{A}''_r.$$

Обозначим через n наибольший номер переменного x , встречающегося в этих тождествах. На основании теоремы 28 данная система тождеств может быть получена из системы $\{A_{1,2,3}, B_m, C_m (m \leq n)\}$. В то же время она полная, значит, из нее можно вывести тождество B_{n+1} . Следовательно,

тогда и из системы $\{A_{1,2,3}, B_m, C_m(m \leq n)\}$ можно было бы вывести тождество B_{n+1} , что противоречит следствию предыдущей леммы.

Теорема доказана.

Таким образом, в P_k при $k > 2$ появляются классы $\mathcal{P}$, для которых нет конечной полной системы тождеств.

В то же время, как показывает нижеследующая теорема, если рассматривать не все формулы данного класса, а только те, которые содержат лишь символы переменных $x_1, \dots, x_n$, то для этой системы формул существует конечная полная система тождеств.

Пусть $\mathcal{P}$ замкнутый класс в P_k , имеющий базис $f_1, \dots, f_s$. Рассмотрим произвольную функцию $f(x_1, \dots, x_n) \in \mathcal{P}$ и запишем ее в виде формулы в данном базисе

$$f(x_1, \dots, x_n) = \mathfrak{A}[f_1, \dots, f_s].$$

Эту формулу удобно изобразить в виде дерева, внутренним вершинам которого приписаны базисные функции, а конечным — символы переменных. При этом порядок ветвления вершины, которой соответствует функция f_i , равен аргументности (числу переменных) функции f_i (рис. 57).

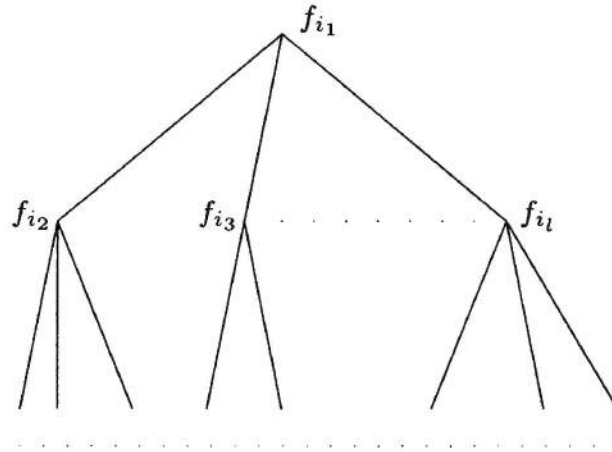


Рис. 57

Очевидно, поддеревьям данного дерева соответствуют подформулы формулы $\mathfrak{A}$. Рассмотрим произвольную ветвь этого дерева. Она, очевидно, определяет цепочку вложенных друг в друга подформул формулы $\mathfrak{A}$

$$\mathfrak{A}' \supseteq \mathfrak{A}'' \supseteq \dots \supseteq \mathfrak{A}^{(r)},$$

причем $\mathfrak{A}' = \mathfrak{A}$.

О п р е д е л е н и е. Формула $\mathfrak{A}$ называется тупиковой, если каждая ее цепочка подформул состоит из попарно не эквивалентных формул.

Обозначим через $\mathfrak{P}_n$ класс всех формул $\mathfrak{A}$ над множеством переменных $x_1, \dots, x_n$. Очевидно, что в тупиковой формуле из $\mathfrak{P}_n$ каждая цепочка подформул содержит не более k^{k^n} членов. Отсюда вытекает, что $\mathfrak{P}_n$ содержит конечное число тупиковых формул.

Пусть $\mathcal{A}$ есть формула из $\mathfrak{P}_n$, обладающая тем свойством, что $\mathcal{A}$ не является тупиковой формулой, а каждая ее собственная подформула является тупиковой.

Данное множество формул обозначим через $\mathfrak{P}_n^0$. Очевидно, что каждая формула $\mathcal{A}$ из $\mathfrak{P}_n^0$ содержит подформулу $\mathcal{A}^0$, эквивалентную $\mathcal{A}$, и в каждой цепочке ее подформул содержится не более одной подформулы, эквивалентной $\mathcal{A}$. Отсюда вытекает, что все цепочки из $\mathcal{A}$ содержат каждая не более $k^{k^n} + 1$ членов и что $\mathfrak{P}_n^0$ конечно.

Т е о р е м а 30. *Класс $\mathfrak{P}_n$ имеет конечную полную систему тождеств.*

Д о к а з а т е л ь с т в о. Для каждой формулы $\mathcal{A} \in \mathfrak{P}_n^0$ выберем любую подформулу $\mathcal{A}^0$, эквивалентную $\mathcal{A}$, и рассмотрим систему тождеств

$$\{\mathcal{A} \sim \mathcal{A}^0\}.$$

Она, очевидно, конечна. Покажем, что каждую формулу $\mathcal{A}'$ из $\mathfrak{P}_n$ можно при помощи этой системы тождеств преобразовать в эквивалентную ей тупиковую формулу. Для этого рассмотрим дерево для формулы $\mathcal{A}'$. Если $\mathcal{A}'$ — тупиковая формула, то утверждение тривиально. В противном случае найдется подформула $\mathcal{A}$, которая принадлежит $\mathfrak{P}_n^0$. В формуле $\mathcal{A}'$ заменим подформулу $\mathcal{A}$ на $\mathcal{A}^0$, тогда мы получим формулу $\mathcal{A}''$, эквивалентную $\mathcal{A}'$ и содержащую меньшее число подформул, и т. д. В конце концов через конечное число шагов мы получим тупиковую формулу, эквивалентную $\mathcal{A}'$ (канонический вид исходной формулы).

Далее добавим всевозможные тождества, являющиеся парами эквивалентных тупиковых формул (очевидно, конечное множество). Эта система тождеств позволяет осуществить переход от одного канонического вида к любому ему эквивалентному.

Теорема доказана.

§ 3. Эквивалентные преобразования схем из функциональных элементов

Этот параграф начнем с некоторых замечаний, касающихся понятия схемы из Ф.Э. [14].

1. Так как при эквивалентных преобразованиях схем из Ф.Э. промежуточные объекты могут оказаться не схемами из Ф.Э., то несколько расширим понятие схемы из Ф.Э. А именно, мы допускаем:

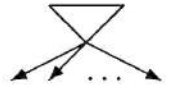
- (а) добавление изолированных входных полюсов;
- (б) наличие выходов, которым не приписаны символы выходного алфавита (выходы, не являющиеся полюсами);
- (с) схемы без выходных полюсов.

При этом естественным образом доопределяется и функционирование схемы: от переменного, приписанного изолированному входу, каждый выход зависит несущественным образом; функционирование на выходах, не являющихся полюсами, не определяется.

2. Определение схемы из Ф.Э. нами дано в геометрической форме. Благодаря этому обеспечивается наглядность объекта, но зато возникает

элемент неопределенности (который может быть полностью устранен, если исходить из абстрактного определения схемы). Поэтому мы вынуждены сделать некоторые оговорки, касающиеся стандартизации изображения схем (см. табл. 8).

Т а б л и ц а 8

	изолированный вход схемы
	вход схемы, совмещенный со входом элемента
	выход схемы, совпадающий со входом схемы
	ветвление выхода элемента
	выход элемента, не являющийся выходом схемы
	выход схемы, совмещенный с выходом элемента

Далее уточним основные понятия, связанные с эквивалентными преобразованиями.

1. Схемы

$$\Sigma' = \Sigma'(x_1, \dots, x_n, z_1, \dots, z_p) \quad \text{и} \quad \Sigma'' = \Sigma''(x_1, \dots, x_n, z_1, \dots, z_p)$$

называются эквивалентными, если уравнения

$$\begin{cases} z_1 = f'_1(x_1, \dots, x_n), \\ \dots\dots\dots \\ z_p = f'_p(x_1, \dots, x_n) \end{cases} \quad \text{и} \quad \begin{cases} z_1 = f''_1(x_1, \dots, x_n), \\ \dots\dots\dots \\ z_p = f''_p(x_1, \dots, x_n), \end{cases}$$

описывающие их функционирование, имеют равные правые части, т. е.

$$\begin{aligned} f'_1(x_1, \dots, x_n) &= f''_1(x_1, \dots, x_n), \\ &\dots\dots\dots \\ f'_p(x_1, \dots, x_n) &= f''_p(x_1, \dots, x_n). \end{aligned}$$

Схемы с одинаковыми входами и без выходных полюсов считаются эквивалентными.

2. Пусть Σ_1 есть часть схемы Σ' , которая является схемой из Ф.Э., тогда она называется подсхемой схемы Σ' . При этом полюсами (входными и выходными) подсхемы Σ_1 являются полюса исходной схемы Σ' , попавшие в Σ_1 , а также вершины (связи), соединяющие Σ_1 с остальной частью схемы, и некоторые выходы элементов из Σ_1 .

3. Операция подстановки состоит в замене подсхемы Σ_1 на схему Σ_2 , у которой такое же число входов и выходов, как и у Σ_1 .

4. В случае, если Σ_2 эквивалентна Σ_1 и подстановка согласована с соответствием полюсов при их эквивалентности, то мы имеем эквивалентную подстановку. Для схем из Ф.Э. справедлив принцип эквивалентной замены.

5. Тождество $\Sigma_1 \sim \Sigma_2$ понимается с точностью до переименования символов из алфавитов X и Z .

Пункты 6–7 определяются как и в общем случае.

Теорема 31 (Горбовицкая [4]). *Для схем из Ф.Э. в базисе из инверторов, конъюнкторов и дизъюнкторов существует конечная полная система тождеств.*

Доказательство. Построение системы тождеств и доказательство ее полноты производятся одновременно. Основная идея стандартная — приведение схемы к каноническому виду и установление возможности преобразования эквивалентных канонических видов друг в друга. Пусть $\Sigma = \Sigma(x_1, \dots, x_n, z_1, \dots, z_p)$ — схема из Ф.Э. и ее функционирование описывается системой уравнений

$$\begin{cases} z_1 = f_1(x_1, \dots, x_n), \\ \dots\dots\dots \\ z_p = f_p(x_1, \dots, x_n). \end{cases}$$

Определим понятие канонического вида, эквивалентного Σ . Для этого возьмем i -ю строку

$$z_i = f_i(x_1, \dots, x_n)$$

и построим схему $\Sigma_i^0(x_1, \dots, x_n, z_i)$, которая при $f_i \equiv 0$ совпадает со схемой, изображенной на рис. 58, а при $f_i \neq 0$ соответствует совершенной д.н.ф. функции f_i . Канонический вид Σ^0 получается путем склейки входов схем Σ_i^0 .

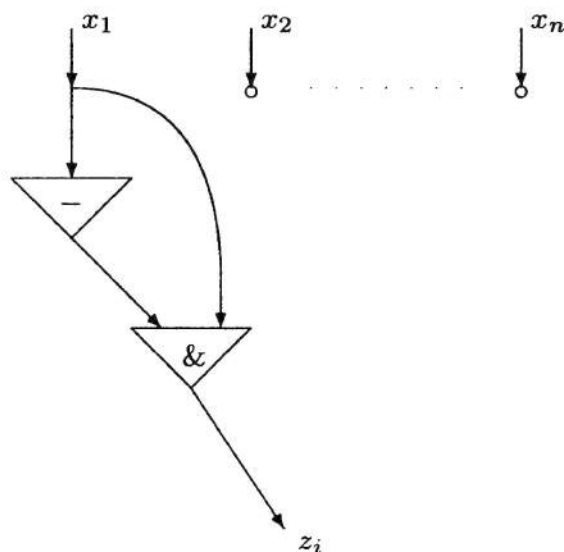


Рис. 58

I этап. Осуществляются преобразования, уничтожающие ветвления на выходах элементов. Для этого используются правила¹⁴ (рис. 59).

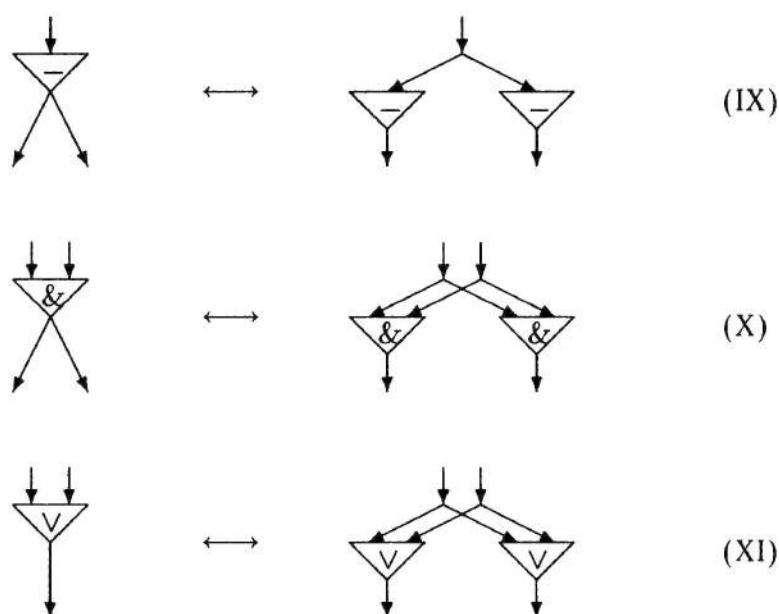


Рис. 59

Очевидно, что в конце I этапа получается схема, эквивалентная исходной, и содержащая разветвления только на входах. Эту схему можно рассматривать как p схем, склеенных на входах, каждая из которых изоморфна формуле в базисе $\{ -, \&, \vee \}$.

II этап. Преобразование схемы, не имеющей ветвлений на выходах элементов, к каноническому виду. Для этого используются результаты по эквивалентным преобразованиям формул в базисе $\{ -, \&, \vee \}$. На рис. 60 представлены графические аналоги правил (I)–(VIII) для преобразования формул.

Данные тождества формально уже, чем соответствующие тождества в алгебре логики, так как здесь нет правила подстановки. Однако косвенно подстановка в схемах присутствует в виде подсхем, подключенных на входы преобразуемой подсхемы.

Чтобы «смоделировать» приведение к каноническому виду формул на схемах из функциональных элементов надо иметь в виду следующие два обстоятельства:

- в результате применения правила (III) могут возникнуть ветвления на выходах элементов;
- при применении правил (VI) и (VII) появляются вершины, не являющиеся выходами.

В обоих случаях мы при помощи указанных правил выходим из класса «формул». Чтобы снова вернуться в класс формул, в первом случае используют правила, уничтожающие ветвления на выходах элемен-

¹⁴Здесь и далее в правилах опускаются символы из алфавитов X и Z .

тов (см. I этап), во втором случае при помощи дополнительных правил (XII)–(XIV) (рис. 61) постепенно удаляют «лишние» элементы.

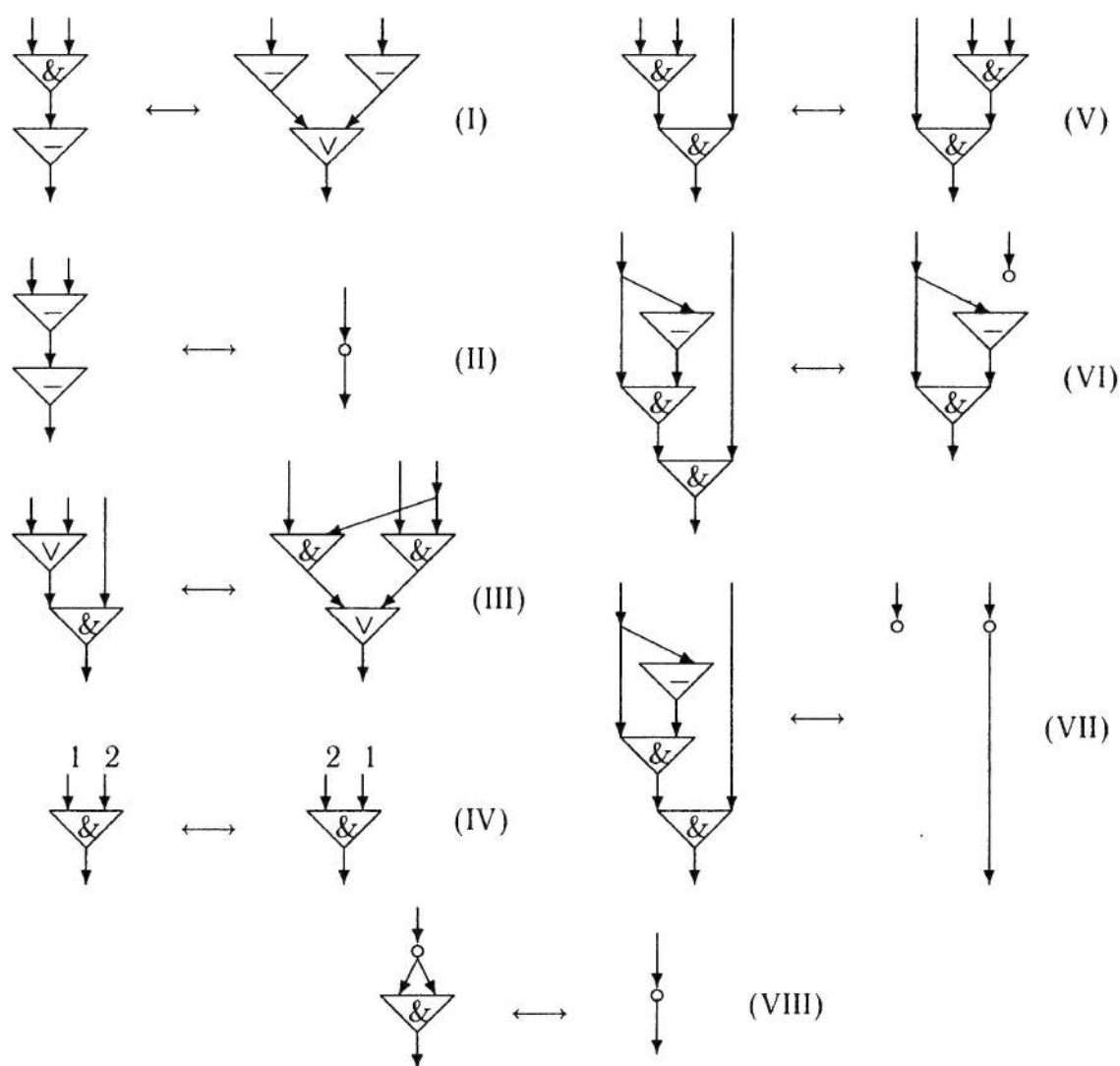


Рис. 60

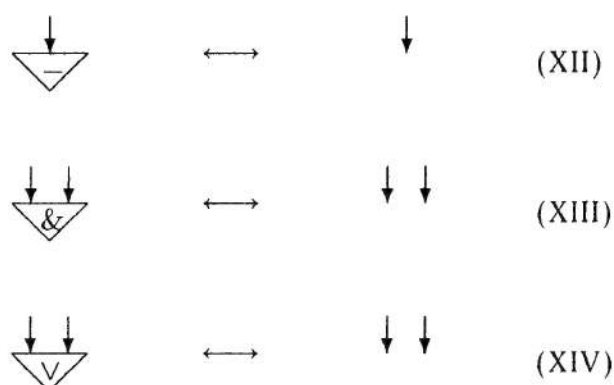


Рис. 61

Перевод эквивалентных канонических видов друг в друга осуществляется теми же правилами в точности так же, как у формул.

Теорема доказана.

§ 4. Эквивалентные преобразования контактных схем

Кратко коснемся основных моментов, связанных с преобразованиями контактных схем [17].

1. Контактные схемы Σ' и Σ'' называются эквивалентными, если существует взаимно однозначное соответствие T между их полюсами, такое, что матрицы

$$\|f'_{ij}\| \quad \text{и} \quad T\|f''_{ij}\|T^{-1}$$

равны, т. е. состоят из соответственно равных функций.

2. Подмножество Σ_1 , состоящее из некоторых вершин схемы Σ' и части контактов, их соединяющих, называется подсхемой схемы Σ' , если в нем выделены полюса так, что:

(а) если вершина из Σ_1 является полюсом в Σ' , то она является также полюсом и Σ_1 ;

(б) если вершина из Σ_1 инцидентна (т. е. является концом) контакту из $\Sigma' \setminus \Sigma_1$, то она является полюсом в Σ_1 ;

(с) некоторое подмножество вершин из Σ_1 (может быть и пустым) считается полюсами Σ_1 .

Для полюсов из Σ_1 выбирается некоторая нумерация.

3. Операция подстановки определяется как и в общем случае.

4. Если контактные схемы Σ_1 и Σ_2 эквивалентны и T — взаимно однозначное соответствие их полюсов, обеспечивающее эквивалентность, и Σ_1 есть подсхема Σ' , то подстановка вместо Σ_1 схемы Σ_2 , согласованная с T , будет эквивалентной подстановкой. Из содержательных соображений ясно, что для контактных схем верен принцип эквивалентной замены: пусть Σ'' — результат эквивалентной подстановки, тогда схемы Σ' и Σ'' эквивалентны. Впрочем, принцип эквивалентной замены для контактных схем может быть и строго доказан.

5. Тождество $\Sigma_1 \longleftrightarrow \Sigma_2$ понимается с точностью до:

(а) согласованных перенумераций полюсов;

(б) согласованных переименований и отождествлений переменных;

(с) согласованных замен для некоторых i

$$x_i \rightarrow \bar{x}_i \quad \text{и} \quad \bar{x}_i \rightarrow x_i.$$

Остальные пункты формулируются так же, как и в общем случае.

На рис. 62 приведены очевидные тождества 1–5 и 6_m ($m = 1, 2, \dots$). Здесь через $\bullet$ обозначена изолированная вершина, не являющаяся полюсом, через $\circ$ — полюс. Кроме того, в правилах 3 и 5 допускается совпадение вершин.

Для дальнейшего полезно развить некоторые навыки к эквивалентным преобразованиям контактных схем. Здесь характер преобразований существенно непохож на способы преобразования формул. Например, в случае контактных схем имеется правило 5, в котором фигурируют трехполюсные схемы, а также есть правила 1, 6_m топологического характера:

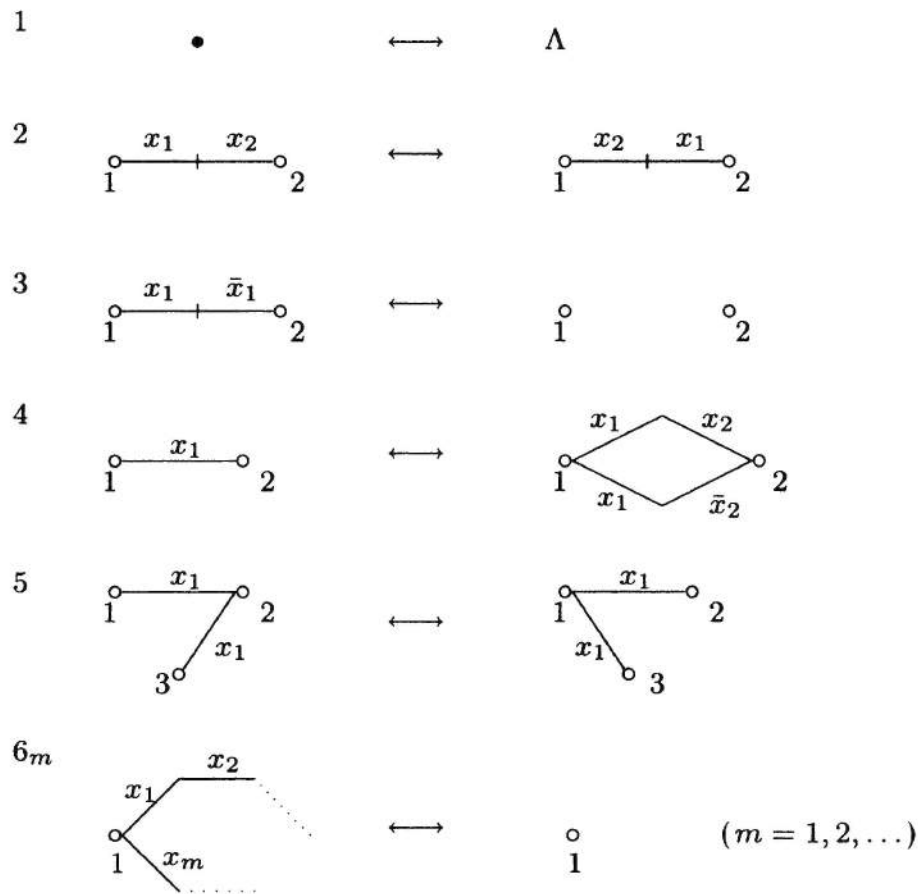


Рис. 62

отбрасывание изолированной вершины и удаление цикла, проходящего через полюсную вершину и не имеющего других полюсов. Именно поэтому мы покажем, что тождества 7 (удаление отростка, состоящего из одного ребра), 8 (уничтожение дублирования контактов при последовательном соединении) и 9 (расклейка, склейка двух «соседних» цепей) (рис. 63) могут быть получены при помощи эквивалентных преобразований из 1–5, 6₁, 6₂.

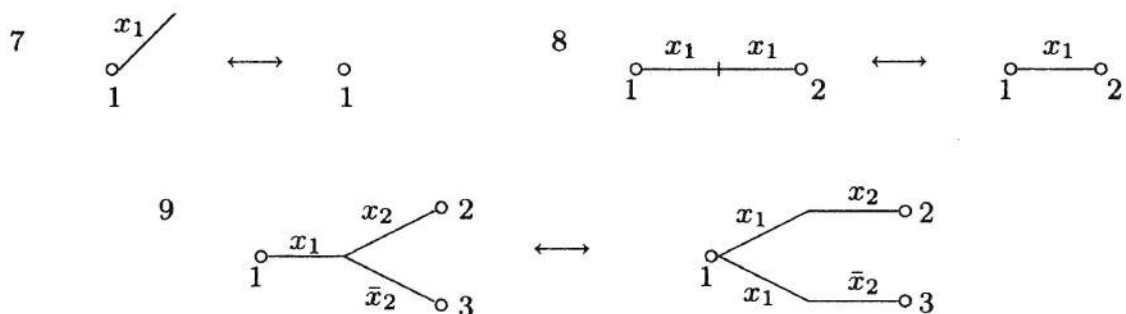


Рис. 63

В самом деле, мы имеем цепочки эквивалентных преобразований (рис. 64). На нем пунктиром помечены подсхемы, на места которых производится подстановка. Номер подстановки приписывается стрелке, стоящей справа от схемы.

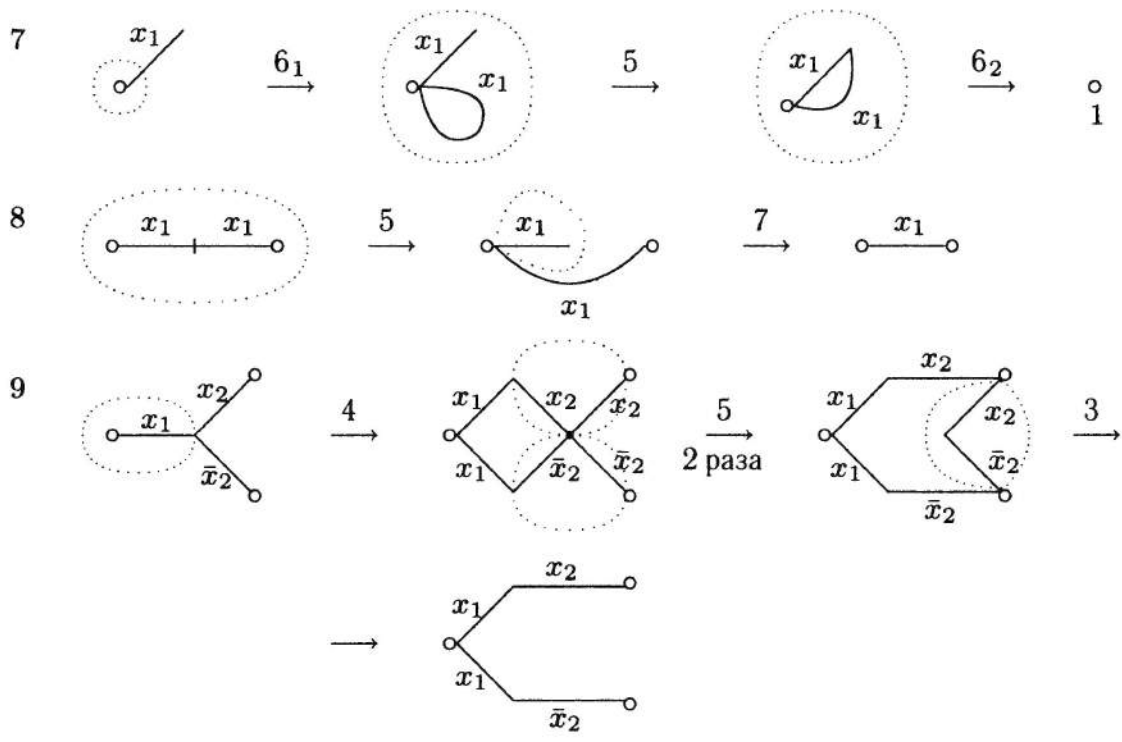


Рис. 64

Тождество 9 может быть обобщено на случай расклейки (склейки) двух соседних цепочек длины n , тождество 9_n (рис. 65).

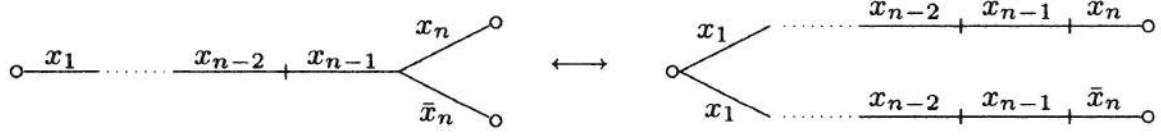


Рис. 65

Доказательство по индукции. При $n = 2$ тождество 9_2 совпадает с 9. Индуктивный переход показан на рис. 66.

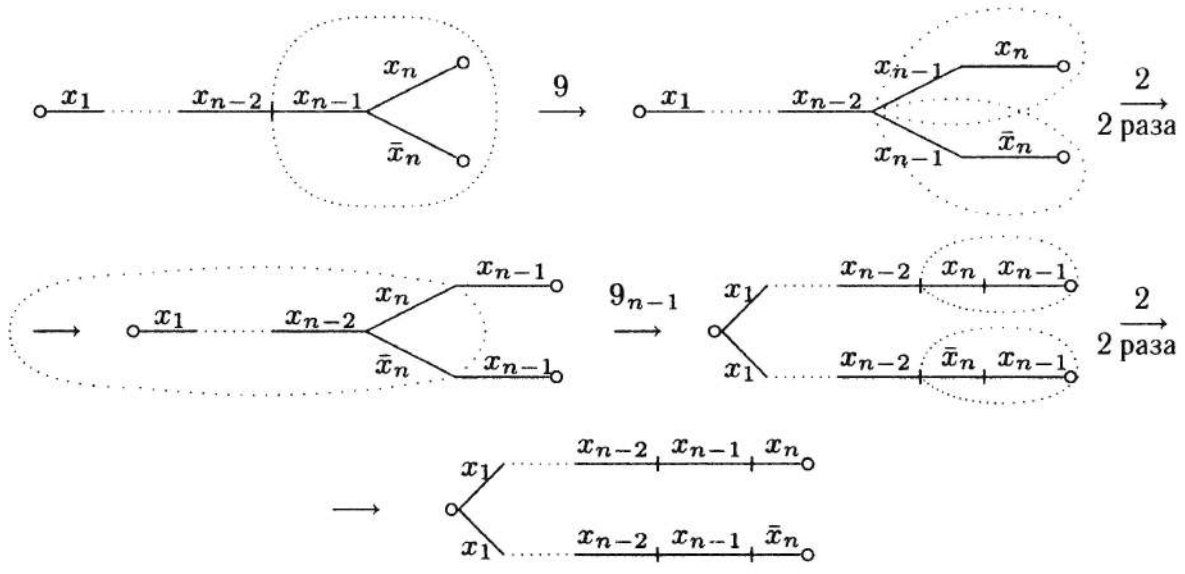


Рис. 66

Рассмотрим далее вспомогательные тождества I–VII. В них и в последующих тождествах обозначены через

I_i , где $i = i(\sigma_1, \dots, \sigma_n)$ — номер набора $(\sigma_1, \dots, \sigma_n)$,

I'_i , где $i = i(\sigma_2, \dots, \sigma_n)$ — номер набора $(\sigma_2, \dots, \sigma_n)$,

I''_i , где $i = i(\sigma_3, \dots, \sigma_n)$ — номер набора $(\sigma_3, \dots, \sigma_n)$,

соответственно цепочки контактов (рис. 67), а символ I обозначает цепочку, соответствующую конъюнкции $x_1 \& \dots \& x_n$.

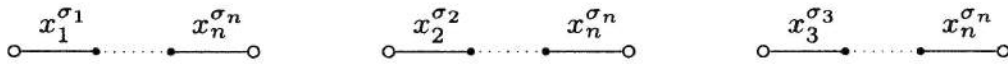


Рис. 67

На рис. 68 приведены вспомогательные тождества.

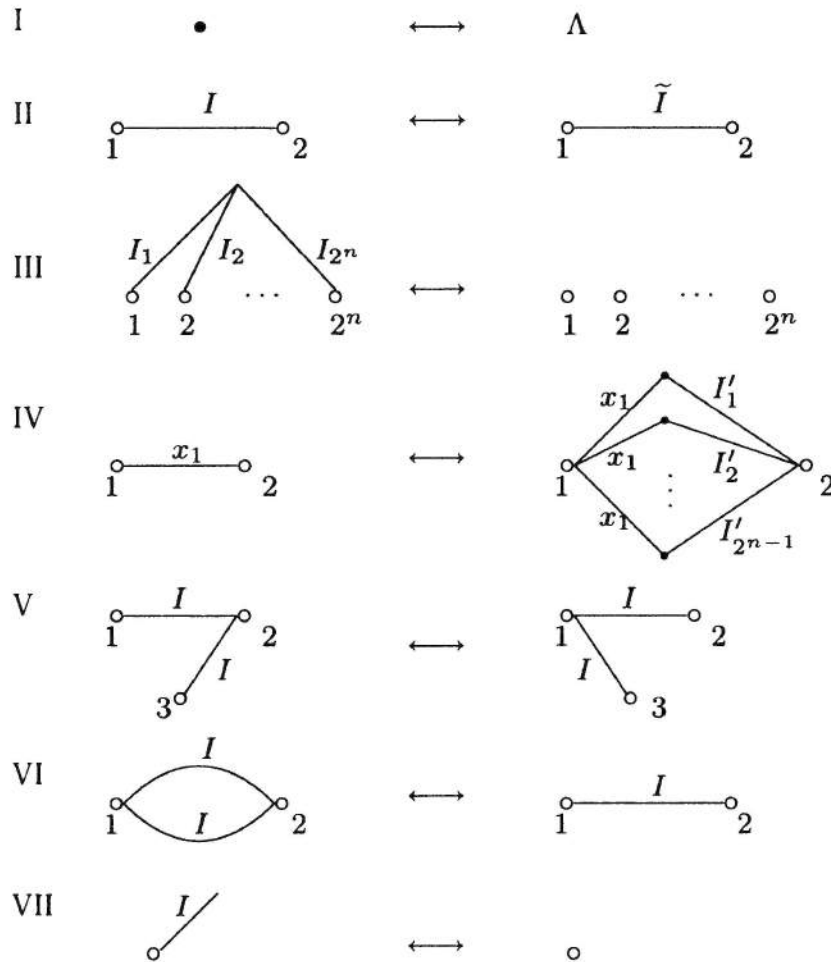


Рис. 68

Здесь через $\tilde{I}$ обозначена произвольная перестановка контактов в I (фактически, правило II — семейство правил для всевозможных перестановок). Кроме того, в правиле III допускаются любые отождествления полюсов.

Ясно, что тождества I–VII выполняются. Однако эту проверку можно не производить, поскольку справедлива следующая лемма.

Лемма 15. Тождества I–VII могут быть получены из тождеств 1–5, 6_m ($m \leq n$) при помощи эквивалентных преобразований.

Доказательство. Тожество I совпадает с тождеством 1.

Тожество II получается многократным применением 2.

Тожество III доказывается по индукции. Для $n = 1$ оно совпадает с тождеством 3. Пусть утверждение справедливо для $r = 1, \dots, n - 1$. Докажем его для $r = n$. Рассмотрим следующую нумерацию наборов (см. табл. 9).

Таблица 9

$x_n \dots x_2 x_1$	i
0 ... 0 0	1
0 ... 0 1	2
0 ... 1 0	3
0 ... 1 1	4
.....	...
1 ... 1 0	2^{n-1}
1 ... 1 1	2^n

Разобьем цепочки схемы из левой части тождества III на пары, соседние по переменному x_1 . Мы получим $(I_1, I_2), (I_3, I_4), \dots, (I_{2^{n-1}-1}, I_{2^n})$. Тогда вывод тождества III для $r = n$ сводится к многократному применению процедуры (9_n) склейки соседних цепей, использованию индуктивного предположения и многократному использованию тождества 3 (рис. 69).

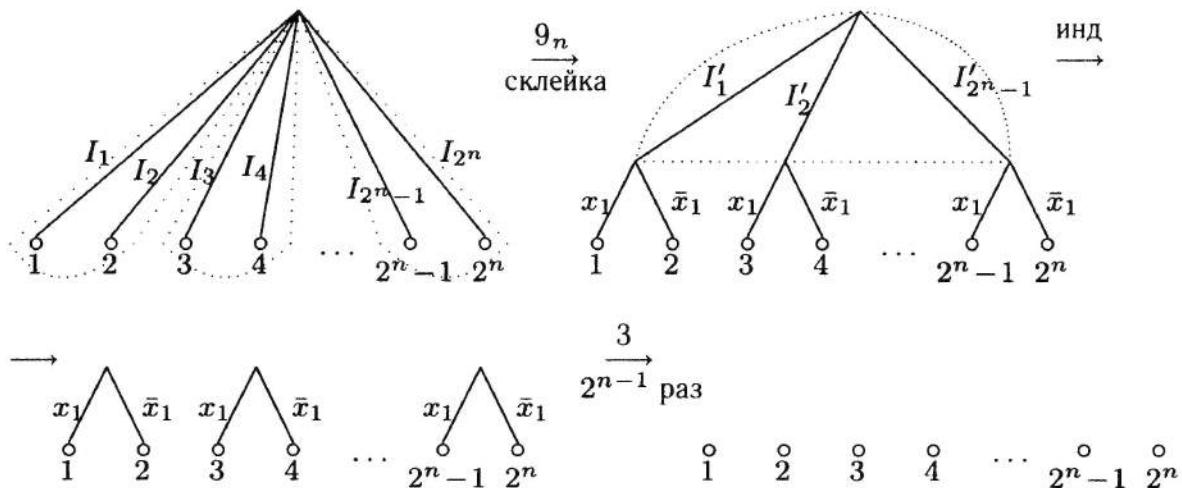


Рис. 69

Тожество IV доказываем индуктивно. При $n = 2$ оно совпадает с 4. Индуктивный переход изображен на рис. 70.

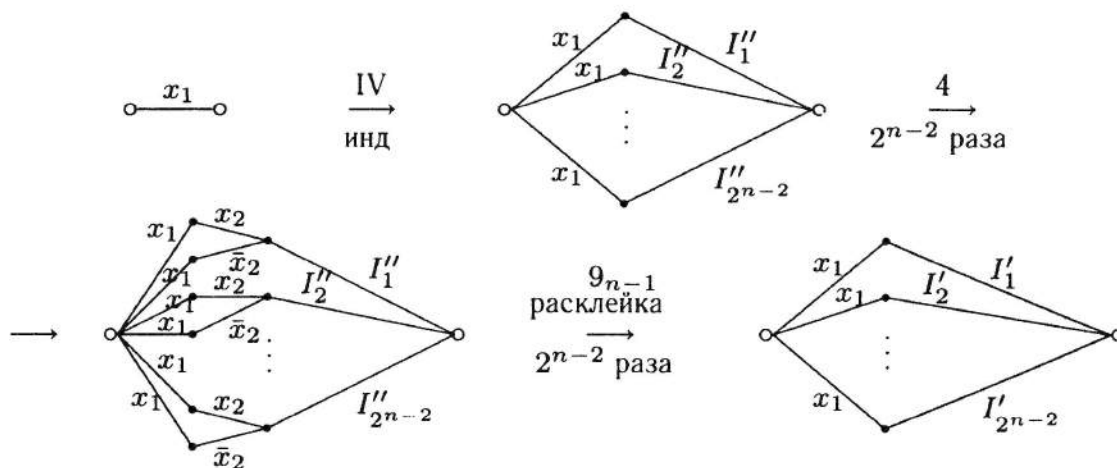


Рис. 70

Тождество V доказываем по индукции. При $n = 1$ оно совпадает с 5. Индуктивный переход изображен на рис. 71.

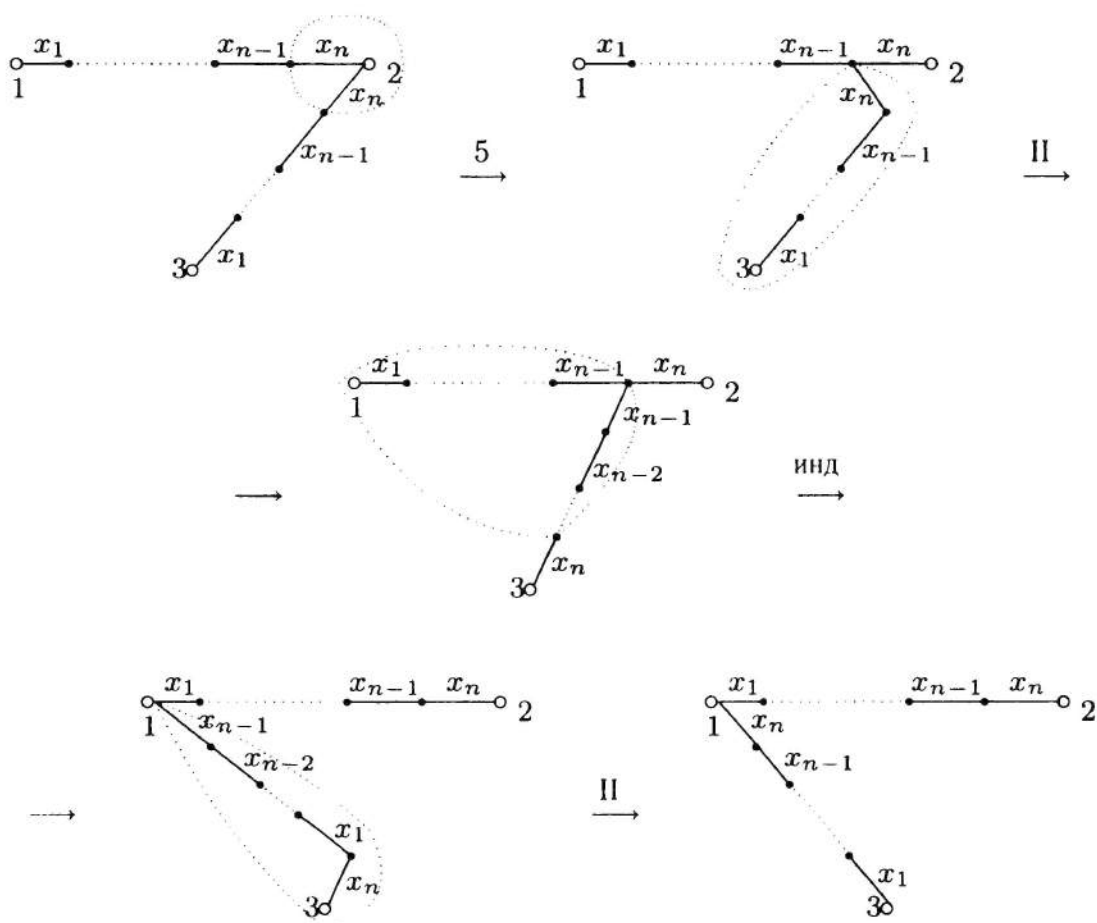


Рис. 71

Тождество VI выводится путем многократного использования тождеств 5 и II, а также 6_n (рис. 72).

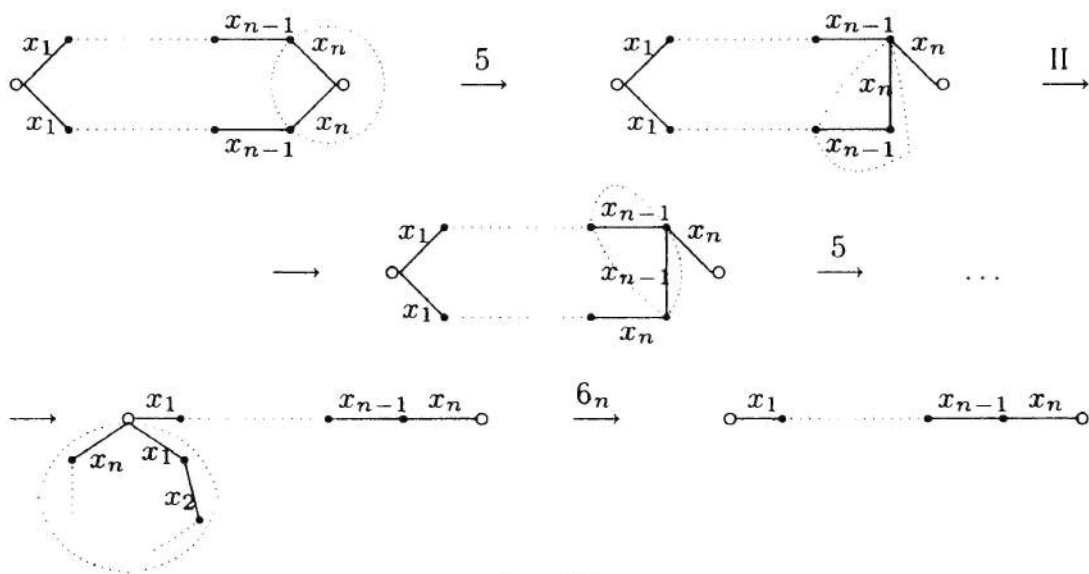


Рис. 72

Тождество VII может быть получено многократным применением 7. Лемма доказана.

З а м е ч а н и е. Тожество III может быть обобщено на случай произвольной склейки полюсов и на случай, в котором присутствуют не все цепочки длины n (рис. 73).

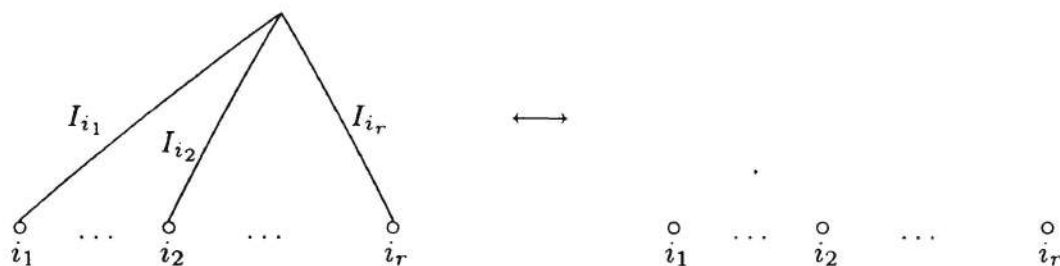


Рис. 73

Доказательство последнего использует многократное применение VII, в результате чего добавляются недостающие цепочки, затем применяется правило III, потом при помощи I удаляются изолированные вершины (рис. 74).

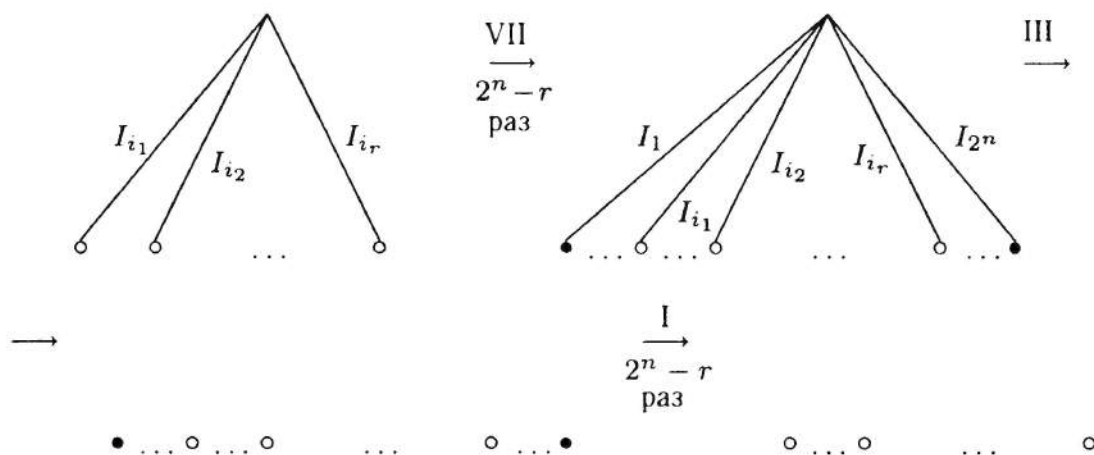


Рис. 74

Л е м м а 16 (о звезде). Тожества, представленные на рис. 75, выводимы из I–VII.

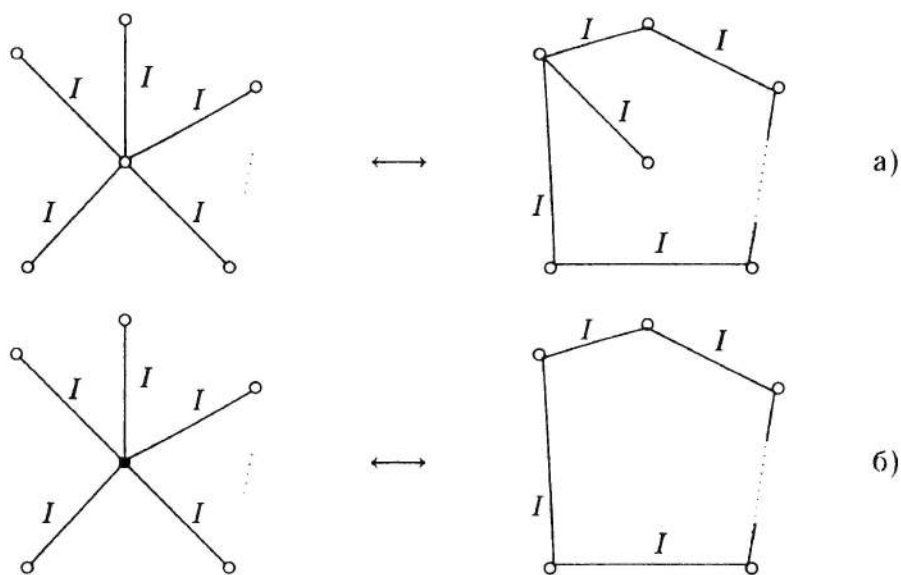


Рис. 75

Доказательство. Рассмотрим первое из них (имеющее центр звезды в качестве полюса). Далее установим его справедливость путем применения правила VI и многократного применения V (рис. 76).

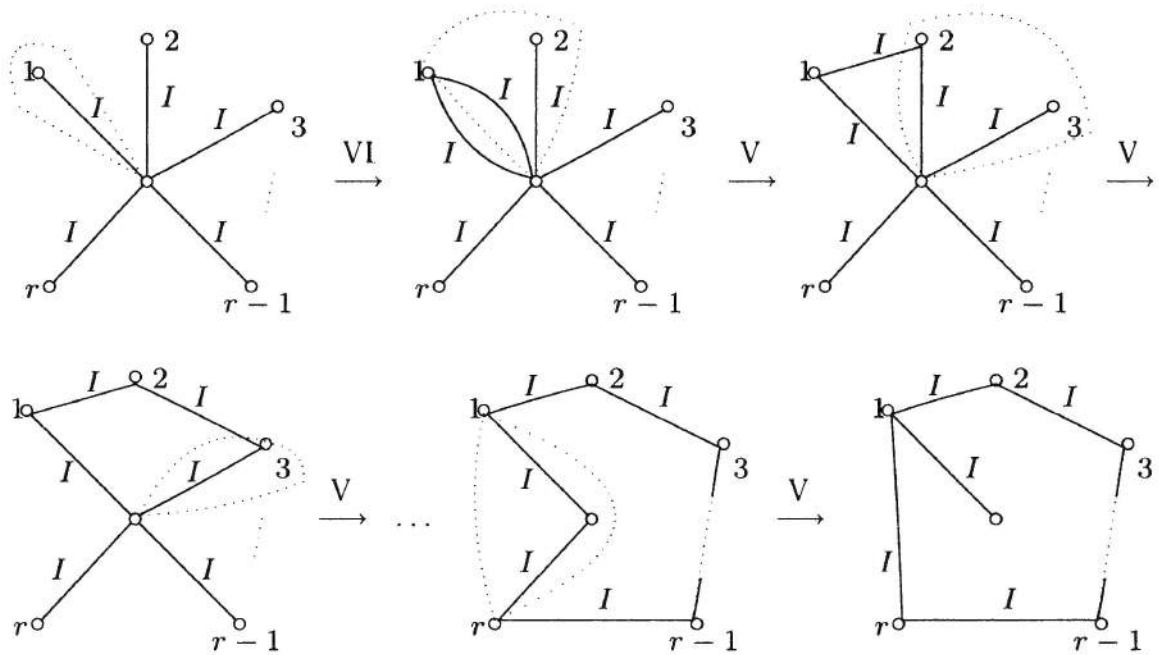


Рис. 76

Второе тождество доказывается с использованием первого и правила VII. Тождество б) о преобразовании звезды в контур является аналогом в дискретном варианте хорошо известного преобразования в электротехнике.

Теорема 32 (Мурский [17]). Если Σ' и Σ'' — две эквивалентных s -полюсных контактных схемы над $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$, то существует эквивалентное преобразование Σ' в Σ'' при помощи тождеств 1–5, 6_m ($m \leq n$).

Доказательство. Сначала определим каноническую форму для схемы Σ над $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$. Пусть $\|f_{ij}(x_1, \dots, x_n)\|$ — ее матрица проводимости. Возьмем s вершин, занумерованных числами $1, 2, \dots, s$, в качестве полюсов определяемой схемы. Возьмем произвольные полюса i и j и рассмотрим $f_{ij}(x_1, \dots, x_n)$. Если $f_{ij} \equiv 0$, то никаких построений не делаем. Если $f_{ij} \neq 0$, то по совершенной д.н.ф.

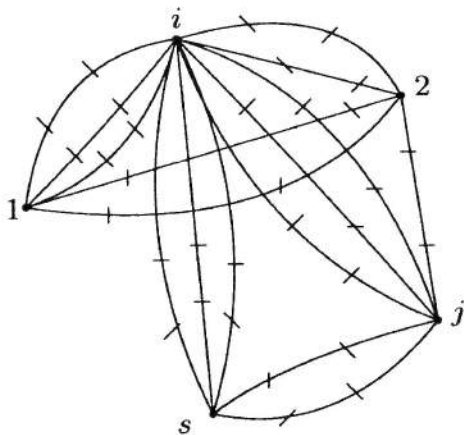


Рис. 77

$$f_{ij}(x_1, \dots, x_n) = \bigvee_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\sigma_1, \dots, \sigma_n)=1}} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n}.$$

Между этими полюсами подключим контактную схему, соответствующую данной д.н.ф. Данную операцию проделаем для всех пар i и j (рис. 77).

Полученная схема Σ_0 , являющаяся каноническим видом схемы Σ , состоит из цепочки длины n , соединяющих полюса, и имеет ту же матрицу проводимости.

Докажем, что при помощи тождеств 1–5, 6_m ($m \leq n$) схему Σ можно «привести» (т. е. преобразовать) к каноническому виду Σ_0 . Для этого достаточно установить, что приведение можно осуществить при помощи вспомогательных правил I–VII. Процесс разбивается на несколько этапов.

1. В схеме Σ каждый контакт $x_i^{\sigma_i}$ заменим, пользуясь правилом IV, на двухполюсную подсхему (см. рис. 68), состоящую из цепочек длины n . Получим схему Σ_1 , состоящую из цепочек, соединяющих некоторые вершины.

2. Пусть a — вершина в Σ_1 , являющаяся концом некоторой цепочки, и a не есть полюс Σ_1 . Покажем, что при помощи правил I–VII ее можно исключить. Рассмотрим звезду из цепочек имеющих своим центром вершину a . Пусть $I_{i_1}, \dots, I_{i_r}$ — различные сорта цепочек из этой звезды. В этой звезде выделим подзвезду из цепочек i_ν -го сорта и к этой подсхеме применим лемму о звезде. В результате этого в исходной звезде останется одна цепочка вида I_{i_ν} , остальные дубликаты I_{i_ν} отойдут на периферию ($\nu = 1, \dots, r$; рис. 78). После этого применяем к преобразованной звезде (а она уже имеет ровно по одному представителю из вышеуказанных сортов цепочек) обобщенное правило III. Этот процесс ведем до тех пор, пока не уничтожим все внутренние вершины, являющиеся концами цепочек. Получим схему Σ_2 .

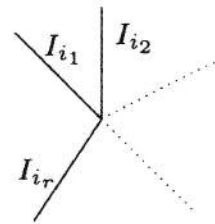


Рис. 78

3. В схеме Σ_2 производим замыкание по транзитивности. Для этого применяем правило, представленное на рис. 79, до тех пор, пока возможно (это правило выводится путем применения VI и V). Обозначим через Σ_3 результат этого замыкания.

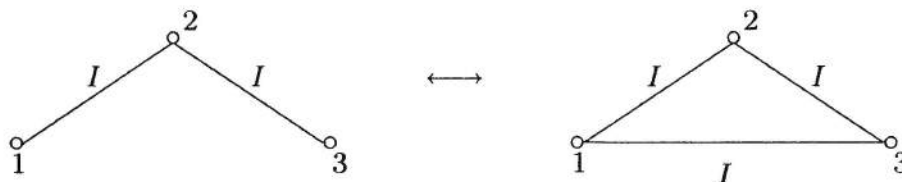


Рис. 79

4. В схеме Σ_3 ликвидируем цепочки, дублирующие друг друга параллельным образом. Для этого используем правило VI. После этого получим искомую схему Σ_0 , являющуюся каноническим видом схемы Σ . Заметим, наконец, что две эквивалентных канонических схемы над $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$ могут различаться лишь порядком контактов в цепочках. Их можно перевести друг в друга при помощи II.

Для завершения доказательства нужно:

- Σ' привести к каноническому виду Σ'_0 ;
- Σ'' привести к каноническому виду Σ''_0 .

Поскольку $\Sigma'_0 \longleftrightarrow \Sigma''_0$, их можно перевести друг в друга, отсюда извлекается искомое эквивалентное преобразование.

Теорема доказана.

С л е д с т в и е. Система правил (тождеств) 1–5, 6_m ($m=1, 2, \dots$) является полной в классе контактных схем.

Далее займемся анализом системы тождеств 1–5, 6_m ($m=1, 2, \dots$). Пусть Σ — контактная схема над $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$. Введем функцию $\varphi_\Sigma(x_1, \dots, x_n)$ следующим образом:

$$\varphi_\Sigma(\alpha_1, \dots, \alpha_n) = p - b + k,$$

где

p — число ребер в графе, получающемся из Σ при подстановке $x_1 = \alpha_1, \dots, x_n = \alpha_n$ (контакт x^σ переходит в ребро, если $x^\sigma = 1$, и выбрасывается, если $x^\sigma = 0$),

b — число вершин данного графа,

k — число связанных компонент этого графа (две вершины принадлежат одной компоненте связности графа, если есть путь в графе, соединяющий эти вершины).

$$\text{Наконец, } \text{Ind } \Sigma = \sum_{(\alpha_1 \dots \alpha_n)} \varphi_\Sigma(\alpha_1, \dots, \alpha_n) \pmod{2}.$$

П р и м е р. Возьмем алфавит $x_1, \dots, x_n, x_{n+1}, \bar{x}_1, \dots, \bar{x}_n, \bar{x}_{n+1}$. Рассмотрим схему Σ_m из 6_m ($m \leq n+1$; рис. 80). Если $m = n+1$ и $\alpha_1 = \dots = \alpha_{n+1} = 1$, то

$$\varphi_{\Sigma_{n+1}}(1, \dots, 1) = (n+1) - (n+1) + 1 = 1.$$

Если $\alpha_i = 0$, $\alpha_1 = \dots = \alpha_{i-1} = \alpha_{i+1} = \dots = \alpha_{n+1} = 1$, то

$$\varphi_{\Sigma_{n+1}}(1 \dots 1 0 1 \dots 1) = n - (n+1) + 1 = 0 \quad (i = 1, \dots, n+1).$$

Когда набор $(\alpha_1, \dots, \alpha_{n+1})$ содержит $d > 1$ нулей, тогда

$$\varphi_{\Sigma_{n+1}}(\alpha_1, \dots, \alpha_{n+1}) = (n+1-d) - (n+1) + d = 0.$$

Отсюда $\text{Ind } \Sigma_{n+1} = 1$. Если $m < n+1$, то $\text{Ind } \Sigma_m = 0$, так как

$$\begin{aligned} \varphi_{\Sigma_m}(\alpha_1, \dots, \alpha_m, \underbrace{0 \dots 0}_{n+1-m}) &= \varphi_{\Sigma_m}(\alpha_1, \dots, \alpha_m, 0 \dots 1) = \dots = \\ &= \varphi_{\Sigma_m}(\alpha_1, \dots, \alpha_m, 1 \dots 1). \end{aligned}$$

Значит,

$$\begin{aligned} \text{Ind } \Sigma_m &= \sum_{(\alpha_1 \dots \alpha_{n+1})} \varphi_{\Sigma_m}(\alpha_1 \dots \alpha_{n+1}) = \\ &= \sum_{(\alpha_1 \dots \alpha_m)} 2^{n+1-m} \varphi_{\Sigma_m}(\alpha_1 \dots \alpha_m 0 \dots 0) = 0 \pmod{2}. \end{aligned}$$

Для схемы Σ_0 — правой части 6_m по тем же причинам $\text{Ind } \Sigma_0 = 0$.

Л е м м а 17. Если Σ' и Σ'' — схемы над алфавитом $x_1, \dots, x_{n+1}, \bar{x}_1, \dots, \bar{x}_{n+1}$ и Σ'' получена из Σ' эквивалентными преобразованиями при помощи тождеств 1–5, 6_m ($m \leq n$, то $\text{Ind } \Sigma'' = \text{Ind } \Sigma'$).

Д о к а з а т е л ь с т в о. Заметим, что если существует эквивалентное преобразование Σ' в Σ'' и некоторые промежуточные схемы зависят от

переменных, не входящих в $x_1, \dots, x_{n+1}$, то можно построить другое эквивалентное преобразование, где все промежуточные схемы зависят только от $x_1, \dots, x_{n+1}$, с употреблением тождеств из 1–5, 6_m ($m \leq n$). Для этого все прочие переменные, участвующие в выводе, следует отождествить, например, с x_1 . При этом каждая эквивалентная подстановка этого вывода

а) либо останется неизменной;

б) либо произойдет в ней согласованное переименование переменных;

в) либо в ней отождествятся некоторые переменные $(2, 4, 6_m)$ — и тогда она или превратится в тавтологию (2), или может быть заменена на комбинацию подстановок из 1–5, 6_m ($m \leq n$), (4), или останется вариантом того же типа подстановки (6_m).

Очевидно, лемма будет доказана, если она будет установлена для частного случая, когда Σ'' получается из Σ' эквивалентной подстановкой из 1–5, 6_m ($m \leq n$). Для этого рассмотрим шесть случаев.

1. Σ'' получена из Σ' при помощи тождества 1. Пусть

$$\begin{aligned}\Delta\varphi &= \varphi_{\Sigma''}(\alpha_1, \dots, \alpha_{n+1}) - \varphi_{\Sigma'}(\alpha_1, \dots, \alpha_{n+1}) = \\ &= (p'' - b'' + k'') - (p' - b' + k') = \Delta p - \Delta b + \Delta k.\end{aligned}$$

Очевидно, мы имеем для тождества 1: $\Delta p = 0$ и $|\Delta\varphi| = |-\Delta b + \Delta k| = 0$. Поэтому $\text{Ind } \Sigma'' = \text{Ind } \Sigma'$.

2. Σ'' получена из Σ' при помощи тождества 2. Здесь, очевидно, $\varphi_{\Sigma''}(\alpha_1, \dots, \alpha_{n+1}) = \varphi_{\Sigma'}(\alpha_1, \dots, \alpha_{n+1})$ для любого набора $(\alpha_1, \dots, \alpha_{n+1})$ и отсюда $\text{Ind } \Sigma'' = \text{Ind } \Sigma'$.

3. Σ'' получена из Σ' при помощи тождества 3. Здесь для каждого набора $\alpha_1, \dots, \alpha_{n+1}$ имеем $\Delta k = 0$ и $\Delta\varphi = \Delta p - \Delta b$, причем при подстановке и p , и b либо одновременно уменьшается на 1, либо увеличивается на 1. Тогда $\Delta\varphi = 0$ и $\text{Ind } \Sigma'' = \text{Ind } \Sigma'$.

4. Σ'' получена из Σ' при помощи тождества 4. Для каждого набора $\alpha_1, \dots, \alpha_{n+1}$, в котором $\alpha_1 = 0$, либо $\Delta p = 1$, $\Delta b = 2$, $\Delta k = 1$, либо $\Delta p = -1$, $\Delta b = -2$, $\Delta k = -1$ (правило применено справа налево). Мы имеем $\Delta\varphi = 0$. Для каждого набора $\alpha_1, \dots, \alpha_{n+1}$, в котором $\alpha_1 = 0$, либо $\Delta p = 2$, $\Delta b = 2$, $\Delta k = 0$, либо $\Delta p = -2$, $\Delta b = -2$, $\Delta k = 0$. Опять получаем $\Delta\varphi = 0$. Поэтому $\text{Ind } \Sigma'' = \text{Ind } \Sigma'$.

5. Σ'' получена из Σ' при помощи тождества 5. В этом случае для каждого набора $\alpha_1, \dots, \alpha_{n+1}$ имеем $\Delta\varphi = 0$. Поэтому $\text{Ind } \Sigma'' = \text{Ind } \Sigma'$.

6. Σ'' получена из Σ' при помощи тождества 6_m ($m \leq n$). Тут также $\text{Ind } \Sigma'' = \text{Ind } \Sigma'$ (см. рассуждения в примере перед этой леммой для случая $m < n + 1$).

Лемма доказана.

С л е д с т в и е. Тождество 6_{n+1} не может быть выведено из тождеств 1–5, 6_m ($m \leq n$).

В самом деле, совершая эквивалентные преобразования схемы Σ_1 (левая часть тождества 6_{n+1}) при помощи тождеств 1–5, 6_m ($m \leq n$), мы будем получать схемы Σ с $\text{Ind } \Sigma = \text{Ind } \Sigma_1 = 1$, в то же время схема Σ_0 (правая часть тождества 6_{n+1}) такова, что $\text{Ind } \Sigma_0 = 0$.

Теорема 33. *Для контактных схем не существует конечной полной системы тождеств.*

Доказательство. Допустим противное, пусть для контактных схем существует конечная полная система тождеств

$$\left\{ \begin{array}{l} \Sigma'_1 \longleftrightarrow \Sigma''_1, \\ \dots\dots\dots \\ \Sigma'_l \longleftrightarrow \Sigma''_l. \end{array} \right.$$

Тогда найдется такое n , что все схемы из этих тождеств будут схемами над $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$. Тогда каждое тождество из этой системы может быть выведено из 1–5, 6_m ($m \leq n$). С другой стороны, система тождеств полна, поэтому из нее может быть получено тождество 6_{n+1} . Следовательно, из 1–5, 6_m ($m \leq n$) выводимо 6_{n+1} , что противоречит следствию предыдущей леммы.

Теорема доказана.

§ 5. Эквивалентные преобразования автоматов

Как и в случае схем из Ф.Э., необходимо сначала расширить понятие автомата, иначе естественные правила преобразований могут вывести за пределы класса автоматов [34].

1. Допускаются изолированные входы. Они отражают несущественность переменных.

2. Могут быть автоматы без входов. В этом случае в канонических уравнениях отсутствуют переменные из алфавита X . Такие автоматы реализуют константы, являющиеся периодическими последовательностями.

3. Допускаются выходы, которым не приписан символ из алфавита Z , т. е. не являющиеся выходами схемы. В частности, схема может быть без выходов. В этом случае в канонических уравнениях отсутствуют переменные из алфавита Z . По определению, функционирование будет пустым.

Для автоматов принимаются те же уточнения в изображении автоматных схем, что и для схем из Ф.Э.

Существенной чертой в проблематике эквивалентных преобразований является то, что эквивалентность двух автоматов определяется через равенство соответствующих о.-д. функций (в случае отсутствия выходов автоматы считаются эквивалентными). В остальном все аналогично случаю схем из Ф.Э.

Как мы видели, исследуемый класс автоматов включает в себя класс схем из функциональных элементов в базисе, состоящем из инверторов, конъюнкторов и дизъюнкторов. А наличие конечной полной системы тождеств для схем их функциональных элементов не позволяет сделать прогнозы о возможности распространения этой ситуации на более широкий класс — класс автоматов. И на самом деле в автоматном случае проблема эквивалентных преобразований решается значительно сложнее.

Мы начнем наши рассуждения с изучения класса $\mathfrak{S}_l$ всех автоматов, содержащих не более l элементов задержки.

Автомат с n входами и m выходами определяет о.-д. функцию, которую можно задать каноническими уравнениями

$$\begin{cases} Z(t) = F(X(t), Q(t-1)), \\ Q(t) = G(X(t), Q(t-1)), \\ Q(0) = 0. \end{cases}$$

Эти канонические уравнения задают нумерацию вершин и нумерацию ребер дерева для о.-д. функции.

Вершинам приписываются числа $\kappa_1, \dots, \kappa_r$, являющиеся номерами различных типов поддеревьев. Далее, α -му ребру, исходящему из вершины κ , приписывается число (вектор) $F(\alpha, \kappa)$, а вершине, в которое ведет ребро, — число (вектор) $G(\alpha, \kappa)$. При этом корню дерева приписывают число $\kappa_1 = 0$ (начальное условие; рис. 81).

Очевидно, функции $F(x, \kappa)$ при фиксированном κ определяют нумерацию ребер в пучке, исходящем из вершины κ .

В таком случае типы этих функций и их число однозначно определяются о.-д. функцией. Пусть

$$F^{(1)}(x_1, \dots, x_n), \dots, F^{(r_0)}(x_1, \dots, x_n) \quad (*)$$

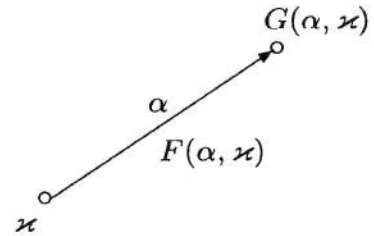


Рис. 81

являются представителями этих типов функций.

Обозначим это множество через $\mathfrak{M}_0$. Мощность этого множества $|\mathfrak{M}_0| = r_0 \leq r$. Пусть о.-д. функция реализована двумя автоматными схемами Σ' и Σ'' , имеющими каждая ровно l элементов задержек. С ними связаны естественные системы канонических уравнений (см. алгоритм получения канонических уравнений по автоматной схеме)

$$\begin{cases} Z(t) = F'(X(t), Q(t-1)), \\ Q(t) = G'(X(t), Q(t-1)) \end{cases} \quad \text{и} \quad \begin{cases} Z(t) = F''(X(t), Q(t-1)), \\ Q(t) = G''(X(t), Q(t-1)) \end{cases}$$

с одинаковыми начальными условиями $Q(0) = 0$, в которых

$$\begin{aligned} X(t) &= (x_1(t), \dots, x_n(t)), \\ Q(t) &= (q_1(t), \dots, q_l(t)), \\ Z(t) &= (z_1(t), \dots, z_m(t)) \end{aligned}$$

и функции F', F'', G', G'' всюду определены. Легко видеть, что вес исходной о.-д. функции удовлетворяет неравенству $r \leq 2^l$. Очевидно, что эти системы в дереве для этой о.-д. функции определяют, вообще говоря, различные нумерации вершин, каждая из которых удовлетворяет следующему свойству: вершины, принадлежащие различным классам эквивалентности, будут иметь различные номера, в то же время поддеревья из одного класса не обязательно имеют один и тот же номер.

Рассмотрим векторные разложения

$$F'(x_1, \dots, x_n, q_1, \dots, q_l) = \bigvee_{(\sigma'_1, \dots, \sigma'_l)} F'(x_1, \dots, x_n, \sigma'_1, \dots, \sigma'_l) \& q_1^{\sigma'_1} \& \dots \& q_l^{\sigma'_l},$$

$$F''(x_1, \dots, x_n, q_1, \dots, q_l) = \bigvee_{(\sigma''_1, \dots, \sigma''_l)} F''(x_1, \dots, x_n, \sigma''_1, \dots, \sigma''_l) \& q_1^{\sigma''_1} \& \dots \& q_l^{\sigma''_l}.$$

Компоненты этих разложений образуют некоторое подмножество $\mathfrak{M}$ вектор-функций от переменных $x_1, \dots, x_n$. Легко видеть, что

$$\mathfrak{M}_0 \subseteq \mathfrak{M} \quad \text{и} \quad r_1 = |\mathfrak{M}| \leq 2^{l+1}.$$

В частности, если набор $(\sigma'_1, \dots, \sigma'_l)$ (или набор $(\sigma''_1, \dots, \sigma''_l)$) является номером некоторой вершины дерева для соответствующей о.-д. функции, то $F'(x_1, \dots, x_n, \sigma'_1, \dots, \sigma'_l) \in \mathfrak{M}_0$ (соответственно $F''(x_1, \dots, x_n, \sigma''_1, \dots, \sigma''_l) \in \mathfrak{M}_0$). Поэтому можно занумеровать функции множества $\mathfrak{M}$ числами $\lambda = (\lambda_1, \dots, \lambda_{l+1})$ и так, что первые r_0 номеров относятся к подмножеству $\mathfrak{M}_0$. Мы имеем

$$\mathfrak{M} = \{F^{(1)}(x_1, \dots, x_n), \dots, F^{(r_0)}(x_1, \dots, x_n), \\ F^{(r_0+1)}(x_1, \dots, x_n), \dots, F^{(r_1)}(x_1, \dots, x_n)\}.$$

Пусть

$$F'(x_1, \dots, x_n, \sigma'_1, \dots, \sigma'_l) = F^{(\lambda')}(x_1, \dots, x_n),$$

$$F''(x_1, \dots, x_n, \sigma''_1, \dots, \sigma''_l) = F^{(\lambda'')}(x_1, \dots, x_n);$$

тогда мы получаем два отображения φ' и φ'' , где

$$\varphi'(\sigma'_1, \dots, \sigma'_l) = (\lambda'_1, \dots, \lambda'_{l+1}) = \lambda',$$

$$\varphi''(\sigma''_1, \dots, \sigma''_l) = (\lambda''_1, \dots, \lambda''_{l+1}) = \lambda''.$$

Рассмотрим разложения

$$G'(x_1, \dots, x_n, q_1, \dots, q_l) = \bigvee_{(\alpha_1 \dots \alpha_n)} G'(\alpha_1, \dots, \alpha_n, q_1, \dots, q_l) \& x_1^{\alpha_1} \& \dots \& x_n^{\alpha_n},$$

$$G''(x_1, \dots, x_n, q_1, \dots, q_l) = \bigvee_{(\alpha_1 \dots \alpha_n)} G''(\alpha_1, \dots, \alpha_n, q_1, \dots, q_l) \& x_1^{\alpha_1} \& \dots \& x_n^{\alpha_n};$$

их компоненты $G'(\alpha_1, \dots, \alpha_n, q_1, \dots, q_l)$ и $G''(\alpha_1, \dots, \alpha_n, q_1, \dots, q_l)$ определяют (l, l) -преобразования, т. е. системы из l булевых функций от l переменных $q_1, \dots, q_l$. Число s таких преобразований, очевидно, есть

$$s = 2^{l2^l}.$$

Обозначим их через

$$G^{(1)}(q_1, \dots, q_l), \dots, G^{(s)}(q_1, \dots, q_l).$$

Мы имеем

$$G'(\alpha_1, \dots, \alpha_n, q_1, \dots, q_l) = G^{(\mu')}(q_1, \dots, q_l), \quad \text{где } \mu' = (\mu'_1, \dots, \mu'_{\log s}),$$

$$G''(\alpha_1, \dots, \alpha_n, q_1, \dots, q_l) = G^{(\mu'')}(q_1, \dots, q_l), \quad \text{где } \mu'' = (\mu''_1, \dots, \mu''_{\log s}).$$

Отсюда получаем два преобразования ψ' и ψ'' :

$$\psi'(\alpha_1, \dots, \alpha_n) = (\mu'_1, \dots, \mu'_{\log s}),$$

$$\psi''(\alpha_1, \dots, \alpha_n) = (\mu''_1, \dots, \mu''_{\log s}).$$

Теперь вычисление о.-д. функции на основе автомата Σ' можно определить в следующей стандартной форме.

1. По входному значению $\alpha_1(t), \dots, \alpha_n(t)$ при помощи функции ψ' находят номер $\mu' = (\mu'_1, \dots, \mu'_{\log s})$ (l, l) -полюсника.

2. По состояниям $(q_1(t-1), \dots, q_l(t-1))$ находим новые состояния $(q_1(t), \dots, q_l(t))$ при помощи функции $G^{(\mu')}(q_1, \dots, q_l)$, так как

$$(q_1(t), \dots, q_l(t)) = G'(\alpha_1(t), \dots, \alpha_n(t), q_1(t-1), \dots, q_l(t-1)) =$$

$$= G^{(\mu')}(q_1(t-1), \dots, q_l(t-1)).$$

3. По состояниям $(q_1(t-1), \dots, q_l(t-1)) = (\sigma'_1, \dots, \sigma'_l)$ и функции φ' находим номер $\lambda' = (\lambda'_1, \dots, \lambda'_{l+1})$ функции $F^{(\lambda')}(x_1, \dots, x_n)$.

4. Находим выходные значения $(\gamma_1(t), \dots, \gamma_m(t))$ при помощи функции $F^{(\lambda')}(x_1, \dots, x_n)$ и входных значений $(\alpha_1(t), \dots, \alpha_n(t))$, а именно:

$$(\gamma_1(t), \dots, \gamma_m(t)) = F'(\alpha_1(t), \dots, \alpha_n(t), q_1(t-1), \dots, q_l(t-1)) =$$

$$= F'(\alpha_1(t), \dots, \alpha_n(t), \sigma'_1, \dots, \sigma'_l) = F^{(\lambda')}(\alpha_1(t), \dots, \alpha_n(t)).$$

Аналогичное вычисление получается на основе автомата Σ'' .

О п р е д е л е н и е. Номера $(\sigma'_1, \dots, \sigma'_l)$ и $(\sigma''_1, \dots, \sigma''_l)$, приписанные одной и той же вершине дерева двумя эквивалентными автоматами, называются согласованными.

З а м е ч а н и е. Для двух согласованных номеров $(\sigma'_1, \dots, \sigma'_l)$ и $(\sigma''_1, \dots, \sigma''_l)$ имеют место следующие соотношения:

- а) если $\lambda' = \varphi'(\sigma'_1, \dots, \sigma'_l)$ и $\lambda'' = \varphi''(\sigma''_1, \dots, \sigma''_l)$, то $\lambda' = \lambda''$;
- б) если $\mu' = \psi'(\alpha_1(t), \dots, \alpha_n(t))$ и $\mu'' = \psi''(\alpha_1(t), \dots, \alpha_n(t))$, то номера

$$G^{(\mu')}(q_1, \dots, q_l) \quad \text{и} \quad G^{(\mu'')}(q_1, \dots, q_l)$$

также согласованы.

Первое соотношение очевидно, второе вытекает из того, что при указанных предположениях мы из некоторой вершины дерева, которой приписаны согласованные номера $(\sigma'_1, \dots, \sigma'_l)$ и $(\sigma''_1, \dots, \sigma''_l)$, смещаемся по ребру $(\alpha_1(t), \dots, \alpha_n(t))$ в новую вершину, которой приписаны номера

$$G^{(\mu')}(\sigma'_1, \dots, \sigma'_l) \quad \text{и} \quad G^{(\mu'')}(\sigma''_1, \dots, \sigma''_l).$$

Теперь можно определить для двух эквивалентных автоматов согласованный канонический вид.

Для этого построим две схемы Σ_1 и Σ_2 (рис. 82).

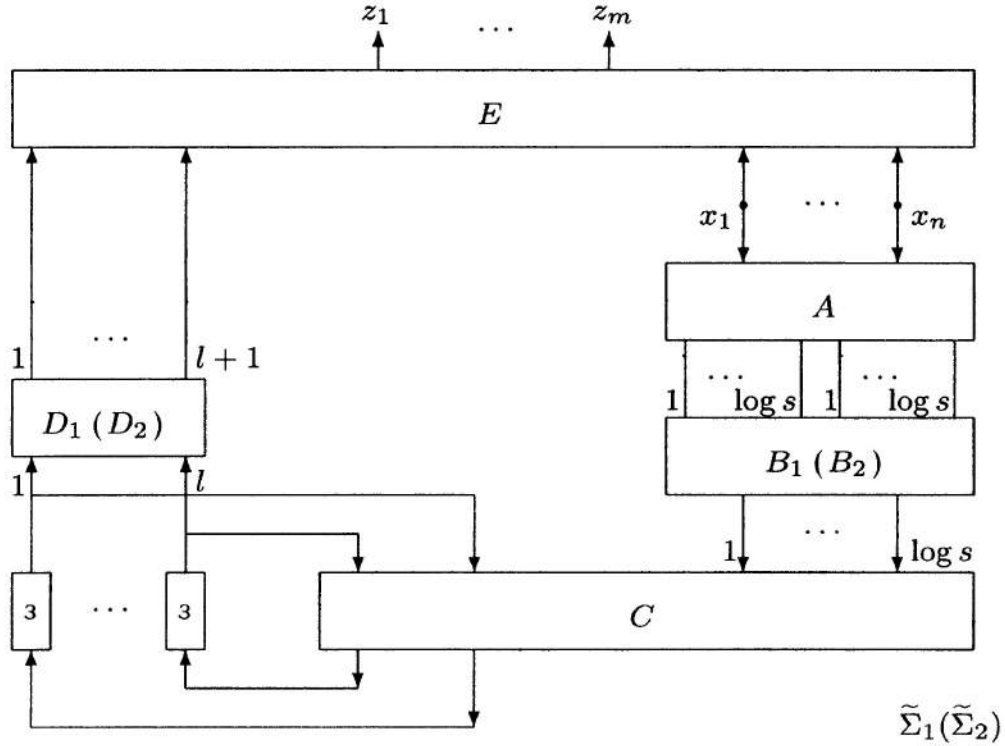


Рис. 82

Блоки $A-E$ представляют собой функциональные многополюсники, реализация которых выбрана в канонической форме, определенной для схемы из Ф.Э. Опишем функциональные характеристики блоков.

Блок A имеет n входов и $2 \log s$ выходов; на первой группе из $\log s$ выходов реализуется функция ψ' , на второй — ψ'' .

Блок $B_1 (B_2)$ имеет $2 \log s$ входов и $\log s$ выходов. Этот блок дает на выходе

а) $(\mu'_1, \dots, \mu'_{\log s})$ (соответственно $(\mu''_1, \dots, \mu''_{\log s})$), если на входе был набор $(\mu'_1, \dots, \mu'_{\log s}, \mu''_1, \dots, \mu''_{\log s})$ такой, что $(\mu'_1, \dots, \mu'_{\log s}) = \psi'(\alpha_1, \dots, \alpha_n)$ и $(\mu''_1, \dots, \mu''_{\log s}) = \psi''(\alpha_1, \dots, \alpha_n)$ для некоторого входного набора $(\alpha_1, \dots, \alpha_n)$,

б) $(\mu_1^0, \dots, \mu_{\log s}^0) = \mu^0$ такой, что $G^{(\mu^0)}(\sigma_1, \dots, \sigma_l) \equiv (\sigma_1, \dots, \sigma_l)$ (тождественное преобразование) — в остальных случаях.

Блок C имеет $\log s + l$ входов и l выходов. Если на вторую группу из $\log s$ входов подать набор $(\mu_1, \dots, \mu_{\log s}) = \mu$, то этот блок реализует (l, l) оператор $G^{(\mu)}(q_1, \dots, q_l)$.

Блок D_1 (D_2) имеет l входов и $l + 1$ выход. Он преобразует входной набор $(\sigma'_1, \dots, \sigma'_l)$ (соответственно $(\sigma''_1, \dots, \sigma''_l)$) в значение (набор) $\lambda' = \varphi'(\sigma'_1, \dots, \sigma'_l)$ (соответственно $\lambda'' = \varphi''(\sigma''_1, \dots, \sigma''_l)$).

Блок E имеет $n + l + 1$ вход и m выходов. В случае если на первые $l + 1$ входов поступает набор $\lambda = (\lambda_1, \dots, \lambda_{l+1})$, то он реализует $F^{(\lambda)}(x_1, \dots, x_n)$ при $\lambda \leq r_1$ и $\tilde{0} = (0, \dots, 0)$ при $\lambda > r_1$.

Очевидно, что автоматы Σ_1 и Σ_2 эквивалентны и эквивалентны также автоматам Σ' и Σ'' .

Лемма 18. При помощи конечной полной системы правил преобразований для схем из Ф.Э. в базисе из конъюнктора, дизъюнктора и инвертора можно преобразовать Σ' в Σ_1 (соответственно Σ'' в Σ_2).

Доказательство. Из построения вытекает, что Σ_1 имеет те же самые канонические уравнения, что и Σ' . Отсюда следует, что функциональные многополюсники, получающиеся из Σ_1 и Σ' путем удаления элементов задержек, при естественном соответствии возникающих входов и выходов, эквивалентны (их функционирование описывается уравнениями, которые строятся из одних и тех же канонических уравнений с полностью определенными функциями). Остальная часть доказательства очевидна.

Обозначим через $\tilde{\Sigma}_1$ часть схемы Σ_1 , образованную из блоков B_1, C, D_1 , и через $\tilde{\Sigma}_2$ часть схемы Σ_2 , образованную из блоков B_2, C, D_2 (см. рис. 82). Эти подсхемы на указанном рисунке очерчены пунктиром.

Схемы $\tilde{\Sigma}_1$ и $\tilde{\Sigma}_2$ имеют $2 \log s$ входов и $l + 1$ выходов и естественное соответствие между входами и между выходами.

Лемма 19. Автоматы $\tilde{\Sigma}_1$ и $\tilde{\Sigma}_2$ эквивалентны.

Доказательство. Автоматы $\tilde{\Sigma}_1$ и $\tilde{\Sigma}_2$ определены так, что при любых входах $\{(\mu'_1(t), \dots, \mu'_{\log s}(t), \mu''_1(t), \dots, \mu''_{\log s}(t))\}$, $t = 1, 2, \dots$, в них вырабатываются согласованные наборы состояний $(\sigma_1(t), \dots, \sigma_l(t))$ (в начальный момент времени имеем наборы из нулей, которые тоже согласованы). Далее, многополюсники D_1 и D_2 согласованные наборы переводят в один и тот же набор $\lambda = (\lambda_1, \dots, \lambda_{l+1})$.

Лемма доказана.

Теорема 34 (Мурский [15]). Для класса автоматов $\mathfrak{E}_2$ над базисом Б, содержащих не более чем l задержек, существует конечная полная система тождеств.

Доказательство. Состоит в постепенном построении системы тождеств и доказательстве ее полноты.

1. В систему тождеств включим конечную полную систему тождеств для схем из Ф.Э., состоящих из инверторов, конъюнкторов и дизъюнкторов, что позволяет преобразовать эквивалентные схемы без элементов задержек.



Рис. 83

2. Далее присоединим тождество, представленное на рис. 83. При помощи его, а также правила VII мы можем любой автомат, содержащий менее l задержек, преобразовать в автомат, содержащий ровно l задержек.

Это наращивание числа задержек может быть сделано путем подключения к выходу автомата цепочки схем, как показано на рис. 84.

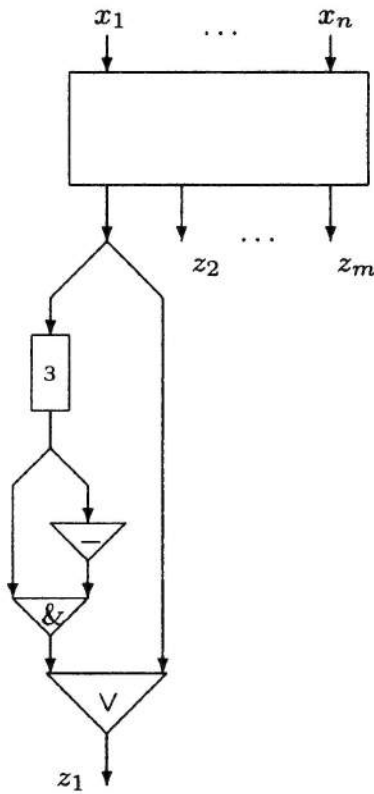


Рис. 84

Данное «подключение» осуществляется сначала присоединением задержки без выхода (правило, указанное на рис. 83), а затем применением правила VII.

Итак, можно предполагать, что эквивалентные автоматы Σ' и Σ'' имеют одинаковое число задержек, равное l .

3. Лемма 18 позволяет схемы Σ' и Σ'' эквивалентным образом преобразовать к согласованному каноническому виду, т. е. к Σ_1 и Σ_2 соответственно.

4. Остается построить эквивалентное преобразование Σ_1 в Σ_2 . Для этого рассмотрим в $\mathfrak{S}_l$ подмножество автоматов с $2 \log s$ входами и $l+1$ выходами. Разобьем его на конечное число классов: два автомата с указанными параметрами относятся к одному классу тогда и только тогда, когда существует такое соответствие элементов задержек, при котором их канонические уравнения будут иметь эквивалентные правые части (или если из их схем удалить элементы задержек, то полученные схемы из Ф.Э. будут эквивалентными).

Очевидно, что число классов не более, чем число функциональных многополюсников с $l + 2 \log s$ входами и $2l + 1$ выходами т. е.

$$\left(2^{2^{l+2 \log s}}\right)^{2l+1} = 2^{(2l+1)2^{l+2l2^l}}.$$

Выберем из каждого класса по одному представителю. Пусть это будут автоматы

$$\Sigma_1^0, \dots, \Sigma_\nu^0, \quad \nu \leq 2^{(2l+1)2^{l+2l2^l}}.$$

Рассмотрим все пары Σ_i^0, Σ_j^0 , которые эквивалентны как автоматы и присоединим к списку тождеств все тождества вида $\Sigma_i^0 \longleftrightarrow \Sigma_j^0$ (очевидно, конечное число).

Теперь можно описать процесс преобразования Σ_1 в Σ_2 . Схемы Σ_1 и Σ_2 имеют тождественные части, а именно блоки A и E ; оставшиеся части-подсхемы $\tilde{\Sigma}_1$ и $\tilde{\Sigma}_2$ по лемме 19 эквивалентны и принадлежат подклассу автоматов с $2 \log s$ входами и $l+1$ выходами. Легко видеть, что существуют такие автоматы Σ_i^0 и Σ_j^0 , что

- $\tilde{\Sigma}_1$ входит в тот же класс эквивалентности, что и Σ_i^0 ,
- $\tilde{\Sigma}_2$ входит в тот же класс эквивалентности, что и Σ_j^0 .

Преобразование $\tilde{\Sigma}_1$ в Σ_i^0 осуществляется применением правил для схем из Ф.Э. Так как $\tilde{\Sigma}_1 \sim \tilde{\Sigma}_2$, то $\Sigma_i^0 \sim \Sigma_j^0$ и потому эта эквивалентность содержится в системе тождеств, а Σ_j^0 можно преобразовать в $\tilde{\Sigma}_2$, применяя правила для схем из Ф.Э.

Теорема доказана.

Легко видеть, что данная теорема является обобщением известного факта для схем из функциональных элементов, так как при $l = 0$ мы имеем $\mathfrak{S}_0$ — класс схем из функциональных элементов. Следует заметить, что сама по себе конечная система тождеств, построенная нами, весьма громоздка даже при $l = 1$. Поэтому остается неясным, насколько возможно эти правила упростить.

Теперь мы перейдем к рассмотрению класса всех автоматов и покажем, что для него не существует конечной полной системы тождеств.

Пусть Σ' — автомат без входов и выходов. Обозначим через $Z_1, \dots, Z_l$ выходы элементов задержки автомата Σ' . Очевидно, на этих выходах автомат $\Sigma'(Z_1, \dots, Z_l)$ будет реализовывать периодическую последовательность. Пусть τ' — ее период.

Л е м м а 20. *Предположим, что в автомате Σ' некий его подавтомат Σ_1 , имеющий k задержек, заменен на эквивалентный ему автомат Σ_2 ($\Sigma_2 \longleftrightarrow \Sigma_1$), в результате чего получается автомат Σ'' .*

Тогда, если p — простое число такое, что $p > 2^k$ и период τ' автомата Σ' делится на p , то и период τ'' автомата Σ'' делится на p .

Д о к а з а т е л ь с т в о. Можно считать, что подавтомат Σ_1 содержит задержки с выходами $Z_1, \dots, Z_k$. Очевидно, что задержки с выходами $Z_{k+1}, \dots, Z_l$ принадлежат как автомату Σ' , так и автомату Σ'' . В силу того, что $\Sigma_2 \longleftrightarrow \Sigma_1$, на выходах $Z_{k+1}, \dots, Z_l$ в автоматах Σ' , Σ'' реализуется одна и та же периодическая последовательность с некоторым периодом τ_0 , причем τ_0 является делителем как τ' , так и τ'' .

Очевидно также, что период автомата Σ' не может быть больше, чем $\tau_0 2^k$, т. е.

$$\tau' \leq \tau_0 2^k.$$

Значит, $\frac{\tau'}{\tau_0}$ — целое число и $\frac{\tau'}{\tau_0} \leq 2^k$.

Так как p — простое число, которое больше 2^k , оно не является делителем $\frac{\tau'}{\tau_0}$. С другой стороны, по условию леммы период τ' делится на p ; значит, и τ_0 делится на p . Следовательно, период τ'' также делится на p .

Лемма доказана.

Т е о р е м а 35. *Для класса автоматов в данном базисе не существует конечной полной системы тождеств.*

Доказательство. Рассмотрим семейство автоматов Σ^n (при $n = 2, 3, \dots$) без входов и выходов (рис. 85).

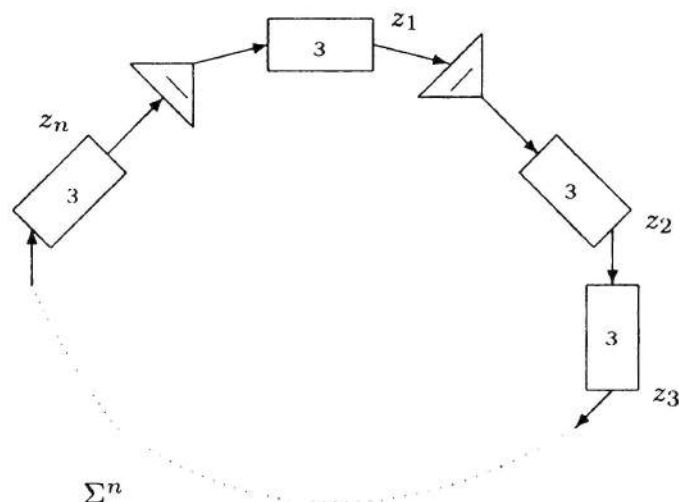


Рис. 85

Данные автоматы по определению попарно эквивалентны. В табл. 10 показано, как во времени меняются состояния на выходах. Из таблицы видно, что период автомата Σ^n равен n .

Т а б л и ц а 10

	0	1	2		$n-1$	n
z_1	0	1	1		1	0
z_2	0	1	0		0	0
z_3	0	0	1		0	0
...	...	...	...		...	...
...	...	...	...		...	...
z_{n-1}	0	0	0		0	0
z_n	0	0	0		1	0

Предположим, что теорема неверна, т. е. существует конечная полная система тождеств. Обозначим через k суммарное число задержек, встречающихся в тождествах этой системы. Возьмем простое число p такое, что $p > 2^k$. Рассмотрим автомат Σ^p . Он реализует на выходах задержек периодическую последовательность с периодом p . В силу доказанной леммы 20 при любой эквивалентной подстановке при помощи тождеств нашей системы мы будем получать автоматы, на выходах задержек которых будет реализовываться периодическая последовательность, кратная p . Следовательно, мы никогда не сможем получить автомат Σ^2 , который эквивалентен Σ^p . Получили противоречие.

Теорема доказана.

Из доказательства теоремы видно, что если рассматривать класс автоматов над заданным конечным входным алфавитом $\{x_1, \dots, x_n\}$, то для него нет также конечной полной системы тождеств, так как он содержит $\{\Sigma^n\}$.

Эта ситуация является новой, ибо для формул в многозначных логиках и для контактных схем в подклассах над конечным алфавитом $\{x_1, \dots, x_n\}$ всегда есть конечная полная система тождеств.

ВВЕДЕНИЕ

Пусть на класс $\mathcal{U}$ управляющих систем (У.С.) действует источник неисправностей И. Под влиянием источника И каждая управляющая система U из класса $\mathcal{U}$ переходит в У.С. $U_1, \dots, U_r$, где $U_1 = U$ (рис. 86)

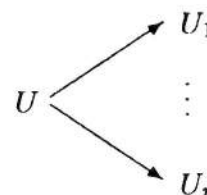


Рис. 86

При этом мы считаем, что данное воздействие происходит в момент t и в течение некоторого промежутка Δt никаких изменений больше не происходит.

У.С. $U_1, \dots, U_r$ принадлежат классу $\mathcal{U}'$, $\mathcal{U}' \supseteq \mathcal{U}$, так как мы считаем, что $U_1 = U$.

Воздействие источника И на У.С. $U = (\Sigma, f)$ может проявляться в появлении

- а) ошибок на входах,
- б) неисправностей элементов,
- в) ошибок в соединении элементов,
- г) изменений состояний памяти,
- д) нарушений алгоритма функционирования и т. п.

Случаи а)–г) относятся к случаям, когда источник воздействует на схему Σ . В этой ситуации схема Σ переходит в «неисправные» состояния $\Sigma_1, \dots, \Sigma_r$, включающие в себя и исходное состояние Σ (считая, что $\Sigma_1 = \Sigma$). Пусть этим схемам соответствуют функции $f_1, \dots, f_r$ ($f_1 = f$), называемые также функциями неисправностей. Тогда $U_1 = (\Sigma_1, f_1), \dots, U_r = (\Sigma_r, f_r)$. В дальнейшем особую роль играют не сами функции $f_1, \dots, f_r$, а классы эквивалентности $g_1, \dots, g_m$, на которые можно разбить эти функции: f_ν и f_μ принадлежат одному классу g тогда и только тогда, когда $f_\nu = f_\mu$ (в качестве g можно взять любой представитель класса эквивалентности). Можно считать, что $g_1 = f_1 = f$. Таким образом, функции $g_1, \dots, g_m$ определяют различные режимы функционирования при воздействии источника И на схему Σ .

Неисправность схемы Σ . Различаем *формальную* неисправность — такое неисправное состояние Σ_i , что $i > 1$, и *фактическую* неисправность — $f_i \neq f_1$. Очевидно, что при формальной неисправности схема Σ_i может функционировать так же, как и исправная; для этого необходимо, чтобы $f_i = f_1$, т. е. функция f_i принадлежала классу g_1 . Очевидно также, что функции неисправностей f_ν и f_μ , принадлежащие одному классу, неразличимы.

Проблематика надежности У.С. развивается в рамках логико-кибернетического подхода в двух направлениях:

- 1) построение надежных схем из ненадежных элементов;
- 2) синтез самокорректирующихся схем.

Эти направления отличаются способами описания источника И. В первом случае источник описывается в вероятностных терминах (вероятностный подход). Во втором случае источник характеризуется ограничениями на возможные функциональные изменения элементов и на число одновременно возможных повреждений элементов (логико-комбинаторный подход).

Проблематика надежности начала складываться в середине 50-х годов прошлого столетия. Первыми работами были:

1) работы Дж. фон Неймана [40] и Мура и Шеннона [39] 1956 г. по построению надежных схем из ненадежных элементов;

2) работа Ю. Г. Потапова и С. В. Яблонского [21] 1960 г. по синтезу самокорректирующихся схем.

В дальнейшем существенный вклад в развитие этого направления внесли советские ученые (см. [35]).

РАЗДЕЛ 1. ПОСТРОЕНИЕ НАДЕЖНЫХ СХЕМ ИЗ НЕНАДЕЖНЫХ ЭЛЕМЕНТОВ

Это направление рассматривается здесь для случая, когда $\mathcal{U}$ — класс схем из функциональных элементов (Ф.Э.). Пусть $U \in \mathcal{U}$ и $U = (\Sigma, f)$. Тогда схема Σ является соединением элементов F_i ($i = 1, \dots, r$), принадлежащих некоторому базису B . Каждый элемент F_i (рис. 87) является элементарным преобразователем с n_i входами и одним выходом, реализующим некоторую булеву функцию f_i^0 от n_i переменных.

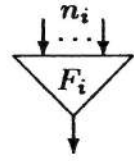


Рис. 87

Для схемы Σ под сложностью $L(\Sigma)$ понимается сумма сложностей $L(F_i)$, входящих в схему Σ . Наряду с $L(\Sigma)$ рассматривается функция Шеннона

$$L(n) = \max_{f \in P_2^n} \min_{\substack{\Sigma \\ \Sigma \text{ реализ. } f}} L(\Sigma),$$

где P_2^n — множество всех булевых функций от n переменных.

Далее мы будем рассматривать источники I , которые воздействуют на элементы схемы независимым образом так, что поврежденный элемент реализует булеву функцию от тех же переменных (рис. 88).

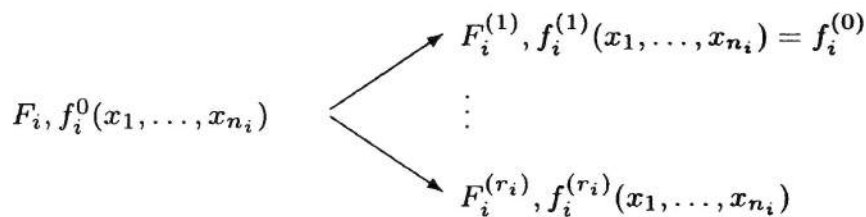


Рис. 88

Можно считать, что все функции неисправности элементов попарно различны, т. е. $f_i^{(j_1)} \neq f_i^{(j_2)}$ при $j_1 \neq j_2$. Элементы, у которых источник I не вызывает неисправностей, называются абсолютно надежными, остальные — ненадежными. Таким образом, базис B по отношению к источнику I разбивается на две части: B_1 — состоящую из абсолютно надежных элементов и B_2 — состоящую из ненадежных элементов, т. е.

$$B = B_1 \cup B_2.$$

§ 1. Вероятностное описание источников помех и повреждений схем

Существуют различные возможности вероятностного описания повреждений схем и элементов.

Вероятность $\mathcal{P}(\Sigma)$ фактической неисправности схемы (элемента) Σ является важнейшей характеристикой схемы.

Возникает вопрос: можно ли найти $\mathcal{P}(\Sigma)$, если известны вероятности повреждения элементов F_i ($F_i \in B_2$), т. е. величины $p_i = \mathcal{P}(F_i)$? Оказывается, если хотя бы для одного из F_i , $F_i \in B_2$, число r_i неисправных

режимов больше или равно 3, то без дополнительной информации этого сделать в общем случае нельзя. Поэтому при этих же ограничениях набор вероятностей $\{p_i\}$ не является полным описанием источника И.

В то же время существует полезная оценка для $\mathcal{P}(\Sigma)$ через величины p_i . Для этого занумеруем все величины из Σ , принадлежащие B_2 , числами $1, 2, \dots, l$, и пусть $\nu(i)$ ($i = 1, \dots, l$) указывает тип элемента с номером i .

Т е о р е м а 36. $\mathcal{P}(\Sigma) \leq 1 - \prod_{i=1}^l (1 - p_{\nu(i)})$.

Д о к а з а т е л ь с т в о следует из того, что правая часть неравенства есть вероятность формальной неисправности схемы Σ , и вероятность фактической неисправности схемы Σ не превосходит вероятности ее формальной неисправности.

Легко видеть, что данное неравенство может быть строгим, т. е. оценка является грубой.

Распределение вероятностей появления для схемы Σ режимов $g_1, \dots, g_m$, где $g_1 = f(x_1, \dots, x_n)$ и $1 \leq m \leq 2^{2^n}$, определяется указанием вероятностей $q^{(1)}, \dots, q^{(m)}$ их появления, для которых $\sum_{i=1}^m q^{(i)} = 1$. Очевидно, что $\mathcal{P}(\Sigma) = 1 - q^{(1)} = \sum_{i=2}^m q^{(i)}$.

Для элементов F_i из B_2 распределение вероятностей имеет вид

$$\begin{pmatrix} f_i^{(1)} & \dots & f_i^{(r_i)} \\ p_i^{(1)} & \dots & p_i^{(r_i)} \end{pmatrix},$$

где $\sum_{j=1}^m p_i^{(j)} = 1$, $f_i^{(1)} = f_i^0(x_1, \dots, x_{n_i})$, $2 \leq r_i \leq 2^{2^{n_i}}$. Можно также считать, что $p_i^{(j)} > 0$ ($1 \leq j \leq r_i$), так как иначе можно было бы выбросить функции, для которых вероятность равна 0.

Оказывается, что, зная распределения для элементов F_i из B_2 , можно построить распределение для схемы Σ над B , реализующей функцию $f(x_1, \dots, x_n)$. Для этого для каждого элемента схемы Σ , принадлежащего B_2 , выбираем одну из возможных функций неисправности и вычисляем вероятность этой выборки как произведение вероятностей появления выбранных неисправностей для отдельных элементов. Затем находим режим схемы Σ , соответствующий данному выбору. Эту процедуру проделываем для всевозможных комбинаций выборов, после чего, суммируя все вероятности, соответствующие режиму g_i , находим величину $q^{(i)}$ ($1 \leq i \leq m$).

Отсюда вытекает, что законы распределения вероятностей для базисных элементов из B_2 являются полной характеристикой источника И.

П р и м е р. I_n — неймановский источник, если для каждого F_i из B_2 распределение вероятностей имеет вид

$$\begin{pmatrix} f_i^{(1)}(x_1, \dots, x_{n_i}) & \dots & f_i^{(2^{2^{n_i}})}(x_1, \dots, x_{n_i}) \\ p_i^{(1)} & \dots & p_i^{(2^{2^{n_i}})} \end{pmatrix},$$

где $f_i^{(1)} = f_i^0(x_1, \dots, x_{n_i})$, $\sum_{j=1}^{2^{n_i}} p_i^{(j)} = 1$ и $p_i^{(j)} > 0$, т. е. у ненадежных элементов неймановский источник вызывает всевозможные функциональные повреждения. Обозначим для F_i из B_2 через $p_{\min}^{(i)} = \min_{1 \leq j \leq 2^{n_i}} p_i^{(j)}$ и $p_{\min} = \min_{i, F_i \in B_2} p_{\min}^{(i)}$.

Теорема 37. Для неймановского источника I_n и $B_1 = \Lambda$

$$\mathcal{P}(\Sigma) \geq p_{\min}.$$

Доказательство. Пусть выход системы Σ является выходом элемента F_i . Обозначим выходы F_i через $y_1, y_2, \dots, y_{n_i}$ (рис. 89).

Пусть $\mathcal{M}$ — событие, состоящее в том, что при воздействии источника I на схему Σ элемент F_i будет реализовывать функцию $f_i^{(j)}$, равную тождественно константе, отличной от функции, реализуемой схемой Σ . Очевидно, что вероятность события $\mathcal{M}$ не меньше, чем $p_i^{(j)}$, где $p_i^{(j)} \geq p_{\min}$, и что схема Σ в любом неисправном состоянии, соответствующем событию $\mathcal{M}$, будет работать неправильно, т. е. $\mathcal{P}(\Sigma) \geq p_{\min}$.

Теорема доказана.

Рассмотрим функцию $q(x_1, \dots, x_n)$, задающую вероятность неправильной работы схемы Σ на входных наборах $(\alpha_1, \dots, \alpha_n)$, $\alpha_i \in \{0, 1\}$, $i = 1, \dots, n$. Данная характеристика удобна с практической точки зрения, так как она позволяет оценивать надежность работы Σ на входных наборах. В случае, если речь идет о базисных элементах F_i , то соответствующие функции будем обозначать через $p_i(x_1, \dots, x_{n_i})$.

Можно показать, что, зная функции $p_i(x_1, \dots, x_{n_i})$ для всех базисных элементов F_i из B_2 , можно однозначно определить функцию $q(x_1, \dots, x_n)$ для схемы Σ над B . Для этого, постепенно продвигаясь от входов Σ при $x_1 = \alpha_1, \dots, x_n = \alpha_n$, вычисляем вероятности появления 0 и 1 на выходах элементов, пока не достигнем выхода. Вероятность значения $\bar{f}(\alpha_1, \dots, \alpha_n)$ и есть $q(\alpha_1, \dots, \alpha_n)$.

В силу сказанного, система функций $\{p_i\}$ для базисных элементов из B_2 является полной характеристикой для источника I .

Теперь перейдем к рассмотрению связей между

$$\begin{pmatrix} g_1, \dots, g_m \\ q^{(1)}, \dots, q^{(m)} \end{pmatrix} \quad \text{и} \quad q(x_1, \dots, x_n).$$

Теорема 38. Функция $q(x_1, \dots, x_n)$ однозначно определяется по распределению $\begin{pmatrix} g_1, \dots, g_m \\ q^{(1)}, \dots, q^{(m)} \end{pmatrix}$.

Доказательство. В самом деле, возможны два случая:

а) $g_1(\alpha_1, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_n) = 0$ и в этом случае

$$q(\alpha_1, \dots, \alpha_n) = q^{(2)} g_2(\alpha_1, \dots, \alpha_n) + \dots + q^{(m)} g_m(\alpha_1, \dots, \alpha_n);$$

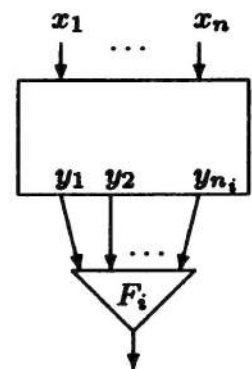


Рис. 89

б) $g_1(\alpha_1, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_n) = 1$ и в таком случае

$$\begin{aligned} q(\alpha_1, \dots, \alpha_n) &= q^{(2)}\overline{g_2}(\alpha_1, \dots, \alpha_n) + \dots + q^{(m)}\overline{g_m}(\alpha_1, \dots, \alpha_n) = \\ &= q^{(2)}(1 - g_2(\alpha_1, \dots, \alpha_n)) + \dots + q^{(m)}(1 - g_m(\alpha_1, \dots, \alpha_n)) = \\ &= 1 - q^{(1)} - (q^{(2)}g_2(\alpha_1, \dots, \alpha_n) + \dots + q^{(m)}g_m(\alpha_1, \dots, \alpha_n)). \end{aligned}$$

Объединяя оба случая, имеем

$$\begin{aligned} q(x_1, \dots, x_n) &= (1 - q^{(1)})g_1(x_1, \dots, x_n) + (q^{(2)}g_2(x_1, \dots, x_n) + \\ &+ \dots + q^{(m)}g_m(x_1, \dots, x_n))(1 - 2g_1(x_1, \dots, x_n)). \end{aligned}$$

Учитывая тождество для булевых величин U и V

$$U \oplus V = U + V - 2UV,$$

получим

$$\begin{aligned} q(x_1, \dots, x_n) &= (q^{(2)}g_1 + q^{(2)}g_2 - 2q^{(2)}g_1g_2) + \dots + \\ &+ (q^{(m)}g_1 + q^{(m)}g_2 - 2q^{(m)}g_1g_m) = \\ &= q^{(2)}(g_1(x_1, \dots, x_n) \oplus g_2(x_1, \dots, x_n)) + \dots + \\ &+ q^{(m)}(g_1(x_1, \dots, x_n) \oplus g_m(x_1, \dots, x_n)). \end{aligned}$$

Если осуществить нормировку режимов функционирования, прибавив к функциям $g_1, \dots, g_m$ по mod2 функцию g_1 , то получим $\tilde{g}_1 = g_1 \oplus g_1 = 0$, $\tilde{g}_2 = g_2 \oplus g_1, \dots, \tilde{g}_m = g_m \oplus g_1$, и выражение для $q(x_1, \dots, x_n)$ примет вид

$$q(x_1, \dots, x_n) = q^{(2)}\tilde{g}_2(x_1, \dots, x_n) + \dots + q^{(m)}\tilde{g}_m(x_1, \dots, x_n)$$

(случай а). В тех случаях, когда важен подсчет вероятностей, можно это делать, считая $g_1(x_1, \dots, x_n) = 0$.

Теорема доказана.

Про функцию q , получаемую по распределению

$$\left(\begin{matrix} g_1, \dots, g_m \\ q^{(1)}, \dots, q^{(m)} \end{matrix} \right),$$

будем говорить, что она соответствует этому распределению.

Т е о р е м а 39. Для каждой функции $q(x_1, \dots, x_n)$ такой, что $0 \leq q(x_1, \dots, x_n) \leq 1$, и схемы Σ , реализующей $f(x_1, \dots, x_n)$, можно найти источник Π с распределением $\left(\begin{matrix} g_1, \dots, g_m \\ q^{(1)}, \dots, q^{(m)} \end{matrix} \right)$ так, что

1) $g_1(x_1, \dots, x_n) = f(x_1, \dots, x_n)$, $g_i \neq g_j$ при $i \neq j$,

2) функция $q(x_1, \dots, x_n)$ соответствует распределению $\left(\begin{matrix} g_1, \dots, g_m \\ q^{(1)}, \dots, q^{(m)} \end{matrix} \right)$.

Доказательство. Если $q(x_1, \dots, x_n) \equiv 0$, то в качестве источника И надо взять источник, не вызывающий в Σ неисправностей — его распределение $\begin{pmatrix} f \\ 1 \end{pmatrix}$.

Если $q(x_1, \dots, x_n) \not\equiv 0$, то покажем, как строится источник для случая $f \equiv 0$.

Обозначим через $\tilde{\alpha}^{(1)}, \dots, \tilde{\alpha}^{(m-1)}$ все наборы, на которых $q > 0$, и пусть они занумерованы так, что

$$q(\tilde{\alpha}^{(1)}) \leq q(\tilde{\alpha}^{(2)}) \leq \dots \leq q(\tilde{\alpha}^{(m-1)}).$$

Возьмем функции $g_1, \dots, g_m$, согласно табл. 11.

Т а б л и ц а 11

	g_1	g_2	g_3		g_{m-1}	g_m
$\tilde{\alpha}^{(1)}$	0	1	0		0	0
$\tilde{\alpha}^{(2)}$	0	1	1		0	0
...	...	...	...		...	...
$\tilde{\alpha}^{(m-2)}$	0	1	1		1	0
$\tilde{\alpha}^{(m-1)}$	0	1	1		1	1
на остальных наборах	0	0	0		0	0

Вероятности $q^{(1)}, \dots, q^{(m)}$ выберем следующим образом:

$$\begin{aligned} q^{(2)} &= q(\tilde{\alpha}^{(1)}), \\ q^{(3)} &= q(\tilde{\alpha}^{(2)}) - q(\tilde{\alpha}^{(1)}), \\ &\dots\dots\dots \\ q^{(m)} &= q(\tilde{\alpha}^{(m-1)}) - q(\tilde{\alpha}^{(m-2)}), \\ q^{(1)} &= 1 - \sum_{i=2}^m q^{(i)} = 1 - q(\tilde{\alpha}^{(m-1)}). \end{aligned}$$

Легко видеть, что построенному распределению вероятностей отвечает исходная функция $q(x_1, \dots, x_n)$:

$$\begin{aligned} & q^{(2)}g_2(x_1, \dots, x_n) + q^{(3)}g_3(x_1, \dots, x_n) + \dots + q^{(m)}g_m(x_1, \dots, x_n) = \\ &= q(\tilde{\alpha}^{(1)})g_2 + (q(\tilde{\alpha}^{(2)}) - q(\tilde{\alpha}^{(1)}))g_3 + \dots + (q(\tilde{\alpha}^{(m-1)}) - q(\tilde{\alpha}^{(m-2)}))g_m = \\ &= q(\tilde{\alpha}^{(1)})(g_2 - g_3) + q(\tilde{\alpha}^{(2)})(g_3 - g_4) + \dots + q(\tilde{\alpha}^{(m-2)})(g_{m-1} - g_m) + \\ &\quad + q(\tilde{\alpha}^{(m-1)})g_m = q(x_1, \dots, x_n). \end{aligned}$$

В случае $f \not\equiv 0$, для построения закона распределений нужно вместо $g_1, \dots, g_m$ взять $g_1 \oplus f, \dots, g_m \oplus f$, а вероятности оставить прежними.

Теорема доказана.

Следующий пример показывает, что выбор распределения по функции $q(x_1, \dots, x_n)$ не однозначен.

Пример. Пусть $q(x_1, \dots, x_n) \equiv \frac{1}{2}$ и Σ реализует $f(x_1, \dots, x_n)$.

1. Возьмем распределение $\left(\frac{g_1}{2^{2^n}}, \dots, \frac{g_{2^{2^n}}}{2^{2^n}}\right)$, где $g_1, \dots, g_{2^{2^n}}$ — все булевы функции от n переменных и $g_1 = f(x_1, \dots, x_n)$. Ясно, что на любом наборе $(\alpha_1, \dots, \alpha_n)$ половина функций принимает значение 0 и половина — 1. Поэтому ровно в половине случаев будет изменяться значение, т. е. происходить ошибка. Отсюда вероятность ошибки на наборе $(\alpha_1, \dots, \alpha_n)$ равна $\frac{1}{2}$.

2. Возьмем распределение $\left(\frac{f}{\frac{1}{2}}, \frac{\bar{f}}{\frac{1}{2}}\right)$. Очевидно, что и в этом случае ошибка на любом наборе имеет вероятность $\frac{1}{2}$.

Итак, в обоих случаях распределениям соответствует одна и та же функция $q(x_1, \dots, x_n)$.

Если рассмотреть распределение $\left(\frac{f(x_1, \dots, x_n)}{1-p}, \frac{\bar{f}(x_1, \dots, x_n)}{p}\right)$, то в этом случае $q(x_1, \dots, x_n) \equiv p$ и проходит доказательство теоремы 37. Поэтому для данного источника $\mathcal{P}(\Sigma) \geq p$.

§ 2. Влияние ошибок на надежность схемы

Появившаяся неисправность элемента в схеме Σ влияет на результат работы других элементов Σ , которые подключены к его выходу, и в конечном счете — на надежность самой схемы. При этом возможны различные эффекты.

1. Эффект нарастания ненадежности. Рассмотрим базис, состоящий из одного ненадежного элемента конъюнктора, и источник И (рис. 90) с распределением вероятностей $\left(\frac{\&}{1-p}, \frac{0}{p}\right)$, $0 < p < 1$.

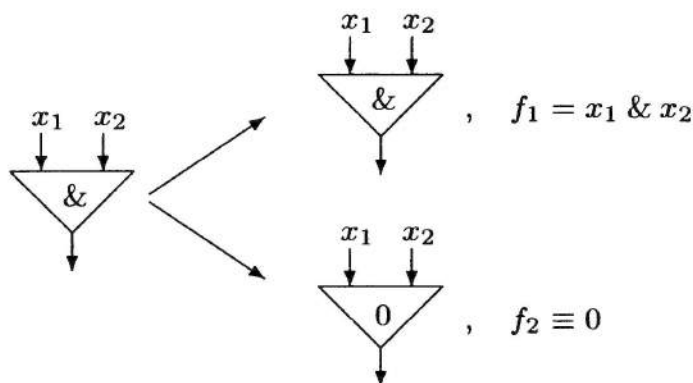


Рис. 90

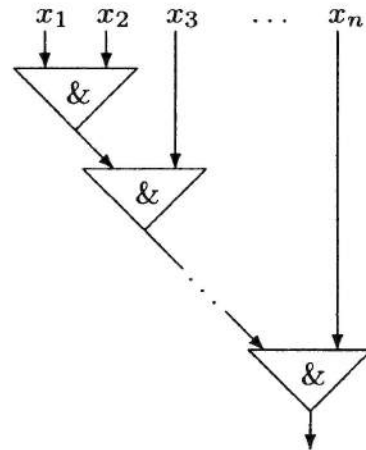


Рис. 91

Очевидно, что схема Σ_n (рис. 91) реализует функцию $x_1 \& \dots \& x_n$ при отсутствии повреждений.

Мы имеем

$$\mathcal{P}(\Sigma_n) = 1 - (1 - p)^{n-1},$$

так как если хоть один элемент поврежден, то на наборе $(1, 1, \dots, 1)$ на выходе получим 0, а не 1. Следовательно, $\mathcal{P}(\Sigma_n) \rightarrow 1$ при $n \rightarrow \infty$, что свидетельствует о нарастании ошибки.

2. В случае базиса $B = B_2$ ($B_1 = \Lambda$), состоящего из одних ненадежных элементов, и источника неймановского типа $\mathcal{P}(\Sigma) \geq p_{\min}$ (теорема 37), т. е. ненадежность схемы Σ ограничена снизу и поэтому не может быть принципиально сделана сколь угодно малой. Другой вывод состоит в том, что в случае неймановского источника невозможно повысить надежность схемы, не имея абсолютно надежных элементов, т. е. $B_1 \neq \Lambda$.

3. Существование абсолютно надежных элементов, способных повышать надежность. В качестве примера рассмотрим элемент голосования H (или F_h), содержащий три выхода и реализующий функцию $h(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ (рис. 92).

Пусть на его входы независимым образом подается одна и та же величина x с вероятностями соответственно p_1, p_2, p_3 , $0 \leq p_1, p_2, p_3 \leq 1$. Тогда вероятность θ ошибки на выходе этого элемента (в предположении, что он абсолютно надежен) вычисляется по формуле $\theta = p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3$. Покажем, что θ — неубывающая функция по каждому переменному p_1, p_2, p_3 . В силу симметрии достаточно проверить это для первого аргумента. Вычислим

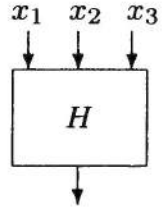


Рис. 92

$$\begin{aligned} \theta(p_1 + \Delta, p_2, p_3) - \theta(p_1, p_2, p_3) &= (p_1 + \Delta)p_2 + (p_1 + \Delta)p_3 + \\ &+ p_2p_3 - 2(p_1 + \Delta)p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3 + 2p_1p_2p_3 = \\ &= \Delta p_2 + \Delta p_3 - 2\Delta p_2p_3 \geq \Delta(p_2 - p_3)^2 \geq 0, \end{aligned}$$

так как $\Delta > 0$, $p_2 \geq p_2^2$, $p_3 \geq p_3^2$.

В силу монотонности θ , если положить $p = \max(p_1, p_2, p_3)$, то $\theta \leq 3p^2 - 2p^3 = \theta_1(p)$. На рис. 93 представлен график функции $\theta_1(p)$. Из графика видно, что при $p < \frac{1}{2}$ имеет место $\theta_1(p) < p$, т. е. ошибка на выходе элемента голосования будет меньше максимальной ошибки на входах, и тем самым элемент голосования позволяет увеличивать надежность входного сигнала.

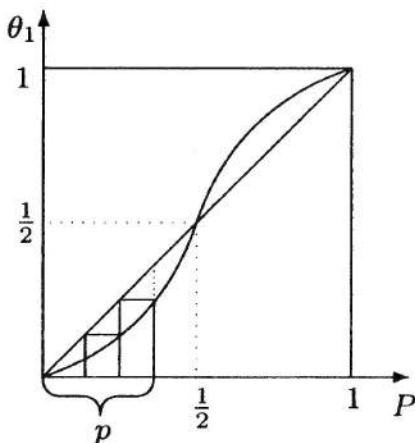


Рис. 93

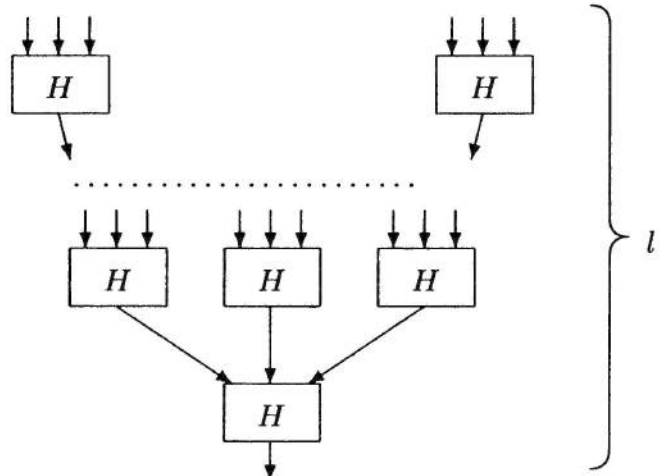


Рис. 94

Рассмотрим схему (рис. 94), представляющую собой дерево с l ярусами, состоящее из элементов H .

Если на входы этой схемы подавать независимым образом величину x с вероятностью ошибки, не превосходящей p , то ошибка на выходе $\theta_l(p)$

будет вычисляться путем итерации функции $\theta_1(p)$:

$$\theta_l(p) = \theta_1(\theta_{l-1}(p)) = \dots = \underbrace{\theta_1(\theta_1(\dots \theta_1(p) \dots))}_{l \text{ раз}},$$

и из графика на рис. 93 видно, что величина $\theta_l(p)$ может быть сделана сколь угодно малой при достаточно большом l . Оценка θ_l через θ_1 выглядит весьма громоздко. Однако, если наложить более жесткие ограничения на p , например, взять $p < \frac{1}{3}$ или, еще лучше, $p < \frac{1}{6}$, то формула существенно упростится:

$$\theta_1 = 3p^2 - 2p^3 < 3p^2 = \frac{1}{3}(3p)^2.$$

Лемма 21. $\theta_l \leq o(\frac{1}{2^{2^l}})$ при $p < \frac{1}{6}$.

Доказательство. Имеем

$$\theta_l(p) \leq \frac{1}{3}(3\theta_{l-1})^{2^1} \leq \frac{1}{3}(3\theta_{l-2})^{2^2} \leq \dots \leq \frac{1}{3}(3\theta_1)^{2^{l-1}} \leq \frac{1}{3}(3p)^{2^l};$$

при $p < \frac{1}{6}$ получаем $3p < \frac{1}{2}$ и $\theta_l(p) = o(\frac{1}{2^{2^l}})$ ($l \rightarrow \infty$).

Лемма доказана.

Возникает вопрос. Задан базис B и источник I . Можно ли для любой булевой функции $f(x_1, \dots, x_n)$ и любого $\varepsilon > 0$ построить схему Σ над B , реализующую функцию $f(x_1, \dots, x_n)$, такую, что $\mathcal{P}(\Sigma) < \varepsilon$? Эту задачу в дальнейшем мы будем называть задачей о построении сколь угодно надежных схем из ненадежных элементов или просто — задачей о построении надежных схем из ненадежных элементов.

Мы уже сразу можем сказать, что эта задача разрешима не всегда: при определенном выборе базисов и источников I сколь угодно надежных схем построить нельзя.

В 1956 г. Дж. фон Нейманом [40] было показано (правда, не совсем в этих терминах), что существует базис и источник I , при которых возможно построение сколь угодно надежных схем.

Теорема 40. Пусть $B = B_1 \cup B_2$, где $B_1 = \{H\}$, $B_2 = \{F_{\neg}, F_{\&}, F_{\vee}\}$ (H — элемент голосования, $F_{\neg}$, $F_{\&}$, $F_{\vee}$ — инвертор, конъюнктор и дизъюнктор соответственно), а источник I таков, что $p_1 = \mathcal{P}(F_{\neg})$, $p_2 = \mathcal{P}(F_{\&})$, $p_3 = \mathcal{P}(F_{\vee})$ и $p = \max\{p_1, p_2, p_3\} < \frac{1}{2}$. Тогда для любой булевой функции $f(x_1, \dots, x_n)$ и любого $\varepsilon > 0$ можно построить схему Σ_{ε} над B , реализующую f и такую, что $\mathcal{P}(\Sigma_{\varepsilon}) < \varepsilon$.

Доказательство. В базисе B для данной функции f построим схему Σ , реализующую f , не налагая на нее никаких требований о надежности. Пусть $L = L(\Sigma)$ — сложность Σ . Заменим в Σ каждый из элементов $F_{\neg}$, $F_{\&}$ и $F_{\vee}$ на $F_{\neg}^{(l)}$, $F_{\&}^{(l)}$ и $F_{\vee}^{(l)}$ (см. рис. 95, где вместо F надо взять $F_{\neg}$, $F_{\&}$, $F_{\vee}$), а полученную схему обозначим через $\Sigma^{(l)}$. Очевидно, что $F_{\neg}^{(l)}$, $F_{\&}^{(l)}$ и $F_{\vee}^{(l)}$ реализует те же функции, что и $F_{\neg}$, $F_{\&}$ и $F_{\vee}$, а поэтому схема $\Sigma^{(l)}$ тоже реализует функцию f .

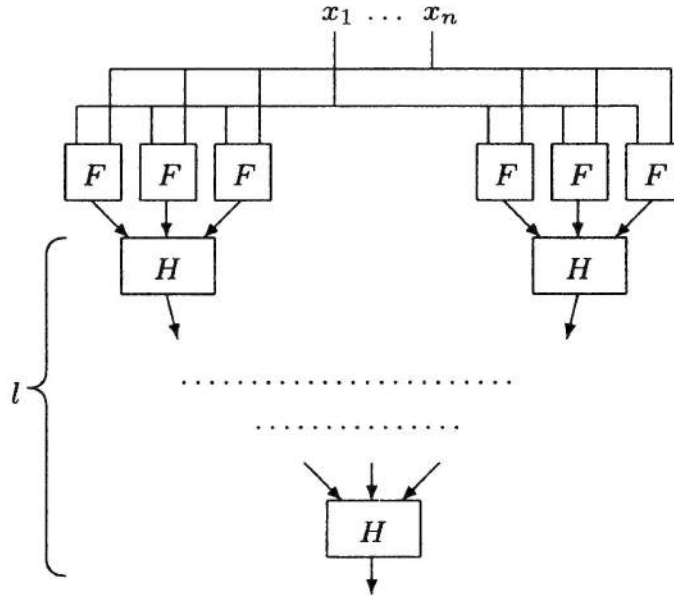


Рис. 95

Выберем $l = l_\varepsilon$ таким, чтобы $\mathcal{P}(F_{\neg}^{(l)})$, $\mathcal{P}(F_{\&}^{(l)})$ и $\mathcal{P}(F_{\vee}^{(l)}) \leq \frac{\varepsilon}{L}$, а построенную таким образом схему $\Sigma^{(l)}$ обозначим через Σ_ε ; возможность указанного выбора вытекает из леммы 21. Эта схема реализует функцию f и для нее

$$\mathcal{P}(\Sigma_\varepsilon) \leq \max\{\mathcal{P}(F_{\neg}^{(l)}), \mathcal{P}(F_{\&}^{(l)}), \mathcal{P}(F_{\vee}^{(l)})\} \cdot L \leq \varepsilon.$$

Теорема доказана.

З а м е ч а н и е. Легко видеть, что схема Σ_ε намного сложнее схемы Σ .

В самом деле, при замене элемента F на $F^{(l)}$ при подсчете сложности схемы вместо $L(F)$ надо взять величину $L(F^{(l)})$, которая может быть найдена на основе рис. 94, 95:

$$L(F^{(l)}) = 3^l L(F) + (1 + 3 + \dots + 3^{l-1})L(H) = 3^l L(F) + \frac{3^l - 1}{2} L(H).$$

Если сложность L обозначает число элементов, т. е. сложность каждого элемента базиса равна 1, то

$$L(F^{(l)}) = \frac{3^{l+1} - 1}{2} \sim \frac{3^{l+1}}{2} \quad (l \rightarrow \infty).$$

Теперь немного подробнее рассмотрим зависимость возможности построения сколь угодно надежных систем для произвольных булевых функций от выбора базиса и источника помех.

Здесь наиболее полный результат получен в 1975 г. В.В. Тарасовым [22, 23] для источников И, которые для всех надежных элементов F_i из B_2 имеют функции $p_i(x_1, \dots, x_{n_i})$, определяющие вероятность неправильной работы элемента на каждом входном наборе, такие, что $0 < \eta < p_i(x_1, \dots, x_{n_i}) < 1 - \eta$ (в частности — для неймановских

источников). Упомянутый результат характеризует необходимые и достаточные условия на базис $B = B_1 \cup B_2$, при которых для любой булевой функции возможно построение сколь угодно надежных схем. Эти условия не очень сложны, однако требуют введения ряда новых понятий, поэтому здесь не формулируются.

В то же время для произвольных источников I можно дать следующий критерий.

Теорема 41. *Для того, чтобы в базисе B с источником I для любой булевой функции можно было построить сколь угодно надежную схему, необходимо и достаточно, чтобы можно было бы построить сколь угодно надежную схему для каждой функции из некоторой полной системы.*

Доказательство. Необходимость условия очевидна. Для установления достаточности рассмотрим некоторую полную систему $\varphi_1, \dots, \varphi_l$, все функции которой допускают сколь угодно надежную реализацию в базисе B .

Пусть $f(x_1, \dots, x_n)$ — произвольная булева функция и $\varepsilon > 0$ — произвольное число. Рассмотрим реализацию f в базисе $\{F_{\varphi_1}, \dots, F_{\varphi_l}\} = B'$. Соответствующую схему обозначим через Σ , а через $L(\Sigma)$ — число элементов в ней. Положим $\delta = \frac{\varepsilon}{L(\Sigma)}$ и построим реализацию функций $\varphi_1, \dots, \varphi_l$ в базисе B с ненадежностью, не превосходящей δ . Если теперь в схеме Σ заменить элементы $F_{\varphi_1}, \dots, F_{\varphi_l}$ на указанные реализации, то получим схему Σ^ε и

$$\mathcal{P}(\Sigma^\varepsilon) \leq \frac{\varepsilon}{L(\Sigma)} \cdot L(\Sigma) = \varepsilon.$$

Теорема доказана.

Замечание. Данная теорема представляет собой обобщение теоремы Неймана (теоремы 40).

Пример (см. [22]). Пусть $B = B_2 = \{F_1\}$, где F_1 — элемент, реализующий в исправном состоянии функцию $f = x_1 + x_2 \pmod{2}$.

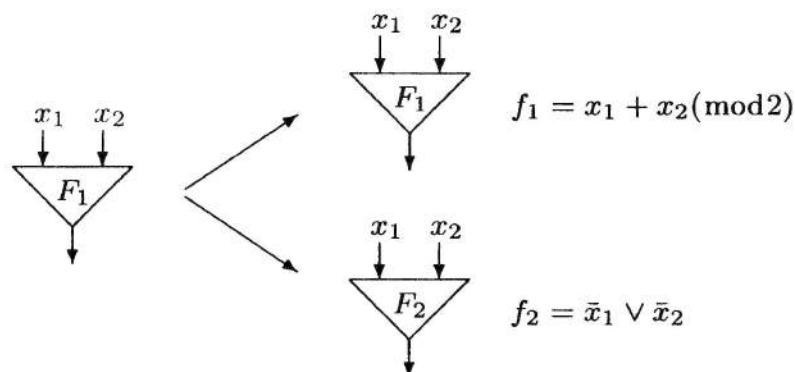


Рис. 96

Пусть, далее, I — источник, действующий на F_1 так, как указано на рис. 96, с распределением вероятностей $\begin{pmatrix} f_1, & f_2 \\ 1-p, & p \end{pmatrix}$, где $0 < p < \frac{1}{2}$.

Функции f_1 и f_2 совпадают на всех наборах кроме $(0, 0)$. Это позволяет легко найти функции, реализуемые схемами Σ_n (рис. 97) и их вероятностные параметры.

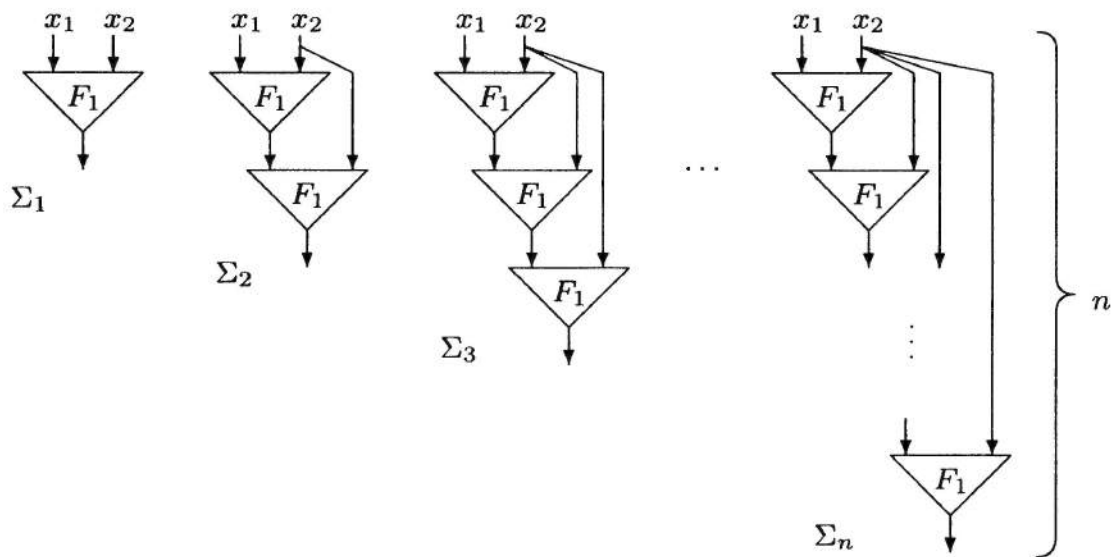


Рис. 97

Для наглядности эти вычисления сведены в таблицы 12–14.

Т а б л и ц а 12

Σ_{2i}	$x_1 \backslash x_2$	0	1
	0	0 1	0
	1	1	1

Т а б л и ц а 13

Σ_{2i+1}	$x_1 \backslash x_2$	0	1
	0	0 1	1
	1	1	0

Т а б л и ц а 14

	x_1	x_2	0	1
Σ_1	0	0	$1 - p$	p
Σ_2	0	0	$(1 - p)^2$	$p + (1 - p)p$
Σ_3	0	0	$(1 - p)^3$	$p + (1 - p)p + (1 - p)^2p$
...	...	...	...	...
Σ_{2i}	0	0	$(1 - p)^{2i}$	$p + (1 - p)p + \dots + (1 - p)^{2i-1}p$
Σ_{2i+1}	0	0	$(1 - p)^{2i+1}$	$p + (1 - p)p + \dots + (1 - p)^{2i}p$

Отсюда видно, что $\{\Sigma_{2i+1}\}$ реализует функцию Шеффера $\bar{x}_1 \vee \bar{x}_2$ сколь угодно надежно при $0 < p < 1$. В силу предыдущей теоремы исходный базис позволяет реализовывать любую булеву функцию сколь угодно надежным образом. При этом следует обратить внимание на то, что:

- 1) базис Б состоит только из ненадежных элементов;
- 2) базис Б в исправном состоянии не является полным;
- 3) наличие источника неисправностей иногда может давать дополнительные возможности для реализации булевых функций.

§ 3. Синтез систем из функциональных элементов в базисе

$$B = \{F_{\neg}, F_{\&}, F_{\vee}, F_h\}$$

Обсуждая вопрос о построении сколь угодно надежных схем, мы никак не касались вопросов сложности. Наша дальнейшая задача — изучение сложности минимальных схем, для которых $\mathcal{P}(\Sigma) < \varepsilon$, и методов их построения. Наши рассуждения будут происходить в конкретном классе схем из функциональных элементов, а именно, в классе схем из Ф.Э. над базисом $B = B_1 \cup B_2$, где $B_1 = F_h$ и $B_2 = \{F_{\neg}, F_{\&}, F_{\vee}\}$. Для решения вышеуказанных задач необходимо уметь строить достаточно простые схемы из Ф.Э. в базисе $B = \{F_{\neg}, F_{\&}, F_{\vee}, F_h\}$ без требования надежности. Последнее можно осуществить, опираясь на общий результат О.Б. Лупанова [12], касающийся синтеза схем из Ф.Э. в произвольном конечном базисе. Однако с практической точки зрения выгодно иметь прямой способ синтеза в указанном базисе, использующий специальные разложения функций через базисные операции $\{\neg, \&, \vee, h\}$ (см. [33]).

Данный параграф начнем с формулировки и доказательства двух вспомогательных утверждений (лемм).

Будем рассматривать ориентированные от корня деревья. В них будем различать концевые вершины и вершины внутренние, не являющиеся концевыми. Совокупность ребер, исходящих из внутренней вершины, называется полужездой. Ориентированное дерево называется однородным порядка k , если все его полужезды имеют порядок k , кроме, быть может, одной — особой полужезды, имеющей порядок k' , где $1 < k' < k$.

Пусть $q > 1$, $k = 3$ и пусть $\lambda = [\log_3 q]$. Построим дерево $\mathcal{D}$, удовлетворяющее следующим свойствам:

- 1) $\mathcal{D}$ — однородное дерево порядка 3;
- 2) в $\mathcal{D}$ все ярусы от 1 до λ заполнены полностью; если $\lambda < \log_3 q$, то $(\lambda + 1)$ -ярус заполнен частично и так, что сначала идут полужезды порядка 3, затем, возможно, особая полужезда порядка 2;
- 3) общее число концевых вершин $\mathcal{D}$ равно q .

В силу выбора $\lambda = [\log_3 q]$ имеем $3^\lambda \leq q < 3^{\lambda+1}$ и для построения требуемого дерева $\mathcal{D}$ берем дерево с λ ярусами, в котором из каждой внутренней вершины исходит ровно три ребра (случай $1 < q < 3$ очевиден). В этом дереве ровно 3^λ концевых вершин и если $q = 3^\lambda$, то процесс построения закончен. Если же $3^{\lambda+1} > q > 3^\lambda$, то рассмотрим равенство

$$q - 3^\lambda = 2v + w, \quad w = 0, 1. \quad (*)$$

К первым v концевым вершинам λ -яруса этого дерева пристраиваем полужезды порядка 3, а если $w = 1$, то к $(v + 1)$ -й концевой вершине — полужезду порядка 2 (см. рис. 98, а).

Очевидно, что построенное дерево удовлетворяет п.п. 1)–3) и в силу равенства (*) имеет q концевых вершин, так как при пристройке полужезды одна концевая вершина уничтожается, а добавляется столько вершин, сколько содержится концевых вершин в полужезде.

Л е м м а 22. *Дерево $\mathcal{D}$, удовлетворяющее п.п. 1)–3), содержит $[q/2]$ внутренних вершин.*

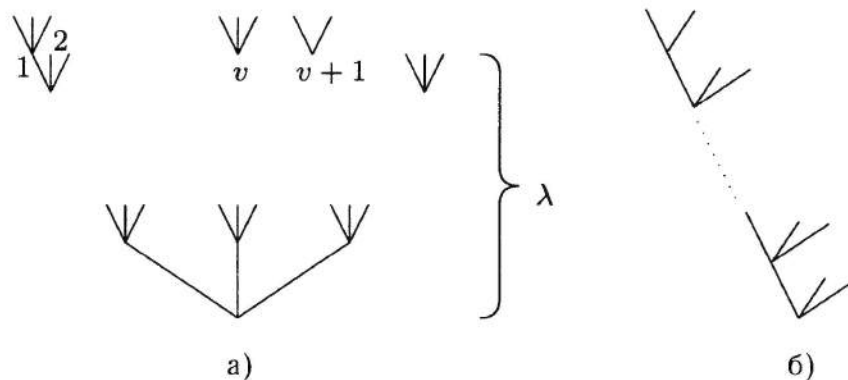


Рис. 98

Доказательство. Основано на преобразовании дерева $\mathcal{D}$ в дерево $\mathcal{D}'$ (рис. 98, б) путем постепенного перемещения полужезд. При каждом таком перемещении некоторая внешняя полужезда сначала отрывается от дерева и при этом возникает новая концевая вершина; затем эта полужезда прикрепляется своим центром к другой концевой вершине, которая перестает быть концевой. Таким образом, на каждом шаге преобразования число концевых вершин, число внутренних вершин и число ребер не меняются. В дереве $\mathcal{D}'$, очевидно, $\lfloor q/2 \rfloor$ внутренних вершин.

Лемма доказана.

В дереве $\mathcal{D}$ пронумеруем концевые вершины числами от 1 до q и для каждой концевой вершины j выберем поддерево $\mathcal{D}_j$ так, что:

- (1) $\mathcal{D}_j$ и $\mathcal{D}$ имеют общий корень;
- (2) $\mathcal{D}_j$ содержит вершину j ;
- (3) концевые вершины $\mathcal{D}_j$ являются концевыми вершинами $\mathcal{D}$;
- (4) каждая внутренняя вершина дерева $\mathcal{D}_j$ имеет порядок полужезды, равный 2.

Очевидно, что $\mathcal{D}_j$ с каждой полужездой дерева $\mathcal{D}$ либо не имеет общих ребер, либо имеет ровно два.

Пусть булева функция $f(x_1, \dots, x_n)$ задана при помощи табл. 15, где значение $f(\sigma_1, \dots, \sigma_k, \sigma_{k+1}, \dots, \sigma_n)$ стоит на пересечении строки $(\sigma_1, \dots, \sigma_k)$ и столбца $(\sigma_{k+1}, \dots, \sigma_n)$.

Т а б л и ц а 15

			σ_{k+1}		x_{k+1}
			$\vdots$		$\vdots$
			σ_n		x_n
$x_1 \dots x_k$					
0 ... 0					s
.....					
					s
.....					s - i-я полоса
$\sigma_1 \dots \sigma_k$					
.....					
1 ... 1					

Строки таблицы разделим на полосы шириной s (кроме, может быть, последней, которая содержит s' строк, $s' \leq s$). Пусть q — число полос. Очевидно, $q = \lceil \frac{2^k}{s} \rceil$. Занумеруем полосы сверху вниз числами $1, \dots, q$. Обозначим через $\psi_i(x_1, \dots, x_k)$ характеристическую функцию i -й полосы. Очевидно, что функция

$$g_{\sigma_{k+1}, \dots, \sigma_n}^i(x_1, \dots, x_k) = \psi_i(x_1, \dots, x_k) f(x_1, \dots, x_k, \sigma_{k+1}, \dots, \sigma_n)$$

определяется пересечением i -й полосы таблицы со столбцом $(\sigma_{k+1}, \dots, \sigma_n)$, т. е. определяет «короткий» столбец таблицы (заштриховано в таблице).

Положим далее

$$G_{\sigma_{k+1}, \dots, \sigma_n}^i(x_1, \dots, x_k) = g_{\sigma_{k+1}, \dots, \sigma_n}^i(x_1, \dots, x_k) \vee \bigvee_{j \in \Xi_i} \psi_j(x_1, \dots, x_k),$$

где множество Ξ_i включает те и только те числа j , для которых дерево $\mathcal{D}_j$ ($j \neq i$) содержит вершину i . Функция $G_{\sigma_{k+1}, \dots, \sigma_n}^i(x_1, \dots, x_k)$ определяет «удлиненный» столбец, состоящий из короткого столбца $g_{\sigma_{k+1}, \dots, \sigma_n}^i$ и единичных столбцов некоторых полос (определяются множеством Ξ_i).

Сопоставим дереву $\mathcal{D}$ функцию $H(z_1, \dots, z_q)$, считая, что каждой полузвезде порядка 3 соответствует функция $h(u, v, w)$, полузвезде порядка 2 — $h(u, v, 0)$, а концевым вершинам $1, \dots, q$ — переменные $z_1, \dots, z_q$.

Л е м м а 23.

$$\begin{aligned} f(x_1, \dots, x_k, \sigma_{k+1}, \dots, \sigma_n) &= \\ &= H(G_{\sigma_{k+1}, \dots, \sigma_n}^1(x_1, \dots, x_k), \dots, G_{\sigma_{k+1}, \dots, \sigma_n}^q(x_1, \dots, x_k)). \end{aligned}$$

Д о к а з а т е л ь с т в о. Пусть $x_1 = \sigma_1, \dots, x_k = \sigma_k$. Найдем значения функций $G_{\sigma_{k+1}, \dots, \sigma_n}^1(\sigma_1, \dots, \sigma_k), \dots, G_{\sigma_{k+1}, \dots, \sigma_n}^q(\sigma_1, \dots, \sigma_k)$. Предположим, что $(\sigma_1, \dots, \sigma_k)$ лежит в i -й полосе. Тогда

$$\begin{aligned} g_{\sigma_{k+1}, \dots, \sigma_n}^\nu(\sigma_1, \dots, \sigma_k) &= \begin{cases} f(\sigma_1, \dots, \sigma_n) & \text{при } \nu = i, \\ 0 & \text{при } \nu \neq i, \end{cases} \\ \psi_j(\sigma_1, \dots, \sigma_k) &= \begin{cases} 1 & \text{при } j = i, \\ 0 & \text{при } j \neq i, \end{cases} \\ G_{\sigma_{k+1}, \dots, \sigma_n}^\nu(\sigma_1, \dots, \sigma_k) &= \begin{cases} f(\sigma_1, \dots, \sigma_n) & \text{при } \nu = i, \\ 1 & \text{при } \nu \neq i, \quad i \in \Xi_\nu, \\ 0 & \text{при } \nu \neq i, \quad i \notin \Xi_\nu. \end{cases} \end{aligned}$$

В последнем выражении условия $i \in \Xi_\nu$ и $i \notin \Xi_\nu$ эквивалентны соответственно $\nu \in \mathcal{D}_i$ и $\nu \notin \mathcal{D}_i$. Таким образом, при $x_1 = \sigma_1, \dots, x_k = \sigma_k$ имеет место равенство

$$H(G_{\sigma_{k+1}, \dots, \sigma_n}^1(\sigma_1, \dots, \sigma_k), \dots, G_{\sigma_{k+1}, \dots, \sigma_n}^q(\sigma_1, \dots, \sigma_k)) = H(\gamma_1, \dots, \gamma_q),$$

где набор $(\gamma_1, \dots, \gamma_q)$ на входах, соответствующих конечным вершинам из $\mathcal{D} \setminus \mathcal{D}_i$, дает 0, а на входах, соответствующих конечным вершинам дерева $\mathcal{D}_i$, дает всюду 1, кроме входа с номером i , на который поступает $f(\sigma_1, \dots, \sigma_n)$ (рис. 99).

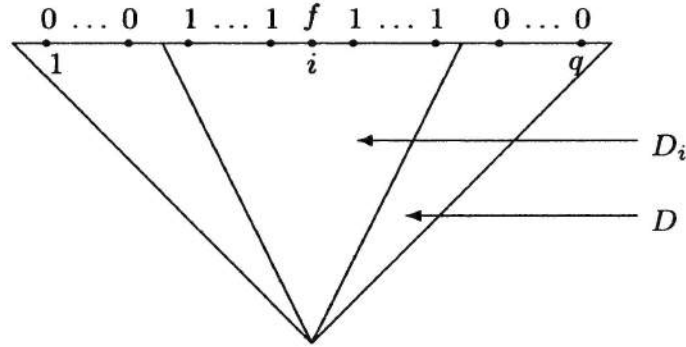


Рис. 99

Из чертежа видно, что, спускаясь по дереву, голосование дает на выходе значение $f(\sigma_1, \dots, \sigma_n)$, т. е.

$$H(\gamma_1, \dots, \gamma_q) = f(\sigma_1, \dots, \sigma_n).$$

Лемма доказана.

Пусть Σ — схема из Ф.Э. в базисе $\mathcal{B}$. Обозначим через $L_{\mathcal{B}}^{\neg, \&, \vee}(\Sigma)$ и $L_{\mathcal{B}}^h(\Sigma)$ соответственно число элементов $F_{\neg}$, $F_{\&}$, $F_{\vee}$ и число элементов F_h в схеме Σ .

Теорема 42. Для любого натурального m , где $m = m(n)$ и $m(n) = o(\frac{n}{\log n})$, существует алгоритм, который для каждой булевой функции $f(x_1, \dots, x_n)$ строит схему $\Sigma_{f(x_1, \dots, x_n)}$ над базисом $\mathcal{B}$ так, что

$$L_{\mathcal{B}}(\Sigma_{f(x_1, \dots, x_n)}) \lesssim \frac{1}{2} \cdot \frac{2^n}{n}$$

и

$$\frac{L_{\mathcal{B}}^{\neg, \&, \vee}(\Sigma_{f(x_1, \dots, x_n)})}{L_{\mathcal{B}}^h(\Sigma_{f(x_1, \dots, x_n)})} = o\left(\frac{1}{n^m}\right).$$

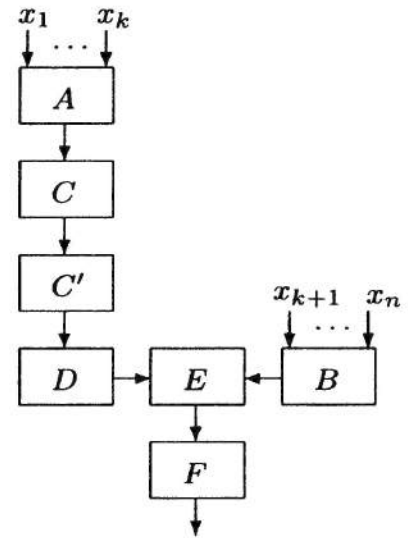


Рис. 100

Доказательство. Будем строить искомую схему Σ_f из блоков A, B, C, C', D, E, F с учетом табл. 15 так, как это указано на рис. 100.

Блок A реализует все конъюнкции $x_1^{\sigma_1} \dots x_k^{\sigma_k}$;

$$L_{\mathcal{B}}(A) \leq k + k2^k.$$

Блок B реализует все конъюнкции $x_{k+1}^{\sigma_{k+1}} \dots x_n^{\sigma_n}$;

$$L_{\mathcal{B}}(B) \leq (n - k) + (n - k)2^{n-k}.$$

Блок C реализует в виде совершенной д.н.ф. все «короткие» столбцы и функции ψ_j ;

$$L_B(C) \leq sq2^s.$$

Блок C' реализует с помощью дизъюнкторов все «удлиненные» столбцы;

$$L_B(C') \leq \sum_{i=1}^q t(i)|\Xi_i| \leq 2^s \sum_{i=1}^q |\Xi_i| \leq 2^s q^2,$$

где $t(i)$ — число различных столбцов в i -й полосе и отдельное слагаемое $t(i)|\Xi_i|$ оценивает число дизъюнкторов, необходимое для получения «удлиненных» столбцов, исходя из «коротких» столбцов i -й полосы.

Блок D реализует все функции $f(x_1, \dots, x_k, \sigma_{k+1}, \dots, \sigma_n)$, согласно лемме 23, исходя из формул

$$H(G_{\sigma_{k+1}, \dots, \sigma_n}^1(x_1, \dots, x_k), \dots, G_{\sigma_{k+1}, \dots, \sigma_n}^q(x_1, \dots, x_k)).$$

Для этого по лемме 22 требуется $[q/2]$ элементов F_h на каждую формулу и, быть может, нужно реализовать 0 (для чего требуется два элемента);

$$L_B(D) = [q/2]2^{n-k} + \Delta \quad (\Delta = 0 \text{ или } 2).$$

Блок E реализует функции вида $x_{k+1}^{\sigma_{k+1}} \dots x_n^{\sigma_n} f(x_1, \dots, x_k, \sigma_{k+1}, \dots, \sigma_n)$;

$$L_B(E) \leq 2^{n-k}.$$

Блок F реализует функцию $f(x_1, \dots, x_n)$;

$$L_B(F) \leq 2^{n-k}.$$

Положим далее $k = [(m+3) \log_2 n]$ и $s = [n - (3m+6) \log_2 n]$. Мы имеем

$$L_B(A) \lesssim (m+3) \log_2 n \cdot n^{m+3} = \frac{2^n}{n^{m+1}} \frac{2^{o(n)}}{2^n} = o\left(\frac{2^n}{n^{m+1}}\right),$$

$$L_B(B) \lesssim \frac{2n \cdot 2^n}{n^{m+3}} = o\left(\frac{2^n}{n^{m+1}}\right),$$

$$L_B(C) \lesssim 2^{s+k} \leq 2^{n-(2m+3) \log_2 n} \sim \frac{2^n}{n^{2m+3}} = o\left(\frac{2^n}{n^{m+1}}\right),$$

$$L_B(C') \lesssim \frac{2^{s+2k}}{s^2} \lesssim \frac{2^{n-m \log_2 n}}{n^2} = \frac{2^n}{n^{m+2}} = o\left(\frac{2^n}{n^{m+1}}\right),$$

$$L_B(D) \sim L_B^h(\Sigma_n) \sim \frac{2^n}{2 \cdot s} \sim \frac{1}{2} \frac{2^n}{n},$$

$$L_B(E) \lesssim L_B(B) = o\left(\frac{2^n}{n^{m+1}}\right),$$

$$L_B(F) \lesssim L_B(B) = o\left(\frac{2^n}{n^{m+1}}\right).$$

Отсюда

$$L_B(n) \leq L_B(\Sigma_{f(x_1, \dots, x_n)}) \sim \frac{1}{2} \frac{2^n}{n}$$

и

$$\frac{L_B^{-, \&, \vee}(\Sigma_{f(x_1, \dots, x_n)})}{L_B^h(\Sigma_{f(x_1, \dots, x_n)})} = \frac{o\left(\frac{2^n}{n^{m+1}}\right)}{\frac{1}{2} \frac{2^n}{n}} = o\left(\frac{1}{n^m}\right).$$

Теорема доказана.

Как установлено в [12], нижняя оценка для $L_B(n)$ имеет вид

$$L_B(n) \gtrsim \frac{1}{2} \frac{2^n}{n}.$$

Поэтому

$$L_B(n) \sim \frac{1}{2} \frac{2^n}{n}.$$

§ 4. Асимптотически оптимальный метод построения надежных схем из ненадежных элементов

В этом параграфе рассматриваются схемы из Ф.Э. в базисе $B_p = B_1 \cup B_2$, где $B_1 = \{F_h\}$ и $B_2 = \{F_-, F_&, F_\vee\}$, а $p = \max\{\mathcal{P}(F_-), \mathcal{P}(F_&), \mathcal{P}(F_\vee)\}$ ($0 < p < \frac{1}{2}$).

Пусть $\varepsilon > 0$ — некоторое число. Обозначим через $\mathfrak{S}^\varepsilon$ класс всех схем Σ в базисе B_p таких, что $\mathcal{P}(\Sigma) < \varepsilon$. В силу теоремы 40 класс $\mathfrak{S}^\varepsilon$ содержит схемы, реализующие любые булевы функции.

Пусть далее

$$L_{B_p}(f, \varepsilon) = \min_{\substack{\Sigma \\ \Sigma \text{ реализ. } f \\ \mathcal{P}(\Sigma) < \varepsilon}} L_{B_p}(\Sigma) \quad \text{и} \quad L_{B_p}(n, \varepsilon) = \max_{f, f \in P_2^n} L_{B_p}(f, \varepsilon).$$

Очевидно, $L_{B_p}(n, \varepsilon)$ — функция Шеннона, характеризующая сложность реализации булевых функций от n переменных в классе $\mathfrak{S}^\varepsilon$.

Теорема 43. *Существует алгоритм, который для каждой булевой функции $f(x_1, \dots, x_n)$ строит схему $\Sigma_{f(x_1, \dots, x_n)}$ из $\mathfrak{S}^\varepsilon$ такую, что*

- 1) $L_{B_p}(\Sigma_{f(x_1, \dots, x_n)}) \lesssim \frac{1}{2} \frac{2^n}{n}$,
- 2) для любого $\varepsilon > 0$ существует $N(\varepsilon)$ такое, что если $n > N(\varepsilon)$, то $\mathcal{P}(\Sigma_{f(x_1, \dots, x_n)}) < \varepsilon$, т. е. $\Sigma_{f(x_1, \dots, x_n)} \in \mathfrak{S}^\varepsilon$.

Доказательство.

1. Положив $m = 3$, построим в соответствии с теоремой 42 последовательность $\{\Sigma'_{f(x_1, \dots, x_n)}\}$ схем над базисом B , для которой

$$L_B(\Sigma'_{f(x_1, \dots, x_n)}) \sim \frac{1}{2} \frac{2^n}{n} \quad \text{и} \quad \frac{L_B^{-, \&, \vee}(\Sigma'_{f(x_1, \dots, x_n)})}{L_B^h(\Sigma'_{f(x_1, \dots, x_n)})} = o\left(\frac{1}{n^3}\right).$$

2. Как в доказательстве теоремы 40, построим элементы $\tilde{F}_\neg = F_\neg^{(l)}$, $\tilde{F}_\& = F_\&^{(l)}$ и $\tilde{F}_\vee = F_\vee^{(l)}$ из элементов базиса B_p так, чтобы

$$\max\{\mathcal{P}(\tilde{F}_\neg), \mathcal{P}(\tilde{F}_\&), \mathcal{P}(\tilde{F}_\vee)\} < \frac{1}{6}.$$

Введем обозначение

$$c = \max\{L_{B_p}(\tilde{F}_\neg), L_{B_p}(\tilde{F}_\&), L_{B_p}(\tilde{F}_\vee)\}.$$

3. Для каждой схемы F рассмотрим схему $\Sigma_F^{(l)}$ (см. рис. 95), содержащую l ярусов элементов голосования, где $l = \lceil \log_2 n \rceil$. Она, очевидно, в исправном состоянии реализует ту же функцию, что и F .

Взяв в качестве схемы F соответственно $\tilde{F}_\neg$, $\tilde{F}_\&$, $\tilde{F}_\vee$, получим схемы $\Sigma_\neg$, $\Sigma_\&$, $\Sigma_\vee$. В этом случае

$$L_{B_p}(\Sigma_F) \leq c3^l + \frac{1}{2}3^l \leq (c+1)3^l \leq 3(c+1)n^{\log_2 3} \leq 3(c+1)n^2.$$

4. Заменим в схеме $\Sigma'_{f(x_1, \dots, x_n)}$ элементы $F_\neg$, $F_\&$, $F_\vee$ соответственно на $\Sigma_\neg$, $\Sigma_\&$, $\Sigma_\vee$, получим схему $\Sigma_{f(x_1, \dots, x_n)}$ над B_p . Очевидно,

$$\begin{aligned} L_{B_p}(\Sigma_f) &\leq L_B^h(\Sigma'_f) + L_B^{\neg, \&, \vee}(\Sigma'_f) \cdot \max\{L_{B_p}(\Sigma_\neg), L_{B_p}(\Sigma_\&), L_{B_p}(\Sigma_\vee)\} \lesssim \\ &\lesssim \frac{1}{2} \frac{2^n}{n} + 3(c+1)n^2 \cdot o\left(\frac{2^n}{n^3}\right) \sim \frac{1}{2} \frac{2^n}{n}, \end{aligned}$$

а с учетом леммы 21

$$\begin{aligned} \mathcal{P}(\Sigma_f) &\leq L_B^{\neg, \&, \vee}(\Sigma'_f) \cdot \max\{\mathcal{P}(\Sigma_\neg), \mathcal{P}(\Sigma_\&), \mathcal{P}(\Sigma_\vee)\} = \\ &= o\left(\frac{2^n}{n^3}\right) \cdot o\left(\frac{1}{2^{2^l}}\right) = o\left(\frac{2^n}{n^3}\right) \cdot o\left(\frac{1}{2^n}\right) = o\left(\frac{1}{n^3}\right), \end{aligned}$$

поскольку $l \geq \log_2 n$, т. е. $2^l \geq n$ и $o\left(\frac{1}{2^{2^l}}\right) = o\left(\frac{1}{2^n}\right)$. Отсюда для любого $\varepsilon > 0$ найдется $N(\varepsilon)$ такое, что при $n > N(\varepsilon)$ будет $\mathcal{P}(\Sigma_f) < \varepsilon$.

Теорема доказана.

С л е д с т в и е. В силу того, что $L_{B_p}(n, \varepsilon) \geq L_B(n)$, и предыдущего результата

$$L_{B_p}(n, \varepsilon) \sim \frac{1}{2} \frac{2^n}{n}.$$

Из свойств нижней оценки и данной асимптотики вытекает также, что при фиксированном $\varepsilon > 0$ для почти всех булевых функций минимальная ε -надежная схема имеет сложность асимптотически равную $\frac{1}{2} \frac{2^n}{n}$, т. е. сложности минимальной схемы без требования надежности. Для указанного класса функций удастся достичь надежной реализации без существенного усложнения схемы.

РАЗДЕЛ 2. СИНТЕЗ САМОКОРРЕКТИРУЮЩИХСЯ СХЕМ

Пусть $\mathcal{U}$ — класс управляющих систем и $\mathcal{I}$ — источник неисправностей. Возьмем У.С. $U \in \mathcal{U}$, где $U = (\Sigma, f)$. Обозначим через $f_1, \dots, f_r$ ($f_1 = f$) функции неисправностей, вызываемые источником $\mathcal{I}$.

Определение. Схема Σ называется самокорректирующейся (относительно источника $\mathcal{I}$), если для любого $i = 1, 2, \dots, r$

$$f_i \equiv f.$$

Естественно, возникает вопрос о существовании самокорректирующихся схем, о методах их построения, об изучении их сложности. Данные вопросы мы рассмотрим для двух классов У.С. — контактных схем и схем из Ф.Э.

§ 1. Построение самокорректирующихся контактных схем

В этом случае обычно рассматривают в качестве источника неисправностей источник $\mathcal{I}_{a,b}$, вызывающий в контактной схеме не более a разрывов и b коротких замыканий контактов, понимая под разрывом (замыканием) контакта x^σ приписывание соответствующему ребру символа 0 (соответственно 1).

При наличии источника $\mathcal{I}_{a,b}$ класс $\mathcal{U}$ расширяется до класса $\mathcal{U}'$, в котором схемы получаются из p -полюсных сетей путем приписывания ребрам символов из алфавита $\{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n, 0, 1\}$. Функционирование определяется естественным образом.

Пусть функция $f(x_1, \dots, x_n)$ реализована контактной схемой Σ . Заменим в ней каждый контакт x^σ на схему, указанную на рис. 101.

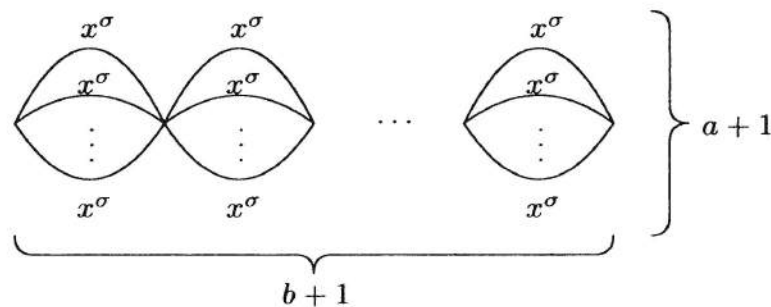


Рис. 101

Полученную схему обозначим через Σ^c . Очевидно, Σ^c реализует ту же функцию $f(x_1, \dots, x_n)$, является самокорректирующейся относительно источника $\mathcal{I}_{a,b}$ и имеет сложность $L(\Sigma^c) = (a + 1)(b + 1)L(\Sigma)$,¹⁵ т. е. в $(a + 1)(b + 1)$ раз большую, чем сложность Σ .

Найденное решение вряд ли можно считать корректным: самокорректирующаяся схема построена за счет усложнений исходной схемы в несколько раз. Можно было бы считать решение корректным, если бы усложнение

¹⁵Сложностью $L(\Sigma)$ контактной схемы называется число контактов в Σ .

схемы Σ было малым по сравнению с $L(\Sigma)$ (при $n \rightarrow \infty$). В дальнейшем приведенное решение будем называть тривиальным. Обозначим через $L_{a,b}(f)$ сложность минимальной самокорректирующейся схемы, реализующей f .

Существуют функции, для которых тривиальные самокорректирующиеся схемы будут минимальными самокорректирующимися схемами. К ним относится, например, функция $x_1 \cdot x_2 \cdot \dots \cdot x_n$. В связи с этим возникает вопрос, а существуют ли нетривиальные самокорректирующиеся схемы? Рассмотрим пример.

Пример. Функция $h(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ может быть реализована схемой Σ (рис. 102), имеющей 5 контактов. В то же время для нее существует самокорректирующаяся схема, относительно $\mathbf{I}_{0,1}$, содержащая 8 контактов (рис. 103) [1].

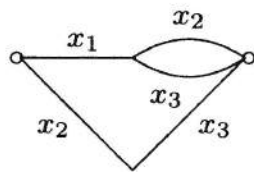


Рис. 102

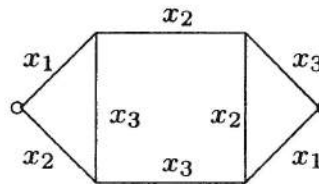


Рис. 103

Отсюда видно, что нетривиальные самокорректирующиеся схемы существуют. Поэтому имеет смысл изучать величину $L_{a,b}(f)$ — сложность минимальных самокорректирующихся относительно $\mathbf{I}_{a,b}$ схем, реализующих функцию f , а также соответствующую функцию Шеннона — $L_{a,b}(n)$. Очевидно, $L_{a,b}(n) \geq L(n)$, т. е. $L_{a,b}(n) \gtrsim \frac{2^n}{n}$. Далее будем исследовать вопрос о построении самокорректирующихся контактных схем для случая простейших источников $\mathbf{I}_{0,1}$ и $\mathbf{I}_{1,0}$.

Теорема 44 (Ю. Г. Потапов, С. В. Яблонский [21]). *Существует метод синтеза, позволяющий для каждой булевой функции $f(x_1, \dots, x_n)$ строить самокорректирующуюся относительно $\mathbf{I}_{0,1}$ схему Σ_f^c такую, что*

$$L(\Sigma_{f(x_1, \dots, x_n)}^c) \lesssim \frac{2^n}{n}.$$

Доказательство.

1. Исходя из разложений

$$f(x_1, \dots, x_n) = \bigvee_{i=1}^p f_i(x_1, \dots, x_n)$$

и

$$f_i(x_1, \dots, x_n) = \bigvee_{j=1}^{t(i)} \bigvee_{h=1}^{\frac{2^r}{r}} f_{ij}^{(1)}(x_1, \dots, x_k) f_{ijh}(x_{k+1}, \dots, x_n),$$

по методу Лупанова [13] находим схему Σ , являющуюся параллельным соединением схем Σ_i , реализующих f_i , для всех $i = 1, \dots, p$. Схема Σ_i

разбивается на три части $\Sigma_i^{(1)}, \Sigma_i^{(2)}, \Sigma_i^{(3)}$ (рис. 104). Часть $\Sigma_i^{(2)}$ состоит из метелок, тип которых определяется центром соответствующей h -й сферы (рис. 105), и объединений контактов, входящих в них. Каждое объединение происходит в пределах метелок одного типа и содержит некоторое количество контактов $x_{k+1}^{\bar{\beta}_{k+1}^h}$, некоторое количество контактов $x_{k+2}^{\bar{\beta}_{k+2}^h}, \dots$, и наконец, некоторое количество контактов $x_{k+r}^{\bar{\beta}_{k+r}^h}$ (рис. 106). На выходах объединений реализуются функции f_{ijk} (где $1 \leq i \leq p \leq \lfloor \frac{2^k}{s} \rfloor$, $1 \leq j \leq t(i) \leq 2^s$, $1 \leq h \leq \frac{2^r}{r}$). Положим далее $\Sigma^{(1)} = \bigcup_i \Sigma_i^{(1)}$, $\Sigma^{(2)} = \bigcup_i \Sigma_i^{(2)}$ и $\Sigma^{(3)} = \bigcup_i \Sigma_i^{(3)}$.

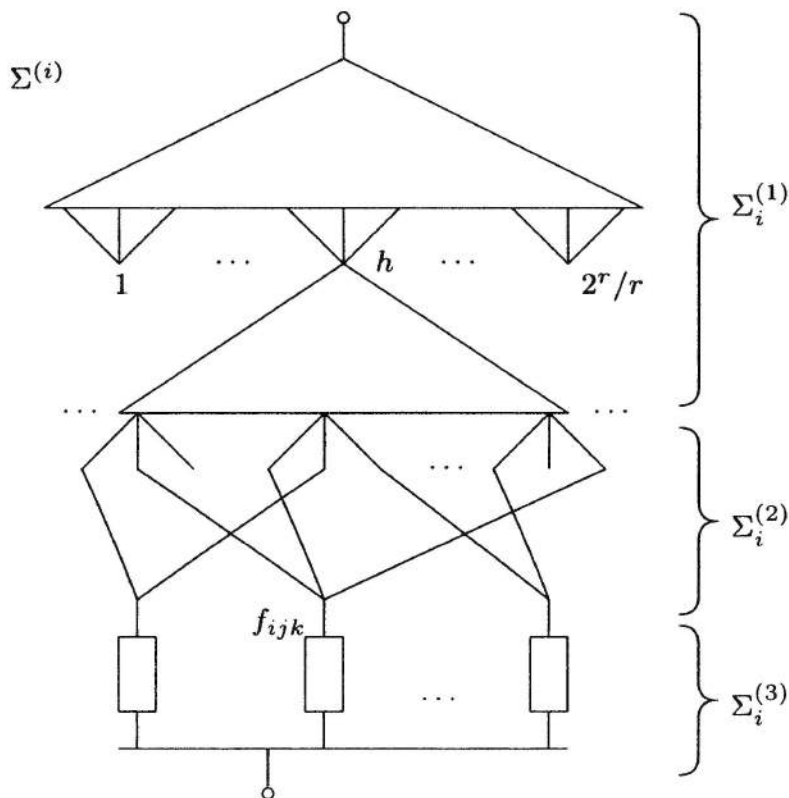


Рис. 104

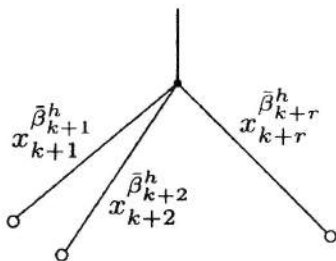


Рис. 105

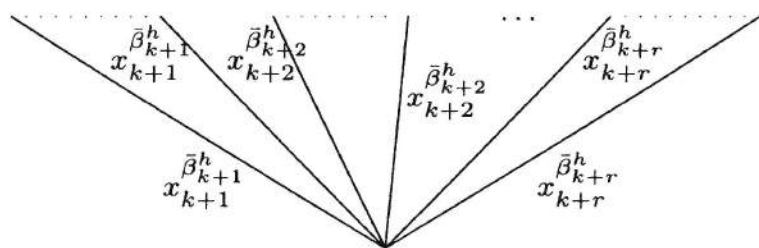


Рис. 106

2. Построим схему Σ_f^c путем переделки схемы Σ . Для этого в частях $\Sigma^{(1)}$ и $\Sigma^{(3)}$ каждый контакт x^σ заменим двумя последовательно соединенными контактами x^σ , а в части $\Sigma^{(2)}$ каждую группу одноименных контактов каждого объединения (рис. 106) последовательно продублируем еще одним

контактом того же типа (рис. 107). Таким образом, на каждую функцию f_{ijh} дополнительно добавляется r контактов. Отсюда

$$L(\Sigma_f^c) \leq 2L(\Sigma^{(1)}) + 2L(\Sigma^{(3)}) + L(\Sigma^{(2)}) + r \frac{2^k}{s} 2^s \frac{2^r}{r}.$$

Нетрудно видеть, что схема Σ_f^c реализует функцию $f(x_1, \dots, x_n)$ и является самокорректирующейся относительно $\Pi_{0,1}$.

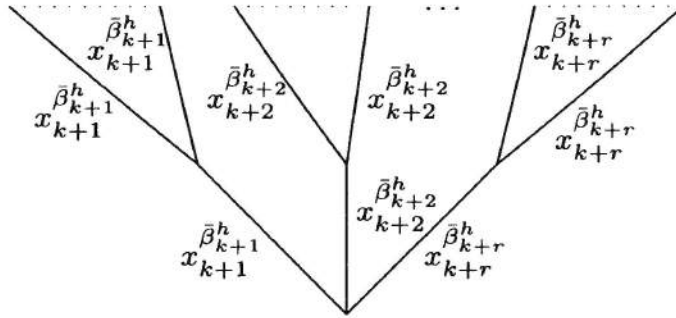


Рис. 107

3. Полагая $r = 2^{\lceil 1/2 \log_2 n \rceil}$, $k = \lfloor 2 \log_2 n \rfloor$ и $s = \lfloor n - 2\sqrt{n} \rfloor$, получим:

$$L(\Sigma^{(2)}) \sim \frac{2^n}{n}, \quad L(\Sigma^{(1)}) = o\left(\frac{2^n}{n}\right), \quad L(\Sigma^{(3)}) = o\left(\frac{2^n}{n}\right)$$

и

$$\frac{2^{k+s+r}}{s} \lesssim n 2^{n-\sqrt{n}} = o\left(\frac{2^n}{n}\right).$$

Следовательно,

$$L(\Sigma_{f(x_1, \dots, x_n)}^c) \lesssim \frac{2^n}{n}.$$

Теорема доказана.

Учитывая нижнюю оценку, мы получаем асимптотику

$$L_{0,1} \sim \frac{2^n}{n},$$

которая означает, что алгоритм синтеза, содержащийся в доказательстве, является асимптотически наилучшим.

Т е о р е м а 45 (Х. А. Мадатян [16]). *Существует метод синтеза, позволяющий для каждой булевой функции $f(x_1, \dots, x_n)$ строить самокорректирующуюся относительно $\Pi_{1,0}$ схему Σ_f^c такую, что*

$$L(\Sigma_{f(x_1, \dots, x_n)}^c) \lesssim \frac{2^n}{n}.$$

Д о к а з а т е л ь с т в о. Отличается от предыдущего вторым этапом. При построении схемы Σ_f^c , исходя из схемы Σ , контакты x^σ из частей

$\Sigma^{(1)}$ и $\Sigma^{(3)}$ заменяются на параллельное соединение двух таких же контактов x^σ , а в части $\Sigma^{(2)}$ каждое объединение, показанное на рис. 106, заменяется на объединение, изображенно на рис. 108.

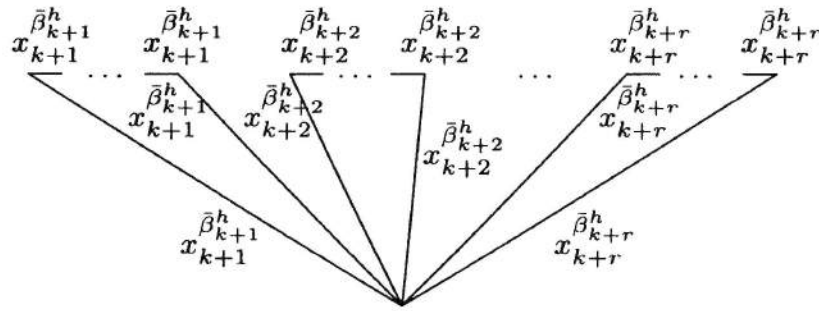


Рис. 108

Эта фигура «двойственная» фигуре на рис. 107. Она состоит из контуров, обеспечивающих связь соответствующих вершин при любом единичном разрыве. Легко видеть, что Σ_f^c является самокорректирующейся относительно $I_{1,0}$ и реализует функцию f . Поскольку число контактов в каждом объединении, показанном на рис. 107, равно числу контактов в соответствующем объединении, изображенном на рис. 108, то выкладочная часть полностью совпадает с выкладками в доказательстве предыдущей теоремы.

Теорема доказана.

Учитывая нижнюю оценку, получаем

$$L_{1,0} \sim \frac{2^n}{n},$$

т. е. алгоритм синтеза является асимптотически наилучшим. Таким образом, для почти всех булевых функций минимальные самокорректирующиеся относительно $I_{0,1}$ (и $I_{1,0}$) схемы имеют сложность асимптотически такую же, как обычные минимальные схемы и асимптотически равную $\frac{2^n}{n}$. Это означает, что предлагаемые в теоремах методы построения самокорректирующихся схем дают корректные решения.

Вопросы построения самокорректирующихся схем относительно источника $I_{a,b}$ исследовались рядом авторов (см. обзор [35]). В частности, показано, что при любых фиксированных a и b имеет место асимптотика

$$L_{a,b}(n) \sim \frac{2^n}{n}.$$

§ 2. Построение самокорректирующихся схем из функциональных элементов

Для данного класса У.С. рассматривается источник I_d , вызывающий неисправности не более d функциональных элементов. При этом предполагается, что под воздействием источника ненадежные элементы могут изменить свое функционирование, сохраняя, однако, прежнее число входов и выходов. Если в рамках указанных ограничений функционирование

каждого ненадежного элемента, находящегося в неисправном состоянии, может быть произвольным, то такой источник будем называть неймановским. В дальнейшем теория рассматривается для неймановских источников. Это объясняется тем, что самокорректирующиеся схемы для неймановских источников I_d будут также самокорректирующимися схемами для более слабых источников с числом единичных повреждений, не превосходящим d .

В случае неймановских источников, очевидно, необходимо, чтобы базис B содержал часть B_1 , состоящую из абсолютно надежных элементов (см. рассуждение в первом параграфе предыдущего раздела).

Итак, $B = B_1 \cup B_2$, где B_1 — часть из надежных элементов, а B_2 — часть из ненадежных элементов.

Теорема 46. Если B_1 содержит элемент голосования H и B — полная система, то для каждой функции $f(x_1, \dots, x_m)$ можно построить самокорректирующуюся относительно I_d схему Σ^c .

Доказательство. Пусть Σ — схема в базисе B , реализующая f . Рассмотрим схему $\Sigma^{(l)}$, которая получается из схемы Σ так же, как схема $F^{(l)}$ получается из схемы F (см. рис. 95). Очевидно, $\Sigma^{(l)}$ реализует f и является самокорректирующейся относительно I_d , если $d \leq \frac{1}{3} \cdot 3^l$. Наименьшее l , удовлетворяющее этому неравенству, есть $l = \lceil \log_3 d \rceil + 1$ и можно считать, что $\Sigma^c = \Sigma^{(l)}$.

Теорема доказана.

Поскольку $L(\Sigma^c) = 3^l L(\Sigma) + \frac{3^l - 1}{2} L(H)$, то видно, что такие самокорректирующиеся схемы — их в дальнейшем будем называть тривиальными — во много раз сложнее исходных. Поэтому, как и в случае контактных схем, данное решение не является корректным. Возникает вопрос о существовании нетривиальных самокорректирующихся схем и об изучении сложности минимальных самокорректирующихся схем.

Пусть $B = B_1 \cup B_2$, где $B_1 = \{H\}$ и $B_2 = \{F_{\neg}, F_{\&}, F_{\vee}\}$, и $L_B(n, d)$ — функция Шеннона для класса самокорректирующихся схем из Ф.Э. над B относительно источника I_d .

Теорема 47 (Г.И. Кириенко [7, 8]¹⁶). Если $\log d(n) = o(n)$, то

$$L_B(n, d) \sim \frac{1}{2} \frac{2^n}{n}.$$

Доказательство. Опирается на конструкцию синтеза схем в базисе B .

1. Возьмем $d(n)$ такое, что $\log d(n) = o(n)$. Выберем целочисленное $l(n)$ из условия

$$d(n) \leq \frac{1}{3} 3^{l(n)}$$

и чтобы $l(n)$ было наименьшим. Тогда

$$\frac{1}{9} \cdot 3^{l(n)} < d(n).$$

¹⁶Здесь дается новое доказательство этого результата.

Далее подберем целочисленную функцию $m(n)$ из условия

$$c3^{l(n)} \leq n^{m(n)},$$

где $c = \max_F (L(F) + \frac{1}{2})$ ($F \in \{F_{\neg}, F_{\&}, F_{\vee}\}$), и чтобы $m(n)$ было наименьшим. Тогда

$$n^{m(n)} < cn3^{l(n)}.$$

Из последнего неравенства и нижней оценки для $d(n)$ имеем

$$\begin{aligned} n^{m(n)} &< cn3^{l(n)} < 9cnd(n), \\ 2^{m(n) \log n} &< 2^{\log d(n) + \log(9cn)}, \\ m(n) \log n &< \log d(n) + \log(9cn). \end{aligned}$$

Отсюда

$$m(n) < \frac{\log d(n)}{\log n} + \frac{\log(9c)}{\log n} + 1 = o\left(\frac{n}{\log n}\right).$$

2. С учетом последней оценки для функции $m(n)$ и $f(x_1, \dots, x_n)$ по теореме 42 можно построить в базисе Б схему Σ_n , ее реализующую и такую, что

$$L_B(\Sigma_n) \sim \frac{1}{2} \frac{2^n}{n} \quad \text{и} \quad \frac{L_{\neg, \&, \vee}(\Sigma_n)}{L^h(\Sigma_n)} = o\left(\frac{1}{n^{m(n)}}\right).$$

3. Элементы $F_{\neg}, F_{\&}, F_{\vee}$ заменяем на $F_{\neg}^{(l(n))}, F_{\&}^{(l(n))}, F_{\vee}^{(l(n))}$, используя конструкцию, указанную на рис. 95. В силу верхней оценки для $d(n)$ схемы $F_{\neg}^{(l(n))}, F_{\&}^{(l(n))}, F_{\vee}^{(l(n))}$ будут самокорректирующимися для $I_{d(n)}$ и их максимальная сложность, учитывая верхнюю оценку для $c3^{l(n)}$, удовлетворяет неравенству

$$\max(L_B(F_{\neg}^{(l(n))}), L_B(F_{\&}^{(l(n))}), L_B(F_{\vee}^{(l(n))})) \leq c3^{l(n)} \leq n^{m(n)}.$$

В результате указанной замены схема Σ_n преобразуется в схему Σ_n^c , реализующую ту же функцию $f(x_1, \dots, x_n)$ и являющуюся самокорректирующейся относительно $I_{d(n)}$.

Из последних оценок имеем

$$\begin{aligned} L_B(\Sigma_n^c) &\lesssim L_B^h(\Sigma_n) + n^{m(n)} L_{\neg, \&, \vee}(\Sigma_n) \sim \\ &\sim L_B^h(\Sigma_n) + L_B^h(\Sigma_n) \cdot o(1) \sim L_B^h(\Sigma_n) \sim \frac{1}{2} \frac{2^n}{n}. \end{aligned}$$

Кроме того, $L_B(n, d) \geq L_B(n)$.

Теорема доказана.

Данная теорема показывает, что для почти всех булевых функций удастся найти корректное решение задачи синтеза самокорректирующихся схем из Ф.Э. в базисе Б относительно источников $I_{d(n)}$, где $\log d(n) = o(n)$,

при котором сложность минимальных самокорректирующихся схем асимптотически равна обычной сложности минимальных схем. Это достигается за счет того, что основная сложность схемы приходится на элементы голосования. В [8] дается другой способ построения, при котором доказывается аналогичная теорема, но доля надежных элементов в самокорректирующейся схеме мала. Развивая эти идеи, Д. Улиг в [24] показал, что при конечном d данного эффекта можно достичь, употребляя конечное число надежных элементов голосования.

ВВЕДЕНИЕ

Рассмотрим класс $\mathcal{U}$ управляющих систем $U = (\Sigma, f)$ и источник неисправностей $\mathcal{I}$. Как отмечалось, он приводит к функциям неисправностей

$$f_1, \dots, f_r, \quad \text{где } f_1 = f,$$

которые, в свою очередь, определяют таблицу функций неисправностей (табл. 16). Поскольку разные неисправности могут приводить к равным функциям неисправностей ($f_i = f_j$), то мы получаем таблицу (табл. 17), в которой представлены функционально различные классы неисправностей исходной таблицы, и $g_1 = f$. Иногда на множестве $E = \{e_i\}$ и $G = \{g_j(e_i)\}$ рассматривают частичный порядок $\preceq$.

Т а б л и ц а 16

	f_1	f_2	$\dots$	f_r
e_1	$f_1(e_1)$	$f_2(e_1)$	$\dots$	$f_r(e_1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
e_N	$f_1(e_N)$	$f_2(e_N)$	$\dots$	$f_r(e_N)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

Т а б л и ц а 17

	g_1	g_2	$\dots$	g_m
e_1	$g_1(e_1)$	$g_2(e_1)$	$\dots$	$g_m(e_1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
e_N	$g_1(e_N)$	$g_2(e_N)$	$\dots$	$g_m(e_N)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

Таблица 17, в принципе, позволяет решать многие вопросы, касающиеся контроля схемы Σ , например, отвечать на вопрос, исправна ли схема Σ , а если нет, то какому классу неисправностей она принадлежит. Во многих практических задачах таблица имеет большое число строк и столбцов, и поэтому непосредственный анализ ее становится весьма трудоемким.

Развиваемая далее теория контроля призвана, с одной стороны, облегчить решение проблем контроля и, с другой стороны, понять глубже указанные выше трудности. Сформулируем далее ряд моментов и понятий, лежащих в основе этой теории.

1. Задается цель контроля (обычно путем указания в терминах функций g некоторого свойства, которое нужно распознать). Например, путем фиксации подмножества $\mathfrak{N}$ пар (i, j) ($1 \leq i, j \leq m$), определяющего некоторое подмножество пар функций (g_i, g_j) . В частности,

- а) $\mathfrak{N} = \{(1, j)\}$, где $j = 2, \dots, m$ (задача о проверке);
- б) $\mathfrak{N} = \{(1, j)\}$, где $i \neq j$ и $(1 \leq i, j \leq m)$ (задача о диагностике).

2. Указываются средства контроля. Их можно разделить на две группы:

а) контроль без вмешательства в схему (разрешается только наблюдать за входами и выходами схемы Σ);

б) контроль с вмешательством в схему (например, допускается введение контрольных точек, перестановка блоков, замена некоторых блоков на эталонные и т. п.).

3. Фиксируется способ получения информации о контролируемом объекте (в терминах, допустимых экспериментов со схемой Σ). Эксперимент — система входных наборов (вопросов), согласованная с порядком $\preceq$ и необходимые для нее выходные значения (ответы), предъявляемые контролируемой схемой. Они делятся на безусловные и условные.

а) Безусловные эксперименты. Различают два типа безусловных экспериментов:

— простые безусловные эксперименты, т. е. последовательности вопросов (рис. 109, а);

— кратные безусловные эксперименты, т. е. конечные множества последовательностей вопросов (рис. 109, б).

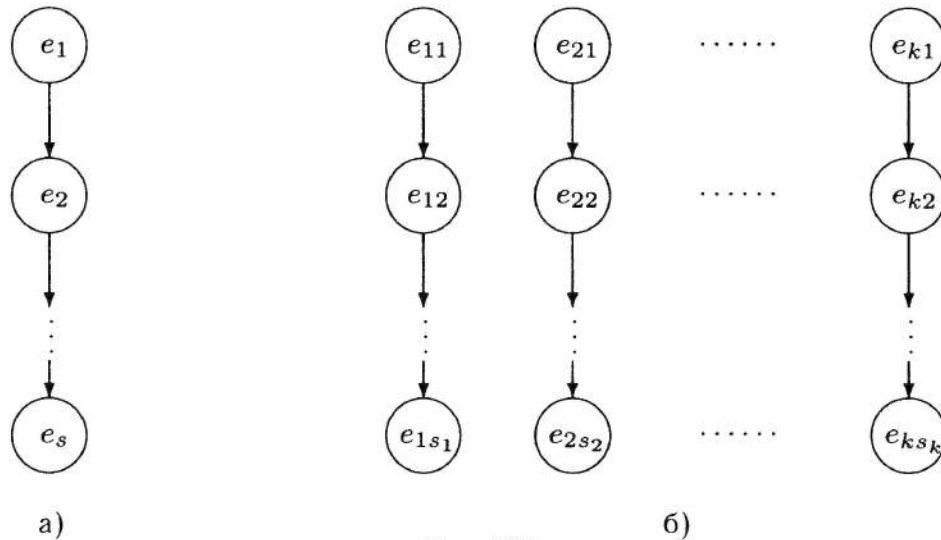


Рис. 109

Множество вопросов $\{e_{i_1}, \dots, e_{i_s}\}$ можно рассматривать как простой безусловный эксперимент с произвольным (при отсутствии $\preceq$) порядком или как кратный безусловный эксперимент (длина каждой последовательности равна единице).

б) Условные эксперименты. Они делятся также на простые условные эксперименты и кратные условные эксперименты:

— простой условный эксперимент — это ориентированное (от корня) дерево, вершинам которого приписаны вопросы, а ребрам — ответы, определяющие выбор следующего вопроса¹⁷;

— кратный условный эксперимент — конечное множество ориентированных (от корня) деревьев, вершинам которого приписаны вопросы, а ребрам — ответы, определяющие выбор следующего вопроса.¹⁷

З а м е ч а н и е. При наличии порядка $\preceq$ указанные последовательности вопросов и деревья вопросов согласуются с ним.

Выбор простых экспериментов связан с ситуацией, когда имеется один экземпляр контролируемого объекта, и мы не можем его переводить в стандартное начальное состояние.

Кратные эксперименты используются там, где либо можно иметь несколько тождественных экземпляров контролируемых объектов (с одной

¹⁷Если выбор следующего вопроса не зависит от ответа, то ребру ничего не приписывается.

и той же неисправностью), либо есть один экземпляр контролируемой системы, но его можно переводить в стандартное начальное состояние.

Очевидно, перечисленные типы экспериментов связаны друг с другом, как указано на диаграмме (рис. 110).



Рис. 110

Исходом эксперимента называется:

а) в случае безусловного эксперимента — система ответов на вопросы эксперимента (эти ответы проставляются на ребрах, идущих от вопросов, для последних вопросов — на дополнительных ребрах);

б) для простого условного эксперимента — ветка дерева, к которой добавлено одно ребро с ответом на последний вопрос;

в) для кратного условного эксперимента — система веток, взятых из каждого дерева по одной, к которым добавлено по одному ребру с ответами на последние вопросы.

Пример. На рис. 111 приведены простые условные эксперименты $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ (обведены штриховыми линиями) и все исходы экспериментов для табл. 18.

4. Каждый эксперимент приводит к разбиению множества $\{g_1, \dots, g_m\}$ на классы, а исход — к выбору компоненты. На рис. 111 для этого примера для всех экспериментов указаны компоненты, получаемые при каждом возможном исходе.

Если разбиение, получаемое в эксперименте $\mathcal{E}$ таково, что для каждой пары (i, j) из $\mathcal{N}$ функции g_i и g_j принадлежат различным компонентам разбиения, то говорят, что эксперимент $\mathcal{E}$ распознает свойство $\mathcal{N}$.

Определение. Эксперимент $\mathcal{E}$, распознающий свойство $\mathcal{N}$, называется тестом (относительно $\mathcal{N}$) и обозначается далее через T .

Если в приведенном выше примере взять за $\mathcal{N}$ множество всех пар, то $\mathcal{E}_1$ не будет тестом, а $\mathcal{E}_2$ и $\mathcal{E}_3$ являются тестами.

Для безусловных экспериментов понятие теста может быть упрощено: система наборов $\{e_{i_1}, \dots, e_{i_s}\}$ является тестом относительно $\mathcal{N}$ тогда и только тогда, когда для любой пары (i, j) из $\mathcal{N}$ найдется набор e из данной системы такой, что $g_i(e) \neq g_j(e)$. Следует отметить, что множество всех

Т а б л и ц а 18

	g_1	g_2	g_3	g_4
e_1	0	0	1	1
e_2	0	1	0	0
e_3	0	0	0	1

вопросов, входящих в произвольный условный тест, является безусловным тестом. Заметим также, что во многих случаях таблица функций неисправностей может быть ограничена по числу строк без утраты возможностей контроля. Пусть s_0 — число строк усеченной таблицы. Тогда множество $T_0 = \{e_1, \dots, e_{s_0}\}$ образует безусловный тест, называемый тривиальным тестом.

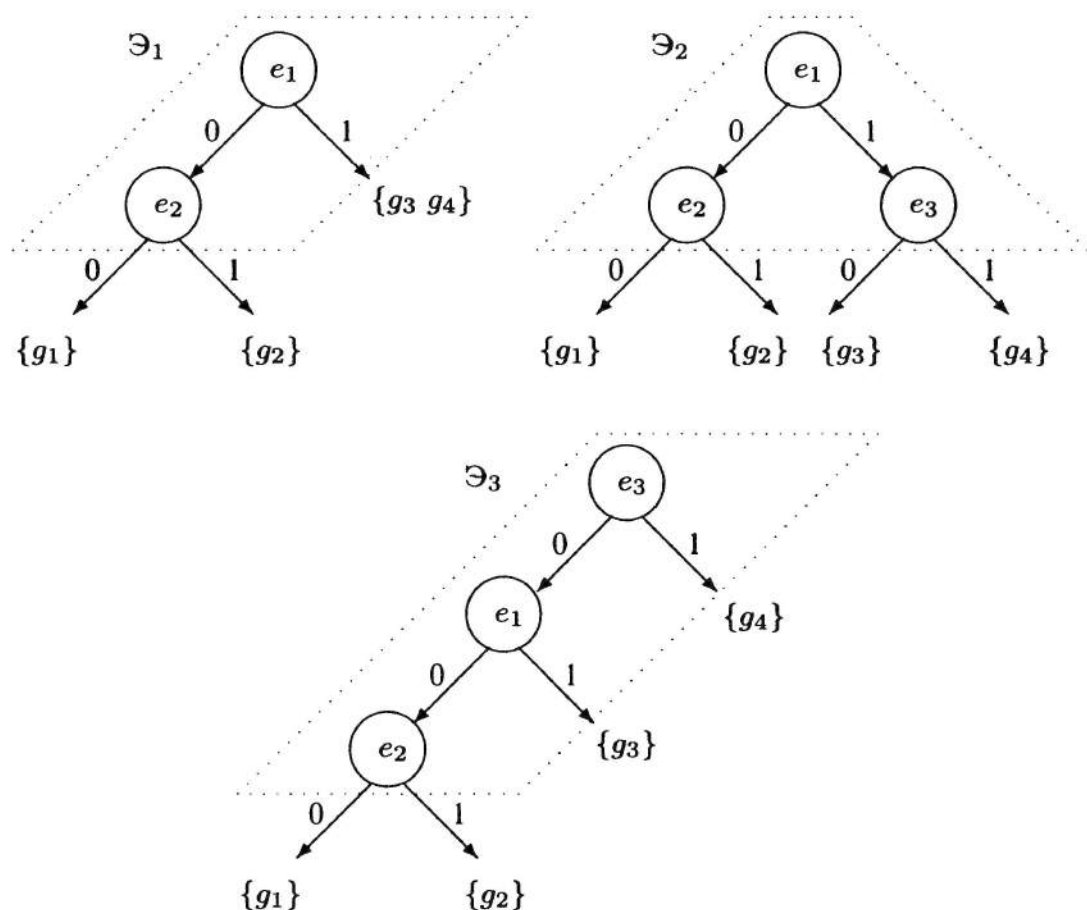


Рис. 111

5. Оказывается, что для задачи контроля таблица, как правило, допускает много тестов. Поэтому на множестве тестов вводят функционал $l(T)$, обозначающий сложность теста T . Этот функционал (в силу диаграммы включений рис. 110) достаточно определить для кратных условных тестов. Приведем несколько вариантов определения такого функционала. Пусть

$l_1(T)$ — число деревьев в T , называемое также кратностью теста T ;

$l_2(T) = \max_{i,j} |B_{ij}|$, где $|B_{ij}|$ — сложность i -й ветки B_{ij} , входящей в j -е

дерево из T (обычно $|B_{ij}|$ есть либо сумма весов наборов, встречающихся в ветке B_{ij} , либо просто число наборов в ветке, $l_2(T)$ в этих случаях характеризует либо время выполнения кратного эксперимента, либо максимальную высоту деревьев);

$l_3(T) = \sum_j l(e_{ij})$, где $l(e_{ij})$ — вес набора e_{ij} , и суммирование ведется

по всем наборам (с учетом повторений), входящим в T ; $l_3(T)$ называется длиной (объемом) теста T .

Функционал $l(T)$ для каждой таблицы и свойства $\mathfrak{M}$ позволяют определить понятие минимального теста как такого теста T , для которого $l(T)$ минимально.

6. К понятию минимального теста тесно примыкает другое понятие — понятие тупикового теста, определение которого не требует использования функционала сложности. В простейшем случае, когда тестами являются некоторые подмножества множества $\{e_1, \dots, e_{s_0}\}$, понятие тупиковости определяется так: тест $T = \{e_{i_1}, \dots, e_{i_s}\}$ называется тупиковым, если удаление любого набора из T приводит к подмножеству, не являющемуся тестом. В общем случае для определения тупикового теста сначала вводится понятие подэксперимента как части исходного эксперимента, и затем тупиковый тест определяется как тест такой, что любые его собственные подэксперименты не являются тестами (ср. [32]). Для функционалов $l(T)$, удовлетворяющих естественным аксиомам, оказывается, что среди тупиковых тестов содержится хотя бы один минимальный тест. Последнее повышает интерес к понятию тупикового теста.

7. Основными задачами теории контроля являются:

— создание методов построения минимальных тестов и оценки их сложности для разных классов управляющих систем, различных источников неисправностей и целей контроля;

— построение алгоритмов контроля и изучение их сложности;

— разработка методов синтеза простотестируемых схем.

Некоторые из них рассматриваются ниже. Материал делится на части:

1) табличный подход к построению тестов;

2) построение тестов с учетом структуры схемы.

§ 1. Методы построения таблицы функций неисправностей по схеме Σ и источнику $\mathbf{I}$ для схем без памяти

I. Контактные схемы с источниками $\mathbf{I}_{a,b}$.

Для наглядности наши рассуждения будем сопровождать примером.

Пусть $X = x_2x_1$ и $Y = y_2y_1$ — двоичные числа, тогда условие $X \geq Y$ может быть описано булевой функцией $f(x_2, x_1, y_2, y_1)$. Реализуем ее контактной схемой (рис. 112; в кружочках указаны номера контактов).

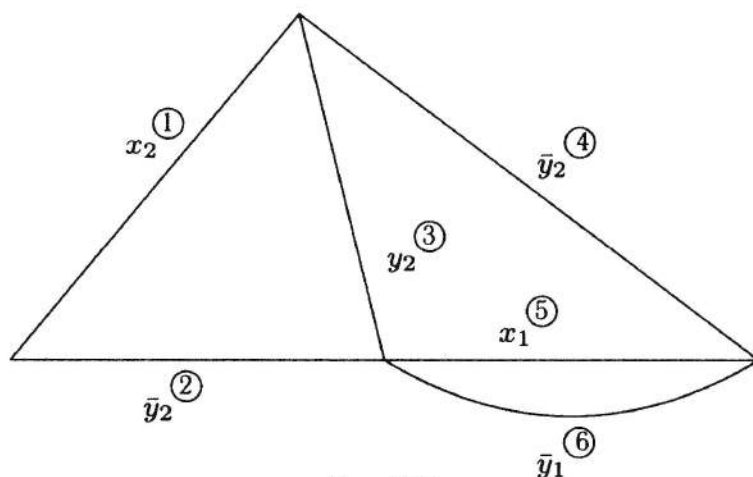


Рис. 112

Пусть имеется два источника $I_{1,0}$ и $I_{0,1}$, вызывающие соответственно не более одного разрыва или не более одного короткого замыкания. Возможны два способа построения таблицы неисправностей.

1. Построение таблицы по столбцам (прямой метод).

В этом случае для каждой неисправности, вызываемой источником И, определяют соответствующую функцию неисправностей. Так, если в контактной схеме контакт x_i^{σ} разомкнулся, то его выбрасывают, если замкнулся накоротко, то отождествляют вершины, которые он связывал. В обоих случаях возникает контактная схема, и проблема нахождения функции неисправностей сводится к нахождению функции, реализуемой данной контактной схемой.

2. Построение таблицы по строкам (путем возбуждения схемы на данном наборе).

Очевидно, что если $f(\alpha_1, \dots, \alpha_n) = 1$ на наборе $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$, то при замыкании контактов соответствующая функция неисправностей f' на этом наборе также равна 1, т. е. $f'(\alpha_1, \dots, \alpha_n) = 1$. Если же $f(\alpha_1, \dots, \alpha_n) = 0$, то при размыкании контактов соответствующая функция неисправностей f'' на этом наборе также равна 0, т. е. $f''(\alpha_1, \dots, \alpha_n) = 0$.

Следовательно, для источника И, вызывающего замыкание, наборы $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$, для которых $f(\tilde{\alpha}) = 1$, не несут информации о повреждении схемы, а для источника И, вызывающего размыкание, наборы $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$, для которых $f(\tilde{\alpha}) = 0$, также не дают информации о повреждении схемы.

Отсюда для $I_{1,0}$ надо рассматривать только те наборы, на которых $f = 1$, а для $I_{0,1}$ — на которых $f = 0$. И задача распадается на две независимые задачи.

Рассмотрим таблицы 19 и 20. На них сплошным отрезком обозначены контакты, замкнутые на данном наборе; в скобках (справа от набора) обозначены номера контактов, неисправность которых обнаруживается на этом наборе; а сами контакты — в случае замыкания (табл. 19) помечены пунктиром, в случае размыкания (табл. 20) — перечеркнуты штрихом.

Т а б л и ц а 19

0001 (1,3,5,6) 	0010 (1,2) 	0011 (нет)
0110 (1,2) 	0111 (1,2) 	1011 (4,5,6)

Таблица 20

0000 (2,6) 	0100 (2) 	0101 (2,5)
1000 (нет) 	1001 (1,4) 	1010 (1,3,6)
1100 (нет) 	1101 (нет) 	1110 (1,3)
1111 (1,3,5) 		

Таблица 21

		g	g'_1	g'_2	g'_3	g'_4	g'_5		g''_1	g''_2	g''_3	g''_4	g''_5	g''_6
	$x_2 x_1 y_2 y_1$	f	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	f''_1	f''_2	f''_3	f''_4	f''_5	f''_6
1	0 0 0 1	0	1		1		1	1	0					
2	0 0 1 0	0	1	1										
3	0 0 1 1	0												
6	0 1 1 0	0	1	1										
7	0 1 1 1	0	1	1										
11	1 0 1 1	0				1	1	1						
0	0 0 0 0	1	1							0				0
4	0 1 0 0	1								0				
5	0 1 0 1	1								0			0	
8	1 0 0 0	1												
9	1 0 0 1	1							0			0		
10	1 0 1 0	1							0		0			0
12	1 1 0 0	1												
13	1 1 0 1	1												
14	1 1 1 0	1							0		0			
15	1 1 1 1	1							0		0		0	

На основании табл. 21 получаем таблицу функций неисправностей, в которой для функций неисправностей проставлены значения в том случае, если они отличаются от значения f .

З а м е ч а н и е. Таблица функций неисправностей может

- 1) содержать одинаковые столбцы (в примере $f'_5 = f'_6$),
- 2) иметь константные строки (у нас — строки, определяемые наборами (0011), (1000), (1100) и (1101)),
- 3) иметь одинаковые строки (в рассматриваемом примере совпадают строки (0010), (0110) и (0111)),
- 4) содержать константные столбцы.

Многие из этих факторов можно выявить из анализа исходной схемы, например, если имеются контакты, соединенные последовательно или параллельно. Благодаря им возможно перейти к более простой таблице, не только содержащей классы неисправностей, но и имеющей меньше строк, чем исходная.

Для рассматриваемого примера и случая замыкания усеченная таблица имеет следующий вид (табл. 22):

Т а б л и ц а 22

$x_2 x_1 y_2 y_1$	g	g'_1	g'_2	g'_3	g'_4	g'_5
0 0 0 1	0	1		1		1
0 0 1 0	0	1	1			
1 0 1 1	0				1	1

II. Схемы из функциональных элементов. В классе источников обычно рассматривают источники, вызывающие константные неисправности

на входах или выходах элементов. Источник I_d одновременно может воздействовать не более, чем на d каналов (входов, выходов).

Для иллюстрации возьмем пример (рис. 113).

Данная схема реализует следующую функцию: $z = x_1 + x_2 \pmod{2}$. Пусть источник I_1 вызывает константную ошибку не более, чем на одном входе конъюнкторов, что приводит наряду с функцией $f_0 = x_1 + x_2$ к восьми функциям $f_1^0, f_2^0, f_3^0, f_4^0, f_1^1, f_2^1, f_3^1, f_4^1$ неисправностей. Их можно вычислить, реализуя соответствующую неисправность (см. табл. 23).

На основе этой таблицы можно построить «по столбцам» таблицу функций неисправностей, а если учесть, что

$$\begin{aligned} f_1^0 &= f_2^0 = g_1, & f_3^0 &= f_4^0 = g_2, \\ f_1^1 &= f_4^1 = g_3, & f_2^1 &= f_3^1 = g_4, \end{aligned}$$

и взять $g_0 = f_0$, то можно перейти к таблице классов неисправностей (см. табл. 24).

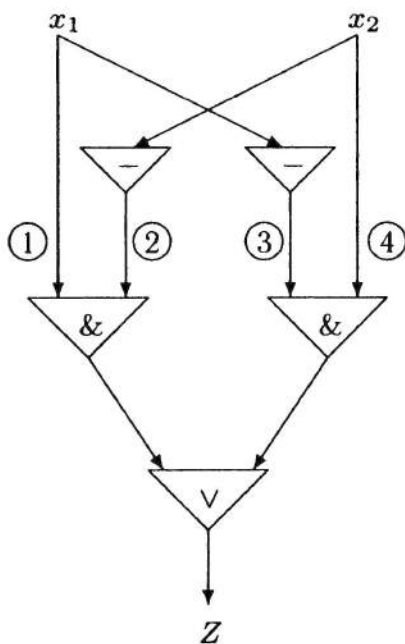
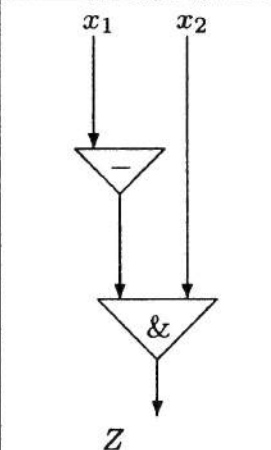
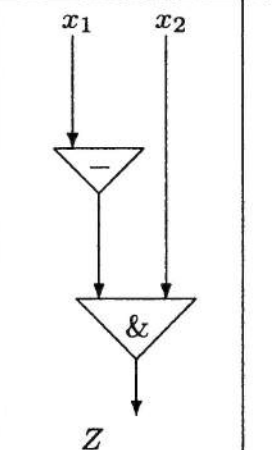
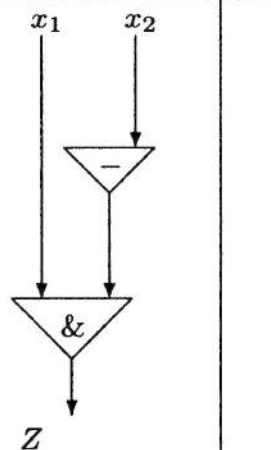
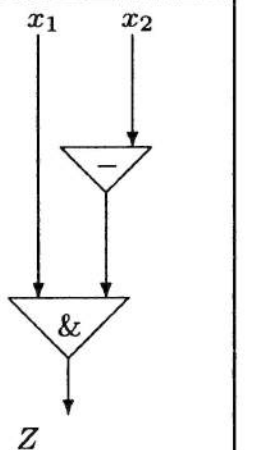
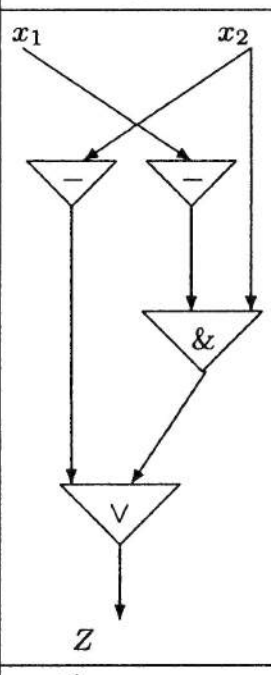
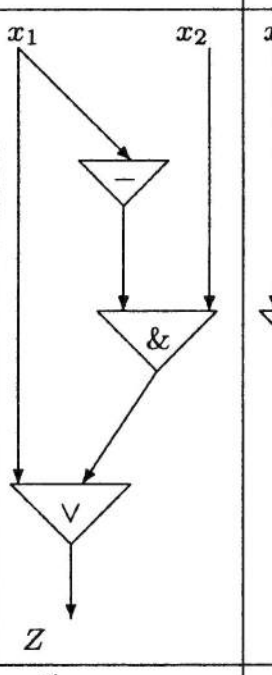
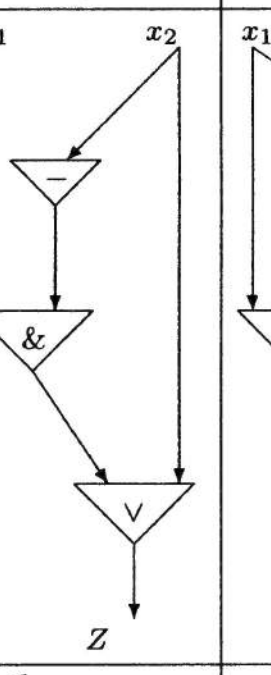
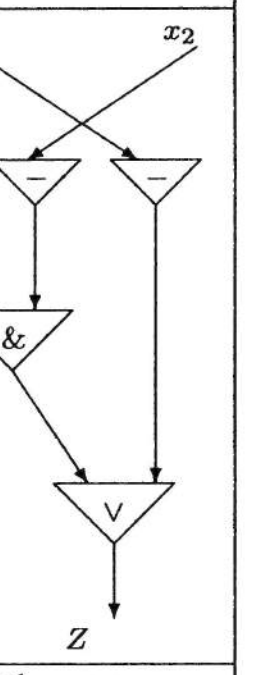


Рис. 113

Константа 0 на входе			
1	2	3	4
			
$f_1^0 = \bar{x}_1 \& x_2$	$f_2^0 = \bar{x}_1 \& x_2$	$f_3^0 = x_1 \& \bar{x}_2$	$f_4^0 = x_1 \& \bar{x}_2$
Константа 1 на входе			
1	2	3	4
			
$f_1^1 = \bar{x}_1 \vee \bar{x}_2$	$f_2^1 = x_1 \vee x_2$	$f_3^1 = x_1 \vee x_2$	$f_4^1 = \bar{x}_1 \vee \bar{x}_2$

Т а б л и ц а 24

$x_1 x_2$	g_0	g_1	g_2	g_3	g_4
0 0	0	0	0	1	0
0 1	1	1	0	1	1
1 0	1	0	1	1	1
1 1	0	0	0	0	1

Эту же таблицу можно получить путем построения ее по строкам. Ниже приведем это построение (см. табл. 25).

В табл. 25 для каждого входного набора указано состояние схемы (пунктиром помечены связи в состоянии 0 и сплошными линиями — в состоянии 1) и вычислена соответствующая ему строка таблицы.

Т а б л и ц а 25

Набор 00	Набор 01
строка 00 0001 001	11 1001 111
Набор 10	Набор 11
строка 10011 1111	00 0000 110

Для дальнейшего упрощения таблицы здесь можно учесть все соображения, которые были выявлены при построении таблиц для контактных схем. Обоснование этих упрощений связано с тем, что понятие тупикового теста для обсуждаемых случаев может быть охарактеризовано через

разбиения. Мы отмечали, что каждая строка e таблицы T определяет разбиение $\mathcal{D}(e)$ функций $g_1, \dots, g_m$ на классы эквивалентности. При этом множеству строк $e_{i_1}, \dots, e_{i_s}$ соответствует разбиение $\mathcal{D}(e_{i_1}, \dots, e_{i_s})$, и $\mathcal{D}(e_{i_1}, \dots, e_{i_s}) = \mathcal{D}(e_{i_1}) \cap \dots \cap \mathcal{D}(e_{i_s})$. Очевидно, что множество различных наборов $\{e_{i_1}, \dots, e_{i_s}\}$ является безусловным тупиковым тестом относительно $\mathfrak{N}$ тогда и только тогда, когда для любых различных наборов $e_{j_1}, \dots, e_{j_t}, e_{j_{t+1}}$ из $\{e_{i_1}, \dots, e_{i_s}\}$ выполняются следующие условия:

1) разбиение $\mathcal{D}(e_{j_1}, \dots, e_{j_t}, e_{j_{t+1}})$ является строгим продолжением разбиения $\mathcal{D}(e_{j_1}, \dots, e_{j_t})$;

2) найдется пара $(i, j) \in \mathfrak{N}$ такая, что g_i и g_j принадлежат одной и той же компоненте разбиения $\mathcal{D}(e_{j_1}, \dots, e_{j_t})$, но разным компонентам разбиения $\mathcal{D}(e_{j_1}, \dots, e_{j_t}, e_{j_{t+1}})$.

3) разбиение $\mathcal{D}(e_{j_1}, \dots, e_{j_s})$ для любой пары $(i, j) \in \mathfrak{N}$ содержит функции g_i и g_j в разных компонентах.

Диагностическая возможность набора e из T определяется разбиением $\mathcal{D}(e)$. Таким образом, два набора e' и e'' имеют одинаковую диагностическую возможность, если $\mathcal{D}(e') = \mathcal{D}(e'')$. Это оправдывает факторизацию таблицы (в случае, когда нет отношения $\preceq$) по строкам. Знание всех тупиковых тестов для факторизованной таблицы легко позволяет строить все тупиковые тесты для исходной таблицы. Указанные упрощения таблиц классов функций неисправностей приводят к таблицам, сохраняющим все типы тупиковых тестов исходной таблицы, поскольку они сохраняют все типы разбиений.

Рассмотрение таблиц классов функций неисправностей позволяет получить очевидные оценки для кратности безусловных тупиковых тестов $l_1(T)$:

- в случае задачи о проверке $1 \leq l_1(T) \leq \min(s, m - 1)$;
- в случае задачи о диагностике $\log_2 m \leq l_1(T) \leq \min(s, m - 1)$.

В дальнейшем диагностические тесты T , для которых $l_1(T) \asymp \log_2 m$, будем называть логарифмическими, а тесты, для которых $l_1(T) \asymp m$, — линейными.

§ 2. Табличный подход в случае автоматов

Вместо о.-д. функций здесь удобно рассматривать словарные функции $f(x_1, \dots, x_n)$, которые преобразуют не бесконечные последовательности значности $N = 2^n$ в бесконечные последовательности значности $M = 2^p$, а входные слова $A = a_1, \dots, a_t$ в алфавите из N букв в слова $B = b_1, \dots, b_t$ той же длины в алфавите из M букв.

Далее предполагается, что источник И неисправностей вызывает неисправности, которые описываются словарными функциями в тех же алфавитах и имеют не более состояний, чем исходная схема.

Наконец, в отличие от предыдущего, здесь между входными словами имеются связи, а именно,

$$A_1 \preceq A_2,$$

если слово A_1 является началом слова A_2 . В этом случае информация, получаемая на слове A_1 , содержится в информации, получаемой на слове A_2 .

Пример. На рис. 114 представлена схема, поведение которой описывается каноническими уравнениями

$$\begin{cases} z(t) = x_1(t) + q(t-1), \\ q(t) = x_1(t) + q(t-1), \\ q(0) = 0. \end{cases}$$

Они определяют словарную функцию $g_0(X)$, где X — произвольное слово в алфавите $\{0, 1\}$, а $g_0(X)$ — слово той же длины, причем последний символ его равен 0, если слово X содержит четное число единиц, и 1 — в противном случае. Таким образом, схема является триггером.

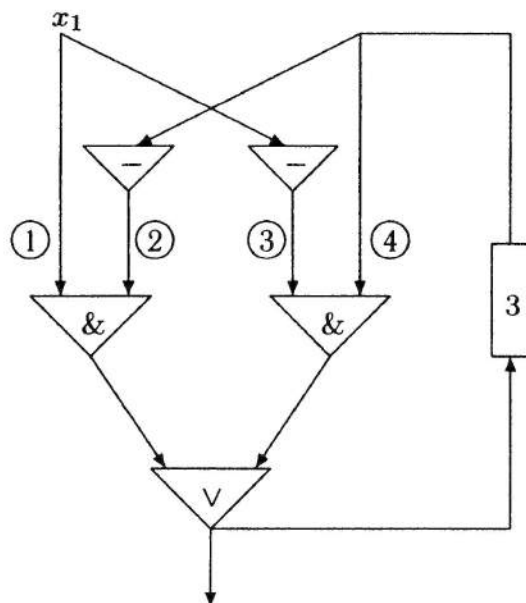


Рис. 114

Пусть источник I_1 вызывает не более, чем одну неисправность на входах конъюнкторов, переводя его в устойчивое константное состояние. В этом случае, используя пример для схем из функциональных элементов, мы получим четыре различные словарные функции $g_1(X)$, $g_2(X)$, $g_3(X)$ и $g_4(X)$, описывающие его неисправные режимы. На основе этого можно построить таблицу классов функций неисправностей. Ее фрагмент представлен ниже (табл. 26).

Т а б л и ц а 26

	$g_0(x)$	$g_1(x)$	$g_2(x)$	$g_3(x)$	$g_4(x)$
0	0	0	0	1	0
1	1	0	1	1	1
0 0	0 0	0 0	0 0	1 1	0 0
0 1	0 1	0 0	0 1	1 0	0 1
1 0	1 1	0 0	1 0	1 1	1 1
1 1	1 0	0 0	1 0	1 0	1 1
...	...	...	...	...	...
...	...	...	...	...	...

Таким образом, в автоматном случае таблица оказывается не бинарной и содержит бесконечное число строк.

Существует несколько способов усечения таблицы, т. е. выделения в ней конечной подтаблицы, дающих возможность решения задач контроля.

1. Выделение конечной подтаблицы, содержащей попарно различные столбцы.

Такое усечение возможно, так как для каждой пары словарных функций $g_i(X)$ и $g_j(X)$ существует слово e_{ij} такое, что $g_i(e_{ij}) \neq g_j(e_{ij})$. Беря наименьший начальный фрагмент, содержащий все строки e_{ij} (их конечное число), получаем требуемое. Указанный способ не дает представлений о размерах этого усечения, и надо рассматривать его как теорему существования.

2. Выделение подтаблицы, содержащей все имеющиеся в таблице типы разбиений на классы.

Поскольку число классов всех разбиений множества из m элементов не превосходит числа $\Phi(m)$, то возможно усечение таблицы, а именно, выделение ее конечного начального куска, содержащего все типы встречающихся в таблице разбиений. Данное решение носит также характер существования.

3. Наконец, существует способ выделения подтаблицы, состоящей из части строк исходной таблицы, определяемой так называемыми неприводимыми словами.

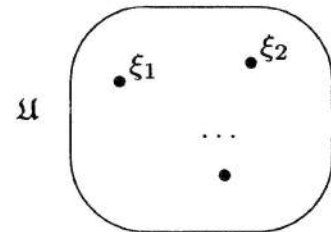


Рис. 115

Далее мы разовьем первый способ. Для этого сначала рассмотрим одну задачу, касающуюся автоматов. Пусть $\mathcal{U}$ — автомат, определяемый диаграммой Мура и имеющий r состояний (рис. 115). Пусть ξ_1 и ξ_2 — его произвольные состояния (две вершины диаграммы). Этим вершинам соответствуют словарные функции $g_{\xi_1}(X)$ и $g_{\xi_2}(X)$, если рассматривать функционирование автомата соответственно из начальной вершины ξ_1 или ξ_2 .

О п р е д е л е н и е. Состояния ξ_1 и ξ_2 автомата $\mathcal{U}$ называются отличимыми, если $g_{\xi_1}(X) \neq g_{\xi_2}(X)$.

Т е о р е м а 48 (Мур [38]). Пусть автомат $\mathcal{U}$ имеет r попарно различных состояний. Тогда эти состояния попарно различимы при помощи безусловного кратного эксперимента, состоящего из всех слов X длины s , где $s \leq r - 1$.

Д о к а з а т е л ь с т в о. Обозначим через X^t множество всех входных слов, длина которых равна t . Очевидно, мощность $|X^t|$ этого множества не превосходит N^t (N — значность входного алфавита), т. е. конечна.

Пусть $\mathcal{D}_t$ — разбиение множества $\{g_1, \dots, g_m\}$ на классы при помощи множества X^t . В один класс относятся функции g_i и g_j тогда и только тогда, когда для любых $x \in X^t$

$$g_i(x) = g_j(x).$$

Таким образом, компоненты разбиения $\mathcal{D}_t$ состоят из функций, попарно неразличимых на словах длины, не превосходящей t .

Если разбиение $\mathcal{D}''$ является продолжением разбиения $\mathcal{D}'$, то будем писать $\mathcal{D}' \supseteq \mathcal{D}''$. Очевидно,

$$\mathcal{D}_0 \supseteq \mathcal{D}_1 \supseteq \dots \supseteq \mathcal{D}_t \supseteq \dots,$$

где $\mathcal{D}_0$ состоит из компоненты $\{g_1, \dots, g_m\}$.

Пусть разбиение $\mathcal{D}_\tau$ содержит хотя бы одну нетривиальную компоненту, т. е. компоненту, содержащую более одного элемента, например, g_{ξ_1} и g_{ξ_2} , тогда разбиение $\mathcal{D}_{\tau+1}$ является строгим разбиением разбиения $\mathcal{D}_\tau$ (содержит больше компонент, чем $\mathcal{D}_\tau$). Обозначим через t длину наименьшего слова X , различающего функции g_{ξ_1} и g_{ξ_2} , т. е. $g_{\xi_1}(x) \neq g_{\xi_2}(x)$. В таком случае $t \geq \tau + 1$. Если $t = \tau + 1$, то утверждение очевидно. Остается рассмотреть случай, когда $t \geq \tau + 2$. Рассмотрим начало слова X длины $t - \tau - 1$, обозначим его через X' . Тогда

$$X = X'X''.$$

В данном случае X' — не пустое слово ($t - \tau - 1 \geq 1$), и на слове X' из вершины ξ_1 мы попадем в вершину ξ'_1 , а из вершины ξ_2 — в вершину ξ'_2 . Очевидно, продолжая эксперимент, взяв далее слово X'' , мы получим то же самое, как если бы двигались из вершин ξ_1 и ξ_2 на слове $X = X'X''$, т. е. функции $g_{\xi'_1}$ и $g_{\xi'_2}$ различимы экспериментом X'' длины $\tau + 1$. В то же время эти функции не различимы более коротким экспериментом, иначе исходный эксперимент X не был бы минимальным. Отсюда

$$\mathcal{D}_0 \supset \mathcal{D}_1 \supset \dots \supset \mathcal{D}_s = \mathcal{D}_{s+1} = \dots$$

В начале этой цепочки последующее разбиение строго разбивает предыдущее. Следовательно, процесс стабилизируется, когда $\mathcal{D}_s$ будет разбиением на одноэлементные компоненты, т. е. $\mathcal{D}_s = \{\{g_1\}, \dots, \{g_m\}\}$ и $s \leq r - 1$.

Теорема доказана.

Следствие 1. Теорема может быть обобщена на случай любых состояний, не обязательно попарно отличимых.

В этом случае разбиваем их на классы эквивалентности и применяем теорему Мура.

Следствие 2. Любые два отличимых состояния автомата с не более, чем r состояниями отличимы на слове длины не более, чем $r - 1$.

К данному результату примыкает

Теорема 49 (Мур [38]). Если $g'(x)$ и $g''(x)$ — две различных словарных функции веса не более r , то они отличимы на слове длины не более $2r - 1$.

Доказательство. По условию обе функции могут быть заданы диаграммами Мура с не более, чем r вершинами, среди которых одна является начальной. Рассмотрим диаграмму, являющуюся суммой этих диаграмм. Она имеет не более $2r$ вершин, причем обе начальные вершины исходных диаграмм будут в этой диаграмме отличимы. Мы на основании

следствий предыдущей теоремы получаем требуемое, т. е. существование слова X длины не более $2r - 1$, на котором они распознаются.

Теорема доказана.

Данная теорема не может быть усилена при исходных предположениях. А именно, существуют две о.-д. функции $f_1(x)$ и $f_2(x)$, реализующие соответственно константные последовательности

$$f_1(x) = \underbrace{(00 \dots 01)}_r \underbrace{(00 \dots 01)}_r \dots, \quad f_2(x) = 0 \underbrace{(00 \dots 01)}_{r-1} \underbrace{(00 \dots 01)}_{r-1} \dots,$$

каждая из которых имеет вес r , и различающиеся впервые в $2r - 1$ позиции.

С л е д с т в и е. Пусть $\{g_1(x), \dots, g_m(x)\}$ — произвольное подмножество попарно различных функций веса не более r . Тогда они распознаются на множестве всех слов длины не более $2r - 1$.

Таким образом, константа $2r - 1$ дает верхнюю оценку для числа строк усеченной таблицы, состоящей из попарно различных словарных функций веса, не превосходящего r , в которой столбцы попарно различны.

В предыдущем примере усеченная таблица имеет вид таблицы 27 (здесь $2r - 1 = 3$).¹⁸

Т а б л и ц а 27

	входные слова	$g_0(x)$	$g_1(x)$	$g_2(x)$	$g_3(x)$	$g_4(x)$	
0	0	0	0	0	1	0	
1	1	1	0	1	1	1	
2	0 0	00	00	00	11	00	*
3	0 1	01	00	01	10	01	
4	1 0	11	00	10	11	11	
5	1 1	10	00	10	10	11	
6	0 0 0	000	000	000	111	000	*
7	0 0 1	001	000	001	110	001	*
8	0 1 0	011	000	010	101	011	
9	0 1 1	010	000	010	101	011	
10	1 0 0	111	000	100	111	111	*
11	1 0 1	110	000	101	110	111	
12	1 1 0	100	000	100	101	111	
13	1 1 1	101	000	101	101	111	*

Данную таблицу можно упростить путем удаления строк, имеющих одинаковое разбиение, но при этом надо это согласовать как с используемым понятием сложности теста, так и с имеющимся отношением частичного порядка между входными словами.

Входные слова 0, 00, 000 приводят к одинаковым разбиениям. В силу того, что 0 является началом слов 00, 000 и является более коротким, оно

¹⁸Кстати, предыдущий ее фрагмент (табл. 26) уже имел попарно различные столбцы.

имеет преимущество, а строки с номерами 2 и 6, в которых расположены 00, 000, могут быть удалены.

Аналогичная ситуация имеет место для слов 10 и 100, а также 11 и 111. Поэтому можно удалить строку 10, где расположено слово 100, а также строку 13, где расположено слово 111.

Может быть удалено также слово 001, так как оно не является началом ни одного из присутствующих в таблице, и, если оно взято, то преимущество имеет более короткое слово 01, имеющее то же разбиение. Таким образом, упрощенная таблица не содержит строк с номерами 2, 6, 7, 10 и 13.

З а м е ч а н и е. Полученная таблица не содержит всех разбиений. Так, набор 0101 находится за ее пределами, и на нем имеем разбиение на одноэлементные компоненты; на наборах усеченной таблицы таких разбиений нет.

В заключение заметим, что построение тестовых таблиц является достаточно громоздкой процедурой, при которой возможны ошибки вычислений. Однако наличие двух способов построения таблицы позволяет выбирать более простой путь, а также корректировать эти ошибки.

§ 3. Построение таблицы отличимости

В дальнейшем наряду с упрощенной таблицей классов функций неисправностей полезно рассматривать таблицу, связанную с цепью контроля $\{(i_\nu, j_\nu)\}$, где $\nu = 1, \dots, \omega$ и $i_\nu \neq j_\nu$ (табл. 28), — называемую далее таблицей отличимости, где наряду со столбцом $g \equiv 0$ присутствуют столбцы (g_{i_ν}, g_{j_ν}) , в которых в строке e_μ стоит

$$\begin{aligned} 0, & \text{ если } g_{i_\nu}(e_\mu) = g_{j_\nu}(e_\mu), \\ 1, & \text{ если } g_{i_\nu}(e_\mu) \neq g_{j_\nu}(e_\mu) \quad (\nu = 1, \dots, \omega; \mu = 1, \dots, s). \end{aligned}$$

Таблица отличимости — бинарная таблица, в то время как исходная таблица может быть и многозначной.

Т а б л и ц а 28

	g	(g_{i_1}, g_{j_1})	(g_{i_2}, g_{j_2})		$(g_{i_\omega}, g_{j_\omega})$
e_1	0				
e_2	0				
...	...	...	...		...
...	...	...	...		...
e_s	0				

Т е о р е м а 50. Задача распознавания свойства $\mathfrak{N}$ для исходной таблицы сводится к задаче о проверке для таблицы отличимости: тесты для этих таблиц совпадают.

Д о к а з а т е л ь с т в о. Пусть T — тест относительно $\mathfrak{N}$ для исходной таблицы. Возьмем произвольный столбец таблицы отличимости, отличный от g . Он определяется некоторой парой (g_i, g_j) , причем $(i, j) \in \mathfrak{N}$.

В этом случае найдется $e \in T$ такой, что $g_i(e) \neq g_j(e)$, и тогда в строке e и столбце (g_i, g_j) стоит значение 1, отличающее этот столбец от столбца g . Отсюда следует, что T будет проверяющим тестом для таблицы отличимости. Верно и обратное. Пусть T — проверяющий тест для таблицы отличимости. Возьмем произвольную пару $(i, j) \in \mathfrak{M}$. Тогда в силу того, что на T отличается столбец (g_i, g_j) таблицы отличимости от столбца g , существует набор $e \in T$, для которого $g_i(e) \neq g_j(e)$. Таким образом, T будет тестом относительно $\mathfrak{M}$ для исходной таблицы.

Теорема доказана.

В таблице отличимости возможны упрощения, аналогичные тем, которые встречались ранее для тестовых таблиц (см. последующие примеры).

Заметим, что при построении тупиковых дизъюнктивных нормальных форм использовалась таблица такого же вида, как и таблицы отличимости, и поэтому построение тупиковых д.н.ф. сводится к решению задачи о построении тестов. Построим таблицу отличимости для контактной схемы из примера (см. рис. 112 и табл. 21) и источника неисправностей $\Pi_{1,0}$ в случае задачи о диагностике. Для краткости в построенной табл. 29 вместо (g''_i, g''_j) будем писать (i, j) . Данная таблица может быть упрощена за счет удаления единичного столбца (1, 2) и дублирующих столбцов (1, 3) и (1, 4).

Т а б л и ц а 29

	g	(01)	(02)	(03)	(04)	(05)	(06)	(12)	(13)	(14)	(15)	(16)	(23)	(24)	(25)	(26)	(34)	(35)	(36)	(45)	(46)	(56)
0	0		1				1	1				1	1	1	1				1		1	1
4	0		1					1					1	1	1	1						
5	0		1			1		1			1		1	1		1		1		1		1
9	0	1			1			1	1		1	1		1			1			1	1	
10	0	1		1			1	1		1	1		1			1	1	1			1	1
14	0	1		1				1		1	1	1	1				1	1	1			
15	0	1		1		1		1		1		1	1		1		1		1	1		1

Перейдем теперь к составлению таблицы отличимости для автоматного примера (см. табл. 27) в случае, когда $\mathfrak{M}$ — множество всех пар. В этой таблице (табл. 30) исключается столбец (13), состоящий из 1, а также столбцы (12) и (14), дублирующие столбец (01).

Т а б л и ц а 30

		g	(01)	(02)	(03)	(04)	(12)	(13)	(14)	(23)	(24)	(34)
0	0	0			1			1		1		1
1	1	0	1				1	1	1			
3	01	0	1		1		1	1	1	1		1
4	10	0	1	1			1	1	1	1	1	
5	11	0	1			1	1	1	1		1	1
8	010	0	1	1	1		1	1	1	1	1	1
9	011	0	1		1	1	1	1	1	1	1	1
11	101	0	1	1		1	1	1	1	1	1	1
12	110	0	1		1	1	1	1	1	1	1	1

§ 4. Методы построения тупиковых и минимальных тестов для тестовых таблиц

Существует несколько подходов в решении этих задач.

1. Алгоритм полного перебора: проверяются в тестовой таблице всевозможные подмножества строчек (их 2^s) и для каждого из них выясняется, является ли соответствующее множество наборов тестом относительно $\mathfrak{M}$. Среди тестовых подмножеств оставляют те, которые не поглощаются никакими другими тестовыми подмножествами. Это и дает множество всех безусловных тупиковых тестов. Оно содержит в себе и минимальные тесты. Данный алгоритм практически малоэффективен.

2. Метод наискорейшего спуска: возьмем таблицу отличимости, и в ней выбираем строку, содержащую наибольшее число единиц. Производим удаление из таблицы всех столбцов, имеющих в этой строке единицу, и затем удаляется и сама строка. Получаем новую таблицу и проделываем с ней то же самое и т. д. до тех пор, пока не будут вычеркнуты все столбцы, кроме первого. Совокупность наборов, соответствующих удаляемым строчкам, очевидно, является тупиковым тестом относительно $\mathfrak{M}$. Эта процедура весьма эффективна, но зато мы в общем случае не можем гарантировать не только минимальности построенного теста, но и его достаточной «близости» к минимальному.

3. Аналитический метод построения всех безусловных тупиковых относительно $\mathfrak{M}$ тестов.

Сначала дается описание соответствующего алгоритма (Яблонский [27]) для схем без памяти.

Мы исходим из усеченной таблицы классов функций неисправностей схемы Σ для источника И, полученной после соответствующих упрощений.

1) Для каждой пары $(i, j) \in \mathfrak{M}$ строим множество $E_{ij} = \{e_1^{ij}, \dots, e_{\nu(ij)}^{ij}\}$ путем выявления всех наборов e_t^{ij} , где $e_t^{ij} \in \{e_1, \dots, e_N\}$, на которых отличаются функции g_i и g_j . Этот шаг равносильен составлению таблицы отличимости.

2) Составляем выражение вида $\&V$:

$$\&V = \bigwedge_{\substack{(i,j) \\ (i,j) \in \mathfrak{M}}} (e_1^{ij} \vee \dots \vee e_{\nu(ij)}^{ij}),$$

где далее символы e_t^{ij} рассматриваются как независимые булевы переменные.

3) Осуществляем преобразование вида $\&V \Rightarrow \&V'$, где выражение $\&V'$ получается из $\&V$ путем применения правила $A \& (A \vee B) = A$ (поглощение множителя). В результате этого из $\&V$ удалятся все поглощаемые множители.

4) Производим преобразование вида $\&V' \Rightarrow \vee\&$ путем раскрытия скобок и приведения подобных в булевой алгебре. Здесь иногда удобно для ускорения этого процесса использовать тождество

$$(A \vee B) \& (A \vee C) = A \vee (B \& C).$$

5) Осуществляем переход вида $\vee \& \Rightarrow \vee \&'$ путем применения правила $A\vee(A\&B) = A$ (поглощение слагаемого). Каждое слагаемое в $\vee \&'$ — произведение некоторых множителей $e_{i_1}, \dots, e_{i_s}$, соответствующее множество $\{e_{i_1}, \dots, e_{i_s}\}$ и будет тупиковым тестом, и все тупиковые относительно $\mathfrak{M}$ тесты содержатся в этом выражении.

§ 5. Обоснование алгоритма

Существует естественное взаимно однозначное соответствие между наборами значений переменных $e_1, \dots, e_s$ и подмножествами множества $\{e_1, \dots, e_s\}$: элемент e принадлежит подмножеству тогда и только тогда, когда набор в разряде, определяемом переменным e , содержит значение 1.

В этом случае значение $\&\vee$ на наборе равно 1 тогда и только тогда, когда соответствующее ему множество является тестом относительно $\mathfrak{M}$ для данной таблицы. Так как в дальнейшем выполнялись эквивалентные преобразования, то то же самое можно сказать и о выражениях $\&\vee'$, $\vee \&$ и $\vee \&'$.

Наконец, переход $\vee \& \Rightarrow \vee \&'$ соответствует переходу от тестов к тупиковым тестам.

В самом деле, пусть $T = \{e_{i_1}, \dots, e_{i_s}\}$ является тупиковым тестом относительно $\mathfrak{M}$. В силу вышесказанного, каждая из скобок выражений $\&\vee$ и $\&\vee'$ содержит, по крайней мере, один элемент из T . Утверждается, что для каждого элемента $e_{i_\nu} \in T$ существует скобка, в которой содержится из T только элемент e_{i_ν} . Если это не так, то множество $T' = T \setminus \{e_{i_\nu}\}$ будет в каждой скобке содержать хотя бы один элемент и, следовательно, будет тестом относительно $\mathfrak{M}$, вопреки тупиковости теста T . При переходе к выражению $\vee \&$ происходит умножение скобок и, в силу предыдущего, появится член $e_{i_1}, \dots, e_{i_s}$, т. е. данный тупиковый тест. Поскольку каждый не тупиковый тест поглощается некоторым тупиковым, то дальнейшее преобразование их уничтожает.

Заметим, что данное построение эквивалентно построению для выражения $\&\vee$ сокращенной д.н.ф. и нахождению нижних единиц соответствующей монотонной булевой функции, что является объектом однозначно определенным.

Перейдем к рассмотрению примера для случая контактных схем. Применим данный алгоритм для построения всех тупиковых тестов в случае размыкания. Используя упрощенную таблицу отличимости 29, имеем

$$\begin{aligned} \&\vee = & \underline{(9 \vee 10 \vee 14 \vee 15)}(0 \vee 4 \vee 5)(10 \vee 14 \vee 15)9(5 \vee 15)(0 \vee 10)\& \\ & \underline{\& (5 \vee 9 \vee 10 \vee 14)(0 \vee 9 \vee 14 \vee 15)(0 \vee 4 \vee 5 \vee 10 \vee 14 \vee 15)\&} \\ & \underline{\& (0 \vee 4 \vee 5 \vee 9)(0 \vee 4 \vee 15)(4 \vee 5 \vee 10)(9 \vee 10 \vee 14 \vee 15)\&} \\ & \underline{\& (5 \vee 10 \vee 14)(0 \vee 14 \vee 15)(5 \vee 9 \vee 15)(0 \vee 9 \vee 10)\&} \\ & \underline{\& (0 \vee 5 \vee 10 \vee 15).} \end{aligned}$$

Производим упрощение, удаляя множители, поглощаемые множителем 9 (подчеркнутые одной чертой), и множители, поглощаемые множителем

$(0 \vee 10)$ (подчеркнутые двумя чертами). Получим

$$\&\vee' = 9(5 \vee 15)(0 \vee 10)(0 \vee 4 \vee 5)(10 \vee 14 \vee 15)(0 \vee 14 \vee 15)\& \\ \& (4 \vee 5 \vee 10)(5 \vee 10 \vee 14)(0 \vee 14 \vee 15).$$

Далее раскрываем скобки. Для этого предварительно перемножаем: $(5 \vee 15)(0 \vee 10) = 0 \cdot 5 \vee 0 \cdot 15 \vee 5 \cdot 10 \vee 10 \cdot 15$. Остальные скобки умножаем на каждое из четырех слагаемых. Имеем после очевидных упрощений:

- 1) $0 \cdot 5 \cdot 9(10 \vee 14 \vee 15) = 0 \cdot 5 \cdot 9 \cdot 10 \vee 0 \cdot 5 \cdot 9 \cdot 14 \vee 0 \cdot 5 \cdot 9 \cdot 15,$
- 2) $0 \cdot 9 \cdot 15(4 \vee 5 \vee 10)(5 \vee 10 \vee 14) =$
 $= 0 \cdot 5 \cdot 9 \cdot 15 \vee 0 \cdot 9 \cdot 10 \cdot 15 \vee 0 \cdot 4 \cdot 9 \cdot 14 \cdot 15,$
- 3) $5 \cdot 9 \cdot 10(0 \vee 4 \vee 15)(0 \vee 14 \vee 15) =$
 $= 0 \cdot 5 \cdot 9 \cdot 10 \vee 5 \cdot 9 \cdot 10 \cdot 15 \vee 4 \cdot 5 \cdot 9 \cdot 10 \cdot 14,$
- 4) $9 \cdot 10 \cdot 15(0 \vee 4 \vee 5) = 0 \cdot 9 \cdot 10 \cdot 15 \vee 4 \cdot 9 \cdot 10 \cdot 15 \vee 5 \cdot 9 \cdot 10 \cdot 15.$

Мы получаем

$$\vee\&' = 0 \cdot 5 \cdot 9 \cdot 10 \vee 0 \cdot 5 \cdot 9 \cdot 14 \vee 0 \cdot 5 \cdot 9 \cdot 15 \vee 0 \cdot 9 \cdot 10 \cdot 15 \vee \\ \vee 5 \cdot 9 \cdot 10 \cdot 15 \vee 4 \cdot 9 \cdot 10 \cdot 15 \vee 0 \cdot 4 \cdot 9 \cdot 14 \cdot 15 \vee 4 \cdot 5 \cdot 9 \cdot 10 \cdot 14.$$

Мы имеем шесть тупиковых тестов длины (кратности) 4 (они же — минимальные) и два тупиковых теста длины 5.

Таким образом, мы видим, что тупиковых тестов может быть много и они могут иметь разную сложность.

Теперь перейдем к описанию алгоритма построения всех безусловных кратных тупиковых тестов относительно $\mathfrak{M}$ для тестовых таблиц в автоматном случае.

Поскольку здесь для входных слов имеется частичный порядок $\preceq$ ($e' \preceq e'' \Leftrightarrow e'$ — начало слова e''), то понятие тупиковости уточняется следующим естественным образом: подмножество¹⁹ $T' = \{e'_{i_1}, \dots, e'_{i_s}\}$ такое, что $e'_{i_1} \preceq e_{i_1}, \dots, e'_{i_s} \preceq e_{i_s}$, и являющееся тестом относительно $\mathfrak{M}$, назовем подтестом теста $T = \{e_{i_1}, \dots, e_{i_s}\}$. Подтест T' называется собственным, если существует ν такое, что $e'_{i_\nu} \neq e_{i_\nu}$. Тест T является тупиковым, если он не содержит собственных подтестов.

При построении тупиковых тестов мы исходим из усеченной таблицы классов функций неисправности и по ней строим таблицу отличимости.

Алгоритм повторяет пункты 1)–5), о которых речь шла в предыдущем случае, и дополняется еще одним пунктом.

6) Выражение $\vee\&'$ преобразуется в выражение $\vee\&''$ с использованием правил, выполнимых при условии $A \preceq B$:

$$A \& B = B, \quad A \vee B = A.$$

¹⁹Некоторые из слов могут быть пустыми.

Первое из них дает в конъюнкции приоритет более длинному слову (более информативному), второе в дизъюнкции — более короткому.

Таким образом, алгоритм работает так же, как и в предыдущем случае. На этом этапе он построит тесты, среди которых содержатся все тупиковые (в новом смысле) тесты, относительно $\mathfrak{M}$. Следующий этап осуществит удаление всех тестов, поглощаемых тупиковыми. Справедливость этого утверждения вытекает из обоснования, относящегося к пунктам 1)–5), и того факта, что всякий тупиковый в новом смысле тест содержится среди тестов, получаемых на данном этапе алгоритма, а также характера дальнейших преобразований: если $T' \subseteq T$ и $T = \{e_{i_1}, \dots, e_{i_s}\}$, а $T' = \{e'_{i_1}, \dots, e'_{i_s}\}$, причем

$$e'_{i_1} \preceq e_{i_1}, \dots, e'_{i_s} \preceq e_{i_s},$$

то

$$e_{i_1} \& \dots \& e_{i_s} \vee e'_{i_1} \& \dots \& e'_{i_s} = e'_{i_1} \& \dots \& e'_{i_s}.$$

Следует, далее, заметить, что вышеуказанный алгоритм может быть усовершенствован, если на шаге 2 допустить преобразование $A \vee B = A$ при условии $A \preceq B$. Эта возможность вытекает из следующей леммы.

Лемма 24. *Если в выражении $\&\vee$ во всех скобках, в которых встречаются одновременно A и B ($A \neq B$) и $A \preceq B$, произвести преобразование $A \vee B = A$, то полученное выражение $\&\vee'$ содержит все тупиковые тесты, встречающиеся в $\&\vee$.*

Доказательство. Очевидно, речь может идти только о тупиковых тестах для $\&\vee$, содержащих B . Пусть T — один из таких тупиковых тестов. Рассмотрим все скобки из $\&\vee$, в которых из T содержится элемент B . Если все они содержат также A , то заменяя в T элемент B на A , мы получим, очевидно, тест T' , являющийся собственным подтестом T , что противоречит тому, что T — тупиковый тест. Значит, существует скобка, содержащая из T только B и не содержащая A . После указанного преобразования тест T перейдет в тест $T' = T \cup \{A\}$ для $\&\vee'$ и, затем, он после применения тождества $A \& B = B$ перейдет в исходный тест T .

Лемма доказана.

Проиллюстрируем этот алгоритм на нашем примере. Опираясь на упрощенную таблицу отличимости, и учитывая также поглощение столбцов, получим

$$\&\vee = (4 \vee 8 \vee 11)(0 \vee 3 \vee 8 \vee 9 \vee 12)(5 \vee 9 \vee 11 \vee 12).$$

Производим упрощения, замечая, что $4 \preceq 11$, $0 \preceq 3, 8, 9$ и $5 \preceq 12$:

$$\&\vee' = (4 \vee 8)(0 \vee 12)(5 \vee 9 \vee 11).$$

Раскрываем скобки

$$\begin{aligned} \vee \& &= 0 \cdot 4 \cdot 5 \vee 0 \cdot 4 \cdot 9 \vee 0 \cdot 4 \cdot 11 \vee 0 \cdot 5 \cdot 8 \vee 0 \cdot 8 \cdot 9 \vee 0 \cdot 8 \cdot 11 \vee \\ &\vee 4 \cdot 5 \cdot 12 \vee 4 \cdot 9 \cdot 12 \vee 4 \cdot 11 \cdot 12 \vee 5 \cdot 8 \cdot 12 \vee 8 \cdot 9 \cdot 12 \vee 8 \cdot 11 \cdot 12. \end{aligned}$$

Производим дальнейшие преобразования с учетом порядка, сначала удаляя множители

$$\begin{aligned} \vee \&' = 0 \cdot 4 \cdot 5 \vee 4 \cdot 9 \vee 0 \cdot 11 \vee 5 \cdot 8 \vee 8 \cdot 9 \vee 8 \cdot 11 \vee 4 \cdot 12 \vee 4 \cdot 9 \cdot 12 \vee \\ &\vee 11 \cdot 12 \vee 8 \cdot 12 \vee 8 \cdot 9 \cdot 12 \vee 8 \cdot 11 \cdot 12 = 0 \cdot 4 \cdot 5 \vee 4 \cdot 9 \vee 0 \cdot 11 \vee \\ &\vee 5 \cdot 8 \vee 8 \cdot 9 \vee 8 \cdot 11 \vee 4 \cdot 12 \vee 11 \cdot 12 \vee 8 \cdot 12, \end{aligned}$$

и затем — слагаемые

$$\vee \&'' = 0 \cdot 4 \cdot 5 \vee 4 \cdot 9 \vee 0 \cdot 11 \vee 5 \cdot 8 \vee 8 \cdot 9 \vee 4 \cdot 12.$$

Мы получаем: тупиковый тест $(0, 101)$ длины 4, четыре тупиковых теста $(0, 10, 11)$, $(11, 010)$, $(10, 110)$ и $(10, 011)$ длины 5, тупиковый тест $(010, 011)$ длины 6.

Этот список не исчерпывает всех тупиковых тестов. Мы уже отмечали, что эксперимент, состоящий из одного входного слова (такие эксперименты называют простыми) 0101, является тестом, его длина равна 4.

В работе [32] предложена методика нахождения всех тупиковых кратных тестов.

§ 6. Условные и безусловные тесты

До сих пор мы занимались изучением безусловных тестов. Естественно, возникает вопрос, как часто использование безусловных тестов является эффективным, и дают ли какие-нибудь преимущества условные тесты по отношению к безусловным? Здесь мы постараемся дать ответы на эти вопросы в случае бинарных таблиц.

Обозначим через $\mathcal{T}_{s,m}$ множество тестовых таблиц с попарно различными столбцами из 0 и 1, имеющих m столбцов и s строк (значит, $2^s \geq m$).

Очевидно,

$$|\mathcal{T}_{s,m}| = 2^s(2^s - 1) \cdot \dots \cdot (2^s - (m - 1)) < 2^{sm}.$$

Пусть $\mathcal{T}_{s,m}^t$ — множество всех таблиц из $\mathcal{T}_{s,m}$ для которых длина минимального относительно $\mathfrak{M}$ безусловного теста не превосходит t .

Теорема 51. Для любого $\varepsilon > 0$, для почти всех при $m \rightarrow \infty$ таблиц из $\mathcal{T}_{s,m}$ существует диагностический безусловный тест, длина которого не превосходит $[2(1 + \varepsilon) \log m]$.

Доказательство. Возможны два случая.

1. $\log m \leq s \leq [2(1 + \varepsilon) \log m]$. Тогда $\mathcal{T}_{s,m}^s = \mathcal{T}_{s,m}$ и утверждение очевидно, если принять $t = s$.

2. $s > [2(1 + \varepsilon) \log m]$. Рассмотрим класс $\tilde{\mathcal{T}}_{s,m}^t$ тестовых таблиц (рис. 116), у которых в первых $t = [2(1 + \varepsilon) \log m]$ строках все столбцы попарно различны, а в остальных строках — произвольны.

$t = [2(1 + \varepsilon) \log m]$	$g_1 \quad \dots \quad g_m$
	попарно различные столбцы
	произвольные

Рис. 116

Очевидно, $\tilde{\mathcal{T}}_{s,m}^t \subseteq \mathcal{T}_{s,m}^t$ и

$$\begin{aligned}
 |\mathcal{T}_{s,m}^t| &\geq |\tilde{\mathcal{T}}_{s,m}^t| = \\
 &= 2^{[2(1+\varepsilon)\log m]} (2^{[2(1+\varepsilon)\log m]} - 1) \cdot \dots \cdot (2^{[2(1+\varepsilon)\log m]} - (m-1)) \times \\
 &\times 2^{m(s-[2(1+\varepsilon)\log m])} > 2^{m(s-[2(1+\varepsilon)\log m])} (2^{[2(1+\varepsilon)\log m]} - m)^m = \\
 &= 2^{ms} \left(1 - \frac{m}{2^{[2(1+\varepsilon)\log m]}}\right)^m.
 \end{aligned}$$

Оценим величину $\frac{|\tilde{\mathcal{T}}_{s,m}^t|}{|\mathcal{T}_{s,m}^t|}$:

$$\begin{aligned}
 1 &\geq \frac{|\tilde{\mathcal{T}}_{s,m}^t|}{|\mathcal{T}_{s,m}^t|} > \left(1 - \frac{m}{2^{[2(1+\varepsilon)\log m]}}\right)^m > \left(1 - \frac{2m}{m^{2(1+\varepsilon)}}\right)^m = \\
 &= \left(1 - \frac{1}{\frac{1}{2}m^{1+2\varepsilon}}\right)^{(-\frac{1}{2}m^{1+2\varepsilon})(-2m^{-2\varepsilon})} \sim e^{-2m^{-2\varepsilon}} \rightarrow 1 \quad (m \rightarrow \infty).
 \end{aligned}$$

Теорема доказана.

На самом деле, мы доказали больше: для любого $\varepsilon > 0$ для почти всех тестовых таблиц первые $t = \min\{s, [2(1 + \varepsilon) \log m]\}$ строк являются безусловным диагностическим тестом. Следовательно, для почти всех тестовых таблиц безусловные тесты имеют сложность (кратность) по порядку логарифмическую, т. е. близкую к оптимальной. Для этого же класса простые условные тесты имеют высоту по порядку также логарифмическую (соответствующие бинарные деревья имеют m концевых вершин), т. е. не дают выгоды.

В заключение покажем, что существуют тестовые таблицы, для которых условные тесты имеют преимущество перед безусловными. Для этого возьмем табл. 31.

Т а б л и ц а 31

	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
e_1	0	0	0	0	1	1	1	1
e_2	0	0	1	1	0	0	0	0
e_3	0	0	0	0	0	0	1	1
e_4	0	1	0	0	0	0	0	0
e_5	0	0	0	1	0	0	0	0
e_6	0	0	0	0	0	1	0	0
e_7	0	0	0	0	0	0	0	1

На рис. 117 представлен для нее диагностический условный тест с указанием компонент разбиения. А безусловный диагностический тест содержит все наборы $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$.

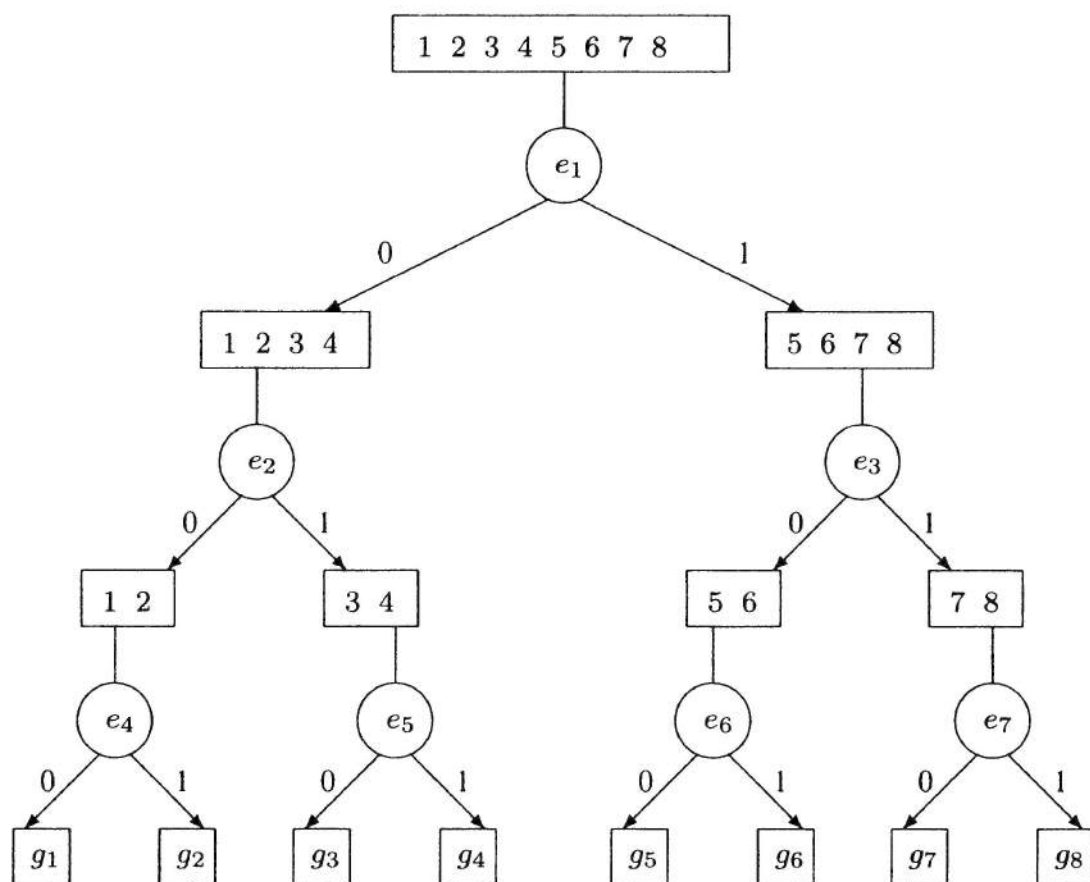


Рис. 117

Длина безусловного теста равна 7, а высота условного — 3. Этот пример легко обобщается на случай $m = 2^k$. Мы получим таблицу, содержащую

$$s = 1 + 2 + \dots + 2^{k-1} = 2^k - 1 = m - 1$$

вопросов. Поэтому длина безусловного теста равна $m - 1$, а высота дерева условного теста — $k = \log m$. Итак, в этом случае условный тест дает наибольшее преимущество перед безусловным.

§ 7. Построение тестов с учетом структуры

Построение тестов при помощи универсального алгоритма для таблиц весьма трудоемко. Поэтому необходимо использовать дополнительную информацию о контролируемом объекте. Здесь существует два пути:

- переходить от класса всех тестовых таблиц к отдельным классам;
- пытаться строить тесты, используя информацию о строении схемы, минуя этап получения таблицы классов функций неисправности.

Последний успешно развивался для класса так называемых блочных контактных схем, представляющих последовательное соединение однотипных блоков — многополюсных схем, зависящих от одного переменного (см. также [27, 28]).

Здесь мы займемся изучением частного примера — счетчика четности (рис. 118, а), представляющего последовательное соединение блоков (рис. 118, б), за исключением первого и последнего. Данная схема реализует функцию

$$\begin{aligned} & x_1 + \dots + x_n \pmod{2} \quad \text{при } n + \sigma \text{ четном} \\ \text{или} & x_1 + \dots + x_n + 1 \pmod{2} \quad \text{при } n + \sigma \text{ нечетном.} \end{aligned}$$

Следовательно, обе линейные функции реализуются схемами, отличающимися последним блоком.

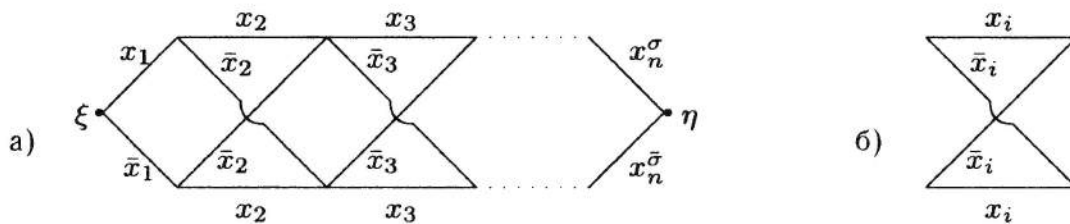


Рис. 118

Замечание 1. Если имеется тест относительно $\mathfrak{N}$ для первой схемы, то путем инвертирования последних координат всех его наборов получается тест относительно $\mathfrak{N}$ для второй схемы.

Замечание 2. Существует взаимно однозначное соответствие между проводящими путями схемы и наборами, на которых реализуемая ею функция равна единице.

Рассмотрим вопрос о построении достаточно простого теста для данной схемы и источника $I_{1,0}$. Пусть $\mathfrak{N}$ — проверка. В этом случае вопрос сводится к построению системы проводящих цепей схемы, покрывающих ее. Такими, например, цепями являются цепи a, b, c, d , изображенные на рис. 119.

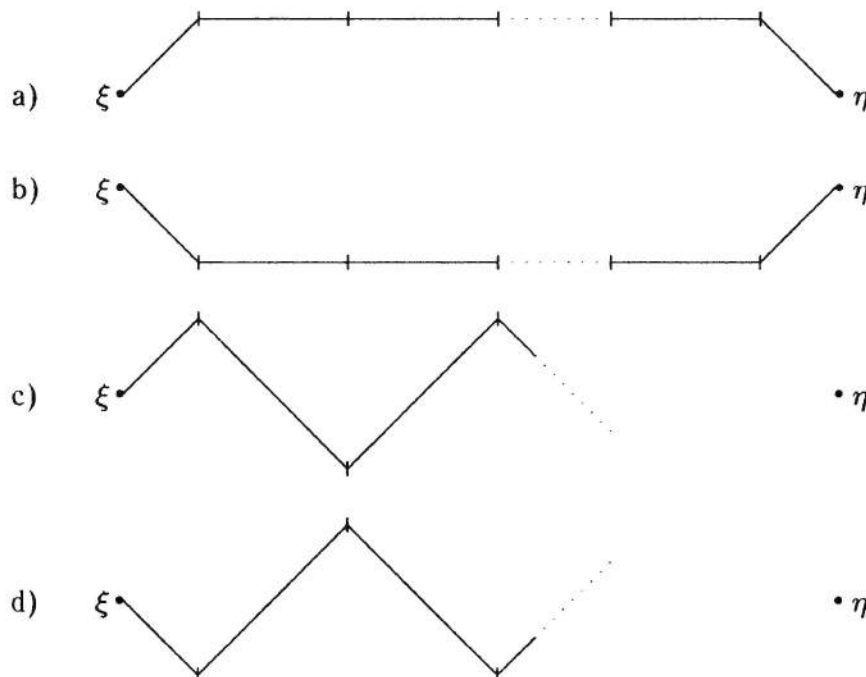


Рис. 119

Они, как нетрудно видеть, порождают минимальный проверяющий тест. Эти цепи обладают свойством: через каждый контакт любого блока, исключая первый и последний, проходит только одна цепь. В силу этого, контакты внутренних блоков разбиваются на контакты типа a , b , c и d , для контактов крайних блоков существует по две возможности. Если рассмотреть произвольную цепь схемы, то ей можно сопоставить слово длины n в 4-буквенном алфавите $\{a, b, c, d\}$ (и притом, четырьмя способами). Исходным четырем цепям проверяющего теста соответствуют четыре слова

$$\underbrace{aa \dots a}_n = a^n, \quad \underbrace{bb \dots b}_n = b^n, \quad \underbrace{cc \dots c}_n = c^n, \quad \text{и} \quad \underbrace{dd \dots d}_n = d^n.$$

По каждому такому слову цепь восстанавливается однозначно. Однако, не каждому слову длины n в 4-буквенном алфавите соответствует цепь. Рассматриваемая схемы обладает следующим свойством: для каждой двух соседних внутренних блоков существует в каждом из них по одному контакту так, что никакая проводящая цепь не проходит через них одновременно.

Теперь перейдем к рассмотрению диагностической задачи.

Теорема 52. Для счетчика четности над переменными $x_1, \dots, x_n$ существует диагностический тест для источника $I_{1,0}$, имеющий длину $2\lceil \log n \rceil + 4$ при $n \geq 5$.

Доказательство. Пусть сначала $n = 2^k$ и $\sigma = 1$. Искомый тест формируем из трех частей.

1. Первая часть состоит из цепей a^n , b^n , c^n и d^n . Устанавливает в какой цепи произошло размыкание.

2. Вторая часть для пар (a^n, d^n) и (b^n, c^n) при помощи цепей

$$a^{2^{k-1}} d^{2^{k-1}}, a^{2^{k-2}} d^{2^{k-2}} a^{2^{k-2}} d^{2^{k-2}}, \dots, a^2 d^2 a^2 d^2 \dots a^2 d^2$$

и

$$b^{2^{k-1}} c^{2^{k-1}}, b^{2^{k-2}} c^{2^{k-2}} b^{2^{k-2}} c^{2^{k-2}}, \dots, b^2 c^2 b^2 c^2 \dots b^2 c^2$$

дихотомическим образом производит локализацию неисправности. На последнем шаге место неисправности сужается до двух соседних блоков. Сделать еще один шаг, употребив слова

$$adad \dots ad \quad \text{и} \quad bcbs \dots bc,$$

необходимые до полной локализации, мы не можем, так как этим словам соответствуют множества ребер, не являющиеся цепями (см. рис. 120).

3. Третья часть получается построением из вышеупомянутых слов двух новых слов²⁰

$$acbdacbd \dots bd \quad \text{и} \quad bdacbdac \dots ac.$$

Им соответствуют две цепи, состоящие одна из нечетных фрагментов (схематически указанных на рис. 120) первого слова и четных фрагментов второго и другая из нечетных фрагментов второго слова и четных первого.

²⁰ Является своеобразным «кроссинговером» — рекомбинацией исходных слов подобно рекомбинации хромосом.

В силу этого они осуществляют оба разбиения блоков до конца. Мы получили диагностический тест и его длина равна $2k + 4 = 2\log n + 4$. Заметим, что 3-я часть необходима при $k \geq 3$. При $k = 2$ тест имеет длину $2k + 2$.

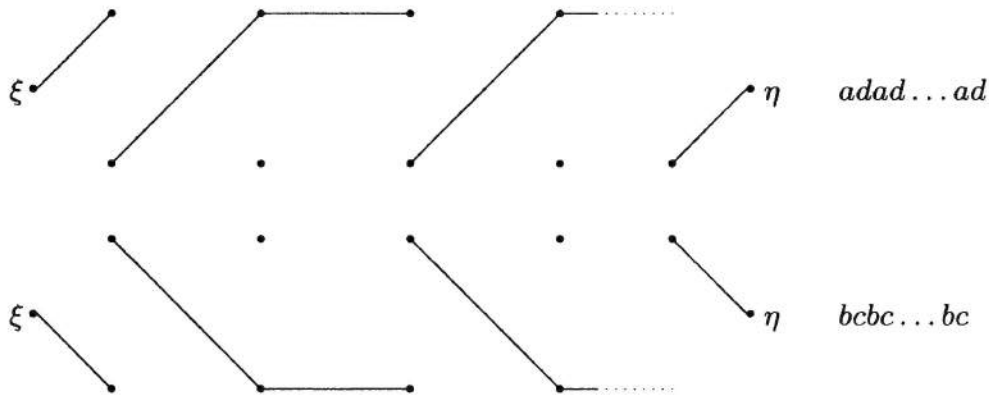


Рис. 120

Общий случай. Подбираем k так, чтобы $2^{k-1} < n \leq 2^k$. Рассмотрим счетчик четности для 2^k переменных. Исходный счетчик является подсхемой последнего: надо удалить все блоки, начиная с $n+1$, и выбросить один из полюсов η_1, η_2 с примыкающими к нему контактами (рис. 121).

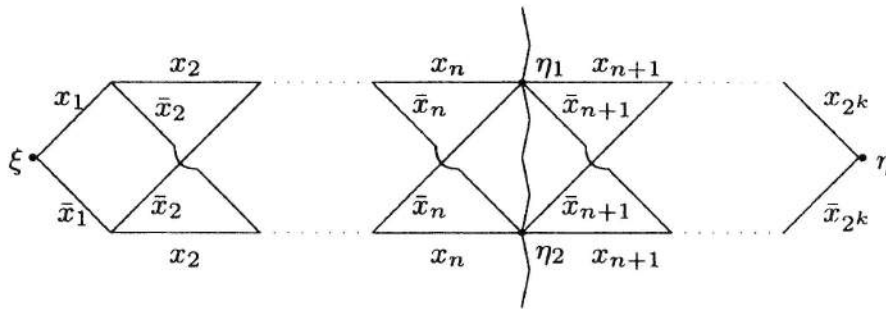


Рис. 121

Диагностический тест для подсхемы получим из диагностического теста для всей схемы так:

- 1) удалим в каждом наборе все разряды, начиная с $n+1$;
- 2) для всех наборов, соответствующие цепи которых проходили через вершину η_2 (см. рис. 121), проинвертируем последний разряд.

Полученный тест имеет длину $2k + 4 = 2\lceil \log n \rceil + 4$.

Теорема доказана.

З а м е ч а н и е. Итак, мы для счетчика четности построили логарифмический тест. Из конструкции видно, что можно построить условный тест, который имеет длину асимптотически в два раза меньшую.

В заключение рассмотрим ситуацию для малых n . При $n = 2$ и $n = 3$: проверяющие тесты и диагностические тесты имеют сложность соответственно 2 и 4. При $n = 4$, как отмечалось, диагностический тест складывается из двух частей и имеет вид

1 1 1 1 0 1 1 0 1 0 0 1 0 0 0 0 1 1 0 0 0 1 0 1.

Его сложность — 6.

ЛИТЕРАТУРА

- [1] *Быков А.Г.* Каталог самокорректирующихся контактных схем для функций трех переменных (случай замыкания). — Проблемы кибернетики. Вып. 19. — М.: Наука, 1967, с. 39–46.
- [2] *Васильев Ю.Л.* Минимальные контактные схемы для булевых функций четырех переменных. — ДАН СССР, 1959, т. 127, №2, с. 242–245.
- [3] *Вишин В.В.* Тожественные преобразования в четырехзначной логике. — ДАН СССР, 1963, т. 150, №4, с. 719–721.
- [4] *Горбовицкая Н.А.* Эквивалентные преобразования автоматов некоторых типов. — Проблемы кибернетики. Вып. 12. — М.: Наука, 1964, с. 5–28.
- [5] *Гринчук М.И.* Сложность реализации 4-местных булевых функций схемами в базисе из всех 2-местных функций. — Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996, с. 339–342.
- [6] *Карпова Н.А.* Минимальные схемы из замыкающих контактов для монотонных функций пяти переменных. — Проблемы кибернетики. Вып. 26. — М.: Наука, 1973, с. 53–94.
- [7] *Кириенко Г.И.* О самокорректирующихся схемах из функциональных элементов. — Проблемы кибернетики. Вып. 12. — М.: Наука, 1964, с. 29–37.
- [8] *Кириенко Г.И.* Синтез самокорректирующихся схем из функциональных элементов для растущего числа ошибок в схеме. — Дискретный анализ. Вып. 16. — Новосибирск, ИМ СО АН СССР, 1970, с. 38–43.
- [9] *Линдон Р.К.* Тожества в двузначных исчислениях (перевод с английского). — Кибернетический сборник 1, ИЛ, 1960, с. 234–245.
- [10] *Линдон Р.К.* Тожества в конечных алгебрах (перевод с английского). — Кибернетический сборник 1, ИЛ, 1960, с. 246–248.
- [11] *Ложкин С.А.* Об одном методе получения линейных нижних оценок сложности контактных схем и некоторых минимальных схемах для линейных функций. — Сборник трудов семинара по дискретной математике и ее приложениям. — М.: Изд-во механико-математического факультета МГУ, 1997, с. 113–115.
- [12] *Лупанов О.Б.* Об одном методе синтеза схем. — Изв. вузов, Радиофизика, 1958, т. 1., №1, с. 120–140.
- [13] *Лупанов О.Б.* О синтезе контактных схем. — ДАН СССР, 1958, т. 119, №1, с. 23–26.
- [14] *Лупанов О.Б.* Об одном классе схем из функциональных элементов (формулы с частичной памятью). — Проблемы кибернетики. Вып. 7. — М.: Физматгиз, 1962, с. 61–114.
- [15] *Лупанов О.Б.* Асимптотические оценки сложности управляющих систем. — М.: Изд-во Московского университета, 1984.
- [16] *Мадатян Х.А.* О синтезе схем, корректирующих размыкание контактов. — ДАН СССР, 1964, т. 159, №2, с. 290–293.
- [17] *Мурский В.Л.* Об эквивалентных преобразованиях контактных схем. — Проблемы кибернетики. Вып. 5. — М.: Физматгиз, 1961, с. 61–76.

- [18] *Мурский В.Л.* О преобразованиях конечных автоматов. — Проблемы кибернетики. Вып. 15. — М.: Наука, 1965, с. 101–116.
- [19] *Мурский В.Л.* Существование в трехзначной логике замкнутого класса с конечным базисом, не имеющего конечной полной системы тождеств. — ДАН СССР, 1965, т. 163, №4, с. 815–818.
- [20] *Поваров Г.Н.* Математическая теория синтеза контактных $(1, k)$ -полюсников. — ДАН СССР, 1955, т. 100, №5, с. 909–912.
- [21] *Потапов Ю.Г., Яблонский С.В.* О синтезе самокорректирующихся контактных схем. — ДАН СССР, 1960, т. 134, №3, с. 544–547.
- [22] *Тарасов В.В.* К проблеме полноты для систем функций алгебры логики с ненадежной реализацией. — Мат. сб., 1975, т. 98, №3, с. 378–394.
- [23] *Тарасов В.В.* К синтезу надежных схем из ненадежных элементов. — Мат. заметки, 1976, т. 20, №3, с. 391–400.
- [24] *Улиг Д.* О синтезе самокорректирующихся схем из функциональных элементов с малым числом надежных элементов. — Мат. заметки, 1974, т. 15, №6, с. 937–944.
- [25] *Храпченко В.М.* О сложности реализации линейной функции в классе П-схем. — Мат. заметки, 1971, т. 9, №1, с. 35–40.
- [26] *Храпченко В.М.* Об одном методе получения нижних оценок сложности П-схем. — Мат. заметки, 1971, т. 10, №1, с. 83–92.
- [27] *Чегис И.А., Яблонский С.В.* Логические способы контроля электрических схем. — Тр. МИАН СССР. — 1958, т. 51, с. 270–360.
- [28] *Яблонский С.В., Чегис И.А.* О тестах для электрических схем. — УМН, 1955, т. 10, Вып. 4 (66), с. 182–184.
- [29] *Яблонский С.В.* Функциональные построения в k -значной логике. — Труды МИАН СССР. — 1958, т. 51, с. 5–142.
- [30] *Яблонский С.В.* Основные понятия кибернетики. — Проблемы кибернетики. Вып. 2. — М.: Физматлит, 1959, с. 7–38.
- [31] *Яблонский С.В.* Об алгоритмических трудностях синтеза минимальных контактных схем. — Проблемы кибернетики. Вып. 2. — М.: Физматлит, 1959, с. 75–121.
- [32] *Яблонский С.В.* О построении тупиковых кратных экспериментов для автоматов. — Труды МИАН СССР. — 1973, т. 83, с. 263–272.
- [33] *Яблонский С.В.* Асимптотически наилучший метод синтеза надежных схем из ненадежных элементов. — Banach center pub., 1982, №7, p. 11–19.
- [34] *Яблонский С.В.* Введение в дискретную математику. — М.: Наука, 1986.
- [35] *Яблонский С.В.* Некоторые вопросы надежности и контроля управляющих систем. — Математические вопросы кибернетики. Вып. 1. — М.: Наука. Физматлит, 1988, с. 5–25.
- [36] *Янов Ю.И.* О логических схемах алгоритмов. — Проблемы кибернетики. Вып. 1. — М.: Физматлит, 1958, с. 75–127.
- [37] *Cardot C.* Quelques résultats sur l'application de l'algèbre de Boole à la synthèse des circuits à relais. — Ann. Telecomm., 1952, v. 7, №2, p. 75–84.

- [38] *Moore E.F.* Gedanken-experiments on sequential machines. Automata studies, edited by Shannon C., McCarty J. — Princeton University Press, 1956, p. 129–153. [Рус. пер.: Автоматы. — М.: ИЛ, 1956, с. 179–210.]
- [39] *Moore E.F., Shannon C.E.* Reliable circuits using less reliable relays. — Journal of the Franklin Institute. — 1956, №3, 4. [Рус. пер.: Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963, с. 114–153.]
- [40] *von Neuman J.* Probabilistic logics and the synthesis of reliable organisms from unreliable components, Automata studies, edited by Shannon C., McCarty I. — Princeton University Press. 1956. — p. 43. [Рус. пер.: Автоматы. — М.: ИЛ, 1956, с. 68–139.]
- [41] *Ninomiya I.* A study of the structures of Boolean functions and its application to the synthesis of switching circuits. — Memoirs of the Fac. of Engineering, Nagoya Univ. 13, №2, 1961.
- [42] *Post E.L.* The two-valued iterative systems of mathematical logic. — Annals of Math. Studies, v. 5, Princeton Univ. Press, Princeton–London, 1941.
- [43] *Shannon C.E.* The systhesis of two-terminal switching circuits. — Bell Syst. Techn. J., 1949, v. 28, №1, p. 59–98. [Рус. пер.: Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963, с. 59–101.]

ОГЛАВЛЕНИЕ

Предисловие редактора	3
---------------------------------	---

Ч А С Т Ь I СИНТЕЗ УПРАВЛЯЮЩИХ СИСТЕМ

ВВЕДЕНИЕ	5
Р А З Д Е Л 1. УНИВЕРСАЛЬНЫЕ МЕТОДЫ СИНТЕЗА	8
Г л а в а 1. Класс контактных схем	8
§ 1. Простейшие методы синтеза	8
§ 2. Алгоритм полного перебора (A_0)	9
§ 3. Метод Шеннона	10
§ 4. Нижняя оценка	14
§ 5. Асимптотически наилучший метод синтеза контактных схем	15
§ 6. Синтез p -полюсных ($p \geq 2$) контактных схем	20
Г л а в а 2. Класс схем из функциональных элементов	23
§ 1. Простейшие методы синтеза	23
§ 2. Алгоритм полного перебора	26
§ 3. Метод Шеннона	26
§ 4. Асимптотически наилучший метод синтеза схем из функциональных элементов в базисе $\{\&, \vee, -\}$	31
§ 5. Нижние мощностные оценки	34
Г л а в а 3. Класс автоматных схем	45
§ 1. Асимптотика для числа о.-д. функций	46
§ 2. Нижняя мощностная оценка	50
§ 3. Синтез автоматов и условия, при которых метод является асимптотически наилучшим	52
Г л а в а 4. Метод каскадов	53
Р А З Д Е Л 2. СИНТЕЗ СХЕМ ДЛЯ ОТДЕЛЬНЫХ КЛАССОВ ФУНКЦИЙ	63
§ 1. Примеры синтеза для некоторых простейших классов функций	63
§ 2. Инвариантные классы и их дескриптивные свойства	66
§ 3. Метрические свойства инвариантных классов	70
§ 4. Синтез схем для инвариантных классов	72
Р А З Д Е Л 3. ПРОБЛЕМА НИЖНИХ ОЦЕНОК СЛОЖНОСТИ УПРАВЛЯЮЩИХ СИСТЕМ	74
§ 1. Линейные нижние оценки для реализации булевых функций контактными схемами	75
§ 2. Квадратичные нижние оценки для контактных π -схем	78

Ч А С Т Ь II

ЭКВИВАЛЕНТНЫЕ ПРЕОБРАЗОВАНИЯ УПРАВЛЯЮЩИХ СИСТЕМ

ВВЕДЕНИЕ	85
§ 1. Эквивалентные преобразования формул в P_2	88
§ 2. Эквивалентные преобразования формул в P_k	93
§ 3. Эквивалентные преобразования схем из функциональных элементов	104
§ 4. Эквивалентные преобразования контактных схем	109
§ 5. Эквивалентные преобразования автоматов	120

Ч А С Т Ь III

НАДЕЖНОСТЬ УПРАВЛЯЮЩИХ СИСТЕМ

ВВЕДЕНИЕ	129
Р А З Д Е Л 1. ПОСТРОЕНИЕ НАДЕЖНЫХ СХЕМ ИЗ НЕНАДЕЖНЫХ ЭЛЕМЕНТОВ	131
§ 1. Вероятностное описание источников помех и повреждений схем	131
§ 2. Влияние ошибок на надежность схемы	136
§ 3. Синтез систем из функциональных элементов в базисе $B = \{F_{\neg}, F_{\&}, F_{\vee}, F_h\}$	142
§ 4. Асимптотически оптимальный метод построения надежных схем из ненадежных элементов	147
Р А З Д Е Л 2. СИНТЕЗ САМОКОРРЕКТИРУЮЩИХСЯ СХЕМ	149
§ 1. Построение самокорректирующихся контактных схем	149
§ 2. Построение самокорректирующихся схем из функциональных элементов	153

Ч А С Т Ь IV

КОНТРОЛЬ УПРАВЛЯЮЩИХ СИСТЕМ

ВВЕДЕНИЕ	157
§ 1. Методы построения таблицы функций неисправностей по схеме Σ и источнику И для схем без памяти	161
§ 2. Табличный подход в случае автоматов	167
§ 3. Построение таблицы отличимости	172
§ 4. Методы построения тупиковых и минимальных тестов для тестовых таблиц	174
§ 5. Обоснование алгоритма	175
§ 6. Условные и безусловные тесты	178
§ 7. Построение тестов с учетом структуры	180
Литература	184