МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им.
М. В. ЛОМОНОСОВА

ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И
КИБЕРНЕТИКИ

В. Б. Алексеев, С. А .Ложкин

# ЭЛЕМЕНТЫ ТЕОРИИ ГРАФОВ, СХЕМ И АВТОМАТОВ

Учебное пособие по курсам "Введение в дискретную математику"и
"Основы кибернетики"

Москва 2000

Рецензенты:

Часть 1. Графы.

## 1. Основные понятия теории графов.

**Определение**. *Графом* $G$ (в широком понимании) называется любая пара $(V, E)$, где $V = \{v_1, v_2, \dots\}$ — множество элементов любой природы, а $E = \{e_1, e_2, \dots\}$ — семейство пар элементов из $V$, причем допускаются пары вида $(v_i, v_i)$ и одинаковые пары. Если пары в $V$ рассматриваются как неупорядоченные, то граф называется *неориентированным*, если как упорядоченные, то граф называется *ориентированным* (*орграфом*).

Элементы множества $V$ называются *вершинами* графа, а пары из $E$ — его *ребрами*; в орграфе они называются ориентированными ребрами или *дугами*.

Говорят, что ребро $e = (u, v)$ в неориентированном графе соединяет вершины $u$ и $v$, а в ориентированном графе дуга $e = (u, v)$ идет из вершины $u$ в вершину $v$.

Графы можно условно изображать следующим образом. Вершины будем изображать точками, а каждое ребро (дугу) $(v_i, v_j) \in E$ — линией, соединяющей точки, соответствующие $v_i$ и $v_j$. Если $(v_i, v_j)$ — дуга, то на этой линии будем указывать стрелку от $v_i$ к $v_j$.

На рис. 1.1 приведены неориентированный и ориентированный графы $G = (V, E)$, где $V = \{1, 2, 3, 4\}$, $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ и $e_1 = (1, 2)$, $e_2 = (2, 3)$, $e_3 = (3, 4)$, $e_4 = (4, 2)$, $e_5 = (1, 4)$, $e_6 = (4, 2)$, $e_7 = (1, 1)$.

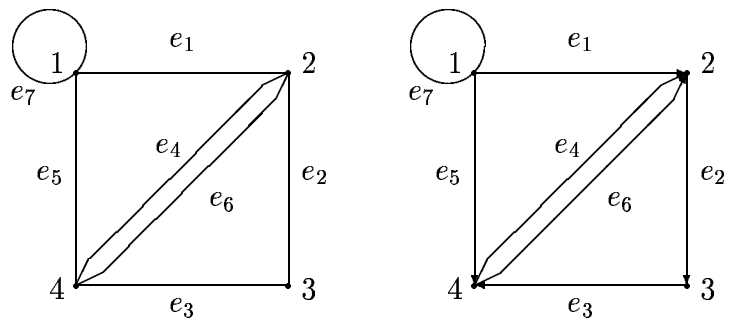



Рис. 1.1.

Пара вида $(v_i, v_i)$ называется *петлей* в вершине $v_i$. Если пара $(v_i, v_j)$ встречается в $E$ более одного раза, то говорят, что $(v_i, v_j)$ — *кратное ребро*. В графах на рис. 1.1 $(4, 2)$ — кратное ребро, $e_7$ — петля.

**Замечание**. Часто в литературе под графом понимается граф без петель и кратных ребер. В этом случае граф с кратными ребрами называют мультиграфом, граф с кратными ребрами и петлями — псевдографом.

Графы очень часто используются в приложениях, поскольку они возникают как модель при изучении многих объектов. Например, структура молекулы является графом, в котором вершинами являются атомы, а ребрами — валентные связи. Блок-схема алгоритма представляет собой орграф, в котором вершинами являются отдельные операторы, а дуги указывают переходы между ними. Другие примеры графов: элементы и соединения в электрической цепи, схема перекрестков и дорог, множество предприятий с указанием двухсторонних связей между ними, группа людей с указанием их психологической совместимости, структура управления с указанием объектов и их подчиненности друг другу и т.д.

**Определение**. Говорят, что вершины $v_i$ и $v_j$ *смежны* в графе $G = (V, E)$, если в $E$ входит пара $(v_i, v_j)$ или $(v_j, v_i)$. Говорят, что ребро (дуга) $(v_i, v_j)$ *инцидентно* вершинам $v_i$ и $v_j$.

**Определение**. *Степенью* вершины в неориентированном графе называется число ребер, инцидентных данной вершине, при этом петли учитываются дважды. Вершины степени 0 называют *изолированными*.

Например, в неориентированном графе на рис. 1.1 степень вершины 3 равна 2, степени остальных вершин равны 4.

**Теорема 1.1**. Пусть в графе $G$ $p$ вершин и $q$ ребер. Пусть $deg\ v_i$ — степень вершины $v_i$. Тогда

$$\sum_{i=1}^{p} deg\ v_i = 2q.$$

**Доказательство**. Когда мы считаем степень одной вершины, мы считаем все ребра, выходящие из нее. Вычисляя сумму всех степеней, мы получаем, что каждое ребро считается дважды, так как оно инцидентно двум вершинам (петли по определению степени также посчитаются дважды). Поэтому общая сумма будет равна удвоенному числу ребер.

В ориентированном графе можно определить степень так же, как в неориентированном графе, если не учитывать ориентацию. Кроме этого, для ориентированных графов вводится следующее определение.

**Определение**. *Полустепенью исхода* $d^-(v)$ (*полустепенью захода* $d^+(v)$) вершины $v$ в ориентированном графе называется число дуг, выходящих из данной вершины (соответственно входящих в данную вершину).

Легко видеть, что в любом ориентированном графе выполняется равенство

$$\sum_{i=1}^{p} deg^-(v_i) = \sum_{i=1}^{p} deg^+(v_i),$$

поскольку в обеих частях равенства каждая дуга учитывается ровно 1 раз.

Для человека удобно геометрическое представление графа, такое, например, как на рис 1.1. В компьютере используют другие, "более дискретные", способы представления графов. Один из наиболее распространенных способов — представление графа матрицей смежности.

**Определение**. Пусть граф $G$ имеет $p$ вершин и пусть его вершины занумерованы числами $1, 2, \ldots, p$. Матрица с $p$ строками и $p$ столбцами называется *матрицей смежности* графа $G$, если для любых $1 \leq i \leq p$ и $1 \leq j \leq p$ $\quad a[i, j]$ равно числу ребер (дуг), идущих из вершины $i$ в вершину $j$.

Например, графы, изображенные на рис. 1.1, представляются следующими матрицами смежности.

$$\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 \end{array} \qquad\qquad \begin{array}{cccc} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 \end{array}$$

При представлении графа матрицей смежности легко выполняются операции добавления или выбрасывания ребра (соответствующий элемент матрицы просто увеличивается или уменьшается на 1), легко считается степень вершины $i$ (достаточно просуммировать числа в $i$-ой строке, диагональный элемент взяв дважды). В целом, матрицы смежности очень удобны.

Однако, если в графе мало ребер, то представление графа матрицей смежности может быть не очень хорошим. Например, если в графе 50 вершин, то матрица будет иметь 2500 элементов, хотя в графе может оказаться лишь несколько сотен ребер. В таких случаях используют *списки смежностей*. Для каждой вершины образуется список, в который заносят все вершины, в которые из данной вершины идут ребра (дуги). Например, графы, изображенные на рис. 1.1, представляются следующими списками смежностей

$$\begin{array}{llllll} 1: & 1, & 2, & 4; & & \\ 2: & 1, & 3, & 4, & 4; & \\ 3: & 2, & 4; & & & \\ 4: & 1, & 2, & 2, & 3. & \end{array} \qquad\qquad \begin{array}{llllll} 1: & 1, & 2, & 4; & & \\ 2: & 3; & & & & \\ 3: & 4; & & & & \\ 4: & 2, & 2. & & & \end{array}$$

При представлении графов списками смежностей и при динамическом изменении графов необходимо использовать алгоритмы работы со списками, что хорошо реализуется в ряде алгоритмических языков.

При изучении структуры графов некоторые графы можно не различать.

**Определение**. Пусть $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ — два графа. Тогда $G_1$ и $G_2$ называются *изоморфными*, если существуют взаимно однозначные отображения $\phi_1 : V_1 \to V_2$, $\phi_2 : E_1 \to E_2$ такие, что для любого ребра (дуги) $(u, v) \in E$ выполняется $\phi_2(u, v) = (\phi_1(u), \phi_1(v))$. Другими словами, соответствующие ребра должны соединять соответствующие вершины.

Для графов без петель и кратных ребер это определение эквивалентно следующему более простому определению.

**Определение** (для графов без петель и кратных ребер). Графы $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ называются *изоморфными*, если существует взаимно однозначное отображение $\phi : V_1 \to V_2$ такое, что $(u, v) \in E_1 \iff (\phi(u), \phi(v)) \in E_2$.

Рассмотрим теперь некоторые понятия, связанные с внутренней структурой графа.

**Определение**. Граф $G_1 = (V_1, E_1)$ называется *подграфом* графа $G = (V, E)$ , если $V_1 \subseteq V$ и $E_1 \subseteq E$.

**Определение**. *Путем* в графе (орграфе) $G = (V, E)$ называется последовательность вершин и ребер (дуг) вида

$v_0, (v_0, v_1), v_1, \ldots, v_{n-1}, (v_{n-1}, v_n), v_n,$

где все $v_i \in E$ и все $(v_i, v_{i+1}) \in E$. *Длина пути* — это число ребер (дуг) в нем. Говорят, что этот путь идет из $v_0$ в $v_n$.

*Цепь* — это путь без повторяющихся ребер (дуг), *простая цепь* — путь без повторяющихся вершин.

**Лемма 1.1**. Из любого пути, идущего из $v_0$ в $v_n$, где $v_0 \neq v_n$, можно выделить подпуть из $v_0$ в $v_n$, являющийся простой цепью.

**Доказательство**. Пусть данный путь — не простая цепь. Тогда в нем повторяется некоторая вершина $v$, то есть он имеет вид: $P_1 = v_0 C_1 v C_2 v C_3 v_n$. Тогда он содержит подпуть $P_2 = v_0 C_1 v C_3 v_n$. Если в $P_2$ повторяется некоторая вершина, то аналогично удалим еще кусок и т.д. Процесс должен закончиться, т.к. $P_1$ — конечный путь.

**Определение**. Путь называется *замкнутым*, если $v_n = v_0$. Путь называется *циклом*, если $v_n = v_0$ и ребра (дуги) не повторяются. Путь называется *простым циклом*, если $v_n = v_0$ и больше нет повторений вершин.

Далее под графом будут пониматься только конечные неориентированные графы.

**Определение**. Граф $G = (V, E)$ называется *связным*, если для любых двух вершин $v_i, v_j \in V$ в $G$ существует путь из $v_i$ в $v_j$.

Отношение "существует путь из вершины $v$ в вершину $w$ в графе $G$"является отношением эквивалентности на множестве вершин. Поэтому, если граф G не связный, то его вершины можно разбить на несколько подмножеств так, что вершины в одном и том же множестве можно соединить путем, а вершины из разных множеств нельзя соединить путем. Каждое такое множество вершин вместе с ребрами графа G, соединяющими эти вершины, называется *связной компонентой* графа $G$. Так, например, граф на рис. 1.2 имеет 3 связных компоненты.

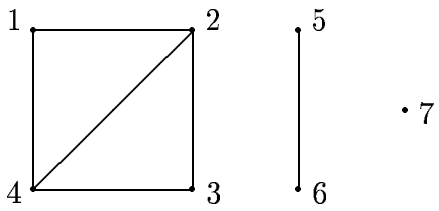



Рис. 1.2.

Докажем теперь несколько вспомогательных утверждений о связности и циклах, которые потребуются нам в дальнейшем.

**Лемма 1.2**. Если граф $G = (V, E)$ связный и $a \in V$, $b \in V$, $a \neq b$, и $(a, b) \notin E$, то при добавлении к графу $G$ ребра $(a, b)$ в полученном графе будет простой цикл.

**Доказательство**. Так как $G$ — связный граф, то в нем есть путь из $a$ в $b$. Тогда по лемме 1.1 в $G$ есть простая цепь $C$ из $a$ в $b$. Поэтому в полученном графе есть цикл $C, (b, a), a$.

**Лемма 1.3**. Если граф $G = (V, E)$ связный и ребро $(a, b)$ содержится в некотором цикле в графе $G$, то при выбрасывании из графа $G$ ребра $(a, b)$ снова получится связный граф.

**Доказательство**. Это утверждение следует из того, что при выбрасывании из графа $G$ ребра $(a, b)$ вершины $a$ и $b$ все равно остаются в одной связной компоненте, поскольку из $a$ в $b$ можно пройти по оставшейся части цикла.

**Лемма 1.4**. Пусть в графе $G = (V, E)$ $p$ вершин и $q$ ребер. Тогда в $G$ не менее $p - q$ связных компонент. Если при этом в $G$ нет циклов, то $G$ состоит ровно из $p - q$ связных компонент.

**Доказательство**. Пусть к некоторому графу $H$, содержащему вершины $u$, $v$, добавляется ребро $(u, v)$. Тогда если $u$, $v$ лежат в разных связных компонентах графа $H$, то число связных компонент уменьшится на 1. Если $u$, $v$ лежат в одной связной компоненте графа $H$, то число связных компонент не изменится. В любом случае число связных компонент уменьшается не более чем на 1. Значит при добавлении $q$ ребер

число связных компонент уменьшается не более чем на $q$. Так как граф $G$ получается из графа $G_1 = (V, \emptyset)$ добавлением $q$ ребер, то в $G$ не менее $p-q$ связных компонент. Пусть теперь в $G$ нет циклов, и пусть в процессе получения $G$ из $G_1$ добавляется ребро $(u, v)$. Если бы $u$, $v$ лежали уже в одной связной компоненте, то в $G$, согласно лемме 1.2, возникал бы цикл. Следовательно, $u$, $v$ лежат в разных связных компонентах и при добавлении ребра $(u, v)$ число связных компонент уменьшается ровно на 1. Тогда $G$ состоит ровно из $p - q$ связных компонент.

**Следствие**. Если $q \leq p-2$, то любой граф с $p$ вершинами и $q$ ребрами не связен.

**Доказательство**. По лемме 1.4 число связных компонент не менее $p - q \geq 2$.

Если граф $G$ с $p$ вершинами задан матрицей смежности $A$, то быстрое нахождение связных компонент можно осуществить следующим образом. Рассмотрим матрицу $I_1$ порядка $p$, в которой на диагонали стоят 1, $I_1(i, j) = 1$, если $a(i, j) > 0$ и $I_1(i, j) = 0$, если $a(i, j) = 0$. Тогда равенство $I_1(i, j) = 1$ равносильно тому, что из вершины с номером $i$ в вершину с номером $j$ существует путь длины не более 1. Определим теперь матрицу $I_k$ порядка $p$, в которой $I_k(i, j) = 1$ тогда и только тогда, когда из вершины с номером $i$ в вершину с номером $j$ существует путь длины не более k. Легко понять, что все матрицы $I_k$ при $k \geq p - 1$ совпадают и элемент с номером $(i, j)$ в них равен 1 тогда и только тогда, когда из вершины с номером $i$ в вершину с номером $j$ существует хотя бы один путь. Обозначим такую матрицу $I_\infty$. Рассмотрим операцию умножения матриц, которая отличается от обычного умножения только тем, что вместо сложения используется дизъюнкция. Тогда легко видеть, что $I_{k+1} = I_k \cdot I_1$.

**Утверждение**. Пусть $p - 1 \leq 2^m$. Тогда матрицу $I_\infty$ можно получить из матрицы $I_1$, используя не более $2p^3m$ операций конъюнкции и дизъюнкции.

**Доказательство**. Будем последовательно вычислять матрицы $I_2$, $I_4$, $I_8$, ..., $I_{2^m}$, возводя предыдущую матрицу в квадрат. Возведение матрицы в квадрат (по обычному правилу: "строчка на столбец") требует не более $2p^3$ операций конъюнкции и дизъюнкции. Доказываемое утверждение следует из того, что $I_{2^m} = I_\infty$, поскольку $p - 1 \leq 2^m$.

## 2. Деревья.

**Определение**. Граф $G = (V, E)$ называется *деревом*, если он связный и не содержит циклов. Вершины степени 1 в дереве называют его листьями.

**Определение**. Подграф $G_1 = (V_1, E_1)$ графа $G = (V, E)$ называется остовным деревом, если $G_1$ — дерево и $V_1 = V$.

**Теорема 2.1**. Любой (конечный) связный граф $G = (V, E)$ содержит хотя бы одно остовное дерево $G_1 = (V, E_1)$.

**Доказательство**. Если в $G$ нет циклов, то положим $G_1 = G$. Если в $G$ есть циклы, то удалим из $G$ какое-нибудь ребро, входящее в цикл. Получится некоторый подграф $G'$ . По лемме 1.3 $G'$ — связный граф. Если в $G'$ нет циклов, то положим $G_1 = G'$, иначе продолжим этот процесс. Процесс должен завершиться, так как $E$ — конечное множество.

**Теорема 2.2**. Пусть в дереве $G$ имеется $p$ вершин и $q$ ребер. Тогда $q = p - 1$.

**Доказательство**. Так как $G$ — связный граф и $G$ не содержит циклов, то $p - q = 1$ по лемме 1.4. Отсюда $q = p - 1$.

Понятие дерева можно определить различными способами, что вытекает из следующей теоремы.

**Теорема 2.3**. Пусть $G = (V, E)$ — неориентированный граф без петель и кратных ребер, $|V| = p$, $|E| = q$. Тогда следующие 5 условий эквивалентны:

1) $G$ — дерево;

2) $G$ — без циклов и $q = p - 1$;

3) $G$ — связный и $q = p - 1$;

4) $G$ — связный, но при удалении любого ребра становится несвязным;

5) $G$ — без циклов, но при добавлении любого нового ребра на тех же вершинах появляется цикл.

**Доказательство**. Докажем следущие переходы 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 4) $\Rightarrow$ 5) $\Rightarrow$ 1), откуда будет следовать, что из любого условия вытекает любое другое.

Переход 1) $\Rightarrow$ 2) следует из теоремы 2.2. Пусть теперь выполняется 2). Тогда по лемме 1.4 в $G$ число связных компонент равно $p - q = 1$, то есть $G$ — связный граф. Отсюда следует переход 2) $\Rightarrow$ 3). Переход 3) $\Rightarrow$ 4) вытекает из следствия к лемме 1.4. Пусть выполняется 4). Тогда если бы в $G$ был цикл, то при удалении любого ребра из этого цикла $G$ остался бы связным, согласно лемме 1.3. Это противоречило бы 4). Значит $G$ не имеет циклов. Вторая часть условия 5) вытекает, согласно лемме 1.2, из того, что $G$ связный. Таким образом, получаем, что 4) $\Rightarrow$ 5). Пусть выполняется 5). Если при этом $G$ — не связный граф и вершины $u$, $v$ лежат в разных связных компонентах графа $G$, то добавление к $G$ ребра $(u, v)$, очевидно, не порождает циклов, что противоречит 5). Отсюда следует, что $G$ — связный граф, то есть 5) $\Rightarrow$ 1). Теорема доказана.

Условия 4) и 5) показывают, что множество всех деревьев - это множество всех минимальных связных графов и, в то же время, множество

всех максимальных графов без циклов.

Для представления данных в информационных системах, в справочниках, при реализации алгоритмов поиска и в других приложениях часто используются *корневые деревья*, то есть деревья с выделенной вершиной, именуемой корнем. Мы дадим следующее индуктивное определение корневого дерева.

**Определение**. 1) Граф, имеющий одну вершину $v$, которая выделена, и не имеющий ребер, является корневым деревом с корнем $v$.

2) Пусть $D_1, D_2, \ldots, D_m$, где $m \geq 1$ — корневые деревья с корнями $v_1, v_2, \ldots, v_m$. Пусть $D_i = (V_i, E_i)$ и $V_i \cap V_j = \emptyset$ при $i \neq j$. Пусть $v \notin V_1 \cup V_2 \cup \cdots \cup V_m$. Тогда граф $D = (V, E)$, где $V = V_1 \cup V_2 \cup \cdots \cup V_m \cup \{v\}$, $E = E_1 \cup E_2 \cup \cdots \cup E_m \cup \{(v, v_1), \ldots, (v, v_m)\}$ и выделена вершина $v$, является корневым деревом с корнем $v$ (см. рис. 2.1). При этом $D_1, D_2, \ldots, D_m$ называются поддеревьями корневого дерева $D$.

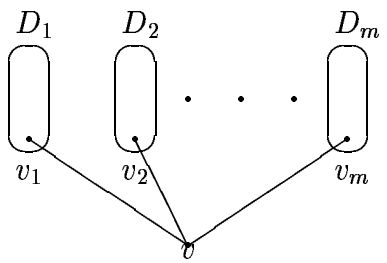



Рис. 2.1.

3) Только такие графы называются корневыми деревьями, которые могут быть построены по 1) и 2).

Например, файловая структура в компьютере является корневым деревом. При этом корню соответствует сам компьютер, вершинам второго яруса соответствуют диски A, B, C, D и т.д., вершинам третьего яруса соответствуют директории, вершинам следующих ярусов соответствуют поддиректории и файлы.

**Определение**. Упорядоченное корневое дерево — это корневое дерево $D$, в котором задан порядок его поддеревьев $D_1, D_2, \ldots, D_m$ (можно считать, что числами $1, 2, \ldots, m$ занумерованы ребра, выходящие из корня дерева $D$) и каждое $D_i$ — само есть упорядоченное корневое дерево.

**Теорема 2.4**. Число упорядоченных корневых деревьев с $q$ ребрами не превосходит $4^q$.

**Доказательство**. Рассмотрим важный для приложений способ обхода упорядоченного корневого дерева, который называют "поиском в глубину". Этот обход описывается рекурсивно следующим образом. 1) Начать из корня дерева $D$; 2) пока есть поддеревья, перейти по ребру в

корень очередного поддерева, рекурсивно обойти это поддерево "в глубину", вернуться в корень исходного дерева. В результате обход "в глубину"проходит по каждому ребру дерева $D$ ровно 2 раза: один раз при переходе в очередное поддерево, второй раз при возвращении из этого поддерева. В соответствии с обходом "в глубину"будем строить последовательность из 0 и 1, записывая на каждом шаге 0 или 1, причем 0 будем записывать, если происходит переход в очередное поддерево, а 1, если мы возвращаемся из поддерева. Получим последовательность из 0 и 1 длины $2q$, которую назовем кодом дерева $D$. По этому коду однозначно восстанавливается дерево $D$, поскольку каждый очередной разряд однозначно указывает, начинать ли строить новое очередное поддерево или возвращаться на ярус ближе к корню. Таким образом, упорядоченных корневых деревьев с $q$ ребрами не больше, чем последовательностей из 0 и 1 длины $2q$, а их число равно $2^{2q} = 4^q$.

Изоморфизм корневых деревьев определяется так же, как изоморфизм обычных графов, но дополнительно требуется, чтобы корню одного дерева сопоставлялся при изоморфизме корень другого дерева. Для упорядоченных корневых деревьев дополнительно требуется, чтобы при изоморфизме сохранялась упорядоченность.

**Следствие**. Число неизоморфных корневых деревьев с $q$ ребрами и число неизоморфных обычных деревьев с $q$ ребрами не превосходит $4^q$.

**Доказательство**. Выделяя в неизоморфных деревьях по одной точке, мы получим неизоморфные корневые деревья. Упорядочивая поддеревья в неизоморфных корневых деревьях, мы получим различные упорядоченные корневые деревья. Поэтому число неизоморфных деревьев с $q$ ребрами не превосходит числа неизоморфных корневых деревьев с $q$ ребрами, которое, в свою очередь, не превосходит числа различных упорядоченных корневых деревьев с $q$ ребрами. Отсюда и из теоремы 2.4 получаем доказываемое следствие.

Отметим, что корневые деревья часто рассматривают как ориентированные.

**Определение**. *Ориентированным деревом* называется корневое дерево, все ребра которого ориентированы к корню.

В ориентированных деревьях нет ориентированных циклов. Но это не единственные графы, обладающие этим свойством.

**Определение**. *Ориентированным ациклическим графом* называется любой ориентированный граф, в котором нет ориентированных циклов.

**Определение**. Вершина ориентированного графа называется *истоком* (*стоком*), если в нее не входит ни одна дуга, то есть $d^+(v) = 0$, (соответственно, из нее не выходит ни одной дуги, то есть $d^-(v) = 0$.

**Утверждение 1.1**. В любом (конечном) ориентированном ацикли-

ческом графе есть хотя бы один исток и хотя бы один сток.

**Доказательство**. Выберем любую вершину и будем строить путь из нее, двигаясь произвольно по направлению дуг. При этом вершины не могут повторяться, так как в данном орграфе нет ориентированных циклов. Поэтому путь должен прийти в тупик, который и является стоком. Для получения истока надо аналогично строить путь, двигаясь против направления дуг.

**Определение**. *Глубиной* вершины $v$ в ориентированном ациклическом графе называется максимальная длина ориентированного пути из всех истоков в вершину $v$.

Это определение корректно в силу утверждения 1.1. При этом глубина каждой вершины в ориентированном ациклическом графе не превосходит $p-1$, где $p$ — число вершин в графе.

**Утверждение 1.2**. Пусть $(u,v)$ — дуга в ориентированном ациклическом графе. Тогда глубина вершины $v$ больше, чем глубина вершины $u$.

Доказательство следует из того, что если из некоторого истока в вершину $u$ существует ориентированный путь длины $k$, то из того же истока в вершину $v$ существует ориентированный путь длины $k+1$.

## 3. Планарные графы.

Пусть задан неориентированный граф $G=(V,E)$. Пусть каждой вершине $v_i$ из $V$ сопоставлена точка $a_i$ в некотором евклидовом пространстве, причем $a_i \neq a_j$ при $i \neq j$. Пусть каждому ребру $e=(v_i,v_j)$ из $E$ сопоставлена непрерывная кривая $L$, соединяющая точки $a_i$ и $a_j$ и не проходящая через другие точки $a_k$. Тогда если все кривые, сопоставленные ребрам графа, не имеют общих точек, кроме концевых, то это множество точек и кривых называется *геометрической реализацией* графа $G$.

**Теорема 3.1**. Каждый конечный граф $G$ можно реализовать в трехмерном евклидовом пространстве (без пересечения ребер).

**Доказательство**. Возьмем в пространстве любую прямую $l$ и разместим на ней все вершины графа $G$. Пусть в $G$ имеется $q$ ребер. Проведем $q$ полуплоскостей через $l$ так, чтобы прямая $l$ была их общим ребром (типа тетрадки). После этого каждое ребро графа $G$ можно изобразить линией в своей полуплоскости и они, очевидно, не будут пересекаться.

**Определение**. Граф называется *планарным*, если существует его планарная реализация, то есть геометрическая реализация на плоскости (без пересечения ребер).

Если имеется планарная реализация графа на плоскости и мы разрежем плоскость по всем линиям этой планарной реализации, то плоскость

распадется на части, которые называются *гранями* этой планарной реализации (одна из граней бесконечна, она называется *внешней гранью*).

**Теорема 3.2 (формула Эйлера)**. Для любой планарной реализации связного планарного графа $G = (V, E)$ с $p$ вершинами, $q$ ребрами и $r$ гранями выполняется равенство: $p - q + r = 2$.

**Доказательство**. При фиксированном $p$ индукцией по $q$. Так как $G$ — связный граф, то $q \geq p - 1$ по следствию из леммы 1.4.

а) Базис индукции: $q = p - 1$. Так как $G$ — связный и $q = p - 1$, то по теореме 2.3 $G$ — дерево, то есть в $G$ нет циклов. Тогда $r = 1$. Отсюда $p - q + r = p - (p - 1) + 1 = 2$.

б) Пусть для $p - 1 \leq q < q_0$ теорема справедлива. Докажем, что для $q = q_0$ она тоже справедлива. Пусть $G$ — связный граф с $p$ вершинами и $q_0$ ребрами и пусть в его планарной реализации $r$ граней. Так как $q_0 > p - 1$, то $G$ — не дерево. Следовательно, в $G$ есть цикл. Пусть ребро $e$ входит в цикл. Тогда к нему с двух сторон примыкают разные грани. Удалим ребро $e$ из $G$. Тогда две грани сольются в одну, а полученный граф $G_1$ по лемме 1.3 останется связным. При этом получится планарная реализация графа $G_1$ с $p$ вершинами, $q_0 - 1$ ребрами и $r - 1$ гранями. Так как $q_0 - 1 < q_0$, то, по предположению индукции, для $G_1$ справедлива формула Эйлера, то есть $p - (q_0 - 1) + (r - 1) = 2$, откуда $p - q_0 + r = 2$. Что и требовалось доказать.

**Следствие 1**. Формула Эйлера справедлива и для геометрической реализации связных графов на сфере.

**Доказательство**. Пусть связный граф $G$ с  вершинами и $q$ ребрами реализован на сфере $S$ так, что число граней равно $r$. Пусть точка $A$ на сфере не лежит на линиях этой геометрической реализации. Пусть $P$ — некоторая плоскость. Поставим сферу $S$ на $P$ так, чтобы точка $A$ была самой удаленной от плоскости. Спроектируем $S$ на $P$ центральным проектированием с центром в $A$. Тогда на плоскости $P$ мы получим геометрическую реализацию связного графа с  вершинами и $q$ ребрами, причем число граней будет равно $r$ (грань на сфере, содержащая $A$, отображается во внешнюю грань на плоскости). По теореме 3.2 получаем $p - q + r = 2$.

**Следствие 2**. Для любого выпуклого многогранника справедливо равенство $p - q + r = 2$, где  - число вершин, $q$ -число ребер, $r$ - число граней.

**Доказательство**. Пусть выпуклый многогранник $M$ имеет  вершин, $q$ ребер и $r$ граней. Пусть $O$ — внутренняя точка многогранника . Рассмотрим сферу $S$ с центром в $O$ настолько большого радиуса, чтобы $M$ целиком лежал внутри $S$. Рассмотрим центральное проектирование с центром в точке $O$, и спроектируем вершины и ребра $M$ на $S$. Тогда на

$S$ мы получим геометрическую реализацию некоторого связного графа с  вершинами, $q$ ребрами и $r$ гранями. Отсюда $p - q + r = 2$.

Формула Эйлера позволяет доказать непланарность некоторых графов.

**Определение**. Графом $K_5$ называется граф с 5 вершинами, в котором каждая пара вершин соединена ребром (см. рис. 3.1).

**Теорема 3.3**. Граф $K_5$ не планарен.

**Доказательство**. Допустим, что для графа $K_5$ существует планарная реализация. Так как граф $K_5$ связен, то для этой планарной реализации справедлива формула Эйлера $p - q + r = 2$. Поскольку в графе $K_5$ имеем $p = 5$ и $q = 10$, то число всех граней должно равняться $r = 2 - p + q = 7$. Пусть грани занумерованы $1, 2, \ldots, r$ и пусть при обходе $i$-ой грани по периметру (по ее краю) проходится $q_i$ ребер. Так как при этом каждое ребро проходится дважды (оно является стороной для двух граней), то $\sum_{i=1}^{r} q_i = 2q = 20$. Но в каждой грани не менее 3 сторон. Поэтому $q_i \geq 3$ для всех $i$. Отсюда $\sum_{i=1}^{r} q_i \geq 3r = 21$. Получаем $20 \geq 21$ — противоречие. Значит для графа $K_5$ не существует планарной реализации.

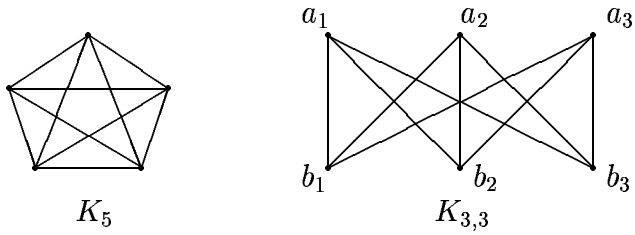



Рис. 3.1.

**Определение**. Графом $K_{3,3}$ называется граф с 6 вершинами $a_1, a_2, a_3$, $b_1, b_2, b_3$, в котором каждая вершина $a_i$ соединена ребром с каждой вершиной $b_j$ и нет других ребер (см. рис. 3.1).

С графом $K_{3,3}$ связана следующая известная задача о трех домах и трех колодцах. Есть 3 дома и 3 колодца, но хозяева домов в большой вражде. Можно ли так проложить дорожки от каждого дома к каждому колодцу, чтобы они нигде не пересекались?

Ответ на этот вопрос дает следующая теорема.

**Теорема 3.4**. Граф $K_{3,3}$ не планарен.

Доказательство. Допустим, что для графа $K_{3,3}$ существует планарная реализация. Так как граф $K_{3,3}$ связен, то для этой планарной реализации справедлива формула Эйлера $p - q + r = 2$. Поскольку в графе $K_{3,3}$ имеем $p = 6$ и $q = 9$, то число всех граней должно равняться $r = 2 - p + q = 5$. Так же, как в доказательстве предыдущей теоремы, получаем,

что $\sum_{i=1}^{r} q_i = 2q = 18$, где $q_i$ — число сторон в $i$-ой грани. Но в графе $K_{3,3}$ нет циклов длины 3. Поэтому в каждой грани не менее 4 сторон. Следовательно, $q_i \geq 4$ для всех $i$. Отсюда $\sum_{i=1}^{r} q_i \geq 4r = 20$. Получаем $18 \geq 20$ — противоречие. Значит для графа $K_{3,3}$ не существует планарной реализации.

Граница любой грани является путем в графе, так, например, границей внутренней грани на рис. 3.2 является путь (указаны только вершины): 1,2,4,5,4,6,4,2,3,1. Пусть длина границы $i$-ой грани (число ребер) равна $q_i$ (для грани на рис. 3.2 $q = 9$).

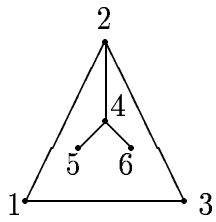



Рис. 3.2.

**Лемма 3.1**. Для любой геометрической реализации на плоскости связного планарного графа с $q$ ребрами выполняется равенство:

$$\sum_{i=1}^{r} q_i = 2q,$$

где суммирование ведется по всем граням (включая внешнюю грань).

**Доказательство**. Равенство следует из того, что у каждого ребра две стороны и при суммировании $q_i$ каждое ребро учитывается дважды: либо оно входит в границы двух соседних граней, либо оно дважды учитывается в одной грани.

**Теорема 3.5**. Если в связном планарном графе $G = (V, E)$ с $p$ вершинами и $q$ ребрами нет циклов длины меньше $k$ ($k \geq 3$), то $q \leq \frac{k}{k-2}(p-2)$.

**Доказательство**. Так как по условию $q_i \geq k$ для всех $k$, то из леммы 3.1 получаем $2q \geq kr$ и $r \leq \frac{2q}{k}$. Из формулы Эйлера $r = 2 - p + q$. Отсюда $2 - p + q \leq \frac{2q}{k}$. Далее $(k-2)q \leq k(p-2)$ и $q \leq \frac{k}{k-2}(p-2)$.

**Следствие 1**. Для любого связного планарного графа $G = (V, E)$ без петель и кратных ребер с $p$ вершинами и $q$ ребрами справедливо неравенство: $q \leq 3(p-2)$.

**Указание**. В теореме 3.5 можно взять $k = 3$.

**Следствие 2**. Для любого планарного графа $G = (V, E)$ без петель и кратных ребер с $p$ вершинами, $q$ ребрами и $m$ связными компонентами справедливо неравенство: $q \leq 3(p - 2m)$.

**Доказательство**. Пусть в $i$-ой связной компоненте ($i = 1, 2, \ldots, m$) $p_i$ вершин и $q_i$ ребер. Тогда в ней по следствию 1 $q_i \leq 3(p_i - 2)$. Суммируя все эти неравенства, получаем $q \leq 3(p - 2m)$.

**Следствие 3**. В любом планарном графа $G = (V, E)$ без петель и кратных ребер есть вершина степени не более 5.

**Доказательство**. Пусть $G$ — планарный граф с $p$ вершинами и $q$ ребрами. Тогда $q \leq 3(p-2) < 3p$. Пусть $d_{min}$ — минимальная степень вершин в $G$. Тогда с учетом теоремы 1.1 получаем

$$6p > 2q = \sum_{i=1}^{p} deg\ v_i \geq pd_{min}.$$

Отсюда $d_{min} < 6$, то есть $d_{min} \leq 5$.

Если ребро графа изображено в виде линии, то можно на ней поставить точку и считать ее новой вершиной степени 2. Формально эта операция определяется следующим образом.

**Определение**. Пусть $G$ — любой граф и $(a, b)$ — его ребро. *Операцией подразделения* ребра $(a, b)$ называется удаление из графа $G$ ребра $(a, b)$, добавление новой вершины $c$ и добавление двух новых ребер $(a, c)$ и $(c, b)$ .

**Определение**. Граф $G_1$ называется *подразделением* графа $G$, если $G_1$ может быть получен из $G$ несколькими подразделениями ребер.

**Определение**. Графы $G_1$ и $G_2$ называются *гомеоморфными*, если существуют их подразделения, которые изоморфны.

Существует следующий критерий планарности.

**Теорема 3.6 (Понтрягина-Куратовского)**. Для того, чтобы граф $G$ был планарным, необходимо и достаточно, чтобы он не содержал ни одного подграфа, гомеоморфного графам $K_5$ или $K_{3,3}$.

**Доказательство**. 1) Необходимость. Пусть $G$ — планарный. Допустим, что он содержит подграф $G_1$, гомеоморфный графу $K_5$ или $K_{3,3}$. Рассмотрим планарную реализацию графа $G$. Удалив лишние вершины и ребра, мы получим планарную реализацию подграфа $G_1$. Но $G_1$ геометрически — это граф $K_5$ или $K_{3,3}$ с точками на ребрах. Если проигнорировать эти точки, то мы получим планарную реализацию графа $K_5$ или $K_{3,3}$. Но это невозможно по теоремам 3.3 и 3.4.

2) Достаточность доказывается тяжело, и здесь мы это доказательство опустим. Доказательство можно найти, например, в [2].

Подмножество вершин графа называется *независимым*, если никакие вершины из этого подмножества не смежны (не соединены ребром). Во многих приложениях рассматриваются разбиения вершин на независимые подмножества. Такие разбиения удобно описывать следующим образом.

**Определение**. Пусть $K = \{C_1, C_2, \ldots, C_m\}$ — произвольное множество элементов, называемых *цветами*. Отображение $C : V \to \{C_1, C_2, \ldots, C_m\}$, где $V$ — множество вершин графа $G$, называется *раскраской* (*вершинной*) графа $G$. Раскраска называется *правильной*, если для любого ребра $(v_1, v_2) \in E$ выполняется $(v_1) \neq (v_2)$.

**Теорема 3.7**. Вершины любого планарного графа можно правильно раскрасить в не более чем 5 цветов.

**Доказательство** (индукцией по числу вершин $p$).

1) Базис индукции: $p = 1$ — очевидно.

2) Пусть для $p < p_0$ утверждение справедливо и пусть $G = (V, E)$ — планарный граф с $|V| = p_0$. По следствию 3 из теоремы 3.5 в $G$ есть вершина $v$ степени не более 5. Рассмотрим укладку на плоскости графа $G$ без пересечения ребер. Удалим из $G$ вершину $v$ и все инцидентные ей ребра. Получим планарный граф $G_1$ с числом вершин $p_0 - 1$. По предположению индукции его вершины можно правильно раскрасить в 5 цветов $C_1, C_2, C_3, C_4, C_5$. Пусть в $G$ вершина $v$ смежна с $v_1, v_2, \ldots, v_k$, (где $k \leq 5$). Рассмотрим 2 варианта:

а) Среди цветов вершин $v_1, v_2, \ldots, v_k$ в $G$ нет цвета $C_i$ $(1 \leq i \leq 5)$. Тогда вершине $v$ припишем цвет $C_i$ и получим правильную раскраску графа $G$ в 5 цветов.

б) Степень вершины $v$ равна 5 и среди вершин $v_1, v_2, \ldots, v_5$ в $G_1$ есть все 5 цветов. Без ограничения общности будем считать, что в укладке графа $G$ ребра $(v, v_1)$, $(v, v_2)$, $(v, v_3)$, $(v, v_4)$, $(v, v_5)$ выходят из $v$ в порядке по часовой стрелке и что $(v_i) = {}_i, i = 1, \ldots, 5$. Пусть $V_1$ — множество всех вершин в $G_1$, до которых можно дойти из $v_1$ по ребрам графа $G_1$, используя только вершины цветов $C_1$ и $C_3$. Возможны 2 варианта:

б1) $v_3 \notin V_1$. Тогда в $V_1$ поменяем цвета $C_1 \to C_3$, $C_3 \to C_1$. Так как вершины из $V_1$ не смежны с другими вершинами цветов $C_1$ и $C_3$, то останется правильная раскраска и среди $v_1, v_2, \ldots, v_5$ не будет цвета $C_1$. Тогда вершине $v$ припишем цвет $C_1$.

б2) $v_3 \in V_1$. Это значит, что в $G_1$ есть цепь из $v_1$ в $v_3$, все вершины которой имеют цвета $C_1$ и $C_3$. Эта цепь вместе с ребрами $(v_3, v)$ и $(v, v_1)$ образует цикл в $G$, причем вершины $v_2$ и $v_4$ лежат по разные стороны от этого цикла. Это значит, что из $v_2$ нельзя пройти в $v_4$ в графе $G_1$ только по вершинам цветов $C_2$ и $C_4$. Пусть $V_2$ — множество всех вершин в $G_1$, до которых можно дойти из $v_2$ по ребрам графа $G_1$, используя только вершины цветов $C_2$ и $C_4$. Тогда $v_4 \notin V_2$ и далее поступаем как в б1).

В любом случае вершины графа $G$ можно правильно раскрасить в не более чем 5 цветов, и теорема доказана.

# Часть 2. Схемы.

В настоящее время получили широкое распространение сложные преобразователи информации, которые составлены из простейших преобразователей (элементов) и в которых движутся сигналы нескольких типов, преобразуемые или передаваемые отдельными элементами в соответствии с определенными законами. В теории управляющих систем рассматриваются различные теоретико-графовые модели таких преобразователей, называемые *схемами*. Каждая схема характеризуется *структурой* – графом определенного вида и *функционированием* – законом преобразования входных наборов или их последовательностей в выходные наборы или их последовательности. Функционирование схемы однозначно определяется ее структурой и функционированием *элементов базиса* – набора простейших преобразователей, из которых построена схема.

При изучении схем решаются две основные задачи: задача анализа и задача синтеза. Задача анализа состоит в нахождении функционирования данной схемы, а задача синтеза – в построении схемы, имеющей (реализующей) заданное функционирование. Каждая из этих задач может рассматриваться либо как индивидуальная задача, и тогда ее решением является конкретное функционирование (схема), либо как массовая задача, и тогда ее решением должен быть алгоритм нахождения функционирования (схемы). Задача синтеза имеет, как правило, множество решений, из которых выбирают решение, оптимальное по какому-либо критерию. Чаще всего в качестве такого критерия выступает *сложность схемы*, понимаемая как сумма сложностей составляющих ее элементов.

В §4-8 мы рассмотрим, как решается задача синтеза для некоторых конкретных видов схем.

## § 4. Формулы и схемы из функциональных элементов. Задача синтеза и простейшие способы ее решения.

В [8, с.14-20] дано индуктивное определение формулы и реализуемой ею функции алгебры логики (ФАЛ). С содержательной точки зрения формула представляет собой слово, построенное из символов "базисных"ФАЛ, символов булевых переменных (БП) и разделителей, которое задает последовательность выполнения операций суперпозиции. Напомним это определение и рассмотрим способ представления формул с помощью деревьев.

Пусть $X$ - счетный упорядоченный алфавит БП, и пусть у нас имеется счетный алфавит функциональных символов (ФС) для обозначения ФАЛ от этих БП. Две ФАЛ считаются, как обычно [8], *равными*, если они имеют одни и те же существенные БП и задают одинаковые отображения области значений этих БП, т.е. единичного куба $B^n$, где $B = \{0,1\}$, а $n$ - число БП, во множество $B$. Функция, существенно зависящая от всех своих БП, называется *существенной*.

Пусть, далее, $= \{\varphi_1, \varphi_2, ..., \varphi_b\}$ - система "исходных"ФАЛ или, иначе, базис, где ФАЛ $\varphi_i$, $i = 1, ..., b$, зависит от $k_i$, $k_i \geq 1$, БП и является

существенной ФАЛ, если $k_i \geq 2$. Предполагается, что система базисных ФАЛ полна в алгебре логики, и допускается, в общем случае, наличие в ней "лишних"ФАЛ, после удаления которых оставшаяся система по-прежнему является полной (см. [8]). Предполагается также, что все ФС $\varphi_i$, $i = 1, ..., b$, различны, хотя, возможно, некоторым из них соответствуют равные ФАЛ.

Сопоставим каждому ФС $\varphi_i$, $i = 1, ..., b$, функциональный элемент (ФЭ) $\mathcal{E}_i$, имеющий $k_i$ входов, причем входу с номером $j$ соответствует $j$-я БП $x_j$ ФАЛ $\varphi_i$, и один выход, на котором эта ФАЛ реализуется (см. рис. 4.1.а). Упрощенный вариант изображения ФЭ $\mathcal{E}_i$ в виде вершины графа с пометкой $\varphi_i$, в которую входят $k_i$ упорядоченных, т.е. пронумерованных числами $1, .., k_i$, дуг, показан на рис. 4.1.б. При этом предполагается, что дуга с номером $j$, $1 \leq j \leq k_i$, соответствует $j$-му входу ФЭ $\mathcal{E}_i$. В дальнейшем мы, как правило, не будем делать существенных различий между ФС $\varphi_i$ и ФЭ $\mathcal{E}_i$. Чаще всего мы будем иметь дело с базисом $_0 = \{\&, \vee, \neg\}$, где базисными являются ФАЛ $x_1 \cdot x_2$, $x_1 \vee x_2$ и $\overline{x_1}$.


а) б)

Рис. 4.1

Дадим индуктивное определение формулы над Б и реализуемой ею ФАЛ (это определение в отличие от [8] неявно предполагает наличие в Б ФАЛ, тождественно равной БП).

Любая БП $x_j$ из $X$ считается *формулой глубины 0* над Б, которая реализует ФАЛ, равную $x_j$. Если для всех $j$, $j = 1, ..., k_i$, определена формула $\mathcal{F}_j$ глубины $q_j$ над базисом Б, которая реализует ФАЛ $f_j$ от БП из $X$, то запись вида

$$\mathcal{F} = \varphi_i(\mathcal{F}_1, ..., \mathcal{F}_{k_i}) \tag{4.1}$$

является *формулой глубины* $q + 1$ над Б, где

$$q = max\{q_1, ..., q_{k_i}\}, \tag{4.2}$$

которая реализует ФАЛ $f$ от БП из $X$ такую, что $f = \varphi_i(f_1, ..., f_{k_i})$. Так, запись вида

$$(\overline{x_1 \cdot x_2}) \cdot (x_1 \vee x_2) \tag{4.3}$$

является формулой глубины 3 над базисом $_0$, которая реализует ФАЛ $x_1 \oplus x_2$. Все записи, полученные в результате указанного индуктивного построения, и только они, считаются *формулами* над Б.

Важным частным случаем формул над базисом $_0$ являются (см., например, [8]) дизъюнктивные нормальные формы (ДНФ). Напомним, что любую ФАЛ

$f(x_1, ..., x_n)$ можно представить ее совершенной ДНФ:

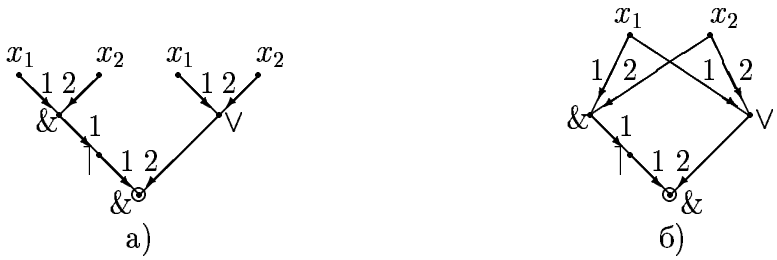
$$f(x_1, ..., x_n) = \bigvee_{\sigma=(\sigma_1,...,\sigma_n)\in N_f} x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}, \qquad (4.4)$$

где, как обычно, $x^0 = \overline{x}$ и $x^1 = x$ , а $N_f$ - множество тех наборов $\sigma, \sigma \in B^n$ , для которых $f(\sigma) = 1$ .

Индукцией по глубине каждой формуле глубины $q$ над Б можно сопоставить упорядоченное корневое дерево глубины $q$ , все ребра которого ориентированы к корню, каждому листу сопоставлена БП из $X$ , а каждой внутренней вершине - ФС из Б. Так, формуле $x_j$ соответствует "тривиальное"дерево с единственной вершиной, являющейся корнем и листом одновременно, которой сопоставлена БП $x_j$ (см. рис. 4.2.а). Формуле $\mathcal{F}$ вида (4.1) соответствует дерево $D$ с корнем $v$ , показанное на рис. 4.2.б, где $D_j$ , $j = 1, ..., k_i$ , - дерево с корнем $v_j$ , которое соответствует формуле $\mathcal{F}_j$ . Граф, который получается из дерева $D$ , соответствующего формуле $\mathcal{F}$ , в результате "склеивания"листьев с одинаковыми пометками, называется *квазидеревом, соответствующим формуле* $\mathcal{F}$ . На рис. 4.3.а показано дерево, а на рис. 4.3.б - квазидерево, которые соответствуют формуле (4.3). Заметим, что формула по сопоставленному ей дереву или квазидереву восстанавливается однозначно.


а) б)

Рис. 4.2




а) б)

Рис. 4.3

Рассмотрим теперь более общую по сравнению с формулами модель - модель схем из функциональных элементов (СФЭ), в которой последовательность операций суперпозиции базисных ФАЛ задается с помощью ориентированного ациклического графа, обобщающего квазидерево, и где возможно многократное использование промежуточных результатов.

Пусть $X$ и $Z$ - счетные упорядоченные попарно не пересекающиеся алфавиты БП, причем БП из $X$ ( $Z$ ) считаются *входными* (соответственно,

*выходными*) БП. Пусть по-прежнему Б, Б= $\{\varphi_i\}_{i=1}^{b}$ , - полный базис, где ФАЛ $\varphi_i$ , $i = 1, ..., b$ , зависит от $k_i$ , $k_i \geq 1$ , БП и является существенной ФАЛ, если $k_i \geq 2$ .

По аналогии с упорядоченными деревьями ориентированнный граф $G$ называется *упорядоченным*, если дуги, входящие в каждую его вершину $v$ , упорядочены, т.е. пронумерованы числами $1, 2, ..., d^+(v)$ .

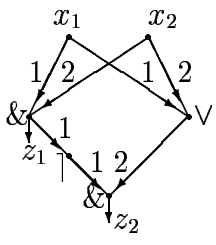
*Определение. Схемой из функциональных элементов над базисом Б* называется ориентированный ациклический упорядоченный граф $\Sigma$ , вершины которого помечены следующим образом:

1) каждый исток $\Sigma$ помечен некоторой БП из $X$ , причем различные истоки помечены различными БП;

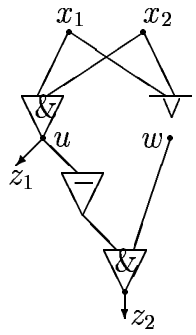
2) каждая отличная от истока вершина $v$ схемы $\Sigma$ помечена ФС $\varphi_i$ , где $k_i = d^+(v)$ ;

3) некоторые вершины $\Sigma$ помечены выходными БП из $Z$ так, что одной и той же вершине может быть сопоставлено несколько БП из $Z$ , но разным вершинам не может быть сопоставлена одна и та же БП. При этом входные (выходные) БП, которые приписаны каким-либо вершинам $\Sigma$ , считаются *входными* (соответственно, *выходными*) БП $\Sigma$ , а те вершины, которым они сопоставлены, - *входами* (соответственно, *выходами*) СФЭ $\Sigma$ .

Заметим, что квазидерево, соответствующее формуле над базисом Б, становится СФЭ над Б, если его корню приписать выходную БП. В связи с этим формулы над Б будем считать частным случаем СФЭ над Б. На рис 4.4.а показан пример СФЭ над базисом $_0$ с входными БП $x_1, x_2$ и выходными БП $z_1, z_2$ , которая получена из квазидерева, приведенного на рис. 4.3.б, а на рис. 4.4.б дано ее более "наглядное"изображение в виде сети (см. [6, с.227- 229]), построенной из соответствующих ФЭ.




а)




б)

Рис. 4.4

Определим теперь функционирование СФЭ $\Sigma$ над базисом Б с входными БП $x_1, x_2, ..., x_n$ и выходными БП $z_1, ..., z_m$ . [1] Сначала индукцией по $q$ , $q = 0, 1, ...$ , определим для каждой вершины $v$ глубины $q$ в схеме $\Sigma$ реализуемую в ней формулу $\mathcal{F}_v = \mathcal{F}_v(x_1, ..., x_n)$ глубины $q$ над базисом Б.

[1] Предполагается, что входные и выходные БП перечислены в соответствии с их упорядоченностью в $X$ и $Z$ .

Если $q = 0$, т.е. $v$ - вход $\Sigma$, положим $\mathcal{F}_v = x_j$, где $x_j$ - входная БП, сопоставленная вершине $v$. Пусть теперь $v$ - вершина глубины $q$, $q \geq 1$, схемы $\Sigma$, которая имеет пометку $\varphi_i$ и в которую входит $k_i$ дуг, причем дуга с номером $j$, $1 \leq j \leq k_i$, исходит из вершины $v_j$ глубины $q_j$, где уже реализована формула $\mathcal{F}_j = \mathcal{F}_{v_j}$ глубины $q_j$, а для чисел $q, q_1, ..., q_{k_i}$ выполнено (4.2). Тогда в вершине $v$ реализуется формула $\mathcal{F} = \mathcal{F}_v$ вида (4.1), которая имеет глубину $q + 1$.

При этом считается, что в вершине $v$ СФЭ $\Sigma$ *реализуется ФАЛ* $f(x_1, ..., x_n)$, если ФАЛ $f$ реализуется формулой $\mathcal{F}_v$, и что СФЭ $\Sigma$ *реализует систему ФАЛ* $F$, $F = (f_1, ..., f_m)$, или *реализует систему булевых уравнений*: $z_1 = f_1, ..., z_m = f_m$, если $f_j$, $j = 1, ..., m$, – ФАЛ, реализованная в той выходной вершине СФЭ $\Sigma$, которой приписана БП $z_j$. Так, СФЭ на рис. 4.4 реализует систему ФАЛ $(x_1 \cdot x_2, x_1 \oplus x_2)$ или систему уравнений: $z_1 = x_1 \cdot x_2, z_2 = x_1 \oplus x_2$. Схемы, реализующие одинаковые системы ФАЛ, называются *эквивалентными*. Заметим, что изменение нумерации дуг, входящих в такую вершину $v$ СФЭ $\Sigma$, которой сопоставлен ФЭ $\varepsilon_i$ с симметрической ФАЛ $\varphi_i$, не изменяет ФАЛ, реализуемую в вершине $v$, а значит, не влияет на функционирование $\Sigma$. В связи с этим в подобных случаях номера дуг, входящих в вершину $v$, могут не указываться.

Две СФЭ $\Sigma'$ и $\Sigma''$ считаются *изоморфными*, если они изоморфны как помеченные графы, т.е. если существуют такие взаимнооднозначные отображения множества вершин $\Sigma'$ на множество вершин $\Sigma''$ и множества дуг $\Sigma'$ на множество дуг $\Sigma''$, которые сохраняют отношение инцидентности вершин и дуг, а также все пометки. Из определения вытекает, что в соответствующих друг другу вершинах изоморфных СФЭ реализуются одинаковые формулы, а значит, и одинаковые ФАЛ. Следовательно, две изоморфные СФЭ эквивалентны.

Пусть СФЭ $\Sigma'$ получается из СФЭ $\Sigma$ в результате удаления вершины $v$ и переноса начальной вершины всех дуг $\Sigma$, исходящих из $v$, а также всех выходных БП, приписанных $v$, в отличную от нее вершину $w$, глубина которой в $\Sigma$ не больше, чем глубина $v$. Тогда СФЭ $\Sigma'$ считается результатом применения к СФЭ $\Sigma$ *операции удаления вершины* $v$, а вершина $w$ называется *преемником* вершины $v$. Тот факт, что СФЭ $\Sigma'$ получается из СФЭ $\Sigma$ в результате (многократной) операции удаления вершин из СФЭ $\Sigma$, будем записывать в виде неравенства $\Sigma' < \Sigma$. Схема $\Sigma$ называется *тупиковой*, если она не эквивалентна ни одной СФЭ $\Sigma'$ такой, что $\Sigma' < \Sigma$.

Вершина СФЭ называется *висячей*, если из нее не выходит ни одна дуга и она не является выходом схемы. Две вершины СФЭ считаются *эквивалентными*, если в них реализуются равные ФАЛ. Применяя к СФЭ $\Sigma$ операцию удаления одной из двух эквивалентных вершин, преемником которой является другая вершина, мы получим СФЭ $\Sigma'$, которая, очевидно, эквивалентна $\Sigma$.

Схема называется *приведенной* (*строго приведенной*), если в ней нет висячих (соответственно висячих и эквивалентных) вершин. Заметим, что тупиковая

СФЭ является строго приведенной, и что из любой СФЭ можно получить эквивалентную ей приведенную (строго приведенную) СФЭ с помощью операции удаления висячих (соответственно висячих и эквивалентных) вершин.

Рассмотрим теперь задачу синтеза на примере СФЭ. Число ФЭ в СФЭ называется ее *сложностью*. Сложность СФЭ $\Sigma$ обозначается через $L(\Sigma)$. Для системы ФАЛ $F$ через $L(F)$ обозначим минимальную сложность тех СФЭ $\Sigma$ над базисом Б, которые реализуют $F$. Величина $L(F)$ называется *сложностью* системы ФАЛ $F$ над базисом Б. При этом СФЭ $\Sigma$, которая реализует $F$, и для которой $L(\Sigma) = L(F)$, считается *минимальной* СФЭ над базисом Б. Заметим, что СФЭ, показанная на рис. 4.4, является минимальной СФЭ над базисом $_0$, и что сложность системы ФАЛ $F = (x_1 \cdot x_2, x_1 \oplus x_2)$ над базисом $_0$ равна 4.

Введем, далее, функцию $L(n)$ натурального аргумента $n$, которая определяется следующим образом:

$$L(n) = \max_{f(x_1,\ldots,x_n)} L(f)$$

и называется *функцией Шеннона* для класса СФЭ над базисом Б. Функция Шеннона характеризует сложность самой "сложной"ФАЛ от БП $x_1, \ldots, x_n$ в классе СФЭ над базисом Б.

Вместо сложности $L(\Sigma)$ СФЭ $\Sigma$ можно рассмотреть ее глубину $D(\Sigma)$, а затем аналогичным образом определить глубину $D(F)$ для системы ФАЛ $F$ в базисе Б и ввести функцию Шеннона $D(n)$. Можно рассмотреть "взвешенную"сложность (глубину) СФЭ, когда при подсчете сложности (соответственно глубины) каждый ФЭ учитывается со своим коэффициентом, и т.п. Можно рассматривать подобные функционалы сложности для подклассов класса СФЭ (класса формул, класса ДНФ и т.д.). В дальнейшем мы, как правило, будем рассматривать оптимальную по сложности реализацию ФАЛ в классе СФЭ над базисом $_0$. В связи с этим индекс $= _0$ будем опускать.

Для решения задачи синтеза СФЭ можно использовать переборный алгоритм, который просматривает все схемы сложности $1, 2, 3, \ldots$ до тех пор, пока не найдет схему, реализующую заданную систему ФАЛ. Следует отметить, что трудоемкость этого метода синтеза очень быстро растет с ростом числа переменных $n$, и что при $n \geq 5$ он становится практически неприменимым.

С другой стороны, всегда можно использовать метод синтеза, основанный на моделировании совершенной ДНФ. Следующее утверждение непосредственно вытекает из (4.4).

**Лемма 4.1.** Для любой ФАЛ $f(x_1, \ldots, x_n)$ существует СФЭ, реализующая $f$ со сложностью не более, чем $n \cdot 2^{n+1}$.

**Следствие.** $L(n) \leq n \cdot 2^{n+1}$

*Замечание.* Во многих случаях после построения СФЭ по лемме 4.1. целесообразно использовать операцию удаления эквивалентных вершин для перехода к соответствующей строго приведенной СФЭ.

## §5. Реализация некоторых "управляющих"систем функций алгебры логики в классе СФЭ.

Рассмотрим примеры решения задачи индивидуального синтеза СФЭ - синтеза СФЭ для систем ФАЛ, которые часто встречаются в практике проектирования дискретных управляющих систем и для которых хотелось бы иметь более простые схемы, чем схемы, построенные по лемме 4.1.

Для множества $A$ и любого натурального $n$ через $(A)^n$ или просто $A^n$ обозначается, как обычно, $n$-я декартова степень множества $A$, т.е. множество наборов (слов, систем) *длины* $n$ с элементами из $A$. Для набора $\beta$, $\beta \in A^n$, через $\beta[i]$, где $1 \leq i \leq n$, обозначается его $i$-й элемент, т.е. $\beta = (\beta[1], ..., \beta[n])$. Если $\alpha \in B^n$, то число $\sum_{i=1}^{n} \alpha[i] \cdot 2^{n-i}$, т.е. число, двоичная запись которого совпадает с $\alpha$, называется *номером* $\alpha$ и обозначается через $|\alpha|$.

Пусть $P_2(n)$, $n = 1, 2, ...$, – множество всех ФАЛ от БП $x_1, x_2, ..., x_n$, а $P_2^m(n)$ – его $m$-я декартова степень, $m = 1, 2, ...$, т.е. множество систем из $m$ ФАЛ от БП $x_1, x_2, ..., x_n$. Определим некоторые "управляющие"системы ФАЛ и рассмотрим реализующие их СФЭ. При этом мы часто будем давать одно и то же название как самой системе ФАЛ, так и СФЭ, которая ее реализует, добавляя к нему в случае необходимости слово "функциональный", если речь идет о системе ФАЛ, и слово "схемный", если речь идет о схеме.

Система ФАЛ $Q_n$ из $P_2(n)$ такая, что при всех $i$, $i = 1, 2, ..., 2^n$, справедливо равенство:

$$Q_n[i] = x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}, \tag{5.1}$$

где $\sigma = (\sigma_1, ..., \sigma_n) \in B^n$ и $|\sigma| = i - 1$, называется (функциональным) *дешифратором порядка* $n$. Это связано с тем, что на любом наборе $\alpha$, $\alpha \in B^n$, значений БП $x_1, ..., x_n$ ровно одна из ФАЛ системы $Q_n$, – ФАЛ с номером $|\alpha| + 1$, – обращается в 1.

Функция $\mu_n$ от (входных) БП $x_1, ..., x_n, y_0, y_1, ..., y_{2^n-1}$ такая, что при всех $\alpha$, $\alpha \in B^n$, и $\beta$, $\beta \in B^{2^n}$, имеет место равенство:

$$\mu_n(\alpha, \beta) = \beta[i],$$

где $(i - 1) = |\alpha|$, называется (функциональным) *мультиплексором порядка* $n$. Если рассматривать БП $x_1, ..., x_n$ как "адресные"БП, а БП $y_0, y_1, ..., y_{2^n-1}$ – как "информационные"БП, то значение мультиплексора $\mu_n$ равно значению той его информационной БП, номер которой поступил на адресные БП $\mu_n$. Легко убедиться в том, что для ФАЛ $\mu_n$ справедливо представление:

$$\mu_n(x_1, ..., x_n, y_0, ..., y_{2^n-1}) = \bigvee_{i=1}^{2^n} Q_n[i] \cdot y_{i-1} \tag{5.2}$$

Под (функциональным) *шифратором порядка* $n$ понимается любая система из $n$ ФАЛ от входных БП $x_0, x_1, ..., x_{2^n-1}$ такая, что каждому входному набору

$\alpha$ , в котором равна 1 только одна БП $x_j$ , $0 \leq j \leq 2^n - 1$ , она сопоставляет выходной набор $\beta, \beta \in B^n$ , для которого $|\beta| = j$ . Тем самым, шифратор вырабатывает "адрес"той входной БП, которая равна 1, если другие входные БП принимают при этом нулевые значения.

Будем называть схемным дешифратором, мультиплексором или шифратором любую СФЭ, которая реализует соответствующую систему ФАЛ.

Обозначим через $\Theta_n$ систему длины $2^{2^n}$ из всех различных ФАЛ множества $P_2(n)$ , в которой столбец значений ФАЛ $\Theta_n[i]$ , $1 \leq i \leq 2^{2^n}$ , рассматриваемый как двоичный набор длины $2^n$ , имеет номер $(i-1)$ . Систему $\Theta_n$ будем называть *универсальной системой ФАЛ порядка* $n$ , а любую СФЭ, которая ее реализует, – *универсальным многополюсником порядка* $n$ .

Отметим, что дешифратор, мультиплексор и шифратор часто используются в качестве составных частей схем записи и чтения информации по заданному адресу.

Рассмотрим теперь вопросы, касающиеся сложности описанных схем.

При построении "сложных"СФЭ из более простых мы будем опираться на понятие подсхемы и принцип эквивалентной замены (см. [9]). СФЭ $\Sigma'$ называется *подсхемой* СФЭ $\Sigma$ , если множество ее вершин (дуг) является подмножеством множества вершин (соответственно дуг) $\Sigma$ , а все те вершины $\Sigma'$ , из которых в $\Sigma$ выходит хотя бы одна дуга, не принадлежащая $\Sigma'$ , или которые являются выходами $\Sigma$ , являются выходами $\Sigma'$ . При этом предполагается, что все дуги в $\Sigma'$ имеют те же номера, что и в $\Sigma$ , а все вершины $\Sigma'$ имеют те же ФС, что и в $\Sigma$ . Принцип эквивалентной замены для СФЭ вытекает из определения их функционирования и состоит в том, что если подсхему $\Sigma'$ СФЭ $\Sigma$ заменить эквивалентной ей СФЭ $\Sigma''$ , то полученная в результате СФЭ $\hat{\Sigma}$ будет эквивалентна СФЭ $\Sigma$ . В связи с этим подсхемы, которые не имеют общих внутренних вершин, можно рассматривать как (многовыходные) макроэлементы.

**Лемма 5.1.** Для любого натурального $n$ существует схемный дешифратор порядка $n$ , имеющий сложность не более, чем $n \cdot 2^{n+1}$ , и глубину не более, чем [2] $]\log n[+1$ .

*Доказательство.* Для построения искомого дешифратора достаточно каждую ФАЛ системы $Q_n$ реализовать по ее совершенной ДНФ (5.1) на основе $d$ -ярусного дерева из $n$ ФЭ $\&$ , где $d = ]\log n[$ (см. рис. 5.1).

[2] Через $]a[$ обозначается ближайшее сверху к $a$ целое число; основание 2 у логарифмов опускается.

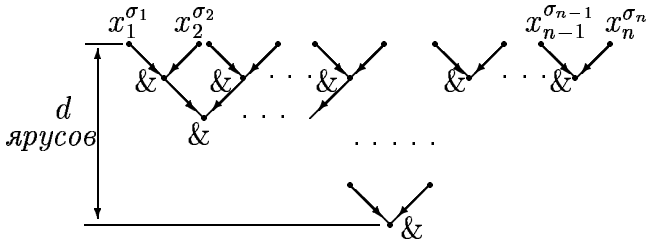


Рис. 5.1

**Следствие.** $L(Q_n) \leq n \cdot 2^{n+1}$ .

Следующее утверждение доказывается, по существу, применением к построенному в лемме 5.1 схемному дешифратору операции удаления эквивалентных вершин (см. §4 ).

**Теорема 5.1.** Сложность минимального схемного дешифратора порядка $n$ равна

$$2^n + O(n \cdot 2^{n/2}).$$

*Доказательство.* Поскольку любой дешифратор порядка $n$ при $n \geq 2$ реализует систему из $2^n$ ФАЛ, отличных от БП, то в нем должно быть по крайней мере $2^n$ вершин, отличных от входов. Следовательно, сложность любого дешифратора порядка $n$ , $n \geq 2$ , в классе СФЭ не меньше, чем $2^n$.

Разобьем набор входных БП $x = (x_1, ..., x_n)$ на поднаборы $x' = (x_1, ..., x_k)$ и $x'' = (x_{k+1}, ..., x_n)$ , где $k$ - некоторый параметр и $1 \leq k \leq (n-1)$ . Пусть $Q'$ и $Q''$ – функциональные дешифраторы порядка $k$ и $(n-k)$ от БП $x'$ и $x''$ , а $\Sigma'$ и $\Sigma''$ – соответствующие им схемные дешифраторы, которые построены по лемме 5.1. Легко видеть, что любую ФАЛ $Q_n[i]$ , $1 \leq i \leq 2^n$ , можно представить в виде

$$Q_n[i] = Q'[j] \cdot Q''[l], \tag{5.3}$$

где $i = 2^{n-k}(j-1) + l$ и $1 \leq j \leq 2^k, 1 \leq l \leq 2^{n-k}$ . Дешифратор $\Sigma$ порядка $n$ от БП $x$ содержит дешифраторы $\Sigma', \Sigma''$ в качестве подсхем и реализует каждую ФАЛ $Q_n[i]$ , $1 \leq i \leq 2^n$ , с помощью одного ФЭ & , входы которого присоединены к выходам $\Sigma'$ и $\Sigma''$ (см. рис. 5.2) в соответствии с (5.3). Из построения $\Sigma$ следует, что

$$L(\Sigma) = 2^n + L(\Sigma') + L(\Sigma'') \leq 2^n + n + k \cdot 2^{k+1} + (n-k)2^{n-k+1},$$

и поэтому при $k = [n/2]$ получим:

$$L(\Sigma) \leq 2^n + O(n \cdot 2^{n/2}).$$

*Теорема доказана.*

**Следствие 1.** Построенный дешифратор порядка $n$ имеет глубину не больше, чем $]\log n[+2$ .

**Следствие 2.** Если в качестве дешифраторов $\Sigma'$ и $\Sigma''$ взять дешифраторы, уже построенные по теореме 5.1, то полученный дешифратор порядка $n$ будет иметь сложность

$$2^n + 2^{[n/2]} + 2^{]n/2[} + O(n \cdot 2^{n/4}) \leq 2^n + \frac{3\sqrt{2}}{2} 2^{n/2} + O(n \cdot 2^{n/4})$$

и поэтому

$$2^n \leq L(Q_n) = 2^n + \frac{3\sqrt{2}}{2} 2^{n/2} + O(n \cdot 2^{n/4}).$$

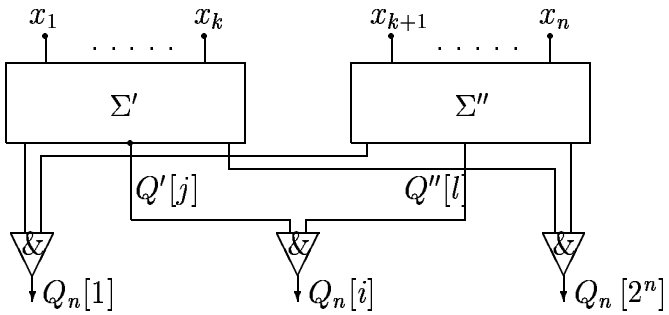


Рис. 5.2

**Лемма 5.2.** Для любого натурального $n$ существует схемный мультиплексор порядка $n$, который имеет сложность не более, чем $3 \cdot 2^n + O(n \cdot 2^{n/2})$

*Доказательство.* Построим схемный мультиплексор $\Sigma$ в соответствии с (5.2) на основе дешифратора $\Sigma''$ порядка $n$, который является его подсхемой. Для этого каждый выход $\Sigma''$ и соответствующий ему информационный вход $\Sigma$ присоединим к входам ФЭ &, а затем продизъюнктируем выходы всех таких ФЭ &. Если дешифратор $\Sigma''$ взять из теоремы 5.1, то полученный таким образом мультиплексор $\Sigma$ будет искомым.

*Лемма доказана.*

**Следствие.** Построенный мультиплексор порядка $n$ имеет глубину не больше, чем $n+]\log n[+3$.

**Теорема 5.2.** Существует схемный мультиплексор порядка $n$, имеющий сложность

$$2^{n+1} + O(2^{n/2}).$$

*Доказательство.* Разобьем набор $x = (x_1, ..., x_n)$ адресных БП мультиплексора $\mu_n$ на поднаборы $x'$ и $x''$ так же, как это было сделано при доказательстве теоремы 5.1, а набор $y = (y_0, ..., y_{2^n-1})$ его информационных БП – на поднаборы $y^{(1)}, ..., y^{(2^k)}$ длины $2^{n-k}$ каждый, где $y^{(j)}[l] = y_{i-1}$ при $i = 2^{n-k}(j-1) + l$ и всех $j, l$ таких, что $1 \leq j \leq 2^k$, $1 \leq l \leq 2^{n-k}$. При этом из (5.2), (5.3) следует, что:

$$\mu_n(x, y) = \bigvee_{j=1}^{2^k} Q'[j] \left( \bigvee_{l=1}^{2^{n-k}} Q''[l] \cdot y^{(j)}[l] \right),$$

и поэтому

$$\mu_n(x,y) = \mu_k(x', \mu_{n-k}(x'', y^{(1)}), ..., \mu_{n-k}(x'', y^{(2^k)})) \qquad (5.4)$$

Рассмотрим мультиплексор $\Sigma$, который реализует $\mu_n$ по формуле (5.4). Для каждого $j$, $j = 1, ..., 2^k$, $\Sigma$ содержит в качестве подсхемы мультиплексор $\Sigma''_j$ порядка $(n-k)$ от БП $x'', y^{(j)}$, причем выходы этих мультиплексоров подаются в соответствии с (5.4) на информационные входы мультиплексора $\Sigma'$ порядка $k$ с адресными БП $x'$ (см. рис. 5.3). Если мультиплексоры $\Sigma'$ и $\Sigma''_j$, $j = 1, ..., 2^k$, построить в соответствии с леммой 5.2, а затем перейти от СФЭ $\Sigma$ к эквивалентной ей строго приведенной СФЭ $\hat{\Sigma}$ (см. §4 ), то при $k = [n/2]$ мы получим искомый мультиплексор. Действительно, из доказательства леммы 5.2 следует, что все мультиплексоры $\Sigma''_j$, $j = 1, ..., 2^k$, имеют общий дешифратор $\Sigma''$ порядка $(n-k)$, и поэтому

$$L(\hat{\Sigma}) \le L(\Sigma') + 2^{n+1} + L(\Sigma'') \le 2^{n+1} + O(2^{n/2})$$

в силу теоремы 5.1.

*Теорема доказана.*

**Следствие.** $L(\mu_n) \le 2^{n+1} + O(2^{n/2})$

Наряду с дешифратором $Q_n$ и мультиплексором $\mu_n$ порядка $n$ иногда рассматривают также *полудешифратор* $\hat{Q}_n$ порядка $n$ с входными БП $x_1, ..., x_n$ и *полумультиплексор* $\hat{\mu}_n$ порядка $n$ с входными БП $x_1, ..., x_n, y_0, ..., y_{2^{n-1}-1}$, такие, что

$$\hat{\mu}_n = \bigvee_{j=0}^{2^{n-1}-1} y_j Q_n[j + 2^{n-1} + 1], \quad \hat{Q}_n[i] = Q_n[2^{n-1} + i],$$

где $i = 1, ..., 2^{n-1}$. Заметим, что при $x_1 = 0$ имеют место равенства:

$$\hat{\mu}_n = 0, \quad \hat{Q}_n[i] = 0.$$

Аналогично доказанным выше утверждениям устанавливаются оценки:

$$L(\hat{Q}_n) = 2^{n-1} + O(2^{n/2}),$$

$$L(\hat{\mu}_n) \le 2^n + O(2^{n/2}).$$

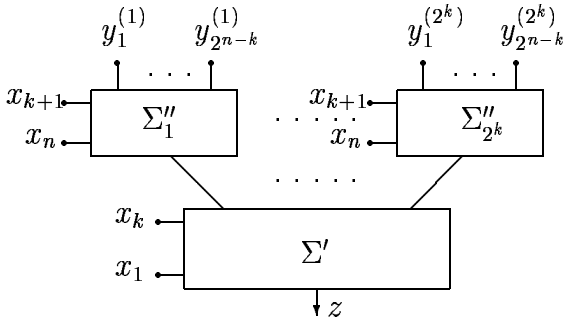



Рис. 5.3

Перейдем теперь к построению шифраторов. Определим систему ФАЛ $D_n$ длины $n$ от БП $x = (x_0, x_1, ..., x_{2^n-1})$ так, что

$$D_n[i] = \bigvee_{\sigma=(\sigma_1,...,\sigma_{i-1},1,\sigma_{i+1},...,\sigma_n)} x_{|\sigma|} \tag{5.5}$$

для всех $i$, $i = 1, ..., n$. Заметим, что $D_n[i] = 1$ тогда и только тогда, когда среди БП $x_j$, $j = 0, 1, ..., 2^n - 1$, номер которых имеет единицу в $i$-м разряде своей двоичной записи, есть хотя бы одна БП, раная единице. Это означает, что система ФАЛ $D_n$ является (функциональным) шифратором порядка $n$. Если для каждого $i$, $i = 1, ..., n$, ФАЛ $D_n[i]$ реализовать формулой (5.5), то мы получим схемный шифратор сложности $n(2^{n-1} - 1)$, так как в каждую дизъюнкцию (5.5) входит ровно половина БП набора $x$. Следовательно, доказано утверждение:

**Лемма 5.3.** Для любого натурального $n$ существует схемный шифратор порядка $n$, который имеет сложность не более, чем $n \cdot 2^{n-1}$.

Более "экономный "схемный шифратор может быть построен с помощью рекурсивного разбиения множества входных БП пополам.

**Теорема 5.3.** Существует схемный шифратор порядка $n$, сложность которого не больше, чем $2^{n+1}$.

*Доказательство.* Разобьем набор БП $x = (x_0, ..., x_{2^n-1})$ на поднаборы $x' = (x_0, ..., x_{2^{n-1}-1})$ и $x'' = (x_{2^{n-1}}, ..., x_{2^n-1})$. Пусть $D'$ и $D''$ – функциональные шифраторы порядка $(n-1)$ от БП $x'$ и $x''$, а $\Sigma'$ и $\Sigma''$ – соответствующие им схемные шифраторы. Из (5.5) следует, что

$$D_n[1] = x_{2^{n-1}} \vee ... \vee x_{2^n-1} = x_{2^{n-1}} \vee \bigvee_{j=1}^{(n-1)} D''[j] \tag{5.6}$$

и

$$D_n[i+1] = D'[i] \vee D''[i] \tag{5.7}$$

для всех $i$, $i = 1, ..., (n-1)$. Следовательно, из шифраторов $\Sigma'$ и $\Sigma''$, а также $(2n-2)$ ФЭ $\vee$ на основе (5.6)-(5.7) можно построить шифратор $\Sigma$ порядка $n$, для которого:

$$L(\Sigma) \le L(\Sigma') + L(\Sigma'') + (2n-2) \tag{5.8}$$

Используя неравенство (5.8) рекурсивно и полагая, что $L(D_1) \le 1$, так как $D_1$ состоит из БП $x_1$, получим:

$$L(\Sigma) \le 2(n-1) + 4(n-2) + ... + 3 \cdot 2^{n-3} + 2 \cdot 2^{n-2} + 2^{n-1} =$$

$$= 2^{n-1}\left(1 + \frac{1}{2} \cdot 2 + ... + \frac{1}{2^{n-1}}(n-1)\right) \le 2^{n-1}\left(\sum_{t=1}^{\infty} \frac{t}{2^{t-1}}\right) = 2^{n-1} \sum_{s=1}^{\infty} \sum_{t=s}^{\infty} \frac{1}{2^{t-1}} = 2^{n+1}$$

*Теорема доказана.*

**Следствие.** $L(D_n) \leq 2^{n+1}$ .

**Теорема 5.4.** Минимальный универсальный многополюсник порядка $n$ имеет сложность $2^{2^n} - n$ .

*Доказательство.* Нижняя оценка следует из того, что универсальный многополюсник порядка $n$ реализует систему из $2^{2^n} - n$ ФАЛ, отличных от БП (см. доказательство теоремы 5.1). Для получения верхней оценки построим универсальный многополюсник $\Sigma$ по совершенным ДНФ всех реализуемых ФАЛ (см. лемму 4.1), а затем перейдем от него к эквивалентной строго приведенной СФЭ $\Sigma'$ (см. §4). Заметим, что число вершин СФЭ $\Sigma'$ , отличных от входов, не больше, чем число различных ФАЛ от БП $x_1, ..., x_n$ , отличных от этих БП. Следовательно,

$$L(\Sigma') \leq 2^{2^n} - n.$$

*Теорема доказана.*

## §6. Реализация некоторых "арифметических"систем ФАЛ в классе СФЭ.

Рассмотрим теперь некоторые "арифметические"системы ФАЛ и построим реализующие их СФЭ.

Системы $S_n$ , $M_n$ и $W_n$ , состоящие из $(n+1)$ , $2n$ и $n$ ФАЛ от БП $x = (x_1, ..., x_n), y = (y_1, ..., y_n)$ соответственно, такие, что

$$|S_n(x,y)| = |x| + |y|, \ |M_n(x,y)| = |x| \cdot |y|,$$

и, если $|x| \geq |y|$ , то

$$|W_n(x,y)| = |x| - |y|,$$

называются (функциональным) *сумматором, умножителем* и *вычитателем порядка* $n$ соответственно.

Система $C_n$ , состоящая из $(n+1)$ ФАЛ от БП $x = (x_1, ..., x_{2^n})$ , такая, что значение $|C_n(x)|$ равно числу единиц в наборе $x$ , называется (функциональным) *счетчиком порядка* $n$ .

В [8] приведен сумматор порядка $n$ , имеющий сложность $9n - 5$ . Мы построим такой же сумматор несколько иначе.

**Теорема 6.1.** Существует схемный сумматор порядка $n$ , имеющий сложость $9n - 5$ .

*Доказательство.* Для $n = 1$ сумматор $\Sigma_1$ показан на рис. 4.4. На рис. 6.1.а показана СФЭ $\Sigma'$ сложности 9, которая реализует систему ФАЛ $S'$ от БП $x$, $y$ и $q'$ такую, что

$$|S'(x,y,q')| = x + y + q',$$

т.е. реализует сложение трех одноразрядных чисел. Действительно, на выходе $z_2$ СФЭ $\Sigma'$ реализуется ФАЛ $x \oplus y \oplus q'$, а на выходе $z_1$ единица появляется только тогда, когда либо $x = y = 1$, либо $x \oplus y = q' = 1$, т.е. на выходе $z_1$ в СФЭ $\Sigma'$ реализуется ФАЛ

$$xy \vee (x \oplus y)q' = xy \vee xq' \vee yq' = h(x, y, q').$$

Схемный сумматор $\Sigma_n$ порядка $n$ с входными БП $x_1, ..., x_n, y_1, ..., y_n$ и выходными БП $z_0, z_1, ..., z_n$ можно построить из сумматора $\Sigma_{n-1}$ порядка $(n-1)$ с входными БП $x_2, ..., x_n, y_2, ..., y_n$ и выходными БП $z'_1, z_2, ..., z_n$, а также одной СФЭ $\Sigma'$ так, как это показано на рис. 6.2. Заметим, что переход от сумматора $\Sigma_{n-1}$ к сумматору $\Sigma_n$ моделирует сложение $n$-разрядных чисел в два этапа: на первом этапе складываются числа, образуемые $(n-1)$ младшими разрядами, а на втором этапе складываются старшие разряды и перенос, возникший на первом этапе. Очевидно, что

$$L(\Sigma_n) = 9n - 5.$$

*Теорема доказана.*

**Следствие.** $L(S_n) \leq 9n - 5$.

*Замечание.* Если схему $\Sigma'$ на рис. 6.2 заменить на схему $\Sigma''$, показанную на рис. 6.1.б, мы получим (схемный) *квазисумматор порядка* $n$, $n \geq 2$, который имеет сложность $9n - 9$ и правильно складывает $n$-разрядные двоичные числа, каждое из которых не превосходит $2^{n-1}$.

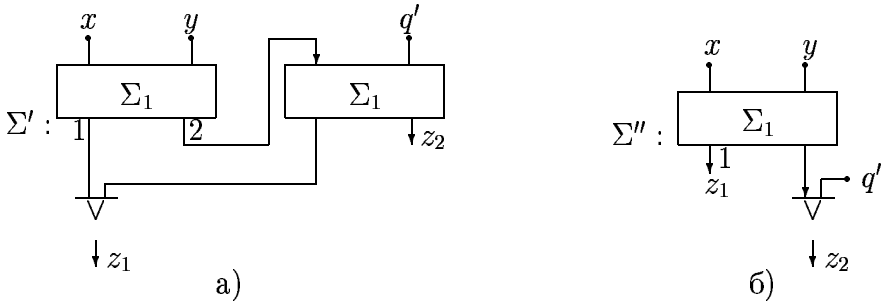



Рис. 6.1

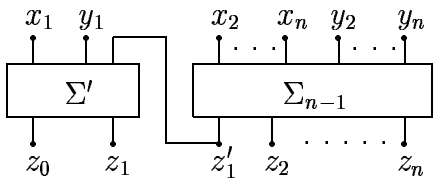



Рис. 6.2

**Теорема 6.2.** Существует схемный вычитатель порядка $n$, имеющий сложность не больше, чем $11n - 5$.

*Доказательство.* Заметим, что

$$|\overline{x}| = 2^n - 1 - |x|,$$

где $x = (x_1, ..., x_n)$ , $\overline{x} = (\overline{x}_1, ..., \overline{x}_n)$ , и поэтому

$$W_n(x, y) = |x| - |y| = 2^n - 1 - (2^n - 1 - |x| + |y|) = \overline{S_n(\overline{x}, y)}$$

Следовательно, схемный вычитатель порядка $n$ может быть получен из схемного сумматора порядка $n$ в результате инвертирования входов его первого слагаемого, а также всех его выходов, и имеет сложность не больше, чем $11n - 5$ .

*Теорема доказана.*

*Замечание.* Из построенного вычитателя в результате "поднятия"отрицаний, присоединенных к выходам $z_2$ схемы $\Sigma'$ или $\Sigma_1$ в соответствии с равенствами

$$z_2 = \overline{u}\&w, \ \overline{z_2} = u \vee \overline{w},$$

где $u$ и $w$ - выходы ФЭ $\&$ и $\vee$ СФЭ $\Sigma_1$ (см. рис. 4.4.б), можно получить вычитатель сложности не больше, чем $10n - 4$ .

**Теорема 6.3.** Существует схемный счетчик порядка $n$ , который имеет сложность не более, чем $9 \cdot 2^n$ .

*Доказательство.* Счетчик $\Sigma_n$ порядка $n$ с входными БП $x_1, ..., x_{2^n}$ и выходными БП $z_1, ..., z_{n+1}$ можно построить из счетчика $\Sigma_{n-1}$ порядка $(n-1)$ с входными БП $x_1, .., x_{2^{n-1}}$ и выходными БП $z'_1, ..., z'_n$ , такого же счетчика $\Sigma_{n-1}$ с входными БП $x_{2^{n-1}+1}, ..., x_{2^n}$ и выходными БП $z''_1, ..., z''_n$ , а также квазисумматора (см. замечание к теореме 6.1) $\hat{\Sigma}$ порядка $n$ с входными БП $z'_1, ..., z'_n, z''_1, ..., z''_n$ и выходными БП $z_1, ..., z_{n+1}$ (см. рис. 6.3), поскольку на выходах счетчиков $\Sigma_{n-1}$ числа, большие, чем $2^{n-1}$ , не позволяются.

В силу замечания к теореме 6.1 квазисумматор $\hat{\Sigma}$ можно построить со сложностью не больше, чем $9n - 9$ , и поэтому

$$L(\Sigma) \leq 2L(\Sigma') + (9n - 9) \tag{6.1}$$

Используя неравенство (6.1) рекурсивно и полагая, что $L(\Sigma_1) = 4$ , так как $C_1[1] = x_1 \cdot x_2$ , $C_1[2] = x_1 \oplus x_2$ , то есть $C_1 = S_1$ , получим

$$L(\Sigma_n) \leq 9(n-1) + 18(n-2) + ... + 9 \cdot 2^{n-2} + 4 \cdot 2^{n-1}$$

Следовательно (см. выкладки в конце доказательства теоремы 5.3),

$$L(\Sigma_n) \leq 9 \cdot 2^n$$

*Теорема доказана.*

**Следствие.** $L(C_n) \leq 9 \cdot 2^n$

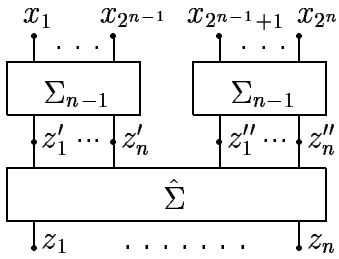



Рис. 6.3

*Замечание.* В общем случае счетчик, то есть схема с $n$ выходами, на которых появляется двоичная запись числа единиц в наборе значений входных переменных, может иметь $N$, $2^{n-1} \leq N < 2^n$, входов. Такой счетчик можно построить из "стандартных"счетчиков, порядки которых соответствуют номерам единичных компонент набора $\alpha$, $\alpha \in B^n$, такого, что $|\alpha| = N$, и не более чем $(n-1)$-го сумматора порядка $n$. Каждый из стандартных счетчиков вычисляет число единиц в своей части набора из $N$ переменных, а сумматоры складывают числа, появившиеся на выходах счетчиков. Сложность построенной схемы не превосходит, очевидно, $9(N+n^2)$.

## §7. Метод Шеннона для синтеза СФЭ. Верхние и нижние оценки функции Шеннона и сложности некоторых ФАЛ.

В §4 был рассмотрен простейший метод синтеза СФЭ для произвольной ФАЛ $f(x_1,...,x_n)$, основанный на моделировании ее совершенной ДНФ. Если при этом воспользоваться замечанием к лемме 4.1 и все конъюнкции вида $x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}$ реализовать с помощью одного схемного дешифратора, то в силу теоремы 5.1 можно построить СФЭ $\Sigma_f$, которая реализует ФАЛ $f(x_1,..,x_n)$ и для которой

$$L(\Sigma_f) \leq 2^{n+1} + O(n \cdot 2^{n/2}).$$

Рассмотрим еще более "экономный"метод синтеза СФЭ – метод Шеннона.

**Теорема 7.1.** Для любой ФАЛ $f(x_1,...,x_n)$ можно построить СФЭ $\Sigma_f$, которая реализует $f$ и для которой

$$L(\Sigma_f) \leq 6 \cdot \frac{2^n}{n} + O\left(\frac{2^n \log n}{n^2}\right).$$

*Доказательство.* Разобьем набор БП $x = (x_1,...,x_n)$ на поднаборы $x' = (x_1,...,x_k)$ и $x'' = (x_{k+1},...,x_n)$, где $k$, $1 \leq k \leq n$, – некоторый параметр. Для любого набора $\sigma' = (\sigma_1,...,\sigma_k)$ из $B^k$ положим:

$$f_{\sigma'}(x'') = f(\sigma', x'').$$

Тогда для ФАЛ $f$ будет справедливо представление:

$$f(x',x'') = \bigvee_{\sigma'=(\sigma_1,...,\sigma_k)\in B^k} x_1^{\sigma_1} \cdot ... \cdot x_k^{\sigma_k} \cdot f_{\sigma'}(x'') = \mu_k(x', f_{\tilde{0}}(x''),..., f_{\tilde{1}}(x'')) \qquad (7.1)$$

Построим СФЭ $\Sigma_f$ из универсального многополюсника $\Sigma''$ порядка $(n-k)$ от БП $x''$ и мультиплексора $\Sigma'$ порядка $k$ с адресными БП $x'$, на информационные входы которого подаются выходы $\Sigma''$ в соответствии с (7.1) (см. рис. 7.1).

Если мультиплексор $\Sigma'$ построить по лемме 5.2, а универсальный многополюсник $\Sigma''$ - по теореме 5.4, то

$$L(\Sigma') \le 3 \cdot 2^k + O(k \cdot 2^{k/2}),\ L(\Sigma'') \le 2^{2^{n-k}}.$$

Следовательно, полагая

$$k = ]n - \log(n - 2\log n)[,$$

получим

$$L(\Sigma_f) \le 6 \cdot \frac{2^n}{n - 2\log n} + O(n \cdot 2^{n/2}) + \frac{2^n}{n^2} = 6 \cdot \frac{2^n}{n} + O\left(\frac{2^n \log n}{n^2}\right)$$

*Теорема доказана.*

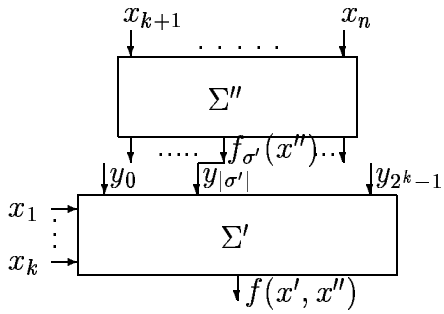



Рис. 7.1

**Следствие.** $L(n) \le 6 \cdot \frac{2^n}{n} + O(\frac{2^n \log n}{n^2})$.

Рассмотрим теперь вопрос о нижних оценках функции Шеннона $L(n)$ и сложности некоторых конкретных ФАЛ.

Пусть $\gamma(L, n)$ - число всех тех попарно неизоморфных неприводимых СФЭ с входными БП $x_1, ..., x_n$ и выходной БП $z_1$, сложность которых не больше, чем $L$.

**Лемма 7.1.** При любых натуральных $L, n$ справедливо неравенство

$$\gamma(L, n) \le (L + n)^{2L+4}$$

*Доказательство.* Пусть $\Sigma$ – неприводимая СФЭ с входными БП $x_1, ..., x_n$ и выходной БП $z_1$, для которой $L(\Sigma) \le L$. Для задания СФЭ $\Sigma$ достаточно:

1) выбрать целые неотрицательные числа $L_1, L_2, L_3$ так, чтобы $L_1 + L_2 + L_3 \le L$, – это можно сделать не более, чем $(L+1)^4$ способами;

2) взять $L_1$ ФЭ $\&$, $L_2$ ФЭ $\vee$ и $L_3$ ФЭ $\neg$, а затем каждый вход каждого из них "присоединить"к выходу некоторого другого ФЭ или к одному из входов $\Sigma$ - это можно сделать не более, чем $(L+n)^{2L}$ способами;

3) поместить единственный сток СФЭ $\Sigma$ к выходной БП $z_1$ .

Следовательно,

$$\gamma(L,n) \le (L+1)^4 \cdot (L+n)^{2L} \le (L+n)^{2L+4}.$$

*Лемма доказана.*

**Лемма 7.2.** При любых натуральных $L, n$ справедливо неравенство:

$$\gamma(L,n) \le (32(L+n))^{L+1}$$

*Доказательство.* Пусть $\Sigma$ - неприводимая СФЭ с входными БП $x_1, ..., x_n$ и выходной БП $z_1$ , для которой $L(\Sigma) = L' \le L$ . Сопоставим СФЭ $\Sigma$ ориентированное корневое упорядоченое помеченное дерево $\mathcal{D}$ , получающееся из графа $\Sigma$ в результате "снятия"входных БП с истоков $\Sigma$ , "отсоединения"от каждой вершины $v$ графа $\Sigma$ , такой, что $d^+(v) > 1$ , каких-либо $(d^+(v) - 1)$ исходящих из нее дуг и объявления начальных вершин этих дуг новыми вершинами-листьями $\mathcal{D}$ (см. рис. 7.2). Заметим, что пометки внутренних вершин дерева $\mathcal{D}$ типами ФЭ базиса $_0$ сохраняются, и что в каждую такую вершину $\mathcal{D}$ с пометкой ФС $\neg$ входит одна дуга, а с пометкой $\&$ или $\vee$ - две дуги.

Заметим также, что для получения СФЭ $\Sigma$ из дерева $\mathcal{D}$ достаточно каждый лист $\mathcal{D}$ присоединить либо к одной из входных вершин СФЭ $\Sigma$ , помеченных БП $x_1, x_2, ..., x_n$ , либо к одной из внутренних вершин самого дерева $\mathcal{D}$ .

Из построения дерева $\mathcal{D}$ следует, что число внутренних вершин (т.е. вершин, отличных от листьев) в нем равно $L'$ , а число ребер не больше, чем $2L'$ , и поэтому число листьев в $\mathcal{D}'$ не больше, чем $L' + 1$ (см. §2). Следовательно, число различных СФЭ $\Sigma$ , связанных с одним и тем же деревом $\mathcal{D}$ , не больше, чем $(L'+n)^{L'+1}$ , а из §2 вытекает, что число различных деревьев $\mathcal{D}$ рассматриваемого вида не больше, чем

$$4^{2L'} \cdot 2^{L'} = 2^{5L'}$$

Следовательно,

$$\gamma(L,n) \le \sum_{L'=1}^{L} (32)^{L'} (L'+n)^{L'+1} \le (32(L+n))^{L+1}$$

*Лемма доказана.*

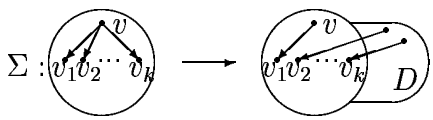



Рис. 7.2

Доказательство двух следующих утверждений основано на т.н. "мощностном"принципе получения нижних оценок функции Шеннона.

**Теорема 7.2.** Для любого натурального $n$ справедливо неравенство

$$L(n) \geq \frac{2^{n-1}}{n}(1 - o(1))$$

*Доказательство.* Из определения функции Шеннона $L(n)$ и величины $\gamma(L, n)$ следует, что

$$\gamma(L(n), n) \geq 2^{2^n}.$$

Логарифмируя это неравенство и применяя лемму 7.1, получим:

$$(2L(n) + 4) \cdot \log(L(n) + n) \geq 2^n,$$

откуда в силу теоремы 7.1 вытекает, что

$$(2L(n) + 4) \cdot (n + o(1)) \geq 2^n.$$

Следовательно,

$$L(n) \geq \frac{2^{n-1}}{n}(1 - o(1))$$

*Лемма доказана.*

**Теорема 7.3.** Для любого натурального $n$ справедливо неравенство:

$$L(n) \geq \frac{2^n}{n}\left(1 + \frac{\log n - 6 - o(1)}{n}\right)$$

*Доказательство.* Рассмотрим множество $\hat{P}_2(n)$ , состоящее из тех ФАЛ $f$ , $f \in P_2(n)$ , для которых

$$L(f) \leq \hat{L}(n) = L'(n) - n, \tag{7.2}$$

где

$$L'(n) = \frac{2^n}{n}\left(1 + \frac{\log n - 6}{n}\right) \tag{7.3}$$

Из (7.2), определения величины $\gamma(L, n)$ и леммы 7.1 следует, что

$$|\hat{P}_2(n)| \leq \gamma(\hat{L}(n), n) \leq (32L'(n))^{L'(n)} \tag{7.4}$$

Логарифмируя (7.4) и используя (7.3), получим:

$$\log|\hat{P}_2(n)| \leq L'(n)(n - \log n + 5 + o(1)) \leq 2^n\left(1 + \frac{\log n - 6}{n}\right)\left(1 - \frac{\log n - 5 - o(1)}{n}\right) \leq$$

$$\leq 2^n\left(1 - \frac{1 - o(1)}{n}\right).$$

Следовательно,

$$2^n - \log|\hat{P}_2(n)| \to \infty \qquad \frac{|\hat{P}_2(n)|}{2^{2^n}} \to 0$$

при $n \to \infty$, а значит, множество $P_2(n) \setminus \hat{P}_2(n)$ не пусто при достаточно больших $n$, и поэтому найдется такая ФАЛ $f$, $f \in P_2(n)$, для которой

$$L(f) > \hat{L}(n) = \frac{2^n}{n}\left(1 + \frac{\log n - 6 - o(1)}{n}\right) \tag{7.5}$$

*Теорема доказана.*

**Следствие.** Неравенство (7.5) выполняется для почти всех ФАЛ $f$ из $P_2(n)$.

Рассмотрим теперь некоторые методы получения нижних оценок сложности конкретных ФАЛ. Соображения, связанные с тем, что сложность СФЭ $\Sigma$, которая реализует систему из $m$ различных ФАЛ, отличных от БП, не может быть меньше, чем $m$, мы уже использовали в теоремах 5.1, 5.3. В случае дешифратора, а также в некоторых подобных случаях эту тривиальную оценку можно несколько уточнить.

**Лемма 7.3.** Сложность схемного дешифратора порядка $n$, $n \geq 2$, не меньше, чем $2^n + \sqrt{2} \cdot 2^{n/2} - n - 1$.

*Доказательство.* Пусть $\Sigma$ – строго приведенный схемный дешифратор порядка $n$, $n \geq 2$, с входными БП $x_1, ..., x_n$. Из строгой приведенности $\Sigma$ следует, что каждый его выходной ФЭ является либо ФЭ $\&$, либо ФЭ $\neg$. Действительно, если бы на выходе ФЭ $\vee$ СФЭ $\Sigma$ реализовалась конъюнкция $K = x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}$, то хотя бы на одном из его входов также реализовалась бы конъюнкция $K$, и в СФЭ $\Sigma$ оказалось бы две различных эквивалентных вершины (см. §4). По этой же причине на входы всех двухвходовых ФЭ СФЭ $\Sigma$ подаются различные ФАЛ. Заметим также, что выход ФЭ $\mathcal{E}'$, который одновременно является выходом $\Sigma$, не может поступать на вход другого ФЭ $\mathcal{E}''$, выход которого также является выходом $\Sigma$, т.к. при этом ФЭ $\mathcal{E}'$ и $\mathcal{E}''$ должны быть ФЭ $\&$ или $\neg$, на выходах которых реализуются разные конъюнкции из $Q_n$, что невозможно. Пусть $a$ – число вершин СФЭ $\Sigma$, отличных от ее выходов. Из указанных особенностей СФЭ $\Sigma$ следует, что

$$2^n \leq \frac{a(a-1)}{2} + a \leq \frac{a(a+1)}{2},$$

и поэтому

$$a \geq \sqrt{2} \cdot 2^{n/2} - 1$$

Таким образом,

$$L(\Sigma) \geq 2^n + a - n \geq 2^n + \sqrt{2} \cdot 2^{n/2} - n - 1.$$

*Лемма доказана.*

**Следствие.** В силу следствия 2 из теоремы 5.1

$$2^n + \sqrt{2} \cdot 2^{n/2} - n - 1 \leq L(Q_n) \leq 2^n + \frac{3}{2}\sqrt{2} \cdot 2^{n/2} + O(n \cdot 2^{n/4}).$$

**Лемма 7.4.** Если СФЭ $\Sigma$ реализует существенную ФАЛ $f(x_1, ..., x_n)$, то $L(\Sigma) \geq n - 1$, а если, кроме того, ФАЛ $f$ немонотонна, то $L(\Sigma) \geq n$.

*Доказательство.* Перейдем от СФЭ $\Sigma$, содержащей $L''$ ФЭ & и $\vee$, к дереву $\mathcal{D}$ так, как это было сделано при доказательстве теоремы 7.1. Заметим, что число БП $f$ не больше, чем число листьев дерева $\mathcal{D}$, которое, в свою очередь, не больше, чем $L'' + 1$. Следовательно,

$$L(\Sigma) \geq L'' \geq n - 1.$$

Если же в СФЭ $\Sigma$ есть хотя бы один ФЭ $\neg$ (в том случае, когда ФАЛ $f$ немонотонна, ФЭ $\neg$ в СФЭ $\Sigma$ обязательно найдется), то

$$L(\Sigma) \geq L'' + 1 \geq n.$$

*Лемма доказана.*

Применяя лемму 7.3 к ФАЛ $f = \overline{x}_1 \vee ... \vee \overline{x}_n$, получим, что $L(f) \geq n$. С другой стороны, ФАЛ $f$ можно реализовать формулой $\overline{x_1 \cdot ... \cdot x_n}$, и поэтому $L(f) \leq n$. Следовательно, формула $\overline{x_1 \cdot ... \cdot x_n}$ является минимальной (в классе СФЭ), и $L(f) = n$.

Будем говорить, что подмножество $U$ множества БП ФАЛ $f$ *забивает* БП $x$, $x \notin U$, ФАЛ $f$, если подстановки некоторых констант вместо БП $U$ из ФАЛ $f$ можно получить ФАЛ, не зависящую существенно от $x$. Множество переменных $X$ ФАЛ $f$ будем называть *незабиваемым*, если любая переменная $x$ из $X$ не забивается множеством $X \setminus \{x\}$. Легко видеть, что при любой подстановке констант вместо некоторых переменных незабиваемого множества $X$ ФАЛ $f$ оставшиеся переменные из $X$ образуют незабиваемое множество переменных для ФАЛ, получающейся в результате этой подстановки. Очевидно также, что все переменные незабиваемого множества $X$ ФАЛ $f$ являются существенными переменными $f$, если $|X| \geq 2$.

**Теорема 7.4.** Если у ФАЛ $f$ есть незабиваемое подмножество из $n$ переменных, то

$$L(f) \geq 2(n - 1)$$

*Доказательство.* При $n = 1$ оценка теоремы, очевидно, верна. Предположив, что эта оценка верна для любой ФАЛ $f$ и любого $n \leq (l - 1)$, где $l \geq 2$, докажем ее справедливость для произвольной ФАЛ $h$, которая имеет незабиваемое подмножество, составленное из существенных переменных $x_1, ..., x_l$ ФАЛ $h$. Пусть $\Sigma$ – минимальная СФЭ, реализующая ФАЛ $h$ со сложностью $L(h)$. Рассмотрим вершину $v$ СФЭ $\Sigma$, в которую ведет дуга

из входной вершины $x_1$, и которой приписана ФАЛ $\varphi$ базиса $_0$. Пусть $\sigma = 0$, если $\varphi = u_1 \cdot u_2$, и $\sigma = 1$ в остальных случаях. Вершина $v$ не может быть выходом $\Sigma$, так как иначе при $x_1 = \sigma$ на выходе $\Sigma$ появлялась бы константа и переменная $x_1$ забивала бы, тем самым, переменные $x_2, ..., x_l$ ФАЛ $h$. Следовательно, найдется вершина $w$ СФЭ $\Sigma$, в которую ведет дуга из вершины $v$. Пусть $\Sigma'$ – СФЭ, получающаяся из СФЭ $\Sigma$ в результате подстановки константы [3] $\sigma$ вместо переменной $x_1$. Схема $\Sigma'$ реализует некоторую ФАЛ $f'$ с незабиваемым множеством из переменных $x_2, ..., x_l$ и не содержит вершин $v$, $w$, то есть имеет сложность не более, чем $L(\Sigma) - 2$. В силу индуктивного предположения $L(f') \geq 2(l-2)$, и поэтому

$$L(h) = L(\Sigma) \geq L(\Sigma') + 2 \geq L(f') + 2 \geq 2(l-1).$$

*Теорема доказана.*

**Следствие.** $L(\mu_n) = 2 \cdot 2^n + O(2^{n/2})$.

Действительно, требуемая верхняя оценка для $L(\mu_n)$ вытекает из теоремы 5.2 (см. следствие), а так как БП $y_0, ..., y_{2^n-1}$ образуют незабиваемое множество БП $\mu_n$, то теорема 7.3 дает необходимую нижнюю оценку.

Рассмотрим, в заключение, вопрос о сложности реализации симметрических ФАЛ.

Функция $f(x_1, ..., x_n)$ называется *симметрической*, если ее значение не меняется при любой перестановке аргументов. Значение симметрической ФАЛ однозначно определяется числом единиц в наборе значений ее переменных, так как два набора с одинаковым числом единиц всегда можно получить друг из друга некоторой перестановкой аргументов. Заметим, что любая отличная от константы симметрическая ФАЛ $f(x_1, ..., x_n)$ является существенной ФАЛ, и поэтому $L(f) \geq n-1$ согласно лемме 7.3.

**Теорема 7.5.** Любую симметрическую ФАЛ от $n$ переменных можно реализовать со сложностью $9n + O\left(\frac{n}{\log n}\right)$.

*Доказательство.* Пусть $f(x_1, ..., x_n)$ – симметрическая ФАЛ, $k = ]\log_2(n+1)[$, а ФАЛ $g(y_1, ..., y_k)$ на наборе $\tilde{\alpha} = (\alpha_1, ..., \alpha_k)$, где $|\tilde{\alpha}| \leq n$, равна значению ФАЛ $f$ на наборах с $|\tilde{\alpha}|$ единицами и принимает произвольные значения на остальных наборах. Пусть $\Sigma'$ – счетчик с входными переменными $x_1, ..., x_n$ (см. замечание к теореме 6.3) сложности не более, чем $9(n + k^2)$, а $\Sigma''$ – СФЭ, реализующая ФАЛ $g$ и имеющая сложность не более, чем $6(1+o(1))\frac{2^k}{k}$ (см. теорему 7.1). Схема $\Sigma_f$, которая получается присоединением выходов СФЭ $\Sigma'$ к входам СФЭ $\Sigma''$, реализует, очевидно, ФАЛ $f$, и

$$L(\Sigma_f) = L(\Sigma') + L(\Sigma'') \leq 9n + O\left(\frac{2^k}{k}\right) = 9n + O\left(\frac{n}{\log n}\right)$$

[3] Подстановка констант вместо некоторых входных переменных СФЭ подразумевает, что "константные"входы схемы, а также те элементы, на входах которых появляются константы, последовательно устраняются применением тождеств $\bar{0} = 1$, $\bar{1} = 0$, $x \cdot 0 = 0$, $x \vee 1 = 1$, $x \cdot 1 = x \vee 0 = x$ до тех пор, пока это возможно.

*Теорема доказана.*

# Список литературы


[1] Алексеев В.Б., Ложкин С.А. Элементы теории графов и схем. М., Изд-во МГУ, 1991. – 40 с.

[2] Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука. Гл. ред. физ.-мат. лит., 1977. – 368 с.

[3] Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. М.: Наука. Гл. ред. физ.-мат. лит., 1990. – 384 с.

[4] Карацуба

[5] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. М.: Наука. Гл. ред. физ.-мат. лит., 1985. – 320 с.

[6] Лупанов О.Б. Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984. – 137 с.

[7] Потемкин И.С. Функциональные узлы цифровой автоматики. М.: Энергоатомиздат, 1988. – 320 с.

[8] Яблонский С.В. Введение в дискретную математику. – 2-е изд. – М.: Наука. Гл. ред. физ.-мат. лит., 1986. – 384 с.

[9] Яблонский С.В. Эквивалентные преобразования управляющих систем. М., Изд-во МГУ, 1986. – 40 с.

Рассмотрим теперь сложность умножителя $M_n$ для умножения двух неотрицательных n-разрядных двоичных чисел $X = |(x_1, x_2, \ldots, x_n)|$ и $Y = |(y_1, y_2, \ldots, y_n)|$. Так как $X < 2^n$ и $Y < 2^n$, то $XY < 2^{2n}$ и для представления результата требуется не более 2n выходов. Обозначим через $L_M(n)$ наименьшее возможное число элементов в умножителе $M_n$. Очевидно, что $L_M(1) = 1$, так как умножение 1-разрядных чисел осуществляет элемент конъюнкция.

**Утверждение.** Существует СФЭ для умножения $n$-разрядного числа $X$ на 1-разрядное число $y$ с числом элементов $n$.

Действительно, если $X = |(x_1, x_2, \ldots, x_n)|$ и $Xy = Z = |(z_1, z_2, \ldots, z_n)|$, то $z_i{=}x_i y$ для всех $i = 1, 2, \ldots, n$.

При умножении двух $n$-разрядных чисел $X$ и $Y$ "в столбик"надо $n$ раз умножить $X$ на 1-разрядное число (всего $n^2$ конъюнкций) и затем $n-1$ раз сложить числа длиной не более 2n. Такой алгоритм (схема) имеет сложность по порядку $n^2$. Следующая теорема показывает, что алгоритм умножения "в столбик"не оптимален по порядку.

**Теорема 6.4** (Карацуба А.А.). Существует такая константа $c$, что для всех $n$ $L_M(n) \leq cn^{\log_2 3}$.

Докажем сначала несколько вспомогательных лемм.

**Лемма 6.1**. Существует константа $c_1$ такая, что $L_M(n{+}1) \leq L_M(n){+}$ $c_1 n$ для всех $n$.

**Доказательство**. Пусть требуется перемножить два $(n{+}1)$-разрядных числа $X_1 = |(x_0, x_1, \ldots, x_n)|$ и $Y_1 = |(y_0, y_1, \ldots, y_n)|$. Тогда обозначим $|(x_1, x_2, \ldots, x_n)| = X$ и $|(y_1, y_2, \ldots, y_n)| = Y$. При этом $X_1 = x_0 2^n + X$, $Y_1 = y_0 2^n + Y$ и

$$X_1 Y_1 = x_0 y_0 2^{2n} + (x_0 Y + y_0 X)2^n + XY.$$

Поэтому для вычисления $X_1 Y_1$ достаточно использовать умножитель $M_n$ для вычисления $XY$, $2n$ элементов для вычисления $x_0 Y$ и $y_0 X$, 1 элемент для вычисления $x_0 y_0$ и 3 сумматора порядка не более $2n + 2$, так как $X_1 Y_1 < 2^{2n+2}$. Отметим, что числа $x_0 y_0$ и $x_0 Y + y_0 X$ надо подавать на сумматоры со сдвигом, одновременно подавая на младшие разряды 0. При этом 0 можно предварительно получить подсхемой с 2 элементами, реализующей $x_0 \bar{x}_0 = 0$.Так как сложность каждого сумматора можно сделать не более $9(2n + 2)$, а сложность $M_n$ равной $L_M(n)$, то сложность полученной схемы будет не больше чем $L_M(n) + c_1 n$ для некоторой константы $c_1$. Лемма доказана.

**Лемма 6.2**(основная). Существует константа $c_2$ такая, что $L_M(2n) \leq$ $3L_M(n) + c_2 n$, для всех $n$.

**Доказательство**. Пусть нужно перемножить два $2n$-разрядных числа $X$ и $Y$. Разобьем их на части, содержащие по $n$ разрядов. Тогда по-

лучим $X = X_1 2^n + X_2$, $Y = Y_1 2^n + Y_2$. Отсюда

$$XY = X_1 Y_1 2^{2n} + (X_1 Y_2 + X_2 Y_1) 2^n + X_2 Y_2 =$$

$$= X_1 Y_1 2^{2n} + [(X_1 + X_2)(Y_1 + Y_2) - X_1 Y_1 - X_2 Y_2] 2^n + X_2 Y_2.$$

Так как $X_1 Y_2 + X_2 Y_1 \geq 0$, то при вычитании в квадратной скобке не возникает отрицательных чисел. Таким образом, схему для умножения $XY$ можно построить, используя 2 оптимальных умножителя $M_n$ с числом элементов $L_M(n)$ в каждом для вычисления $X_1 Y_1$ и $X_2 Y_2$, умножитель $M_{n+1}$ с числом элементов $L_M(n+1)$ для вычисления $(X_1 + X_2)(Y_1 + Y_2)$, 4 сумматора порядка не более $4n$ (так как $XY < 2^{4n}$) и 2 вычитателя порядка $2n + 2$. В некоторых сумматорах опять на младшие разряды надо подавать 0, который реализуем подсхемой с 2 элементами: $0 = x\bar{x}$, где $x$ - любая входная переменная. Для построенной схемы $M_{2n}$ с учетом леммы 6.1 получим для некоторых констант $c$ и $c_2$:

$$L(M_{2n}) \leq 2L_M(n) + L_M(n+1) + cn \leq 3L_M(n) + c_1 n + cn = 3L_M(n) + c_2 n$$

.

**Лемма 6.3**. Существует такая константа $c_3$, что для любого натурального $k$ выполняется $L_M(2^k) \leq c_3 3^k$.

**Доказательство**. Положим $f(k) = \frac{L_M(2^k)}{3^k}$. Тогда из предыдущей леммы имеем

$$\frac{L_M(2^k)}{3^k} \leq \frac{L_M(2^{k-1})}{3^{k-1}} + \frac{c_2}{3}(\frac{2}{3})^{k-1}$$

и

$$f(k) \leq f(k-1) + \frac{c_2}{3}(\frac{2}{3})^{k-1} \leq f(k-2) + \frac{c_2}{3}(\frac{2}{3})^{k-2} + \frac{c_2}{3}(\frac{2}{3})^{k-1} \leq$$

$$\leq \cdots \leq f(1) + \frac{c_2}{3}[\frac{2}{3} + (\frac{2}{3})^2 + \cdots + (\frac{2}{3})^{k-1}] \leq c_3$$

для некоторой константы $c_3$, поскольку сумма в квадратных скобках не превосходит сумму 2 бесконечно убывающей геометрической прогрессии с первым членом $\frac{2}{3}$ и знаменателем $\frac{2}{3}$. Таким образом $\frac{L_M(2^k)}{3^k} \leq c_3$ и $L_M(2^k) \leq c_3 3^k$.

**Доказательство теоремы Карацубы**. Пусть $n$ - любое натуральное число и $n > 1$. Тогда существует натуральное $k$ такое, что $2^{k-1} < n \leq 2^k$. Для умножения $n$-разрядных чисел будем использовать схему $M_{2^k}$ с числом элементов $L_M(2^k)$, подавая на старшие $2^k - n$ входных разрядов обоих сомножителей 0, предварительно реализованный подсхемой из 2 элементов. Тогда имеем

$$L_M(n) \leq L_M(2^k) + 2 \leq c_3 3^k + 2 = 3c_3 3^{k-1} + 2 =$$

$$= 3c_3 2^{(k-1)\log_2 3} + 2 < 3c_3 n^{\log_2 3} + 2 \leq cn^{\log_2 3}$$

для некоторой константы $c$.

В заключение отметим, что существует алгоритм Шенхаге и Штрассена для умножения двух $n$-разрядных чисел, дающий оценку $L_M(n) \leq cn \log n \log\log n$, где $c$ - некоторая константа и логарифмы можно считать двоичными.

Часть 3. Автоматы.

## 8. Автоматные функции. Их реализация схемами из функциональных элементов и элементов задержки.

В данном параграфе рассматриваются некоторые вопросы, связанные с автоматами и осуществляемыми ими отображениями. Подробное изложение теории автоматов можно найти в (?) . В (?) рассматриваются автоматные отображенияия и операции над ними. Здесь мы рассмотрим связь между автоматными отображениями и схемами из функциональных элементов и элементов задержки.

**Определение**. *Инициальным автоматом* называется любая шестерка $(A, B, Q, G, F, q_0)$, где $A$, $B$, $Q$ - произвольные множества, $G$ — функция, отображающая пары из декартова произведения $A \times Q$ в $Q$, $F$ — функция, отображающая пары из $A \times Q$ в $B$, и $q_0 \in Q$. Множества $A$, $B$, $Q$ называются, соответственно, *входным алфавитом*, *выходным алфавитом* и *алфавитом* (*множеством*) *состояний*. Функция $G$ называется *функцией переходов*, функция $F$ — *функцией выхода*, $q_0$ называется *начальным состоянием*.

Определим *функционирование* автомата. Будем рассматривать параметр $t$, принимающий значения $0, 1, 2, \ldots$ , который можно интерпретировать как дискретное время. Будем считать, что на вход автомата может поступить любая последовательность $a(1), a(2), a(3), \ldots$ (конечная или бесконечная), где $a(t) \in A$ для всех $t$. Введем переменные $q(t)$, $t = 0, 1, \ldots$ и $z(t)$, $t = 1, 2, \ldots$, которые будем называть *состоянием автомата в момент* $t$ и *выходным значением в момент* $t$. Пусть $x(t)$ — значение входа в момент $t$. Тогда определим $z(t)$ и $q(t)$ равенствами

$$\begin{cases} z(t) &= F(x(t), q(t-1)) \\ q(t) &= G(x(t), q(t-1)) \\ q(0) &= q_0 \end{cases} \tag{8.1}$$

Эти равенства называются каноническими уравнениями автомата. Легко видеть, что из канонических уравнений по $x(1)$ и $q(0) = q_0$ однозначно определяются $z(1)$ и $q(1)$. Затем по $q(1)$ и $x(2)$ однозначно определяются $z(2)$ и $q(2)$ и т.д. В результате по входной последовательности $x(1), x(2), \ldots, x(n)$ однозначно определяется выходная последовательность $z(1), z(2), \ldots, z(n)$, то есть автомат осуществляет отображение последовательностей любой длины (конечной или бесконечной) с элементами из $A$ в последовательности той же длины с элементами из $B$.

**Определение**. Пусть $A$ и $B$ — два множества. Отображение последовательностей с элементами из $A$ в последовательности с элементами из $B$ называется *автоматной функцией*, если существует инициальный автомат, осуществляющий это отображение.

**Пример**. Пусть $A = B = Q = \{0, 1\}$ и автомат описывается следующими каноническими уравнениями

$$\begin{cases} z(t) &= q(t-1) \\ q(t) &= x(t) \\ q(0) &= 0. \end{cases} \tag{8.2}$$

Легко видеть, что входная последовательность $a(1), a(2), a(3), \ldots$ отображается таким автоматом в последовательность $0, a(1), a(2), \ldots$. Этот автомат называется *единичной задержкой*.

Автоматы удобно задавать геометрически с помощью ориентированных графов. При этом каждому состоянию из множества $Q$ сопоставляется вершина орграфа, и каждой паре $(a, q)$, где $a \in A$, $q \in Q$ сопоставляется дуга, идущая из вершины, соответствующей $q$, в вершину, соответствующую $G(a, q)$. Этой дуге приписывается пометка $(a, F(a, q))$. Вершина, соответствующая начальному состоянию $q_0$, помечается (мы будем помечать ее звездочкой). Описанный граф с пометками называется диаграммой Мура заданного автомата. Например, на рис. 8.1 представлена диаграмма Мура для задержки.

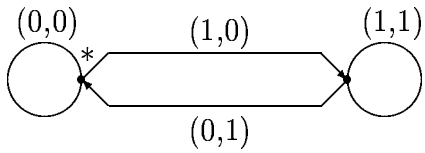



Рис. 8.1

Легко видеть, что диаграмма Мура однозначно задает автомат. По дугам и пометкам на дугах однозначно определяются функции переходов и выхода.

Рассмотрим теперь класс схем, с помощью которых можно реализовать автоматные функции.

**Определение**. Пусть задан базис Б=$\{\mathcal{E}_1, \ldots, \mathcal{E}_s, R\}$, где $\mathcal{E}_1, \ldots, \mathcal{E}_s$ — функциональные элементы (см. параграф 4), а R — элемент единичной задержки, имеющий один вход и один выход. Схемой из функциональных элементов и элементов задержки (СФЭЗ) в базисе Б называется граф, который удовлетворяет пунктам 1)-3) определения СФЭ (см. стр. ?) и в котором любой ориентированный цикл проходит хотя бы через одну вершину, соответствующую элементу задержки.

Будем считать, что все переменные СФЭЗ принимают значения из множества $\{0,1\}$ и могут менять их в моменты времени $t = 1, 2, \ldots$. При этом функционирование элемента $R$ описывается уравнениями (8.2), а функционирование ФЭ $\mathcal{E}_i$, имеющего $k_i$ входов, по-прежнему описывается ФАЛ $\varphi_i(u_1, \ldots, u_{k_i}), i = 1, \ldots, s$. Для описания функционирования СФЭЗ с $r$ элементами задержки $R$ поступим следующим образом.

Пусть $i$-я задержка $R_i$, $i = 1, \ldots, r$, приписана вершине $v_i$, в которую идет дуга из вершины $w_i$. Для всех $i = 1, \ldots, r$ удалим из СФЭЗ дуги $(w_i, v_i)$. По определению СФЭЗ в полученном после этого графе не будет ориентированных циклов и он, тем самым, будет представлять собой СФЭ. Входами этой СФЭ будут все входы исходной схемы, а также все вершины $v_i$, $i = 1, \ldots, r$ (заметим, что все они различны и отличны от входов исходной схемы). Выходами полученной СФЭ объявим все выходы исходной схемы и вершины $w_i$, $i = 1, \ldots, r$. Пусть в исходной схеме выходам приписаны переменные $z_1, \ldots, z_m$, входам — переменные $x_1, \ldots, x_n$. Вершинам $v_i$ припишем переменные $q'_1, \ldots, q'_r$, а вершинам $w_i$ — переменные $q_1, \ldots, q_r$. В соответствии с определением функционирования СФЭ, для некоторых ФАЛ $f_i$, $g_j$ справедливо:

$$\begin{cases} z_i &= f_i(x_1, \ldots, x_n, q'_1, \ldots, q'_r), i = 1, \ldots, m \\ q_j &= g_j(x_1, \ldots, x_n, q'_1, \ldots, q'_r), j = 1, \ldots, r. \end{cases} \tag{8.3}$$

Естественно считать, что равенства (8.3) выполняются в каждый момент времени $t = 1, 2, 3, \ldots$, то есть

$$\begin{cases} z_i(t) &= f_i(x_1(t), \ldots, x_n(t), q'_1(t), \ldots, q'_r(t)), i = 1, \ldots, m \\ q_j(t) &= g_j(x_1(t), \ldots, x_n(t), q'_1(t), \ldots, q'_r(t)), j = 1, \ldots, r. \end{cases} \tag{8.4}$$

Так как, в соответствии с каноническими уравнениями (8.2), выход элемента задержки в момент $t$ совпадает с его входом в момент $t-1$, то естественно считать, что в исходной схеме $q'_i(t) = q_i(t-1)$ при $t = 1, 2, \ldots$ для всех $i = 1, \ldots, r$, где $q_i(0) = 0$. Тогда равенства (8.4) принимают вид (где $i = 1, \ldots, m$ и $j = 1, \ldots, r$):

$$\begin{cases} z_i(t) &= f_i(x_1(t), \ldots, x_n(t), q_1(t-1), \ldots, q_r(t-1)), \\ q_j(t) &= g_j(x_1(t), \ldots, x_n(t), q_1(t-1), \ldots, q_r(t-1)), \\ q_j(0) &= 0. \end{cases} \tag{8.5}$$

Полученные равенства определяют функционирование СФЭЗ и называются ее каноническими уравнениями.

Пример. СФЭ $\Sigma'$ на рис. 4.4б является ячейкой сумматора и реализует ФАЛ $z_1 = xy \vee xq' \vee yq'$, $z_2 = x \oplus y \oplus q'$. Тогда схема на рис. 8.2 будет

иметь канонические уравнения

$$\begin{cases} z(t) &= x(t) \oplus y(t) \oplus q(t-1) \\ q(t) &= x(t)\&y(t) \vee x(t)\&q(t-1) \vee y(t)\&q(t-1) \\ q(0) &= 0. \end{cases}$$

Если на входы $x$ и $y$ этой СФЭЗ подавать два двоичных числа по одному разряду в каждый момент времени, начиная с младших разрядов, то на выходе схемы будет выдаваться сумма этих чисел, начиная с младших разрядов. Эта схема называется *последовательным сумматором.*

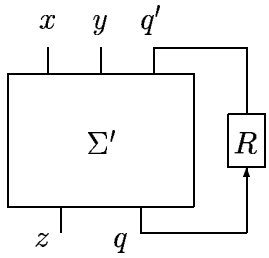



Рис. 8.2

Пусть $E_2^n$ — множество всех наборов длины $n$ с элементами 0 и 1. Если задана последовательность наборов из $E_2^n$ в качестве значений входных переменных $x_i(t)$, $i = 1, \ldots, n$, $t = 1, 2, \ldots$, то согласно (8.5) по ним однозначно определяется последовательность наборов длины $m$ $z_1(t), \ldots, z_m(t)$ для $t = 1, 2, \ldots$. Таким образом, схема осуществляет преобразование последовательностей с элементами из $E_2^n$ в последовательности с элементами из $E_2^m$.

**Определение**. Пусть автоматная функция $\varphi$ отображает последовательности в конечном алфавите $A$ в последовательности в конечном алфавите $B$. Пусть СФЭЗ $\Sigma$ осуществляет преобразование $\psi$ последовательностей с элементами из $E_2^n$ в последовательности с элементами из $E_2^m$. Будем говорить, что $\Sigma$ *моделирует* $\varphi$, если существуют отображения (*кодирования*) $K_1 : A \to E_2^n$ и $K_2 : B \to E_2^m$, сопоставляющие разным элементам разные элементы и обладающие свойством: для любой последовательности $T = a(1)a(2)\ldots a(t)$ в алфавите $A$, если $\varphi(P) = R = b(1)b(2)\ldots b(t)$, то $\psi(K_1(P)) = K_2(T)$, где

$$K_1(P) = K_1(a(1))K_1(a(2))\ldots K_1(a(t)),$$

$$K_2(T) = K_2(b(1))K_2(b(2))\ldots K_2(b(t)).$$

**Теорема 8.1**. 1) Отображение, осуществляемое любой СФЭЗ, является автоматной функцией. 2) Для любой автоматной функции существует моделирующая ее СФЭЗ в базисе из функциональных элементов дизъюнкции, конъюнкции, отрицания и элемента задержки.

Доказательство. 1) Пусть отображение $\psi$, осуществляемое схемой $\Sigma$, задается каноническими уравнениями (8.5). Введем переменные $X = (x_1, \ldots, x_n)$, $Q = (q_1, \ldots, q_r)$, $Z = (z_1, \ldots, z_m)$, принимающие значения, соответственно в $E_2^n$, $E_2^r$, $E_2^m$. Положим $q_0 = (0, \ldots, 0)$. Тогда (8.5) можно переписать в виде

$$\begin{cases} Z(t) &= F(X(t), Q(t-1)) \\ Q(t) &= G(X(t), Q(t-1)) \\ Q(0) &= q_0, \end{cases}$$

где функции $F$, $G$ не зависят явно от $t$. Отсюда видно, что отображение, осуществляемое схемой, совпадает с отображением, задаваемым автоматом $(E_2^n, E_2^m, E_2^r, G, F, q_0)$, то есть является автоматной функцией.

2) Пусть автоматная функция дана автоматом $D = (A, B, Q, G, F, q_0)$. Выберем $n$, $m$, $r$ так, что $2^n \geq |A|$, $2^m \geq |B|$, $2^r \geq |Q|$. Рассмотрим произвольные отображения (кодирования) $K_1 : A \to E_2^n$, $K_2 : B \to E_2^m$, $K_3 : Q \to E_2^r$, при которых разные элементы отображаются в разные элементы. Дополнительно потребуем, чтобы $K_3(q_0) = (0, \ldots, 0)$. Рассмотрим отображения $G' : E_2^n \times E_2^r \to E_2^r$ и $F' : E_2^n \times E_2^r \to E_2^m$ такие, что для любых $a \in A$ и $q \in Q$ выполняется

$$\begin{cases} G'(K_1(a), K_3(q)) &= K_3(G(a, q)) \\ F'(K_1(a), K_3(q)) &= K_2(F(a, q)). \end{cases} \tag{8.6}$$

Равенства (8.1) определяют отображения $G'$ и $F'$ только для пар $\tilde{\alpha} \in E_2^n$, $\tilde{\beta} \in E_2^r$ таких, что $\alpha$ является кодом некоторой буквы из $A$, а $\beta$ является кодом некоторой буквы из $B$. Для остальных пар отображения $G'$ и $F'$ доопределим произвольно. Пусть $\tilde{0} = (0, \ldots, 0)$. Рассмотрим автомат $H = (E_2^n, E_2^m, E_2^r, G', F', \tilde{0})$ с каноническими уравнениями

$$\begin{cases} Z(t) &= F'(X(t), Q(t-1)) \\ Q(t) &= G'(X(t), Q(t-1)) \\ Q(0) &= \tilde{0} \end{cases} \tag{8.7}$$

Из (8.6) вытекает, что если автомат $D$ преобразует последовательность $P$ в алфавите $A$ в последовательность $T$ в алфавите $B$, то $H$ преобразует код $K_1(P)$ последовательности $P$ в код $K_2(T)$ последовательности $T$. Таким образом, достаточно показать, что автоматную функцию, задаваемую равенствами (8.7), можно реализовать схемой. Так как значением переменной $X$ являются наборы длины $n$ из $E_2^n$, то ее можно рассматривать как набор переменных $(x_1, \ldots, x_n)$, принимающих значения из $E_2$. Аналогично для переменных $Q$ и $Z$. Тогда (8.7) можно переписать в виде

(8.4) для некоторых ФАЛ $f_i$, $g_j$. По теореме 4.2 можно построить СФЭ в базисе {дизъюнкция, конъюнкция, отрицание} с $n+r$ входами и $m+r$ выходами, реализующую семейство функций

$$\begin{cases} z_i &= f_i(x_1, \ldots, x_n, q'_1, \ldots, q'_r), i = 1, \ldots, m \\ q_j &= g_j(x_1, \ldots, x_n, q'_1, \ldots, q'_r), j = 1, \ldots, r. \end{cases}$$

Пусть в этой СФЭ входная переменная $q'_j$ приписана вершине $v_j$, а выходная переменная $q_j$ — вершине $w_j$. Добавим дугу $(w_j, v_j)$ и сопоставим вершине $v_j$ элемент задержки. Проделав это для всех пар $q_j$, $q'_j$ $(j = 1, \ldots, r)$ получим СФЭЗ, функционирование которой описывается каноническими уравнениями (8.5). Эта схема является искомой. Теорема доказана.

**Пример** (*ячейка памяти*). Пусть требуется построить СФЭЗ для автомата с двумя входами, в котором выход в момент времени $t$ всегда совпадает с состоянием в момент $t-1$, а состояние остается неизменным, если $x_2 = 0$ (ячейка закрыта для записи), и состояние становится равным $x_1$, если $x_2 = 0$ (ячейка открыта для записи). Канонические уравнения такого автомата имеют вид

$$\begin{cases} z(t) &= q(t-1) \\ q(t) &= x_1(t)x_2(t) \vee q(t-1)\bar{x}_2(t) \\ q(0) &= 0. \end{cases}$$

На рис. 8.3 приведена СФЭЗ, реализующая ячейку памяти.

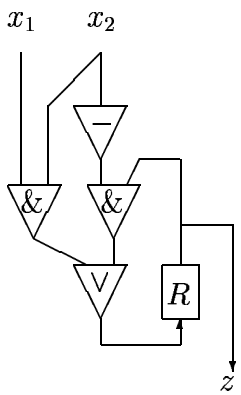



Рис. 8.3

Для получения памяти из $2^n$ ячеек с записью одного бита по адресу достаточно взять $2^n$ ячеек памяти, их входы $x_2$ присоединить к различным выходам дешифратора порядка $n$, а все входы $x_1$ присоединить к единому входу, на который поступает записываемый бит. Чтобы дополнительно

обеспечить считывание по адресу достаточно выходы всех ячеек подать на различные информационные входы мультиплексора порядка $n$.

## 9. Эксперименты с автоматами. Теорема Мура.

Будем теперь рассматривать автоматы, в которых не выделено начальное состояние, то есть автомат задается пятеркой $(A, B, Q, G, F)$.

Через $A^*$ будем обозначать множество всех конечных слов в алфавите $A$. Расширим функции $F$ и $G$, определив $F(\bar{a}, q_i)$ и $G(\bar{a}, q_i)$ для любого состояния $q_i \in Q$ и любого слова $\bar{a} = (a(1), a(2), \ldots, a(m)) \in A^*$. Пусть автомат $(A, B, Q, G, F)$ находится в состоянии $q_i \in Q$ и на вход подается слово $\bar{a} = (a(1), a(2), \ldots, a(m))$. Тогда на выходе будет последовательно выдаваться некоторое слово $\bar{b} = (b(1), b(2), \ldots, b(m))$ и после подачи всего слова $\bar{a}$ автомат окажется в некотором состоянии $q_k$. Расширим функции $F$ и $G$, положив $F(\bar{a}, q_i) = \bar{b}$, $G(\bar{a}, q_i) = q_k$.

**Определение.** Два состояния $q_i$ и $q_j$ автомата $(A, B, Q, G, F)$ называются отличимыми, если существует входное слово $\bar{a} \in A^*$ такое, что $F(\bar{a}, q_i) \neq F(\bar{a}, q_j)$. При этом слово $\bar{a}$ называют экспериментом, отличающим $q_i$ и $q_j$, а длину $l(\bar{a})$ - длиной этого эксперимента.

**Теорема 9.1**(Мур). Если в автомате $(A, B, Q, G, F)$ состояния $q_i$ и $q_j$ отличимы и $|Q| = r$, то существует эксперимент $\bar{a}$, отличающий $q_i$ и $q_j$, длины $l(\bar{a}) \leq r - 1$.

**Лемма 9.1.** Пусть в автомате $(A, B, Q, G, F)$ есть 2 состояния $q_u$ и $q_v$, отличимые экспериментом длины $p$ и не отличимые более коротким экспериментом, тогда для любого $k$, где $1 \leq k \leq p$, существуют 2 состояния, отличимые экспериментом длины $k$ и не отличимые более коротким экспериментом.

bf Доказательство. Пусть состояния $q_u$,$q_v$ отличимы экспериментом $\bar{a}$ длины $p$ и не отличимы экспериментом меньшей длины. Пусть $F(\bar{a}, q_u) = \bar{b}$, $F(\bar{a}, q_v) = \bar{c}$. Тогда, $\bar{b} \neq \bar{c}$, причем $\bar{b}$ и $\bar{c}$ различаются только последней буквой. Разобьем все слова $\bar{a}$, $\bar{b}$, $\bar{c}$ на 2 подслова $\bar{a} = \bar{a}_1\bar{a}_2$, $\bar{b} = \bar{b}_1\bar{b}_2$, $\bar{c} = \bar{c}_1\bar{c}_2$, где $l(\bar{a}_2) = l(\bar{b}_2) = l(\bar{c}_2) = k$. Пусть $G(\bar{a}_1, q_u) = q'$, $G(\bar{a}_1, q_v) = q''$. Тогда $F(\bar{a}_2, q') = \bar{b}_2$, $f(\bar{a}_2, q'') = \bar{c}_2$. Так как $\bar{b}_2$ и $\bar{c}_2$ различаются последней буквой, то $q'$ и $q''$ отличимы экспериментом длины $l(\bar{a}_2) = k$. Допустим, что $q'$ и $q''$ отличимы экспериментом $\bar{a}_3$ длины $l(\bar{a}_3) < k$. Тогда $F(\bar{a}_3, q') = \bar{b}_3$, $F(\bar{a}_3, q'') = \bar{c}_3$ и $\bar{b}_3 \neq \bar{c}_3$. Но тогда $F(\bar{a}_1\bar{a}_3, q_u) = \bar{b}_1\bar{b}_3$, $F(\bar{a}_1\bar{a}_3, q_v) = \bar{c}_1\bar{c}_3$ и $\bar{b}_1\bar{b}_3 \neq \bar{c}_1\bar{c}_3$. Следовательно, $q_u$ и $q_v$ отличимы экспериментом $\bar{a}_1\bar{a}_3$ длины $l(\bar{a}_1\bar{a}_3) = l(\bar{a}_1) + l(\bar{a}_3) < (p-k)+k = p$. Это противоречит условию. Значит (от противного) $q'$ и $q''$ не отличимы экспериментом длины меньшей, чем $k$. Лемма доказана.

**Доказательство теоремы Мура**. Пусть состояния $q_i$ и $q_j$ отличимы экспериментом длины $p$ и не отличимы более коротким экспериментом. Рассмотрим в данном автомате следующее отношение $R_m$ на множестве состояний $Q$ ($m$=0,1,...,$p$): состояния $q_i$ и $q_j$ не отличимы экспериментом длины $m$ (считаем, что любые 2 состояния не отличимы экспериментом длины 0). Если для любого слова $\bar{a} \in A^*$ длины $m$ $F(\bar{a}, q_i) = F(\bar{a}, q_j)$ и $F(\bar{a}, q_j) = F(\bar{a}, q_k)$, то $F(\bar{a}, q_i) = F(\bar{a}, q_k)$, поэтому $R_m$ — это отношение эквивалентности для каждого $m = 0, 1, 2, \ldots, p$. Относительно $R_m$ $Q$ разбивается на классы эквивалентности $Q_1^{(m)}$, $Q_2^{(m)}$,..., $Q_{s(m)}^{(m)}$, так что любые два состояния из одного класса не отличимы экспериментом длины $m$, а любые два состояния из разных классов отличимы экспериментом длины $m$. При этом $s(0) = 1$ и $Q = Q_1^{(0)}$. Посмотрим как меняются эти классы при переходе от $m$ к $m + 1$. Если 2 состояния отличимы экспериментом длины $m$, то они отличимы и экспериментом длины $m + 1$, поэтому эксперименты из разных классов остаются в разных классах. По лемме 9.1 для любого $m = 0, 1, \ldots, p - 1$ существуют 2 состояния, отличимые экспериментом длины $m + 1$ и не отличимые экспериментом длины $m$. Следовательно, хотя бы один из классов эквивалентности относительно $R_m$ распадается не менее чем на 2 класса эквивалентности относительно $R_{m+1}$. Отсюда $1 = s(0) < s(1) < s(2) < \cdots < s(p-1) < s(p) \leq r$. Так как все $s(i)$ - натуральные числа, то $p \leq r - 1$. Теорема доказана.

Пример автомата на рис. 9.1 показывает, что оценку $r - 1$ в теореме Мура в общем случае улучшить нельзя. Здесь, независимо от входного символа $a$ $G(a, q_i) = 0$, для $i = 2, 3, \ldots, r$ и $G(a, q_1) = 1$.

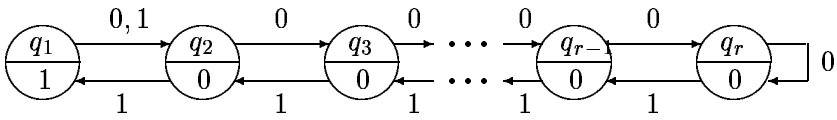



Рис. 9.1

Для того, чтобы отличить состояния $q_{r-1}$ и $q_r$ надо перевести хотя бы одно из них в $q_1$ (входным словом длины $r - 2$) и затем подать еще один входной символ. Следовательно, минимальная длина эксперимента, отличающего $q_{r-1}$ и $q_r$, равна $r - 1$.

**Определение.** Пусть 2 автомата $(A, B, Q_1, G_1, F_1)$ и $(A, B, Q_2, G_2, F_2)$ имеют одинаковые входной и выходной алфавиты. Пусть $q_i \in Q_1$ и $q_j \in Q_2$. Будем говорить, что эксперимент $\bar{a} \in A^*$ отличает состояния $q_i$ и $q_j$, если $F_1(\bar{a}, q_i) \neq F_2(\bar{a}, q_j)$.

**Теорема 9.2.** Пусть даны 2 автомата $(A, B, Q_1, G_1, F_1)$, $(A, B, Q_2, G_2, F_2)$. Пусть $|Q_1| = r$, $|Q_2| = m$ и $q_i \in Q_1$, $q_j \in Q_2$. Тогда, если $q_i$ и $q_j$ отличимы, то существует отличающий их эксперимент $\bar{a}$ длины $l(\bar{a}) \leq r + m - 1$.

**Доказательство**. Можно считать, что $Q_1 \cap Q_2 = \emptyset$. Рассмотрим автомат $(A, B, Q, G, F)$, в котором $Q = Q_1 \cup Q_2$ и диаграмма которого получается объединением диаграмм исходных автоматов. Тогда $|Q| = r + m$ и по предыдущей теореме $q_i$, $q_j$ отличимы экспериментом $\bar{a}$ длины $l(\bar{a}) \leq r + m - 1$. Теорема доказана.

Следующий пример (рис. 9.2) показывает, что оценка $r + m - 1$ в общем случае неулучшаема. Здесь предполагается $m \geq r$ и опять выходной символ зависит только от текущего состояния и не зависит от входного символа.

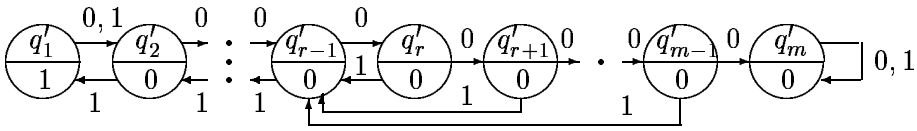



Рис. 9.2

Легко видеть, что если не использовать состояние $q'_m$ второго автомата, то нельзя отличить состояния $q_1$ и $q'_1$. Поэтому сначала надо перевести второй автомат словом $\bar{a}_1$ из $q'_1$ в $q'_m$. При этом $l(\bar{a}_1) \geq m - 1$ и первый автомат под действием $\bar{a}$ перейдет из $q_1$ в $q_r$. Чтобы далее получить различные выходные последовательности, надо перевести первый автомат из $q_r$ в $q_1$ и подать еще один символ. Всего для того, чтобы отличить $q_1$ от $q'_1$, потребуется входное слово длины $(m-1)+(r-1)+1 = m+r-1$.

**Определение.** Автомат, в котором все состояния попарно отличимы, называется приведенным автоматом.

Неотличимые состояния в автомате образуют классы эквивалентности.

**Определение.** Число классов неотличимых состояний называется *весом* автомата.

Если склеить все неотличимые между собой состояния, то диаграмма корректно перейдет в диаграмму приведенного автомата, который реализует то же автоматное отображение входных слов в выходные, что и исходный автомат.

Рассмотрим следующую задачу. Дан автомат с известной диаграммой, но неизвестно его начальное состояние. Всегда ли существует эксперимент $\bar{a}$, позволяющий определить это начальное состояние? Последнее равносильно тому, что $F(\bar{a}, q_i) \neq F(\bar{a}, q_j)$ для любых состояний $q_i \neq q_j$.

**Теорема 9.3**. Существует приведенный автомат, в котором нельзя определить начальное состояние.

**Доказательство**. Рассмотрим автомат на рис. 9.3 . Здесь первое число в скобках обозначает входной символ, а второе — выходной символ.

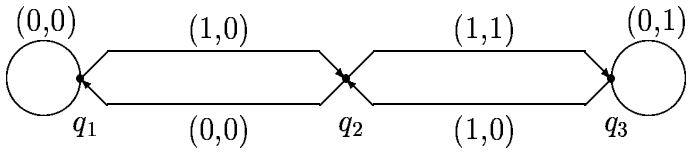



Рис. 9.3

Он приведенный, так как $q_2$ отличается от $q_1$ и $q_3$ экспериментом 1, а $q_1$ отличается от $q_3$ экспериментом 0. С другой стороны, нет единого эксперимента, отличающего все состояния, так как любой эксперимент, начинающийся с 0, не отличает $q_1$ и $q_2$, а любой эксперимент, начинающийся с 1, не отличает $q_1$ и $q_3$. Теорема доказана.