Министерство образования Республики Беларусь

Учреждение образования
“Гомельский государственный университет
имени Франциска Скорины”

В. В. АНИСЬКОВ,   И. В. БЛИЗНЕЦ

ДИСКРЕТНАЯ МАТЕМАТИКА

КУРС ЛЕКЦИЙ

Гомель, 2006

Министерство образования Республики Беларусь

Учреждение образования
“Гомельский государственный университет
имени Франциска Скорины”

В. В. АНИСЬКОВ, И. В. БЛИЗНЕЦ

ДИСКРЕТНАЯ МАТЕМАТИКА

КУРС ЛЕКЦИЙ

для студентов 1 курса
специальности 1–31 03 01–02 — “Математика
(научно-педагогическая деятельность)”

Гомель, 2006

УДК 519.1(075.8)
ББК 22.174 я 173
А 674

Рецензенты:
В. Н. Семенчук, доктор физико-математических наук;
кафедра алгебры и геометрии учреждения образования "Гомельский государственный университет имени Франциска Скорины"

Рекомендовано к изданию научно-методическим советом учреждения образования "Гомельский государственный университет имени Франциска Скорины"

Аниськов, В. В., Близнец И.В.
А 674 Дискретная математика: курс лекций для студентов 1 курса специальности 1–31 03 01–02 — "Математика (научно-педагогическая деятельность)" / В. В. Аниськов, И. В. Близнец; Мин-во обр. РБ, — Гомельский государственный университет им. Ф.Скорины. — УО "ГГУ им. Ф.Скорины". — 2006. — 108 с.
ISBN

Курс лекций предназначен студентам 1 курса математического факультета специальности 1–31 03 01–02 — "Математика (научно-педагогическая деятельность)", изучающим дисциплину "Дискретная математика". Может быть использован для самостоятельного изучения.

УДК 519.1(075.8)
ББК 22.174 я 173

ISBN

Содержание

Введение

Понятие "Дискретная математика"можно рассматривать как в широком, так и в узком смысле. В широком смысле дискретная математика — это та часть математики, которая не использует понятия предела и непрерывности. Это прежде всего алгебра и теория чисел, аналитическая геометрия, комбинаторика, математическая логика. В узком смысле дискретная математика понимается как различные приложения математики для функционирования ЭВМ. В настоящем курсе лекций рассматриваются некоторые разделы дискретной математики как в широком смысле, так и в узком: "Элементы комбинаторики", "Графы", "Булевы функции", "Функции k-значной логики", "Дизъюнктивные нормальные формы булевых функций", "Схемы из функциональных элементов". Эти разделы являются необходимой частью образования современного математика, поскольку содержащийся в них материал способствует выработке дискретных методов мышления.

Курс "Дискретная математика"предусмотрен учебным планом специальности 1 31 03 01-02 — "Математика (научно-педагогическая деятельность)"и изучается на 1 курсе. В связи с этим настоящий курс лекций по разделам "Элементы комбинаторики", "Графы", "Функции k-значной логики"дает только основные понятия, поскольку указанные разделы изучаются на старших курсах.

1. Элементы комбинаторики

1.1. Перестановки и сочетания

Определение 1.1. Пусть дано некоторое множество, состоящее из n элементов. Выберем из A некоторое подмножество, состоящее из m элементов ($m \geqslant 1$). Такое подмножество называется *выборкой* или, более точно, *выборкой из n элементов по m элементов*.

Например, $1, 2, 4$ — трёхэлементная выборка из множества 1, 2, 3, 4, 5, 6.

Если получено некоторое множество выборок, с одинаковым количеством элементов, то говорят, что *сделан выбор*.

Определение 1.2. Выбор называется *неупорядоченным*, если полученные в результате такого выбора выборки, состоящие из одних и тех же элементов и различающиеся лишь порядком их следования, считаются равными. Такие выборки называются *неупорядоченными* и обозначаются $[r_1, r_2, \ldots, r_t]$.

Например, $[1, 4, 3] = [4, 3, 1]$.

Определение 1.3. Выбор называется *упорядоченным*, если две выборки, полученные в результате такого выбора, равны только в том случае, когда они состоят из одинакового количества элементов и одинаковы по порядку их следования. Такие выборки называются *упорядоченными* и обозначаются $(r_1, r_2, \ldots, r_t)$.

Например, $(1, 3, 5) \neq (5, 3, 1)$.

Определение 1.4. Выбор называется *без возвращения*, если каждый элемент выбирается только один раз.

Определение 1.5. Выбор называется *с возвращением*, если каждый элемент может быть выбран сколь угодно раз.

Например, $(1, 1, 3)$, $(3, 1, 1)$, $[3, 3, 4, 4, 4, 5]$ — выборки с возвращением.

Определение 1.6. Упорядоченная выборка из n элементов по n элементов называется *перестановкой n-элементного множества*.

Число всех возможных перестановок n-элементного множества без возвращения обозначается $P(n)$, с возвращением — $\tilde{P}(n)$.

Определение 1.7. Упорядоченная выборка из n элементов по m элементов называется *размещением из n элементов по m элементов* ($0 \leqslant m \leqslant n$).

Число различных размещений из n элементов по m элементов без возвращения обозначается A_n^m. Считается, что если $m > n$, то $A_n^m =$

$= 0$. Число различных размещений из n элементов по m элементов с возвращением обозначается $\tilde{A}_n^m$.

Определение 1.8. Неупорядоченная выборка из n элементов по m элементов называется *сочетанием из n элементов по m элементов.*

Различают сочетания без повторений (число различных сочетаний без повторений обозначается C_n^m) и сочетания с повторениями (число различных сочетаний с повторениями обозначается H_n^m).

Для комбинаторики следующее утверждение является аксиомой, которая называется правилом суммы:

Если объект A может быть выбран m способами, а объект B может быть выбран n способами, то выбор "или A, или B"может быть осуществлен $m + n$ способами.

Еще одно утверждение в комбинаторике считается аксиомой и называется правилом произведения:

Если объект A может быть выбран m способами и для каждого из таких выборов объект B может быть выбран n способами, то выбор AB в этом порядке может быть осуществлен mn способами.

Теорема 1.1. *Имеют место следующие равенства:*

1) $A_n^m = \dfrac{n!}{(n-m)!}$;

2) $P(n) = n!$;

3) $C_n^m = \dfrac{n!}{m!(n-m)!}$;

4) $H_n^m = C_{n+m-1}^m$;

5) $\tilde{P}(n) = n^n$;

6) $\tilde{A}_n^m = n^m$.

Доказательство. Пусть дано множество A из n элементов ($|A| = n$). При получении любого размещения этого множества первый элемент выборки может быть выбран n способами. Поскольку выбор без повторения, то следующий элемент выбирается из $(n-1)$ элементов, то есть $(n-1)$ способами. Поэтому, используя правило произведения, получаем, что всё размещение из n элементов по m элементов может быть выбрано $n(n-1)(n-2)\dots(n-m+1) = \dfrac{n!}{(n-m)!}$ способами. Таким образом доказано равенство 1).

Равенство 2) следует непосредственно из равенства 1), т.к. $P(n) = A_n^n = \dfrac{n!}{(n-n)!} = n!$

Докажем равенство 3). Пусть $[r_1, r_2, \ldots, r_m]$ — произвольное сочетание без повторений. Из этого сочетания, согласно 2), можно составить $m!$ перестановок из m элементов. Пусть $[r_1, r_2, \ldots, r_m]$ и $[a_1, a_2, \ldots, a_m]$ — произвольные два различные сочетания без повторения. Предположим, что нам удалось получить из них хотя бы две одинаковые перестановки. Тогда оказалось бы, что $\{r_1, r_2, \ldots, r_m\} = \{a_1, a_2, \ldots, a_m\}$ и мы пришли бы к противоречию с тем, что $[r_1, r_2, \ldots, r_m]$ и $[a_1, a_2, \ldots, a_m]$ — различные сочетания. Поэтому наше предположение неверно и мы приходим к заключению о том, что можно применить правило произведения. Значит справедливо соотношение $A_n^m = P(m)C_n^m$. Отсюда

$$C_n^m = \frac{A_n^m}{P(m)}.$$

Теперь, используя 1) и 2) получим:

$$C_n^m = \frac{A_n^m}{P(m)} = \frac{n!}{m!(n-m)!}.$$

Докажем равенство 4). Построим биективное отображение $f : A \to$ $\to X$ по произвольному правилу, где $X = \{1, 2, \ldots, n\}$. Пусть нами выбрано некоторое сочетание из m элементов с повторениями из множества X. Запишем его следующим образом: $[i_1, i_2, \ldots, i_m]$, где $i_1 \leqslant i_2 \leqslant \ldots \leqslant$ $\leqslant i_m$.

Составим теперь множество $\tilde{X} = \{1, 2, \ldots, n, n+1, \ldots, n+m-1\}$ и построим отображение $g : X \to \tilde{X}$ по правилу:

$$g([i_1, i_2, \ldots, i_m]) = [i_1, i_2 + 1, \ldots, i_m + m - 1].$$

Убедимся сначала, что отображение g является инъекцией. Пусть $[i_1, \ldots, i_m] \neq [j_1, \ldots, j_m]$ — два различных сочетания с повторениями. Тогда существует хотя бы одно k $(1 \leqslant k \leqslant m)$ такое, что $i_k \neq j_k$. Но тогда $i_k + k - 1 \neq j_k + k - 1$ и поэтому $[i_1, i_2 + 1, \ldots, i_m + m - 1] \neq [j_1, j_2 +$ $+ 1, \ldots, j_m + m - 1]$. Обратно: пусть $[i_1, i_2 + 1, \ldots, i_m + m - 1] \neq [j_1, j_2 +$ $+ 1, \ldots, j_m + m - 1]$. Тогда существует хотя бы одно k $(1 \leqslant k \leqslant m)$ такое, что $i_k + k - 1 \neq j_k + k - 1$. Но тогда $i_k \neq j_k$ и поэтому $[i_1, \ldots, i_m] \neq$ $\neq [j_1, \ldots, j_m]$. Значит, отображение g является инъекцией. Если взять произвольный элемент $[x_1, x_2, \ldots, x_m]$ из множества $\tilde{X}$, то для него, в качестве прообраза при отображении g найдётся в множестве X элемент $[x_1, x_2 - 1, \ldots, x_m - m + 1]$. Значит, отображение g является к тому же и сюръективным. Следовательно, оно является биекцией. Поэтому число элементов в множествах X и $\tilde{X}$ равно. А так как f — биекция, то равно число элементов и в множествах A и $\tilde{X}$. Но $[i_1, i_2+1, i_2+2, \ldots, i_m+m-$ $-1]$ — сочетание без повторений из $n+m-1$ элементов по m. Поэтому $|\tilde{X}| = C_{n+m-1}^m$ Значит, $H_n^m = C_{n+m-1}^m$.

Докажем вначале 6). В этом случае очередной элемент выборки выбирается каждый раз из n-элементного множества. Поэтому, по правилу произведения, $\tilde{A}_n^m = nnn\ldots n = n^m$. Отсюда непосредственно следует равенство 5), т.к. $\tilde{P}(n) = \tilde{A}_n^n = n^n$.

Теорема доказана.

Замечание 1.1. *Если $m > n$ или $m = 0$, то считается, что $C_n^m =$ $= 1$.*

Теорема 1.2. $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$.

Доказательство. Пусть $A = |n|$. Зафиксируем в A некоторый элемент x. Пусть A_x — множество всех m-элементных сочетаний без повторений, содержащих элемент x, а A^x — множество всех m-элементных сочетаний без повторений, не содержащих элемент x. Число всех m-элементных сочетаний без повторений множества A будет тогда равно $|A_x| + |A^x|$, т. е., $C_n^m = |A_x| + |A^x|$. Рассмотрим множество $A \setminus \{x\}$. Множество всех m-элементных сочетаний без повторений из элементов множества $A \setminus \{x\}$ совпадает с множеством A^x. Но в множестве $A \setminus \{x\}$ число всех элементов равно $n-1$. Поэтому число всех m-элементных сочетаний без повторений из элементов множества $A \setminus \{x\}$ равно C_{n-1}^m. Значит, $|A^x| = C_{n-1}^m$. Если из каждого из сочетаний, составляющих множество A_x убрать элемент x, то мы получим множество всех возможных $(m-$ $-1)$-элементных сочетаний без повторений из $n-1$ элементов. Поэтому $|A_x| = C_{n-1}^{m-1}$. Таким образом, $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$.

Существует еще одно доказательство данной теоремы:

$$C_n^m = \frac{n!}{m!(n-m!)} = \frac{n(n-1)!}{m!(n-m)!} = \frac{(n-m+m)(n-1)!}{m!(n-m)!} =$$
$$= \frac{(n-m)(n-1)! + m(n-1)!}{m!(n-m)!} = \frac{(n-m)(n-1)!}{m!(n-m)!} + \frac{m(n-1)!}{m!(n-m)!} =$$
$$= \frac{(n-1)!}{m!((n-m)-1)!} + \frac{(n-1)!}{(m-1)!(n-1-m+1)!} =$$
$$= \frac{(n-1)!}{m!((n-1)-m)!} + \frac{(n-1)!}{(m-1)!(n-1-(m-1))!} =$$
$$= C_{n-1}^m + C_{n-1}^{m-1}.$$

Теорема доказана.

Теорема 1.3 (Биномиальная теорема Ньютона). *Для любых* *действительных чисел x, y и натуральных n и k имеет место равенство:*

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}.$$

Доказательство. Проведем доказательство теоремы по индукции. Основание индукции. При $n=1$ и $n=2$ равенство выполняется:

$$(x+y)^1 = C_1^0 x^0 y^1 + C_1^1 x^1 y^0 = x + y.$$

$$(x+y)^2 = C_2^0 x^0 y^2 + C_2^1 x^1 y^1 + C_2^2 x^2 y^0 = y^2 + 2xy + x^2.$$

Индуктивное предположение. Допустим, что равенство верно для $n-1$:

$$(x+y)^{n-1} = \sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-1-k}.$$

Индуктивный переход:

$$(x+y)^n = (x+y)(x+y)^{n-1} = (x+y)\left(\sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-1-k}\right) =$$

$$= x\sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-1-k} + y\sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-1-k} =$$

$$= x\sum_{k=1}^{n} C_{n-1}^{k-1} x^{k-1} y^{n-1-(k-1)} + \sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-k} =$$

$$= \sum_{k=1}^{n} C_{n-1}^{k-1} x^k y^{n-k} + \sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-k} =$$

$$= x^n + \sum_{k=1}^{n-1} C_{n-1}^{k-1} x^k y^{n-k} + \sum_{k=1}^{n-1} C_{n-1}^{k-1} x^k y^{n-k} + y^n =$$

$$= x^n + \sum_{k=1}^{n-1}(C_{n-1}^{k-1} + C_{n-1}^k) x^k y^{n-k} + y^n = x^n + \sum_{k=1}^{n-1} C_n^k x^k y^{n-k} + y^n =$$

$$= \sum_{k=n}^{n} C_n^k x^k y^{n-k} + \sum_{k=1}^{n-1} C_n^k x^k y^{n-k} + \sum_{k=0}^{0} C_n^k x^k y^{n-k} = \sum_{k=0}^{n} C_n^k x^k y^{n-k}.$$

Теорема доказана.

Теорема 1.4 (Полиномиальная теорема). *Для любых действительных чисел x_1, x_2, $\ldots$, $x_m \in \mathbb{R}$ и натурального n имеет место* *равенство:*

$$(x_1 + x_2 + \ldots + x_m)^n = \sum_{\substack{k_1+k_2+\ldots+k_m=n \\ k_i \geqslant 0 \ (i=\overline{1,m})}} \frac{n!}{k_1!k_2!\ldots k_m!} x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m},$$

где суммирование ведется по всем возможным целым неотрицательным разбиениям числа n.

Доказательство. Проведем доказательство теоремы по индукции.

Основание индукции. Основанием индукции является биномиальная теорема для x_1 и x_2:

$$(x_1 + x_2)^n = \sum_{k=0}^{n} C_n^k {x_1}^k {x_2}^{n-k}.$$

Допустим, что теорема верна для $x_1, x_2, \ldots, x_{m-1}$. Тогда

$$(x_1 + x_2 + \ldots + x_m)^n = \big((x_1 + x_2 + \ldots + x_{m-1}) + x_m\big)^n =$$

$$= \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} (x_1 + x_2 + \ldots + x_{m-1})^k x_m^{n-k} =$$

$$= \sum_{k+(n-k)=n} \frac{n!}{k!(n-k)!} \Bigg(\sum_{l_1+l_2+\ldots+l_{m-1}=k} \frac{k!}{l_1! \cdot l_2! \cdot \ldots \cdot l_{m-1}!} \cdot$$

$$\cdot x_1^{l_1} x_2^{l_2} \cdot \ldots \cdot x_{m-1}^{l_{m-1}} \Bigg) \cdot x^{n-(l_1+\ldots+l_{m-1})} =$$

$$= \sum_{l_1+l_2+\ldots+l_m=n} \frac{n!}{l_1! \cdot l_2! \cdot \ldots \cdot l_{m-1}! \cdot l_m!} x_1^{l-1} x_2^{l_2} \cdot \ldots \cdot x_{m-1}^{l_{m-1}} x_m^{l_m}.$$

Теорема доказана.

Теорема 1.5. *Число всех возможных разбиений n-элементного множества на k непересекающихся подмножеств имеющих порядки $n_1, n_2, \ldots, n_k$ ($0 \leqslant n_i \leqslant n$) выражается формулой*

$$C_n^{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \ldots n_k!}.$$

Доказательство. Пусть $|A| = n$, и пусть $n_1 + n_2 + \ldots + n_k = n$ — некоторое натуральное разбиение числа n. Тогда множество A_1, состоящее из n_1 элементов можно выбрать $C_n^{n_1}$ способами. Множество $A_2 = A \setminus A_1$ можно выбрать $C_{n-n_1}^{n_2}$ способами и так далее. Значит, используя правило произведения, получим:

$$C_n^{n_1,n_2\dots n_k} = C_n^{n_1} C_{n-n_1}^{n_2} \dots C_{n-n_1-n_2-\dots-n_{k-1}}^{n_k} =$$

$$= \frac{n!(n-n_1)!(n-n_1-n_2)!\dots(n-n_1-\dots-n_k)!}{n_1!(n-n_1)!n_2!(n-n_1-n_2)!\dots n_k!(n-n_k)!} = \frac{n!}{n_1!n_2!\dots n_k!}.$$

Теорема доказана.

Если $|A| = n$, то число всех подмножеств множества A равно $\sum\limits_{k=0}^{n} C_n^k$. Используя биномиальную теорему, это число легко найти:

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

Так же легко установить равенство $C_n^m = C_n^{n-m}$:

$$C_n^m = \frac{n!}{m!(n-m)!} = \frac{n!}{(n-m)!(n-(n-m))!} = C_n^{n-m}.$$

1.2. Принцип включения и исключения

Пусть X — некоторое не пустое множество и пусть X_i ($1 \leqslant i \leqslant n$) некоторое подмножество X. Нетрудно убедится в том, что верна следующая формула

$$|X_1 \cup X_2| = |X_1| + |X_2| - |X_1 \cap X_2|, \tag{1.1}$$

где X_1 и X_2 — некоторые множества. Действительно, каждый элемент из $X_1 \cup X_2$ учитывается только один раз, в правой же части он учитывается либо в X_1, либо в X_2, либо, если он принадлежит $X_1 \cap X_2$, то учитывается дважды. Поэтому из правой части вычитается число $|X_1 \cap X_2|$.

Если $X_1 \cap X_2 = \varnothing$, то $|X_1 \cap X_2| = 0$ и, ввиду (1.1):

$$|X_1 \cup X_2| = |X_1| + |X_2|. \tag{1.2}$$

Пусть X — некоторое непустое множество. Из свойств операций над множествами легко получить следующие утверждения:

$$(X \setminus (X_1 \cup X_2)) \cap (X_1 \cup X_2) = \varnothing;$$

$$X = (X \setminus (X_1 \cup X_2)) \cup (X_1 \cup X_2).$$

Значит, можно использовать равенство (1.2):

$$|X| = |X \setminus (X_1 \cup X_2)| + |X_1 \cup X_2|;$$

$$|X \setminus (X_1 \cup X_2)| = |X| - |X_1 \cup X_2|.$$

Теперь используем (1.1):

$$|X \setminus (X_1 \cup X_2)| = |X| - (|X_1| + |X_2| - |X_1 \cap X_2|);$$

$$|X \setminus (X_1 \cup X_2| = |X| - |X_1| - |X_2| + |X_1 \cap X_2|.$$

Пусть X — множество элементов, каждый из которых может обладать свойством a_1 или свойством a_2 (союз "или" здесь используется в соединительном смысле). Пусть X_1 — множество всех элементов, обладающих свойством a_1; X_2 — множество всех элементов, обладающих свойством a_2. Тогда $X \setminus (X_1 \cup X_2)$ — есть подмножество всех тех элементов из X, которые не обладают ни свойством a_1 ни свойством a_2. Введём следующие обозначения: $|X_1| = N(a_1)$; $|X_2| = N(a_2)$; $|X_1 \cap X_2| = N(a_1, a_2)$; $|X \setminus (X_1 \cup X_2)| = N(\overline{a}_1, \overline{a}_2)$. Тогда

$$N(\overline{a}_1, \overline{a}_2) = N - N(a_1) - N(a_2) + N(a_1, a_2).$$

Полученную формулу, которая носит название формулы включения и исключения можно обобщить.

Пусть имеется множество X из N элементов, каждый из элементов которого может обладать одним или несколькими свойствами a_1, a_2, ... , a_n. Через $N(a_1, \ldots, a_k)$ $(1 \leqslant k \leqslant n)$ обозначим количество элементов из X, которые обладают свойствами a_1, ... , a_k и может быть некоторыми другими. Число элементов, не обладающих ни одним из свойств обозначим через $N(\overline{a}_1, \ldots, \overline{a}_n)$. Тогда справедлива следующая формула включений и исключений:

Теорема 1.6.

$$\begin{gathered} N(\overline{a}_1, \ldots, \overline{a}_n) = N - N(a_1) - \ldots - N(a_n) + N(a_1, a_2) + \\ +N(a_1, a_3) + \ldots + N(a_{n-1}, a_n) - N(a_1, a_2, a_3) - \\ -N(a_1, a_2, a_4) - \ldots - N(a_{n-2}, a_{n-1}, a_n) + \ldots \\ +(-1)^n N(a_1, \ldots, a_k) \end{gathered} \tag{1.3}$$

Доказательство. Покажем сначала по индукции справедливость для любых конечных множеств X_i $(1 \leqslant i \leqslant n;\ n \geqslant 2)$ равенства:

$$\begin{gathered} |X_1 \cup X_2 \cup \ldots \cup X_n| = (|X_1| + |X_2| + \ldots + |X_n|) - \\ -(|X_1 \cap X_2| + |X_1 \cap X_3| + \ldots + |X_{n-1} \cap X_n|) + \\ +(|X_1 \cap X_2 \cap X_3| + |X_1 \cap X_2 \cap X_4| + \ldots + |X_{n-2} \cap \\ \cap X_{n-1} \cap X_n|) + \ldots + (-1)^{n+1} |X_1 \cap X_2 \cap \ldots \cap X_n|. \end{gathered} \tag{1.4}$$

Перепишем это равенство в следующем виде:

$$|\bigcup_{i=1}^{n} X_i| = \sum_{i=1}^{n} |X_i| - \sum_{1\leqslant i<j<k\leqslant n} |X_i \cap X_j \cap X_k| + \ldots$$
$$\ldots + (-1)^{n+1}|X_1 \cap \ldots \cap X_n|. \qquad (1.5)$$

В правой части формулы (1.2) содержится $2^n - 1$ слагаемых. (т.к. это множество всех подмножеств n-элементного множества без пустого подмножества). Поскольку число всех подмножеств данного множества не может быть превышено, то доказывать будем индукцией по числу слагаемых.

Основание индукции. Для двух множеств — X_1 и X_2 утверждение выполняется ввиду (1.1). Кроме того, в правой части (1.1) содержится $2^2 - 1 = 3$ слагаемых. Предположим, что (1.2) верно для случая $n-1$ подмножеств и в правой части его содержится $2^{n-1} - 1$ слагаемых. Тогда

$$|X_1 \cup X_2 \ldots \cup X_n| = |(X_1 \cup \ldots \cup X_{n-1}) \cup X_n| \overset{\text{по (1.1)}}{=}$$
$$\overset{\text{по (1.1)}}{=} |X_1 \cup \ldots \cup X_{n-1}| + |X_n| - |(X_1 \cup \ldots \cup X_{n-1}) \cap X_n|$$

или, обозначив $Y_i = X_i \cap X_n$ $(1 \leqslant i \leqslant n-1)$ получаем

$$|X_1 \cup \ldots \cup X_n| = |X_1 \cup \ldots \cup X_{n-1}| + |X_n| - |Y_1 \cup \ldots \cup Y_{n-1}| \qquad (1.6)$$

Первое и третье слагаемые правой части попадают под предположение индукции. Рассмотрим эти слагаемые отдельно и более подробно:

а)

$$|X_1 \cup \ldots \cup X_{n-1}| = \sum_{i=1}^{n-1} |X_i| - \sum_{1\leqslant i\leqslant j\leqslant n-1} |X_i \cap X_j| +$$
$$+ \sum_{1\leqslant i<j<k<n-1} |X_i \cap X_j \cap X_k| - \ldots + (-1)^n |X_1 \cap \ldots \cap X_{n-1}|;$$

б)

$$|Y_1 \cup \ldots \cup Y_{n-1}| = \sum_{i=1}^{n-1} |Y_i| - \sum_{1 \leqslant i \leqslant j \leqslant n-1} |Y_i \cap Y_j| +$$

$$+ \sum_{1 \leqslant i < j < k < n-1} |Y_i \cap Y_j \cap Y_k| - \ldots + (-1)^n |Y_1 \cap \ldots \cap Y_{n-1}| =$$

$$= \sum_{i=1}^{n-1} |X_i \cap X_n| - \sum_{1 \leqslant i < j \leqslant n-1} |X_i \cap X_j \cap X_n| +$$

$$+ \sum_{1 \leqslant i < j < k \leqslant n-1} - \ldots + (-1)^n |X_1 \cap \ldots \cap X_n|.$$

В каждой из формул а) и б) в правой части имеется по $2^{n-1}-1$ слагаемых. Подставив а) и б) в (1.6), получим (1.2). Следовательно, поскольку в правой части (1.6) три слагаемых, то число слагаемых в правой части (1.2) равно $2(2^{n-1} - 1) + 1 = 2^n - 1$. Таким образом, мы доказали, что равенство (1.2) верно и для случая n множеств.

Так как

$$(X \setminus (X_1 \cup X_2 \ldots \cup X_n)) \cap (X_1 \cup X_2 \ldots \cup X_n) = \varnothing$$

и

$$(X \setminus (X_1 \cup X_2 \ldots \cup X_n)) \cup (X_1 \cup X_2 \ldots \cup X_n) = X,$$

то можно применить равенство (1.2). Мы получим, что

$$|X \setminus (X_1 \cup X_2 \ldots \cup X_n)| = |X| - |X_1 \cup X_2 \ldots \cup X_n|.$$

Используя теперь в последнем равенстве формулу (1.2) и обозначения, о которых говорилось перед формулировкой теоремы, мы получим (1.6).

Теорема доказана.

1.3. Рекуррентные соотношения

Определение 1.9. *Рекуррентным соотношением* (*рекуррентной формулой*) называется формула вида $a_n = f(n, a_{n-1} \ldots a_{n-k})$ выражающая при $n > k$ каждый член последовательности a_n через предыдущие k членов a_{n-1}, a_{n-2}, $\ldots$, a_{n-k}. Число k называется *порядком* рекуррентного соотношения.

При составлении треугольника Паскаля используется равенство $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$. В функциональных обозначениях оно будет иметь

вид:
$$g(n,m) = g(n-1,m) + g(n-1,m-1), \quad i \leqslant m \leqslant n.$$
Это один из примеров рекуррентного соотношения.

Если известно рекуррентное соотношение и начальные члены последовательности (которые называются начальными условиями), то вычислить всю последовательность легко. Однако, для того, чтобы вычислить n-ный член последовательности, необходимо вычислить все предыдущие. Поэтому, в целях экономии, важно иметь для рекуррентного соотношения формулу, которая позволяет вычислять член последовательности по его номеру.

Определение 1.10. Последовательность $\{a_n\}$ называют *решением рекуррентного соотношения*, если при ее подстановке в это рекуррентное соотношение, оно тождественно выполняется.

Определение 1.11. Решение рекуррентного соотношения называется *частным*, если оно не зависит от произвольной постоянной и каждый его член определяется однозначно, завися лишь от номера.

Определение 1.12. Решение рекуррентного соотношения k-того порядка называется *общим*, если оно зависит от k произвольных постоянных C_1, C_2, ... , C_k. Путем подбора этих постоянных можно получить любое частное решение данного рекуррентного соотношения, удовлетворяющее k начальным условиям.

Таким образом, общее решение рекуррентного соотношения — это общая формула, "собирающая"все частные решения.

Пример 1.1. Рекуррентное соотношение
$$f(n+2) = 3f(n+1) - 2f(n), \tag{1.7}$$
имеет порядок 2 и последовательность 2^n — является его решением. Другим решением является последовательность $C \cdot 2^n$, где C — const, 2^n является частным решением, $C \cdot 2^n$ — общим.

Общих правил для решения рекуррентных соотношений нет, однако существует важный класс рекуррентных соотношений, которые решаются определёнными методами. В настоящее время разработан теоретический аппарат, позволяющий рекуррентное соотношение любого порядка из этого класса решить одним методом.

Определение 1.13. Рекуррентное соотношение вида:
$$f(n+k) = a_1 f(n+k-1) + a_2 f(n+k-2) + \\ + a_3 f(n+k-3) \ldots + a_k f(n) + \vartheta(n), \tag{1.8}$$

где $a_1, \ldots, a_k \in \mathbb{C}$, $\vartheta(n) \not\equiv 0$ называется *линейным рекуррентным соотношением с постоянными коэффициентами.*

Определение 1.14. Рекуррентное соотношение вида:

$$f(n+k) = a_1 f(n+k-1) + a_2 f(n+k-2) + \ldots + a_k f(n) \tag{1.9}$$

где $a_1, \ldots, a_n \in \mathbb{C}$ называется *линейным однородным рекуррентным соотношением с постоянными коэффициентами.*

Пример 1.2. Рекуррентное соотношение (1.7) — линейное однородное рекуррентное соотношение с постоянными коэффициентами.

Определение 1.15. Уравнение

$$x^k - a_1 x^{k-1} \ldots - a_k = 0 \tag{1.10}$$

называется *характеристическим уравнением* рекуррентного соотношения (1.9).

Теорема 1.7. *Общее решение линейного однородного рекуррентного соотношения* (1.9) *имеет вид*

$$\alpha(n) = \sum_{i=1}^{s} (C_{i_1} + C_{i_2} n + \ldots + C_{i_r} n^{r-1}) \lambda_i^n,$$

где C_{ij} ($1 \leqslant i \leqslant s$; $1 \leqslant j \leqslant r$) — комплексные числа, а $\lambda_1, \ldots, \lambda_s$ — различные корни характеристического уравнения соответственно кратности $r_1, \ldots, r_s$.

Теорема 1.8. *Общее решение рекуррентного соотношения* (1.8) *можно представить в виде суммы общего решения соответствующего однородного соотношения* (1.9) *и некоторого частного решения соотношения* (1.8).

Для каждого из видов функции $\vartheta(n)$ рекуррентного соотношения (1.8), частное решение имеет определенный вид. В целях ознакомления рассмотрим лишь тот случай, когда $\vartheta(n) = R_m(n)\lambda^n$, где R_m — многочлен степени m, соответствующий n-ному члену последовательности и $\lambda \neq 0$. Частное решение соотношения (1.8) имеет вид $Q_m(n)\lambda^n$, где Q_m — многочлен степени m, соответствующий n-ному члену последовательности, если λ не является корнем характеристического уравнения и вид $n^r Q_m(n)\lambda^n$, если λ — корень характеристического уравнения кратности r ($r \geqslant 1$).

1.4. Производящие функции

Одним из наиболее эффективных средств решения некоторых комбинаторных задач является метод производящих функций. Основная идея этого метода заключается в том, что каждой числовой последовательности ставится в соответствие функция действительного или комплексного переменного. Причем отношения между последовательностями выражаются в отношениях между функциями. К самим функциям можно применять аналитические методы исследования, которые иногда оказываются более простыми и удобными, чем непосредственное оперирование с числовыми последовательностями.

Вместо $a_0, a_1, \ldots, a_n$ будем писать a_n $(n \geqslant 0)$.

Определение 1.16. *Производящей функцией* последовательности a_n $(n \geqslant 1)$ называется степенной ряд вида

$$A(z) = \sum_{n=0}^{\infty} a_n z^n. \tag{1.11}$$

Экспоненциальной производящей функцией последовательности a_n $(n \geqslant 1)$ называется степенной ряд вида

$$A^*(z) = \sum_{n=1}^{\infty} \frac{a_n}{n!} z^n. \tag{1.12}$$

Числа a_n называются коэффициентами производящей функции, а числа $\dfrac{a_n}{n!}$ называются коэффициентами экспоненциальной производящей функции.

Если ряды (1.11) и (1.12) являются сходящимися, то их суммы можно рассматривать как некоторые функции и, исследуя эти функции, получать полезную информацию об исходной последовательности. Если радиус сходимости этих рядов равен нулю, то оперировать с ними можно только рассматривая их как некоторые формальные объекты. Оперирование с такими объектами проводится в рамках алгебры формальных степенных рядов. В этой алгебре основными операциями являются следующие.

1° если для любого $n = 1, 2, \ldots$ $a_n = b_n$, то

$$\sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} b_n z^n;$$

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n = \sum_{n=0}^{\infty} \frac{b_n}{n!} z^n;$$

2°

$$\sum_{n=0}^{\infty} a_n z^n \pm \sum_{n=0}^{\infty} b_n z^n = \sum_{n=0}^{\infty} (a_n \pm b_n) z^n;$$

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n \pm \sum_{n=0}^{\infty} \frac{b_n}{n!} z^n = \sum_{n=0}^{\infty} \frac{a_n \pm b_n}{n!} z^n;$$

3° если $c_n = \sum\limits_{i=0}^{n} a_i b_{n-i}$, то

$$(\sum_{n=0}^{\infty} a_n z^n)(\sum_{n=0}^{\infty} b_n z^n) = \sum_{n=0}^{\infty} c_n z^n;$$

если $d_n = \sum\limits_{i=0}^{n} a_i b_{n-i}$, то

$$(\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n)(\sum_{n=0}^{\infty} \frac{b_n}{n!} z^n) = \sum_{n=0}^{\infty} \frac{d_n}{n!} z^n.$$

4° $\forall c \in \mathbb{R}$ справедливы равенства:

$$c(\sum_{n=0}^{\infty} a_n z^n) = \sum_{n=0}^{\infty} c a_n z^n;$$

$$c(\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n) = \sum_{n=0}^{\infty} c \frac{a_n}{n!} z^n.$$

Последовательности c_n и d_n, определяемые указанными выше равенствами называются *свертками* последовательностей a_n и b_n. Если известны производящие функции $A(z)$ и $B(z)$ соответственно последовательностей a_n и b_n, то их сверткой является функция $A(z)B(z)$.

Из курса математического анализа известно, что ряд $\sum\limits_{n=0}^{\infty} z^n$ сходится к нулю при $|z| < 1$ и сумма этого ряда равна $(1-z)^{-1}$ т.е. для указанных z, $\sum\limits_{n=0}^{\infty} z^n = (1-z)^{-1}$. Согласно определению производящей функции, этот же ряд является производящей функцией для последовательности 1, 1, 1, ... Это обстоятельство является иллюстрацией основного принципа теории производящих функций, заключающегося в том, что операции, участвующие в формулах должны иметь смысл хотя бы для формальных степенных рядов.

Получим теперь производящие функции для некоторых рекуррентных соотношений.

1. Согласно формуле бинома Ньютона,

$$(1+t)^n = \sum_{m=0}^{n} C_n^m t^m 1^{n-m} = \sum_{m=0}^{n} C_n^m t^m.$$

Поэтому для последовательности C_n^m производящей функцией будет $(1+ + t)^n$.

2. Для последовательности 2^n производящей функцией может быть $(1-2z)^{-1}, |z| < 1$, так как

$$\sum_{n=0}^{\infty} 2^n z^n = \sum_{n=0}^{\infty} (2z)^n = (1-2z)^{-1}.$$

3. Поскольку аналитическую функцию можно почленно дифференцировать, то, используя полученную выше для последовательности z^n производящую функцию $(1-z)^{-1}$, можно получить следующее равенство (которое использует в некотором смысле дифференцирование в обратную сторону):

$$\sum_{n=0}^{\infty} nz^n = z\sum_{n=0}^{\infty} nz^{n-1} = z\frac{d}{dz}(\sum_{n=0}^{\infty} z^n) =$$

$$z\frac{d}{dz}(1-z)^{-1} = z(1-z)^{-2}.$$

Значит функция $z(1-z)^{-2}$ является производящей функцией для последовательности n.

4. Если использовать введенные выше формальные операции, то в результате перемножения двух производящих функций, мы получим новую производящую функцию: $(1+z)^r(1+z)^s = (1+z)^{r+s}$. Эта функция является производящей функцией для последовательности C_{r+s}^n. Если теперь приравнять коэффициенты при z^n, то можно получить тождество Коши:

$$\sum_{k=0}^{n} C_r^k C_s^{n-k} = C_{r+s}^n.$$

5. Поскольку

$$(1-z)^n = \sum_{n=0}^{\infty} C_r^n (-1)^n z^n,$$

то функция $(1-z)^r$ является производящей функцией для последовательности $(-1)^n C_r^n$. Перемножив производящие функции

$$(1-z)^r (1+z)^r = (1-z^2)^r,$$

получаем следующее равенство:

$$\sum_{k=0}^{n} C_r^k C_r^{n-k} (-1)^k = \begin{cases} (-1)^n C_r^n, & \text{если } n \text{ — четно,} \\ 0, & \text{если } n \text{ — нечетно.} \end{cases}$$

6. Используя введённую выше операцию 3°, получим:

$$(1+z)^m (1+z)^m = \sum_{n=0}^{\infty} C_m^n z^n \sum_{n=0}^{\infty} C_m^n z^n = \sum_{n=0}^{\infty} C_n z^n,$$

где

$$C_n = \sum_{k=0}^{n} C_m^k C_m^{n-k}.$$

С другой стороны,

$$(1+z)^m (1+z)^m = (1+z)^{2m} = \sum_{n=0}^{\infty} C_{2m}^n z^n.$$

Поскольку же

$$\sum_{k=0}^{\infty} C_m^k C_m^{n-1} = \sum_{k=0}^{n} (C_m^k)^2,$$

то, приравняв коэффициенты при степенях z, окончательно получаем:

$$\sum_{k=0}^{n} (C_m^k)^2 = C_{2m}^m.$$

Иногда удается использовать свойства исходной последовательности при получении уравнения для производящей функции. Если удается решить полученное уравнение, то из разложения решения в степенной ряд можно получить формулу членов исходной последовательности. Например, рассмотрим последовательность f_n $(n \geqslant 1)$ такую, что $f_0 = f_1 = 1$ и $f_n = f_{n-1} + f_{n-2}$ при $n \geqslant 2$. Она называется *последовательностью*

Фибоначчи. Найдем формулу для вычисления f_n. Производящей функцией этой последовательности будет функция $F(z) = \sum\limits_{n=0}^{\infty} f_n z^n$. Выполняя алгебраические преобразования, получим:

$$F(z) = f_0 + zf_1 + \sum_{n=2}^{\infty}(f_{n-1} + f_{n-2})z^n =$$

$$= f_0 + zf_1 + \sum_{n=2}^{\infty} f_{n-1}z^n + \sum_{n=2}^{\infty} f_{n-2}z^n =$$

$$= f_0 + zf_1 + \sum_{n=1}^{\infty} f_n z^{n+1} + \sum_{n=0}^{\infty} f_n z^{n+2}.$$

Т.о. получаем, что

$$F(z) = f_0 + zf_1 + \sum_{n=1}^{\infty} f_n z^{n+1} + \sum_{n=0}^{\infty} f_n z^{n+2} \tag{1.13}$$

Т.к.

$$\sum_{n=1}^{\infty} f_n z^{n+1} = z\sum_{n=1}^{\infty} f_n z^n = zf_0 + z\sum_{n=1}^{\infty} f_n z^n - zf_0 =$$

$$= z\sum_{n=0}^{\infty} f_n z^n - zf_0 = zF(z) - zf_0 = z(F(z) - f_0)$$

и, поскольку,

$$\sum_{n=1}^{\infty} f_n z^{n+2} = z^2 F(z),$$

то из (1.13) получаем:

$$F(z) = f_0 + f_1 z + z(F(z) - f_0) + z^2 F(z) =$$
$$= 1 + z + z(F(z) - 1) + z^2 F(z) = 1 + zF(z) + z^2 F(z).$$

Отсюда $F(z) - zF(z) - z^2 F(z) = 1$. Поэтому

$$F(z) = \frac{1}{1 - z - z^2}.$$

Найдя корни уравнения $1 - z - z^2 = 0$, получим разложение

$$1 - z - z^2 = (1 - az)(1 - bz),$$

где
$$a=\frac{1+\sqrt{5}}{2},\quad b=\frac{1-\sqrt{5}}{2}.$$
Тогда
$$F(z)=\frac{C}{1-az}+\frac{D}{1-bz},$$
где
$$C=\frac{a}{a-b},\quad D=-\frac{b}{a-b}.$$

Поскольку для малых положительных z (таких, чтобы выполнялось $0<cz<1$) верно равенство
$$(1-cz)^{-1}=\sum_{n=0}^{\infty}(cz)^n,$$
то получаем:
$$F(z)=C(1-az)^{-1}+D(1-bz)^{-1}=$$
$$=C\cdot\sum_{n=0}^{\infty}(az)^n+D\cdot\sum_{n=0}^{\infty}(bz)^n=\sum_{n=0}^{\infty}\frac{a^{n+1}-b^{n+1}}{a-b}z^n.$$

Отсюда по 1°
$$f_n=\frac{a^{n+1}-b^{n+1}}{a-b}=\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right).$$

Этот пример демонстрирует связь дискретного и непрерывного анализа.

Рассмотрим еще один пример производящих функций. Экспоненциальной производящей функцией последовательности 1, 1, 1, … является
$$e^z=\exp z=\sum_{n=0}^{\infty}\frac{z^n}{n!}.$$
Пусть при $n\geqslant 0$ мы имеем экспоненциальную производящую функцию для последовательности d_n: $\sum\limits_{n=0}^{\infty}d_n\frac{z^n}{n!}$. Умножим ее почленно на z :

$$z\sum_{n=0}^{\infty}\frac{z^n}{n!}=\sum_{n=0}^{\infty}\frac{z^{n+1}}{n!}=\sum_{n=1}^{\infty}d_{n-1}\frac{z^n}{(n-1)!}=\sum_{n=1}^{\infty}nd_{n-1}\frac{z^n}{n!}.$$

Таким образом получаем производящую функцию для последовательности $d_0,\ 2d_1,\ 3d_2,\ \ldots$ После дифференцирования по z экспоненциальной производящей функции для последовательности d_n $(n \geqslant 0)$ получаем

$$\sum_{n=0}^{\infty} n d_n \frac{z^{n-1}}{n!} = \sum_{n=1}^{\infty} d_n \frac{z^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} d_{n+1} \frac{z^n}{n!}.$$

Полученная функция является экспоненциальной производящей функцией для последовательности d_n $(n \geqslant 1)$.

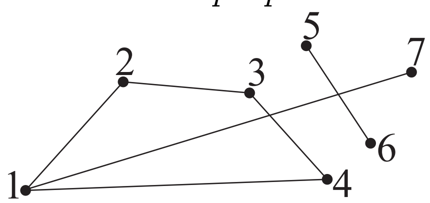
2. Графы

Появившись как развлекательное математическое приложение при решении головоломок, графы выделились в отдельную математическую дисциплину в связи с развитием комбинаторики и топологии в начале XX века. В настоящее время графы используются почти во всех разделах дискретной математики.

Здесь мы рассмотрим только основные понятия, связанные с графами и дадим некоторые наиболее важные результаты без доказательства.

2.1. Начальные понятия

Определение 2.1. *Графом* называется пара $G = (V, E)$ множеств V и E таких, что $V \neq \varnothing$ и $E \subseteq [V]^2$ (где $[V]^2$ — множество всех возможных неупорядоченных двухэлементных выборок из элементов множества V). Такие графы называются *неориентированными* или *неорграфами*. Элементы множества V называются *вершинами*, элементы множества E называются *ребрами*.



$V = \{1, 2, \ldots, 7\}$; $E = \{\{1, 2\}; \{2, 3\}; \{3, 4\}; \{5, 6\}; \{1, 7\}\}$. Выражение "граф на V" означает граф со множеством вершин V.

Множество вершин графа G обозначается $V(G)$, множество ребер обозначается $E(G)$. Число вершин графа G называется его *порядком* и обозначается $|G|$, число ребер — $\|G\|$. В зависимости от порядка графы делятся на конечные и бесконечные. В дальнейшем, если нет специальной оговорки, будем рассматривать конечные графы.

Вершину графа G, как элемент множества V, будем обозначать через v, ребро графа, как элемент множества E будем обозначать через e.

Определение 2.2. Вершина v называется *инцидентной* ребру e, если $v \in e$. Две вершины инцидентные одному ребру называются его *концевыми* вершинами. Обычно ребро, которому инцидентны вершины x и y (являются его концевыми вершинами) будем обозначать через xy.

Определение 2.3. Две вершины x и y графа G называются *соседними* если $xy \in E(G)$. Два ребра f и g называются *смежными* если $f \neq g$ и им обоим инцидентна одна вершина. Если все вершины графа G попарно соседние, то граф называется *полным*.

Определение 2.4. Множество попарно несмежных вершин называется *независимыми.*

Определение 2.5. *Неорграфом пересечений* соответствующим системе множеств $F = \{A_1, A_2, \ldots, A_m\}$ (каждое A_i не пустое), называется такой неорграф $G = (F, E)$, в котором вершины из A_i и A_j являются соседними тогда и только тогда, когда $A_i \cap A_j \neq \varnothing$.

Утверждение 2.1. *Каждый неорграф является неорграфом пересечений для соответствующего семейства множеств.*

Множество $\{0,1\}^n$ представляет собой множество всевозможных наборов $(s_1, s_2, \ldots, s_n)$, где $s_i \in \{0,1\}$ для любого $i = 1, \ldots, n$.

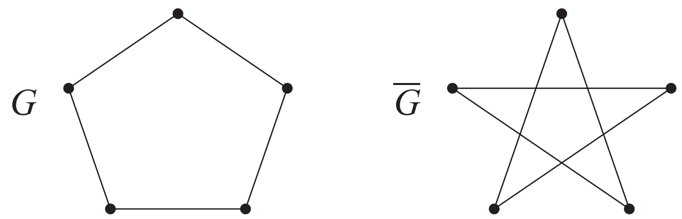
Определение 2.6. *n-мерным кубом* $(n \geqslant 1)$ называется неорграф, множество вершин которого совпадает со множеством $\{0,1\}^n$, и в котором соседними являются любые две вершины, различающиеся ровно в одной компоненте.

Определение 2.7. Графы $G = (V, E)$ и $G' = (V', E')$ называются изоморфными, если существует биекция $\varphi : V \to V'$ такая, что для любого ребра $xy \in E$ всегда $\varphi(x)\varphi(y) \in E'$. Если графы $G = (V, E)$ и $G' = (V', E')$ изоморфны, то пишут $G \simeq G'$.

Изоморфизм двух графов означает, что они могут быть представлены одной фигурой. Понятно, что изоморфизм является отношением эквивалентности, т.е. разбивает множество всех графов на непересекающиеся классы. Поэтому в дальнейшем делать различия между изоморфными графами мы не будем.

Определение 2.8. Если $V' \subseteq V, E' \subseteq E$, то граф $G' = (V', E')$ называется *подграфом* графа $G = (V, E)$.

Определение 2.9. Дополнением графа $G = (V, E)$ называется граф $\overline{G}$, построенный на множестве вершин V с ребрами из множества $[V]^2 \setminus E$, т.е. $\overline{G} = (V, [V]^2 \setminus E)$



В данном случае $G \simeq \overline{G}$.

2.2. Степень вершины

Пусть $G = (V, E)$. Множество вершин, соседних с вершиной v в графе G обозначим через $E(v)$.

Определение 2.10. *Степенью* вершины v называется число $|E(v)|$, т.е. число вершин, инцидентных вершине v. Вершина степени 0 называется *изолированной*. Обозначается степень вершины v графа G через $d_G(v)$ или, если речь идет только о вершинах одного графа, то через $d(v)$.

Определение 2.11. Число $\delta := \min\{d(v) \mid v \in V\}$ называется *минимальной* степенью графа G. Число $\Delta{:=}\max\{d(v) \mid v \in V\}$ называется *максимальной* степенью графа. Обычно употребляются обозначения $\delta(G)$ и $\Delta(G)$.

Определение 2.12. Если все вершины графа G имеют одинаковую степень k, то он называется *k-регулярным*. 3-регулярный граф называется *кубическим*.

Определение 2.13. Число $d(G) = \dfrac{1}{|V|}\sum\limits_{v \in V} d(v)$ называется *средней* степенью графа G.

Очевидно, что

$$\delta(G) \leqslant d(G) \leqslant \Delta(G).$$

Поскольку ребро соединяет две вершины, то очевидно следующее утверждение.

Утверждение 2.2. $|E| = \dfrac{1}{2}\sum\limits_{v \in V} d(v) = \dfrac{1}{2}d(G)|V|$.

Теорема 2.1. *Число вершин нечетной степени в графе всегда четно.*

Доказательство. Предположим, что некоторый граф $G(V, E)$ имеет нечетное число вершин нечетной степени. Тогда сумма степеней всех вершин, которую мы обозначили $\sum\limits_{v \in V} d(v)$, будет нечетным числом. Следовательно, число $\dfrac{1}{2}\sum\limits_{v \in V} d(v)$ не является натуральным и поэтому не может быть равно количеству вершин. Но это противоречит предыдущему утверждению.

Теорема доказана.

2.3. Пути и циклы

Определение 2.14. *Путем* из вершины x_0 в вершину x_k в графе G называется набор $x_0, x_1, \ldots, x_k$, где $x_i \in V$ $(i = \overline{0,k})$ и $x_{j-1}x_j \in E$ $(j = \overline{1,k})$. Число ребер пути называется его *длиной*.

Путь длины k обозначим через p^k. Путь из вершины x_0 в вершину x_k будем задавать последовательностью вершин, т.е $p^k = x_0x_1x_2\ldots x_{k-1}x_k$.

Определение 2.15. Путь $p = x_0x_1\ldots x_{k-1}x_kx_0$ называется *циклом*, если $\forall i, j \in \{0, \ldots, k\}$ из того, что $i \neq j$ всегда следует что $x_i \neq x_j$. *Длиной цикла* называется число его ребер.

Теорема 2.2. *Любой граф G содержит путь длины $\delta(G)$ и цикл длины не менее $\delta(G) + 1$.*

Определение 2.16. *Расстоянием* $\rho_G(x, y)$ между вершинами x и y в графе G называется длина кратчайшего пути из x в y. Если пути из x в y не существует, то пишут $\rho_G(x, y) := \infty$.

Определение 2.17. Наибольшее расстояние между двумя произвольными вершинами графа G называется *диаметром* графа G, и обозначается $\mathrm{diam}\,(G)$.

Определение 2.18. Вершина называется *центральной*, если ее максимальное расстояние до любой вершины минимально. это расстояние называется *радиусом* и обозначается $\mathrm{rad}\,(G)$.

Утверждение 2.3. *Справедлива следующая формула:*

$$\mathrm{rad}\,(G) \leqslant \dim(G) \leqslant 2\mathrm{rad}\,(G).$$

Определение 2.19. *Маршрутом длины k* в графе G называется непустая чередующаяся последовательность $v_0e_0v_1e_1\ldots e_{k-1}v_k$ вершин и ребер в G таких, что $\forall k$ $e_i = \{v_iv_{i+1}\}$. Если $v_0 = v_k$, то маршрут называется *замкнутым*. Если все вершины в маршруте различны, то он есть путь.

2.4. Деревья, двудольные графы и эйлеровы циклы

Определение 2.20. Непустой граф G называется *связным*, если любые две его вершины связаны путем в G.

Определение 2.21. Граф, не содержащий циклов, называется *лесом*. Связный лес называется *деревом*. Вершины степени 1 в дереве называются *листьями*.

Теорема 2.3. *Следующие утверждения эквивалентны для графа T:*

1) T — *дерево;*

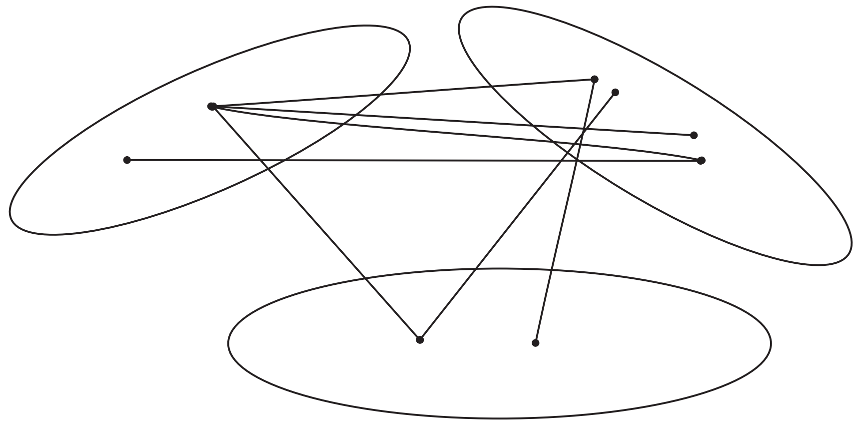
2) *любые вершины связаны единственным путем;*

3) $\forall e \in T$ *граф* T *связен, а* $T \setminus e$ *не связен;*

4) *граф* T *не содержит циклов, но граф* $T+XY$ *содержит цикл для любых двух вершин* X, Y *графа* T, *которые не являются инцидентными.*

Теорема 2.4. *Связанный граф на* n *вершинах является деревом тогда и только тогда, когда он содержит* $n-1$ *число ребер.*

Определение 2.22. Пусть $r \in \mathbb{Z}_+ \setminus \{0, 1\}$. Граф $G = (V, E)$ называется *r-дольным*, если множество V можно разбить на r классов так, что каждое ребро имеет свои концевые вершины в разных классах. Если $r = 2$, то граф называется *двудольным.*



3-дольный граф

Определение 2.23. r-дольный граф в котором любые две вершины разных классов смежны, называется *полным.*

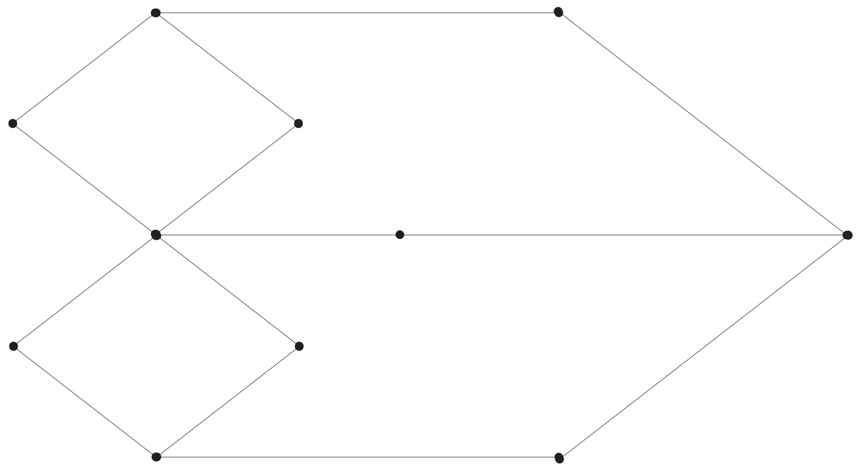
Теорема 2.5. *(Теорема Кёнига) Граф является двудольным тогда и только тогда, когда он не содержит циклов нечетной длины.*

Определение 2.24. Замкнутый маршрут в графе называется *эйлеровым циклом,* если он проходит через каждое ребро графа ровно один раз. Граф называется *эйлеровым,* если он содержит эйлеровый цикл.

Эйлеровы графы были открыты Эйлером при решении знаменитой задачи о Кёнигсбергских мостах.

Теорема 2.6. *Связный граф является эйлеровым тогда и только тогда, когда каждая вершина графа имеет четную степень.*

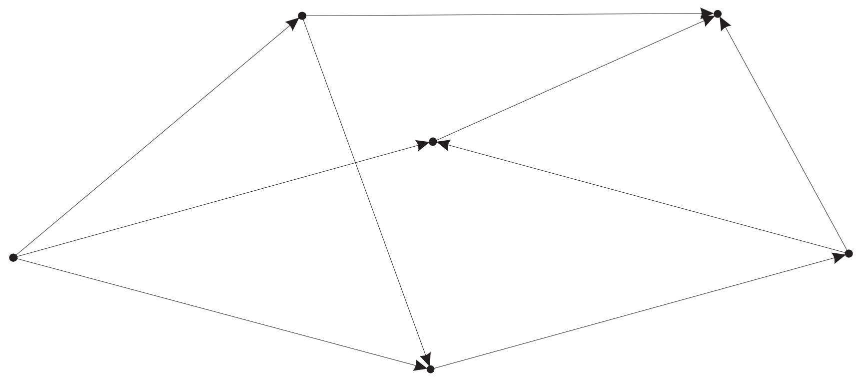
Определение 2.25. *Ориентированным* графом или *орграфом* называется пара (V, R), где $V \neq \varnothing$, а $R \subseteq (V)^2$ (где $(V)^2$ — множество



Граф для решения задачи
о Кёнигсбергских мостах

всех возможных упорядоченных 2-х элементных выборок из множества V. Элементы множества V называются *вершинами*, а элементы множества R называются *дугами* или *ориентированными ребрами.*

При геометрическом изображении графа в пространстве (или на плоскости), дуга, которая соединяет вершину v с вершиной w представляется отрезком со стрелкой, направленной от v к w.



3. Булевы функции и их свойства

3.1. Элементарные булевы функции

Определение 3.1. Функция $f : B^n \to B$, где $B = \{0, 1\}$ называется *булевой функцией* или *функцией алгебры логики.*

Аргументы булевых функций берутся из некоторого множества $U = \{u_1, u_2, \ldots, u_m, \ldots\}$. Например, запись $f(u_1, u_2, \ldots, u_n)$ означает булеву функцию от n аргументов. Элементы из множества U будем обозначать буквами $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n, x, y, z$. Различные буквы при этом обозначают различные элементы.

Пусть $x_1, x_2, \ldots, x_n$ — некоторые аргументы (переменные) из множества U. Тогда каждая из этих переменных принимает значение из множества $\{0, 1\}$. Поэтому говорят о *наборах значений переменных*, которые являются упорядоченными n-элементными выборками с возвращением из множества $\{0, 1\}$.

Переменные $x_1, x_2, \ldots, x_n$ называют еще *пропозициональными* или *пропозиционными.*

Если $f(x_1, x_2, \ldots, x_n)$ — булева функция и $(a_1, a_2, \ldots, a_n)$ — некоторая выборка из B^2, то $f(a_1, a_2, \ldots, a_n)$ есть *значение этой функции на наборе* $(a_1, a_2, \ldots, a_n)$, если это значение на указанном наборе определено (может быть и противное).

Обозначим через P_2 множество *всех всюду определенных булевых функций*, а через $P_2^{(n)}$ обозначим *множество всех булевых функций от n аргументов* $(n \geqslant 1)$.

Будем писать $\tilde{x}^n = (x_1, x_2, \ldots, x_n)$ и называть это выражение *векторным заданием аргумента.*

Булеву функцию можно задавать с помощью таблицы в которой в первых n столбцах стоят все возможные наборы значений переменных, а в $n+1$ столбце — значения самой булевой функции. Наборы значений переменных принято располагать в так называемом естественном порядке.

x_1	x_2	x_3	$\cdots$	x_{n-2}	x_{n-1}	x_n	$f(\tilde{x}^n)$
0	0	0	$\cdots$	0	0	0	a_1
0	0	0	$\cdots$	0	0	1	a_2
0	0	0	$\cdots$	0	1	0	a_3
$\ldots$	$\ldots$	$\ldots$	$\ddots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	1	1	$\cdots$	1	0	1	a_{2^n-2}
1	1	1	$\cdots$	1	1	0	a_{2^n-1}
1	1	1	$\cdots$	1	1	1	a_{2^n}

Рассмотрим пример конкретной булевой функции от 3-х аргументов.

x_1	x_2	x_3	$f(\tilde{x}^3)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Соглашение о задании значений переменных в естественном порядке позволяет использовать более компактное векторное задание булевой функции. Так, в рассмотренном примере, $f(\tilde{x}^3) = (11010110)$.

Теорема 3.1 (О числе различных булевых функций от n аргументов.). $|P_2^{(n)}| = 2^{2^n}$.

Доказательство. Число всевозможных упорядоченных выборок с возвращением из двух элементов по n-элементов (т.е. число всевозможных упорядоченных строк таблицы истинности), согласно утверждению 6) теоремы 1.1, равно 2^n. Для каждой строки таблицы истинности возможен один из случаев — либо в этой строке функция имеет значение 1, либо ее значение в этой строке равно 0. Следовательно, для каждого из наборов значений переменных снова происходит выбор из двухэлементного множества. Поэтому, опять применив утверждение 6) теоремы 1.1, получим, что число различных булевых функций от n аргументов равно 2^{2^n}.

Теорема доказана.

Определение 3.2. Булева функция $f(x_1, x_2, \ldots, x_n)$ *существенно зависит* от переменной x_i $(i = 1, 2, \ldots, n)$, если существует такой набор $(a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ значений переменных $x_1, x_2, \ldots$

$\ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, что

$$f(a_1, a_2, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq$$
$$f(a_1, a_2, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Эта переменная x_i называется *существенной*. Переменная которая не является существенной называется *фиктивной*.

Определение 3.3. Пусть булева функция $f(\tilde{x}^n)$ задана таблично и для некоторого $i = \overline{1, n}$ переменная x_i является ее фиктивной переменной. Вычеркивание из этой таблицы всех строк, которые соответствуют наборам $(a_1, a_2, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n)$, где $(a_1, a-2, \ldots, a_{i-1}, a_{i+1}, \ldots$ $\ldots, a_n)$ — некоторые наборы переменных $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ и столбца в котором стоит переменная x_i, задает булеву функцию $f_1(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ от $n-1$ переменных. Такое вычеркивание называется *удалением фиктивной переменной* x_i.

Определение 3.4. Операция, обратная операции удаления фиктивной переменной называется *операцией введения фиктивной переменной*.

Определение 3.5. Две булевы функции называются *равными*, если одна из них может быть получена из другой, путем удаления или введения фиктивных переменных.

Поскольку мы рассмотрели операции удаления и введения фиктивных переменных, то следующее утверждение является очевидным.

Замечание 3.1. *Любое множество булевых функций $f_1, f_2, \ldots, f_s$ можно рассматривать как множество функций зависящих от одних и тех же переменных.*

Определение 3.6. *Элементарными булевыми функциями* называются функции, заданные с помощью следующих таблиц.

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

x	y	$x \wedge y$	$x \vee y$	$x \Rightarrow y$	$x \Leftrightarrow y$	$x \oplus y$
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	0

x — *тождественная функция*;
$\bar{x}$ — *отрицание*;
0 — *константа* 0;
1 — *константа* 1;
$x \wedge y$ — *конъюнкция*;
$x \vee y$ — *дизъюнкция*;
$x \Rightarrow y$ — *импликация* (x — *посылка*, y — *заключение*);

$x \Leftrightarrow y$ — *эквиваленция*;

$x \oplus y$ — *сумма по модулю* 2.

Вместо $x \wedge y$ будем употреблять всюду, где возможно, запись xy.

3.2. Свойства элементарных булевых функций

Через F обозначим некоторое непустое множество булевых функций, а через F_0 — множество элементарных булевых функций.

Определение 1.6 (Индуктивное определение формулы над множеством F булевых функций). Каждая функция $f(\tilde{x}^n)$ из множества F называется *формулой* над F.

Если $f(x_1, x_2, \ldots, x_n) \in F$ и $A_1, A_2, \ldots, A_n$ — формулы над F или переменные из множества U, то выражение $f(A_1, A_1, \ldots, A_n)$ называется *формулой* над F.

Пример 3.1. $x \vee y$ и $y \vee (x \oplus z)$ — формулы; $x_1 \vee \wedge\, x_2$, $\vee(x_1 \Rightarrow x_2)$ — не формулы.

Если A и B — некоторые формулы и $f(A, B) \in F_0$, то говорят, что к формулам A и B применена операция булевой алгебры. Таким образом, в множество операций булевой алгебры входят элементарные булевы функции: дизъюнкция, конъюнкция, импликация, эквиваленция, сумма по модулю 2. Кроме этих операций в булевой алгебре существуют еще две операции, которые так же являются элементарными булевыми функциями, но применимы только к одной формуле — взятие отрицания: $\bar{A}$ и тождественная операция: A.

Иногда вместо записи $\bar{A}$ используется запись $\rceil A$. Это обозначение оказывается особенно удобным, если отрицание применяется к большой формуле, либо отрицаний достаточно много. Особенно удобным такое обозначение оказывается при составлении таблиц истинности.

Как в алгебре существует закон старшинства операций, так в булевых функциях существуют правила раскрытия скобок: $((((\rceil)\ \wedge)\ \vee)\ \Rightarrow)\ \Leftrightarrow$. Для операции $\oplus$ правило раскрытия скобок можно определить так: $((((\rceil)\ \wedge)\ \vee)\ \Rightarrow)\ \oplus$.

Если при построении формулы А используются только функции $f_1, f_2, \ldots f_n$, то пишут $A[f_1, f_2, \ldots f_n]$.

Если при построении формулы А используются только переменные $x_1, x_2, \ldots x_n$, то пишут $A[x_1, x_2, \ldots x_n]$.

Определение 3.7. Формулы, которые используются в построении данной формулы называются ее *подформулами*.

Определение 3.8. Каждой формуле $A(x_1, x_2, \dots x_n)$ над множеством F можно сопоставить булеву функцию $f(x_1, x_2, \dots, x_n)$ по правилу: для каждого набора $(a_1, a_2, \dots, a_n)$ значений переменных $x_1, x_2, \dots$ $\dots, x_n$ по определению полагается $f(x_1, x_2, \dots, x_n) = A(a_1, a_2, \dots, a_n)$. Такую функцию $f(\tilde{x}^n)$ называют *суперпозицией функций* из множества F.

Говорят также, что формула $A(x_1, x_2, \dots, x_n)$ реализует некоторую булеву функцию $f(\tilde{x}^n)$. Эту функцию для A будем обозначать f_A.

Определение 3.9. Формулы A и B называют *эквивалентными*, если $f_A = f_B$, при этом пишут $A = B$.

Свойство 3.1. *Справедливы следующие утверждения:*

1. Ассоциативные законы:

1.1. $(x \wedge y) \wedge z = x \wedge (y \wedge z)$;

1.2. $(x \vee y) \vee z = x \vee (y \vee z)$;

1.3. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$;

2. Коммутативные законы:

2.1. $x \wedge y = y \wedge x$;

2.2. $x \vee y = y \vee x$;

2.3. $x \oplus y = y \oplus x$;

3. Дистрибутивные законы:

3.1. $x(y \vee z) = xy \vee xz$;

3.2. $x \vee yz = (x \vee y)(x \vee z)$;

3.3. $x(y \oplus z) = xy \oplus xz$.

4. Свойства операций $\urcorner, \wedge, \vee$:

4.1. Закон двойного отрицания: $\overline{\overline{x}} = x$;

4.2. $x \wedge x = x \vee x = x$;

Законы Де-Моргана:

4.3. $\overline{x \vee y} = \overline{x} \wedge \overline{y}$;

4.4. $\overline{x \wedge y} = \overline{x} \vee \overline{y}$.

5. Свойства констант:

$x\overline{x} = 0$; $\quad x \vee \overline{x} = 1$; $\quad x \oplus x = 0$;

$x0 = 0$; $\quad x \vee 1 = 1$; $\quad x \oplus 0 = x$;

$x1 = x$; $\quad x \vee 0 = x$; $\quad x \oplus 1 = \overline{x}$.

6. Выражение $\oplus$, $\Rightarrow$, $\Leftrightarrow$ *через* $\urcorner$, $\vee$, $\wedge$:

$$x \oplus y = x\overline{y} \vee \overline{x}y; \quad x \Leftrightarrow y = xy \vee \overline{x}\,\overline{y};$$
$$x \Rightarrow y = \overline{x} \vee y; \quad x \Leftrightarrow y = (x \vee \overline{y})(\overline{x} \vee y).$$

Доказательство. Доказательство всех утверждений проводится прямой проверкой с использованием таблиц истинности.

Определение 3.10. Для $n \geqslant 1$ определим следующие операции:

$\bigwedge\limits_{i=1}^{n} x_i = x_1 \wedge x_2 \wedge \ldots \wedge x_n$ — логическое произведение;

$\bigvee\limits_{i=1}^{n} x_i = x_1 \vee x_2 \vee \ldots \vee x_n$ — логическая сумма;

$\bigoplus\limits_{i=1}^{n} x_i = x_1 \oplus x_2 \oplus \ldots \oplus x_n.$

Свойство 3.2. *Если A — некоторая формула и A' — некоторая ее подформула, то при замене некоторых вхождений A' в формулу A на B', которая эквивалентна A', мы получим формулу B, эквивалентную A.*

С помощью этого свойства легко доказать следующие свойства:

Свойство 3.3. *Справедливы следующие правила:*

1. $x \vee xy = x$ *— правило поглощения конъюнкции;*
2. $x(x \vee y) = x$ *— правило поглощения дизъюнкции;*
3. $xy \vee x\overline{y} = x$ *— правило склеивания;*

Свойство 3.4. *Имеют место следующие равенства:*

$0 \Rightarrow x = 1$;

$1 \Rightarrow x = x$;

$x \Rightarrow 0 = \overline{x}$;

$x \Rightarrow 1 = 1$;

Доказательство проводится с помощью свойства 3.3 или таблиц истинности.

Определение 3.11. Формула A называется *тавтологией*, если при любом наборе истинностных значений ее переменных она принимает значение 1, т.е. $f_A = 1$.

Если A — тавтология, то будем писать: $\models A$.

Определение 3.12. Формула A называется *противоречием*, если для любого набора истинностных значений ее переменных она принимает значение 0, т.е. $f_A = 0$.

Если A — противоречие, то будем писать $\models \overline{A}$.

Теорема 3.2. *Формула A равна B тогда и только тогда, когда $\models A \Leftrightarrow B$.*

Доказательство. Если $A = B$, то $f_A = f_B$. Значит, $f_A = f_B$ для любого набора значений переменных. Следовательно, $\models f_A \Leftrightarrow f_B$ и поэтому $\models A \Leftrightarrow B$.

Если $\models A \Leftrightarrow B$, то для любого набора значений переменных $f_A = f_B$ и, значит, $A = B$.

Теорема доказана.

Понятия формулы, эквивалентной формулы и суперпозиции булевых функций позволяют использовать свойства элементарных булевых функций для получения формулы, которая равносильна данной (т.е. реализует ту же функцию), но имеет более простое строение. Такие действия называются *равносильными преобразованиями.*

3.3. Принцип двойственности

Определение 3.13. Булева функция $f^*(\tilde{x}^n) = \overline{f}(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n)$ называется *двойственной* к булевой функции $f(\tilde{x^n})$.

Используя таблицы истинности легко убедиться, что 0 двойственна к 1; 1 двойственна к 0; x двойственна к x; $\overline{x}$ двойственна к $\overline{x}$; $\wedge$ двойственна к $\vee$; $\vee$ двойственна к $\wedge$.

Теорема 3.3. *Для любой булевой функции $f(\tilde{x}^n)$ имеет место следующее равенство $(f^*)^* = f$.*

Доказательство.

$$(f^*)^*(\tilde{x}^n) = \overline{f}^*(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n) =$$

$$\overline{\overline{f}}(\overline{\overline{x}}_1, \overline{\overline{x}}_2, \ldots, \overline{\overline{x}}_n) = f(x_1, x_2, \ldots, x_n) = f(\tilde{x}^n).$$

Теорема доказана.

Теорема 3.4 (О двойственной функции). *Если*

$$\Phi(\tilde{x}^n) = f(f_1(\tilde{x}^n), f_2(\tilde{x}^n), \ldots, f_k(\tilde{x}^n)),$$

то

$$\Phi^*(\tilde{x}^n) = f^*(f_1^*(\tilde{x}^n), f_2^*(\tilde{x}^n), \ldots, f_k^*(\tilde{x}^n)).$$

Доказательство.

$$\Phi^*(\tilde{x}^n) = \Phi^*(x_1, x_2, \ldots, x_n) = \overline{\Phi}(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n) =$$

$$\overline{f}(f_1(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n), f_2(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n), \ldots \overline{f}_m(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n)) =$$

$$= \overline{f}(\overline{\overline{f}}_1(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n), \overline{\overline{f}}_2(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n), \ldots \overline{\overline{f}}_k(\overline{x_1}, \overline{x}_2, \ldots, \overline{x}_n)) =$$

$$\overline{f}(\overline{f}_1^*(\tilde{x}^n), \ldots, \overline{f}_m^*(\tilde{x}^n)) = f^*(f_1^*(\tilde{x}^n), \ldots, f_m^*(\tilde{x}^n)).$$

Теорема доказана.

Свойство 3.5 (Принцип двойственности). *Если формула $A[f_1, f_2, \ldots, f_s]$ реализует булеву функцию $f(\tilde{x}^n)$, то формула $A[f_1^*, f_2^*, \ldots$ $\ldots, f_s^*]$ реализует $f^*(\tilde{x_n})$.*

Определение 3.14. Формула $A[f_1^*, f_2^*, \ldots, f_n^*]$ называется *двойственной* к формуле $A[f_1^*, f_2^*, \ldots, f_n^*]$. При этом пишут $A^* = A[f_1^*, f_2^*, \ldots \ldots, f_s^*]$.

Если $F = \{0, 1, x, \overline{x}, xy, x \vee y\}$, то для формулы над F принцип двойственности заключается в том, чтобы заменить всюду в данной конкретной формуле A каждую операцию на операцию, ей двойственную и тогда мы получим A^*.

Свойство 3.6. *Если $A = B$, то $A^* = B^*$.*

Доказательство. Следует из того, что $f_A = f_B$ (по определению эквивалентности формул).

Таким образом, принцип двойственности позволяет в два раза сократить доказательства тождеств, построенных на двойственных операциях. Действительно, доказав некоторое тождество A, мы получим после замены операций на двойственные, новое тождество.

3.4. Разложения булевых функций

Пусть $a \in B = \{0; 1\}$. Определим выражение x^a следующим образом: $x^a = xa \vee \overline{x}\,\overline{a}$. Тогда, очевидно, что

$$x^a = \begin{cases} x, & \text{если } a = 1, \\ \overline{x}, & \text{если } a = 0. \end{cases}$$

Непосредственно из определения выражения x^a, следует утверждение.

Лемма 3.1. *$x^a = 1$ тогда и только тогда, когда $x = a$.*

Теорема 3.5 (О дизъюнктивном разложении БФ). *Для любого $k = 1, 2, \ldots, n$ и для любой булевой функции $f(\tilde{x}^n)$ справедливо следующее равенство*

$$f(\tilde{x}^n) = \bigvee_{(a_1, a_2, \ldots, a_k)} x_1^{a_1} x_2^{a_2} \ldots x_k^{a_k} f(a_1, a_2, \ldots, a_k, x_{k+1}, \ldots, x_n),$$

где дизъюнкция берется по всем возможным наборам $(a_1, a_2, \ldots \ldots, a_k)$ значений переменных $x_1, x_2, \ldots, x_k$.

Доказательство. Пусть $(b_1, b_2, \ldots, b_n)$ — произвольный набор значений переменных $x_1, x_2, \ldots, x_n$. Тогда в левой части доказываемого равенства получаем $f(b_1, b_2, \ldots, b_n)$. Правая часть принимает вид

$$\bigvee_{a_1, a_2, \ldots, a_k} {b_1}^{a_1} {b_2}^{a_2} \ldots {b_k}^{a_k} f(a_1, a_2, \ldots, a_k, b_{k+1}, \ldots, b_n).$$

Если хотя бы для одного $i = 1, 2, \dots, k$, $a_i \neq b_i$, то, по лемме 3.1, $b_i^{a_i} = 0$. В этом случае вся дизъюнкция равна 0. Если же $\forall i = 1, 2, \dots, k$ всегда $b_i = a_i$, то в правой части получим $f(b_1, b_2, \dots, b_k, b_{k+1}, \dots, b_n) = f(b_1, b_2, \dots, b_n)$, т.е. то же что и в левой части. Ввиду произвольности выбора переменных и наборов их значений, равенство выполняется всегда.

Теорема доказана.

Свойство 3.7. *Для любой булевой функции $f(\tilde{x}^n)$ справедливы следующие равенства:*

$$f(\tilde{x}^n) = x_n f(\tilde{x}^{n-1}, 1) \vee \overline{x}_n f(\tilde{x}^{n-1}, 0) \tag{3.1}$$

$$f(\tilde{x}^n) = \bigvee_{a_1, a_2, \dots, a_n} x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} f(a_1, a_2, \dots, a_n) \tag{3.2}$$

Если $f(\tilde{x}^n)$ не является противоречием, то

$$f(\tilde{x}^n) = \bigvee_{\substack{(a_1, a_2, \dots, a_n) \\ f(a_1, a_2, \dots, a_n) = 1}} x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} \tag{3.3}$$

Доказательство. Воспользуемся предыдущей теоремой. Возьмём только одну переменную — x_n. Для нее возможно только два набора — (1) и (0). Если x_n имеет значение 1, то $x_n^a = x_n$ и поэтому дизъюнктивный член будет равен $x_n f(\tilde{x}^{n-1}, 1)$, а, если x_n имеет значение 0, то $x_n^a = \overline{x}_n$ и поэтому дизъюнктивный член будет равен $\overline{x}_n f(\tilde{x}^{n-1}, 0)$. Равенство (3.3) доказано.

Равенство (5.1) так же следует из предыдущей теоремы, если $k = n$.

Рассмотрим равенство (5.1). Если на данном наборе $(a_1, a_2, \dots, a_n)$ переменных $x_1, x_2, \dots, x_n$ мы получаем, что $f(a_1, a_2, \dots, a_n) = 0$, то весь дизъюнктивный член имеет значение 0 (как конъюнкция некоторого числа булевых функций, одна из которых имеет значение 0). Поэтому, по свойству константы 0, этот дизъюнктивный член исключается. Следовательно, перебрав все наборы переменных, мы исключим все те дизъюнктивные члены, которые соответствуют наборам, обращающим функцию $f(\tilde{x}_n)$ в ноль. Значит, останутся только те наборы $(a_1, a_2, \dots, a_n)$ для которых $f(a_1, a_2, \dots, a_n) = 1$, т.е. мы получим равенство (5.2).

Свойство доказано.

Определение 3.15. Равенство

$$f(\tilde{x}^n) = x_n f(\tilde{x}^{n-1}, 1) \vee \overline{x}_n f(\tilde{x}^{n-1}, 0)$$

называют *разложением булевой функции по переменной.*

Определенное выше разложение по переменной оказывается полезным, когда какие-либо свойства булевых функций устанавливаются по индукции.

Определение 3.16. Если булева функция $f(\tilde{x}^n)$ не является противоречием, то выражение

$$f(\tilde{x}^n) = \bigvee_{\substack{(a_1,a_2,\ldots,a_n)\\ f(a_1,a_2,\ldots,a_n)=1}} x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$$

называют ее *совершенной дизъюнктивной нормальной формой* (*СДНФ*).

Пусть булева функция $f(\tilde{x}^n)$ не является тавтологией. Тогда, поскольку константа 1 двойственна константе 0, то функция $f^*(\tilde{x}_n)$ не является противоречием. Следовательно, для функции $f^*(\tilde{x}_n)$ можно построить СДНФ:

$$f^*(\tilde{x}^n) = \bigvee_{\substack{(a_1,a_2,\ldots,a_n)\\ f^*(a_1,a_2,\ldots,a_n)=1}} x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}.$$

Воспользуемся теперь результатами, полученными выше:

$$f(\tilde{x}^n) = (f^*(\tilde{x}^n))^* = \left(\bigvee_{\substack{(a_1,a_2,\ldots,a_n)\\ f^*(a_1,a_2,\ldots,a_n)=1}} x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} \right)^* =$$

$$= \left(\bigvee_{\substack{(a_1,a_2,\ldots,a_n)\\ \overline{f}^(\overline{a}_1,\overline{a}_2,\ldots,\overline{a}_n)=1}} x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} \right)^* = \left[\begin{array}{c} \text{Воспользуемся} \\ \text{принципом} \\ \text{двойственности} \end{array} \right] =$$

$$\bigwedge_{\substack{(a_1,a_2,\ldots,a_n)\\ \overline{f}(\overline{a}_1,\overline{a}_2,\ldots,\overline{a}_n)=1}} (x_1^{a_1} \vee x_2^{a_2} \ldots \vee x_n^{a_n}) =$$

$$\bigwedge_{\substack{(a_1,a_2,\ldots,a_n)\\ f(\overline{a}_1,\overline{a}_2,\ldots,\overline{a}_n)=0}} (x_1^{a_1} \vee x_2^{a_2} \vee \ldots \vee x_n^{a_n}) =$$

$$\left[\begin{array}{c} \text{заменим теперь} \\ a_i \text{ на } \overline{a}_i \ (i = \overline{1,n}) \end{array} \right] = \bigwedge_{\substack{(a_1,a_2,\ldots,a_n)\\ f(a_1,a_2,\ldots,a_n)=0}} \left(x_1^{\overline{a}_1} \vee x_2^{\overline{a}_2} \vee \ldots \vee x_n^{\overline{a}_n} \right).$$

Использованная выше замена возможна по той причине, что выражение $(a_1, a_2, \ldots, a_n)$ в данном случае означает просто некоторый набор.

Определение 3.17. Если булева функция $f(\tilde{x}^n)$ не является тавтологией, то выражение

$$f(\tilde{x}^n) = \bigwedge_{\substack{a_1, a_2, \ldots, a_k \\ f(a_1, a_2, \ldots, a_n) = 0}} (x_1^{\overline{a}_1} \vee x_2^{\overline{a}_2} \vee \ldots \vee x_n^{\overline{a}_n})$$

называется ее *совершенной конъюнктивной нормальной формой* (*СКНФ*)

СДНФ и СКНФ можно определить индуктивно.

Определение 3.18. *Элементарной конъюнкцией* называется конъюнкция некоторого числа переменных и отрицаний переменных из множества $U = \{u_1, u_2, \ldots, u_m, \ldots\}$, причем для любой переменной указанного множества в этой конъюнкции может присутствовать либо сама переменная, либо ее отрицание. Любая переменная или ее отрицание так же является элементарной конъюнкцией.

Определение 3.19. *Элементарной дизъюнкцией* называется дизъюнкция некоторого числа переменных и отрицаний переменных из множества $U = \{u_1, u_2, \ldots, u_m, \ldots\}$, причем для любой переменной указанного множества в этой дизъюнкции может присутствовать либо сама переменная, либо ее отрицание. Любая переменная или ее отрицание так же является элементарной дизъюнкцией.

Определение 3.20. *Конъюнктивной нормальной формой* (*КНФ*) называется всякая элементарная дизъюнкция, либо конъюнкция некоторого числа элементарных дизъюнкций.

Определение 3.21. *Дизъюнктивной нормальной формой* (*ДНФ*) называется всякая элементарная конъюнкция, либо дизъюнкция некоторого числа элементарных конъюнкций.

Определение 3.22. *Совершенной конъюнктивной нормальной формой* (*СКНФ*) называется всякая КНФ, в каждую элементарную дизъюнкцию которой всякая переменная либо ее отрицание входит ровно 1 раз, если эта переменная либо ее отрицание, входит в какую-либо другую элементарную дизъюнкцию этой СКНФ.

Определение 3.23. *Совершенной дизъюнктивной нормальной формой* (*СДНФ*) называется всякая ДНФ, в каждую элементарную конъюнкцию которой всякая переменная либо ее отрицание входит ровно 1 раз, если эта переменная либо ее отрицание, входит в какую-либо другую элементарную конъюнкцию этой СКНФ.

Определение 3.24. Для произвольной элементарной конъюнкции всякий ее элемент (т.е. некоторая переменная, либо отрицание некоторой переменной) называется ее *множителем.*

Непосредственно из теорем 3.4 и 3.5, а так же из (3.1) следует утверждение

Теорема 3.6. *Всякая булева функция, отличная от константы, имеет единственные СДНФ и СКНФ, но может иметь несколько ДНФ и КНФ.*

Теорема 3.7. *Для любой булевой функции $f(\tilde{x}^n)$ справедливо равенство:*

$$f(\tilde{x}^n) = (x_1 \Rightarrow \rceil f(1, x_2, \ldots, x_n)) \Rightarrow \rceil (\overline{x}_1 \Rightarrow \rceil f(0, x_2, \ldots, x_n)).$$

Доказательство. Пусть $f(\tilde{x}^n)$ — произвольная булева функция. Для переменной x_1 возможны два случая: $x_1 = 1$ и $x_1 = 0$.

Если $x_1 = 1$, то доказываемое равенство принимает вид:

$$f(\tilde{x}^n) = (1 \Rightarrow \rceil f(1, x_2, \ldots, x_n)) \Rightarrow \rceil (0 \Rightarrow \rceil f(0, x_2, \ldots, x_n)).$$

Импликация, стоящая в последних скобках по определению имеет значение 1. Поэтому заключение импликации, которая выполняется последней имеет значение 0. Следовательно, равенство принимает вид:

$$f(\tilde{x}^n) = (1 \Rightarrow \rceil f(1, x_2, \ldots, x_n)) \Rightarrow 0.$$

Используя теперь выражение импликации через дизъюнкцию и отрицание, получим:

$$f(\tilde{x}^n) = \rceil (0 \vee \rceil f(1, x_2, \ldots, x_n);$$
$$f(\tilde{x}^n) = \rceil \rceil f(1, x_2, \ldots, x_n);$$
$$f(\tilde{x}^n) = f(1, x_2, \ldots, x_n).$$

Но т.к. $x_1 = 1$ то равенство справедливо.

Случай $x_1 = 0$ доказывается аналогично:

$$f(\tilde{x}^n) = (0 \Rightarrow \rceil f(1, x_2, \ldots, x_n)) \Rightarrow \rceil (1 \Rightarrow \rceil f(0, x_2, \ldots, x_n));$$
$$f(\tilde{x}^n) = 1 \Rightarrow \rceil (1 \Rightarrow \rceil f(0, x_2, \ldots, x_n));$$
$$f(\tilde{x}^n) = 0 \vee \rceil (1 \Rightarrow f(0, x_2, \ldots, x_n));$$
$$f(\tilde{x}^n) = \rceil (0 \vee f(0, x_2, \ldots, x_n));$$
$$f(\tilde{x}^n) = \rceil \rceil (f(0, x_2, \ldots, x_n));$$
$$f(\tilde{x}^n) = f(0, x_2, \ldots, x_n)$$

Теорема доказана.

Пусть выражение $\underset{1 \leqslant i \leqslant n}{\rightarrow} A_i$ обозначает формулу

$$A_1 \Rightarrow (A_2 \Rightarrow (\ldots (A_{n-1} \Rightarrow \overline{A}_n) \ldots)).$$

частный случай этой формулы при $n = 1$ есть $\overline{A}_1$.

Утверждение теоремы 3.7 в этих обозначениях принимает вид:

$$f(\tilde{x}^n) \underset{v_1 \in \{1,0\}}{\underset{v_1}{\rightarrow}} (x_1^{v_1} \Rightarrow \rceil (f(v_1, x_2, \ldots, x_n)) .$$

Свойство 3.8. *Для любой булевой функции $f(\tilde{x}^n)$ и для любого $k = 1, \ldots, n$, справедливо следующее равенство:*

$$f(\tilde{x}^n) = \underset{v_i \in \{0,1\},\ i=\overline{1,k}}{\underset{v_1,\ldots,v_k}{\rightarrow}} (x_1^{v_1} \Rightarrow (x_2^{v_2} \Rightarrow (\ldots$$

$$\ldots (x_k^{v_k} \Rightarrow \rceil f(v_1, v_2, \ldots, v_k, x_{k+1}, \ldots, x_n)) \ldots))).$$

Если же $f(\tilde{x}^n)$ не является противоречием и $k = n$, то справедливо равенство

$$f(\tilde{x}^n) = \underset{f(v_1,v_2,\ldots,v_n)=1}{\underset{(v_1,v_2\ldots,v_n)}{\rightarrow}} (x_1^{v_1} \Rightarrow (x_2^{v_2} \Rightarrow (\ldots (x_{n-1}^{v_{n-1}} \Rightarrow \overline{x}_n^{v_n}) \ldots))).$$

Доказательство. Доказательство заключается в том, что бы использовать теорему 3.7 k раз.

Определение 3.25. Если булева функция $f(\tilde{x}^n)$ не является противоречием, то выражение

$$f(\tilde{x}^n) = \underset{f(v_1,v_2,\ldots,v_n)=1}{\underset{(v_1,v_2,\ldots,v_n)}{\rightarrow}} (x_1^{v_1} \Rightarrow (x_2^{v_2} \Rightarrow (\ldots (x_{n-1}^{v_{n-1}} \Rightarrow \overline{x}_n^{v_n}) \ldots))).$$

называется ее *совершенной импликативной нормальной формой* (*СИНФ*).

Определение 3.26. *Полиномом по модулю 2 (полиномом Жегалкина) от n переменных $x_1, x_2, \ldots, x_n$* называется выражение, которое записывается следующим образом:

$$\bigoplus_{i_1,i_2,\ldots,i_s} a_{i_1,i_2,\ldots,i_s} x_{i_1} x_{i_2} \ldots x_{i_s},$$

где сумма берется по всевозможным подмножествам индексов из множества $1, 2, \ldots, n$, $a_{i_1 \ldots i_s} \in B$.

Теорема 3.8 (Жегалкина). *Каждая булева функция может быть задана полиномом по модулю 2 и при том единственным образом.*

Доказательство. Очевидно, что полином Жегалкина — это булева функция. Число произведений $x_{i_1} x_{i_2} \ldots x_{i_s}$ равно количеству всех возможных подмножеств из n-элементного множества, т.е. 2^n, а так как $a_{i_1,i_2,\ldots,i_s} \in \{0, 1\}$, то искомое число полиномов равно 2^{2^n}, т.е. числу булевых функций от тех же переменных. Отсюда следует к тому же и единственность.

Теорема доказана.

Полином Жегалкина можно рассматривать, как разложение булевой функции над базисом $\{\wedge, \oplus\}$.

4. Дизъюнктивные нормальные формы булевых функций

4.1. Проблема минимизации дизъюнктивных нормальных форм булевых функций

Изучая булевы функции, мы убедились, что всякая булева функция имеет несколько дизъюнктивных нормальных форм. В связи с этим возникает проблема нахождения дизъюнктивных нормальных форм более простого вида. Причем оказывается, что найти дизъюнктивную нормальную форму простого вида гораздо труднее, чем построить совершенную дизъюнктивную нормальную форму. Для того, чтобы для каждой конкретной булевой функции можно было однозначно определить, является ли одна дизъюнктивная нормальная форма более простой, чем другая, используется понятие индекса простоты.

Определение 4.1. Индексом простоты дизъюнктивной нормальной формы K называется некоторое число из множества $\{0\} \cup \mathbb{N}$, которое обозначается $L(K)$ и удовлетворяет следующим аксиомам:

1. Аксиома неотрицательности: для любой дизъюнктивной нормальной формы K, $L(K) \geqslant 0$.

2. Аксиома монотонности: если $K = K_1 V x_i^{\sigma_i} K_2$, то $L(K) \geqslant L(K_1) + L(K_2)$.

3. Аксиома выпуклости: если $K = K_1 \vee K_2$ и $K_1 \wedge K_2 = 0$, то $L(K) = L(K_1) + L(K_2)$.

4. Аксиома инвариантности: если дизъюнктивная нормальная форма K_1 получена из дизъюнктивной нормальной формы K путем переименования переменных, то $L(K_1) = L(K)$.

Определение 4.2. Для данной дизъюнктивной нормальной формы индексами простоты являются:

$L_{\text{Б}}(K)$ — число букв переменных;

$L_{\text{К}}(K)$ — число элементарных конъюнкций;

$L_{\text{О}}(K)$ — число символов отрицания.

Теорема 4.1. *Число всевозможных дизъюнктивных нормальных форм для всех булевых функций от n переменных равно 2^{3^n}.*

Доказательство. Пусть дана некоторая булева функция $f(\tilde{x}^n)$ от n переменных. При построении очередной элементарной конъюнкции произвольной дизъюнктивной нормальной формы этой функции, для каждой переменной x_i возможен один из 3 вариантов — x_i, $\bar{x}_i$ и $\varnothing$ (знак пустого множества означает, что в элементарную конъюнкцию не входят ни переменная ни ее отрицание). Таким, поскольку всего переменных n, то мы имеем выборку из трехэлементного множества $\{x_i, \bar{x}_i, \varnothing\}$ по n элементов. Всех возможных таких выборок согласно теореме 1.1, будет 3^n. Поскольку же каждая построенная дизъюнктивная нормальная форма может принимать одно из двух значений, то теперь получаем выборку из двух элементов. Следовательно, снова применив теорему 1.1, получаем, что число всевозможных дизъюнктивных нормальных форм для всех булевых функций от n переменных равно 2^{3^n}.

Теорема доказана.

Определение 4.3. Дизъюнктивная нормальная форма K, реализующая функцию $f(\tilde{x}^n)$ и имеющая минимальный индекс $L(K)$, называется минимальной дизъюнктивной нормальной формой относительно K.

В дальнейшем минимальную дизъюнктивную нормальную форму относительно $L_{\text{Б}}(K)$ будем называть просто минимальной дизъюнктивной нормальной формой, а минимальную дизъюнктивную нормальную форму относительно индекса $L_{\text{К}}(K)$ — кратчайшей дизъюнктивной нормальной формой.

Пример 4.1. 1. $x_1 \vee \overline{x}_2\overline{x}_3$ является минимальной дизъюнктивной нормальной формой, поскольку все ее переменные являются существенными;

2. $x_1 \vee \overline{x}_2\overline{x}_3$ является кратчайшей дизъюнктивной нормальной формой, поскольку она не может быть представлена в виде одной элементарной конъюнкции;

3. $x_1 \vee \overline{x}_2\overline{x}_3$ является минимальной дизъюнктивной нормальной формой относительно $L_{\text{O}}(K)$.

Определение 4.4. Проблемой минимизации булевых функций называется задача построения минимальной дизъюнктивной нормальной формы относительного заданного индекса простоты.

Конечно, существует простейший алгоритм, позволяющий решить проблему минимизации чисто механически. Он включает в себя следующие этапы:

— строятся все возможные дизъюнктивные нормальные формы для n переменных;

— среди построенных отбираются те дизъюнктивные нормальные формы, которые реализуют данную булеву функцию;

— среди выбранных на предыдущем этапе дизъюнктивных нормальных форм путем вычисления и дальнейшего сопоставления выбирается та, для которой заданный индекс простоты является минимальным.

Однако такой алгоритм является очень трудоемким, ведь уже для $n = 3$ мы будем иметь дело с $2^9 = 512$ дизъюнктивными нормальными формами. Поэтому появляется необходимость в создании других алгоритмов, которые также решают задачу минимизации булевых функций, но не являются такими трудоемкими.

4.2. Упрощение дизъюнктивных нормальных форм. Тупиковые дизъюнктивные нормальные формы

Пусть K — произвольная дизъюнктивная нормальная форма. Пусть M — некоторая элементарная конъюнкция из K и K' — дизъюнктивная нормальная форма, образованная остальными элементарными конъюнкциями из K. Пусть $x_i^{\sigma_i}$ — некоторый множитель из M и M' — произведение остальных множителей из M (или из K, что в данном случае одно и то же). Допустим, что выполняются равенства $K = K' \vee M$ и $K = K' \vee x_i^{\sigma_i} M'$. Рассмотрим два вида преобразований дизъюнктивной нормальной формы K.

I. *Операция удаления элементарной конъюнкции*

В результате этой операции осуществляется переход от K к K'. При этом происходит удаление элементарной конъюнкции M. Это преобразование определено тогда и только тогда, когда $K = K'$.

II. *Операция удаления множителя*

В результате этой операции осуществляется переход от K к $K' \vee$ $\vee M'$. При этом происходит удаление множителя $x_i^{\sigma_i}$. Это преобразование определено тогда и только тогда, когда $K' \vee M' = K$.

Определение 4.5. Дизъюнктивная нормальная форма, которую нельзя упростить при помощи операций I и II называется тупиковой дизъюнктивной нормальной формой (относительно операций I и II).

Алгоритм упрощения дизъюнктивной нормальной формы

1. Выбирается некоторая дизъюнктивная нормальная форма для функции $f(\tilde{x}^n)$ в качестве исходной. Проще всего взять совершенную дизъюнктивную нормальную форму.

2. Осуществляется упорядочение элементарных конъюнкций и в каждой элементарной конъюнкции упорядочение множителей. Таким образом, выбирается определенная запись дизъюнктивной нормальной формы.

3. Слева направо производится просмотр записи дизъюнктивной нормальной формы. Для очередной элементарной конъюнкции сначала пробуют применить операцию удаления элементарной конъюнкции. Если это не удается, то просматривают в том же порядке (слева направо) все множители этой конъюнкции и для каждого из них пробуют применить операцию удаления множителя. После этого переходят к следующей элементарной конъюнкции.

4.Закончив обработку последней элементарной конъюнкции, еще раз просматривают полученную дизъюнктивную нормальную форму и пробуют применить операцию удаления элементарной конъюнкции (такое действие возможно даст результаты, если на предыдущем этапе в каких-либо элементарных конъюнкциях удалось применить операцию удаления множителя).

Замечание 4.1. *Результат действия алгоритма зависит от упорядочения исходной дизъюнктивной нормальной формы.*

Следующая теорема является очевидной, поскольку следует непосредственно из определения тупиковой дизъюнктивной нормальной формы и описания алгоритма упрощения дизъюнктивной нормальной формы.

Теорема 4.2. *Дизъюнктивная нормальная форма, полученная в результате применения алгоритма упрощения дизъюнктивной нормальной формы, является тупиковой нормальной формой (относительно операций I и II).*

Следующую теорему приведем без доказательства, ввиду его трудоемкости.

Теорема 4.3. *Пусть $f(\tilde{x}^n)$ — некоторая булева функция, которая не является тавтологией. Пусть*

$$K = \bigvee_{i=1}^{s} M_i$$

— ее произвольная тупиковая дизъюнктивная нормальная форма (относительно операций I и II). Тогда существует такое упорядочение для совершенной дизъюнктивной нормальной формы функции $f(\tilde{x}^n)$ из которого, при помощи алгоритма упрощения дизъюнктивной нормальной формы, получается K.

Следствие 4.1. *При подходящем выборе упорядочения, алгоритм упрощения дизъюнктивной нормальной формы позволяет получить из совершенной дизъюнктивной нормальной формы минимальную дизъ-*

юнктивную нормальную форму (относительно операций I и II).

4.3. Постановка задачи в геометрической форме

Множество E^n можно рассматривать как множество вершин n-мерного куба.

Пусть $n = 3$. тогда E^n — множество вершин трехмерного куба (т.е. куба в обычном понимании), у которого одна из вершин находится в начале координат, длина ребра равна 1 и три грани лежат в координатных плоскостях (рис.4). Все элементы множества

$$E^3 = \{(0,0,0); (0,0,1); (0,1,0); (0,1,1);$$
$$(1,0,0); (1,0,1); (1,1,0); (1,1,1)\}$$

являются вершинами.

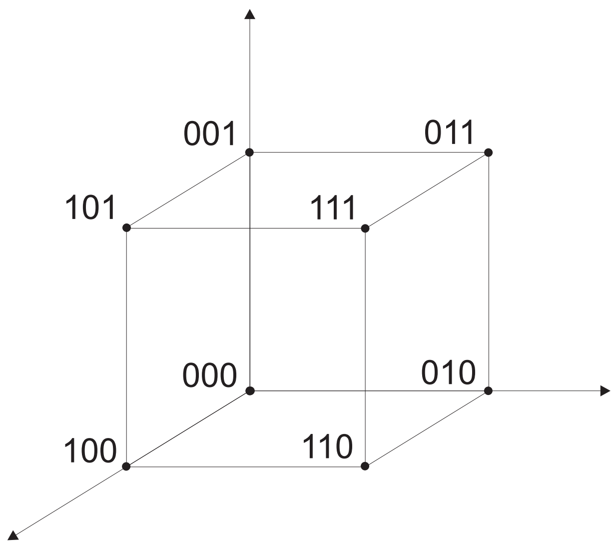


Рис. 4

Легко заметить следующую закономерность построения этого куба. У всех вершин, которые лежат на одной грани, одна из координат имеет одинаковое значение, а для вершин, лежащих на одном ребре одинаковое значение имеют две координаты. Эта закономерности позволяет определить понятие грани n-мерного куба.

Определение 4.6. Пусть $s_{i_1}, s_{i_2}, \dots, s_{i_r}$ — фиксированная система чисел из множества $\{0,1\}$. Множество всех вершин n-мерного куба $(a_1, a_2, \dots, a_n)$ таких, что

$$a_{i_1} = s_{i_1}, \quad a_{i_2} = s_{i_2}, \quad \dots, \quad a_{i_r} = s_{i_r},$$

называется $(n-r)$-мерной гранью.

Пусть теперь $n=4$. Тогда

$$E^4 = \{(0,0,0,0);(0,0,0,1);(0,0,1,0);(0,0,1,1);$$
$$(0,1,0,0);(0,1,0,1);(0,1,1,0);(0,1,1,1);$$
$$(1,0,0,0);(1,0,0,1);(1,0,1,0);(1,0,1,1);$$
$$(1,1,0,0);(1,1,0,1);(1,1,1,0);(1,1,1,1)\}.$$

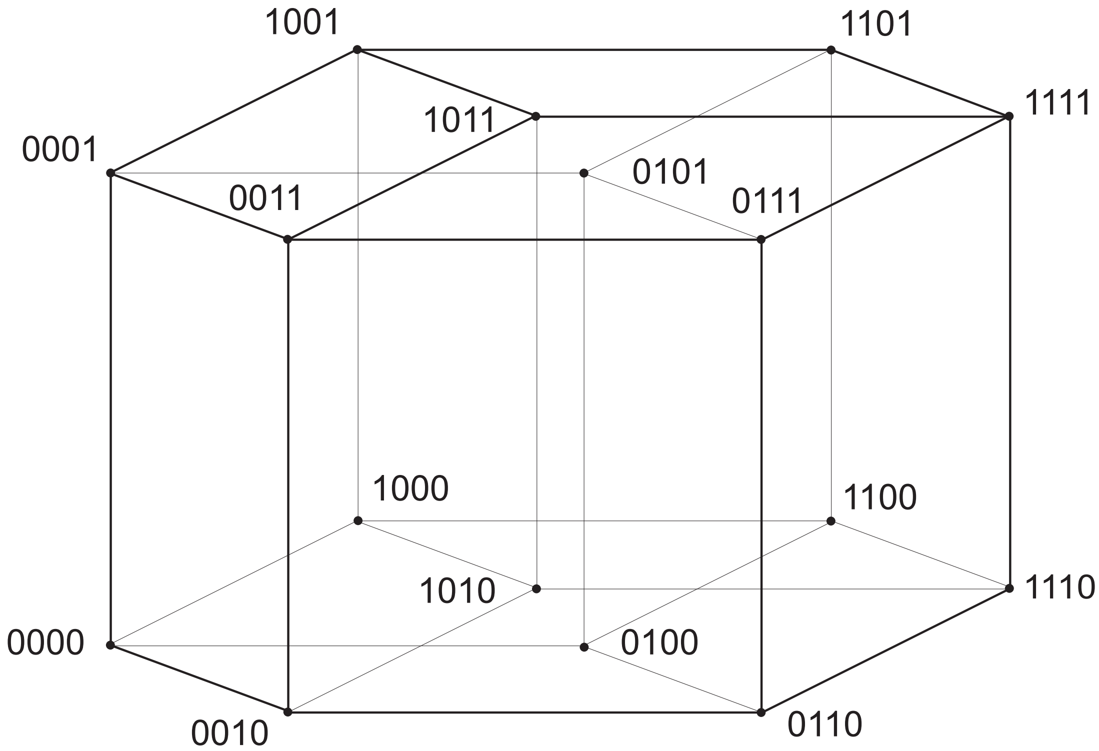


Рис. 5

Схематичное изображение четырехмерного куба позволяет довольно наглядно представить все $(n-r)$-мерные грани, среди которых трехмерные (их образуют вершины, имеющие одинаковое значение одной фиксированной координаты), двухмерные (вершины с одинаковым значением двух фиксированных координат) и одномерные (когда таких координат три) (рис. 5).

Пусть $f(\tilde{x}^n)$ — некоторая булева функция. Составим множество N_f следующим образом: $(a_1, a_2, \ldots, a_n) \in N_f$ тогда и только тогда, когда $f(a_1, a_2, \ldots, a_n) = 1$. Тогда $N_f \subseteq E^n$. Очевидно, что если известно множество N_f, то функцию $f(\tilde{x}^n)$ можно построить единственным образом.

Определение 4.7. *Рангом* элементарной конъюнкции называется число ее множителей.

Определение 4.8. Множество N_K, которое соответствует некоторой элементарной конъюнкции

$$K(x_1, x_2, \ldots, x_n) = x_{i_1}^{a_1} x_{i_2}^{a_2} \ldots x_{i_r}^{a_r}$$

называется *интервалом ранга* n.

Теорема 4.4. *Интервал* r*-го ранга является* $(n-r)$*-мерной гранью.*

Доказательство. Пусть N_K — некоторый интервал ранга r. Тогда существует такая элементарная конъюнкция

$$K(x_1, x_2, \ldots, x_n) = x_{i_1}^{a_1} x_{i_2}^{a_2} \ldots x_{i_r}^{a_r},$$

которая истинна только на одном наборе значений переменных $x_{i_1}, x_{i_2}, \ldots$ $\ldots, x_{i_r}$.

Если $r = n$, то $\{x_{i_1}^{a_1} x_{i_2}^{a_2} \ldots x_{i_r}^{a_r}\} = \{x_1, x_2, \ldots, x_n\}$. Следовательно, речь идет об единственном наборе значений переменных $x_1, x_2, \ldots, x_n$, т.е. об одной вершине, которая является 0-мерной гранью.

Пусть теперь $r < n$. Рассмотрим множество

$$S = \{x_1, x_2, \ldots, x_n\} \setminus \{x_{i_1}, x_{i_2}, \ldots, x_{i_r}\}.$$

Ввиду рассматриваемого случая оно является непустым. Следовательно, в множестве S содержатся переменные, которые для конъюнкции K являются фиктивными. Обозначим множество таких переменных через F. Всевозможные наборы значений переменных $x_1, x_2, \ldots, x_n$ у которых переменные из множества F принимают все возможные значения, а переменные $x_{i_1}, x_{i_2}, \ldots, x_{i_r}$ принимают только те значения, при которых конъюнкция K истинна, составляют по определению множество N_K. С другой стороны, поскольку мы зафиксировали для переменных $x_{i_1}, x_{i_2}, \ldots, x_{i_r}$ некоторый набор, то мы тем самым зафиксировали некоторую систему r чисел, взятых из множества $\{0, 1\}$. Поэтому, по определению, N_K — $(n-r)$-мерная грань.

Теорема доказана.

Определение 4.9. Покрытием множества N_f интервалами $N_{K_1}, N_{K_2}, \ldots$ $\ldots, N_{K_s}$ называется выражение

$$N_f = N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s},$$

т.е. представление множества N_f в виде объединения множеств $N_{K_1}, N_{K_2}, \ldots, N_{K_s}$.

Теорема 4.5. *Тогда и только тогда функция* $f(\tilde{x}^n)$ *обладает дизъ-*

юнктивной нормальной формой D такой, что

$$D = K_1 \vee K_2 \vee \ldots \vee K_s,$$

когда

$$N_f = N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s},$$

т.е. представление булевой функции дизъюнктивной нормальной формой равносильно покрытию множества N_f интервалами, соответствующими элементарным конъюнкциям этой дизъюнктивной нормальной формы.

Доказательство. Пусть некоторая булева функция $f(\tilde{x}^n)$ представлена своей дизъюнктивной нормальной формой, т.е.

$$f(\tilde{x}^n) = K_1 \vee K_2 \vee \ldots \vee K_s, \tag{4.1}$$

где $K_1, K_2, \ldots, K_s$ — элементарные конъюнкции, составляющие дизъюнктивную нормальную форму. Покажем, что в этом случае

$$N_f = N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s}. \tag{4.2}$$

Пусть $(a_1, a_2, \ldots, a_n) \in N_f$. Это возможно только тогда, когда $f(a_1, a_2, \ldots \ldots, x_n) = 1$. Следовательно, существует хотя бы одна элементарная конъюнкция K_t из (4.1), которая на указанном наборе имеет значение 1. Поэтому существует соответствующий интервал N_{K_t}, который содержит этот набор. Значит, справедливо включение

$$N_f \subseteq N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s}.$$

Пусть теперь $(a_1, a_2, \ldots, a_n) \in N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s}$. Тогда существует по крайней мере один интервал N_{K_t} такой, что $(a_1, a_2, \ldots, a_n) \in N_{K_t}$. Следовательно, в (4.1) существует по крайней мере одна конъюнкция K_t такая, что $K_t(a_1, a_2, \ldots, a_n) = 1$. Значит, $f(a_1, a_2, \ldots, x_n) = 1$. Поэтому $(a_1, a_2, \ldots, a_n) \in N_f$ и получаем, что справедливо включение

$$N_f \subseteq N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s}.$$

Из полученных включений следует равенство (4.2). Итак, мы доказали, что из (4.1) следует (4.2).

Допустим теперь, что выполняется (4.2). Восстановим по множеству N_f функцию $f(\tilde{x}^n)$. По каждому из интервалов $N_{K_1}, n_{K_2}, \ldots, N_{K_s}$ восстановим соответствующие им элементарные конъюнкции $K_1, K_2, \ldots, K_s$. Как уже отмечалось выше, такое восстановление осуществляется единственным образом. Составим из полученных элементарных конъюнкций дизъюнктивную нормальную форму $K_1 \vee K_2 \vee \ldots \vee K_s$.

Пусть на некотором наборе $(a_1, a_2, \ldots, a_n)$ значений переменных $x_1, x_2, \ldots, x_n$ составленная нами дизъюнктивная нормальная форма $K_1 \vee \vee K_2 \vee \ldots \vee K_s$ принимает значение 0. Тогда каждая из составляющих ее элементарных конъюнкций на этом наборе принимает значение 0. Следовательно, набор $(a_1, a_2, \ldots, a_n)$ не принадлежит ни одному из интервалов $N_{K_1}, n_{K_2}, \ldots, N_{K_s}$. Поэтому он не принадлежит и множеству N_f. Это означает, что на указанном наборе функция $f(\tilde{x}^n)$ принимает значение 0.

Пусть теперь на некотором наборе $(a_1, a_2, \ldots, a_n)$ значений переменных $x_1, x_2, \ldots, x_n$ составленная нами дизъюнктивная нормальная форма $K_1 \vee K_2 \vee \ldots \vee K_s$ принимает значение 1. Тогда в этой форме найдется хотя бы одна элементарная конъюнкция K_t, которая на этом наборе также принимает значение 1. Поэтому набор $(a_1, a_2, \ldots, a_n)$ принадлежит интервалу N_{K_t}. Значит, согласно (4.2), этот набор принадлежит множеству N_f. Это означает, что $f(a_1, a_2, \ldots, a_n) = 1$. Итак, на всех возможных наборах значений переменных, функции $f(\tilde{x}^n)$ и $K_1 \vee K_2 \vee \ldots \vee K_s$ принимают одинаковые значения. Равенство (4.1) доказано.

Теорема доказана.

Определение 4.10. *Покрытием множества* N_f называется всякое выражение вида $N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s}$, где $N_{K_1}, N_{K_2}, \ldots . N_{K_s}$ — интервалы, соответствующие элементарным конъюнкциям $K_1, K_2, \ldots, K_n$, которые составляют некоторую дизъюнктивную нормальную форму функции $f(\tilde{x}^n)$.

Определение 4.11. Пусть $N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s}$ — некоторое покрытие. *Рангом покрытия* называется число

$$r = \sum_{i=1}^{s} r_i,$$

где r_i — ранг интервала N_{K_i}.

Теперь задачу минимизации дизъюнктивной нормальной формы можно свести к эквивалентной задаче: найти для данного множества N_f такое покрытие интервалами, принадлежащими этому множеству, чтобы его ранг был наименьшим.

4.4. Сокращенная дизъюнктивная нормальная форма

Определение 4.12. Интервал N_K, содержащийся в N_f называется *максимальным* (относительно N_f), если не существует интервала $N_{K'}$ такого, что:

1) ранг интервала $N_{K'}$ меньше ранга интервала N_K;

2) $N_K \subseteq N_{K'} \subseteq N_f$.

Определение 4.13. Конъюнкция K, соответствующая максимальному интервалу N_K множества N_f, называется *простой импликантой функции* f.

Теорема 4.6. *Из простой импликанты нельзя удалить ни одного множителя.*

Доказательство. Пусть

$$K = x_{i_1}^{\sigma_{i_1}} x_{i_2}^{\sigma_{i_2}} \dots x_{i_n}^{\sigma_{i_n}}$$

— простая импликанта булевой функции $f(\tilde{x}^n)$, определяемой множеством N_f. Это в частности означает, что интервал N_K является максимальным. Предположим, что нам удалось удалить из конъюнкции K некоторый множитель $x_{i_t}^{\sigma_{i_t}}$ $(1 \leqslant t \leqslant s)$ и получить элементарную конъюнкцию

$$K' = x_{i_1}^{\sigma_{i_1}} x_{i_2}^{\sigma_{i_2}} \dots x_{i_{t-1}}^{\sigma_{i_{t-1}}} x_{i_t+1}^{\sigma_{i_{t+1}}} \dots x_{i_n}^{\sigma_{i_n}}.$$

Тогда, если до удаления этого множителя интервал N_K содержал либо набор

$$(a_1, a_2, \dots, a_{i_{t-1}}, 1, a_{i_{t+1}}, \dots, a_n),$$

либо набор

$$(a_1, a_2, \dots, a_{i_{t-1}}, 0, a_{i_{t+1}}, \dots, a_n),$$

то после удаления, интервал $N_{K'}$ будет содержать оба этих набора. Таким образом, после удаления множителя мы получим интервал $N_{K'}$ меньшего ранга чем N_K, такой, что $N_K \subset N_{K'}$. Но это противоречит определению интервала N_K как максимального.

Теорема доказана.

Пусть

$$N_{K_1^0},\ N_{K_2^0},\ \dots, N_{K_n^0}$$

— список всех максимальных интервалов множества N_f. Поскольку каждый интервал состоит из элементов множества N_f, то очевидно включение

$$N_{K_1^0} \vee N_{K_2^0}, \vee \dots \vee N_{K_n^0} \subseteq N_f.$$

С другой стороны, пусть $(a_1, a_2, \dots, a_n)$ — некоторый произвольный набор из множества N_f. Тогда $f(a_1, a_2, \dots, a_n) = 1$. Поэтому $(a_1, a_2, \dots, a_n)$ содержится в некотором интервале N_t, который соответствует элементарной конъюнкции $x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ Если из N_t нельзя удалить ни одного множителя, то этот интервал является максимальным. в противном случае, после удаления некоторого множителя x_i, мы получим интервал N_{t_i} в который входит набор $(a_1, a_2, \dots, a_n)$. Если полученный интервал не является максимальным, то снова применим операцию удаления множителя. В конечном итоге, окажется, что набор $(a_1, a_2, \dots, a_n)$ принадлежит некоторому максимальному интервалу. Таким образом, справедливо и обратное включение:

$$N_{K_1^0} \vee N_{K_2^0}, \vee \ldots \vee N_{K_n^0} \supseteq N_f.$$

Поэтому получаем равенство

$$N_{K_1^0} \vee N_{K_2^0}, \vee \ldots \vee N_{K_n^0} = N_f.$$

Это равенство эквивалентно равенству

$$f = K_1^0 \vee K_2^0 \vee \ldots \vee K_n^0.$$

Определение 4.14. Дизъюнктивная нормальная форма, являющаяся дизъюнкцией всех простых импликант, называется *сокращенной дизъюнктивной нормальной формой.*

Алгоритм построения сокращенной дизъюнктивной нормальной формы

1. Для данной булевой функции $f(x_1, x_2, \dots, x_n)$ берут некоторую конъюнктивную нормальную форму (можно взять совершенную конъюнктивную нормальную форму).

2. Производят раскрытие скобок, которое сводится к преобразованию вида

$$\wedge\vee \to \vee \wedge .$$

3. В полученном выражении совершают преобразования вида

$$K_1K_2 \vee K_1 = K_1,$$
$$K_1 \vee K_1 = K_1,$$

которые ликвидируют поглощаемые и дублирующие множители. Кроме того, удаляют элементарные конъюнкции, которые содержат одновременно какую-либо переменную и ее отрицание.

В результате этих преобразований получается сокращенная дизъюнктивная нормальная форма.

5. Полнота и замкнутость систем булевых функций

5.1. Полные системы булевых функций

Определение 5.1. Система булевых функций M называется *полной*, если любую булеву функцию можно представить как формулу над M.

Пример 5.1. Система P_2 является полной; система $\{0, 1\}$ не является полной.

Теорема 5.1 (О системе $\{\rceil, \wedge, \vee\}$). *Система $\{\rceil, \wedge, \vee\}$ является полной.*

Доказательство. Если $f(\tilde{x}^n)$ не является противоречием, то для нее всегда существует СДНФ, которая является формулой над $\{\rceil, \wedge, \vee\}$. Если же $f(\tilde{x}^n)$ является противоречием, то $f(\tilde{x}^n) = x_1 \wedge \overline{x}_1$.

Теорема доказана.

Следующее утверждение является очевидным.

Лемма 5.1. *Пусть даны две системы булевых функций*

$$\{f_1, f_2, \ldots, f_m\} \tag{5.1}$$

и

$$\{g_1, g_2, \ldots, g_s\} \tag{5.2}$$

такие, что система (5.1) *является полной и каждая ее функция может быть задана формулой над* (5.2). *Тогда система* (5.2) *является полной.*

Теорема 5.2. *Полными являются системы* $\{\rceil, \wedge\}$, $\{\rceil, \vee\}$, $\{0, 1, \wedge, \oplus\}$.

Доказательство. Как было доказано выше, система $\{\rceil, \wedge, \vee\}$ полна. Используя законы де Моргана, дизъюнкцию можно выразить через конъюнкцию и отрицание. Поэтому, ввиду леммы 5.1, получаем полноту системы $\{\rceil, \wedge\}$. Аналогично устанавливается полнота системы $\{\rceil, \vee\}$.

Покажем полноту системы $\{0, 1, \oplus, \wedge\}$. Действительно, так как мы доказали полноту системы $\{\rceil, \wedge\}$, то, используя одно из приведенных выше свойств констант $\overline{x} = x \oplus 1$ и лемму 5.1, приходим к полноте системы $\{0, 1, \oplus, \wedge\}$.

Теорема доказана.

Понятно, что система, содержащая все операции полна. Системы $\{\rceil, \vee\}$ и $\{\rceil, \wedge\}$ содержат всего две операции. Возникает вопрос: существуют ли системы, которые состоят из одной операции и являются полными?

Определение 5.2. *Вспомогательными булевыми функциями* называются булевы функции, заданные с помощью следующей таблицы

x	y	$\mid$	$\downarrow$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

$x|y$ — *штрих Шеффера*;

$x \downarrow y$ — *стрелка Пиркса.*

Свойство 5.1. *Справедливы следующие равенства:* $\overline{x} = x|x$; $\overline{x} = x \downarrow x$; $x \vee y = \overline{x}|\overline{y}$; $xy = \overline{x} \downarrow \overline{y}$.

Доказательство. Доказательство проводится прямой проверкой с использованием таблиц истинности.

Непосредственно из приведенного выше свойства и леммы 5.1, следует утверждение.

Теорема 5.3. *Системы* $\{|\}$ *и* $\{\downarrow\}$ *полны.*

5.2. Важнейшие замкнутые классы булевых функций

Определение 5.3. Пусть M — некоторое непустое множество булевых функций. *Замыканием* множества M называется множество, которое обозначается через $[M]$ и состоит из всех булевых функций, которые могут быть заданы формулой над M.

Используя понятие замыкания, полную систему булевых функций можно определить по-другому.

Определение 5.4. Система булевых функций M называется полной, если $[M] = P_2$.

Определение 5.5. Класс M называется *замкнутым*, если $[M] = M$.

Свойство 5.2. *Для замыкания справедливы следующие соотношения:*

1) $M \subseteq [M]$;

2) $[M] = [[M]]$;

3) если $M_1 \subseteq M_2$, *то* $[M_1] \subseteq [M_2]$;

4) $[M_1] \cup [M_2] \subseteq [M_1 \cup M_2]$.

Определение 5.6. Булева функция $f(\tilde{x}^n)$ называется *булевой функцией, сохраняющей константу* 0, если $f(0,0,\ldots,0)=0$. Множество всех булевых функций от n переменных, сохраняющих константу 0 называется *классом булевых функций сохраняющих константу* 0 и обозначается T_0.

Определение 5.7. Булева функция $f(\tilde{x}^n)$ называется *булевой функцией, сохраняющей константу* 1, если $f(1,1,\ldots,1)=1$. Множество всех булевых функций от n переменных, сохраняющих константу 1 называется *классом булевых функций сохраняющих константу* 1 и обозначается T_1.

Лемма 5.2. *Класс T_0 булевых функций замкнут и содержит ровно 2^{2^n-1} булевых функций, зависящих от n переменных.*

Доказательство. Докажем сначала замкнутость класса T_0. Любую функцию, построенную на T_0 можно представить в виде

$$A=f(f_1(\tilde{x}^n),f_2(\tilde{x}^n),\ldots,f_k(\tilde{x}^n)),$$

где $f(\tilde{x}^n),f_1(\tilde{x}^n),f_2(\tilde{x}^n),\ldots,f_k(\tilde{x}^n)$ — функции из класса T_0. Тогда

$$A(0,0,\ldots,0)=$$
$$f(f_1(0,0,\ldots,0),f_2(0,0,\ldots,0),\ldots,f_k(0,0,\ldots,0))=$$
$$f(0,0,\ldots,0)=0.$$

Следовательно, любая булева функция, построенная на множестве функций из класса T_0, принадлежит классу T_0. Таким образом, замкнутость класса T_0 доказана.

Если рассмотреть множество всех булевых функций от n переменных, то легко заметить, что все они делятся на два класса. Один класс состоит из тех функций, которые на наборе $(0,0,\ldots,0)$ принимают значение 0, а другой — из тех функций, которые на этом наборе принимают значение 1. Поскольку на значения этих функций на других наборах никаких ограничений не накладывается, то очевидно, что эти классы равны по количеству элементов. Теперь, вспомнив, что число всех булевых функций от n аргументов равно 2^{2^n}, получим, что число всех булевых функций от n аргументов, сохраняющих константу 0, равно $\frac{1}{2}\cdot 2^{2^n} = 2^{2^n-1}$.

Лемма доказана.

Аналогично доказывается

Лемма 5.3. *Класс T_1 булевых функций замкнут и содержит ровно 2^{2^n-1} булевых функций, зависящих от n переменных.*

Определение 5.8. Булева функция $f(\tilde{x}^n)$ называется *линейной булевой функцией*, если существуют $a_0, a_1, \ldots, a_n \in \{0, 1\}$ такие, что

$$f(\tilde{x}^n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n.$$

Множество всех булевых функций от n переменных, которые являются линейными, называется *классом линейных булевых функций* и обозначается L.

Лемма 5.4 (лемма о линейной функции). *Если линейная булева функция $f(\tilde{x}^n)$ не является константой, то ее векторное задание содержит 2^{n-1} единиц.*

Доказательство. Докажем лемму используя принцип математической индукции. При $n = 1$ получаем функцию, зависящую от 1 переменной. Различных таких функций $2^{2^1} = 2^2 = 4$. Это будут функции, которые реализуются формулами $0,\ 1,\ x, \overline{x}$. Из них константами не являются x и $\overline{x}$. Каждая из них линейна: $x = 0 \oplus x$; $\overline{x} = 1 \oplus x$. Кроме того, если для этих функций построить таблицы истинности, то мы увидим, что векторное задание каждой из них содержит $2^{1-1} = 2^0 = 1$ число единиц. Итак, при $n = 1$ утверждение выполняется.

Пусть теперь $n = 2$, т.е. булева функция зависит от 2 переменных. Пусть x и y — такие переменные. Тогда число всех возможных булевых функций будет равно $2^{2^2} = 16$. Воспользуемся теоремой Жегалкина для перечисления всех формул, реализующих эти функции:

$$0,\ 1,\ x,\ y,\ 1 \oplus x,\ 1 \oplus y,\ x \oplus y,\ 1 \oplus x \oplus y,$$

$$xy,\ x \oplus xy,\ y \oplus xy,\ 1 \oplus xy,\ 1 \oplus x \oplus xy,$$

$$1 \oplus y \oplus xy,\ x \oplus y \oplus xy,\ 1 \oplus x \oplus y \oplus xy.$$

Те из них, которые содержат xy не являются линейными. Кроме того, исключим из рассмотрения так же константы 0 и 1. Составим для оставшихся функций таблицу истинности.

x	y	$1 \oplus x$	$1 \oplus y$	$x \oplus y$	$1 \oplus x \oplus y$
0	0	1	1	0	1
0	1	1	0	1	0
1	0	0	1	1	0
1	1	0	0	0	1

Из таблицы видно, что векторные задания каждой из этих функций содержат $2^{n-1} = 2^{2-1} = 2$ единицы. Следовательно, утверждение выполняется и для $n = 2$.

Предположим теперь, что лемма выполняется для всех булевых функций, число переменных которых не превышает $n-1$, т.е. если $f(\tilde{x}^{n-1})$ — линейная булева функция, отличная от константы, то число единиц в ее векторном задании равно 2^{n-2}. Пусть $f(\tilde{x}^n)$ — произвольная линейная булева функция. Тогда существуют $a_0, a_1, \ldots, a_n \in \{0,1\}$ такие, что

$$f(\tilde{x}^n) = a_0 \oplus a_1x_1 \oplus \ldots \oplus a_nx_n. \qquad (*)$$

Составим функцию

$$f_1(\tilde{x}^{n-1}) = a_0 \oplus a_1x_1 \oplus \ldots \oplus a_{n-1}x_{n-1}. \qquad (**)$$

Тогда

$$f(\tilde{x}^n) = f_1(\tilde{x}^{n-1}) \oplus a_nx_n.$$

Каждому набору $(a_1, a_2, \ldots, a_{n-1})$ переменных $x_1, x_2, \ldots, x_{n-1}$ функции $f(\tilde{x}^{n-1})$ соответствует два набора переменных $x_1, x_2, \ldots, x_n$ функции $f(\tilde{x}^n)$ — $(a_1, a_2, \ldots, a_{n-1}, 1)$ и $(a_1, a_2, \ldots, a_{n-1}, 0)$. Если на наборе $(a_1, a_2, \ldots, a_{n-1})$ функция $(**)$ принимает значение 1, то на наборе $(a_1, a_2, \ldots, a_{n-1}, 1)$ функция $(*)$ принимает значение 0, а на наборе $(a_1, a_2, \ldots, a_{n-1}, 0)$ — значение 1. Если же на наборе $(a_1, a_2, \ldots, a_{n-1})$ функция $(**)$ принимает значение 0, то на наборе $(a_1, a_2, \ldots, a_{n-1}, 1)$ функция $(*)$ принимает значение 1, а на наборе $(a_1, a_2, \ldots, a_{n-1}, 0)$ — значение 0. Таким образом, число единиц в векторном задании функции $(*)$ оказывается в два раза больше, чем число единиц в векторном задании функции $(**)$, т.е. $2 \cdot 2^{n-2} = 2^{n-1}$.

Лемма доказана.

Следствие 5.1. *При $n \geqslant 2$ векторное задание линейной булевой функции $f(\tilde{x}^n)$ содержит четное число единиц.*

Следствие 5.2. *Если при $n \geqslant 2$ векторное задание булевой функции $f(\tilde{x}^n)$ содержит нечетное число единиц, то функция $f(\tilde{x}^n)$ не является линейной.*

Очевидно, что в результате составления линейного полинома из линейных полиномов, снова получается линейный полином. Поэтому справедливо следующее утверждение.

Свойство 5.3. *Класс L замкнут.*

Определение 5.9. Булева функция $f(\tilde{x}^n)$ называется *самодвойственной булевой функцией*, если $f(\tilde{x}^n) = \overline{f}(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n)$. Множество всех самодвойственных булевых функций называется *классом самодвойственных булевых функций* и обозначается через S. Класс S можно определить еще и так: $S = \{f \mid f = f^*\}$.

Определение 5.10. Наборы $(a_1, a_2, \ldots, a_n)$ и $(\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n)$ переменных $x_1, x_2, \ldots, x_n$ называются *противоположными.*

Лемма 5.5. *Класс S замкнут и содержит ровно $\sqrt{2^{2^n}}$ булевых функций от n переменных.*

Доказательство. Любую функцию, построенную на S можно представить в виде

$$A = f(f_1(\tilde{x}^n), f_2(\tilde{x}^n), \ldots, f_k(\tilde{x}^n)),$$

где $f(\tilde{x}^n), f_1(\tilde{x}^n), f_2(\tilde{x}^n), \ldots, f_k(\tilde{x}^n)$ — функции из класса S. Тогда, ввиду теоремы о двойственной функции,

$$A^* = f^*(f_1^*(\tilde{x}^n), f_2^*(\tilde{x}^n), \ldots, f_k^*(\tilde{x}^n)) =$$

$$f^*(f_1(\tilde{x}^n), f_2(\tilde{x}^n), \ldots, f_k(\tilde{x}^n)) =$$

$$f(f_1(\tilde{x}^n), f_2(\tilde{x}^n), \ldots, f_k(\tilde{x}^n)) = A.$$

Следовательно, любая булева функция, построенная на множестве функций из класса S, принадлежит классу S. Таким образом, замкнутость класса S доказана.

Для самодвойственной функции $f(x_1, x_2, \ldots, x_n) = \overline{f}(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n)$. Это значит, что на противоположных наборах самодвойственная функция принимает противоположные значения (векторное задание такой функции является как-бы "симметричным наоборот"). Следовательно, самодвойственная функция полностью определяется своими значениями на первой половине строк, т.е. $\dfrac{1}{2} \cdot 2^n = 2^{n-1}$ строками, и, поскольку в каждой строке она может принимать два значения, то число таких функций равно числу упорядоченных выборок с возвращением из 2 элементов по 2^{n-1} элементов. Таким образом, число всех возможных самодвойственных булевых функций от n переменных оказывается равным $2^{2^{n-1}} = \sqrt{2^{2^n}}$.

Лемма доказана.

На множестве $\{0, 1\}$ определим бинарное отношение $\leqslant$ следующим образом: $0 \leqslant 0,\ 0 \leqslant 1,\ 1 \leqslant 1$.

Определение 5.11. Вектор $(a_1, a_2, \ldots, a_n)$ *предшествует* вектору $(b_1, b_2, \ldots, b_n)$ если $a_1 \leqslant b_1,\ a_2 \leqslant b_2, \ldots, a_n \leqslant b_n$. При этом используется обозначение

$$(a_1, a_2, \ldots, a_n) \prec (b_1, b_2, \ldots, b_n).$$

Определение 5.12. Булева функция $f(\tilde{x}^n)$ называется *монотонной булевой функцией*, если для любых наборов $(a_1, a_2, \ldots, a_n)$ и $(b_1, b_2, \ldots$

$\ldots, b_n)$ таких, что

$$(a_1, a_2, \ldots, a_n) \prec (b_1, b_2, \ldots, b_n)$$

всегда выполняется

$$f(a_1, a_2, \ldots, a_n) \leqslant f(b_1, b_2, \ldots, b_n).$$

Множество всех монотонных булевых функций называется *классом монотонных булевых функций* и обозначается через M.

Лемма 5.6. *Класс M замкнут.*

Доказательство. Любую функцию, построенную на M можно представить в виде

$$A = f(f_1(\tilde{x}^n), f_2(\tilde{x}^n), \ldots, f_k(\tilde{x}^n)),$$

где $f(\tilde{x}^n), f_1(\tilde{x}^n), f_2(\tilde{x}^n), \ldots, f_k(\tilde{x}^n)$ — функции из класса M. Пусть $(a_1, a_2, \ldots, a_n)$ и $(b_1, b_2, \ldots, b_n)$ — такие два набора переменных $x_1, x_2, \ldots$ $\ldots, x_n$, что

$$(a_1, a_2, \ldots, a_n) \prec (b_1, b_2, \ldots, b_n).$$

Тогда, по определению монотонной булевой функции,

$$f_1(a_1, a_2, \ldots, a_n) \leqslant f_1(b_1, b_2, \ldots, b_n);$$

$$f_2(a_1, a_2, \ldots, a_n), \leqslant f_2(b_1, b_2, \ldots, b_n); \ldots;$$

$$f_k(a_1, a_2, \ldots, a_n) \leqslant f_k(b_1, b_2, \ldots, b_n).$$

Значит,

$$(f_1(a_1, a_2, \ldots, a_n), f_2(a_1, a_2, \ldots, a_n) \ldots, f_k(a_1, a_2, \ldots, a_n)) \prec$$
$$(f_1(b_1, b_2, \ldots, b_n), f_2(b_1, b_2, \ldots, b_n), \ldots, f_k(b_1, b_2, \ldots, b_n)).$$

Поэтому, поскольку f так же является монотонной булевой функцией, снова воспользовавшись определением, получаем окончательно

$$f(f_1(a_1, a_2, \ldots, a_n), f_2(a_1, a_2, \ldots, a_n), \ldots, f_k(a_1, a_2, \ldots, a_n)) \leqslant$$
$$f(f_1(b_1, b_2, \ldots, b_n), f_2(b_1, b_2, \ldots, b_n), \ldots, f_k(b_1, b_2, \ldots, b_n)).$$

Итак, $A(a_1, a_2, \ldots, a_n) \leqslant A(b_1, b_2, \ldots, b_n)$. Следовательно, класс M замкнут.

Лемма доказана.

Лемма 5.7. *Если монотонная булева функция не является константой, то она может быть задана ДНФ без отрицаний переменных.*

Доказательство. Если монотонная булева функция не является константой, то для нее можно построить СДНФ. Если построенная СДНФ не содержит отрицаний переменных, то лемма доказана. Пусть некоторая элементарная конъюнкция такой СДНФ содержит отрицание некоторой переменной x_i. Это значит, что существует такой набор $(a_1, \ldots$ $\ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$, что $f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) = 1$. В силу монотонности $f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n) = 1$. Значит среди элементарных конъюнкций рассматриваемой СДНФ найдется конъюнкция содержащая x_i, поэтому, применив правило склеивания, получим ДНФ, которая не будет содержать $\overline{x}_i$. Поступая аналогично необходимое число раз получим ДНФ без отрицаний переменных.

Лемма доказана.

Свойство 5.4. *Классы T_0, T_1, S, M, L различны.*

Доказательство. Для доказательства, того факта, что два класса — K_1 и K_2 булевых функций различны, достаточно привести пример функции, которая принадлежит одному из них и не принадлежит другому. Поэтому доказательством этого свойства будет таблица истинности

	T_0	T_1	L	S	M
0	$+$	$-$	$+$	$-$	$+$
1	$-$	$+$	$+$	$-$	$+$
$\overline{x}$	$-$	$-$	$+$	$+$	$-$

в которой принадлежность функции конкретному классу обозначается знаком $+$, а непринадлежность обозначается знаком $-$.

Свойство доказано.

Используя определенное нами выше понятие формулы, построенной над некоторым множеством булевых функций, докажем следующие три леммы.

Лемма 5.8 (О несамодвойственной функции). *Если булева функция $f(\tilde{x}^n)$ не является самодвойственной, то из нее путем подстановки функций x и $\overline{x}$ можно получить формулу, которая реализует несамодвойственную булеву функцию одного переменного, т.е. константу.*

Доказательство. Пусть $f(\tilde{x}^n)$ — некоторая несамодвойственная булева функция. Тогда существует такой набор $(a_1, a_2, \ldots, a_n)$ переменных $x_1, x_2, \ldots, x_n$,что

$$f(\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n) = f(a_1, a_2, \ldots, a_n).$$

Определим функцию $\varphi(x)$ следующим образом:

$$\varphi(x) = f(\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x)),$$

где $\varphi_i(x) = x^{a_i}$ $(i = 1, 2, \ldots, n)$. Тогда

$$\varphi(0) = f(\varphi_1(0), \varphi_2(0), \ldots, \varphi_n(0)) =$$

$$f(0^{a_1}, 0^{a_2}, \ldots, 0^{a_n}) = f(\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n) =$$

$$f(a_1, a_2, \ldots, a_n) = f(1^{a_1}, 1^{a_2}, \ldots, 1^{a_n}) = \varphi(1).$$

Таким образом мы получаем функцию, которая при любом наборе значений переменных принимает одно и то же значение, т. е. константу.

Лемма доказана.

Определение 5.13. Наборы $\tilde{a}$ и $\tilde{b}$ называются *соседними* по i-ой координате, если

$$\tilde{a} = (a_1, a_2, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n),$$

$$\tilde{b} = (a_1, a_2, \ldots, a_{i-1}, \overline{a}_i, a_{i+1}, \ldots, a_n).$$

Выше мы определили на множестве $\{0, 1\}$ бинарное отношение $\leqslant$. Определим теперь на этом же множестве бинарное отношение $<$, которое образует только одну пару элементов: $0 < 1$ и аналогично бинарное отношение $>$, которое так же образует только одну пару: $1 > 0$.

Лемма 5.9 (О немонотонной функции). *Если булева функция $f(\tilde{x}_n)$ не является монотонной, то из нее путем подстановки констант $0, 1$ и функции x, можно получить формулу, которая реализует булеву функцию $\overline{x}$.*

Доказательство. Пусть $f(\tilde{x}_n)$ — некоторая немонотонная булева функция. Тогда существуют наборы

$$(a_1^1, a_2^1, \ldots, a_n^1) \prec (b_1^1, b_2^1, \ldots, b_n^1)$$

такие что

$$f(a_1^1, a_2^1, \ldots, a_n^1) > f(b_1^1, b_2^1, \ldots, b_n^1).$$

Предположим, что эти наборы не являются соседними. Тогда они различаются в t координатах, причем, ввиду данного нами выше определения предшествования наборов, эти t координат имеют в наборе $(a_1^1, a_2^1, \ldots$ $\ldots, a_n^1)$ значение 0, а в наборе $(b_1^1, b_2^1, \ldots, b_n^1)$ значение 1. Поэтому можно составить цепочку соседних наборов

$$(a_1^1, a_2^1, \ldots, a_n^1) \prec$$

$$(a_1^2, a_2^2, \ldots, a_n^2) \prec$$

$$\dots\dots\dots$$
$$(a_1^t, a_2^t, \dots, a_n^t) \prec$$
$$(b_1^1, b_2^1, \dots, b_n^1).$$

В этой цепочке, в каждой из отмеченных t координат, последовательно заменяется 0 на 1. Поскольку же

$$f(a_1^1, a_2^1, \dots, a_n^1) > f(b_1^1, b_2^1, \dots, b_n^1),$$

то и для значения самой функции такая замена должна произойти, хотя это и произойдет только один раз. Поэтому найдется пара таких соседних наборов (обозначим их через $(a_1, a_2, \dots, a_n)$ и $(b_1, b_2, \dots, b_n)$), что

$$f(a_1, a_2, \dots, a_n) > f(x_1, x_2, \dots, x_n).$$

Пусть эти наборы имеют соседство по i-той координате:

$$(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n),$$
$$(b_1, b_2, \dots, b_n) = (a_1, a_2, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n).$$

Пусть

$$\varphi(x) = (a_1, a_2, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n).$$

Тогда

$$\varphi(0) = f(a_1, a_2, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) =$$
$$f(a_1, a_2, \dots, a_n) > f(b_1, b_2, \dots, b_n) =$$
$$f(a_1, a_2, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n) = \varphi(1).$$

Значит, $\varphi(0) = 1$, а $\varphi(1) = 0$. Следовательно, $\varphi(x) = \overline{x}$.

Лемма доказана.

Лемма 5.10 (о нелинейной функции). *Если булева функция $f(\tilde{x})$ не является линейной, то из нее путем подстановки констант $0, 1$, функций $x, \overline{x}$, а также может быть и взятием от нее отрицания, можно получить формулу, которая реализует булеву функцию $x_1 x_2$.*

Доказательство. Пусть $f(\tilde{x})$ — некоторая нелинейная булева функция. Построим для рассматриваемой функции полином Жегалкина (такой полином, согласно теореме Жегалкина, всегда можно построить):

$$f(\tilde{x}^n) = \bigoplus_{(i_1, i_2, \dots, i_s)} a_{i_1 i_2 \dots i_s} x_{i_1} x_{i_2} \dots x_{i_s}.$$

Поскольку функция $f(\tilde{x})$ не является линейной, то и построенный полином не является линейным. Это значит, что в нем найдется хотя бы одна конъюнкция, которая будет содержать не менее двух множителей. Без ограничения общности доказательства можно считать, что этими множителями являются x_1 и x_2. Представим построенный нами полином в следующем виде:

$$x_1x_2f_1(x_3,x_4,\ldots,x_n)\oplus x_1f_2(x_3,x_4,\ldots,x_n)\oplus$$
$$\oplus x_2f_3(x_3,x_4,\ldots,x_n)\oplus f_4(x_3,x_4,\ldots,x_n),$$

где f_1,f_2,f_3,f_4 — некоторые булевы функции. Поскольку полином Жегалкина для каждой функции единственен, то $f_1(x_3,x_4,\ldots,x_n)\not\equiv 0$. Следовательно, найдется такой набор $(a_3,a_4,\ldots,a_n)$, что $f(a_3,a_4,\ldots,a_n)=$ $=1$. Определим следующую функцию:

$$\varphi(x_1,x_2)=f(x_1,x_2,a_3,a_4,\ldots,a_n)=x_1x_2\oplus\alpha x_1\oplus\beta x_2\oplus\Gamma,$$

где $\alpha,\beta,\Gamma\in B$. Рассмотрим также функцию

$$\Psi(x_1,x_2)=\varphi(x_1\oplus\beta,x_2\oplus\alpha)\oplus\alpha\beta\oplus\Gamma.$$

тогда

$$\Psi(x_1,x_2)=(x_1\oplus\beta)(x_2\oplus\alpha)\oplus\alpha(x_1\oplus\beta)\oplus\beta(x_2\oplus\alpha)\oplus\Gamma\oplus\alpha\beta\oplus\Gamma=$$
$$=x_1x_2\oplus\alpha x_1\oplus\beta x_2\oplus\alpha\beta\oplus\alpha x_1\oplus\alpha\beta\oplus\beta x_2\oplus\alpha\beta\oplus\Gamma\oplus\alpha\beta\oplus\Gamma=x_1x_2.$$

Лемма доказана.

5.3. Критерии полноты

Теорема 5.4. *Для того, чтобы система булевых функций была полной необходимо и достаточно чтобы она целиком не содержалась ни в одном из классов T_0, T_1, S, M, L.*

Доказательство. *Необходимость.* Пусть K — некоторая система булевых функций, которая является полной. Это значит, что $[K]=P_2$. Предположим, что $K\subseteq N$, где N — один из классов T_o, T_1, S, M, L. Тогда, по свойству замыкания, $[K]\subseteq[N]$. Поэтому, поскольку класс N в любом случае замкнут, то получим $P_2=T_0=T_1=S=M=L$. Но выше мы доказали, что эти классы различны. Следовательно, наше предположение о том, что $K\subseteq N$ неверно и поэтому необходимость доказана.

Достаточность. Пусть некоторая система булевых функций K не содержится ни в одном из классов T_0,T_1,S,M,L. Тогда в K можно выбрать подсистему K', содержащую не более пяти функций $\{f_i,f_j,f_s,f_m,f_l\}$ таких, что $f_i\not\subseteq T_0$, $f_j\not\subseteq T_1$, $f_s\not\subseteq S$, $f_m\not\subseteq M$, $f_l\not\subseteq L$.

Можно считать, что эти функции зависят от одних и тех же переменных $x_1, x_2, \ldots, x_n$. Для того, чтобы показать полноту K' достаточно построить над K' полную систему. Построим над K' систему $\{\overline{x}, xy\}$. В этом нам помогут леммы 5.8, 5.9 и 5.10.

I. Построим вначале константы 0 и 1. Поскольку $f_i \notin T_0$, то $f_i(0, 0, \ldots$ $\ldots, 0) = 1$, а, поскольку, $f_j \notin T_1$, то $f_j(1, 1, \ldots, 1) = 0$.

Пусть $f_i(1, 1, \ldots, 1) = 1$ и $f_j(0, 0, \ldots, 0) = 0$. Тогда f_i является константой 1, а f_j является константой 0.

Пусть $f_i(1, 1, \ldots, 1) = 0$. Тогда f_i реализует функцию $\overline{x}$, т.к. при $x =$ $= 1$, $f_i(x, x, \ldots, x) = 0$, а при $x = 0$, $f_i(x, x, \ldots, x) = 1$. Если при этом $f_j(0, 0, \ldots, 0) = 0$, то f_j является константой 0 и, используя построенную в рассматриваемом случае функцию $\overline{x}$, получаем также и константу 1. Если же $f_j(0, 0, \ldots, 0) = 1$, то и f_j реализует функцию $\overline{x}$. Поэтому мы сможем реализовать функцию $\overline{\overline{x}} = x$. Взяв теперь функцию f_s, согласно лемме 5.8, мы можем построить одну из констант, а с помощью функции $\overline{x}$ и другую.

Осталось рассмотреть случай, когда $f_i(1, 1, \ldots, 1) = 1$ и $f_j(1, 1, \ldots$ $\ldots, 1) = 1$. Тогда f_i является константой 1, а f_j реализует функцию $\overline{x}$. Поэтому приходим к уже рассмотренной выше ситуации.

Итак, в любом случае константы 0 и 1 могут быть построены.

II. Если на этапе I константы были построены сразу, то функцию $\overline{x}$ можно построить в виду леммы 5.9, используя эти константы и f_m.

III. Ввиду леммы 5.10 используя $0, 1, \overline{x}, f_l$ можно построить функцию xy.

Итак, нами построена над K', а значит и над K система $\{\overline{x}, xy\}$, которая является полной. Следовательно, $[K] = P_2$.

Теорема доказана.

Следствие 5.3. *Всякий замкнутый класс K булевых функций такой, что $K \neq P_2$ содержится хотя бы в одном из классов T_0, T_1, S, M, L.*

Доказательство. Действительно, если некоторый класс булевых функций K целиком не содержится ни в одном из перечисленных классов, то по только что доказанной теореме, он является полной системой. Поэтому $[K] = P_2$, а, т.к. класс K замкнут, то $[K] = K$ и приходим к противоречию.

Следствие доказано.

Определение 5.14. Класс $K \subset P_2$ называется *предполным* (или *максимальным*), если K не является полным, но для любой функции $f \in P_2 \setminus K$ система $\{f\} \cup K$ полна.

Можно показать, что предполный класс является замкнутым. Действительно, если K — предполный класс, то $K \subseteq [K] \subset P_2$. Если допустить, что $K \neq [K]$, то существует хотя бы одна функция $f \in [K] \setminus K$. Но тогда $f \in P_2 \setminus K$. Следовательно, система $\{f\} \cup K$ полна. Это значит, что $[\{f\} \cup K] = P_2$. Поэтому $[K] \subset \{f\} \cup K$, чего быть не может, поскольку $\{f\} \cup K \subseteq [K]$. Поэтому наше предположение о том, что $K \subset$ $\subset [K]$ неверно и приходится заключить, что $K = [K]$, т.е. что класс K замкнут.

Согласно доказанной выше теореме, существует ровно 5 предполных классов — T_0, T_1, S, M, L. Действительно, если некоторый класс K булевых функций является предполным, и не совпадает ни с одним из указанных классов, то он ни в одном из них не содержится. Но тогда, по указанной теореме, этот класс является полным. Полученное противоречие показывает, что рассматриваемый случай невозможен.

Пример 5.2. Система $A = \{x_1x_2; 0; 1; x_1 \oplus x_2 \oplus x_3\}$ является полной.

Действительно, используя таблицы истинности, легко убедиться в том, что $x_1x_2 \notin S$, $0 \notin T_1$, $1 \notin T_0$, $x_1 \oplus x_2 \oplus x_3 \notin M$; $x_1x_2 \notin L$.

С другой стороны, так же с помощью таблиц истинности, можно показать, что

$$A_1 = \{0; 1; x_1 \oplus x_2 \oplus x_3\} \subset L,$$

$$A_2 = \{x_1x_2; 1; x_1 \oplus x_2 \oplus x_3\} \subset T_1,$$

$$A_3 = \{x_1x_2; 0; x_1 \oplus x_2 \oplus x_3\} \subset T_0,$$

$$A_4 = \{x_1x_2; 0; 1\} \subset M,$$

т.е. подсистемы A_1, A_2, A_3, A_4 не являются полными.

Определение 5.15. Система A из замкнутого класса M называется полной в M, если любая функция из M может быть задана формулой над A.

Определение 5.16. Система A из замкнутого класса M называется его *базисом*, если система A полна в M, но любая ее собственная подсистема не полна в M.

Пример 5.3. Система A из примера 5.2 является базисом в P_2.

Теорема 5.5 (О минимальном базисе). *Из любой полной системы булевых функций можно выделить подсистему, содержащую не более четырех функций, которая также полна.*

Доказательство. Пусть система K полна, тогда в ней существует полная подсистема K', состоящая не более чем из пяти функций не содержащихся в предполных классах. Возьмем функцию $f \in K'$ такую, что $f \notin T_0$. Это значит, что $f(0,0,\ldots,0)=1$. Если $f(1,1,\ldots,1)=0$, то $f \notin T_1$. Если же $f(1,1,\ldots,1)=1$, то $f \notin S$, следовательно эта функция f не принадлежит еще одному предполному классу. Следовательно, в подсистеме K' можно выделить подсистему K'', которая состоит из четырех функций и является полной.

Теорема доказана.

Ввиду примера 5.2 нельзя требовать дальнейшего уменьшения числа функций.

Теорема 5.6 (Первая теорема Поста). *Каждый замкнутый класс булевых функций имеет конечный базис.*

Теорема 5.7 (Вторая теорема Поста). *Множество всех замкнутых классов в P_2 счетно.*

6. Функции k-значной логики

6.1. Понятие функции k-значной логики

Обозначим через E_k множество $\{0, 1, \ldots, k-1\}$, $k \geqslant 2$.

Определение 6.1. Функция $f : E_k^n \mapsto E_k$ называется *функцией k-значной логики.*

Аналогично рассмотренным выше булевым функциям, определим *аргументы функции k-значной логики* как элементы некоторого множества $U = \{u_1, u_2, \ldots, u_m, \ldots\}$ и тогда запись $f(u_1, u_2, \ldots, u_n)$ будет означать функцию k-значной логики от n аргументов.

Так же как и для булевых функций, определим *наборы значений переменных* для функций k-значной логики, которые являются упорядоченными выборками с возвращением из множества E_k. Если $f(x_1, x_2, \ldots$ $\ldots, x_1)$ — некоторая функция k-значной логики и $(a_1, a_2, \ldots, x_n)$ — некоторый набор значений переменных $x_1, x_2, \ldots, x_n$, то $f(a_1, a_2, \ldots, a_n)$ есть *значение этой функции на наборе* $(a_1, a_2, \ldots, a_n)$, если это значение на указанном наборе определено (может быть и противное).

Обозначим через P_k *множество всех всюду определенных функций k-значной логики*, а через $P_k^{(n)}$ — *множество всех функций k-значной логики от n аргументов.* Так же как и для булевых функций будем использовать обозначение $\tilde{x}^n = (x_1, x_2, \ldots, x_n)$ и называть это выражение *векторным заданием аргумента.*

Функции k-значной логики так же как и булевы функции можно задавать с помощью таблицы в которой в первых n столбцах стоят все возможные наборы значений переменных, а в $n+1$ столбце — значения самой функции. Наборы значений переменных располагаются в том же естественном порядке.

x_1	x_2	x_3	$\cdots$	x_{n-2}	x_{n-1}	x_n	$f(\tilde{x}^n)$
0	0	0	$\cdots$	0	0	0	a_1
0	0	0	$\cdots$	0	0	1	a_2
0	0	0	$\cdots$	0	0	2	a_3
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
0	0	0	$\cdots$	0	0	$k-1$	a_k
0	0	0	$\cdots$	0	1	0	a_{k+1}
0	0	0	$\cdots$	0	1	1	a_{k+2}
0	0	0	$\cdots$	0	1	2	a_{k+3}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
0	0	0	$\cdots$	0	1	$k-1$	a_{2k}
0	0	0	$\cdots$	0	2	0	a_{2k+1}
0	0	0	$\cdots$	0	2	1	a_{2k+2}
0	0	0	$\cdots$	0	2	2	a_{2k+3}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
0	0	0	$\cdots$	0	2	$k-1$	a_{3k}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
0	0	0	$\cdots$	0	$k-1$	$k-1$	a_{k^2}
0	0	0	$\cdots$	1	0	0	a_{k^2+1}
0	0	0	$\cdots$	1	0	1	a_{k^2+2}
0	0	0	$\cdots$	1	0	2	a_{k^2+3}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
0	0	0	$\cdots$	1	0	$k-1$	a_{k^2+k}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$k-1$	$k-1$	$k-1$	$\cdots$	$k-1$	$k-1$	$k-2$	a_{k^n-1}
$k-1$	$k-1$	$k-1$	$\cdots$	$k-1$	$k-1$	$k-1$	a_{k^n}

Теорема 2.1 (О числе различных функций k-значной логики от n аргументов). $|P_k^{(n)}| = k^{k^n}$.

Доказательство. Число всевозможных упорядоченных выборок с возвращением из k элементов по n-элементов (т.е. число всевозможных упорядоченных строк таблицы истинности), согласно утверждению 6) теоремы 1.1, равно k^n. Для каждой строки таблицы истинности возможен один из k случаев — в этой строке функция может принимать одно из k значений. Следовательно, для каждого из наборов значений переменных снова происходит выбор из k-элементного множества. Поэтому, опять применив утверждение 6) теоремы 1.1, получим, что число различных булевых функций от n аргументов равно k^{k^n}.

Теорема доказана.

Определение 6.2. Функция k-значной логики $f(\tilde{x}^n)$ *существенно* зависит от переменной x_i $(1 \leqslant i \leqslant n)$, если существует такой набор $a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ значений переменных $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots$ $\ldots, x_n$, что по крайней мере хотя бы для двух значений a' и a'' переменной x_i таких, что $a' \neq a''$ выполняется

$$f(a_1, a_2, \ldots, a_{i-1}, a', a_{i+1}, \ldots, a_n) \neq$$
$$f(a_1, a_2, \ldots, a_{i-1}, a'', a_{i+1}, \ldots, a_n).$$

Переменная x_i называется *существенной переменной*. Если переменная не является существенной, то она называется *фиктивной*.

Замечание 6.1. *Отметим, что для функций k-значной логики понятие фиктивной переменной оказывается несколько более сложным, нежели понятие фиктивной переменной для булевой функции. Если некоторая переменная x_i является фиктивной переменной для функции k-значной логики $f(\tilde{x}^n)$, то для любого набора $a_1, a_2, \ldots$ $\ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ значений переменных $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ и для любых значений a' и a'' переменной x_i выполняется*

$$f(a_1, a_2, \ldots, a_{i-1}, a', a_{i+1}, \ldots, a_n) =$$
$$f(a_1, a_2, \ldots, a_{i-1}, a'', a_{i+1}, \ldots, a_n).$$

Определение 6.3. Пусть функция k-значной логики $f(\tilde{x}^n)$ задана таблично и для некоторого $i = 1, 2, \ldots, n$ переменная x_i является ее фиктивной переменной. Вычеркивание из этой таблицы столбца в котором стоит переменная x_i и всех строк, которые соответствуют наборам

$$(a_1, a_2, \ldots, a_{i-1}, a', a_{i+1}, \ldots, a_n)$$

(где $(a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ — некоторые наборы переменных $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ и $a' = 1, 2, \ldots, k-1$), задает функцию k-значной логики $f_1(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ от $n-1$ переменных. Такое вычеркивание называется *удалением фиктивной переменной x_i*.

Определение 6.4. Операция, обратная операции удаления фиктивной переменной называется *операцией введения фиктивной переменной*.

Определение 6.5. Две функции k-значной логики называются *равными*, если одна из них может быть получена из другой, путем удаления или введения фиктивных переменных.

Можно дать еще одно определение равенства функций k-значной логики, из которого непосредственно следует метод истинностных таблиц.

Определение 6.6. Две функции k-значной логики f_1 и f_2 называются *равными*, если на одних и тех же наборах значений переменных значения функций равны.

Ввиду рассмотренных операций введения и удаления фиктивных переменных, как и для булевых функций, для функций k-значной логики справедливо следующее довольно простое, но вместе с тем очень важное утверждение.

Замечание 6.2. *Любое множество функций k-значной логики $f_1, f_2, \dots, f_s$ можно рассматривать как множество функций зависящих от одних и тех же переменных.*

Определение 6.7. *Элементарными* функциями k-значной логики называют следующие функции:

1) *константы* $0, 1, \dots, k-1$;

2) $\overline{x} = x + 1 \pmod k$ — *отрицание Поста или циклический сдвиг (первое обобщение отрицания)*;

3) $\sim x = k - 1 - x$ — *отрицание Лукасевича (второе обобщение отрицания)*;

4) $I_m(x) = \begin{cases} k-1, & x = m, \\ 0, & x \neq m, \end{cases}$ где $0 \leqslant m \leqslant k-1$;

5) $J_m(x) = \begin{cases} 1, & x = m, \\ 0, & x \neq m, \end{cases}$ — *характеристическая функция числа m*, где $0 \leqslant m \leqslant k-1$;

6) $\min(x_1, x_2)$ — *обобщение конъюнкции*;

7) $\max(x_1, x_2)$ — *обобщение дизъюнкции*;

8) $x_1 * x_2 \pmod k$ — *умножение по модулю k* или *второе обобщение конъюнкции*;

9) $x_1 + x_2 \pmod k$ — *сложение по модулю k*,

которые зададим с помощью истинностных таблиц.

x	0	1	$\ldots$	$k-1$	$\overline{x}$	$\sim x$	$I_m(x)$	$J_m(x)$
0	0	1	$\ldots$	$k-1$	1	$k-1$	0	0
1	0	1	$\ldots$	$k-1$	2	$k-2$	0	0
2	0	1	$\ldots$	$k-1$	3	$k-3$	0	0
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$m-1$	0	1	$\ldots$	$k-1$	m	$k-m-1$	0	0
m	0	1	$\ldots$	$k-1$	$m+1$	$k-m-2$	1	$k-1$
$m+1$	0	1	$\ldots$	$k-1$	$m+2$	$k-m-3$	0	0
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$k-2$	0	1	$\ldots$	$k-1$	$k-1$	1	0	0
$k-1$	0	1	$\ldots$	$k-1$	0	0	0	0

x_1	x_2	$min(x_1, x_2)$	$max(x_1, x_2)$	$x_1 + x_2$	$x_1 * x_2$
0	0	0	0	0	0
0	1	0	1	1	0
0	2	0	2	2	0
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
0	$k-1$	0	$k-1$	$k-1$	0
1	0	0	1	1	0
1	1	1	1	2	1
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	$k-1$	1	$k-1$	0	$k-1$
2	0	0	2	2	0
2	1	1	2	3	2
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$k-1$	$k-2$	$k-2$	$k-2$	$k-3$	1
$k-1$	$k-1$	$k-1$	$k-1$	$k-2$	0

Множество всех элементарных функций k-значной логики будем обозначать через P_k^0.

6.2. Реализации функций k-значной логики формулами. Основные равносильности

Пусть F — некоторое непустое множество функций k-значной логики. Аналогично булевым функциям, используя те же фразы и обозначения, легко определить понятие *формулы* над множеством F, *подформулы*, *суперпозиции функций* из множества F и *эквивалентных формул* для функций k-значной логики. Например, суперпозициями функций из P_k^0 являются следующие функции для любой функции $f(\tilde{x}^n)$:

$$K_{\tilde{x}}^f(\tilde{x}^n) = \min(I_{a_1}(x_1), I_{a_2}(x_2), \dots, I_{a_n}(x_n), f(a_1, a_2, \dots, a_n));$$

$$C_{\tilde{x}}^f(\tilde{x}^n) = J_{a_1}(x_1) * J_{a_2}(x_2) * \dots * J_{a_n}(x_n) * f(a_1, a_2, \dots, a_n);$$

$$D_{\tilde{x}}^f(\tilde{x}^n) = \max(\sim I_{a_1}(x_1), \sim I_{a_2}(x_2), \dots, \sim I_{a_n}(x_n), f(a_1, a_2, \dots, a_n)),$$

Если переменные $x_1, x_2, \dots, x_n$ принимают значения набора $(a_1, a_2, \dots$ $\dots, a_n)$, то из приведенных выше равенств получим:

$$K_{\tilde{x}}^f(a_1, a_2, \dots, a_n) = C_{\tilde{x}}^f(a_1, a_2, \dots, a_n) = \\ = D_{\tilde{x}}^f(a_1, a_2, \dots, a_n) = f(a_1, a_2, \dots, a_n). \tag{3.1}$$

Если же переменные $x_1, x_2, \dots, x_n$ принимают значения какого-либо другого, отличного от $(a_1, a_2, \dots, a_n)$ набора $(b_1, b_2, \dots, b_n)$ то получаем следующие равенства:

$$K_{\tilde{x}}^f(b_1, b_2, \dots, b_n) = C_{\tilde{x}}^f(b_1, b_2, \dots, b_n) = 0 \tag{3.2}$$

$$D_{\tilde{x}}^f(b_1, b_2, \dots, b_n) = k - 1. \tag{3.3}$$

Свойство 6.1. *Для элементарных функций k-значной логики справедливы следующие утверждения:*

1. Ассоциативные законы:

1.1. $x_1 * (x_2 * x_3 \pmod k) \pmod k = (x_1 * x_2 \pmod k) * x_3 \pmod k)$;

1.2. $x_1 + (x_2 + x_3 \pmod k) \pmod k = (x_1 + x_2 \pmod k)) + x_3 \pmod k)$;

1.3. $min(min(x_1, x_2), x_3) = min(x_1, min(x_2, x_3))$;

1.4. $max(max(x_1, x_2), x_3) = max(x_1, max(x_2, x_3))$;

2. Коммутативные законы:

2.1. $x_1 * x_2 = x_2 * x_1$;

2.2. $x_1 + x_2 = x_2 + x_1$;

2.3. $min(x_1, x_2) = min(x_2, x_1)$;

2.4. $max(x_1, x_2) = max(x_2, x_1)$;

3. Дистрибутивные законы:

3.1. $min(max(x_1, x_2), x_3) = max(min(x_1, x_3), min(x_2, x_3))$;

3.2. $max(min(x_1, x_2), x_3) = min(max(x_1, x_3), max(x_2, x_3))$;

3.3. $x_1 * (x_2 + x_3) \pmod k = (x_1 * x_2) + (x_1 * x_3) \pmod k$.

Обозначим через $x_1 \wedge x_2$ операцию $\min(x_1, x_2)$, а через $x_1 \vee x_2$ операцию $\max(x_1 x_2)$. Будем считать, что вначале выполняется конъюнкция, а затем дизъюнкция.

Свойство 6.2. *Для элементарных функций k-значной логики справедливы следующие утверждения:*

$$1. I_\sigma(I_\tau(x)) = \begin{cases} I_0(x) \vee I_1(x) \vee \ldots \vee I_{\tau-1}(x) \vee \\ I_{\tau+1}(x) \vee \ldots \vee I_{k-1}(x), \\ \text{если } \sigma = 0; \\ 0, \text{если } 0 < \sigma < k-1; \\ I_\tau(x), \text{если } \sigma = k-1. \end{cases}$$

$$2. I_\sigma(x_1 \wedge x_2) = I_\sigma(x_1) \wedge (I_\sigma(x_2) \vee I_{\sigma+1}(x_2) \vee \ldots \vee I_{k-1}(x_2)) \vee$$
$$I_\sigma(x_2) \wedge (I_\sigma(x_1) \vee I_{\sigma+1}(x+1) \ldots \vee I_{k-1}(x_1));$$

$$3. I_\sigma(x_1 \vee x_2) = I_\sigma(x_1) \wedge (I_0(x_2) \vee I_1(x_2) \vee \ldots \vee I_\sigma(x_2)) \vee$$
$$I_\sigma(x_2) \wedge (I_0(x_1) \vee I_1(x_1) \vee \ldots \vee I_\sigma(x_1));$$

$$4. x = 1 \wedge I_1(x) \vee 2 \wedge I_2(x) \vee \ldots \vee (k-1) \wedge I_{k-1}(x);$$

$$5. x_1 = x_1 \wedge (I_0(x_2) \vee I_1(x_2) \vee \ldots \vee I_{k-1}(x_2));$$

$$I_\sigma(x) \wedge I_\tau(x) = \begin{cases} I_\sigma(x), & \text{если } \sigma = \tau, \\ 0, & \text{если } \sigma \neq \tau. \end{cases}$$

$$(k-1) \wedge x = x; \quad (k-1) \vee x = k-1;$$

$$0 \wedge x = 0; \quad 0 \vee x = x.$$

Замечание 6.3. *Рассмотренные свойства, справедливые для функций k-значной логики могут служить основанием предположению о том, что эти свойства являются обобщением свойств соответствующих булевых функций. Однако это происходит не всегда. Например, при $k \geqslant 3$, получаем следующие утверждения:*

$$\sim(\sim x) = x; \qquad \overline{\overline{x}} \neq x;$$

$$\sim\max(x_1, x_2) = \min(\sim x_1, \sim x_2);$$

$$\overline{\max}(x_1, x_2) \neq \min(\overline{x}_1, \overline{x}_2).$$

Из равенств (3.1)–(3.3) вытекает следующая теорема.

Теорема 6.2. *Для любой функции k-значной логики имеют место следующие свойства:*

$$f(\tilde{x}^n) = \bigvee_{\sigma_1,\sigma_2,\ldots,\sigma_n} K_{\tilde{x}}^f(\tilde{x}^n) \tag{6.1}$$

$$f(\tilde{x}^n) = \sum_{\sigma_1,\sigma_2,\ldots,\sigma_n} C_{\tilde{x}}^f(\tilde{x}^n) \pmod k \tag{6.2}$$

$$f(\tilde{x}^n) = \bigwedge_{\sigma_1,\sigma_2,\ldots,\sigma_n} D_{\tilde{x}}^f(\tilde{x}^n) \tag{6.3}$$

Операции здесь берутся по всем наборам $\tilde{x}$ из E_k^n.

Правые части равенств (6.1)–(6.3) называются соответственно первой, второй и третьей формами представления функций k-значной логики.

Таким образом, для функций k-значной логики существуют способы разложения, аналогично дизъюнктивной, конъюнктивной и импликативной формам булевых функций.

7. Схемы из функциональных элементов

7.1. Дискретные преобразователи

В современной электронной технике, а в особенности в электронных вычислительных устройствах, важное место занимают так называемые дискретные преобразователи.

Определение 7.1. *Дискретным преобразователем* называется устройство, которое обладает некоторым числом входов и выходов и преобразует наборы сигналов, поступающие на входы в наборы сигналов, поступающие на выходы. Наборы сигналов берутся из некоторого конечного множества.

Мы будем рассматривать такие дискретные преобразователи в которых временем преобразования сигнала можно пренебречь. В качестве множества из которого берутся сигналы будем рассматривать множество $\{0, 1\}$. Техническая реализация таких дискретных преобразователей оказывается очень простой, поскольку значение сигнала 0 можно отождествить со слабым сигналом, а значение сигнала 1 — с сильным. С такой задачей с успехом справляются полупроводниковые приборы, технологические разработки которых в настоящее время находятся на достаточно высоком уровне. Кроме того, сохранение информации о сигналах такого типа легко осуществимо ввиду еще одного отождествления: сигнал 0 эквивалентен полностью разряженному конденсатору, а сигнал 1 — полностью заряженному.

7.2. Контактные схемы

Наиболее простой разновидностью дискретных преобразователей являются *Контактные схемы.*

Определение 7.2. *Контактной схемой* называется схема, состоящая из следующих элементов:

1) замыкающие контакты (которым соответствуют некоторые пропозициональные переменные);

2) размыкающие контакты (которым соответствуют отрицания некоторых пропозициональных переменных);

3) последовательное соединение контактов (которым соответствует конъюнкция некоторых пропозициональных переменных или их отрицаний);

4) параллельное соединение контактов (которым соответствует дизъюнкция некоторых пропозициональных переменных или или их отрицаний).

Поскольку каждый из определенных выше элементов контактной схемы можно рассматривать как некоторую булеву функцию, то их можно отождествить с некоторыми пропозициональными переменными и тогда, согласно принципу суперпозиции, возможно построение более сложных схем (рис. 6).

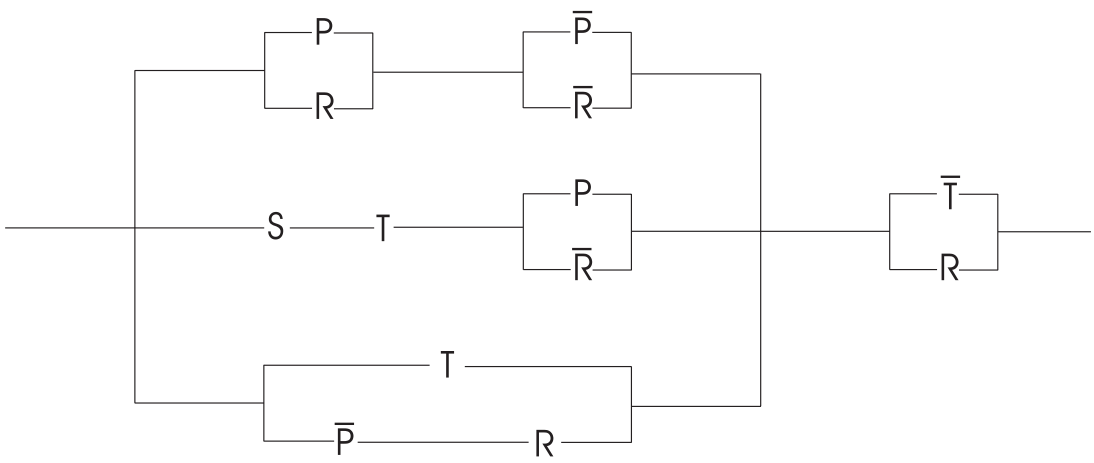


Рис. 6

Между множеством всех контактных схем и всех булевых функциях, построенных над базисом ⌉, ∨, ∧ очевидно взаимно-однозначное соответствие: для каждой контактной схемы можно построить над базисом ⌉, ∨, ∧ единственную булеву функцию и, с другой стороны, для каждой булевой функции, построенной над базисом ⌉, ∨, ∧, можно построить единственную контактную схему. Таким образом, для контактных схем можно сформулировать следующие задачи.

Задача синтеза. Как по известным условиям работы некоторого контактного устройства построить его схему.

Задача анализа. Как по известной схеме контактного устройства определить условия его работы.

Задача упрощения. Задача упрощения состоит из следующих этапов:

1) решить задачу анализа и построить для данного контактного устройства соответствующую формулу;

2) используя законы для булевых функций, максимально упростить полученную формулу;

3) построить контактную схему, которая соответствует упрощенной формуле и, следовательно, содержит меньшее число контактов.

Решать эти задачи помогают таблицы истинности.

Контактные схемы используются во многих устройствах: схемы для голосования, электронные управляющие схемы различных типов и т.д.

7.3. Понятие схемы из функциональных элементов

Теория контактных схем оказывается несостоятельной при решении более сложных задач. Более сложные задачи и, в частности, задачи вычисления для арифметических операций, способны решить так называемые схемы из функциональных элементов.

Определение 7.3. Функциональным элементом называется математическая модель дискретного преобразователя с одним выходом, у которого время преобразования сигнала мало по сравнению с длительностью сигнала.

Определим сначала структуру схемы из функциональных элементов.

1. Берется некоторое конечное множество $F = F_1, F_2, \ldots, F_k$ функциональных элементов. Каждый элемент имеет n_i входов и один выход (рис.7).

2. Строится *логическая сеть* Σ, представляющая собой объект в котором имеется некоторое число n входов и некоторое число p выходов (рис. 8). Построение цепи осуществляется по следующим правилам:

а). Одна изолированная вершина, которая является одновременно входом и выходом, называется *тривиальной логической сетью* (рис. 9).

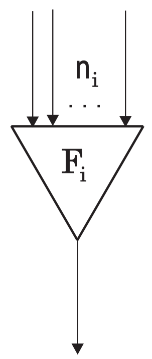


Рис. 7

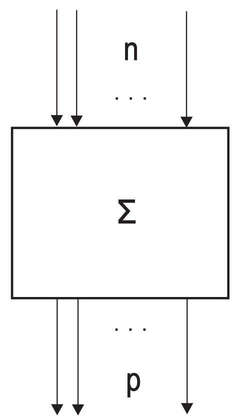


Рис. 8

Рис. 9

б). Если даны две непересекающиеся сети Σ_1 и Σ_2, имеющие соответственно n_1 и n_2 входов и p_1 и p_2 выходов, то к этим сетям можно применить *операцию объединения непересекающихся сетей*, в результате которой получается новая сеть Σ', входами которой являются все входы сетей Σ_1 и Σ_2, а выходами — выходы этих сетей. Таким образом, сеть Σ' имеет $n_1 + n_2$ входов и $p_1 + p_2$ выходов (рис. 10).

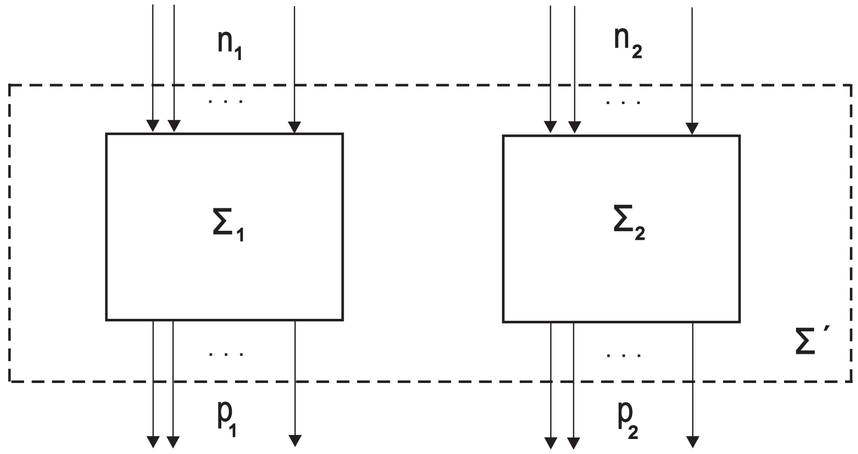


Рис. 10

в). Если дана некоторая логическая сеть Σ с n входами и p выходами и элемент F с n_i входами, причем $p \geqslant n_i$ и среди выходов сети Σ выбраны выходы $j_1, j_2, \ldots, j_{n_i}$. Тогда можно применить *операцию присоединения элемента*, в результате которой получается логическая сеть Σ'', входами которой являются входы сети Σ, а выходами — выход элемента F и все выходы сети Σ кроме выходов $j_1, j_2, \ldots, j_{n_i}$. Таким образом, логическая сеть Σ'' имеет n входов и $p - n_i + 1$ выходов (рис. 11).

г). Если дана некоторая логическая сеть Σ с n входами и p выходами и в этой сети выделен некоторый выход j. Тогда можно применить *операцию расщепления выхода*, в результате которой получится логическая сеть Σ''', входами которой являются все входы сети Σ, а выходами — выходы $1, 2, \ldots, i-1, i+1, \ldots, p$ и еще два выхода, возникших из выхода с номером j сети Σ. Таким образом, логическая сеть Σ имеет n входов и $p + 1$ выход (рис. 12).

3. Пусть заданы алфавиты некоторых переменных $X = \{x_1, x_2, \ldots$ $\ldots, x_i, \ldots\}$ и $Z = \{z_1, z_2, \ldots, z_i, \ldots\}$ и пусть дана некоторая логическая сеть Σ, которая имеет n входов и p выходов. *Схемой из функциональных элементов* называется логическая сеть, входам и выходам которой при-

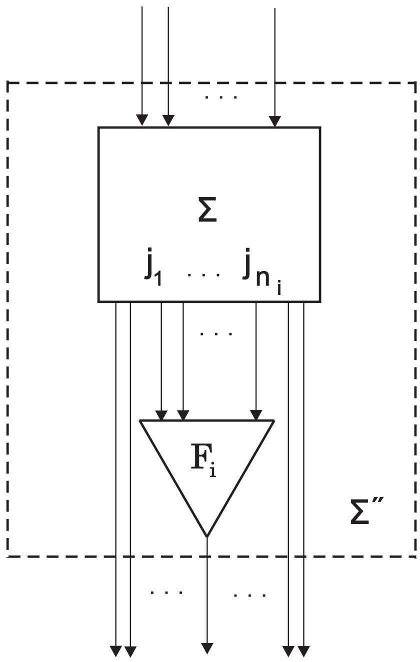


Рис. 11

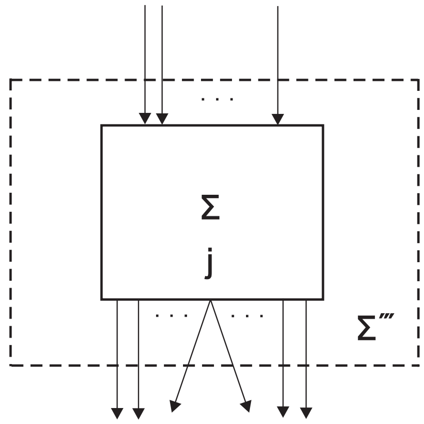


Рис. 12

писаны различные буквы $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ и $z_{j_1}, z_{j_2}, \ldots, z_{j_n}$ соответственно из алфавитов X и Z (рис. 13). Полученная таким образом схема обозначается

$$\Sigma(x_{i_1}, x_{i_2}, \ldots, x_{i_n}; z_{j_1}, z_{j_2}, \ldots, z_{j_n}).$$

Если множество F состоит из трех элементов, которые соответствуют отрицанию, конъюнкции и дизъюнкции (рис. 14), то фигуры Σ_1 (рис. 15) и Σ_2 (рис. 16) являются схемами из функциональных элементов.

Определим теперь функционирование схемы из функциональных элементов.

Пусть $\Sigma(x_1, x_2, \ldots, x_n; z_1, z_2, \ldots, z_p)$ — схема из функциональных элементов. Каждому элементу множества F поставим в соответствие некоторую булеву функцию. Тогда, используя правила построения формул и законы для булевых функций, указанной схеме из функциональных элементов можно сопоставить систему уравнений булевых функций:

$$z_1 = f_1(x_1, x_2, \ldots, x_n);$$
$$z_2 = f_2(x_1, x_2, \ldots, x_n);$$
$$\ldots$$
$$z_p = f_p(x_1, x_2, \ldots, x_n);$$

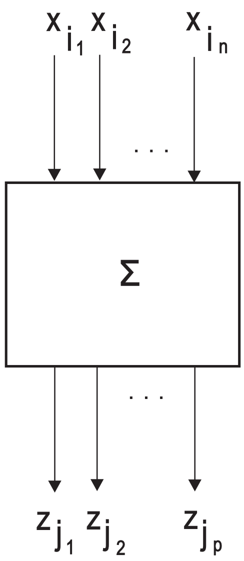


Рис. 13

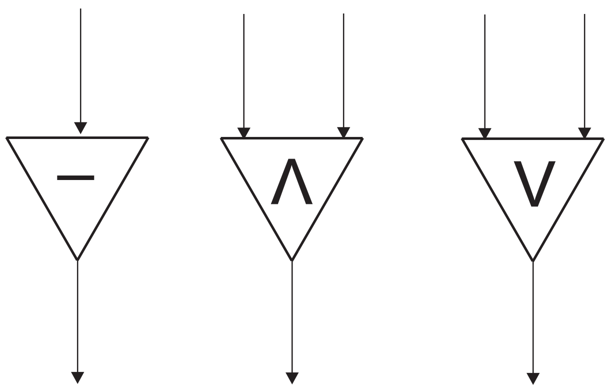


Рис. 14

Эта система уравнений называется *проводимостью данной схемы из функциональных элементов*

Рассмотрим построение проводимости для каждой из рассмотренных выше операций для логических сетей.

а). Если Σ — тривиальная схема (т.е. схема, построенная на тривиальной логической сети), то ей соответствует одно уравнение

$$z_1 = x_1$$

и проводимость есть тождественная функция.

б). Если Σ_1 и Σ_2 — схемы из функциональных элементов, сети которых не пересекаются и входам и выходам которых сопоставлены различные переменные, то их можно обозначить следующим образом

$$\Sigma_1(x_1, x_2, \ldots, x_n; z_1, z_2, \ldots, z_p);$$

$$\Sigma_2(x_{n+1}, x_{n+2}, \ldots, x_{n+m}; z_{p+1}, z_{p+2}, \ldots, z_{p+q}),$$

где n и m — число входов соответственно схем Σ_1 и Σ_2, а p и q — число их выходов. Пусть указанным схемам соответствуют системы уравнений

$$\begin{aligned} z_1 &= f_1(x_1, x_2, \ldots, x_n); \\ z_2 &= f_2(x_1, x_2, \ldots, x_n); \\ &\ldots \\ z_p &= f_p(x_1, x_2, \ldots, x_n); \end{aligned} \tag{$*$}$$

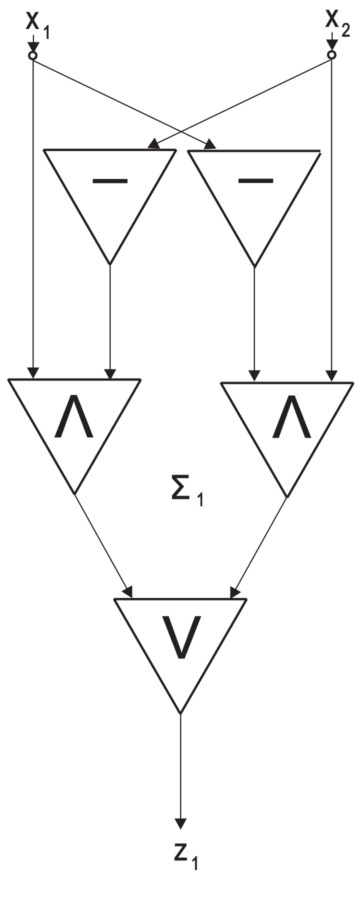


Рис. 15

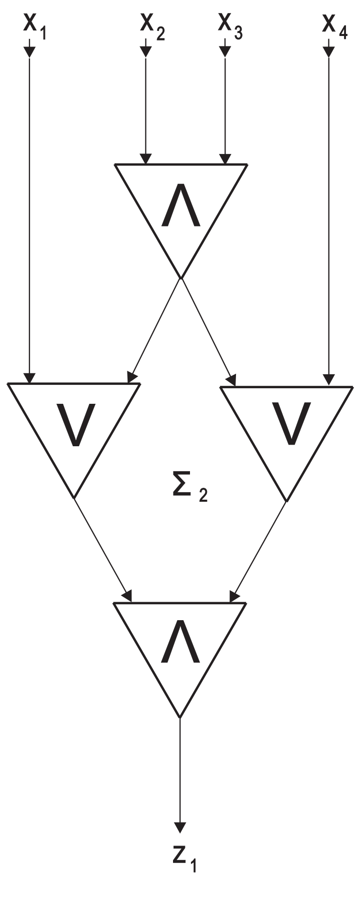


Рис. 16

и

$$
\begin{aligned}
z_{p+1} &= f_{p+1}(x_{n+1}, x_{n+2}, \ldots, x_{n+m});\\
z_{p+2} &= f_{p+2}(x_{n+1}, x_{n+2}, \ldots, x_{n+m});\\
&\ldots \qquad\qquad (**)\\
z_{p+q} &= f_{p+q}(x_{n+1}, x_{n+2}, \ldots, x_{n+m}).
\end{aligned}
$$

Тогда схеме $\Sigma'(x_1, x_2, \ldots x_{n+m}; z_1, z_2, \ldots, z_{p+q})$, которая является объединением схем Σ_1 и Σ_2, можно поставить в соответствие систему уравнений, которая представляет собой объединение систем уравнений (*) и (**):

$$
\begin{aligned}
z_1 &= f_1'(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m});\\
z_2 &= f_2'(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m});\\
&\ldots\\
z_p &= f_p'(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m});\\
z_{p+1} &= f_{p+1}'(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m})\\
z_{p+2} &= f_{p+2}'(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m})\\
&\ldots\\
z_{p+q} &= f_{p+q}'(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+m}),
\end{aligned}
$$

где функции $f_1', f_2', \ldots, f_p'$ не зависят существенно от переменных $x_{p+1}, x_{p+2}, \ldots, x_{n+m}$, а функции $f_{p+1}', f_{p+2}', \ldots, f_{p+q}'$ не зависят существенно от переменных $x_1, x_2, \ldots, x_n$ и

$$
f_1' = f_1, \quad f_2' = f_2, \ldots, f_p' = f_p,
$$

$$
f_{p+1}' = f_{p+1}, \quad f_{p+2}' = f_{p+2}, \ldots, f_{p+q}' = f_{p+q}.
$$

в). Пусть схема

$$
\Sigma''(x_1, \ldots, x_n; z_1, \ldots, z_{j_1-1}, z_{j_1+1}, \ldots, z_{j_{n_i}+1}, \ldots, z_p)
$$

получена из схемы $\Sigma(x_1, x_2, \ldots, x_n; z_1, z_2, \ldots, z_p)$ путем присоединения к выходам $z_{j_1}, z_{j_2}, \ldots, z_{j_{n_i}}$ входов элемента F_i и полученному новому выходу присвоена буква z_{p+1}. Тогда схеме Σ'' можно сопоставить систему уравнений, которая получается из (*) вычеркиванием $j_1, j_2, \ldots, j_{n_i}$ строчек и добавлением строки

$$
z_{p+1} = f_i^0(f_{j_1}(x_1, x_2, \ldots, x_n), \ldots, f_{j_{n_i}}(x_1, x_2, \ldots, x_n)).
$$

Таким образом, мы получим систему уравнений

$$z_1 = f_1(x_1, x_2, \ldots, x_n),$$

$$z_2 = f_2(x_1, x_2, \ldots, x_n),$$

$$\ldots$$

$$z_{j_1-1} = f_{j_1-1}(x_1, x_2, \ldots, x_n),$$

$$z_{j_1+1} = f_{j_1+1}(x_1, x_2, \ldots, x_n),$$

$$\ldots$$

$$z_{j_{n_i}-1} = f_{j_{n_i}-1}(x_1, x_2, \ldots, x_n),$$

$$z_{j_{n_i}+1} = f_{j_{n_i}-1}(x_1, x_2, \ldots, x_n),$$

$$\ldots$$

$$z_p = f_p(x_1, x_2, \ldots, x_n),$$

$$z_{p+1} = f_i^0(f_{j_1}(x_1, x_2, \ldots, x_n), \ldots, f_{j_n}(x_1, x_2, \ldots, x_n)).$$

г). Пусть схема $\Sigma'''(x_1, x_2, \ldots, x_n; z_1, z_2, \ldots, z_p, z_{p+1})$ получена из схемы $\Sigma(x_1, x_2, \ldots, x_n; z_1, z_2, \ldots, z_p)$ расщеплением выхода с номером j на два выхода и полученным выходам присвоены соответственно буквы z_j и z_{p+1}. Тогда этой схеме можно поставить в соответствие систему уравнений

$$z_1 = f_1(x_1, x_2, \ldots, x_n),$$

$$z_2 = f_2(x_1, x_2, \ldots, x_n),$$

$$\ldots$$

$$z_{j-1} = f_{j_1}(x_1, x_2, \ldots, x_n),$$

$$z_j = f_j(x_1, x_2, \ldots, x_n),$$

$$z_{j+1} = f_{j+1}(x_1, x_2, \ldots, x_n),$$

$$\ldots$$

$$z_p = f_p(x_1, x_2, \ldots, x_n),$$

$$z_{p+1} = f_p(x_1, x_2, \ldots, x_n).$$

Таким образом, каждой из рассмотренных нами схем из функциональных элементов может быть сопоставлена система уравнений, каждое из которых определяется некоторой булевой функцией.

Обозначим через $\mathfrak{S}$ класс всех схем из функциональных элементов над F, а через $\mathfrak{S}_0$ класс всех тех схем из функциональных элементов над F у которых имеется ровно один выход и разветвления имеются только на входах. Пусть $\mathfrak{B}$ — некоторая система булевых функций. Обозначим через $\mathfrak{S}_{\mathfrak{B}}$ класс формул над системой $\mathfrak{B}$. Поскольку всякая булева функция может быть рассмотрена как некоторый функциональный элемент с некоторым количеством входов и одним выходом, то очевидно, что каждой формуле из класса $\mathfrak{S}_{\mathfrak{B}}$ можно единственным образом сопоставить некоторую схему из $\mathfrak{S}_0$. Допустим теперь, что некоторая схема Σ содержит элемент F_i, у которого на выходе есть j разветвлений. Тогда этот элемент можно заменить на j элементов $F_{i_1}, F_{i_2}, \ldots, F_{i_j}$ у которых на выходах разветвления отсутствуют (рис. 17).

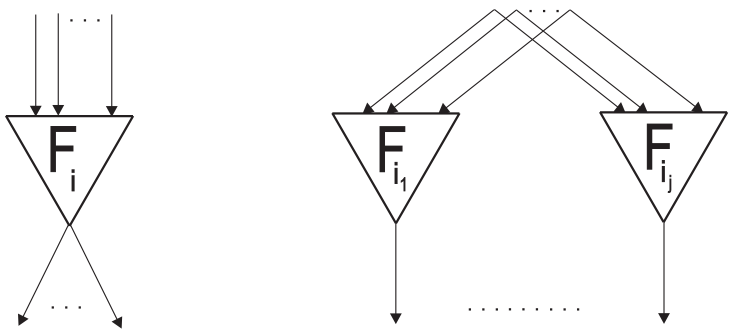


Рис. 17

Следовательно, если система $\mathfrak{B}$ полна, то для схемы Σ можно составить некоторую формулу из класса $\mathfrak{S}_{\mathfrak{B}}$.

Таким образом, мы доказали теорему.

Теорема 7.1. *Для того, чтобы для произвольной системы булевых уравнений*

$$z_1 = f_1(x_1, x_2, \ldots, x_n);$$
$$z_2 = f_2(x_1, x_2, \ldots, x_n);$$
$$\ldots$$
$$z_p = f_p(x_1, x_2, \ldots, x_n).$$

существовала схема $\Sigma(x_1, x_2, \ldots, x_n, z_1, z_2, \ldots, z_p)$ в некотором базисе функциональных элементов, которая реализует эту систему уравнений, необходимо и достаточно, чтобы система булевых функций

$$f_1, f_2, \ldots, f_n.$$

соответствующих этому базису была полной.

7.4. Проблема синтеза схем из функциональных элементов

Проблема синтеза схем из функциональных элементов заключается в следующем.

Пусть задан некоторый базис F функциональных элементов и взята произвольная система булевых уравнений

$$z_1 = f_1(x_1, x_2, \ldots, x_n);$$

$$z_2 = f_2(x_1, x_2, \ldots, x_n);$$

$$\ldots$$

$$z_p = f_p(x_1, x_2, \ldots, x_n).$$

Требуется построить схему $\Sigma(x_1, x_2, \ldots, x_n, z_1, z_2, \ldots, z_p)$ из функциональных элементов над данным базисом, которая реализует данную систему уравнений.

Ввиду приведенной выше теоремы, решение проблемы синтеза существует, если система булевых функций, соответствующих базису F была полной. При изучении булевых функций мы видели, что любая булева функция может быть реализована множеством формул. Уже по этой причине проблема синтеза имеет много решений. Поэтому возникает необходимость выбора среди них более оптимального решения.

Определение 7.4. *Сложностью схемы* Σ называется функционал $L(\Sigma)$, который равен числу элементов схемы.

Определение 7.5. Схема называется *минимальной*, если она имеет наименьшее значение сложности среди всех схем, реализующих одну и ту же систему булевых уравнений.

Определение 7.6. Пусть имеется некоторое количество входов, выходов и функциональных элементов. *Соединением* S данных входов, выходов и элементов называется геометрическая фигура, состоящая из этих объектов, такая, что каждый вход подключен либо к входу, либо к выходу и каждый выход подключен либо к входу, либо к выходу.

Любая схема из функциональных элементов является, очевидно, соединением. Однако не всякое соединение является схемой из функциональных элементов (рис. 18, 19).

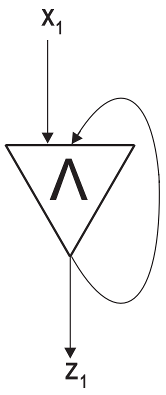


Рис. 18

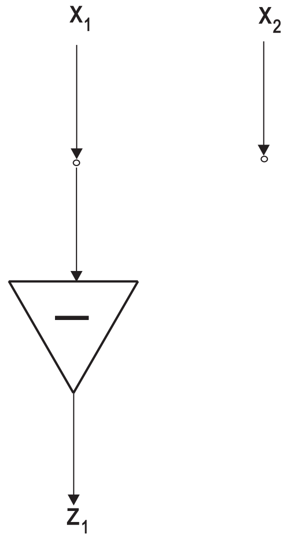


Рис. 19

Лемма 7.1. *Число $S^*(n,p,h)$ всех соединений, содержащих n входов $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$, p выходов $z_{j_1}, z_{j_2}, \ldots, z_{j_p}$ и h функциональных элементов не превосходит*

$$H_r^h \cdot (n+h)^{hv+p},$$

где $v = max_{1 \leqslant i \leqslant r} n_i$ и r — число всех элементов базиса.

Доказательство. Выберем h функциональных элементов , что можно осуществить H_r^h способами. Поскольку v — это число входов элемента с самым большим числом входов, то множество всех выходов и входов выбранных элементов не превышает $hv+p$ штук. Подключим их либо к входам, либо к выходам элементов, число которых равно $n+h$. Мы получим упорядоченную выборку без возвращения из $n+h$ элементов по $hv+p$ элементов. Число всех возможных выборок будет равно

$$(n+h)^{hv+p}.$$

Поскольку же выбор функциональных элементов и выбор вариантов подключения — независимые события, то, применив правило произведения, получим, что число рассматриваемых соединений не превосходит

$$H_r^h \cdot (n+h)^{hv+p}.$$

Лемма доказана.

Следствие 7.1. *Число $S(n,p,h)$ схем из функциональных элементов, содержащих n входов $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$, p выходов $z_{j_1}, z_{j_2}, \ldots, z_{j_p}$ и h функциональных элементов удовлетворяет неравенству*

$$S(n,p,h) \leqslant S^*(n,p,h) \leqslant H_r^h \cdot (n+h)^{hv+p} \leqslant r^h \cdot (n+h)^{hv+p}.$$

Выше мы определили операции для логических сетей. Такие же операции можно определить и для соединений:

I *операция объединения двух соединений.*

II*операция подключения элемента.*

III*операция разветвления выхода.*

Очевидны следующие две леммы.

Лемма 7.2. *Результат применения операций I,II,III к соединениям является соединением.*

Лемма 7.3. *Соединение, отличное от тривиальной схемы является схемой тогда и только тогда, когда выполнено одно из следующих условий:*

1) соединение получается объединением соединений, которые являются схемами;

2) соединение получается из некоторой схемы путем подключения некоторого элемента;

3) соединение получается из некоторой схемы путем разветвления выхода.

Теорема 7.2. *Существует алгоритм, который для каждого соединения выясняет, является ли оно схемой или нет.*

Доказательство. Доказательство проведем индукцией по числу d связей соединения S. При $d = 1$ соединение S либо не является схемой, либо является тривиальной схемой.

Допустим теперь, что теорема выполняется для всех $d = 1, 2, \dots t$. Покажем, что она справедлива и для $d = t + 1$. Пусть S — некоторое соединение, которое имеет $t+1$ связь. Тогда возможны следующие случаи:

1. S не получается из соединений с меньшим числом связей путем применения ни одной из операций 1)-3). Тогда очевидно, что рассматриваемое соединение не является схемой.

2. S является результатом операции над соединениями с меньшим числом связей. В этом случае достаточно рассмотреть все варианты разложений. Это возможно поскольку вариантов разложения — конечное число. Затем выясняем для компонент разложения, являются ли они схемами или нет, что возможно сделать ввиду предположения индукции. Если найдется такое разложение, все компоненты которого являются схемами, то, ввиду предыдущей леммы, соединение S является схемой. Если же в каждом из возможных разложений хотя бы одна из компонент не будет схемой, то соединение S не будет схемой.

Теорема доказана.

Теорема 7.3. *Существует алгоритм, который для каждой системы булевых уравнений, строит минимальную схему Σ.*

Доказательство. Пусть система уравнений имеет следующий вид:

$$z_1 = f_1(x_1, x_2, \ldots, x_n);$$

$$z_2 = f_2(x_1, x_2, \ldots, x_n);$$

$$\ldots$$

$$z_p = f_p(x_1, x_2, \ldots, x_n).$$

Нужно просмотреть все возможные соединения с входами $x_1, x_2, \ldots, x_n$ и выходами $z_1, z_2, \ldots, z_p$ у которых число элементов равно h.

Пусть сначала $h = 0$. Тогда мы получим некоторое конечное число соединений, которые не содержат элементов вообще. Применив алгоритм распознавания, выясняем, является ли данное соединение схемой. Если это соединение является схемой, то выясняем, реализует ли оно данную систему уравнений. в конечном итоге, требуемая схема либо найдется (в этом случае она будет минимальной), либо среди схем сложности $L(\Sigma) = 0$ искомой схемы нет и эта схема имеет порядок сложности $L(\Sigma) > 0$.

Пусть теперь $h = 1$. Получим некоторое конечное число соединений, которые содержат один элемент. Поступая как и выше, мы либо найдем требуемую схему, либо придем к выводу, что среди рассматриваемых соединений искомой схемы снова нет и что порядок сложности этой схемы $L(\Sigma) > 1$.

Поскольку рассматриваемая в условии система функций является полной для соответствующего класса схем, то производимый нами процесс прервется и мы в результате построим минимальную схему.

Теорема доказана.

Предложенный в только что доказанной теореме алгоритм построения минимальных схем является алгоритмом полного перебора и поэтому является непрактичным.

Рассмотрим более простую задачу. когда исходная система уравнений содержит одно уравнение

$$z = f(x_1, x_2, \ldots, x_n),$$

т. е. искомая схема Σ имеет один выход. Сложность минимальной, которая соответствует приведенному уравнению, естественно обозначить через $L(f)$.

Определение 7.7. Пусть $L_A(f)$ — минимальная сложность схем, которые получаются при помощи алгоритма A. Пусть

$$L(n) = max_{f \in P^{(n)}} L(f); \quad L_A(n) = max_{f \in P^{(n)}} L_A(f).$$

Функции $L(n)$ и $L_A(n)$ называются *функциями Шеннона.*

Очевидно, что

$$L_A(n) \geqslant L(n).$$

Теперь задачу синтеза можно поставить следующим образом: найти такой алгоритм A, сложность схем которого была бы как можно ближе к сложности схем, получаемых при помощи алгоритма полного перебора и чтобы трудоемкость алгоритма A была существенно меньше, чем трудоемкость алгоритма полного перебора. Такая постановка задачи не требует нахождения минимальной схемы, что в некоторых случаях как раз и требует максимальных усилий.

7.5. Элементарные методы синтеза схем из функциональных элементов

Пусть дана некоторая булева функция $f(x_1, x_2, \ldots, x_n)$, которая не является константой. Поставим задачу построения некоторой схемы из функциональных элементов, которая реализует эту функцию.

Алгоритм А.1. Рассмотрим разложение функции $f(x_1, x_2, \ldots, x_n)$ в виде совершенной дизъюнктивной нормальной формы:

$$f(x_1, x_2, \ldots, x_n) = \bigvee_{\substack{(\sigma_1, \sigma_2, \ldots, \sigma_n) \\ f(\sigma_1, \sigma_2, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} x_2^{\sigma_2} \ldots x_n^{\sigma_n} = \bigvee_{i=1}^{s} K_i. \qquad (*)$$

Для того, чтобы изобразить схему Σ_K, которая реализует конъюнкцию $K = x_1^{\sigma_1} x_2^{\sigma_2}, \ldots, x_n^{\sigma_n}$, введем вспомогательный элемент (рис. 20). Тогда указанная схема может быть легко изображена (рис. 21).

Поскольку блоков, содержащих символ конъюнкции, на один меньше чем блоков, изображающих введенный нами вспомогательный элемент, то получаем оценку

$$L(\Sigma_K) \leqslant n + (n - 1).$$

Кроме того, схема Σ_K содержит подсхему Σ'_K, которая имеет сложность $n - 1$.

Составим для каждой из конъюнкций K_i разложения (*) схему Σ_{K_i} ($i = 1, \ldots, s$). Теперь "склеим"полученные схемы следующим образом. Сначала наложим друг на друга все переменные x_1 из каждой схемы

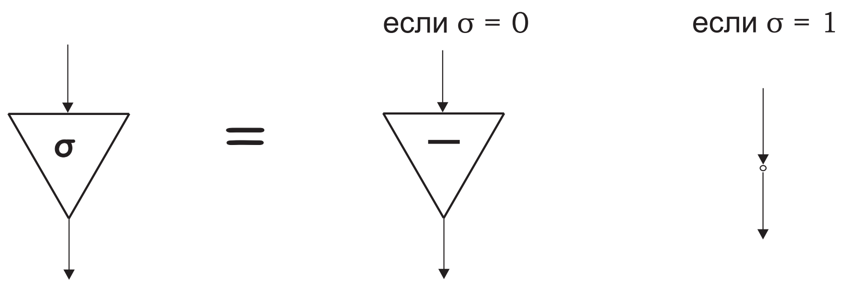


Рис. 20

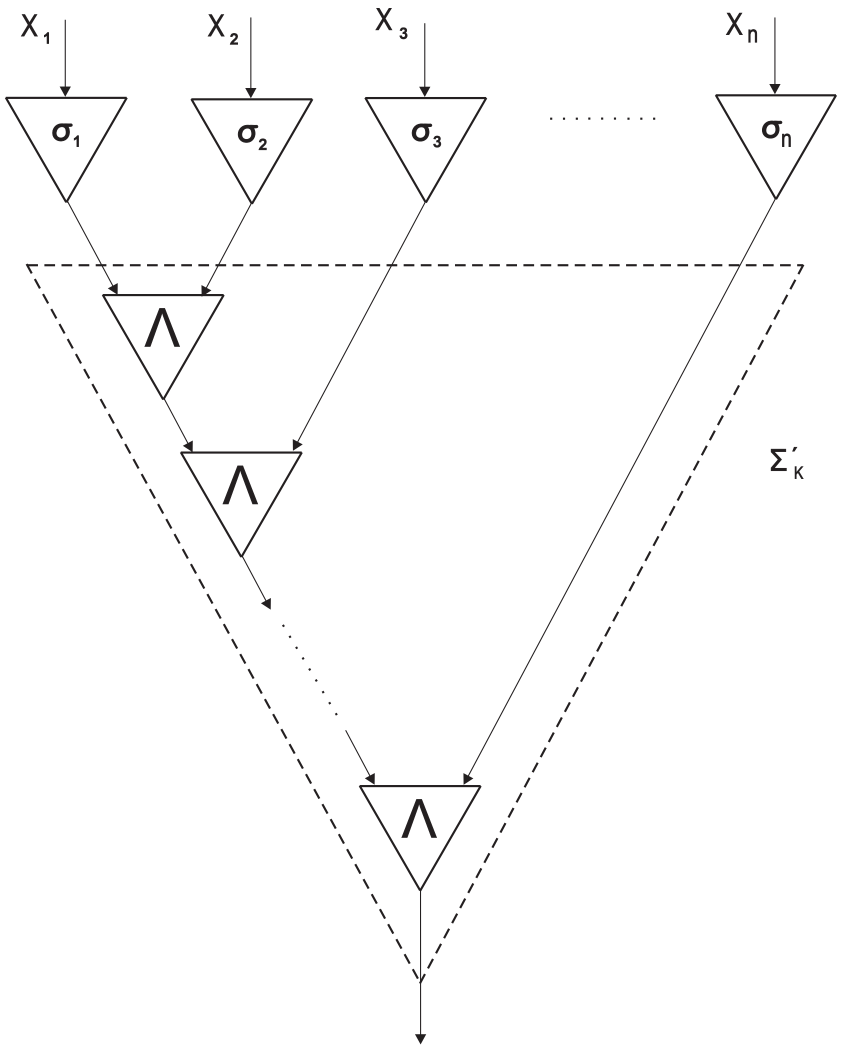


Рис. 21

Σ_{K_i}, затем наложим друг на друга все переменные x_2 из каждой схемы и так далее, пока все переменные вплоть до x_n не окажутся склеенными. Теперь таким же образом наложим друг на друга одинаковые вспомогательные элементы для каждой из схем. Мы получим, что на выходе каждого из вспомогательных элементов окажется разветвление выходов, причем каждое такое разветвление будет содержать ровно s выходов — по числу схем Σ_{K_i}. В результате такого "склеивания", мы получим схему Σ (рис. 22).

Поскольку внутри каждой из схем Σ_{K_i} содержится, как установлено выше, не более $(n-1)$ элементов, то получаем оценку

$$L(\Sigma) \leqslant n + s(n-1).$$

Если теперь подключить схему Σ к схеме из дизъюнкторов, то мы получим схему для функции $f(x_1, x_2, \ldots, x_n)$ (рис. 23).

Итак, мы окончательно получили описание метода синтеза по совершенной дизъюнктивной нормальной форме. Составим окончательно оценку сложности этого алгоритма:

$$L_{A_1}(f) \leqslant n + s(n-1) + s - 1 < n + ns = n(s+1).$$

Поскольку функция f не является тавтологией, то хотя бы на одном наборе переменных ее значение равно 0. Это означает, что в совершенной дизъюнктивной нормальной форме этой функции будет отсутствовать хотя бы одна элементарная конъюнкция. Поэтому совершенная дизъюнктивная нормальная форма будет содержать в любом случае не более $2^n - 1$ элементарных конъюнкций. Следовательно, $s \leqslant 2^n - 1$ и поэтому

$$L_{A_1}(f) \leqslant n(s+1) \leqslant n(2^n - 1 + 1) = n2^n.$$

Кроме того, можно так же получить оценку для функции Шеннона:

$$LA_1(n) \leqslant n2^n.$$

Рассмотренный нами алгоритм называется *Методом синтеза, основанным на совершенной дизъюнктивной нормальной форме.*

Алгоритм А.2. Рассмотрим теперь другой метод синтеза схемы из функциональных элементов. Построим вначале все возможные элементарные конъюнкции, которые получаются из переменных $x_1, x_2, \ldots$ $\ldots, x_n$. Для этого построим схему Σ, которая и будет реализовывать все возможные конъюнкции. Для построения этой схемы воспользуемся индуктивным методом, т.е. построим вначале схему для реализации всех возможных конъюнкций для 1 переменной, затем схему для реализации всех возможных конъюнкций для 2 переменных и наконец покажем, как в указанную схему, построенную для $n-1$ переменных, ввести новые элементы, чтобы получить схему для n элементов (рис. 24).

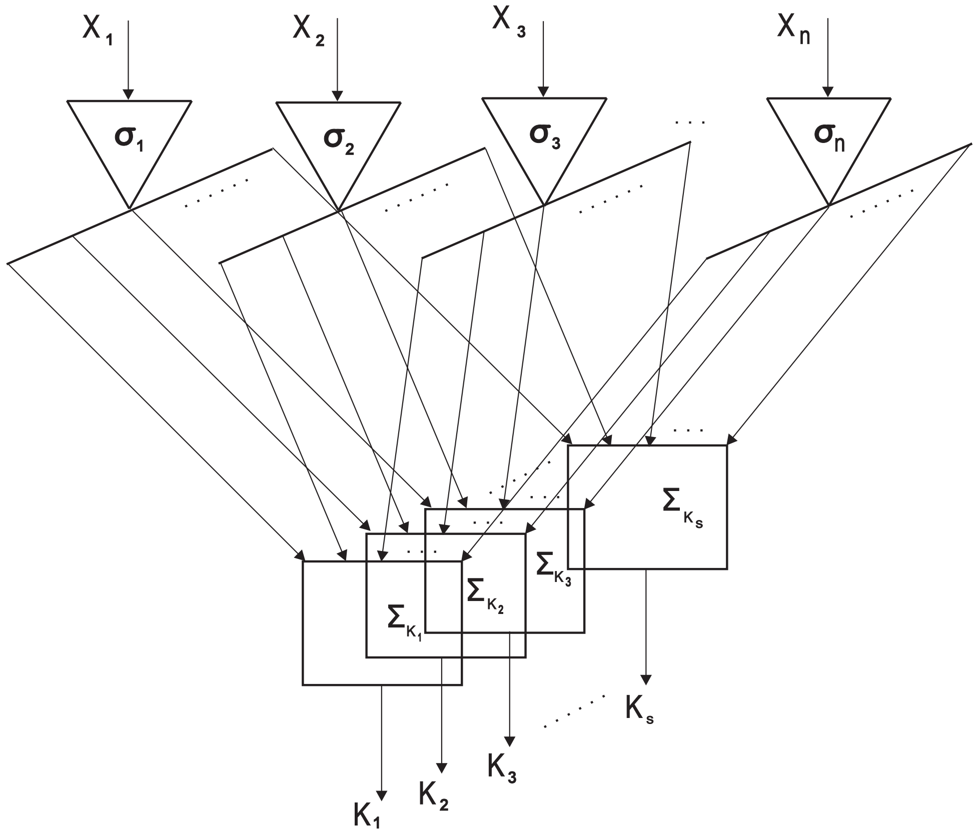


Рис. 22

Составим оценку для этого алгоритма.

$$L(\Sigma_1) = 1,$$

$$L(\Sigma_2) = 1 + 1 + 4 = L(\Sigma_1) + 1 + 2^2,$$

$$L(\Sigma_n) = L(\Sigma_{n-1}) + 1 + 2^n,$$

$$L(\Sigma_n) = L(\Sigma_{n-2} + 1 + 2^{n-1} + 1 + 2^n,$$

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

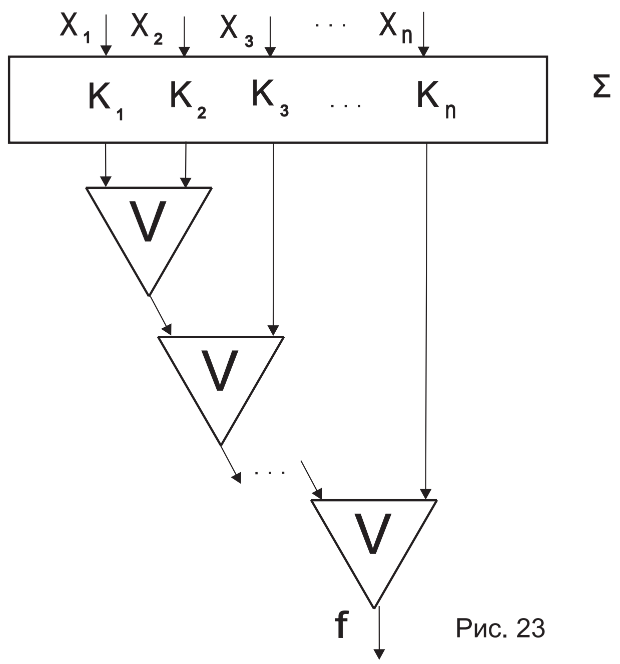


Рис. 23

Для того, чтобы построить схему, реализующую функцию $f(x_1, x_2, \ldots$ $\ldots, x_n)$, нужно в построенном многополюснике Σ_n выбрать только те выходы, которые соответствуют членам совершенной дизъюнктивной нормальной формы функции, т.е. конъюнкциям $K_1, K_2, \ldots, K_s$, подключить эти выходы к схеме, состоящей из дизъюнкторов (рис. 22), которая осуществляет логическое сложение и удалить лишние элементы. Для этого потребуется еще не более

$$s \leqslant 2^n - 1$$

дизъюнкторов. Поэтому получаем для алгоритма A.2. следующие оценки:

$$L_{A_2}(f) \leqslant 3 \cdot 2^n + n - 5$$

и

$$L_{A_2}(n) \leqslant 3 \cdot 2^n + n - 5.$$

Алгоритм A.3. Разложим рассматриваемую нами функцию следующим образом:

$$f(x_1, x_2, \ldots, x_{n-1}, x_n) =$$

$$(x_n \wedge f(x_1, x_2, \ldots, x_{n-1}, 1)) \vee (\overline{x}_n \wedge f(x_1, x_2, \ldots, x_{n-1}, 0)).$$

Можно продолжить это разложение:

$$f(x_1, x_2, \ldots, x_{n-2}, x_{n-1}, x_n) =$$

$$(x_n \wedge x_{n-1} \wedge f(x_1, x_2, \ldots, x_{n-2}, 1, 1)) \vee (x_n \wedge \overline{x}_{n-1} \wedge f(x_1, x_2, \ldots, x_{n-2}, 0, 1)) \vee$$

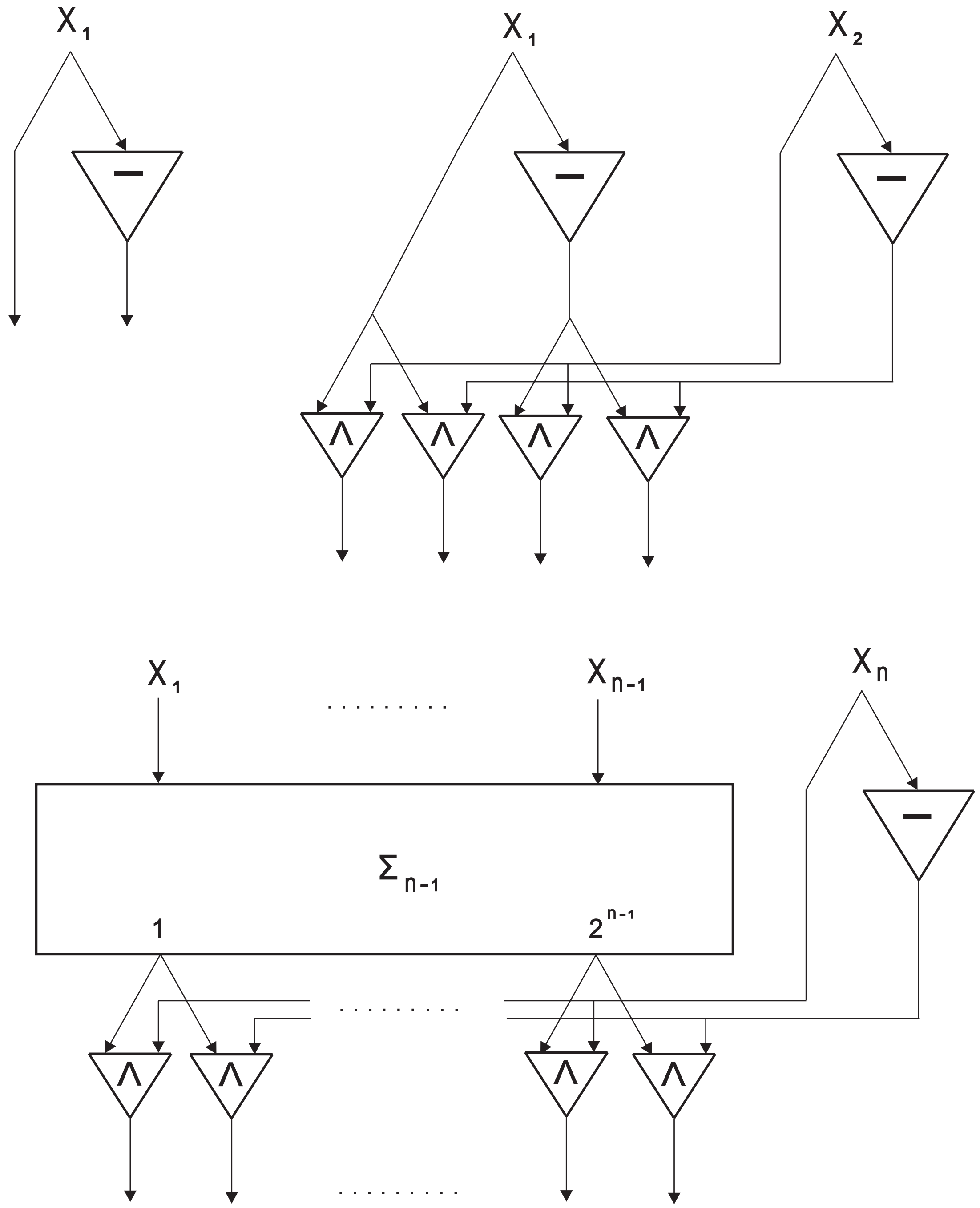


Рис. 24

$$(\overline{x}_n \wedge x_{n-1} \wedge f(x_1, x_2, \ldots, x_{n-2}, 1, 0)) \vee (\overline{x}_n \wedge \overline{x}_{n-1} \wedge f(x_1, x_2, \ldots, x_{n-2}, 0, 0)).$$

Таким образом, через n шагов мы получим разложение нашей функции по всем переменным. Теперь поставим цель построить схему, двигаясь в обратном направлении.

Обозначим

$$f' = f(x_1, x_2, \ldots, x_{n-1}, 1)$$

и

$$f'' = f(x_1, x_2, \ldots, x_{n-1}, 0).$$

Тогда полученное выше разложение можно представить более компактно:

$$f(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_n \wedge f') \vee (\overline{x}_n \wedge f''). \qquad (*)$$

Пусть рассматриваемая функция является функцией от одной переменной. Тогда возможно два случая: $f(x) = x$, т.е. функция является тождественной функцией (рис. 25) и $f(x) = \overline{x}$, т.е. функция является отрицанием (рис. 26). Кроме того, получаем, что $f' = f(1)$ и $f'' = f(0)$ Для того, чтобы в схему ввести константы 1 и 0, воспользуемся схемами, представленными на рис. 27. Таким образом, если рассматриваемая функция является функцией от одной переменной, то

$$f(x_1) = (x_1 \wedge f') \vee (\overline{x}_1 \wedge f'')$$

или

$$f(x_1) = (x_1 \wedge f(1)) \vee (\overline{x}_1 \wedge f(0)).$$

Пусть, например, наша функция является отрицанием. Тогда последнее равенство запишется в виде

$$f(x_1) = (x_1 \wedge 0) \vee (\overline{x}_1 \wedge 1).$$

Для построения схемы, реализующей функцию от n переменных, снова воспользуемся методом индукции. Основанием индукции будем считать схемы, построенные на рис. 25-27. Поскольку функции f' и f" являются функциями от числа переменных на единицу меньшего, чем функция f, то индуктивным переходом можно считать переход от функций f' и f'' к функции f. Таким образом, мы получим схему, представленную на рис. 28

Полученная схема и представляет собой алгоритм A_3. Проведем оценки этого алгоритма:

$$L_{A_3}(1) = 2;$$

$$L_{A_3}(n) \leqslant 2L_{A_3}(n-1) + 4.$$

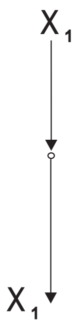


Рис. 25

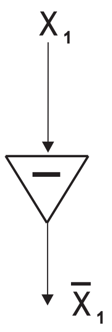


Рис. 26

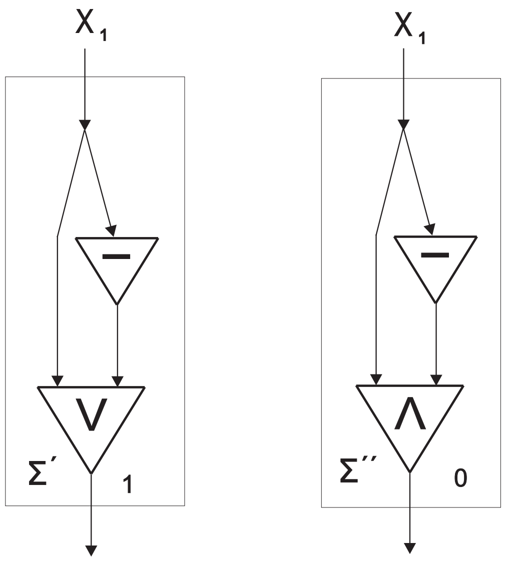


Рис. 27

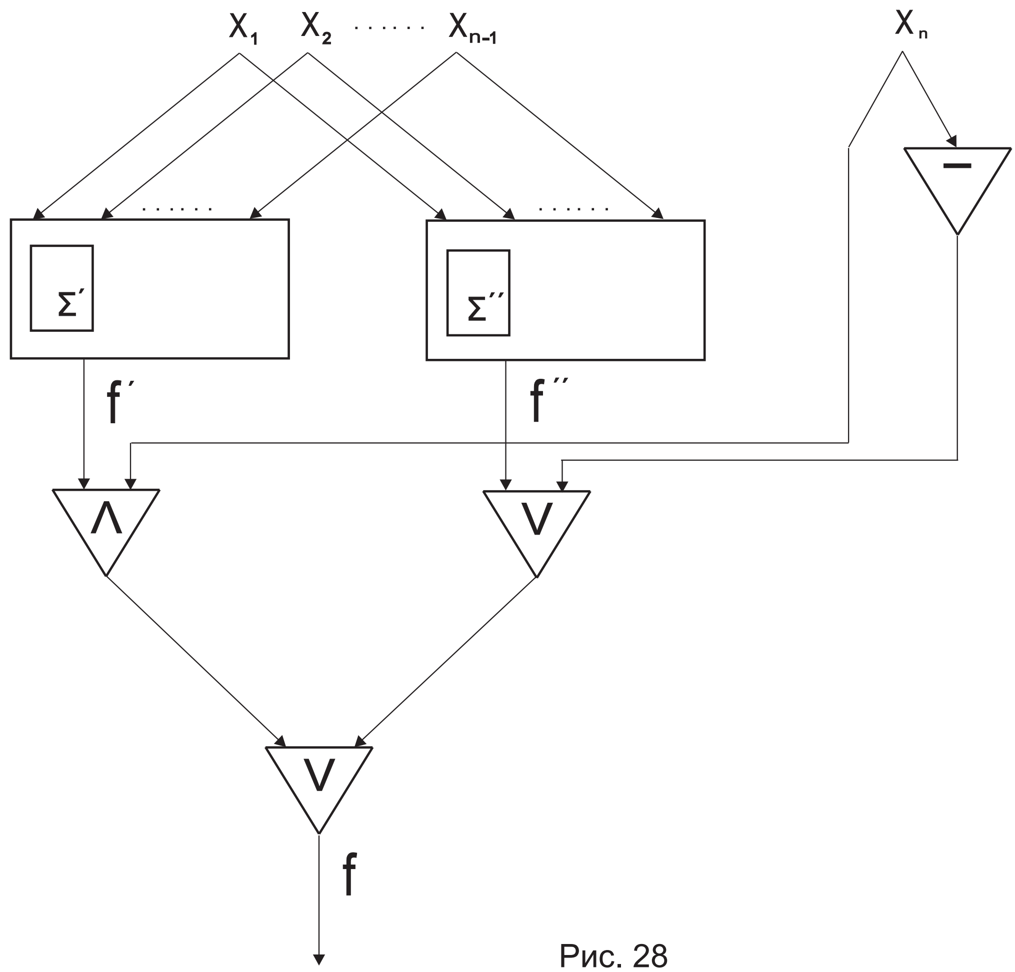


Рис. 28

Если теперь учесть все дополнительные элементы, которые могут быть вставлены (см. описание алгоритмов А.1 и А.2)

$$s \leqslant 2^n - 1,$$

то получаем следующую оценку:

$$L_{A_3}(n) \leqslant 3 \cdot 2^n - 4.$$

Возможно получение еще более лучшей оценки, если имеется информация о реализации функции от двух переменных, например, что

$$L_{A_3}(2) \leqslant 5.$$

Тогда для схемы, реализующей функцию от n переменных, получаем оценку:

$$L_{A_3}(n) \leqslant 2,25 \cdot 2^n - 4.$$

Таким образом, рассмотренные нами алгоритмы A_1, A_2, A_3 дают все более лучшие оценки функций Шеннона и, поэтому, все более компактные схемы для реализации функций.

7.6. Метод Шеннона

Для того, чтобы судить о трудоемкости того или иного алгоритма, нужно знать, насколько оценка $L_A(n)$ отличается от оценки $L(n)$. Сравнение указанных величин обычным способом оказывается трудной задачей, поскольку их вычисление крайне сложно, а в некоторых случаях и невозможно. Поэтому для такого сравнения применяется так называемый асимптотический метод. С помощью этого метода было установлено, что существует метод синтеза, который приводит к функции Шеннона, по порядку совпадающей с нижней оценкой. Этот метод был создан К.Шенноном.

Определение 7.8. Функциональный элемент, соответствующий конъюнкции называется *конъюнктором.*

Определение 7.9. Функциональный элемент, соответствующий дизъюнкции называется *дизъюнктором.*

Определение 7.10. Функциональный элемент, соответствующий отрицанию называется *инвентором.*

Пусть $f_1(x_1, x_2, , \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_s(x_1, x_2, \ldots, x_n)$ — такое множество булевых функций, что при $i \neq j$ всегда выполняется $f_i \not\equiv f_j$.

Определение 7.11. Многополюсник из функциональных элементов, имеющий n входов и s выходов называется *универсальным* для данного множества функций, если для каждого i $(1 \leqslant i \leqslant s)$ в многополюснике найдется выход $\tau(i)$ такой, что на нем реализуется функция $f_i(x_1, x_2, \ldots, x_n)$.

Примером универсального многополюсника для множества $K_1, K_2, \ldots$ $\ldots, K_s$ является схема, построенная на рис. 22.

Теорема 7.4. *Для любого n можно построить универсальный многополюсник U_n для множества всех булевых функций от n переменных $x_1, x_2, \ldots, x_n$ и при этом*

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

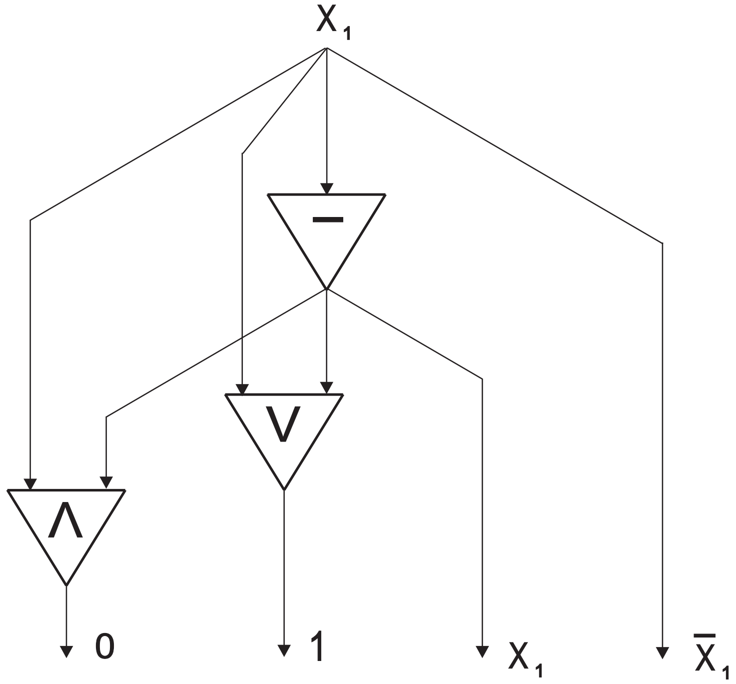


Рис.29

Доказательство. Построим многополюсник U_n индуктивным способом. Основанием индукции может служить многополюсник, изображенный на рис. 29, который реализует функцию от 1 переменной. Для этого многополюсника получаем следующую оценку:

$$L(U_1) = 3 < 2 \cdot 2^{2^1}.$$

Совершим теперь индуктивный переход. Предположим, что универсальный многополюсник U_{n-1} для множества всех булевых функций, зависящих от n переменных $x_1, x_2, \ldots, x_{n-1}$ уже построен и при этом

$$L(U_{n-1}) \leqslant 2 \cdot 2^{2^1}.$$

Рассмотрим разложение

$$f(x_1, x_2, \ldots, x_{n-1}) =$$
$$(x_n \wedge f(x_1, x_2, \ldots, x_{n-1}, 1)) \vee (\overline{x} \wedge f(x_1, x_2, \ldots, x_{n-1}, 0)) =$$
$$(x_n \wedge f') \vee (\overline{x}_n \; f''),$$

где, как и выше,

$$f' = f(x_1, x_2, \ldots, x_{n-1}, 1)$$

и

$$f'' = f(x_1, x_2, \ldots, x_{n-1}, 0).$$

Множество всех функций, зависящих от переменных $x_1, x_2, \ldots, x_n$ разобьем на три непересекающихся класса.

1. $f' \equiv f'' \equiv 0$. Этот класс содержит только одну функцию $f \equiv 0$.

2. Ровно одна из функций f' или f'' тождественно равна 0. В этом классе содержатся функции f вида

$$f = x_n \wedge f',$$

где

$$f' \not\equiv 0$$

или

$$f = \overline{x}_n \wedge f'',$$

где

$$f'' \not\equiv 0.$$

Число таких функций будет равно $2 \cdot (2^{2^{n-1}} - 1)$. Действительно, число всех булевых функций от $n-1$ переменных равно $2^{2^{n-1}}$. Из этого числа нужно вычесть 1, поскольку только одна функция тождественно равна нулю и умножить полученное число на 2, поскольку функция f' составляет конъюнкцию с переменной x_n, а функция f'' — с ее отрицанием и поэтому множества этих конъюнкций не могут содержать одинаковых элементов.

3. Все остальные функции, т.е. функции у которых

$$f' \not\equiv 0$$

и

$$f'' \not\equiv 0.$$

Количество различных таких функций вычислить нетрудно. поскольку это те функции, которые не принадлежат первым двум классам:

$$2^{2^n} - 2 \cdot (2^{2^{n-1}} - 1) - 1.$$

Рассмотрим теперь схему, изображенную на рис. 30. На ней изображен многополюсник U_n. Здесь выходы многополюсника U_{n-1} занумерованы числами $1, 2, \ldots, 2^{2^{n-1}}$, причем считается, что на выходе 1 реализуется константа 0. Выходы многополюсника разбиты на три класса в соответствии с разбиением множества всех булевых функций, зависящих от переменных $x_1, x_2, \ldots, x_n$. Данный многополюсник содержит:

1) подсхему U_{n-1};

2) кроме указанной подсхемы:

а) один инвентор;

б) $2(2^{2^{n-1}} - 1)$ конъюнкторов;

в) $2^{2^n} - 2(2^{2^{n-1}} - 1) - 1$ дизъюнкторов.

Поэтому мы получаем окончательно следующую оценку

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

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

Теорема доказана.

7.7. Синтез сумматора

Общая теория синтеза схем из функциональных элементов приводит к важному выводу о том, что большинство булевых функций (при $n \to \to \infty$) имеет сложные минимальные схемы. Это означает, что практическую ценность с точки зрения синтеза представляет весьма узкий класс булевых функций. Поэтому наряду с универсальными методами синтеза (методами, которые позволяют строить схемы, реализующие любую функцию). необходимо иметь методы синтеза, приспособленные к отдельным классам булевых функций, полнее учитывающие свойства отдельных функций.

Одной из схем из функциональных элементов, применяемых для построения отдельного класса булевых функций, является многополюсник, реализующий сложение двух чисел, заданных в двоичной системе счисления.

Пусть даны два числа, заданных в двоичной системе счисления:

$$x = x_n x_{n-1} \ldots x_1$$

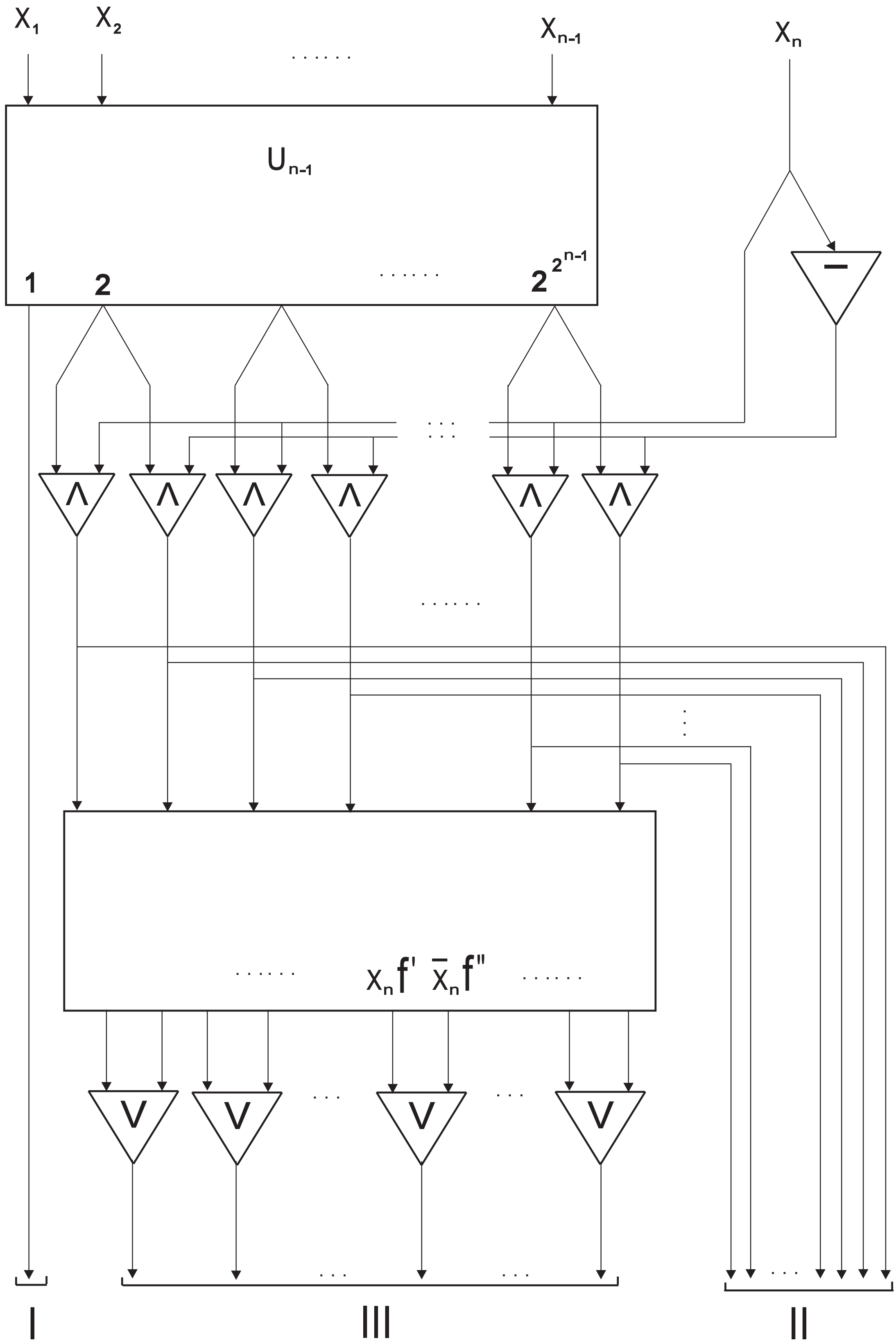


Рис.30

$$y = y_n y_{n-1} \dots y_1.$$

Рассмотрим хорошо известный алгоритм сложения чисел x и y "столбиком":

$$\begin{array}{cccc} q_{n+1} & q_n & \dots & q_1 \\ + & x_n & \dots & x_1 \\ & y_n & \dots & y_1 \\ \hline z_{n+1} & z_n & \dots & z_1 \end{array}$$

Здесь числа$q_{n+1}, q_n \dots, q_1$ обозначают результаты предыдущих переносов из предыдущих разрядов ($q_1 = 0$). Очевидно, что

$$z_i = x_i + y_i + q_i (mod 2),$$

$$q_{i+1} = (x_i \wedge y_i) \vee (x_i \wedge q_i) \vee (y_i \wedge q_i).$$

Если воспользоваться тождеством

$$x_i + y_i + q_i =$$

$$\overline{(x_i \wedge y_i) \vee (x_i \wedge q_i) \vee (y_i \wedge q_i)}$$

$$\wedge (x_i \vee y_i \vee q_i) \vee (x_i \wedge y_i \wedge q_i),$$

то легко получить схему, реализующую соответствующее преобразование величин $x_i,\ y_i,\ q_i$ в величины $z_i,\ q_{n+1}$ (см. рис. 31).

Обозначим только что построенную схему через B_i $(1 < i \leqslant n)$. Тогда искомая нами схема Σ_n, которая представляет собой сумматор для двух n-разрядных двоичных чисел, получается путем последовательного соединения блоков B_i (см. рис. 32). В этой схеме $z_{n+1} = q_{n+1}$ и блок B_1 осуществляет преобразование

$$z_1 = x_1 + y_1 = \overline{x_1 \wedge y_1} \wedge (x_1 \vee y_1),$$

$$q_2 = x_1 \wedge y_1.$$

Очевидно, что

$$L(B_1) = 4$$

и

$$L(B_i) = 9 \quad (1 < i \leqslant n).$$

Таким образом, получаем следующую оценку:

$$L(\Sigma_n) \leqslant 9 \cdot (n-1) + 4 = 9n - 5 < 9n.$$

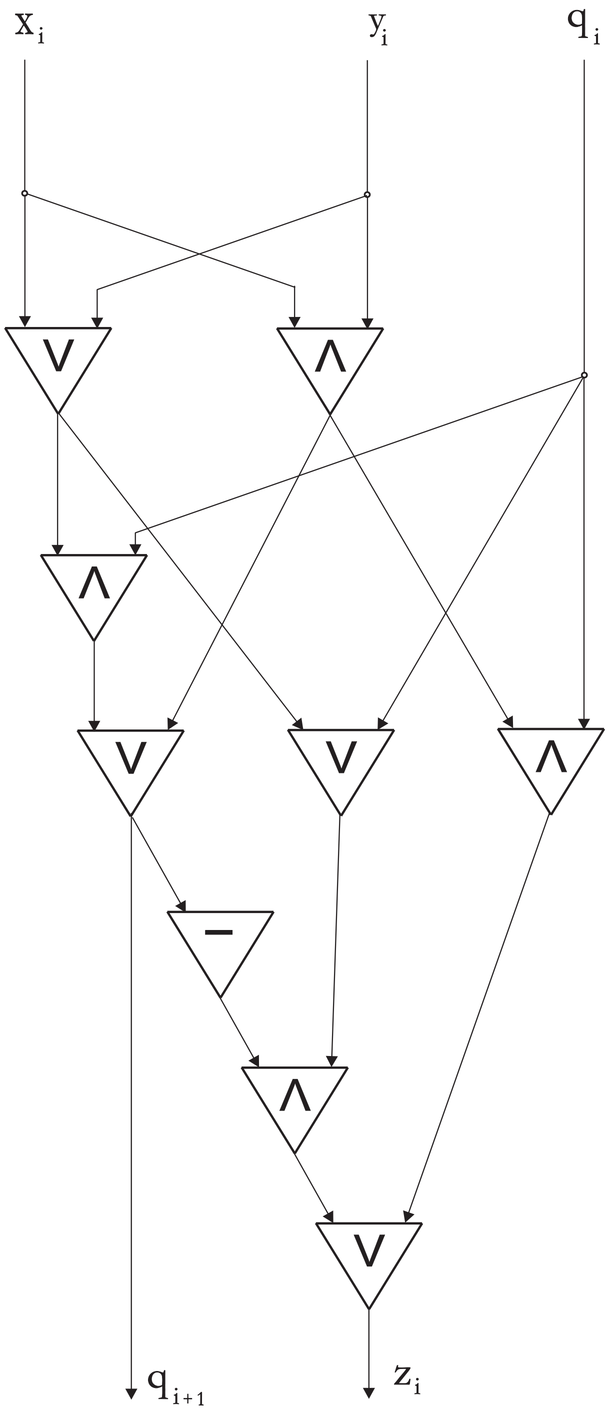


Рис. 31

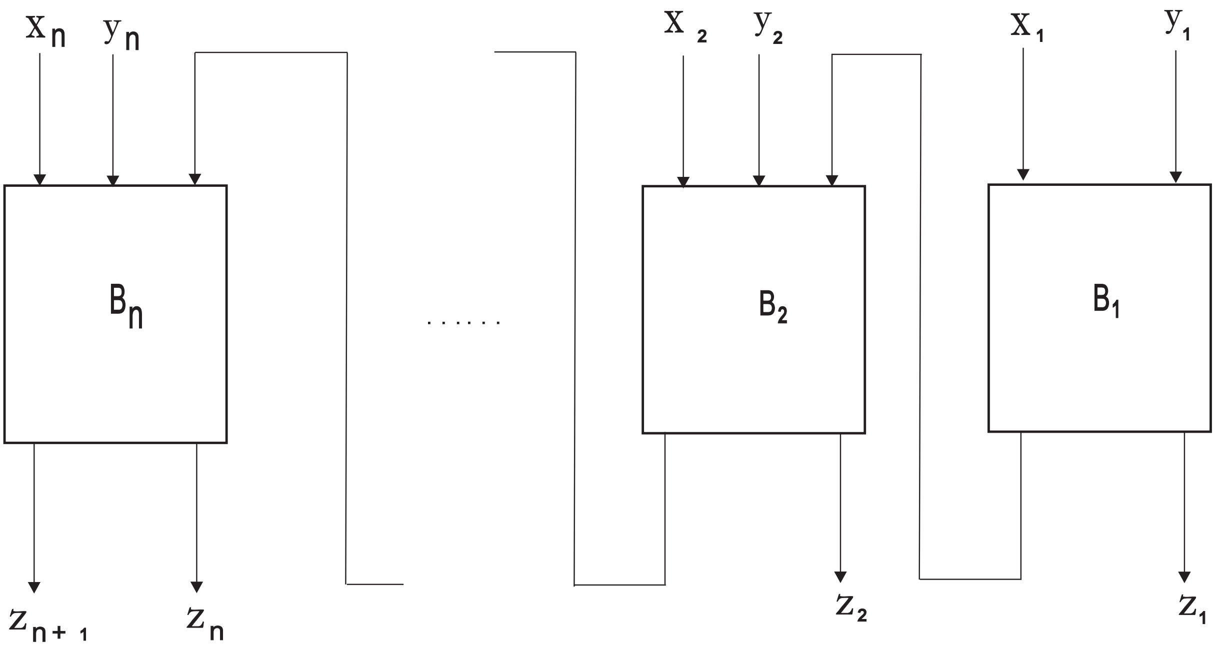


Рис. 32

Литература

1 Карпов.В.Г., Мощенский В.А. Математическая логика и дискретная математика. — Мн.: Выш. шк., 1977.

2 Мощенский В.А. Лекции по математической логике. — Мн.: БГУ, 1973.

3 Мощенский А.В., Мощенский В.А. Математические основы информатики. — Мн.: БГУ, 2002.

4 Дискретная математика и математические вопросы кибернетики. Под общей редакцией С.В. Яблонского и О.Б. Лупанова. — М.: Наука, 1974.

5 Яблонский С.В. Введение в дискретную математику. — М.: Наука, 1979.

6 Гиндикин С.Г. Алгебра логики в задачах. — М.: Наука, 1972.

7 Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. — М.: Наука, 1977.

8 Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов. — М.: Наука, 1984.

Учебное издание

Аниськов Валерий Валерьевич
Близнец Игорь Васильевич

ДИСКРЕТНАЯ МАТЕМАТИКА

КУРС ЛЕКЦИЙ

для студентов 1 курса
специальности 1–31 03 01–02 — "Математика
(научно-педагогическая деятельность)"

В авторской редакции

Подписано в печать 26.10.2006 г. (72) Формат 60×84 1/16. Бумага писчая № 1. Гарнитура "Таймс". Усл. п. л. 6,3 Уч.-изд. л. 4,9 Тираж 25 экз.

Отпечатано с оригинала-макета на ризографе
учреждения образования
"Гомельский государственный университет
имени Франциска Скорины"
246019, г. Гомель, ул. Советская, 104