МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

Н.В. Труб
Д.В. Нуцубидзе

Булевы алгебры

Учебное пособие

Москва
2017

УДК 512
ББК 22.14
Т 77

Рецензенты:

Е.В. Петрунина – канд. тех. наук, доцент кафедры прикладной математики и информатики

Л.Н. Осикова – канд. пед. наук, доцент кафедры романо-германских языков МГГЭУ

Труб Н.В., Нуцубидзе Д.В.
Т 77 Булевы алгебры: учебное пособие. - М.: МГГЭУ, 2017. - 58 с.

В учебном пособии рассмотрены элементы математической логики и основы теории дискретных функций и их минимизация. Даны определения булевой алгебры, замкнутых классов булевых функций, функциональной полноты, формул алгебры высказываний, дизъюнктивных и конъюнктивных нормальных форм. Сформулированы и доказаны основные теоремы, раскрывающие свойства введенных понятий в их взаимосвязи друг с другом. Структура пособия соответствует традиционным тематическим разделам дисциплины «Дискретная математика». Для студентов, обучающихся по специальностям «Прикладная математика и информатика» и «Прикладная информатика».

ISBN 978-5-9799-0095-7

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В 2015 году было опубликовано учебное пособие Н.В. Труб «Множества, функции и отношения», в котором систематически изложены основы теории множеств, элементы алгебры и комбинаторики, предложены и в деталях проиллюстрированы практическими примерами понятия мощности множества, отношений, функций и базовых алгебраических структур. Учебное пособие оказалась достаточно востребованным, получило хорошие отзывы и представлено в библиотеке Московского государственного гуманитарно-экономического университета.

Настоящая работа является продолжением учебного пособия «Множества, функции и отношения». Она будет полезна для студентов факультета прикладной математики и информатики как конспект лекций по традиционным тематическим разделам курса «Дискретная математика». Вместе с тем пособие содержит темы, не вошедшие в этот курс, но представляющие интерес для студентов с учебной и с научно-исследовательской точки зрения. Пособие также может быть рекомендовано в помощь студентам при написании курсовой работы по учебной дисциплине «Дискретная математика».

Изложение ведется в естественной логической последовательности с соблюдением постепенного перехода от простого к сложному.

Пособие включает большое количество примеров, хорошо иллюстрирующих практическое применение изложенного теоретического материала.

Для студентов, обучающихся по специальностям «Прикладная математика и информатика» и «Прикладная информатика».

ГЛАВА 1. ИЗОМОРФИЗМ БУЛЕВЫХ АЛГЕБР

§ 1.1. Определение булевой алгебры

Определение 1. Булевой алгеброй называется множество A с двумя бинарными операциями ($\wedge$, $\vee$), одной унарной операцией ($'$) и двумя фиксированными элементами 0 и I. Причем для любых $x, y, z \in A$ выполняются соотношения:

1. $x \wedge x = x, x \vee x = x$ (идемпотентность);

2. $x \wedge y = y \wedge x, \quad x \vee y = y \vee x$ (коммутативность);

3. $x \wedge (y \wedge z) = (x \wedge y) \wedge z,$
$x \vee (y \vee z) = (x \vee y) \vee z$ (ассоциативность);

4. $x \wedge (x \vee y) = x, \quad x \vee (x \wedge y) = x$ (поглощение);

5. $x \wedge [y \vee (x \wedge z)] = (x \wedge y) \vee (x \wedge z),$
$x \vee [y \wedge (x \vee z)] = (x \vee y) \wedge (x \vee z)$ (модулярность);

6. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ дистрибутивность);

7. $x \wedge 0 = 0, \quad x \vee 0 = x$
$x \wedge I = x, \quad x \vee I = I$(универсальные границы);

8. $x \wedge x' = 0, \quad x \vee x' = I$(дополнение);

9. $(x')' = x$ (инволютивность);

10. $(x \wedge y)' = x' \vee y', \quad (x \vee y)' = x' \wedge y'$(законы де Моргана), где:

$\wedge$ — булево произведение; $\vee$ — булева сумма; 0, I — универсальные границы.

Пример 1. Для натурального n обозначим через $\bar{n}$ множество $\bar{n} = \{1,2, \dots, n\}$. Рассмотрим следующую систему: $\mathcal{B}^n = \langle P(\bar{n}), \cap, \cup, \bar{\ }, \emptyset, \bar{n} \rangle$. Эта система будет булевой алгеброй. Здесь пересечение $\cap$ — булево произведение, объединение $\cup$ — булева сумма, в качестве унарной операции $'$ выступает дополнение — $\bar{\ }$, а отмеченные элементы 0 и I есть $\emptyset$ и $\bar{n}$ соответственно. Все свойства 1—10 доказаны в теории множеств.

Данная булева алгебра называется булевой алгеброй подмножеств. Понятно, что в качестве основного множества можно брать не обязательно $\bar{n}$, а любое множество *из* n элементов. Множество M может быть и бесконечным, тогда получим бесконечную алгебру подмножеств.

Пример 2. Пусть $A = \{0,1\}$. Рассмотрим множество A^n, т.е. множество последовательностей $(a_1, a_2, \dots, a_n)$, где каждое a_i принимает значение 0 или 1.

Введем на этих последовательностях булевы операции:

для $a = (a_1, \dots, a_n)$ и $b = (b_1, \dots, b_n)$ положим

$a \vee b = \big(max(a_1, b_1), \dots, max(a_n, b_n)\big);$

$a \wedge b = \big(min(a_1, b_1), \dots, min(a_n, b_n)\big)$;

$a' = (1 - a_1, \dots, 1 - a_n)$; $0 = (0, \dots, 0)$; $\mathrm{I} = (1, \dots, 1)$.

Получим булеву алгебру $\mathcal{A}^n = \langle A^n, \wedge, \vee, ', 0, \mathrm{I}\rangle$. Все аксиомы легко проверяемы.

Между булевой алгеброй подмножеств и алгеброй булевых последовательностей существует тесная связь. Эта связь позволяет все операции на множествах легко реализовать на ЭВМ.

Пример 3. Любая функция $f: \{0,1\}^n \to \{0,1\}$ называется булевой функцией от n переменных. Другими словами, булева функция f отображает множество всех наборов из n нулей и единиц во множество $\{0,1\}$.

Пусть F^n — множество всех булевых функций от n переменных.

Для этого надо показать, что для любого набора из 0 и 1 $(x_1, \dots, x_n)$ имеет место равенство $(f \vee g)'(x_1, \dots, x_n) = (f' \wedge g')(x_1, \dots, x_n)$. Возможны четыре случая:

1. $f(x_1, \dots, x_n) = 0$, $g(x_1, \dots, x_n) = 0$, тогда $(f \vee g)(x_1, \dots, x_n) = 0$,
$(f \vee g)'(x_1, \dots, x_n) = 1 - 0 = 1$.

С другой стороны, $f'(x_1, \dots, x_n) = 1 - 0 = 1$, $g'(x_1, \dots, x_n) = 1 - 0 = 1$ и
$(f' \wedge g')(x_1, \dots, x_n) = min\{1,1\} = 1$,
т.е. $(f \vee g)'(x_1, \dots, x_n) = (f' \wedge g')(x_1, \dots, x_n)$.

2. $f(x_1, \dots, x_n) = 1$, $g(x_1, \dots, x_n) = 0$.

Тогда $(f \vee g)(x_1, \dots, x_n) = max\{1,0\} = 1$, а значит, $(f \vee g)'(x_1, \dots, x_n) =$
$= 1 - 1 = 0$.

С другой стороны, $f'(x_1, \dots, x_n) = 1 - 1 = 0$, $g'(x_1, \dots, x_n) = 1 - 0 = 1$ и $(f' \wedge g')(x_1, \dots, x_n) = min\{0,1\} = 0$, т.е. опять $(f \vee g)'(x_1, \dots, x_n) =$
$= (f' \wedge g')(x_1, \dots, x_n)$.

Аналогично проверяются случаи:

3. $f(x_1, \dots, x_n) = 0$, $g(x_1, \dots, x_n) = 1$.

4. $f(x_1, \dots, x_n) = 1$, $g(x_1, \dots, x_n) = 0$.

Булева алгебра $\mathcal{F}^n = \langle F^n, \wedge, \vee, ', \emptyset, I\rangle$ называется булевой алгеброй булевых функций от n переменных.

Нетрудно проверить, что булева алгебра булевых функций от n переменных состоит из 2^{2^n} функций. Рассмотрим, к примеру, алгебру функций от двух переменных в следующей таблице:

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

По таблице, к примеру, легко проверить, что $f_3 \vee f_5 = f_7$, $f_3 \wedge f_5 = f_1$, $f_6{}' = f_9$ и т.д.

Определение 2. Пусть U – произвольное множество из n элементов и S – некоторое его подмножество. Характеристической функцией подмножества S множества U называется функция, определяемая следующим образом:

$$\chi_s(x) = \begin{cases} 1, \text{если } x \in S, \\ 0, \text{если } x \notin S. \end{cases}$$

Таким образом, имеем отображение $f : S \to \chi_s(x)$ из множества P(U) во множество булевых последовательностей. Легко проверить, что f – это биекция.

Заметим, что характеристические функции можно ввести и для бесконечного множества U, и также можно построить биекцию из P(U) во множество булевых последовательностей, но уже бесконечных (число элементов в этих последовательностях равно $|U|$). Но нас будут интересовать лишь конечные множества.

Для любых подмножеств $A, B \subset U$ легко проверить следующие соотношения: $\chi_{A \cup B} = \chi_A \vee \chi_B$, $\chi_{A \cap B} = \chi_A \wedge \chi_B$, $\chi_{\bar{A}} = \chi_A{}'$. Кроме того, отметим, что $\chi_A = (a_1, \dots, a_n)$, $\chi_B = (b_1, \dots, b_n)$, то $\chi_{A \setminus B} = (a_1 \setminus b_1, \dots, a_n \setminus b_n)$, где $a_i \setminus b_i = 1$ тогда и только тогда, когда $a_i = 1$ и $b_i = 0$.

Указанные соотношения позволяют проводить, как уже отмечалось, вычисления на множествах.

Пусть $N = \{1,2,3,4,5,6,7,8,9\}$, $A = \{1,3,5,6,8,9\}$, $B = \{2,4,5,7,8\}$, $C = \{1,2,5,7,8,9\}$.

Из каких элементов состоит множество $X = [(A \cup B) \setminus C] \cap [(A \cup C) \setminus B]$? Рассмотрим это в следующей таблице:

χ_A	1	0	1	0	1	1	0	1	1
χ_B	0	1	0	1	1	0	1	1	0
χ_C	1	1	0	0	1	0	1	1	1
$\chi_{A \cup B}$	1	1	1	1	1	1	1	1	1
$\chi_{(A \cup B) \setminus C}$	0	0	1	1	0	1	0	0	0
$\chi_{A \cup C}$	1	1	1	0	1	1	1	1	1
$\chi_{(A \cup C)/B}$	1	0	1	0	0	1	0	0	1
χ_X	0	0	1	0	0	1	0	0	0

Итак, $X = \{3,6\}$.

Пример 4.

Доказать равенство множеств $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$

Сущность доказательства равенств множеств с помощью характеристических функций заключается в том, чтобы показать, что $\chi_{A \cap (B \setminus C)}(x) = \chi_{(A \cap B) \setminus (A \cap C)}(x)$ для любого x. В предлагаемых равенствах фигурируют три множества: A, B, C. Поэтому нас интересуют три функции: χ_A, χ_B, χ_C, а точнее, их значения: $\chi_A(x)$, $\chi_B(x)$, $\chi_C(x)$. Эти три значения могут быть: (0,0,0); (0,0,1); (0,1,1); и т.д. (всего восемь троек значений).

Проводим вычисления в следующей таблице, обозначив для удобства правую часть равенства через X, а левую часть – через Y:

$\chi_A(x)$	$\chi_B(x)$	$\chi_C(x)$	$\chi_{B\setminus C}(x)$	$\chi_X(x)$	$\chi_{A\cap B}(x)$	$\chi_{A\cap C}(x)$	$\chi_Y(x)$
0	0	0	0	**0**	0	0	**0**
0	0	1	0	**0**	0	0	**0**
0	1	0	1	**0**	0	0	**0**
0	1	1	0	**0**	0	0	**0**
1	0	0	0	**0**	0	0	**0**
1	0	1	0	**0**	0	0	**0**
1	1	0	1	**1**	1	0	**1**
1	1	1	0	**0**	1	1	**0**

Отсюда видно, что $\chi_X(x) = \chi_Y(x)$ для любого x. Следовательно, $X = Y$.

Пример 5. Как связаны между собой множества $X = (A \cup B)\setminus C$ и $Y = (A\setminus C) \cap (B\setminus C)$? Так же, как и в предыдущем примере, вычисляем $\chi_X(x)$ и $\chi_Y(x)$в следующей таблице:

$\chi_A(x)$	$\chi_B(x)$	$\chi_C(x)$	$\chi_{A\cup B}(x)$	$\chi_X(x)$	$\chi_{A\setminus C}(x)$	$\chi_{B\setminus C}(x)$	$\chi_Y(x)$
0	0	0	0	**0**	0	0	**0**
0	0	1	0	**0**	0	0	**0**
0	1	0	1	**1**	0	1	**0**
0	1	1	1	**0**	0	0	**0**
1	0	0	1	**1**	1	0	**0**
1	0	1	1	**0**	0	0	**0**
1	1	0	1	**1**	1	1	**1**
1	1	1	1	**0**	0	0	**0**

Сравнивая между собой $\chi_X(x)$ и $\chi_Y(x)$ видим, что там, где $\chi_Y(x) = 0$, $\chi_X(x)$ равно либо 0, либо 1, но там, где $\chi_Y(x) = 1$, $\chi_X(x)$ тоже равно 1. Это говорит о том, что $Y \subset X$, т.е. $(A\setminus C) \cap (B\setminus C) \subset (A \cup B)\setminus C$. Причем это включение строгое, т.к. например, на третьем наборе $\chi_X(x) = 1$, а $\chi_Y(x) = 0$.

Определение 3. Пусть $\mathcal{B}_1 = \langle B_1, \vee_1, \wedge_1, {'^1}, 0_1, I_1 \rangle$ и $\mathcal{B}_2 = \langle B_2, \vee_2, \wedge_2, {'^2}, 0_2, I_2 \rangle$ — две булевы алгебры. Алгебры $\mathcal{B}_1$ и $\mathcal{B}_2$ называются изоморфными, если существует такая биекция $\varphi: B_1 \to B_2$, что $\varphi(0_1) = 0_2$, $\varphi(I_1) = I_2$, $\varphi(a \vee_1 b) = \varphi(a) \vee_2 \varphi(b)$, $\varphi(a \wedge_1 b) = \varphi(a) \wedge_2 \varphi(b)$, $\varphi\left(a'^1\right) = [\varphi(a)]'^2$.

Приведем без доказательства 3 теоремы, которые понадобятся нам в дальнейшем.

Теорема 1. Булевы алгебры $P(\bar{n}\ )$ и A^n изоморфны.

Теорема 2. Булева алгебра подмножеств $P(\bar{n})$ изоморфна алгебре булевых функций F^n.

Теорема 3. Любая конечная булева алгебра изоморфна алгебре $P(\bar{n})$ для подходящего $n \in N$.

Итак, любая конечная булева алгебра есть фактически алгебра подмножеств. В алгебре подмножеств естественным образом задается отношение частичного порядка: $A\rho B$ тогда и только тогда, когда $A \subseteq B$. Введем по аналогии частичный порядок в любой булевой алгебре.

Лемма 1. В любой булевой алгебре из $a \wedge x = 0$ и $a \vee x = I$ следует, что $x = a'$.

Доказательство.

$$x = x \wedge I = x \wedge (a \vee a') = (x \wedge a) \vee (x \wedge a') = 0 \vee (x \wedge a') =$$
$$= (a \wedge a') \vee (x \wedge a') = (a \vee x) \wedge a' = I \wedge a' = a'.$$

Следствие. В любой булевой алгебре $0' = I$, $I' = 0$.

Лемма 2. В любой булевой алгебре следующие условия эквивалентны: (1) $a \wedge b = a$, (2) $a \vee b = b$, (3) $a' \vee b = I$, (4) $a \wedge b' = 0$.

Доказательство:

$(1) \Rightarrow (2)$ $a \vee b = (a \wedge b) \vee b = b$ по закону поглощения.

$(2) \Rightarrow (3)$ $a' \vee b = a' \vee (a \vee b) = (a' \vee a) \vee b = I \vee b = I$.

$(3) \Rightarrow (4)$ $a \wedge b' = (a' \vee b)' = I' = 0$ по закону де Моргана.

$(4) \Rightarrow (1)$ $a \wedge b = (a \wedge b) \vee 0 = (a \wedge b) \vee (a \wedge b') = a \wedge (b \vee b') =$
$= a \wedge I = a$.

Эквивалентность этих условий леммы 2 задает частичный порядок в произвольной булевой алгебре.

Теорема 4. В любой булевой алгебре отношение $a \leq b$ тогда и только тогда, когда $a \wedge b = a$ задает частичный порядок.

При этом $a \wedge b = inf\{a, b\}$ и $a \vee b = sup\{a, b\}$.

Доказательство. Так как $a \wedge a = a$, то $a \leq a$. Значит, $\leq$ рефлексивно.

Если $a \leq b$ и $b \leq a$, то $a \wedge b = a$ и $b \wedge a = b$. Так как $a \wedge b = b \wedge a$, то $a = b$, т.е. $\leq$ антисимметрично. Наконец, пусть $a \leq b$ и $b \leq c$, тогда $a \wedge b = a$, $b \wedge c = b$, а поэтому $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$, т.е. $\leq$ транзитивно. Значит, $\leq$ — частичный порядок.

Теперь докажем утверждение об *inf* и *sup*. Так как $a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b$, то $a \wedge b \leq a$. Аналогично $(a \wedge b) \wedge b = a \wedge (b \wedge b) = a \wedge b$, т.е. $a \wedge b \leq b$. Значит $a \wedge b$ — нижняя граница для $\{a, b\}$. Пусть c — нижняя граница для $\{a, b\}$, т.е. $c \leq a$, $c \leq b$ или $c \wedge a = c$, $c \wedge b = c$. Надо показать, что $c \leq a \wedge b$. Имеем $(a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge c = c$, т.е. $c \leq a \wedge b$. Аналогично показывается, что $a \vee b = sup\{a, b\}$.

Следствие 1. Во всякой булевой алгебре для любого элемента a справедливо $0 \leq a \leq I$.

Доказательство. Так как $0 \wedge a = 0$, то $0 \leq a$. И так как $a \wedge I = a$, то $a \leq I$.

Следствие 2. Оправдывает названия универсальных границ для 0 и I.

Рассмотрим, к примеру, что означает частичный порядок для A^n и для F^n.

Пусть $x = (x_1, \dots, x_n)$ и $y = (y_1, \dots, y_n)$ — два элемента из A^n и пусть $x \leq y$, т.е. $x \wedge y = x$. По определению, $x \wedge y = \big(min(x_1, y_1), \dots, min(x_n, y_n)\big)$, поэтому для любого $i = 1,2, \dots, n$ $min(x_i, y_i) = x_i$. Это означает, что $x_i \leq y_i$. Другими словами, $x \leq y$ тогда и только тогда, когда для любого $i = 1,2, \dots, n$ из условия $x_i = 1$ следует, что $y_i = 1$.

Пусть даны две функции: $f(x) = f(x_1, \dots, x_n)$ и $g(x) = g(x_1, \dots, x_n)$ из $\mathcal{F}^n$. Если $f(x) \leq g(x)$, то $f(x) \wedge g(x) = f(x)$, т.е. $min\{f(x), g(x)\} = f(x)$. Значит, для любого $x = (x_1, \dots, x_n)$ $f(x) \leq g(x)$. Другими словами, $f(x) \leq g(x)$ тогда и только тогда, когда из того, что $f(x) = 1$ для некоторого $x = (x_1, \dots, x_n)$, следует $g(x) = 1$.

§ 1.2. Функциональная полнота

Любую формулу из алгебры высказываний можно записать, используя систему $\Sigma_0 = \{\wedge, \vee, \overline{}\}$. Остальные можно получить с помощью их суперпозиций.

Определение 1. Система булевых функций Σ называется функционально полной системой, если любая булева функция может быть представлена в виде формулы над Σ, т.е. любая логическая функция может быть получена суперпозицией из функций этой системы Σ.

Значит, Σ_0 — функционально полная система.

Утверждение. Даны две системы функций Σ^* и Σ. Пусть Σ^* функционально полна и каждая функция из Σ^* представима над Σ, тогда Σ будет функционально полной. Тогда говорят, что Σ сводится к Σ^*.

Примеры функционально полных систем.

1. $\Sigma_1 = \{\wedge, \overline{}\}$, так как $x_1 \vee x_2 = \overline{\overline{x_1} \wedge \overline{x_2}}$, то Σ_1 сводится к Σ_0.

2. $\Sigma_2 = \{\vee, \overline{}\}$, так как $x_1 \wedge x_2 = \overline{\overline{x_1} \vee \overline{x_2}}$, то Σ_2 сводится к Σ_0.

3. $\Sigma_3 = \{\downarrow\}$, состоящая из одной булевой функции $f_8(x_1, x_2) = x_1 \downarrow x_2$, является функционально полной. Так как $\bar{x} = x \downarrow x$ и $x_1 \vee x_2 =$
$= (x_1 \downarrow x_2) \downarrow (x_2 \downarrow x_1)$, то Σ_3 свелась к Σ_2.

4. $\Sigma_4 = \{|\}$, состоящая из одной булевой функции $f_{14}(x_1, x_2) = x_1 | x_2$, является функционально полной. Так как $\bar{x} = x|x$ и $x_1 \wedge x_2 = (x_1|x_2)|(x_2|x_1)$, то Σ_4 сводится к Σ_3.

5. $\Sigma_5 = \{\rightarrow, \overline{}\}$, так как $x_1 \vee x_2 = \overline{x_1} \rightarrow x_2$, то Σ_5 сводится к Σ_2.

Рассмотрим $\Sigma_6 = \{\wedge, \oplus, 1\}$, где $f_6(x_1, x_2) = x_1 \oplus x_2$ является сложением по модулю 2. Так как $\bar{x} = x \oplus 1$, то Σ_6 сводится к Σ_1.

§ 1.3. Алгебра Жегалкина

Определение 1. Множество логических функций от n переменных с двумя бинарными операциями $\wedge, \oplus$ и фиксированными постоянными 0, 1 называется алгеброй Жегалкина. Обозначается $\langle F^n, \wedge, \oplus \quad, 0, 1 \rangle$.

Свойства алгебры Жегалкина:

1. $x \oplus y = y \oplus x$
2. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
3. $x \oplus x = 0$
4. $x \oplus 0 = x$
5. $x(y \oplus z) = xy \oplus xz$
6. $xy = yx$
7. $(xy)z = x(yz)$
8. $xx = x$
9. $x1 = x$
10. $x0 = 0$
11. $\bar{x} = x \oplus 1$.

Проверим с помощью свойств алгебры Жегалкина равносильность $x \vee y = xy \oplus x \oplus y$. Заметим, что если $xy = 0$, то $x \vee y = x \oplus y$.

$$x \vee y = \overline{\bar{x}\bar{y}} = (x \oplus 1)(y \oplus 1) \oplus 1 = xy \oplus x \oplus y \oplus 1 \oplus 1 = xy \oplus x \oplus y$$

Если в формуле алгебры Жегалкина раскрыть все скобки и привести подобные слагаемые, используя свойства 1–11, то получим полином Жегалкина.

Определение 2. Полиномом Жегалкина называется многочлен, являющийся суммой по модулю два $(\oplus)$ константы и различных одночленов, в которые каждая из переменных входит не выше, чем в первой степени.

Многочлен Жегалкина от константы равен самой константе. Многочлен от одной переменной – это либо x, либо $\bar{x} = x \oplus 1$. Многочлен от двух переменных $a_0 + a_1x + a_2y + a_3xy$. Многочлен от трех переменных $a_0 + a_1x + a_2y + a_3z + a_4xy + a_5xz + a_6yz + a_7xyz$ и так далее, где коэффициенты a_i принимают значения 0 или 1, а число слагаемых в формуле равно 2^n, где n — число переменных (так как число подмножеств множества состоящего из n элементов 2^n).

Теорема (Жегалкина). Для любой булевой функции существует равносильный ей полином Жегалкина и притом только один.

Доказательство. Любая булева функция сводится к логическим операциям $\wedge, \vee, \overline{}$. В свою очередь, отрицание можно заменить по свойству 11 $\bar{x} = x \oplus 1$, а дизъюнкцию по свойству 12 $x \vee y = xy \oplus x \oplus y$. Тогда получаем формулу, зависящую от логических операций $\wedge, \oplus$, и с помощью преобразований получаем полином Жегалкина.

Покажем единственность (с точностью до порядка следования слагаемых). Пусть дана формула от n переменных. Тогда всевозможных произведений можно составить 2^n, а сумм из этих произведений получится 2^{2^n} — это число всевозможных полиномов Жегалкина. Каждому полиному можно поставить в соответствие вектор длины 2^n из 0 и 1. Таких векторов 2^{2^n}. Фактически каждому полиному Жегалкина ставим в соответствие двоичный вектор, т.е. разным полиномам соответствуют разные вектора. Получили инъекцию. Так как и полиномов, и двоичных векторов 2^{2^n}, то инъекция будет биекцией, т.е. установили взаимно-однозначное соответствие. Таким образом, любой булевой функции ставится в соответствие единственный двоичный вектор, а ему — единственный полином.

Примеры.

1. $x\bar{y} \vee \bar{x}z = (11) = x\bar{y}\bar{x}z \oplus x\bar{y} \oplus \bar{x}z = x(y \oplus 1) \oplus (x \oplus 1)z = xy \oplus x \oplus xz \oplus z$
$== xy \oplus xz \oplus x \oplus z$;

2. $\overline{xy \vee y\bar{z}} = \overline{xy} \wedge \overline{y\bar{z}} = (\bar{x} \vee \bar{y})(\bar{y} \vee z) = \bar{x}\bar{y} \vee \bar{x}z \vee \bar{y} \vee \bar{y}z = \bar{x}z \vee \bar{y} =$
$= (x \oplus 1)z \oplus (y \oplus 1) \oplus (x \oplus 1)(y \oplus 1)z =$
$= xz \oplus z \oplus y \oplus 1 \oplus (xy \oplus x \oplus y \oplus 1)z =$
$= xz \oplus z \oplus y \oplus 1 \oplus xyz \oplus xz \oplus yz \oplus z = xyz \oplus yz \oplus y \oplus 1$;

3. $\overline{xy \vee y\bar{z}} = (xy \vee y\bar{z}) \oplus 1 = xy\bar{z} \oplus xy \oplus y\bar{z} \oplus 1 = xy(z \oplus 1) \oplus xy \oplus y(z \oplus 1)$
$== xyz \oplus xy \oplus xy \oplus yz \oplus y \oplus 1 = xyz \oplus yz \oplus y \oplus 1$;

4. $xy \vee \bar{x}\bar{y} = xy \oplus (x \oplus 1)(y \oplus 1) = xy \oplus xy \oplus x \oplus y \oplus 1 = x \oplus y \oplus 1$.

Сформулируем алгоритм построения многочлена Жегалкина. Выше говорилось, что любую не тождественно ложную формулу алгебры высказываний можно представить в виде совершенной дизъюнктивной нормальной формы (СДНФ). Так как в СДНФ нет двух одинаковых элементарных конъюнкций и все переменные входят в каждую элементарную конъюнкцию либо сами, либо их отрицания, то в формуле $x \vee y = xy \oplus x \oplus y$ можно заменить дизъюнкцию сложением по модулю два. Здесь любая конъюнкция двух элементарных конъюнкций будет равна нулю, потому что содержит хотя бы одну переменную вместе с ее отрицанием. На этом основан первый алгоритм поиска полинома Жегалкина.

Находим множество двоичных наборов, на которых формула принимает значение 1.

Составляем СДНФ.

1. В СДНФ каждую дизъюнкцию заменим сложением по модулю два.
2. Упрощаем, если можно, полученное выражение, используя тождество $\overline{x_i} \oplus x_i = 1$.
3. В полученной формуле каждое отрицание заменяем $\overline{x_i} = x_i \oplus 1$.
4. Раскрываем скобки в полученной формуле, содержащей только $\wedge, \oplus$ и константу 1.
5. Приводим подобные члены, используя тождество $\mathrm{x_i} \oplus \mathrm{x_i} = 0$.

Используя метод неопределенных коэффициентов, получаем второй алгоритм определения полинома Жегалкина. Составляем систему линейных уравнений относительно 2^n неизвестных коэффициентов, содержащую 2^n уравнений. Ее решением являются коэффициенты $a_0, a_1, \dots, a_{2^n-1}$ полинома Жегалкина. Проиллюстрируем этот алгоритм на примере.

Пример. Выразить $x \vee y$ в виде полинома Жегалкина методом неопределенных коэффициентов.

Составим полином Жегалкина для булевой функции двух переменных $x \vee y = a_0 + a_1 x + a_2 y + a_3 xy$. Придавая различные значения переменным, найдем неизвестные коэффициенты.

При $x = y = 0$ имеем $a_0 = 0$;
при $x = 0, y = 1$ имеем $a_0 + a_2 = 1$, значит, $a_2 = 1$;
при $x = 1, y = 0$ имеем $a_0 + a_1 = 1$, значит, $a_1 = 1$;
при $x = 1, y = 1$ имеем $a_0 + a_1 + a_2 + a_3 = 1$,
следовательно, $0 + 1 + 1 + a_3 = 1$, значит, $a_3 = 1$.

§ 1.4. Замкнутые классы функций

Определение 1. Функция, у которой полином Жегалкина имеет вид $\alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \dots \oplus \alpha_n x_n \oplus \gamma$, где α_i и γ либо 0, либо 1, называется линейной.

Пример. $xy \vee \bar{x}\bar{y} = xy \oplus (x \oplus 1)(y \oplus 1) = xy \oplus xy \oplus x \oplus y \oplus 1 = x \oplus y \oplus 1$ — функция линейная.

Определение 2. Множество M логических функций называется замкнутым классом, если любая суперпозиция функций из M есть снова функция из M.

Возьмем любую систему Σ логических функций и будем строить суперпозиции этих функций, получим новый класс функций. Он называется замыканием класса Σ. Обозначается $[\Sigma]$.

Класс Σ замкнут тогда и только тогда, когда $[\Sigma] = \Sigma$.

Если M — функционально полный класс, тогда $[M]$ — класс всех функций.

Примеры.

1. Множество всех дизъюнкций — замкнуто.
2. Множество всех линейных функций — замкнуто. Нельзя получить из линейных функций с помощью суперпозиции конъюнкцию и дизъюнкцию.

Упражнения.

1. Получить из нелинейной функции с помощью суперпозиций функцию, которая является линейной.
2. Получить из немонотонной функции с помощью суперпозиций функцию, которая является монотонной.

Определение 3. Два булевых вектора $\delta = (\delta_1, \dots, \delta_n)$ и $\tau = (\tau_1, \dots, \tau_n)$ сравнимы по возрастанию $\delta \le \tau$, тогда и только тогда, когда $\delta_i \le \tau_i$ для всех $i = 1, 2, \dots, n$. Имеем отношение частичного порядка на множестве этих векторов.

Определение 4. Булева функция от n переменных $f(x_1, \dots, x_n)$ называется монотонной, если из того, что $\delta \le \tau$ следует, что $f(\delta) \le f(\tau)$.

Примеры.

1. Константы 0 и 1 — монотонные функции.
2. Отрицание $\bar{x}$ — немонотонная функция, так как при $0 < 1$ получим $\bar{0} > \bar{1}$.
3. Конъюнкция и дизъюнкция — монотонные функции.

Теорема 1. Любая логическая формула, не содержащая отрицаний, представляет монотонную функцию, отличную от констант 0 и 1.

Обратно. Любая монотонная функция отличная от 0 и 1 представляет логическую формулу без знаков отрицаний.

Теорема 2. Множество монотонных функций является замкнутым классом.

Это следствие из теоремы 1, так как отрицание является немонотонной функцией.

Следствие. Класс монотонных функций является замыканием для $\{\wedge, \vee, 0, 1\}$.

Лемма 1 (о немонотонных функциях). Если булева функция от n переменных $f(x_1, \dots, x_n)$ немонотонна, то подстановкой констант из нее можно получить отрицание.

Доказательство. Функция $f(x_1, \dots, x_n)$ по условию немонотонна. Значит, существуют такие наборы δ и τ, что $\delta < \tau$, а $f(\delta) = 1$ и $f(\tau) = 0$. Пусть δ и τ отличаются в k компонентах, где $\delta_i \le \tau_i$, а остальные компоненты совпадают. Тогда можно получить цепочку наборов: $\delta < \omega^1 < \omega^2 < \dots < \, < \omega^{k-1} < \tau$. В этой цепочке обязательно найдется два соседних элемента ω^j и ω^{j+1}, такие что $f(\omega^j) = 1$ и $f(\omega^{j+1}) = 0$. Пусть ω^j и ω^{j+1} отличаются на компоненте ω_i^j. Другими словами, $\omega_i^j = 0$, а $\omega_i^{j+1} = 1$. Остальные совпадающие компоненты подставляем в функцию.

Покажем, что $f(*, \dots, *, x_i, *, \dots, *) = \varphi(x_i) = \overline{x_i}$:

$$\varphi(0) = \varphi\left(\omega_i^j\right) = f(\omega^j) = 1 = \bar{0}$$

$$\varphi(1) = \varphi\left(\omega_i^{j+1}\right) = f(\omega^{j+1}) = 0 = \bar{1}$$

Следовательно, $\varphi(x) = \bar{x}$.

Лемма 2 (о нелинейных функциях). Пусть $f(x_1, \dots, x_n)$ нелинейная функция, тогда с помощью подстановки констант и используя отрицание можно получить конъюнкцию и дизъюнкцию.

Доказательство. Если $f(x_1, \dots, x_n)$ нелинейная функция, тогда ее полином Жегалкина содержит хотя бы одно произведение. Пусть самое короткое произведение по количеству множителей $x_{i_1} \cdot \dots \cdot x_{i_k}$. Положим $x_{i_3} = \dots = x_{i_k} = 1$, а все остальные переменные, которые не вошли в произведение, равны 0.

Тогда полином Жегалкина имеет вид $x_{i_1} \cdot x_{i_2} + \alpha x_{i_1} + \beta x_{i_2} + \gamma$, где $\alpha, \beta, \gamma \in \{0,1\}$. Теперь имеем функцию двух переменных $\varphi = xy \oplus \alpha x \oplus \beta y \oplus \gamma$. Рассмотрим всевозможные (8) полиномы Жегалкина для нелинейной функции двух переменных в следующей таблице:

$\boldsymbol{\varphi}$	$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$	$\boldsymbol{\gamma}$	**Вид полинома**	**Логическая формула**	**Супер-позиция для $\boldsymbol{x \wedge y}$**	**Супер-позиция для $\boldsymbol{x \vee y}$**
φ_0	0	0	0	$x \cdot y$	$x \wedge y = \overline{\bar{x} \vee \bar{y}}$	$\varphi_0(x, y)$	$\overline{\varphi_0(\bar{x}, \bar{y})}$
φ_1	0	0	1	$x \cdot y \oplus 1$	$\overline{x \wedge y} = \bar{x} \vee \bar{y}$	$\overline{\varphi_1(x, y)}$	$\varphi_1(\bar{x}, \bar{y})$
φ_2	0	1	0	$x \cdot y \oplus y$	$\bar{x} \wedge y = \overline{x \vee \bar{y}}$	$\varphi_2(\bar{x}, y)$	$\overline{\varphi_2(x, \bar{y})}$
φ_3	0	1	1	$x \cdot y \oplus y \oplus 1$	$\overline{\bar{x} \wedge y} = x \vee \bar{y}$	$\overline{\varphi_3(\bar{x}, y)}$	$\varphi_3(x, \bar{y})$
φ_4	1	0	0	$x \cdot y \oplus x$	$x \wedge \bar{y} = \overline{\bar{x} \vee y}$	$\varphi_4(x, \bar{y})$	$\overline{\varphi_4(\bar{x}, y)}$
φ_5	1	0	1	$x \cdot y \oplus x \oplus 1$	$\overline{x \wedge \bar{y}} = \bar{x} \vee y$	$\overline{\varphi_5(x, \bar{y})}$	$\varphi_5(\bar{x}, y)$
φ_6	1	1	0	$x \cdot y \oplus x \oplus y$	$\overline{\bar{x} \wedge \bar{y}} = x \vee y$	$\overline{\varphi_6(\bar{x}, \bar{y})}$	$\varphi_6(x, y)$
φ_7	1	1	1	$x \cdot y \oplus x \oplus y \oplus 1$	$\bar{x} \wedge \bar{y} = \overline{x \vee y}$	$\varphi_7(\bar{x}, \bar{y})$	$\overline{\varphi_7(x, y)}$

В любом случае мы получим либо конъюнкцию, либо дизъюнкцию и с помощью законов де Моргана можем из конъюнкции получить дизъюнкцию и наоборот. Что и требовалось доказать.

Определение 5. Будем говорить, что система Σ функционально полна в слабом смысле, если из системы $\Sigma \cup \{0,1\}$ можно получить все логические функции.

Терема о функциональной полноте в слабом смысле. Для того, чтобы система Σ была функционально полной в слабом смысле необходимо и достаточно, чтобы она содержала хотя бы одну немонотонную функцию и хотя бы одну нелинейную функцию.

Доказательство.

Достаточность. Пусть система Σ содержит немонотонную и нелинейную функции (они могут совпадать). По лемме 1 из немонотонной функции можно получить отрицание. По лемме 2 из нелинейной функции с помощью отрицания и констант получим конъюнкцию и дизъюнкцию. Получили $\left\{\wedge, \vee, \overline{\quad}, 0,1\right\}$ – функционально полную систему.

Необходимость. Пусть система $\Sigma \cup \{0,1\}$ функционально полна. Значит, из этой системы с помощью суперпозиций можно получить любую функцию.

Предположим, что в Σ нет немонотонных функций. Так как класс монотонных функций замкнут, то с помощью суперпозиций и подстановкой констант мы получим только монотонные функции, а отрицание немонотонно. Получили противоречие с функциональной полнотой системы $\Sigma \cup \{0,1\}$.

Предположим, что в Σ нет нелинейных функций. Так как класс линейных функций замкнут, то с помощью суперпозиций, даже подставляя константы и используя отрицание, мы получим только линейные функции, а $x \wedge y$ и $x \vee y$ – нелинейные функции. Получили противоречие с функциональной полнотой системы $\Sigma \cup \{0,1\}$. Что и требовалось доказать.

Пример. Показать, что $\Sigma = \{f(x,y,z)\}$ — функционально полна в слабом смысле. Значит, система $\{f(x,y,z); 0; 1\}$ — функционально полна и можно получить все функции с помощью суперпозиции.

$$\begin{aligned} f(x,y,z) = \bar{x}\bar{y}z \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee xyz = \\ &= (x\oplus 1)(y\oplus 1)z\oplus(x\oplus 1)yz\oplus x(y\oplus 1)(z\oplus 1)\oplus xyz = \\ &= (xy\oplus x\oplus y\oplus 1)z\oplus xyz\oplus yz\oplus x(yz\oplus y\oplus z\oplus 1)\oplus xyz = \\ &= xyz\oplus xz\oplus yz\oplus z\oplus yz\oplus xyz\oplus xy\oplus xz\oplus x = xy\oplus x\oplus z. \end{aligned}$$

Полином Жегалкина содержит конъюнкцию, значит $f(x,y,z)$ — нелинейная функция.

Монотонность функции $f(x,y,z)$ нарушается на наборах $(0,0,1) < (1,0,1)$, так как $f(0,0,1) = 1 > f(1,0,1) = 0$.

Следовательно, $\Sigma = \{f(x, y, z)\}$ — функционально полна в слабом смысле.

Определение 6. Будем говорить, что булева функция $f(x_1, \dots, x_n)$ сохраняет ноль, если $f(0, \dots, 0) = 0$ и функция сохраняет единицу, если $f(1, \dots, 1) = 1$.

Определение 7. Функция $f(x_1, \dots, x_n)$ называется самодвойственной, если для любого набора выполняется равенство $f(x_1, \dots, x_n) = \overline{f(\overline{x_1}, \dots, \overline{x_n})}$.

Замечания.

1. Множество функций, сохраняющих ноль, замкнуто.
2. Множество функций, сохраняющих единицу, замкнуто.
3. Класс самодвойственных функций замкнут.

§1.5. Критерий функциональной полноты

Теорема (Поста). Для того чтобы система функций была функционально полной, необходимо и достаточно, чтобы система Σ содержала хотя бы одну нелинейную, немонотонную, несамодвойственную, не сохраняющую ноль и не сохраняющую единицу функцию.

Доказательство. Необходимость следует из замкнутости всех пяти классов булевых функций.

Предположим, что в Σ нет нелинейных функций, значит, все функции в ней линейные. Так как класс линейных функций замкнут, то с помощью суперпозиций мы получим только линейные функции, а $x \wedge y$ и $x \vee y$ – нелинейные функции. Получили противоречие с функциональной полнотой системы Σ. Аналогично доказывается для других замкнутых классов.

Достаточность. По теореме о функциональной полноте в слабом смысле мы можем получить отрицание, дизъюнкцию и конъюнкцию. Значит, осталось получить константы 0 и 1. Пусть $f_0(x_1, \dots, x_n)$ — не сохраняет ноль, а $f_1(x_1, \dots, x_n)$ — не сохраняет единицу и $f(x_1, \dots, x_n)$ — несамодвойственная функция. Следовательно, $f_0(0, \dots, 0) = 1$ и $f_1(1, \dots, 1) = 0$.

Рассмотрим два случая.

1. Пусть $f_0(1, \dots, 1) = 1$ рассмотрим функцию $\varphi(x) = f_0(x, \dots, x)$.

При $x = 0$, имеем $\varphi(0) = f_0(0, \dots, 0) = 1$.

При $x = 1$, имеем $\varphi(1) = f_0(1, \dots, 1) = 1$. Значит $\varphi(x) = 1$.

Построим функцию $\psi(x) = f_1\big(\varphi(x), \dots, \varphi(x)\big)$.

При $x = 0$, имеем $\psi(0) = f_1(1, \dots, 1) = 0$.

При $x = 1$, имеем $\psi(1) = f_1(1, \dots, 1) = 0$. Значит $\psi(x) = 0$.

2. Пусть теперь $f_0(1, \dots, 1) = 0$, тогда:

если $x = 0$, то $\varphi(0) = f_0(0, \dots, 0) = 1 = \overline{0}$;

если $x = 1$, то $\varphi(1) = f_0(1, \dots, 1) = 0 = \overline{1}$.

Значит, $\varphi(x) = f_0(x, \dots, x) = \bar{x}$.

Так как $f(x_1, \dots, x_n)$ — несамодвойственная функция, то найдется такой набор $(\delta_1, \dots, \delta_n)$, на котором выполняется равенство $f(\delta_1, \dots, \delta_n) =$ $= f\left(\overline{\delta_1}, \dots, \overline{\delta_n}\right)$. Введем обозначения: $x^\delta = 1$, если $x = \delta$ и $x^\delta = 0$, если $x \neq \delta$. Тогда $0^0 = 1^1 = 1$ и $0^1 = 1^0 = 0$.

Рассмотрим функцию $f_c(x) = f\left(x^{\delta_1}, \dots, x^{\delta_n}\right)$ и покажем, что она является константой.

$f_c(0) = f\left(0^{\delta_1}, \dots, 0^{\delta_n}\right) = f\left(\overline{\delta_1}, \dots, \overline{\delta_n}\right) = f(\delta_1, \dots, \delta_n) = f\left(1^{\delta_1}, \dots, 1^{\delta_n}\right) = f_c(1)$, значит, $f_c(0) = f_c(1) = f_c(x)$ — одна из констант, тогда вторая константа $\overline{f_c(x)} = \varphi\left(f_c(x)\right) = f_0\left(f_c(x), \dots, f_c(x)\right)$. Что и требовалось доказать.

ГЛАВА 2. ЭЛЕМЕНТЫ МАТЕМАТИЧЕСКОЙ ЛОГИКИ

§ 2.1. Высказывания и операции над ними

Определение 1. Под высказыванием понимается любое повествовательное предложение. При этом содержание самого высказывания нас совершенно не интересует. Нас будет интересовать только вопрос истинности или ложности данного высказывания.

Примеры.

1. Число 20 нацело делится на 4.
2. Рим — столица Франции.
3. Реки впадают в моря.
4. Да здравствует Первое мая!
5. Любая квадратная матрица имеет обратную.
6. Чему равна площадь этого треугольника?
7. Дом летит, медведь голубой.

В этих примерах высказываниями являются предложения 1, 2, 3, 5, из которых 1 и 3 истинны, а 2 и 5 ложны.

Предложения 4 и 6 не являются высказываниями, т.к. они не являются повествовательными. А предложение 7 хотя и является повествовательным, но не будет высказыванием, поскольку о нем ничего нельзя сказать, истинно оно или ложно.

Произвольные высказывания будем обозначать заглавными буквами $\mathrm{A}, \mathrm{B}, \mathrm{C}$. Так же, как в русском языке из простых предложений можно строить сложные, на множестве высказываний можно ввести ряд операций, с помощью которых из простых высказываний строятся более сложные.

Определение 2. Конъюнкцией высказываний А и В называется такое высказывание, которое истинно тогда и только тогда, когда истинны оба высказывания.

Обозначать конъюнкцию высказываний А и В будем через $A \wedge B$ (иногда обозначают А&В). Читается как «А и В».

Если через И обозначим истину, а через Л ложь, то значение истинности или ложности конъюнкции $A \wedge B$ можно записать в виде следующей таблицы, которая называется таблицей истинности:

A	B	$A \wedge B$
Л	Л	Л
Л	И	Л
И	Л	Л
И	И	И

Например, рассмотрим высказывание «π — целое число и в году 12 месяцев». Здесь мы имеем высказывание А «π — целое число» и высказывание В «В году 12 месяцев», а наше высказывание есть конъюнкция $A \wedge B$. Эта конъюнкция ложна, т.к. первое высказывание А ложно (хотя второе высказывание В истинно).

Определение 3. Дизъюнкцией высказываний А и В называется такое высказывание, которое истинно тогда и только тогда, когда истинно хотя бы одно из высказываний А или В.

Обозначать дизъюнкцию будем через $A \vee B$. Читается дизъюнкция как «А или В». В разговорной речи союз «или» употребляется в двух смыслах:

1) Включающее «или», т.е. либо А, либо В, либо оба вместе;

2) включающее «или», т.е. либо А, либо В.

Здесь союз «или» употребляется как включающий. Таблица истинности для дизъюнкции будет следующая таблица:

A	B	$A \vee B$
Л	Л	Л
Л	И	И
И	Л	И
И	И	И

Например, для предыдущих высказываний: A («π — целое число») и B («В году 12 месяцев») их дизъюнкция $A \vee B$ («π — целое число или в году 12 месяцев») будет истинной, т.к. высказывание B истинно.

Определение 4. Импликацией высказываний A и B называется высказывание, которое ложно тогда и только тогда, когда A истинно и B ложно. Обозначается импликация через $A \to B$ и читается по-разному: «если A, то B»; «A влечет B»; «из A следует B» и т.п. При этом высказывание A называется посылкой, а B – следствием.

Таблица истинности для высказывания $A \to B$ имеет следующий вид:

A	B	$A \to B$
Л	Л	И
Л	И	И
И	Л	Л
И	И	И

Например, для предыдущих высказываний A и B можно построить две импликации:

1) «если π — целое число, то в году 12 месяцев»: $A \to B$;

2) «если в году 12 месяцев, то π — целое число»: $B \to A$.

По определению высказывание $A \to B$ истинно, а $B \to A$ ложно.

Импликация наиболее сложна для восприятия. Обычно в русском языке принято, что когда имеем импликацию «из A следует B», то между посылкой A и следствием B имеется некоторая связь. Например, если натуральное число делится на четыре (посылка A), то оно делится на 2 (следствие B).

На самом деле импликация не предполагает какой-либо связи между посылкой и следствием. Например, в высказывании «Если тигр — это растение, то Рим — столица Франции» нет никакой связи между посылкой и следствием. Тем не менее это высказывание истинно, т.к. и посылка, и следствие ложны. Здесь при определении истинности высказывания $A \to B$ надо руководствоваться теми соображениями, что из истины можно получить только истину, а из лжи можно получить что угодно.

Определение 5. Эквивалентностью высказываний A и B называется высказывание, которое истинно тогда и только тогда, когда высказывание A и B принимают одинаковое значение.

Обозначается эквивалентность через А~В. Читается как «А эквивалентно В», или «А тогда и только тогда, когда В», или « А необходимо и достаточно для В» и т.п. Таблица истинности для эквивалентности имеет следующий вид:

А	В	А~В
Л	Л	И
Л	И	Л
И	Л	Л
И	И	И

Истинность (ложность) эквивалентности А~В вполне соответствует обычным восприятиям эквивалентности в русском языке: истина эквивалентна истине и ложь эквивалентна лжи. Например, высказывание «Натуральное число делится нацело на 6 тогда и только тогда, когда оно делится на 3» ложно, а выказывание «Натуральное число делится на 6 тогда и только тогда, когда оно делится на 2 и на 3» истинно.

Все введенные на множестве высказываний операции являются бинарными алгебраическими операциями. На этом же множестве вводится еще одна важная унарная операция.

Определение 6. Отрицанием высказывания А называется такое высказывание, которое истинно тогда и только тогда, когда А ложно. Обозначается отрицанием через $\overline{A}$ (иногда через ¬А). Читается отрицание $\overline{A}$ как «не А», или «неверно, что А». Его таблицей истинности будет следующая таблица:

А	$\overline{A}$
Л	И
И	Л

Например, высказывание «Неверно, что 6 — нечетное число» является истинным, т.е. оно есть отрицание ложного высказывания «6 — нечетное число».

Используя введенные логические операции можно из простых высказываний строить сложные.

Определение 7. Сложные высказывания, построенные из простых с помощью логических операций $\vee, \wedge, \rightarrow, \sim, \overline{\ \ }$ — называются формулами логики высказываний. Простейшие высказывания, входящие в формулу, называются переменными высказываниями. Формулы логики высказываний будем обозначать прописными буквами $\mathcal{A}, \mathcal{B}, \mathcal{F}$ т.д. Если мы хотим отметить какие переменные высказывания входят в формулу $\mathcal{A}$, то будем писать $\mathcal{A}(x_1, \dots, x_n)$ где $x_1, \dots, x_n$ — переменные высказывания.

При составлении формул обычно используют скобки, указывающие, в какой последовательности производятся операции.

Например, $\big((A \vee B) \rightarrow C\big) \sim \big((B \vee C) \rightarrow A\big)$. Иногда скобки опускают. При этом руководствуются следующими правилами. Первой выполняется конъюнкция, затем дизъюнкция, потом импликация и наконец, эквивалентность. Кроме того, считают, что знак отрицания, стоящий над формулой, делает излишними скобки.

Например, в формуле $B \sim \bar{C} \vee D \wedge A \rightarrow B$ скобки восстанавливаются следующим образом:

$B \sim (\bar{C}) \vee D \wedge A \rightarrow B$, $\quad B \sim (\bar{C}) \vee (D \wedge A) \rightarrow B$, $\quad B \sim \big((\bar{C}) \vee (D \wedge A)\big) \rightarrow B$, $B \sim \Big(\big((\bar{C}) \vee (D \wedge A)\big) \rightarrow B\Big)$.

Мы, как правило, будем использовать скобки.

Задачи логики высказываний состоят в изучении зависимостей между истинностью и ложностью простых и сложных высказываний, т.е. в определении истинности или ложности формулы в зависимости от того, какие значения истинности – ложности принимают входящие в них переменные высказывания.

Пример 2. Каково значение формулы $\overline{\overline{(X \vee Y)} \wedge \Big(Z \rightarrow \big(U \rightarrow (V \rightarrow W)\big)\Big)}$, если переменные высказывания принимают значения $X = И$, $Y = Л$, $Z = И$, $U = И$, $V = Л$ и $W = Л$?

Подставляя в формулу значения переменных и применяя определения операций, имеем:

$\overline{\overline{(И \vee Л)} \wedge \Big(И \rightarrow \big(И \rightarrow (Л \rightarrow Л)\big)\Big)}$ или $\overline{\bar{И} \wedge \big(И \rightarrow (И \rightarrow И)\big)}$,

или $\overline{Л \wedge (И \rightarrow И)}$ или $\overline{Л \wedge И}$, или $\bar{Л}$, или И.

Таким образом, при данных значениях переменных высказываний формула принимает значение И.

Если имеем формулу $\mathcal{A}(x_1, \dots, x_n)$, то можно вычислить все значения истины — лжи формулы $\mathcal{A}$ при различных значениях переменных. Для этого достаточно составить таблицу истинности для формулы $\mathcal{A}$, в которой переменным $(x_1, \dots, x_n)$ придаются всевозможные наборы значений И или Л. Известно, что таких наборов будет 2^n.

Пример 3. Построим таблицу истинности для формулы

$$\mathcal{A} = \big(\mathrm{A} \rightarrow (\mathrm{B} \sim \mathrm{C})\big) \vee \big(\mathrm{B} \rightarrow (\bar{\mathrm{C}} \sim \bar{\mathrm{A}})\big):$$

A	B	C	$\mathrm{B}\sim\mathrm{C}$	$\mathrm{A}\rightarrow(\mathrm{B}\sim\mathrm{C})$	$\bar{\mathrm{C}}$	$\bar{\mathrm{A}}$	$\bar{\mathrm{C}}\sim\bar{\mathrm{A}}$	$\mathrm{B}\rightarrow(\bar{\mathrm{C}}\sim\bar{\mathrm{A}})$	$\mathcal{A}$
Л	Л	Л	И	И	И	И	И	И	И
Л	Л	И	Л	И	Л	И	Л	И	И
Л	И	Л	Л	И	И	И	И	И	И
Л	И	И	И	И	Л	И	Л	Л	И
И	Л	Л	И	И	И	Л	Л	И	И
И	Л	И	Л	Л	Л	Л	И	И	И
И	И	Л	Л	Л	И	Л	Л	Л	Л
И	И	И	И	И	Л	Л	И	И	И

Таким образом, данная формула всегда истинна, кроме случая, когда $\mathrm{A} = \text{И}$, $\mathrm{B} = \text{И}$, $\mathrm{C} = \text{Л}$.

§ 2.2. Равносильные формулы

Определение 1. Две формулы $\mathcal{A}$ и $\mathcal{B}$ называются равносильными, если при любых значениях $x_1, \dots, x_n$, где $x_1, \dots, x_n$ — совокупность всех переменных входящих в $\mathcal{A}$ и $\mathcal{B}$, эти формулы принимают одинаковые значения. Обозначается равносильность через $\mathcal{A} \equiv \mathcal{B}$. Считается, что если некоторая переменная X_i явно не входит в формулу, то она входит в нее фиктивно.

Теорема 1. Отношение равносильности является отношением эквивалентности на множестве всех формул.

Доказательство. Очевидно, что $\mathcal{A} \equiv \mathcal{A}$, т.е. отношение равносильности рефлексивно. Далее, если $\mathcal{A} \equiv \mathcal{B}$, то при любом наборе значений переменных формула $\mathcal{A}$ принимает те же значения, что и $\mathcal{B}$. Но тогда формула $\mathcal{B}$ принимает те же значения, что и $\mathcal{A}$, т.е. $\mathcal{B} \equiv \mathcal{A}$. Следовательно, отношение равносильности симметрично. Наконец, пусть $\mathcal{A} \equiv \mathcal{B}$, $\mathcal{B} \equiv \mathcal{D}$, и пусть при каком-то наборе значений переменных формула $\mathcal{A}$ принимает значение И. Тогда из $\mathcal{A} \equiv \mathcal{B}$ следует, что при этом наборе значений переменных формула $\mathcal{B}$ принимает значение И, а из $\mathcal{B} \equiv \mathcal{D}$ следует, что и $\mathcal{D}$ принимает значение И. Аналогично, если при каком-то наборе значений переменных формула $\mathcal{A}$

принимает значение Л, то и $\mathcal{D}$ принимает значение Л. Следовательно, $\mathcal{A} \equiv \mathcal{D}$, т.е. отношение равносильности транзитивно.

Таким образом, множество всех формул разбивается на непересекающиеся классы равносильных формул. Поэтому, естественно, в каждом классе для изучения всех формул класса достаточно выбрать наиболее простую формулу, которая будет принимать те же значения, что и любая формула из данного класса. Кроме того, если в данной формуле некоторую ее часть (подформулу) заменить ей равносильной, то полученная формула будет равносильна исходной. Итак, одной из основных задач логики высказываний является задача преобразования данной формулы в более простую, равносильную исходной. При этом используют новые типы равносильностей, указанные в следующей теореме – теореме 2.

Теорема 2. Для любых высказываний X, Y и Z справедливы следующие равносильности:

$\overline{\overline{X}} \equiv X$ — инволютивность;

$X \wedge X \equiv X$ — идемпотентность конъюнкции и дизъюнкции,

$X \vee X \equiv X$ — соответственно;

$X \wedge Y \equiv Y \wedge X$ — коммутативность конъюнкции и дизъюнкции,

$X \vee Y \equiv Y \vee X$ — соответственно;

$(X \wedge Y) \wedge Z \equiv X \wedge (Y \wedge Z)$ — ассоциативность конъюнкции;

$(X \vee Y) \vee Z \equiv X \vee (Y \vee Z)$ — ассоциативность дизъюнкции;

$X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)$ — дистрибутивность конъюнкции относительно дизъюнкции;

$X \vee (Y \wedge Z) \equiv (X \vee Y) \wedge (X \vee Z)$ — дистрибутивность дизъюнкции относительно конъюнкции;

$X \wedge (X \vee Y) \equiv X$ — законы поглощения;

$X \vee (X \wedge Y) \equiv X$

$\overline{X \wedge Y} \equiv \overline{X} \vee \overline{Y}$ — законы де Моргана;

$\overline{X \vee Y} \equiv \overline{X} \wedge \overline{Y}$

$X \wedge \overline{X} \equiv Л$

$X \vee \overline{X} \equiv И$;

$X \wedge Л \equiv Л$

$X \vee Л \equiv X$;

$X \wedge И \equiv X$

$X \vee И \equiv И$.

Доказательства всех этих равносильностей проводятся непосредственно составлением таблиц истинности для левых и правых частей и их сравнением.

Пример 1. Упростить формулу $((X \vee X) \wedge Y) \vee (X \vee X)$.

Используем равносильности из теоремы 2 $((X \vee X) \wedge Y) \vee (X \vee X))$. Далее, применяя свойство идемпотентности $|\equiv(X \wedge Y) \vee X\equiv|$, используем коммутативность дизъюнкции $|\equiv X \vee (X \wedge Y)\equiv|$ и используем закон поглощения $|\equiv X$.

Основные типы равносильностей в теореме 2 приведены только для операций $\wedge,\vee$ и $\overline{}$. Дело в том, что в записи формул можно обходиться и без импликации, и без эквивалентности. Рассмотрим, к примеру, таблицу истинности для формулы $(X \to Y) \wedge (Y \to X)$:

X	Y	$X \to Y$	$Y \to X$	$(X \to Y) \wedge (Y \to X)$
Л	Л	И	И	И
Л	И	И	Л	Л
И	Л	Л	И	Л
И	И	И	И	И

Мы видим, что таблица истинности для этой формулы совпадает с таблицей истинности для формулы $X\sim Y$, т.е. $X\sim Y\equiv(X \to Y) \wedge (Y \to X)$. Эта равносильность говорит о том, что в любую формулу, содержащую операцию $\sim$, можно заменить равносильной, но не содержащей эту операцию. То же самое можно сказать и об операции импликации, поскольку, как легко проверить, имеет место равносильность $X \to Y\equiv\overline{X} \vee Y$.

Таким образом, имеет место следующая теорема.

Теорема 3. Всякую формулу логики высказываний можно заменить равносильной, содержащей лишь операции $\wedge,\vee,\overline{}$, причем знак отрицания будет стоять лишь над переменными высказываниями.

Доказательство.

Применив равносильности $X \to Y\equiv\overline{X} \vee Y$ и $X\sim Y\equiv(X \to Y) \wedge (Y \to X)$, получим равносильную формулу, содержащую лишь операции $\wedge,\vee,\overline{}$. Если при этом формула содержит подформулу типа $\overline{A \wedge B}$ (или $\overline{A \vee B}$), то заменяем их равносильными $\overline{A} \vee \overline{B}$ (соответственно, $\overline{A} \wedge \overline{B}$) согласно законам де Моргана. Если после этого снова получим подформулы такого же типа, то повторяем снова подобную замену. И так до тех пор, пока не добьемся, чтобы знак отрицания стоял только над переменными высказываниями. При этом при необходимости используем равносильность $\overline{\overline{A}}\equiv A$.

Пример 2.

$$(A \to B) \vee (\overline{(B\sim C)} \wedge (\overline{C \to A}))\equiv$$
$$\equiv(\overline{A} \vee B) \vee (\overline{((B \to C) \wedge (C \to B))} \wedge \overline{(\overline{C} \vee A)})\equiv$$

$$\equiv(\overline{A} \vee B) \vee (\overline{((\overline{B} \vee C) \wedge (\overline{C} \vee B))} \wedge \overline{(\overline{C} \vee A)})\equiv$$

$$\equiv(\overline{A} \vee B) \vee \Big((\overline{(\overline{B} \vee C)} \vee \overline{(\overline{C} \vee B)}) \wedge \big(\overline{\overline{C}} \wedge \overline{A}\big)\Big)\equiv$$

$$\equiv(\overline{A} \vee B) \vee (((\overline{\overline{\overline{B}}} \wedge \overline{C}) \vee (\overline{\overline{C}} \wedge \overline{B})) \wedge (C \wedge \overline{A}))\equiv$$

$$\equiv(\overline{A} \vee B) \vee \Big(\big((B \wedge \overline{C}) \vee (C \wedge \overline{B})\big) \wedge (C \wedge \overline{A})\Big).$$

Определение 2. Пусть формулы $\mathcal{A}$ и $\mathcal{A}^*$ приведены к виду, в котором присутствуют лишь операции $\wedge$,$\vee$ и $\overline{\ \ }$, а знак отрицания стоит только над переменными высказываниями. Формулы $\mathcal{A}$ и $\mathcal{A}^*$ называются двойственными, если одна из них получена из другой заменой конъюнкций на дизъюнкции, а дизъюнкций на конъюнкции. При этом говорят, что конъюнкция двойственна дизъюнкции и наоборот.

Теорема 4. Если формулы $\mathcal{A}(X_1, \dots, X_n)$ и $\mathcal{A}^*(X_1, \dots, X_n)$ двойственны, то $\overline{\mathcal{A}(X_1, \dots, X_n)}\equiv\mathcal{A}^*(\overline{X_1}, \dots, \overline{X_n})$.

Доказательство. Прежде всего заметим, что если в равносильностях теоремы 2 переменные X, Y, Z заменим произвольными формулами $\mathcal{A}, \mathcal{B}, \mathcal{C}$ то снова получим равносильные формулы. Рассмотрим, к примеру, формулу $\mathcal{A} \vee (\mathcal{A} \wedge \mathcal{B})\equiv\mathcal{A}$ (закон поглощения). Пусть при некотором наборе значений переменных формула $\mathcal{A}$ принимает значение И. Тогда, независимо от того, какое значение принимает формула $\mathcal{B}$ при этом наборе значений переменных, имеем либо И $\vee$ И$\equiv$И, либо И $\vee$ Л$\equiv$И, т.е. то же значение, что и $\mathcal{A}$. Если при каком-то наборе значений переменных формула $\mathcal{A}$ принимает значение Л, то независимо от значения $\mathcal{B}$, формула $\mathcal{A} \wedge \mathcal{B}$ принимает значений Л, а поэтому $\mathcal{A} \vee (\mathcal{A} \wedge \mathcal{B})\equiv$Л $\vee$ Л$\equiv$Л, т.е. то же значение, что и у формулы $\mathcal{A}$.

Таким образом, $\mathcal{A} \vee (\mathcal{A} \wedge \mathcal{B})\equiv\mathcal{A}$.

Аналогично доказывается и для остальных равносильностей.

После этого замечания утверждение теоремы достаточно доказать для случая, когда формула $\mathcal{A}$ имеет вид $X \wedge Y$, $X \vee Y$ или X.

Итак, пусть $\mathcal{A}(X, Y)\equiv X \wedge Y$. Тогда $\mathcal{A}^*(X, Y)\equiv X \vee Y$. В таком случае, имеем $\overline{\mathcal{A}(X, Y)}\equiv\overline{X \wedge Y}\equiv\overline{X} \vee \overline{Y}\equiv\mathcal{A}^*(\overline{X}, \overline{Y})$.

Аналогично, если $\mathcal{A}(X, Y)\equiv X \vee Y$, то $\overline{\mathcal{A}(X, Y)}\equiv\overline{X \vee Y}\equiv\overline{X} \wedge \overline{Y}\equiv\mathcal{A}^*(\overline{X}, \overline{Y})$.

Наконец, если $\mathcal{A}(X)\equiv X$, то $\mathcal{A}^*(X)\equiv X$, и поэтому $\overline{\mathcal{A}(X)}\equiv\overline{X}\equiv\mathcal{A}^*(\overline{X})$.

Теорема 5 (закон двойственности). Если $\mathcal{A}\equiv\mathcal{B}$, то тогда $\mathcal{A}^*\equiv\mathcal{B}^*$.

Доказательство. Пусть $X_1, \dots, X_n$ — переменные, входящие в формулы $\mathcal{A}$ и $\mathcal{B}$. По условию $\mathcal{A}(X_1, \dots, X_n)\equiv\mathcal{B}(X_1, \dots, X_n)$, т.е. формулы $\mathcal{A}$ и $\mathcal{B}$ принимают одинаковые значения при любых значениях переменных $X_1, \dots, X_n$. Значит, они принимают одинаковые значения и для переменных $\overline{X_1}, \dots, \overline{X_n}$ т.е. $\mathcal{A}(\overline{X_1}, \dots, \overline{X_n})\equiv\mathcal{B}(\overline{X_1}, \dots, \overline{X_n})$. Отсюда $\overline{\mathcal{A}(\overline{X_1}, \dots, \overline{X_n})}\equiv\overline{\mathcal{B}(\overline{X_1}, \dots, \overline{X_n})}$. Согласно предыдущей теореме, $\overline{\mathcal{A}(\overline{X_1}, \dots, \overline{X_n})}\equiv\mathcal{A}^*\big(\overline{\overline{X_1}}, \dots, \overline{\overline{X_n}}\big)\equiv\mathcal{A}^*(X_1, \dots, X_n)$

и $\overline{\mathcal{B}(\overline{X_1},\dots,\overline{X_n})}$≡$\mathcal{B}^*(\overline{\overline{X_1}},\dots,\overline{\overline{X_n}})$≡$\mathcal{B}^*(X_1,\dots,X_n)$,

т.е. $\mathcal{A}^*(X_1,\dots,X_n)$≡$\mathcal{B}^*(X_1,\dots,X_n)$.

Теорема двойственности говорит о том, что если мы доказали какую-либо равносильность для формул, то мы автоматически имеем аналогичную равносильность и для двойственных формул.

Определение 3. Если переход от формулы $\mathcal{A}$ к формуле $\mathcal{B}$ осуществляется путем каких-то равносильных преобразований, то соответствующие преобразования, переводящие $\mathcal{A}^*$ в $\mathcal{B}^*$, называются двойственными к исходным преобразованиям.

При доказательстве теоремы 8 для случая $\mathcal{A}(X) \equiv X$ мы получили, что формула $\mathcal{A}$ совпадает с формулой $\mathcal{A}^*$. Это есть частный случай более общего понятия самодвойственной формулы.

Определение 4. Формула $\mathcal{A}(X_1,\dots,X_n)$ называется самодвойственной, если $\mathcal{A}(X_1,\dots,X_n) \equiv \mathcal{A}^*(X_1,\dots,X_n)$. Другими словами, согласно теореме 8., формула $\mathcal{A}(X_1,\dots,X_n)$ самодвойственна, если $\overline{\mathcal{A}(X_1,\dots,X_n)} \equiv \mathcal{A}(\overline{X_1},\dots,\overline{X_n})$ или (что то же самое) $\mathcal{A}(X_1,\dots,X_n) \equiv \overline{\mathcal{A}(\overline{X_1},\dots,\overline{X_n})}$

§ 2.3. Проблема разрешения

Определение 1. Формула $\mathcal{A}(X_1,\dots,X_n)$ называется тождественно истинной или тавтологией, если она принимает значение И при любых входящих в нее переменных $X_1,\dots,X_n$.

Формула $\mathcal{A}(X_1,\dots,X_n)$ называется выполнимой, если она принимает значение И хотя бы при одном наборе значений входящих в нее переменных.

Формула $\mathcal{A}(X_1,\dots,X_n)$ называется невыполнимой, или тождественно ложной, или противоречием, если она принимает значение Л при любом наборе значений входящих в нее переменных.

Любая из формул, определяющих операции $\wedge, \vee, \rightarrow, \sim$, т.е. формул $A \wedge B$, $A \vee B$, $A \rightarrow B$ и $A \sim B$, является выполнимой.

Простейшим примером тождественно истинной формулы является формула $A \vee \overline{A}$. Очевидно, что отрицание тождественно истинной формулы будет тождественно ложной формулой. В частности, $A \wedge \overline{A}$ — простейший пример тождественно ложной формулы. Легко видеть, что формула $(A \vee \overline{A}) \rightarrow (A \wedge \overline{A})$ тождественно ложна, т.к. посылка всегда истинна, а следствие всегда ложно. Этот пример является частным случаем более общего утверждения: если A тождественно истинна, B тождественно ложна, а D — любая формула, то формула $A \rightarrow B$ тождественно ложна, а $B \rightarrow D$ тождественно истинна.

Одной из важнейших задач является задача нахождения единых алгоритмов, позволяющих выяснить, будет ли данная формула тождественно истинной (тождественно ложной, выполнимой). На самом деле достаточно знать один из требуемых алгоритмов, с помощью которого можно отвечать на каждый из трех вопросов.

Пусть мы владеем некоторым алгоритмом S, позволяющим отвечать на вопрос, тождественно истинна формула или нет, и пусть $\mathcal{A}$ — произвольная формула. Требуется выяснить, какова формула $\mathcal{A}$. С помощью алгоритма S проверяем формулу $\mathcal{A}$ на тождественную истинность. Если она тождественно истинна, то ответ получен. Пусть она не тождественно истинна, т.е. при каком-то наборе значений переменных значение формулы $\mathcal{A}$ есть Л. Значит, формула $\mathcal{A}$ может быть либо тождественно ложной, либо выполнимой. После этого проверяем с помощью алгоритма S формулу $\bar{\mathcal{A}}$ на тождественную истинность. Если $\bar{\mathcal{A}}$ тождественно истинна, то формула $\bar{\mathcal{A}}$ тождественно ложна. Если же при каком-то наборе значений переменных формула $\bar{\mathcal{A}}$ принимает значение Л, исходная формула $\mathcal{A}$ принимает значение И, т.е. $\mathcal{A}$ выполнима.

Пусть мы владеем некоторым алгоритмом S, позволяющим отвечать на вопрос, является ли данная формула тождественно ложной или нет. Для произвольной формулы $\mathcal{A}$ проверяем на тождественную ложность. Если $\mathcal{A}$ тождественно ложна, то ответ получен. В противном случае с помощью алгоритма S проверяем на тождественную ложность формулу $\bar{\mathcal{A}}$. Если $\bar{\mathcal{A}}$ тождественно ложна, то тогда исходная формула $\mathcal{A}$ тождественно истинна. Если же $\bar{\mathcal{A}}$ не тождественно ложна, то исходная формула $\mathcal{A}$ выполнима.

Наконец, пусть мы владеем алгоритмом S, позволяющим определять выполнимость любой формулы, и пусть $\mathcal{A}$ — произвольная формула. Проверяем формулу $\mathcal{A}$ на выполнимость с помощью алгоритма S. Если $\mathcal{A}$ невыполнима, то она тождественно ложна. Если же $\mathcal{A}$ выполнима, то она может быть тождественно истинной. Проверяем формулу $\bar{\mathcal{A}}$ на выполнимость. Если $\bar{\mathcal{A}}$ невыполнима, то она тождественно ложна, а тогда $\mathcal{A}$ тождественно истинна. Если же $\bar{\mathcal{A}}$ выполнима, то $\mathcal{A}$ тоже выполнима.

Итак, мы показали, что вместо трех алгоритмов достаточно владеть одним. Как правило, рассматривают вопрос об алгоритме, проверяющем формулу на тождественную истинность. Проблема существования и нахождения такого алгоритма и носит название проблемы разрешения.

Проблема разрешения. Указать единый способ (алгоритм), позволяющий для любой формулы логики высказываний выяснять, является ли она тождественно истинной.

Один из таких алгоритмов будет указан в следующем параграфе.

§ 2.4. Дизъюнктивные и конъюнктивные нормальные формы

Определение 1. Элементарным произведением называется конъюнкция переменных или их отрицаний. Элементарной суммой называется дизъюнкция переменных или их отрицаний.

Теорема 1. Элементарное произведение тождественно ложно тогда и только тогда, когда в нем содержится хотя бы одна пара множителей, из которых один есть переменная, а другой — ее отрицание.

Доказательство. Пусть элементарное произведение P содержит пару таких множителей, т.е. $\mathrm{P} \equiv \mathrm{X} \wedge \mathrm{Y} \wedge \ldots \wedge \overline{\mathrm{X}} \wedge \ldots \wedge \mathrm{Z}$.

Тогда $\mathrm{P} \equiv (\mathrm{X} \wedge \overline{\mathrm{X}}) \wedge \mathrm{Y} \wedge \ldots \wedge \mathrm{Z} \equiv Л \wedge \mathrm{Y} \wedge \ldots \wedge \mathrm{Z} \equiv Л$, т.е. P тождественно ложна.

Обратно, пусть $\mathrm{P} \equiv Л$, но такой пары множителей в P нет. Придадим каждой переменной, входящей в P, следующие значения: если переменная входит в произведение без знака отрицания, то ей придаем значение И; если же входит со знаком отрицания, то ей придаем значение Л. Такие значения для множителей придать можно. Их нельзя было бы подставить в формулу P только в случае, когда какой-то переменной пришлось бы одновременно придавать и значение И, и значение Л. Но тогда бы эта переменная входила бы в P и со знаком отрицания, и без него, чего у нас нет. Итак, придав такие значения переменным, мы получим, что формула P принимает значение И, что противоречит тождественной ложности формулы P. Полученное противоречие говорит о том, что формула P обязательно содержит два множителя, из которых один является отрицанием другого.

Теорема 2. Элементарная сумма тождественно истинна тогда и только тогда, когда она содержит хотя бы одну пару слагаемых, из которых одно есть переменная, а другое — ее отрицание.

Доказательство. Доказательство теоремы аналогично доказательству предыдущей. Если элементарная сумма S имеет вид $\mathrm{S} \equiv \mathrm{X} \vee \mathrm{Y} \vee \ldots \vee \overline{\mathrm{X}} \vee \ldots \vee \mathrm{Z}$, то $\mathrm{S} \equiv (\mathrm{X} \vee \overline{\mathrm{X}}) \vee \mathrm{Y} \vee \ldots \vee \mathrm{Z} \equiv И \vee \mathrm{Y} \vee \ldots \vee \mathrm{Z} \equiv И$. Обратно, пусть $\mathrm{S} \equiv И$ и пусть S не содержит пары слагаемых, из которых одно является отрицанием другого. Придав тем переменным, которые входят в S без знака отрицания, значение Л, а тем, которые входят со знаком отрицания, значение И, получим, что S принимает значение Л, что противоречит условию.

Определение 2. Формула, равносильная данной формуле $\mathcal{A}$ и представляющая собой дизъюнкцию элементарных произведений, называется дизъюнктивной нормальной формой формулы $\mathcal{A}$ (д.н.ф.).

Формула, равносильная данной формуле $\mathcal{A}$ и представляющая собой конъюнкцию элементарных сумм, называется конъюнктивной нормальной формой формулы $\mathcal{A}$ (к.н.ф.).

Теорема 3. Для каждой формулы логики высказываний существует как д.н.ф., так и к.н.ф.

Доказательство. Как уже отмечалось, всякую формулу можно привести к равносильной, содержащей лишь операции $\wedge, \vee, \overline{}$, причем знак отрицания стоит только над переменными высказываниями. Затем, применяя тот или иной закон дистрибутивности, приводим формулу либо к дизъюнкции элементарных конъюнкций, либо к конъюнкции элементарных дизъюнкций.

Пример 1. Найти к.н.ф. и д.н.ф. для формулы $(\overline{X \vee Y}) \sim (X \wedge Y)$.

Сначала приведем эту формулу к формуле, содержащей лишь операции $\wedge, \vee, \overline{}$, и причем к такой, в которой знак отрицания стоит над переменными высказываниями. Для этого применяем равносильность $A \sim B \equiv (\overline{A} \vee B) \wedge (A \vee \overline{B})$, а также законы де Моргана.

$$(\overline{X \vee Y}) \sim (X \wedge Y) \equiv \left((\overline{\overline{X \vee Y}}) \vee (X \wedge Y)\right) \wedge \left((\overline{X \vee Y}) \vee (\overline{X \wedge Y})\right) \equiv$$

$$\equiv \left((X \vee Y) \vee (X \wedge Y)\right) \wedge \left((\overline{X} \wedge \overline{Y}) \vee (\overline{X} \vee \overline{Y})\right) \equiv \text{(применяем закон дистрибутивности)}$$

$$\equiv \left((X \vee Y \vee X) \wedge (X \vee Y \vee Y)\right) \wedge \left((\overline{X} \vee \overline{Y} \vee \overline{X}) \wedge (\overline{X} \vee \overline{Y} \vee \overline{Y})\right) \equiv$$

$\equiv \left((X \vee Y) \wedge (X \vee Y)\right) \wedge \left((\overline{X} \vee \overline{Y}) \wedge (\overline{X} \vee \overline{Y})\right) \equiv (X \vee Y) \wedge (\overline{X} \vee \overline{Y})$ — это и есть к.н.ф. для исходной формулы.

Для нахождения д.н.ф. можно снова преобразовывать в д.н.ф. исходную формулу, а можно использовать уже найденную к.н.ф.

Итак, $(\overline{X \vee Y}) \sim (X \wedge Y) \equiv (X \vee Y) \wedge (\overline{X} \vee \overline{Y}) \equiv$ (применяем законы дистрибутивности) $\equiv \left((X \vee Y) \wedge \overline{X}\right) \wedge \left((X \vee Y) \wedge \overline{Y}\right) \equiv$ (еще раз применяем законы дистрибутивности) $\equiv (X \wedge \overline{X}) \vee (Y \wedge \overline{X}) \vee (X \wedge \overline{Y}) \vee (Y \wedge \overline{Y}) \equiv$ $\equiv Л \vee (Y \wedge \overline{X}) \vee (X \wedge \overline{Y}) \vee Л \equiv (\overline{X} \wedge Y) \vee (X \wedge \overline{Y})$ — это и есть д.н.ф. для исходной формулы.

Теорема 4. Формула логики высказываний является тождественно истинной тогда и только тогда, когда каждый множитель ее к.н.ф. имеет, по крайней мере, два слагаемых, из которых одно является отрицанием другого.

Доказательство.

Пусть формула $\mathcal{A}$ тождественно истинна. Тогда тождественно истинной является ее к.н.ф., т.е. конъюнкция элементарных сумм. Конъюнкция истинна только в случае, когда истинен каждый ее множитель. Следовательно, каждая элементарная сумма тождественно истинна. Тогда по теореме 2 каждая элементарная сумма содержит хотя бы одну пару слагаемых, из которых одно является отрицанием другого.

Обратно, пусть в к.н.ф. каждая элементарная сумма содержит хотя бы одну указанную пару слагаемых. По теореме 2 каждая такая элементарная сумма тождественно истинна. В таком случае конъюнкция этих элементарных сумм, т.е. к.н.ф., является тождественно истинной. А значит, тождественно истинна и сама формула $\mathcal{A}$.

Аналогичным образом доказывается следующая теорема.

Теорема 5. Формула $\mathcal{A}$ является тождественно ложной тогда и только тогда, когда каждое слагаемое ее д.н.ф. содержит хотя бы одну пару множителей, из которых один является отрицанием другого.

Пример 2. Выяснить, какой будет формула $(X \wedge Y) \vee (\overline{X} \wedge \overline{Y})$ — тождественно истинной, тождественно ложной или выполнимой?

Т.к. формула уже представлена в виде д.н.ф. и ни одно слагаемое не содержит переменной вместе с ее отрицанием, то формула не будет тождественно ложной. Проверим, будет ли она тождественно истинной. Для этого найдем для нее к.н.ф.

Итак, $(X \wedge Y) \vee (\overline{X} \wedge \overline{Y}) \equiv [(X \wedge Y) \vee \overline{X}] \wedge [(X \wedge Y) \vee \overline{Y}] \equiv$

$\equiv [(X \vee \overline{X}) \wedge (Y \vee \overline{X})] \wedge [(X \vee \overline{Y}) \wedge (Y \vee \overline{Y})] \equiv$

$\equiv И \wedge (Y \vee \overline{X}) \wedge (X \vee \overline{Y}) \wedge И \equiv (X \vee \overline{Y}) \wedge (\overline{X} \vee Y)$.

Это и есть к.н.ф. для данной формулы. В ней тоже нет ни одного множителя, который в качестве слагаемого содержит некоторую переменную вместе со своим отрицанием. Значит, наша формула не будет тождественно истинной, следовательно, она просто выполнима.

§ 2.5. Совершенные дизъюнктивные и конъюнктивные нормальные формы

Простейшие примеры показывают, что для данной формулы д.н.ф. (как и к.н.ф.) определяется неоднозначно. Например, формула $X \vee (Y \wedge Z)$ уже записана в виде д.н.ф. С другой стороны, $X \vee (Y \wedge Z) \equiv (X \vee Y) \wedge (X \vee Z) \equiv$
$\equiv (X \wedge X) \vee (X \wedge Z) \vee (Y \wedge X) \vee (Y \wedge Z)$ — тоже д.н.ф. для нашей формулы.

Введем специальный вид д.н.ф. (и к.н.ф.), который определяется однозначно.

Определение 1. Совершенной дизъюнктивной нормальной формой (с.д.н.ф.) формулы $\mathcal{A}(X_1, \ldots, X_n)$ от n различных переменных называется такая ее д.н.ф., которая обладает следующими свойствами:

1) в ней нет двух одинаковых слагаемых;
2) ни одно из слагаемых не содержит двух одинаковых множителей;
3) никакое слагаемое не содержит переменной вместе с ее отрицанием;
4) в каждом слагаемом любая из n переменных X_i либо сама входит в качестве множителя, либо ее отрицание.

Определение 2. Совершенной конъюнктивной нормальной формой (с.к.н.ф.) формулы $\mathcal{A}(X_1, \ldots, X_n)$ от n различных переменных называется такая ее к.н.ф., которая обладает следующими свойствами:

1) в ней нет двух одинаковых множителей;
2) ни один из множителей не содержит двух одинаковых слагаемых;

3) никакой множитель не содержит переменной вместе с ее отрицанием;

4) в каждом множителе любая из n переменных X_i либо сама входит в качестве слагаемого, либо ее отрицание.

Теорема 1. Любая не тождественно ложная формула $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_\mathrm{n})$ логики высказываний обладает единственной с.д.н.ф.

Доказательство.

Приведем формулу $\mathcal{A}$ к какой-нибудь д.н.ф. Если какое-либо элементарное произведение В в этой д.н.ф. не содержит ни переменную $\mathrm{X_i}$, ни ее отрицание $\overline{\mathrm{X_i}}$ то заменяем это слагаемое суммой $(\mathrm{X_i} \wedge \mathrm{B}) \vee (\overline{\mathrm{X_i}} \wedge \mathrm{B})$. Во-первых, это снова будет сумма элементарных произведений. А во-вторых, после этой замены мы опять получим равносильную д.н.ф., поскольку $(\mathrm{X_i} \wedge \mathrm{B}) \vee (\overline{\mathrm{X_i}} \wedge \mathrm{B}) \equiv (\mathrm{X_i} \vee \overline{\mathrm{X_i}}) \wedge \mathrm{B} \equiv \text{И} \wedge \mathrm{B} \equiv \mathrm{B}$. Проводим такие замены до тех пор, пока не получим д.н.ф., в которой каждое слагаемое будет содержать любую переменную или ее отрицание. Пусть в полученной д.н.ф. есть одинаковые слагаемые. Поскольку $\mathrm{B} \vee \mathrm{B} \equiv \mathrm{B}$, то удалив их все, кроме одного, получим снова равносильную д.н.ф. Пусть в каком-то слагаемом есть одинаковые множители. Так как $\mathrm{X} \wedge \mathrm{X} \equiv \mathrm{X}$, то, удалив их все, кроме одного, получим снова равносильную д.н.ф.

Наконец, пусть некоторое слагаемое В содержит в качестве множителей переменные $\mathrm{X_i}$ и $\overline{\mathrm{X_i}}$. Поскольку $\mathrm{X_i} \wedge \overline{\mathrm{X_i}} \equiv \text{Л}$ и для любой формулы D имеем $\text{Л} \vee \mathrm{D} \equiv \mathrm{D}$, то, удалив это слагаемое В, мы опять получим равносильную д.н.ф., которая и будет с.д.н.ф.

Прежде чем доказывать единственность с.д.н.ф., введем следующие обозначения. Пусть σ обозначает И или Л. Для переменного высказывания X положим $\mathrm{X}^\sigma \equiv \begin{cases} \text{И, если } \mathrm{X} \equiv \sigma \\ \text{Л, если } \mathrm{X} \not\equiv \sigma \end{cases}$.

Теперь рассмотрим, что в этих обозначениях означают $\mathrm{X}^{\text{И}}$ и $\mathrm{X}^{\text{Л}}$. Пусть $\mathrm{X} \equiv \text{И}$, и тогда $\mathrm{X}^{\text{И}} \equiv \text{И}^{\text{И}} \equiv \text{И} \equiv \mathrm{X}$. Если же $\mathrm{X} \equiv \text{Л}$, то $\mathrm{X}^{\text{И}} \equiv \text{Л}^{\text{И}} \equiv \text{Л} \equiv \mathrm{X}$. Таким образом $\mathrm{X}^{\text{И}} \equiv \mathrm{X}$.

Аналогично рассмотрим $\mathrm{X}^{\text{Л}}$. Если $\mathrm{X} \equiv \text{И}$, то $\mathrm{X}^{\text{Л}} \equiv \text{И}^{\text{Л}} \equiv \text{Л} \equiv \overline{\text{И}} \equiv \overline{\mathrm{X}}$. Если же $\mathrm{X} \equiv \text{Л}$, то $\mathrm{X}^{\text{Л}} \equiv \text{Л}^{\text{Л}} \equiv \text{И} \equiv \overline{\text{Л}} \equiv \overline{\mathrm{X}}$. Таким образом, $\mathrm{X}^{\text{Л}} \equiv \overline{\mathrm{X}}$, т.е. имеем следующие равносильности: $\mathrm{X}^\sigma \equiv \begin{cases} \mathrm{X}, \text{ если } \sigma \equiv \text{ И} \\ \overline{\mathrm{X}}, \text{ если } \sigma \equiv \text{Л} \end{cases}$.

Рассмотрим произвольный вектор $(\sigma_1, \sigma_2, \dots, \sigma_\mathrm{n})$, где σ_i есть либо И, либо Л. Тогда выражение $\mathrm{X}_1^{\sigma_1} \wedge \mathrm{X}_2^{\sigma_2} \wedge \dots \wedge \mathrm{X}_\mathrm{n}^{\sigma_\mathrm{n}}$ получается следующим образом. В конъюнкции $\mathrm{X}_1 \wedge \mathrm{X}_2 \wedge \dots \wedge \mathrm{X}_\mathrm{n}$ переменная $\mathrm{X_i}$, остается без изменения, если $\sigma_\mathrm{i} \equiv \text{И}$, и берется со знаком отрицания, если $\sigma_\mathrm{i} \equiv \text{Л}$. Например, если возьмем вектор $(\text{И}, \text{Л}, \text{Л}, \text{И}, \text{Л})$, то соответствующая конъюнкция будет иметь вид $\mathrm{X}_1 \wedge \overline{\mathrm{X}_2} \wedge \overline{\mathrm{X}_3} \wedge \mathrm{X}_4 \wedge \overline{\mathrm{X}_5}$.

Выражение $X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \dots \wedge X_n^{\sigma_n}$ есть элементарное произведение, для которого выполняются следующие условия: каждая переменная присутствует либо сама, либо со знаком отрицания; не имеется двух одинаковых переменных; ни одна переменная не присутствует вместе со своим отрицанием. Таким образом, любая с.д.н.ф. имеет вид:

$$\bigvee_{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\Omega} X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \dots \wedge X_n^{\sigma_n},$$

где Ω — некоторый набор векторов $(\sigma_1, \sigma_2, \dots, \sigma_n)$ с σ_i равным либо И, либо Л.

Теперь докажем единственность с.д.н.ф. для данной формулы $\mathcal{A}(X_1, \dots, X_n)$. Приведем эту формулу к некоторой с.д.н.ф. Как уже отмечалось, с.д.н.ф. имеет вид:

$$\bigvee_{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\Omega} X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \dots \wedge X_n^{\sigma_n}$$

Пусть $(\tau_1, \tau_2, \dots, \tau_n)$ — произвольный набор значений переменных, где τ_i равно И или Л, и пусть $\mathcal{A}(\tau_1, \tau_2, \dots, \tau_n)\equiv$И. Значит дизъюнкция

$$\bigvee_{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\Omega} X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \dots \wedge X_n^{\sigma_n}$$

при этих значениях переменных принимает значение И. Следовательно, одно из слагаемых $X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \dots \wedge X_n^{\sigma_n}$ при этих значениях переменных принимает значение И, т.е. $\tau_1^{\sigma_1} \wedge \tau_2^{\sigma_2} \wedge \dots \wedge \tau_n^{\sigma_n}\equiv$И. Это возможно лишь в случае, когда $\tau_i = \sigma_i$, где $i = 1, \dots, n$. Итак, для каждого набора значений переменных $(\tau_1, \tau_2, \dots, \tau_n)$, для которого $\mathcal{A}(\tau_1, \tau_2, \dots, \tau_n)\equiv$И, в с.д.н.ф. существует слагаемое вида $X_1^{\tau_1} \wedge X_2^{\tau_2} \wedge \dots \wedge X_n^{\tau_n}$, причем одно, по определению с.д.н.ф.

Обратно, пусть в с.д.н.ф. имеется некоторое слагаемое $X_1^{\tau_1} \wedge X_2^{\tau_2} \wedge \dots \wedge X_n^{\tau_n}$. Поскольку $\tau_1^{\tau_1} \wedge \tau_2^{\tau_2} \wedge \dots \wedge \tau_n^{\tau_n}\equiv$И, то $\mathcal{A}(\tau_1, \tau_2, \dots, \tau_n)\equiv$И. Очевидно, что любое другое слагаемое с.д.н.ф., отличное от $X_1^{\tau_1} \wedge X_2^{\tau_2} \wedge \dots \wedge X_n^{\tau_n}$, будет принимать значение Л при $X_i = \tau_i$, где $i = 1, \dots, n$.

Таким образом, получили, что каждое слагаемое в с.д.н.ф. однозначно определяется набором $(\tau_1, \tau_2, \dots, \tau_n)$ значений переменных, для которого $\mathcal{A}(\tau_1, \tau_2, \dots, \tau_n)\equiv$И. То есть с.д.н.ф. для формулы $\mathcal{A}(X_1, \dots, X_n)$ имеет вид:

$$\bigvee_{\mathcal{A}(\tau_1,\tau_2,\dots,\tau_n)\equiv И} X_1^{\tau_1} \wedge X_2^{\tau_2} \wedge \dots \wedge X_n^{\tau_n}$$

Понятно, что этот вид не зависит от способа приведения формулы $\mathcal{A}(X_1, \dots, X_n)$ к с.д.н.ф., а однозначно определяется самой формулой $\mathcal{A}(X_1, \dots, X_n)$.

Доказательство этой теоремы дает следующий алгоритм нахождения с.д.н.ф. для формулы $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_\mathrm{n})$:

1. Строим таблицу истинности для формулы $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_\mathrm{n})$.

2. Для любого набора значений переменных $(\tau_1, \tau_2, \dots, \tau_\mathrm{n})$, для которого $\mathcal{A}(\tau_1, \tau_2, \dots, \tau_\mathrm{n}) \equiv$И, строим элементарное произведение $\mathrm{X}_1^{\tau_1} \wedge \mathrm{X}_2^{\tau_2} \wedge \dots \wedge \mathrm{X}_\mathrm{n}^{\tau_\mathrm{n}}$.

3. Дизъюнкция построенных элементарных произведений и будет искомой с.д.н.ф.

Пример 1. Найти с.д.н.ф. для формулы

$\mathcal{A}(\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3) = \big((\mathrm{X}_1 \sim \mathrm{X}_2) \to (\mathrm{X}_1 \wedge \mathrm{X}_2)\big) \wedge (\mathrm{X}_3 \to \mathrm{X}_1)$.

Строим таблицу истинности для формулы $\mathcal{A}$:

X_1	X_2	X_3	$(\mathrm{X}_1 \sim \mathrm{X}_2)$	$(\mathrm{X}_1 \wedge \mathrm{X}_2)$	$(\mathrm{X}_1 \sim \mathrm{X}_2) \to (\mathrm{X}_1 \wedge \mathrm{X}_2)$	$(\mathrm{X}_3 \to \mathrm{X}_1)$	$\mathcal{A}$
Л	Л	Л	И	Л	Л	И	Л
Л	Л	И	И	Л	Л	Л	Л
Л	И	Л	Л	Л	И	И	И
Л	И	И	Л	Л	И	Л	Л
И	Л	Л	Л	Л	И	И	И
И	Л	И	Л	Л	И	И	И
И	И	Л	И	И	И	И	И
И	И	И	И	И	И	И	И

Для всех значений переменных, для которых $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_\mathrm{n}) \equiv$И, строим конъюнкции вида $\mathrm{X}_1^{\text{Л}} \wedge \mathrm{X}_2^{\text{И}} \wedge \mathrm{X}_3^{\text{Л}}$, $\mathrm{X}_1^{\text{И}} \wedge \mathrm{X}_2^{\text{Л}} \wedge \mathrm{X}_3^{\text{Л}}$, $\mathrm{X}_1^{\text{И}} \wedge \mathrm{X}_2^{\text{Л}} \wedge \mathrm{X}_3^{\text{И}}$, $\mathrm{X}_1^{\text{И}} \wedge \mathrm{X}_2^{\text{И}} \wedge \mathrm{X}_3^{\text{Л}}$ и $\mathrm{X}_1^{\text{И}} \wedge \mathrm{X}_2^{\text{И}} \wedge \mathrm{X}_3^{\text{И}}$.

По определению, это будут следующие элементарные произведения, соответственно: $\overline{\mathrm{X}_1} \wedge \mathrm{X}_2 \wedge \overline{\mathrm{X}_3}$, $\mathrm{X}_1 \wedge \overline{\mathrm{X}_2} \wedge \overline{\mathrm{X}_3}$, $\mathrm{X}_1 \wedge \overline{\mathrm{X}_2} \wedge \mathrm{X}_3$, $\mathrm{X}_1 \wedge \mathrm{X}_2 \wedge \overline{\mathrm{X}_3}$ и $\mathrm{X}_1 \wedge \mathrm{X}_2 \wedge \mathrm{X}_3$. Тогда искомая с.д.н.ф. имеет вид $(\overline{\mathrm{X}_1} \wedge \mathrm{X}_2 \wedge \overline{\mathrm{X}_3}) \vee (\mathrm{X}_1 \wedge \overline{\mathrm{X}_2} \wedge \overline{\mathrm{X}_3}) \vee$ $\vee (\mathrm{X}_1 \wedge \overline{\mathrm{X}_2} \wedge \mathrm{X}_3) \vee (\mathrm{X}_1 \wedge \mathrm{X}_2 \wedge \overline{\mathrm{X}_3}) \vee (\mathrm{X}_1 \wedge \mathrm{X}_2 \wedge \mathrm{X}_3)$.

Отметим, что обычно при записи с.д.н.ф. (а также д.н.ф.) знаки конъюнкции опускают и пишут обычное произведение. В дальнейшем мы также будем опускать знак конъюнкции. Так что вышеуказанная с.д.н.ф. будет иметь вид $\overline{X_1}X_2\overline{X_3} \vee X_1\overline{X_2X_3} \vee X_1\overline{X_2}X_3 \vee X_1X_2\overline{X_3} \vee X_1X_2X_3$.

В доказанной выше теореме 1 исключены из рассмотрения тождественно ложные формулы. Дело в том, что тождественно ложная формула не может иметь с.д.н.ф.

Действительно, пусть

$$\bigvee_{(\sigma_1,\sigma_2,\ldots,\sigma_n)\in\Omega} X_1^{\sigma_1}X_2^{\sigma_2}\ldots X_n^{\sigma_n}$$

тождественно ложна. Тогда по определению дизъюнкции тождественно ложно каждое слагаемое $X_1^{\sigma_1}X_2^{\sigma_2}\ldots X_n^{\sigma_n}$. Согласно теореме 1 предыдущего параграфа, в этом случае каждое такое слагаемое содержит хотя бы одну переменную вместе со своим отрицанием, что противоречит определению с.д.н.ф.

Теорема 2. Каждая не тождественно истинная формула $\mathcal{A}(X_1,\ldots,X_n)$ алгебры высказываний обладает единственной с.к.н.ф., основанной на нахождении с.д.н.ф.

Доказательство. Доказательство этой теоремы можно провести по аналогии с доказательством теоремы 1. Докажем ее несколько иным способом, который дает алгоритм нахождения с.к.н.ф.

Как мы определяли, $X^\sigma \equiv X$, если $\sigma \equiv$ И и $X^\sigma \equiv \overline{X}$, если $\sigma \equiv$ Л. В таком случае, $\overline{X^\sigma} \equiv \overline{X}$ если $\sigma \equiv$ И и $\overline{X^\sigma} \equiv X$ если $\sigma \equiv$ Л. Но это то же самое, что $X^{\overline{\sigma}}$, т.е. $\overline{X^\sigma} \equiv X^{\overline{\sigma}}$.

Пусть дана некоторая с.д.н.ф.

$$\bigvee_{(\sigma_1,\sigma_2,\ldots,\sigma_n)\in\Omega} X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \ldots \wedge X_n^{\sigma_n}$$

Заменим в этой с.д.н.ф. все дизъюнкции на конъюнкции, конъюнкции — на дизъюнкции, а σ_i на $\overline{\sigma_i}$. Легко видеть, что получим некоторую с.к.н.ф.

$$\bigwedge_{(\sigma_1,\sigma_2,\ldots,\sigma_n)\in\Omega} X_1^{\overline{\sigma_1}} \vee X_2^{\overline{\sigma_2}} \vee \ldots \vee X_n^{\overline{\sigma_n}}$$

Но эта с.к.н.ф. является не чем иным, как отрицанием заданной с.д.н.ф.

В самом деле, по законам Моргана:

$$\overline{\bigvee_{(\sigma_1,\sigma_2,\ldots,\sigma_n)\in\Omega} \left(X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \ldots \wedge X_n^{\sigma_n}\right)} \equiv \bigwedge_{(\sigma_1,\sigma_2,\ldots,\sigma_n)\in\Omega} \overline{\left(X_1^{\sigma_1} \wedge X_2^{\sigma_2} \wedge \ldots \wedge X_n^{\sigma_n}\right)} \equiv$$

$$\equiv \bigwedge_{(\sigma_1,\sigma_2,\ldots,\sigma_n)\in\Omega} \left(\overline{X_1^{\sigma_1}} \vee \overline{X_2^{\sigma_2}} \vee \ldots \vee \overline{X_n^{\sigma_n}}\right) \equiv \bigwedge_{(\sigma_1,\sigma_2,\ldots,\sigma_n)\in\Omega} \left(X_1^{\overline{\sigma_1}} \vee X_2^{\overline{\sigma_2}} \vee \ldots \vee X_n^{\overline{\sigma_n}}\right).$$

Таким образом, получим следующий алгоритм нахождения с.к.н.ф. для формулы $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_n)$:

1. По теореме 1 ищем с.д.н.ф. для формулы $\overline{\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_n)}$:

$$\bigvee_{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\Omega} \left(\mathrm{X}_1^{\sigma_1} \wedge \mathrm{X}_2^{\sigma_2} \wedge \dots \wedge \mathrm{X}_n^{\sigma_n}\right)$$

2. В найденной с.д.н.ф. производим замены: $\vee$ на $\wedge$, а $\wedge$ на $\vee$ и σ_i на $\overline{\sigma_i}$. Полученная формула и будет с.к.н.ф. для $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_n)$.

Отсюда видно, что с.к.н.ф. для формулы $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_n)$ определяется единственным образом. В самом деле, если формула $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_n)$ имеет две различных с.к.н.ф., то произведя в них замены ($\vee$ на $\wedge$, а $\wedge$ на $\vee$ и σ_i на $\overline{\sigma_i}$), получим две различных с.д.н.ф. для формулы $\mathcal{A}(\mathrm{X}_1, \dots, \mathrm{X}_n)$, что противоречит теореме 1. Кроме того, этот алгоритм показывает, почему тождественно истинная формула $\mathcal{A}$ не может иметь с.к.н.ф. Действительно, если бы такая с.к.н.ф. существовала, то, проведя в ней вышеуказанные замены, получили бы с.д.н.ф. для тождественно ложной формулы $\bar{\mathcal{A}}$, чего быть не может.

Пример 2. Найти с.к.н.ф. для формулы из примера 1.

Используя таблицу истинности для формулы $\mathcal{A}(\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3)$, получим следующую таблицу истинности для формулы $\overline{\mathcal{A}(\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3)}$:

X_1	X_2	X_3	$\overline{\mathcal{A}(\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3)}$
Л	Л	Л	И
Л	Л	И	И
Л	И	Л	Л
Л	И	И	И
И	Л	Л	Л
И	Л	И	Л
И	И	Л	Л
И	И	И	Л

Тогда с.д.н.ф. для формулы $\overline{\mathcal{A}(\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3)}$ будет иметь следующий вид: $(\overline{\mathrm{X}_1} \wedge \overline{\mathrm{X}_2} \wedge \overline{\mathrm{X}_3}) \vee (\overline{\mathrm{X}_1} \wedge \overline{\mathrm{X}_2} \wedge \mathrm{X}_3) \vee (\overline{\mathrm{X}_1} \wedge \mathrm{X}_2 \wedge \mathrm{X}_3)$.

Проведя вышеуказанные замены, получим следующую с.к.н.ф.:
$(\mathrm{X}_1 \vee \mathrm{X}_2 \vee \mathrm{X}_3) \wedge (\mathrm{X}_1 \vee \mathrm{X}_2 \vee \overline{\mathrm{X}_3}) \wedge (\mathrm{X}_1 \vee \overline{\mathrm{X}_2} \vee \overline{\mathrm{X}_3})$.

§ 2.6. Булевы функции и формулы алгебры высказываний

Напомним, что булевой функцией $f(x_1, \dots, x_n)$ от n переменных называется функция, отображающая n-ю степень множества $\{0,1\}$ во множество $\{0,1\}$, т.е. функция отображающая множество A_n во множество $\{0,1\}$.

Пусть $\mathcal{A}(X_1, \dots, X_n)$ — некоторая формула алгебры высказываний. Для любого вектора $(\sigma_1, \sigma_2, \dots, \sigma_n)$, где σ_i принимает значения И или Л, формула $\mathcal{A}(X_1, \dots, X_n)$ принимает значения И или Л. Другими словами, формула $\mathcal{A}(X_1, \dots, X_n)$ определяет некоторую функцию, отображающую n-ю степень множества $\{И, Л\}$ во множество $\{И, Л\}$. Если мы сопоставим истинному значению И единицу, а ложному значению Л сопоставим ноль, то тем самым формула $\mathcal{A}(X_1, \dots, X_n)$ определит некоторую булеву функцию от n переменных. Таким образом, любую формулу $\mathcal{A}(X_1, \dots, X_n)$ алгебры высказываний можно рассматривать как булеву функцию от n переменных при отождествлении $И \equiv 1$ и $Л \equiv 0$.

Пример 1. Рассмотрим формулу $\big(X_1 \to (X_1 \vee X_2)\big) \sim (\overline{X_2} \to X_1)$

Составим таблицу истинности для этой формулы:

X_1	X_2	$X_1 \vee X_2$	$X_1 \to (X_1 \vee X_2)$	$\overline{X_2} \to X_1$	$\mathcal{A}(X_1, X_2)$
Л	Л	Л	И	Л	Л
Л	И	И	И	И	И
И	Л	И	И	И	И
И	И	И	И	И	И

Проведя отождествление $И \equiv 1$ и $Л \equiv 0$, получим функцию $f(x_1, x_2)$, которая задается следующей таблицей:

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	1

Эту таблицу надо понимать так:
$f(0,0) = 0$, и $f(0,1) = f(1,0) = f(1,1) = 1$.

Естественно, возникает вопрос: можно ли любую булеву функцию рассматривать как формулу алгебры высказываний при отождествлении $1 \equiv$ И и $0 \equiv$ Л?

Пример 2. Запишем в виде таблицы все булевы функции от двух переменных (16 функций):

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Проанализировав эту таблицу (при отождествлении $0 \equiv$ Л и $1 \equiv$ И), получим следующее:

$f_7(x_1, x_2) = x_1 \vee x_2$; $f_1(x_1, x_2) = x_1 \wedge x_2$;

$f_{13}(x_1, x_2) = x_1 \rightarrow x_2$; $f_9(x_1, x_2) = x_1 \sim x_2$.

Таким образом, функции f_7, f_1, f_{13}, и f_9 реализуются в виде формул алгебры высказываний. Ответ на вопрос о реализации остальных функций из этой таблицы, а также о реализации любой булевой функции в виде формулы алгебры высказываний дает следующая теорема.

Теорема 1. Пусть $f(x_1, \dots, x_n)$ — булева функция. Тогда формула

$$\bigvee_{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\Omega} f(\sigma_1, \sigma_2, \dots, \sigma_n) X_1^{\sigma_1} X_2^{\sigma_2} \dots X_n^{\sigma_n} = \mathcal{A}(X_1, \dots, X_n)$$

представляет данную функцию, т.е. если для вектора $(\tau_1, \tau_2, \dots, \tau_n) f(\tau_1, \tau_2, \dots, \tau_n) = 1$ (или 0), то соответствующее значение формулы $\mathcal{A}(\tau_1, \tau_2, \dots, \tau_n) =$ И (или Л) и наоборот. При этом 1 и И (0 и Л) отождествляются.

Доказательство. Доказательство непосредственно следует из доказательства теоремы 1. Оно основано на том, что конъюнкция $X_1^{\sigma_1} X_2^{\sigma_2} \dots X_n^{\sigma_n}$ принимает значение И только в случае, когда $X_i = \sigma_i$. Поэтому

$$\mathcal{A}(\tau_1, \tau_2, \dots, \tau_n) = \bigvee_{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\Omega} f(\sigma_1, \sigma_2, \dots, \sigma_n) \tau_1^{\sigma_1} \tau_2^{\sigma_2} \dots \tau_n^{\sigma_n} =$$

$$= f(\tau_1, \tau_2, \dots, \tau_n) \tau_1^{\sigma_1} \tau_2^{\sigma_2} \dots \tau_n^{\sigma_n} = f(\tau_1, \tau_2, \dots, \tau_n)$$

В этих равенствах, естественно, проведены отождествления $\text{И} \equiv 1$ и $\text{Л} \equiv 0$.

Таким образом, любая булева функция реализуется в виде формулы алгебры высказываний как некоторая с.д.н.ф.

Например, $f_9(x_1, x_2) = \overline{x_1}\,\overline{x_2} \vee x_1 x_2$ или $f_6(x_1, x_2) = \overline{x_1} x_2 \vee x_1 \overline{x_2}$.

Очевидно, что каждая формула алгебры высказываний представляет единственную булеву функцию. Естественно, равносильные формулы представляют одну и ту же булеву функцию. Поэтому каждая булева функция представляется не единственной формулой алгебры высказываний, но она однозначно определяет класс равносильных формул алгебры высказываний. Таким образом, между всеми булевыми функциями и классами равносильных формул существует биекция.

В дальнейшем, в зависимости от ситуации, мы будем булевы функции рассматривать либо как функции, либо как формулы алгебры высказываний. При этом не будем каждый раз говорить об отождествлений $1 \equiv$ И и $0 \equiv$ Л, а будем работать в основном с нулем и единицей.

§ 2.7. Решение логических задач с использованием алгебры высказываний

Здесь мы на трех задачах проиллюстрируем применение алгебры высказываний для решения логических задач.

Задача 1. Следователь одновременно допрашивал трех свидетелей: Клода, Жака и Дика. Их показания противоречили друг другу, и каждый из них обвинял во лжи кого-нибудь:

1) Клод утверждал, что Жак лжет;

2) Жак обвинял во лжи Дика;

3) Дик уговаривал следователя не верить ни Клоду, ни Жаку. Кто же говорил правду?

Решение. Обозначим через К, Ж и Д высказывания: «Клод (соответственно, Жак, Дик) говорит правду». Тогда $\overline{\text{К}}$, $\overline{\text{Ж}}$, и $\overline{\text{Д}}$ будут отвечать высказываниям: «Клод (соответственно, Жак, Дик) говорит неправду». В таком случае их показания приводят к следующим истинным формулам:

1) $(\text{К} \wedge \overline{\text{Ж}}) \vee (\overline{\text{К}} \wedge \text{Ж})$;

2) $(\text{Ж} \wedge \overline{\text{Д}}) \vee (\overline{\text{Ж}} \wedge \text{Д})$;

3) $(\text{Д} \wedge \overline{\text{К}} \wedge \overline{\text{Ж}}) \vee (\overline{\text{Д}} \wedge (\text{К} \vee \text{Ж}))$.

Приведя формулы 1) и 2) к к.н.ф., имеем:

$$(\text{К} \wedge \overline{\text{Ж}}) \vee (\overline{\text{К}} \wedge \text{Ж}) \equiv [(\text{К} \wedge \overline{\text{Ж}}) \vee \overline{\text{К}}] \wedge [(\text{К} \wedge \overline{\text{Ж}}) \vee \text{Ж}] \equiv$$
$$\equiv (\text{К} \vee \overline{\text{К}}) \wedge (\overline{\text{Ж}} \vee \overline{\text{К}}) \wedge (\text{К} \vee \text{Ж}) \wedge (\overline{\text{Ж}} \vee \text{Ж}) \equiv \text{И} \wedge (\overline{\text{Ж}} \vee \overline{\text{К}}) \wedge (\text{К} \vee \text{Ж}) \wedge \text{И} \equiv$$
$$\equiv (\overline{\text{Ж}} \vee \overline{\text{К}}) \wedge (\text{К} \vee \text{Ж}).$$

Аналогично $(Ж \wedge \overline{Д}) \vee (\overline{Ж} \wedge Д) \equiv (Ж \vee Д) \wedge (\overline{Ж} \vee \overline{Д})$. Так как формулы $(\overline{Ж} \vee \overline{К}) \wedge (К \vee Ж)$ и $(Ж \vee Д) \wedge (\overline{Ж} \vee \overline{Д})$ истинны, то истинна и их конъюнкция $(\overline{Ж} \vee \overline{К}) \wedge (К \vee Ж) \wedge (Ж \vee Д) \wedge (\overline{Ж} \vee \overline{Д})$. Конъюнкция истинна только в случае, когда каждый из множителей истинен.

а) Пусть $Ж = И$. Поскольку $(\overline{Ж} \vee \overline{К}) \equiv И$ и $\overline{Ж} \equiv Л$, то $К \equiv Л$. Аналогично $(\overline{Ж} \vee \overline{Д}) \equiv И$ и $\overline{Ж} \equiv Л$, поэтому $Д \equiv Л$. Итак, если $Ж \equiv И$, то $К \equiv Д \equiv Л$.

б) Пусть $Ж = Л$. Так как $(К \vee Ж) \equiv И$ и $Ж = Л$, то $К \equiv И$. Аналогично $(Ж \vee Д) \equiv И$ и $Ж = Л$, следует что $Д \equiv И$. Таким образом, если $Ж = Л$, $К \equiv Д \equiv И$. Но при этом формула 3) тоже должна быть истинной.

Случай а) для формулы $(Д \wedge \overline{К} \wedge \overline{Ж}) \vee (\overline{Д} \wedge (К \vee Ж))$ дает значение И, а случай б) дает значение Л. таким образом, правду говорил Жак, а Дик с Клодом лгали.

Задача 2. Пятеро студентов: A, B, C, D и E, проживающих в одной комнате в общежитии, купили в складчину телевизор. В первый же вечер, просмотрев программу телепередач, они заспорили, кто с кем и какую передачу будет смотреть. Их спор вылился в следующие пожелания:

1. Если студент A будет смотреть телевизор, то B будет делать то же самое;
2. Студенты D и E, оба или один из них, смотрят телевизор;
3. Из двух студентов B и C смотрит телевизор один и только один;
4. Студенты C и D либо оба смотрят, либо оба не смотрят телевизор;
5. Если студент E смотрит телевизор, то A и D делают то же самое.

Кто из студентов смотрел телевизор первый вечер?

Решение. Обозначим через A, B, C, D, E высказывания, означающие, что телевизор смотрели студент A, B, C, D, E соответственно. Тогда пожелания 1–5 запишутся в виде следующих истинных формул:

$$A \to B \equiv \overline{A} \vee B;$$
$$D \vee E;$$
$$(\overline{B} \wedge C) \vee (B \wedge \overline{C});$$
$$(C \wedge D) \vee (\overline{C} \wedge \overline{D});$$
$$E \to (A \wedge D) \equiv \overline{E} \vee (A \wedge D).$$

Поскольку все эти формулы истинны, то истинна их конъюнкция. Рассмотрим конъюнкцию формул 1), 2), 4) и 5) и преобразуем ее. Итак, имеем:

$$(\overline{A} \vee B) \wedge (D \vee E) \wedge [(C \wedge D) \vee (\overline{C} \wedge \overline{D})] \wedge [\overline{E} \vee (A \wedge D)] \equiv$$
$$\equiv (\overline{A} \vee B) \wedge (D \vee E) \wedge \left[\left(C \vee (\overline{C} \wedge \overline{D})\right) \wedge \left(D \vee (\overline{C} \wedge \overline{D})\right)\right] \wedge [(\overline{E} \vee A) \wedge (\overline{E} \vee D)] \equiv$$
$$\equiv (\overline{A} \vee B) \wedge (D \vee E) \wedge (C \vee \overline{D}) \wedge (D \vee \overline{C}) \wedge (\overline{E} \vee A) \wedge (\overline{E} \vee D) \equiv$$
$$\equiv (\overline{A} \vee B) \wedge \left(D \vee (E \wedge \overline{E})\right) \wedge (C \vee \overline{D}) \wedge (D \vee \overline{C}) \wedge (\overline{E} \vee A) \equiv$$
$$\equiv (\overline{A} \vee B) \wedge D \wedge (C \vee \overline{D}) \wedge (D \vee \overline{C}) \wedge (\overline{E} \vee A) \equiv$$
$$\equiv (\overline{A} \vee B) \wedge D \wedge (C \vee \overline{D}) \wedge (\overline{E} \vee A)$$

Поскольку эта конъюнкция истинна, то истинен каждый из множителей. В частности, $\mathrm{D} = \text{И}$. Так как $(\mathrm{C} \vee \overline{\mathrm{D}}) = \text{И}$ и $\overline{\mathrm{D}} = \text{Л}$, то $\mathrm{C} = \text{И}$. Утверждение 3 по условию также истинно, т.е. $(\overline{\mathrm{B}} \wedge \mathrm{C}) \vee (\mathrm{B} \wedge \overline{\mathrm{C}}) = \text{И}$. Поскольку $\mathrm{C} = \text{И}$, то отсюда получаем, что $\mathrm{B} = \text{Л}$. Так как $(\overline{\mathrm{A}} \vee \mathrm{B}) = \text{И}$ и $\mathrm{B} = \text{Л}$, то $\mathrm{A} = \text{Л}$. Наконец, $\mathrm{E} = \text{Л}$, потому что $(\overline{\mathrm{E}} \vee \mathrm{A}) = \text{И}$ и $\mathrm{A} = \text{Л}$. Таким образом, в первый вечер передачи смотрели студенты C и D.

Задача 3. Старосте студенческой группы задали вопрос: «Кто из студентов А, В или С сдаст экзамен по дискретной математике с первого захода?» Староста сделал такой прогноз: «Если А сдаст, то сдаст и С, но совершенно неверно, что за сдачей экзамена студентом В последует сдача экзамена студентом С». Прогноз оказался верным. Кто же сдал экзамен с первого захода?

Решение. Прогноз старосты можно записать в виде формулы $\mathrm{X} = (\mathrm{A} \to \mathrm{C}) \wedge \wedge \overline{(\mathrm{B} \to \mathrm{C})}$, где А, В, С означают высказывания: «А — сдал студент А (соответственно, В и С)». Построим для этой формулы таблицу истинности:

A	B	C	$(\mathrm{A} \to \mathrm{C})$	$\overline{(\mathrm{B} \to \mathrm{C})}$	X
0	0	0	1	0	0
0	0	1	1	0	0
0	1	0	1	1	1
0	1	1	1	0	0
1	0	0	0	0	0
1	0	1	1	0	0
1	1	0	0	1	0
1	1	1	1	0	0

Поскольку прогноз оказался истинным, то единственный вариант, дающий истину, есть $\mathrm{A} = 0$, $\mathrm{B} = 1$ и $\mathrm{C} = 0$, т.е. сдал экзамен студент В, а студенты А и С не сдали.

ГЛАВА 3. МИНИМИЗАЦИЯ БУЛЕВЫХ ФУНКЦИЙ

В этой главе будет рассмотрена задача нахождения минимальной д.н.ф. из всех д.н.ф., реализующих данную функцию $f(x_1, \dots, x_n)$.

§ 3.1. Геометрическая интерпретация дизъюнктивных нормальных форм

Определение 1. Пусть дана элементарная конъюнкция $K = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \ldots x_{i_r}^{\delta_r}$, где все x_{i_j} различны. Число r называется рангом конъюнкции. В случае $r = 0$ конъюнкция называется пустой и получается равной 1.

Определение 2. Пусть дана д.н.ф. $D = K_1 \vee K_2 \vee \ldots \vee K_m$, где все конъюнкции K_i различны между собой. Число m называется длиной д.н.ф. D. Если $m = 0$, то D называется пустой.

Определение 3. Минимальной д.н.ф. функции $f(x_1, \ldots, x_n)$ называется д.н.ф., реализующая $f(x_1, \ldots, x_n)$ и содержащая наименьшее число символов переменных по сравнению с другими д.н.ф., реализующими $f(x_1, \ldots, x_n)$.

Другими словами, д.н.ф. $D = K_1 \vee K_2 \vee \ldots \vee K_m$ называется минимальной д.н.ф. функции $f(x_1, \ldots, x_n)$, если она реализует функцию $f(x_1, \ldots, x_n)$ и число $r = r_1 + \ldots + r_m$ принимает наименьшее значение среди всех д.н.ф., реализующих функцию $f(x_1, \ldots, x_n)$. Будем обозначать минимальную д.н.ф. через м.д.н.ф.

Естественно, существует тривиальный алгоритм нахождения м.д.н.ф. для произвольной функции $f(x_1, \ldots, x_n)$. Для этого надо все д.н.ф., составленные из символов $x_1, \ldots, x_n$ и $\overline{x_1}, \ldots, \overline{x_n}$, упорядочить по числу символов. Затем по порядку для каждой д.н.ф. проверяется равносильность булевой функции, и в случае равносильности она и будет искомой м.д.н.ф. В принципе, м.д.н.ф. может быть несколько.

Уже при сравнительно небольших n этот метод приводит к перебору огромного числа д.н.ф. Некоторое представление о трудоёмкости данного метода даёт следующая теорема.

Теорема 1. Число различных д.н.ф., составленных из переменных $x_1, \ldots, x_n$, равно 2^{3^n}.

Доказательство.

Покажем сначала, что число различных конъюнкций, составленных из переменных $x_1, \ldots, x_n$, равно 3^n. Докажем это утверждение индукцией по n. Если $n = 1$, то из одной переменной x_1 можно составить 3^1 различных конъюнкций. Действительно, это будут конъюнкции 1, x_1 и $\bar{x}_1$. Пусть из $(n-1)$ переменных можно составить 3^{n-1} различных конъюнкций, тогда рассмотрим все конъюнкции от переменных $x_1, \ldots, x_n$.

Все эти конъюнкции можно получить следующим образом.

Пусть M — множество всех конъюнкций, составленных из переменных $x_1, \ldots, x_n$. По индуктивному предположению, $\left| M \right| = 3^{n-1}$. Если Mx_n и $M\bar{x}_n$ — два множества конъюнкций, полученных путём умножения каждой конъюнкции из M на x_n и на $\bar{x}_n$, то множество всех конъюнкций от переменных $x_1, \ldots, x_n$ будет равно $M \cup Mx_n \cup M\bar{x}_n$. В таком случае, мощность этого множества равна $3^{n-1} + 3^{n-1} + 3^{n-1} = 3^n$.

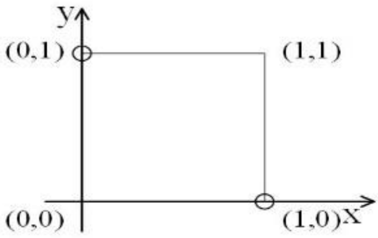
Итак, число всех конъюнкций, составленных из переменных $x_1, \ldots, x_n$, равно 3^n. Тогда общее число дизъюнкций, которые можно составить из данных конъюнкций, равно 2^{3^n}.

Для наглядности рассуждений будем использовать геометрическую модель. Множество всех точек $(\delta_1, \ldots, \delta_n)$, у которых $\delta_i \in \{0,1\}$, обозначим через E^n.

Другими словами, E^n — это множество всех вершин единичного n-мерного куба. Каждой функции $f(x_1, \ldots, x_n)$ ставим в соответствие её носитель $N_f \subseteq E^n$, т.е. множество всех таких вершин куба $(\delta_1, \ldots, \delta_n)$, что $f(\delta_1, \ldots, \delta_n) = 1$.

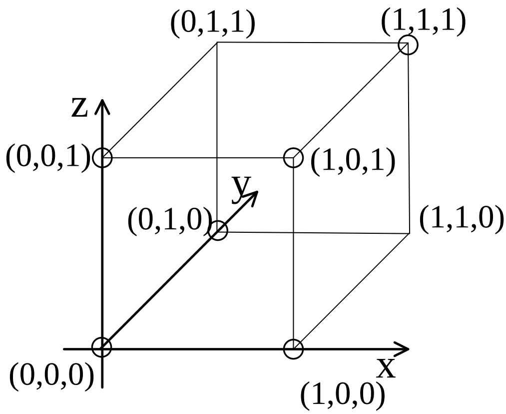
Пример 1. Рассмотрим функции $\varphi(x, y)$ и $f(x, y, z)$:

x	y	$\varphi(x,y)$
0	0	0
0	1	1
1	0	1
1	1	0



x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Тогда соответствующие вершины куба изобразятся следующим образом:



Данное соответствие является биекцией и обладает следующими свойствами. Пусть $f_1(x_1,\ldots,x_n)$ и $f_2(x_1,\ldots,x_n)$ — произвольные две функции. Тогда имеют место следующие соотношения:

1) функции f_1 соответствует подмножество $E^n \setminus N_{f_1}$;

2) функции $f_1 \wedge f_2$ соответствует подмножество $N_{f_1} \bigcap N_{f_2}$;

3) функции $f_1 \vee f_2$ соответствует подмножество $N_{f_1} U\ N_{f_2}$;

4) $f_1 \leq f_2 \Leftrightarrow N_{f_1} \leq\ N_{f_2}$;

Доказательство этих свойств очевидно по определению.

Определение 4. Подмножество $N_K \subseteq E^n$ называется интервалом ранга r, если оно соответствует элементарной конъюнкции K ранга r.

Пусть $K =\ x_{i_1}^{\delta_1}\, x_{i_2}^{\delta_2} \ldots x_{i_r}^{\delta_r}$, и пусть N_K — интервал соответствующий этой конъюнкции. Очевидно, что N_K состоит из всех вершин $(x_1,\ldots,x_n)$ куба E^n, у которых координаты $x_{i_1},\ldots,x_{i_n}$ равны, соответственно, $\delta_1,\ldots,\delta_n$, а значения остальных координат произвольны. Таким образом, каждая вершина куба E^n есть интервал ранга n, множество всех вершин куба — это интервал нулевого ранга. Интервал ранга r представляет собой геометрически некоторое подмножество вершин куба E^n, заполняющих его $(n-r)$ −мерную грань.

Теорема 2. Для каждой д.н.ф. $K_1 \vee K_2 \vee\ldots\vee K_m$ функции $f(x_1,\ldots,x_n)$ справедливо равенство $N_f = \bigcup_{i=1}^{m} N_{K_i}$. Обратно, для любого набора интервалов $N_{K_1}, \dots, N_{K_m}$, удовлетворяющих свойству $N_f = \bigcup_{i=1}^{m} N_{K_i}$, д.н.ф. $K_1 \vee K_2 \vee \ldots \vee K_m$ реализует функцию $f(x_1, \dots, x_n)$.

Доказательство. Пусть д.н.ф. $K_1 \vee K_2 \vee \ldots \vee K_m$ реализует функцию $f(x_1, \dots, x_n)$, и покажем, что $N_f = \bigcup_{i=1}^{m} N_{K_i}$. Если $f(\delta_1, \dots, \delta_n) \in N_f$, то $f(\delta_1, \dots, \delta_n) = 1$. Т.к. дизъюнкция принимает значение 1, когда хотя бы одно из слагаемых принимает значение 1 , то существует индекс j такой, что $K_j(\delta_1, \dots, \delta_n) = 1$. Но тогда $(\delta_1, \dots, \delta_n) \in N_{K_j}$, значит, $(\delta_1, \dots, \delta_n) = \bigcup_{i=1}^{m} N_{K_i}$.

Обратно, если $(\delta_1, \dots, \delta_n) = \bigcup_{i=1}^{m} N_{K_i}$, то существует j такой, что $(\delta_1, \dots, \delta_n) \in N_{K_j}$, а значит $K_j(\delta_1, \dots, \delta_n) = 1$. Но тогда при этом наборе $(\delta_1, \dots, \delta_n)$ д.н.ф. $K_1 \vee K_2 \vee \ldots \vee K_m$ принимает значение 1, и следовательно, $f(\delta_1, \dots, \delta_n) = 1$, т.е. $(\delta_1, \dots, \delta_n) \in N_f$.

Пусть $N_f = \bigcup_{i=1}^{m} N_{k_i,}$ и рассмотрим $D = K_1 \vee K_2 \vee \ldots \vee K_m$. Покажем, что данная д.н.ф. D реализует функцию f, т.е. для любого набора $(\delta_1, \dots, \delta_n)$ из $f(\delta_1, \dots, \delta_n) = 1$ и наоборот. Если $f(\delta_1, \dots, \delta_n) = 1$, то $(\delta_1, \dots, \delta_n) \in N_f$, а значит, если имеет место равенство $N_f = \bigcup_{i=1}^{m} N_{K_i}$, то $(\delta_1, \dots, \delta_n) \in K_j$ для некоторого j. В таком случае $K_j(\delta_1, \dots, \delta_n) = 1$, а значит, и $D(\delta_1, \dots, \delta_n) = 1$. Аналогично показывается, что если $D(\delta_1, \dots, \delta_n) = 1$, то и $f(\delta_1, \dots, \delta_n) = 1$.

Определение 5. Совокупность интервалов $N_{K_1}, \dots, N_{K_m} \subset N_f$ таких, что $N_f = \bigcup_{i=1}^{m} N_{K_i}$, называется покрытием множества N_f.

Итак, согласно теореме 2, каждой д.н.ф. для функции f соответствует некоторое покрытие множества N_f, и наоборот, любое покрытие множества N_f определяет д.н.ф. для функции f. Если r_i — ранг интервала N_{K_i}, то сумма $r = \sum_{i=1}^{m} r_i$ совпадает с числом букв в д.н.ф. Значит, задача построения м.д.н.ф. сводится к отысканию такого покрытия множества N_f интервалами $N_{K_1}, \dots, N_{K_m}$, что сумма $\sum_{i=1}^{m} r_i$ принимает минимальное значение.

Тогда при отыскании м.д.н.ф. естественно рассматривать только такие конъюнкции K, для которых $N_K \subseteq N_f$.

Определение 6. Интервал N_k и соответствующая ему конъюнкция K называется допустимыми, если $N_k \subseteq N_f$, т.е. $N_k \cap \left(E^n \backslash N_f\right) = \emptyset$.

Значит, можно повысить эффективность тривиального алгоритма следующим образом. Выделим только допустимые конъюнкции для функции $f(x_1, \dots, x_n)$ и уже к ним применим тривиальный алгоритм. Насколько этим повышается эффективность тривиального алгоритма, можно судить по следующему примеру.

Пример 2. Рассмотрим функцию $f(x, y, z)$ из примера 1. Как мы уже отмечали, для функций от трех переменных существует $3^3 = 27$ различных конъюнкций, из которых можно составить 2^{27}возможных д.н.ф. То есть тривиальный алгоритм поиска м.д.н.ф. мы должны применять к 2^{27} различным д.н.ф. Найдём для нашей функции допустимые конъюнкции и посмотрим, до какого количества снизится общее число д.н.ф., подлежащих рассмотрению. Для каждого найденного варианта всех допустимых конъюнкций удобно составить следующую таблицу:

Точки множества $E^n \backslash N_f$	**Конъюнкции, обращающиеся в единицу в точках множества $E^n \backslash N_f$**
(0,1,1)	1; $\bar{x}$, y, z; $\bar{x}y$, $\bar{x}z$, yz; $\bar{x}yz$;
(1,0,0)	1; x, $\bar{y}$, $\bar{z}$; $x\bar{y}$, $x\bar{z}$, $\bar{y}\bar{z}$, $x\bar{y}\bar{z}$;
(1,1,0)	1; x, y, $\bar{z}$; xy, $x\bar{z}$, $y\bar{z}$; $xy\bar{z}$;

Все конъюнкции, указанные в таблице, не являются допустимыми. Значит, допустимыми будут оставшиеся 9 конъюнкций, а именно: $\bar{x}\bar{y}\bar{z}$, $\bar{x}\bar{y}z$, $\bar{x}y\bar{z}$, $x\bar{y}z$, xyz, $\bar{x}\bar{y}$, $\bar{x}\bar{z}$, xz, $\bar{y}z$. Из этих девяти конъюнкций можно построить 2^9 различных д.н.ф. (что значительно меньше, чем 2^{27}), которые и подлежат рассмотрению.

§ 3.2. Сокращенные дизъюнктивные нормальные формы

Итак, в предыдущем параграфе мы выяснили, что важную роль при нахождении д.н.ф. для функции $f(x_1, \ldots, x_n)$ играют допустимые интервалы $N_k \subseteq N_f$, а также покрытия N_f допустимыми интервалами. Следующая простая теорема даёт очень важные свойства интервалов.

Теорема 1.

Для интервалов N_K и $N_{K'}$ следующие условия эквивалентны:

(1) $N_K \subset N_{K'}$;

(2) $K > K'$;

(3) Конъюнкция K' получается из конъюнкции K путём удаления из неё некоторого непустого множества сомножителей.

Доказательство: Собственно говоря, эквивалентность условий (1) и (2) отмечена выше. Поэтому докажем эквивалентность условий (1) и (3).

Итак, пусть $N_K \subset N_{K'}$, $K = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \ldots x_{i_r}^{\delta_r}$ и предположим, что конъюнкция K' содержит x_i^{δ}, где $i \neq i_1, \ldots, i \neq i_r$. Если вектор $(\tau_1, \ldots, \tau_n) \in N_K$, то $\tau_{i_j} = \delta_j$, $j = 1, \ldots, r$, а остальные значения координат произвольны. Возьмём вектор $(\tau_1, \ldots, \tau_n)$, у которого $\tau_{i_j} = \delta_j$, где $j = 1, \ldots, r$, тогда $\tau_i = \bar{\delta}$, а остальные координаты произвольны. В таком случае $K(\tau_1, \ldots, \tau_n) = 1$, поэтому $(\tau_1, \ldots, \tau_n) \in N_K$, а значит, $(\tau_1, \ldots, \tau_n) \in N_{K'}$. Таким образом,

$K'(\tau_1, \dots, \tau_n) = 1$, что невозможно, т.к. $\tau_i^\delta = \bar{\delta}^\delta = 0$, а значит, и $K'(\tau_1, \dots, \tau_n) = 0$, поскольку x_i^δ входит в K' является множителем в K.

Т.к. $K' \neq K$, то это и означает, что K' получена из K путем удаления непустого множества множителей.

Обратно, пусть конъюнкции K и K' удовлетворяют условию (3). Это значит, что их можно представить в виде $K' = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \dots x_{i_r}^{\delta_r}$ и $K = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \dots x_{i_r}^{\delta_r} x_{i_{r+1}}^{\tau_{r+1}} \dots x_{i_m}^{\tau_m}$, где $m > r$. Отсюда очевидно, что если $K(\tau_1, \dots, \tau_n) = 1$, то и $K'(\tau_1, \dots, \tau_n) = 1$, т.е. $N_K \subset N_{K'}$. Т.к. $m > r$, то включение строгое.

Определение 1. Интервал N_K называется максимальным для функции $f(x_1, \dots, x_n)$, если не существует интервала $N_{K'}$ такого, что $N_K \subset N_{K'} \subseteq N_f$.

Другими словами, интервал N_K является максимальным, если для любой конъюнкции K', полученной из K удалением хотя бы одного множителя, интервал $N_{K'}$ не является допустимым, т.е. $N_{K'} \nsubseteq N_f$.

Пусть $\{N_{K_i}\}$ $j = 1, \dots, m$ — совокупность всех максимальных интервалов для функции f. Ясно, что эта совокупность однозначно определяется самой функцией f. Тогда $N_f = \bigcup_{j=1}^{m} N_{K_j}$. Это следует из того, что, во–первых, $N_{K_j} \subseteq N_f$, $j = 1, \dots\ m$, а во-вторых, любой допустимый интервал N_K входит в некоторый максимальный N_{K_j}. Итак, любая функция f обладает покрытием $N_f = \bigcup_{j=1}^{m} N_{K_j}$, в котором все интервалы N_{K_j} максимальны.

Определение 2. Д.н.ф. $\bigvee_{j=1}^{m} K_j$, реализующая функцию $f(x_1, \dots, x_n)$ и соответствующая покрытию множества N_f всеми максимальными для f интервалами, называется сокращённой д.н.ф. для функции f. Будем её обозначать через $D_c(f)$.

Из определения $D_c(f)$ и однозначности совокупности всех максимальных для f интервалов следует, что сокращённая д.н.ф. определяется для функции f однозначно. Следующая теорема говорит о важности сокращённых д.н.ф.

Теорема 2.

Минимальная д.н.ф. для функции $f(x_1, \dots, x_n)$ получается из сокращённой д.н.ф. функции $f(x_1, \dots, x_n)$ путём удаления некоторых элементарных конъюнкций.

Доказательство.

Пусть $K_1 \vee K_2 \vee \dots \vee K_m$ — некоторая м.д.н.ф. функции $f(x_1, \dots, x_n)$ и $N_f = \bigcup_{j=1}^{m} N_{K_j}$ — соответствующее ей покрытие. Теорема будет доказана, если мы покажем, что каждый интервал N_{K_j} является максимальным для f. Предположим противное: пусть, например, N_{K_1} не максимальный интервал.

Тогда он содержится в некотором максимальном $N_{K'}$, причем ранг r' конъюнкций K' строго меньше ранга r_1. Т.к. $N_f = N_{K'} \cup \left(\bigcup_{j=2}^{m} N_{K_j}\right)$, то соответствующая этому покрытию д.н.ф. $K' \vee K_2 \vee \ldots \vee K_m$ будет иметь ранг $r' + r_2 + \cdots + r_m$, который строго меньше, чем $r_1 + r_2 + \cdots + r_m$. Это противоречит минимальности д.н.ф. $K_1 \vee K_2 \vee \ldots \vee K_m$.

Следствие. Если конъюнкция K не является слагаемым сокращённой д.н.ф. для функции f, то она не входит в качестве слагаемого ни в одну из м.д.н.ф.

Пример 1. Рассмотрим всё ту же функцию из примера 1 предыдущего параграфа. Как было получено в примере 2, для функции $f(x, y, z)$ допустимыми являются конъюнкции $\bar{x}\bar{y}\bar{z}$, $\bar{x}\bar{y}z$, $\bar{x}y\bar{z}$, $x\bar{y}z$, xyz, $\bar{x}\bar{y}$, $\bar{x}\bar{z}$, xz, $\bar{y}z$. Если в конъюнкции $\bar{x}\bar{y}\bar{z}$ удалим $\bar{z}$, то получим снова допустимую конъюнкцию $\bar{x}\bar{y}$. Следовательно, $N_{\bar{x}\bar{y}\bar{z}}$ не является максимальным интервалом, т.к. $N_{\bar{x}\bar{y}\bar{z}} \subset N_{\bar{x}\bar{y}}$. Аналогично интервалы, соответствующие конъюнкциям $\bar{x}\bar{y}z$, $\bar{x}y\bar{z}$, $x\bar{y}z$, xyz, не являются максимальными. В то же время интервалы, соответствующие конъюнкциям $\bar{x}\bar{y}$, $\bar{x}\bar{z}$, xz, $\bar{y}z$, будут максимальными, поскольку удаление хотя бы одного символа в каждой из них приводит к недопустимым конъюнкциям. Итак, $D_c(f) = \bar{x}\bar{y} \vee \bar{x}\bar{z} \vee xz \vee \bar{y}z$. Применение тривиального алгоритма к $D_c(f)$ ещё более сокращает объём работы. Осталось у выражения $D_c(f)$ убирать по одному (по два, по три) слагаемому и каждый раз проверять полученную д.н.ф. на совпадение с функцией $f(x, y, z)$. Например, удалим из $D_c(f)$ конъюнкцию $\bar{x}\bar{z}$ или xz и сравним с функцией $f(x, y, z)$:

x	y	z	$f(x, y, z)$	$\bar{x}\bar{y} \vee xz \vee \bar{y}z$	$\bar{x}\bar{y} \vee \bar{x}\bar{z} \vee \bar{y}z$
0	0	0	1	1	1
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	0	0	0
1	0	0	0	0	0
1	0	1	1	1	1
1	1	0	0	0	0
1	1	1	1	1	0

Как видим из вышеприведенной таблицы, $f(x, y, z) \neq \bar{x}\bar{y} \vee xz \vee \bar{y}z$ и $f(x, y, z) \neq \bar{x}\bar{y} \vee \bar{x}\bar{z} \vee \bar{y}z$. Это говорит о том, что конъюнкции $\bar{x}\bar{z}$ и xz обязательно должны присутствовать в м.д.н.ф. После этого легко проверить, что дизъюнкции $\bar{x}\bar{z} \vee xz \vee \bar{x}\bar{y}$ и $\bar{x}\bar{z} \vee xz \vee \bar{y}z$ будут являться минимальными д.н.ф. для функции $f(x, y, z)$.

Из этого из этого примера видно, что минимальная д.н.ф. не обязана совпадать с сокращённой д.н.ф. Но для некоторых классов функций такое совпадение есть.

Теорема 3.

Если функция $f(x_1, \dots, x_n)$ монотонна, то её сокращённая д.н.ф. не содержит отрицаний переменных и является единственной её м.д.н.ф.

Доказательство.

Докажем, что сокращённая д.н.ф. не содержит отрицаний. Пусть $N_K \subseteq N_f$ является максимальным интервалом, и пусть $K = x_{i_1} \dots x_{i_r}\bar{x}_{i_{r+1}} \dots \bar{x}_{i_t}$, причем $t > r$. Тогда конъюнкция K, а вместе с ней и функция f, обращается в 1 во всех вершинах куба E^n, для которых $x_{i_1} = \dots = x_{i_r} = 1$ и $x_{i_{r+1}} = \dots = x_{i_t} = 0$, а значения остальных координат произвольны. Если рассмотрим вершину куба E^n, у которой $x_{i_1} = \dots =$ $= x_{i_r} = 1$, а остальные координаты произвольны, то эта вершина будет больше, чем вершина с $x_{i_1} = \dots = x_{i_r} = 1$, $x_{i_{r+1}} = \dots = x_{i_t} = 0$, и при этом остальные координаты останутся прежними. Ввиду монотонности функции f её значение в любой такой вершине также будет равно 1. Значит, для $K' = x_{i_1} \dots x_{i_r}$ интервал $N_{K'}$ будет допустимым и $N_K \subset N_{K'}$, поскольку $t > r$. Это же будет допустимым максимальности интервала N_K.

Теперь мы покажем, что $D_c(f)$ является м.д.н.ф. По только что приведенному доказательству, любая конъюнкция K из $D_c(f)$ имеет вид $K = x_{i_1} \dots x_{i_r}$ Эта конъюнкция обращается в единицу в вершине куба E^n с координатами $x_{i_1} = \dots = x_{i_r} = 1$ и нулевыми остальными координатами. Значит, и функция f в этой вершине обращается в единицу . Покажем, что никакая другая конъюнкция в $D_c(f)$ в этой вершине обращаться в единицу не может. Это будет обозначать, что конъюнкция K обязательно должна входить в м.д.н.ф. Итак, пусть некоторая конъюнкция K' тоже обращается в единицу в указанной вершине куба. Т.к. К$'$ не содержит отрицаний, то в неё в качестве сомножителей не должны входить переменные, отличные от $x_{i_1}, \dots, x_{i_r}$, иначе бы она обращалась в ноль в указанной вершине. Значит, К$'$ есть произведение, каких-то из переменных $x_{i_1}, \dots, x_{i_r}$, но не всех, т.к. $K' \neq K$. Но тогда $N_K \subset N_{K'} \subseteq N_f$, что противоречит максимальности интервала N_K.

Итак, задача нахождения м.д.н.ф. свелась, в первую очередь, к нахождению её сокращённой д.н.ф. Существуют различные алгоритмы нахождения сокращенной д.н.ф. Мы ограничиваемся двумя из них.

Алгоритм 1

Иногда его ещё называют методом Блейка. Этот алгоритм основан на применении следующих преобразований:

1) склеивание: $xK \vee \bar{x}K = K$;

2) поглощение: $K' \vee K'K'' = K'$;

3) неполное склеивание: $xK \vee \bar{x}K = xK \vee \bar{x}K \vee K$;

4) обобщённое склеивание: $xK' \vee \bar{x}K'' = xK' \vee \bar{x}K'' \vee K'K''$.

Легко заметить, что операции 1) и 3) легко получаются из 2) и 4). Метод основан на том, что к конъюнкциям произвольной д.н.ф. D функции $f(x_1, \dots, x_n)$ применяются преобразования 2) и 4) таким образом, что в итоге получаем $D_c(f)$.

Покажем сначала, что с помощью преобразований 4) можно каждую конъюнкцию K, соответствующую максимальному интервалу N_K, включить в д.н.ф. Достаточно рассмотреть случай, когда K не входит в D.

Сначала отметим, что в K входят только те переменные, которые содержатся в D. Если бы это было бы не так, то, удалив из K переменную, не входящую в D, мы получили бы конъюнкцию K' такую, что $N_K \subset N_{K'} \subseteq N_D = N_f$, а это противоречит максимальности K.

Рассмотрим теперь множество конъюнкций $\{K_j\}$, удовлетворяющих трём условиям:

a) K_j содержит только те переменные, которые входят в D;

b) $N_{K_j} \subseteq N_K$;

c) $N_{K_j} \nsubseteq N_H$ для всех конъюнкций H из д.н.ф. в D.

Множество $\{K_j\}$ содержит конъюнкцию K, поэтому оно не пусто. Выберем во множестве $\{K_j\}$ конъюнкции $K_1, \dots, K_m$, наибольшего ранга. Рассмотрим конъюнкцию K_1. Она не может содержать все переменные, входящие в D, т.к. в этом случае интервал N_{K_1} состоял бы из одной вершины, а это противоречит условию b). Возьмём переменную x, от которой зависит D и не зависит K_1. Рассмотрим конъюнкции xK_1 и $\bar{x}K_1$. Эти конъюнкции удовлетворяют условиям a) и b) и имеют ранг больший, чем ранг K_1. Значит, xK_1 и $\bar{x}K_1$ не удовлетворяют условию b). Следовательно, в д.н.ф. D есть конъюнкции H_1 и H_2 такие, что $N_{xK_1} \subseteq N_{H_1}$ и $N_{\bar{x}K_1} \subseteq N_{H_2}$. Элемент x (соответственно $\bar{x}$) входит в конъюнкцию H_1 (соответственно, в конъюнкцию H_2), т.к. $N_{K_1} \nsubseteq N_{H_1}$ и $N_{K_1} \nsubseteq N_{H_2}$. Значит, $H_1 = xH_1'$ и $H_2 = \bar{x}H_2'$, где $N_{K_1} \subseteq N_{H_1'}$, $N_{K_1} \subseteq N_{H_2'}$. Теперь, применяя преобразование типа 4), т.е. $xH_1' \vee \bar{x}H_2' = xH_1' \vee \bar{x}H_2' \vee H_1'H_2'$, получим, что конъюнкцию K_1можно включить в д.н.ф. Повторяя те же рассуждения, включим в д.н.ф. конъюнкции $K_2, \dots, K_m$. После этого в системе $\{K_j\}$ конъюнкции наибольшего ранга будут иметь ранг, меньший, чем у $K_1, \dots, K_m$. С ними повторяем ту же процедуру, пока не доберёмся до конъюнкции K.

Итак, все конъюнкции, соответствующие максимальным интервалам, можно включить в д.н.ф. Далее, используя преобразование 2), избавляемся от конъюнкций, соответствующих не максимальным интервалам. Это проделываем следующим образом. Пусть K – конъюнкция соответствующая немаксимальному интервалу N_K. Этот интервал входит в некоторый максимальный $N_{K'}$, причем конъюнкция K' входит в нашу д.н.ф. Т.к. $N_K \subset N_{K'}$, то $K = K'K''$ для некоторой конъюнкции K''. Тогда в д.н.ф. есть слагаемое $K'K'' \vee K'$, которое, согласно 2), можно заменить на одно слагаемое K'.

Пример 2. Рассмотрим ту же функцию $f(x,y,z)$, что и в примере 1 предыдущего параграфа. Исходим из её с.д.н.ф.

$$\bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}y\bar{z} \vee x\bar{y}z \vee xyz=$$
$$= \bar{x}\bar{y} \vee \bar{x}y\bar{z} \vee x\bar{y}z \vee xyz(\text{правило 1}) =$$
$$= \bar{x}\bar{y} \vee \bar{x}y\bar{z} \vee xz \text{ (правило 1)} = \bar{x}\bar{y} \vee \bar{x}y\bar{z} \vee \bar{x}\bar{z} \vee xz \text{ (правило 4)} =$$
$$= \bar{x}\bar{y} \vee \bar{x}\bar{z} \vee xz \text{ (правило 2)} = \bar{x}\bar{y} \vee xz \vee \bar{y}z \vee \bar{x}\bar{z} \text{ (правило 4)}.$$

Это и будет $D_c(f)$.

Алгоритм 2

Два n – мерных булевых вектора назовём соседними, если они отличаются всего одной координатой. Для двух соседних векторов $(\delta_1, \dots, \delta_{i-1}, 0, \delta_{i+1}, \dots, \delta_n)$ и $(\delta_1, \dots, \delta_{i-1}, 1, \delta_{i+1}, \dots, \delta_n)$ определим операцию «склеивания», означающую составление вектора $(\delta_1, \dots, \delta_{i-1}, -, \delta_{i+1}, \dots, \delta_n)$.

Далее, алгоритм заключается в следующем.

1) Разбиваем носитель на классы по числу единиц в векторах, т.е. $N_f = S_{i_1} \cup S_{i_2} \cup \dots \cup S_{i_k}$, где $0 \le i_1 \le i_1 < \dots < i_k$. Причем вектор $\delta \in N_f$ принадлежит классу S_{i_j}, если число единиц в его координате равно i_j.

2) Составляем треугольную таблицу, содержащую k строк и k столбцов. В первом столбце будет k клеток, в каждую из которых по порядку записываем векторы множеств $S_{i_1}, S_{i_2}, \dots, S_{i_k}$. Клетки первого столбца нумеруем как $(1,1), (2,1), \dots, (k,1)$.

3) Каждый вектор δ_m из класса S_{i_j} сравниваем с каждым вектором δ_l из класса $S_{i_{j+1}}$. Если векторы δ_m и δ_l оказались соседними, то производим их склеивание и результат записываем в клетку с номером $(j, 2)$. При этом векторы, участвующие в склеивании, помечаем каким-либо символом, например, *.

4) Векторы из клетки $(j, 2)$ сравниваем на склеивание с векторами из клетки $(j + 1{,}2)$. При этом склеивание производим только тех векторов, у которых прочерки «–» стоят на одних и тех же местах.

5) Проделываем ту же процедуру с третьим столбцом, с четвертым и т.д. до тех пор, пока возможно производить склеивание.

6) Выписываем множество W всех векторов, которые не участвовали в склеивании (они не помечены символом *). Каждому вектору $\delta = (\delta_1, \dots, \delta_n)$ из W, где δ_i равно 0, 1 или «-», ставим в соответствие конъюнкцию $K = x_{i_1}^{\delta_1} \dots x_{i_m}^{\delta_m}$, где $\delta_1, \dots, \delta_m$ — все, отличные от прочерка «-», координаты. Тогда $D = \bigvee_{\delta \in W} x_{i_1}^{\delta_1} \dots x_{i_m}^{\delta_m}$ и будет искомой сокращённой $\delta \epsilon W$ д.н.ф. для функции $f(x_1, \dots, x_n)$.

Пример 3. Пусть функция $f(x_1, x_2, x_3, x_4)$ задана своей с.д.н.ф. $f(x_1, x_2, x_3, x_4) = x_1 x_2 \overline{x_3} x_4 \vee x_1 \overline{x_2}\, \overline{x_3} x_4 \vee \overline{x_1} x_2 \overline{x_3}\, \overline{x_4} \vee \overline{x_1}\, \overline{x_2} x_3 \overline{x_4} \vee x_1 x_2 x_3 \overline{x_4} \vee$
$\vee\, x_1 \overline{x_2} x_3 x_4$. Найти для функции f её $D_c(f)$.

Из задания функции f следует, что
$N_f = \{(1;1;0;1); (1;0;0;1); (0;1;0;0); (0;0;1;0); (1;1;1;0); (1;0;1;1)\}$.

Составляем множества, S_i, а именно:

$S_1 = \{(0,1,0,0), (0,0,1,0)\}$,

$S_2 = \{(1,0,0,1)\}$,

$S_3 = \{(1,1,0,1), (1,1,1,0), (1,0,1,1)\}$.

Строим соответствующую треугольную таблицу и проводим необходимые склеивания:

(0,1,0,0) (0,0,1,0)	
(1,0,0,1)*	(1,-,0,1) (1,0,-,0)
(1,1,0,0)* (1,1,1,0) (1,0,1,1)*	

Таким образом, требуемой $D_c(f)$ будет $\overline{x_1} x_2 \overline{x_3 x_4} \vee \overline{x_1 x_2} x_3 \overline{x_4} \vee$
$\vee\, x_1 x_2 x_3 \overline{x_4} \vee x_1 \overline{x_3} x_4 \vee x_1 \overline{x_2} x_4$.

§ 3.3. Тупиковые дизъюнктивные нормальные формы

Определение 1. Покрытие подмножества N_f максимальными интервалами называется неприводимым, если после удаления из него любого интервала оно перестаёт быть покрытием.

Определение 2. Д.н.ф. функции f называется тупиковой, если ей соответствует неприводимое покрытие подмножества N_f. Очевидно, что всякая м.д.н.ф. является тупиковой. Процесс построения м.д.н.ф. на основе сокращённой д.н.ф. сводится к следующему:

1. Выделяются все максимальные интервалы, и строится сокращенная д.н.ф. (которая определяется однозначно).
2. Используя найденную $D_c(f)$, строятся все тупиковые д.н.ф.
3. Среди всех тупиковых д.н.ф. выбираются те, которые содержат наименьшее число переменных. Это и будут все м.д.н.ф.

Процесс перехода от сокращённой д.н.ф. к тупиковой разбивается на элементарные шаги, каждый из которых представляет собой удаление из д.н.ф. D, полученной на предыдущем шаге, одной элементарной конъюнкции K.

Удаляемая конъюнкция K такова, что $N_K \subseteq \bigcup_{j=1}^{m} N_{K_j}$, где K_j – конъюнкции из D, отличные от K.

Определение 3. Говорят, что дизъюнкция $D = K_1 \vee K_2 \vee \ldots \vee K_m$ элементарных конъюнкций поглощает элементарную конъюнкцию K, если $K \leq D$.

Другими словами, конъюнкция K поглощается дизъюнкцией $D = \bigvee_{j=1}^{m} K_j$, если $N_K \subseteq \bigcup_{j=1}^{m} N_{K_j}$.

Теорема 1. Дизъюнкция $D = \bigvee_{j=1}^{m} K_j$ поглощает элементарную конъюнкцию K тогда и только тогда, когда каждая конъюнкция K_j представима в виде $K_j = K'_j K''_j$ так, что:

a) $K \leq \bigwedge_{j=1}^{m} K'_j$;

b) $\bigvee_{j=1}^{m} K''_j = 1$.

Доказательство.

Пусть выполнены условия теоремы, и покажем, что $K \leq D$. Рассмотрим произвольный набор значений переменных $\delta = (\delta_1, \ldots, \delta_n)$. Если $K(\delta) = 0$, то очевидно, что $K(\delta) \leq D(\delta)$. Пусть $K(\delta) = 1$. В силу условия а), $K(\delta) \leq$ $\leq \bigwedge_{j=1}^{m} K'_j\ (\delta)$, т.е. $\bigwedge_{j=1}^{m} K'_j\ (\delta) = 1$. В таком случае, для любого $j = 1, \ldots, m$ $K_j(\delta) = 1$. Тогда $D(\delta) = \bigvee_{j=1}^{m} K'_j(\delta) K''_j(\delta) = \bigvee_{j=1}^{m} K''_j = 1$ (последнее равенство справедливо в силу условия b)). Итак, получаем, что $D(\delta) = 1$, т.е. $K(\delta) \leq D(\delta)$. Это и означает, что $K \leq D$.

Обратно, пусть $K \leq D$, и покажем справедливость условий теоремы. Для каждого $j = 1, \ldots, m$ обозначим через K'_j произведение всех сомножителей вида $x_i^{\delta_i}$, входящих в K и K_j(если таких сомножителей нет, то $K'_j = 1$). Конъюнкцию оставшихся сомножителей из K_j обозначим через K''_j (если таких нет, то $K''_j = 1$). По строению, произведение $\bigwedge_{j=1}^{m} K'_j$ состоит только из сомножителей, входящих в K (быть может, не всех).

Из теоремы 1 предыдущего параграфа 3.2 следует, что $K \leq \bigwedge_{j=1}^{m} K'_j$, т.е. условие а) выполнено.

Докажем, что выполнено условие b), т.е. что $\bigvee_{j=1}^{m} K''_j = 1$. Рассмотрим произвольный набор значений переменных $\delta = (\delta_1, \ldots, \delta_n)$. Если $K(\delta) = 1$, то ввиду того, что $K \leq D$, $D(\delta) = 1$. Т.к. $K \leq \bigwedge_{j=1}^{m} K'_j$, то для любого $j = 1, \ldots, m$ $K'_j(\delta) = 1$.

В таком случае $1 = D(\delta) = \bigvee_{j=1}^{m} K_j = \bigvee_{j=1}^{m} K'_j(\delta) K''_j(\delta) = \bigvee_{j=1}^{m} K''_j(\delta)$.

Пусть теперь $K(\delta) = 0$. Изменим в наборе δ значение переменных, входящих в K, так, чтобы получился набор τ со свойством $K(\tau) = 1$. По только что доказанному $\bigvee_{j=1}^{m} K''_j(\tau) = 1$. По построению, конъюнкция K''_j не содержит сомножителей, общих с K. Поэтому при переходе от набора δ к набору τ каждый из сомножителей в K''_j, сохраняет своё значение (либо изменяется с 1 на 0). Следовательно, $\bigvee_{j=1}^{m} K''_j(\delta) \geq \bigvee_{j=1}^{m} K''_j(\tau) = 1$, т.е. и в этом случае $\bigvee_{j=1}^{m} K''_j(\delta) = 1$.

Таким образом, для того, чтобы проверить поглощение конъюнкции K дизъюнкцией $K_1 \vee K_2 \vee \ldots \vee K_m$, надо из всех K_j, $j = 1, \ldots, m$ удалить все буквы $x_i^{\delta_i}$, встречающиеся в K. После этого проверяется, будет ли после такого удаления дизъюнкция $K''_1 \vee \ldots \vee K''_m$ всегда равна 1 или нет.

Используя теорему 1, можно из сокращённой д.н.ф. $K_1 \vee K_2 \vee \ldots \vee K_m$ построить все тупиковые, проверяя поочерёдно на поглощение каждой из конъюнкций K_j дизъюнкцией остальных конъюнкций K_i, $i \neq j$.

Рассмотрим ещё один алгоритм построения всех тупиковых д.н.ф. из сокращённой д.н.ф.

Пусть нами получена сокращённая д.н.ф. $D_c(f) = K_1 \vee K_2 \vee \ldots \vee K_m$. Каждой конъюнкции K_j поставим в соответствие булеву переменную k_j. Для каждой д.н.ф. D, составленной из конъюнкций K_j, полагаем, что $k_j = 1$, если K_j входит в D, и $k_j = 0$ в противном случае.

Пусть N_f состоит из вершин $\delta^1, \ldots, \delta^t$. Для каждой вершины δ^i, $i = 1, \ldots, t$ выделяем в $D_c(f)$ все такие конъюнкции $K_{j(i,1)}, \ldots, K_{j(i,l(i))}$, что $K_{j(i,h)}(\delta^i) = 1$, $h = 1, \ldots, l(i)$. Очевидно, что д.н.ф. D реализует функцию f тогда и только тогда, когда $\bigwedge_{i=1}^{t} \bigvee_{h=1}^{l(i)} k_{j(i,h)} = 1$.

Пользуясь законами дистрибутивности, приводим левую часть данного равенства к виду $\wedge$, $\vee$ (при этом одновременно удаляем поглощаемые конъюнкции). В результате будем иметь $\vee k_{j_1} \ldots k_{j_m} = 1$. Каждой конъюнкции из этого равенства ставим в соответствие д.н.ф. $K_{j_1} \vee \ldots \vee K_{j_m}$. Эти д.н.ф. и будут тупиковыми.

Пример 1. Пусть функция $f(x, y, z)$ задана своей с.д.н.ф. $f = \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \vee \bar{x}y\bar{z} \vee x\bar{y}z \vee xyz \vee xy\bar{z}$, т.е.

$N_f = \{(0,0,0), (0,0,1), (1,0,1), (1,1,1), (1,1,0), (0,1,0)\}$. Найти для функции $f(x, y, z)$ все тупиковые д.н.ф.

Найдём для функции $f(x, y, z)$ её сокращённую д.н.ф. $D_c(f)$. Для этого построим для неё таблицу склеек:

(0,0,0)*	(0,0,-) (0,-,0)
(0,0,1)* (0,1,0)*	(-,0,1) (-,1,0)
(1,0,1)* (1,1,0)*	(1,-,1) (1,1,-)
(1,1,1)*	

Итак, $D_c(f) = \bar{x}\bar{y} \vee \bar{x}\bar{z} \vee \bar{y}z \vee y\bar{z} \vee xz \vee xy$. Соответственно предыдущему алгоритму, пусть $\delta^1 = (0,0,0)$, $\delta^2 = (0,0,1)$, $\delta^3 = (1,0,1)$, $\delta^4 = (1,1,1)$, $\delta^5 = (1,1,0)$ и $\delta^6 = (0,1,0)$. Далее, обозначим $\bar{x}\bar{y} = K_1$, $\bar{y}z = K_2$, $xz = K_3$, $xy = K_4$, $y\bar{z} = K_5$, $\bar{x}\bar{z} = K_6$.

		N_f					
		(0,0,0)	(0,0,1)	(1,0,1)	(1,1,1)	(1,1,0)	(0,1,0)
K_1	$\bar{x}\bar{y}$	1	1				
K_2	$\bar{y}z$		1	1			
K_3	xz			1	1		
K_4	xy				1	1	
K_5	$y\bar{z}$					1	1
K_6	$\bar{x}\bar{z}$	1					1

Составляем левую часть равенства $\bigwedge_{i=1}^{t} \bigvee_{h=1}^{l(i)} k_{j(i,h)} = 1$.

Т.к. $K_1(\delta^1) = K_6(\delta^1) = 1$, то первым сомножителем в этой конъюнкции будет $k_1 \vee k_6$. Далее, поскольку $K_1(\delta^2) = K_2(\delta^2) = 1$, то следующий множитель будет $k_1 \vee k_2$, и т.д. Таким образом, левая часть вышеуказанного равенства принимает следующий вид:

$(k_1 \vee k_6)(k_1 \vee k_2)(k_2 \vee k_3)(k_3 \vee k_4)(k_4 \vee k_5)(k_5 \vee k_6)$.

Преобразуя её к виду: $\bigwedge \quad , \bigvee$,

получаем $k_1k_3k_5 \vee k_2k_4k_6 \vee k_1k_2k_4k_5 \vee k_1k_3k_4k_6 \vee k_2k_3k_5k_6$.

Далее, по закону поглощения:

$$(k_1 \vee k_6)(k_1 \vee k_2)(k_2 \vee k_3)(k_3 \vee k_4)(k_4 \vee k_5)(k_5 \vee k_6) =$$
$$= (k_1 \vee k_1k_2 \vee k_1k_6 \vee k_2k_6)(k_2k_3 \vee k_2k_4 \vee k_3 \vee k_3k_4)(k_4k_5 \vee k_4k_6 \vee k_5 \vee k_5k_6) =$$
$$= (k_1 \vee k_2k_6)(k_2k_4 \vee k_3)(k_4k_6 \vee k_5) =$$
$$= (k_1k_2k_4 \vee k_1k_3 \vee k_2k_4k_6 \vee k_2k_3k_6)(k_4k_6 \vee k_5) =$$
$$= k_1k_2k_4k_6 \vee k_1k_3k_4k_6 \vee k_2k_4k_6 \vee k_2k_3k_4k_6 \vee k_1k_2k_4k_5 \vee k_1k_3k_5 \vee$$
$$\vee k_2k_4k_5k_6 \vee k_2k_3k_5k_6 =$$
$$= k_1k_3k_5 \vee k_2k_4k_6 \vee k_1k_2k_4k_5 \vee k_1k_3k_4k_6 \vee k_2k_3k_5k_6.$$

В таком случае функция $f(x, y, z)$ имеет пять тупиковых д.н.ф.:

$D_1 = \bar{x}\bar{y} \vee xz \vee y\bar{z}$;

$D_2 = y\bar{z} \vee xy \vee \bar{x}\bar{z}$;

$D_3 = \bar{x}\bar{y} \vee \bar{y}z \vee xy \vee y\bar{z}$;

$D_4 = \bar{x}\bar{y} \vee xz \vee xy \vee \bar{x}\bar{z}$;

$D_5 = \bar{y}z \vee xz \vee y\bar{z} \vee \bar{x}\bar{z}$;

Отсюда видно, что д.н.ф. D_1 и D_2 являются минимальными д.н.ф.

ЛИТЕРАТУРА

1. *Биркгоф Г., Барти Т.* Современная прикладная алгебра /пер. с англ. Ю.И. Манина. - М.: Мир, 1976. - 400 с.
2. *Кузнецов О.П., Адельсон-Вельский Г.М.* Дискретная математика для инженера. - М.: Энергия, 1980. - 344 с.
3. *Нефёдов В.Н., Осипова В.А.* Курс дискретной математики. - М.: Наука, 1992. - 264 с.
4. *Логинов Б.М.* Введение в дискретную математику. - Калуга: Облиздат, 1998. — 424 с.
5. *Ерусалимский Я.М.* Дискретная математика. - М.: Вузовская книга, 2000. - 280 с.
6. *Лавров И.А., Максимова Л.Л.* Задачи по теории множеств, математический логике и теории алгоритмов. - М.: Физматгиз, 2004.

Учебное издание

Наталья Васильевна **Труб**

Булева алгебра

Учебное пособие

Технический редактор - К.А. Антонов
Редактор\корректор - Ю.Ф. Кравчинская
Компьютерная верстка - Ю.Ф. Кравчинская
Дизайн обложки - О.В. Кузнецова

Подписано в печать 10.04.2017. Формат 60x84 $^{1}/_{16}$.
Бумага офисная. Гарнитура *Times New Roman*. Печ. лист 3,5.
Тираж 100 экз. Заказ № 20.

Московский государственный гуманитарно-экономический университет
107150, Москва, ул. Лосиноостровская, д. 49.
Отпечатано в типографии МГГЭУ по технологии CtP.

Для заметок

Для заметок