6. Логические исчисления
6.1. Булевы алгебры
6.1.1. Высказывание. Логические операции. Формулы алгебры высказываний. Приоритет операций

Высказывание – это…

Пример.

«Рим – столица Италии» – высказывание истинно;

«$2\times2=5$» – высказывание ложно.

Элементарное высказывание – это …

Сложное высказывание – это...

Операции над высказываниями являются предметом части математической логики, называемой *логикой высказываний*.

Обозначение высказываний: A, B, C,..., их значений: *Л* – ложь, *И* – истина.

Операции над высказываниями

Пусть даны два произвольных высказывания A и B.

1) *Отрицанием* высказывания A называется высказывание, истинное тогда и только тогда, когда высказывание A ложно.

Обозначается $\overline{A}$ (или $\neg A$, A') и читается «не A».

2) *Конъюнкцией* двух высказываний A и B называется высказывание, истинное тогда и только тогда, когда оба высказывания истинны.

Обозначается $A \wedge B$ (или $A\&B$) и читается «A и B».

3) *Дизъюнкцией* двух высказываний A и B называется высказывание, ложное тогда и только тогда, когда оба высказывания ложны.

Обозначается $A \vee B$ и читается «A или B».

4) *Импликацией* двух высказываний A и B называется высказывание, ложное тогда и только тогда, когда A истинно, а B ложно.

Обозначается $A \to B$ (или $A \supset B$, $A \Rightarrow B$) и читается «A влечёт B» (или «если A, то B», «из A следует В»). Высказывание A называется *посылкой* импликации, а высказывание B – *заключением* импликации.

5) *Эквивалентностью* двух высказываний A и B называется высказывание, истинное тогда и только тогда, когда истинностные значения A и B совпадают.

Обозначается $A \sim B$ и читается «A эквивалентно B».

6) *Суммой по mod 2* двух высказываний A и B называется высказывание, истинное тогда и только тогда, когда истинностные значения A и B различны.

Обозначается $A \oplus B$ и читается «A сумма по модулю 2 B».

7) *Штрих Шеффера* – антиконъюнкция. *Антиконъюнкцией* двух высказываний A и B называется высказывание, ложное тогда и только тогда, когда оба высказывания истинны.

Обозначается $(A \mid B) = \overline{(A \wedge B)}$ и читается «A штрих Шеффера B».

8) *Стрелка Пирса* – антидизъюнкиция. *Антидизюнкцией* двух высказываний A и B называется высказывание, истинное тогда и только тогда, когда оба высказывания ложны. Обозначается $(A \downarrow B) = \overline{(A \vee B)}$ и читается «A стрелка Пирса B».

Формула алгебры высказываний – это …

Пример.

Пусть высказывание X принимает значение $Л$, высказывание Y – $Л$, высказывание Z – $И$, тогда формула $A = (Y \wedge (Z \rightarrow X)) \vee (\bar{X} \sim \bar{Y})$ примет значение

$$A = (Л \wedge (И \rightarrow Л)) \vee (И \sim И) = (Л \wedge Л) \vee И = Л \vee И = И.$$

Все операции можно полностью описать таблицей истинности (табл.6.1, 6.2).

Операция отрицание. Таблица 6.1

X	$\bar{X}$
$Л$	$И$
$И$	$Л$

Логические операции $\wedge, \vee, \rightarrow, \sim, \oplus, |, \downarrow$. Таблица 6.2

X	Y	$X \wedge Y$	$X \vee Y$	$X \rightarrow Y$	$X \sim Y$	$X \oplus Y$	$X \mid Y$	$X \downarrow Y$
$Л$	$Л$	$Л$	$Л$	$И$	$И$	$Л$	$И$	$И$
$Л$	$И$	$Л$	$И$	$И$	$Л$	$И$	$И$	$Л$
$И$	$Л$	$Л$	$И$	$Л$	$Л$	$И$	$И$	$Л$
$И$	$И$	$И$	$И$	$И$	$И$	$Л$	$Л$	$Л$

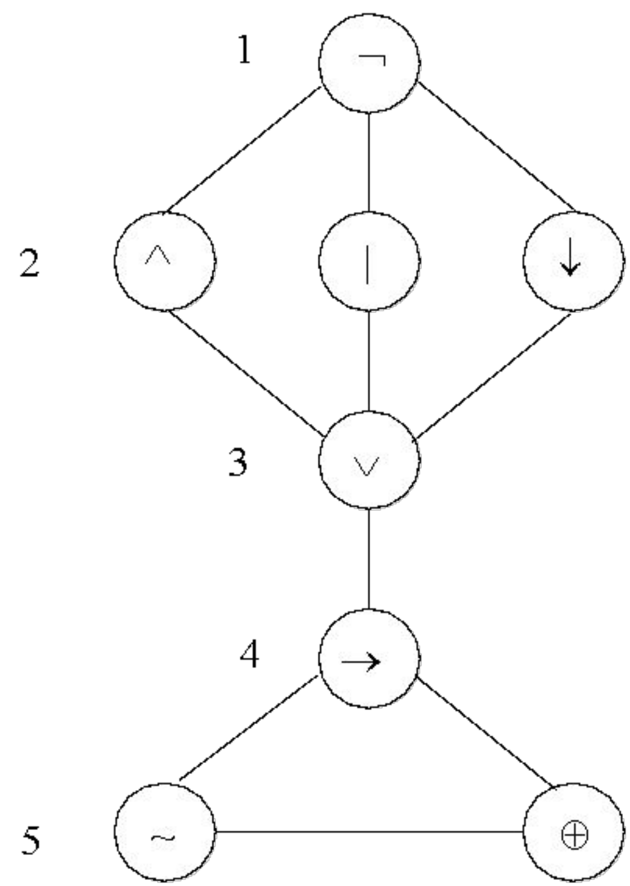

Рис. 6.1. Приоритет операций

Пример. Расставить приоритет операций

$$A = X \overset{5}{\oplus} \overset{1}{\overline{Y}} \overset{3}{\wedge} \overset{2}{\overline{Z}} \overset{6}{\sim} X \overset{4}{\vee} Z.$$

Пример. Составить таблицы истинности формул $A(X,Y) = X \oplus Y \wedge \overline{X}$ (табл. 6.3) и $B(X,Y,Z) = (\overline{Y} \vee Z) \downarrow (\overline{X} \sim Y)$ (табл. 6.4).

Формула $A(X, Y)$ Таблица 6.3

X	Y	$\overline{X}$	$Y \wedge \overline{X}$	$X \oplus Y \wedge \overline{X}$
Л	*Л*	*И*	*Л*	*Л*
Л	*И*	*И*	*И*	*И*
И	*Л*	*Л*	*Л*	*И*
И	*И*	*Л*	*Л*	*И*

Формула $B(X, Y, Z)$. Таблица 6.4

X	Y	Z	$\overline{Y}$	$\overline{Y} \vee Z$	$\overline{X}$	$\overline{X} \sim Y$	$(\overline{Y} \vee Z) \downarrow (\overline{X} \sim Y)$
Л	*Л*	*Л*	*И*	*И*	*И*	*Л*	*Л*
Л	*Л*	*И*	*И*	*И*	*И*	*Л*	*Л*
Л	*И*	*Л*	*Л*	*Л*	*И*	*И*	*Л*
Л	*И*	*И*	*Л*	*И*	*И*	*И*	*Л*
И	*Л*	*Л*	*И*	*И*	*Л*	*И*	*Л*
И	*Л*	*И*	*И*	*И*	*Л*	*И*	*Л*
И	*И*	*Л*	*Л*	*Л*	*Л*	*Л*	*И*
И	*И*	*И*	*Л*	*И*	*Л*	*Л*	*Л*

6.1.2. Равносильность формул

Две формулы A и B называются *равносильными*, если они принимают одинаковые значения на одном и том же списке переменных $X_1, X_2, ..., X_n$, входящих в A и B. Равносильность формул обозначается: $A \equiv B$.

Основные равносильности формул

Для любых формул A, B, C справедливы следующие равносильности:

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

Логические операции $\overline{}, \wedge, \vee, \rightarrow, \sim, \oplus, |, \downarrow$ не являются независимыми друг от друга. Одни из них можно выразить через другие так, что при этом получаются равносильные формулы:

22) $A \sim B \equiv (A \rightarrow B) \wedge (B \rightarrow A) \equiv (A \wedge B) \vee (\overline{A} \wedge \overline{B})$;

23) $A \rightarrow B \equiv \overline{A} \vee B \equiv \overline{(A \wedge \overline{B})}$;

24) $A \vee B \equiv \overline{A} \rightarrow B \equiv \overline{(\overline{A} \wedge \overline{B})}$;

25) $A \wedge B \equiv \overline{(A \rightarrow \overline{B})} \equiv \overline{(\overline{A} \vee \overline{B})}$;

26) $A \oplus B \equiv (\overline{A} \wedge B) \vee (A \wedge \overline{B})$;

27) $A \mid B = \overline{(A \wedge B)}$;

28) $A \downarrow B = \overline{(A \vee B)}$.

6.1.3. Закон двойственности

Пусть $X_1,...,X_n$ – все входящие в формулу A элементарные высказывание. Формула $A^*(X_1,...,X_n) \equiv \overline{A}(\overline{X}_1,...,\overline{X}_n)$ называется *двойственной* к формуле A. Очевидно, что A^{**} совпадает с A.

Пример.

1. $A = X \vee Y$; $A^*(X,Y) \equiv \overline{A}(\overline{X},\overline{Y}) \equiv \overline{(\overline{X} \vee \overline{Y})} \equiv X \wedge Y$. Таким образом, операция дизъюнкция ($\vee$) двойственна операции конъюнкция ($\wedge$), и наоборот.

2. $A(X_1,...,X_n) \equiv Л; A^*(X_1,...,X_n) \equiv \overline{Л} \equiv И$. Т. о., $Л$ двойственна $И$, и наоборот.

Формула называется *самодвойственной*, если $A^* = A$.

Теорема 6.1 (закон двойственности). Если формулы A и B равносильны друг другу, то и двойственными к ним также равносильны, т.е. если $A \equiv B$, то и $A^* \equiv B^*$.

Доказательство. Пусть $A(X_1,...,X_n) \equiv B(X_1,...,X_n)$, *где* $X_1,...,X_n$ – входящие в них элементарные высказывания. Тогда

$$A^*(X_1,...,X_n) \equiv \overline{A}(\overline{X}_1,...,\overline{X}_n) \text{ и } B^*(X_1,...,X_n) \equiv \overline{B}(\overline{X}_1,...,\overline{X}_n).$$

Формулы $A(X_1,...,X_n)$ и $B(X_1,...,X_n)$ принимают одинаковые значения при любых значениях переменных $X_1,...,X_n$. Следовательно, A и B будут равносильны и при переменных $\overline{X}_1,...,\overline{X}_n$, т.е. $A(\overline{X}_1,...,\overline{X}_n) \equiv B(\overline{X}_1,...,\overline{X}_n)$. Применим операцию отрицание к формуле. Значение формул *Л* поменяется на значение *И*, а *И* – на *Л*. Но формулы при этом останутся равносильными, т.е. $\overline{A}(\overline{X}_1,...,\overline{X}_n) \equiv \overline{B}(\overline{X}_1,...,\overline{X}_n)$. Таким образом, так как $A^* = \overline{A}(\overline{X}_1,...,\overline{X}_n)$, $B^* = \overline{B}(\overline{X}_1,...,\overline{X}_n)$, получаем $A^* \equiv B^*$.

Доказательство завершено.

6.1.4. Тождественно истинные и ложные формулы

Пусть формула A зависит от списка переменных $X_1,...,X_n$.

Формула A называется *тавтологией* (или *тождественно-истинной формулой*), если на любых оценках списка переменных $X_1,...,X_n$ она принимает значение *И*.

<u>Пример.</u> $X \vee \overline{X}$.

Формула A называется *выполнимой*, если на некоторой оценке списка переменных $X_1,...,X_n$ она принимает значение *И*.

<u>Пример.</u> $\overline{X} \wedge Y$.

Формула A называется *тождественно-ложной*, если на любых оценках списка переменных $X_1,...,X_n$ она принимает значение *Л*.

<u>Пример.</u> $X \wedge \overline{X}$.

Формула A называется *опровержимой*, если на некоторой оценке списка переменных $X_1,...,X_n$ она принимает значение *Л*.

<u>Пример.</u> $X \vee Y$.

Утверждение 6.1.

1. A – тавтология $\Leftrightarrow$ A не является опровержимой.
2. A – тождественно-ложна $\Leftrightarrow$ A не является выполнимой.
3. A – тавтология $\Leftrightarrow$ $\overline{A}$ – тождественно-ложна.
4. A – тождественно-ложна $\Leftrightarrow$ $\overline{A}$ – тавтология.
5. $A \sim B$ – тавтология $\Leftrightarrow A \equiv B$.

Ниже указаны наиболее важные тавтологии (A, B, C – произвольные формулы).

1) $A \vee \overline{A}$ (закон исключающего третьего);
2) $A \to A$;
3) $A \to (B \to A)$;
4) $(A \to B) \to ((B \to C) \to (A \to C))$ (цепное рассуждение);
5) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$;
6) $(A \wedge B) \to A$, $\quad (A \wedge B) \to B$;
7) $A \to (B \to (A \wedge B))$;
8) $A \to (A \vee B), B \to (A \vee B)$;
9) $(\overline{B} \to \overline{A}) \to ((\overline{B} \to A) \to B)$;
10) $((A \to B) \to A) \to A$ (закон Пирса).

Каждую из этих тавтологий можно обосновать, например, составив таблицу истинности при произвольных значениях A, B, C.

6.1.5. Нормальные формы (дизъюнктивные нормальные формы и конъюнктивные нормальные формы)

Рассмотрим выражения

$$A_1 \wedge A_2 \wedge \ldots \wedge A_k \qquad (6.1)$$

$$A_1 \vee A_2 \vee \ldots \vee A_k \qquad (6.2)$$

Выражение (6.1) называют *многочленной конъюнкцией*, выражение (6.2) – *многочленной дизъюнкцией*.

Запишем обобщенные законы дистрибутивности и обобщенные законы де Моргана

1)

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_k) \vee (B_1 \wedge B_2 \wedge \ldots \wedge B_l) \equiv (A_1 \vee B_1) \wedge (A_1 \vee B_2) \wedge \ldots \wedge (A_1 \vee B_l) \wedge$$

$$\wedge (A_2 \vee B_1) \wedge (A_2 \vee B_2) \wedge \ldots \wedge (A_2 \vee B_l) \wedge \ldots \wedge (A_k \vee B_1) \wedge (A_k \vee B_2) \wedge \ldots \wedge (A_k \vee B_l)$$

(6.3)

2)

$$(A_1 \vee A_2 \vee \ldots \vee A_k) \wedge (B_1 \vee B_2 \vee \ldots \vee B_l) \equiv (A_1 \wedge B_1) \vee (A_1 \wedge B_2) \vee \ldots \vee (A_1 \wedge B_l) \vee$$

$$\vee (A_2 \wedge B_1) \vee (A_2 \wedge B_2) \vee \ldots \vee (A_2 \wedge B_l) \vee \ldots \vee (A_k \wedge B_1) \vee (A_k \wedge B_2) \vee \ldots \vee (A_k \wedge B_l)$$

(6.4)

3) $\overline{(A_1 \wedge A_2 \wedge \ldots \wedge A_k)} = \overline{A_1} \vee \overline{A_2} \vee \ldots \vee \overline{A_k}$ (6.5)

4) $\overline{(A_1 \vee A_2 \vee \ldots \vee A_k)} = \overline{A_1} \wedge \overline{A_2} \wedge \ldots \wedge \overline{A_k}$ (6.6)

Формулу называют *элементарной конъюнкцией*, если…

Пример.

$A_1(X,Y)=X$; $A_2(X,Y,Z)=\overline{Y}$; $A_3(X,Y,Z)=X\wedge\overline{Z}$; $A_4(X,Y,Z)=\overline{Y}\wedge\overline{X}\wedge Z$.

Говорят, что формула находится в *дизъюнктивной нормальной форме* (ДНФ), если …

Пример.

$A_1(X,Y)=\overline{Y}$; $A_2(X,Y)=(X)\vee(Y)$; $A_3(X,Y,Z)=(X\wedge\overline{Y}\wedge Z)$;

$A_4(X,Y,Z)=(X)\vee(Y\wedge Z)$; $A_5(X,Y,Z)=(Y\wedge\overline{Z})\vee Z\vee(Z\wedge\overline{X}\wedge Y)$.

Теорема 6.2 (о приведении к ДНФ). Для любой формулы A можно найти такую формулу B, находящуюся в ДНФ, что $A\equiv B$. Формула B называется дизъюнктивной нормальной формой формулы A.

Доказательство. Доказательство теоремы распадается на три этапа.

1). Для формулы A строим такую формулу A_1, что $A\equiv A_1$ и в A_1 не содержатся операции $\rightarrow, \sim, \oplus, |, \downarrow$ (равносильности 22 – 28).

2). Докажем, что для формулы A_1 можно найти равносильную ей формулу A_2, в которой операция отрицание находится только над переменными - *формула с «тесными» отрицаниями*.

Доказательство по индукции. Пусть число логических символов (операций) формулы A_1 равно n.

❖ Если $n=0$, то A_1 есть какая-то переменная X_i (либо $\overline{X_i}$). В качестве A_2 нужно взять X_i (либо $\overline{X_i}$).

❖ Пусть утверждение выполняется для всех формул A_1 с числом символов меньше n.

❖ Пусть в формуле A_1 содержится n логических операций. Рассмотрим случаи.

а) $A_1 \equiv B_1 \vee C_1$. Тогда в B_1, C_1 логических символов меньше, чем n. Поэтому $\exists$ B_2, C_2 такие, что $B_1 \equiv B_2, C_1 \equiv C_2$ и в B_2, C_2 отрицание только над переменными. Отсюда $B_2 \vee C_2 \equiv A_2$ и является формулой с «тесными» отрицаниями.

б) $A_1 \equiv B_1 \wedge C_1$. Аналогично.

в) $A_1 \equiv \overline{\overline{B_1}}$. Тогда $A_1 \equiv B_1$ (применили равносильность 21) и в B_1 логических операций меньше, чем n.

г) $A_1 \equiv \overline{B_1 \vee C_1}$. Тогда $A_1 \equiv \overline{B_1} \wedge \overline{C_1}$ (применили равносильность 8) и в $\overline{B_1}, \overline{C_1}$ логических символов меньше, чем n …

д) A_1 имеет вид $\overline{B_1 \wedge C_1}$. Тогда $A_1 \equiv \overline{B_1} \vee \overline{C_1}$ (применили равносильность 7) …

Пример. Преобразуем выражение к формуле с «тесными» отрицаниями (в скобках указаны номера равносильностей):

$$\overline{((X_1 \vee \overline{(\overline{X}_1 \vee X_3)}) \vee (\overline{X}_2 \wedge X_3))} \equiv (8) \equiv \overline{(X_1 \vee \overline{(\overline{X}_1 \vee X_3)})} \wedge \overline{(\overline{X}_2 \wedge X_3)} \equiv (8{,}7)$$

$$\equiv \overline{X}_1 \wedge \overline{\overline{(\overline{X}_1 \vee X_3)}} \wedge (\overline{\overline{X}}_2 \vee \overline{X}_3) \equiv (21) \equiv \overline{X}_1 \wedge (\overline{X}_1 \vee X_3) \wedge (X_2 \vee \overline{X}_3).$$

3). К полученной формуле A_2 применяем законы (6.3) и (6.4). В итоге формула B будет удовлетворять требованиям теоремы.

Доказательство завершено.

Пример. Применим преобразования 3-го этапа к формуле с «тесными» отрицаниями, полученной в предыдущем примере:

$$\overline{X}_1 \wedge (\overline{X}_1 \vee X_3) \wedge (X_2 \vee \overline{X}_3) \equiv (6) \equiv [(\overline{X}_1 \wedge \overline{X}_1) \vee (\overline{X}_1 \wedge X_3)] \wedge (X_2 \vee \overline{X}_3) \equiv (6) \equiv$$

…

$$\equiv (\overline{X}_1 \wedge X_2) \vee (\overline{X}_1 \wedge \overline{X}_3) \vee (\overline{X}_1 \wedge X_3 \wedge X_2).$$ - ДНФ

Говорят, что формула A находится в *конъюнктивной нормальной форме* (КНФ), если формула A^* определена (то есть в A нет операций $\to, \sim, \oplus, |, \downarrow$) и находится в ДНФ. – первое определение

Формулу называют *элементарной дизъюнкцией*, если ...

Пример.

$A_1(X,Y) = \bar{Y}$; $A_2(X,Y,Z) = Z$; $A_3(X,Y,Z) = X \vee Y$; $A_4(X,Y,Z) = \bar{Z} \vee \bar{Y} \vee X$.

Формула находится в *конъюнктивной нормальной форме* (КНФ), если ... - второе определение

Пример.

$A_1(X,Y) = Y$; $A_2(X,Y) = (Y) \wedge (X)$; $A_3(X,Y,Z) = (\bar{Y} \vee \bar{X} \vee Z)$;

$A_4(X,Y) = \bar{Z} \wedge (\bar{Y} \vee X)$; $A_5(X,Y,Z) = (\bar{X} \vee \bar{Z} \vee \bar{Y}) \wedge (X \vee \bar{Y}) \wedge Z$.

Теорема 6.3 (о приведении к КНФ). Для любой формулы A можно найти такую формулу B, находящуюся в КНФ, что $A \equiv B$. Формула B называется конъюнктивной нормальной формой A.

Доказательство первое. Пусть $A \equiv A_1$ и A_1 не содержит операций $\to, \sim, \oplus, |, \downarrow$. Пусть B_1 – ДНФ для формулы A_1^*. Тогда B_1^* находится в КНФ (по определению) и по принципу двойственности $B_1^* \equiv (A_1^*)^* \equiv A_1 \equiv A$. Значит, B_1^* удовлетворяет требованиям теоремы.

Доказательство второе. Аналогично доказательству теоремы 6.2 о ДНФ. *Доказательство завершено.*

<u>Пример.</u>

Приведём к КНФ формулу:

$(X_2 \downarrow \overline{X}_3) \oplus (X_1 \mid X_2) \equiv (26) \equiv$

$\equiv [\overline{(X_2 \downarrow \overline{X}_3)} \wedge (X_1 \mid X_2)] \vee [(X_2 \downarrow \overline{X}_3) \wedge \overline{(X_1 \mid X_2)}] \equiv (28,\ 27) \equiv$

…

$\equiv (X_2 \vee \overline{X}_3) \wedge (\overline{X}_1 \vee \overline{X}_2)$. - КНФ

6.1.6. Совершенные нормальные формы (совершенные дизъюнктивные нормальные формы и совершенные конъюнктивные нормальные формы)

Пусть формула A зависит от n переменных. Говорят, что A находится в СДНФ относительно этих переменных, если выполняются следующие условия:

а) A находится в ДНФ (дизъюнкция элементарных конъюнкций);

б) в ней нет двух одинаковых дизъюнктивных членов (т.е. элементарных конъюнкций);

в) каждый дизъюнктивный член (элементарная конъюнкция) формулы A является n-членной конъюнкцией, причем на i-ом месте ($1 \leq i \leq n$) этой конъюнкции обязательно стоит либо переменная X_i, либо её отрицание $\overline{X}_i$.

Пример. Пусть (X_1, X_2, X_3) – список переменных. Тогда формулы

$$A(X_1, X_2, X_3) = X_1 \wedge \overline{X}_2 \wedge X_3;$$

$$B(X_1, X_2, X_3) = (\overline{X}_1 \wedge X_2 \wedge X_3) \vee (X_1 \wedge \overline{X}_2 \wedge \overline{X}_3) \vee (X_1 \wedge X_2 \wedge X_3)$$

находятся в СДНФ относительно этого списка переменных. А формула

$$C(X_1, X_2, X_3) = (\overline{X}_2 \wedge X_3) \vee (\overline{X}_3 \wedge X_1 \wedge X_2)$$

не является СДНФ (привести к СДНФ).

Теорема 6.4. Пусть формула A зависит от списка переменных $(X_1, \ldots, X_n)$ и A не тождественно-ложная формула. Тогда существует такая формула B, что $A \equiv B$ и B находится в СДНФ относительно списка этих переменных.

Доказательство. По теореме 6.2 существует формула A_1 такая, что $A \equiv A_1$ и A_1 находится в ДНФ. Пусть A_1 зависит от списка переменных $(X_1, \ldots, X_n)$. Рассмотрим все её элементарные конъюнкции:

1. Пусть в элементарную конъюнкцию одновременно входит какая-нибудь переменная X_i и её отрицание $\overline{X_i}$. Тогда $X_i \wedge \overline{X_i} \equiv Л$. Если эта элементарная конъюнкция единственная, то и вся формула $A \equiv Л$, что невозможно …

Следовательно, имеются другие элементарные конъюнкции:

$$\left(X_i \wedge \overline{X_i} \wedge C\right) \vee D,$$

где C – остальные члены элементарной конъюнкции, D – остальные дизъюнктивные члены всей формулы.

Но поскольку $X_i \wedge \overline{X_i} \wedge C \equiv Л$, то $\left(X_i \wedge \overline{X_i} \wedge C\right) \vee D \equiv D$. Следовательно, рассматриваемую конъюнкцию можно отбросить.

2. Пусть в некоторой элементарной конъюнкции переменная X_i(или $\overline{X_i}$) встречается несколько раз. Тогда в силу идемпотентности (равносильность 9) ...

3. Далее возможны только следующие варианты:

а) элементарная конъюнкция D содержит один разX_i и не содержит ни разу $\overline{X_i}$;

б) элементарная конъюнкция D содержит один раз $\overline{X_i}$ и не содержит ни разу X_i;

в) элементарная конъюнкция D не содержит ниX_i, ни $\overline{X_i}$.

В последнем случае заменяем D на $(D \wedge X_i) \vee (D \wedge \overline{X_i})$ по первой формуле расщепления (равносильность 19) (для выполнения условий а) или б)).

4. Переупорядочим в каждой элементарной конъюнкции её члены так, чтобы на *i*-ом месте в ней стояла X_i или $\overline{X_i}$.

5. Если в преобразованной формуле несколько раз встречается одна и та же элементарная конъюнкция, то, пользуясь равносильностью 10 (идемпотентность $\vee$), выбрасываем все её вхождения, кроме одного.

Доказательство завершено.

<u>Пример.</u> Приведем формулу к СДНФ

$$(X_1 \mid X_2) \oplus X_3 \equiv (26) \equiv [\overline{(X_1 \mid X_2)} \wedge X_3] \vee [(X_1 \mid X_2) \wedge \bar{X}_3] \equiv (27) \equiv$$

$$\equiv [\overline{\overline{(X_1 \wedge X_2)}} \wedge X_3] \vee [\overline{(X_1 \wedge X_2)} \wedge \bar{X}_3] \equiv (21, 7) \equiv$$

$$\equiv [X_1 \wedge X_2 \wedge X_3] \vee [(\bar{X}_1 \vee \bar{X}_2) \wedge \bar{X}_3] \equiv (6) \equiv$$

…

$$\equiv (X_1 \wedge X_2 \wedge X_3) \vee (\bar{X}_1 \wedge X_2 \wedge \bar{X}_3) \vee (\bar{X}_1 \wedge \bar{X}_2 \wedge \bar{X}_3) \vee (X_1 \wedge \bar{X}_2 \wedge \bar{X}_3).$$

Теорема 6.5 (о единственности СДНФ). Если B_1 и B_2 – СДНФ формулы A относительно списка переменных $(X_1,\ldots,X_n)$, то B_1 и B_2 могут отличаться только порядком своих дизъюнктивных членов.

Замечание. Если расширить список переменных $(X_1,\ldots,X_n)$, от которого зависит формула A, новыми переменными, реально в A не входящими, то относительно нового списка будем иметь другую СДНФ.

Пример. Пусть формула A, зависящая от одной переменной, находится в СДНФ относительно списка (X_1)

$$A(X_1) = X_1.$$

Тогда относительно списка переменных (X_1, X_2) СДНФ формулы A будет иметь вид

$$A(X_1, X_2) = (X_1 \wedge X_2) \vee (X_1 \wedge \bar{X}_2).$$

Пусть формула A зависит от n переменных. Тогда говорят, что A находится в СКНФ относительно переменных, если формула A^* находится в СДНФ относительно тех же переменных.

Эквивалентное определение.

Говорят, что A находится в СКНФ относительно списка переменных, если выполняются следующие условия:

а) A находится в КНФ (конъюнкция элементарных дизъюнкций);

б) в ней нет двух одинаковых конъюнктивных членов (т.е. элементарных дизъюнкций);

в) каждый конъюнктивный член (элементарная дизъюнкция) формулы A является n-членной дизъюнкцией, причем на i-ом месте ($1\le i \le n$) этой дизъюнкции обязательно стоит либо переменная X_i, либо её отрицание $\overline{X}_i$.

Пример. Пусть (X_1, X_2, X_3) – список переменных. Тогда формулы

$$A(X_1, X_2, X_3) = \overline{X}_1 \vee \overline{X}_2 \vee X_3;$$

$$B(X_1, X_2, X_3) = (X_1 \vee X_2 \vee X_3) \wedge (X_1 \vee \overline{X}_2 \vee \overline{X}_3) \wedge (X_1 \vee \overline{X}_2 \vee X_3)$$

находятся в СКНФ относительно этого списка переменных. А формула

$$C(X_1, X_2, X_3) = (\overline{X}_1 \vee X_3 \vee X_2) \wedge (\overline{X}_1)$$

не является СКНФ относительно этого списка переменных (привести к СКНФ)

Теорема 6.6. Пусть формула A зависит от списка переменных $(X_1, \ldots, X_n)$ и A не тождественно-истинная. Тогда существует такая формула B, что $A \equiv B$ и B находится в СКНФ относительно списка этих переменных.

Доказательство первое. Пусть A уже находится в КНФ. По условию A на каком-то наборе переменных принимает значение $Л$. Тогда A^* на двойственном наборе принимает значение $И$ и по теореме о СДНФ существует такая формула B_1, что $A^* \equiv B_1$ и B_1 находится в СДНФ. По принципу двойственности $B_1^* = A$ и B_1^* находится в СКНФ.

Доказательство второе. Аналогично доказательству теоремы 6.4. При этом применяются равносильности $\left(X_i \vee \overline{X_i} \vee C\right) \wedge D \equiv D$, $D \equiv \left(D \vee X_i\right) \wedge \left(D \vee \overline{X_i}\right)$ и законы идемпотентности (равносильности 9, 10). *Доказательство завершено.*

Теорема 6.7 (о единственности СКНФ). Если B_1 и B_2 – СКНФ формулы A относительно списка переменных $(X_1, \ldots, X_n)$, то B_1 и B_2 могут отличаться только порядком своих конъюнктивных членов.

Доказательство. При доказательстве можно воспользоваться принципом двойственности

Пример. Приведем формулу к СКНФ

$$(X_1 \vee X_3) \to X_2 \equiv (23) \equiv \overline{(X_1 \vee X_3)} \vee X_2 \equiv (8) \equiv (\overline{X}_1 \wedge \overline{X}_3) \vee X_2 \equiv (5) \equiv$$

…

$$\equiv (\overline{X}_1 \vee X_2 \vee X_3) \wedge (\overline{X}_1 \vee X_2 \vee \overline{X}_3) \wedge (X_1 \vee X_2 \vee \overline{X}_3).$$

Теорема 6.8 (критерий равносильности). Две формулы A_1 и A_2, зависящие от одних и тех же переменных $(X_1, \ldots, X_n)$ и не равные тождественно *Л* (*И*), равносильны в том и только том случае, если они приводятся к СДНФ (СКНФ), отличающимся лишь порядком своих дизъюнктивных (конъюнктивных) членов.

Доказательство.

С одной стороны, если A_1 и A_2 приводятся к одной СДНФ B, то $A_1 \equiv B$ *и* $A_2 \equiv B$. Следовательно, $A_1 \equiv A_2$.

С другой стороны, если $A_1 \equiv A_2$ и B_1 – СДНФ для A_1, а B_2 – СДНФ для A_2, то $B_1 \equiv A_1 \equiv A_2$, т.е. для формулы A_2 будет 2 СДНФ: B_2 и B_1. Тогда в силу теоремы (6.5) B_1 должна отличаться от B_2 только порядком своих дизъюнктивных членов. *Доказательство завершено.*

6.2. Булевы функции

6.2.1. Представление булевой функции формулой алгебры высказываний. Таблицы истинности

Булевой функцией $f(x_1, \ldots, x_n)$ называется произвольная n-местная функция, действующая из множества $\{0, 1\}$ во множество $\{0, 1\}$.

Пусть истинностному значению И – 1,
истинностному значению Л – 0.
Тогда каждой формуле алгебры F – булеву функцию f.

Если формуле F_1 – функция f_1, а формуле F_2 – функция f_2 и $F_1 \equiv F_2$, то $f_1 \equiv f_2$.

Представление булевой функции таблицей истинности. Таблица 6.7

x_1	x_2	x_3	Число	$f(x_1, x_2, x_3)$
0	0	0	0	$f(0,0,0)$
0	0	1	1	$f(0,0,1)$
0	1	0	2	$f(0,1,0)$
0	1	1	3	$f(0,1,1)$
1	0	0	4	$f(1,0,0)$
1	0	1	5	$f(1,0,1)$
1	1	0	6	$f(1,1,0)$
1	1	1	7	$f(1,1,1)$

Пример. $f(x_1,x_2,x_3)=\bar{x}_3 \to (x_1 \sim x_2)$

Функция $f(x_1,x_2,x_3)$ Таблица 6.8

x_1	x_2	x_3	$x_1 \sim x_2$	$\bar{x}_3$	$f(x_1,x_2,x_3)$
0	0	0	1	1	1
0	0	1	1	0	1
0	1	0	0	1	0
0	1	1	0	0	1
1	0	0	0	1	0
1	0	1	0	0	1
1	1	0	1	1	1
1	1	1	1	0	1

Лемма 6.1 (о числе слов). В алфавите $A=\{a_1,\dots,a_r\}$ из r букв можно построить ровно r^m различных слов длины m.

Доказательство. Проведем индукцию по m.

Пусть $k=m=1$. Тогда получаем ровно $r^1=r$ слов длины 1.

Пусть верно для $k=m-1$, т.е. существует ровно r^{m-1} различных слов длины $(m-1)$.

Для $k=m$. Для каждого слова длины $(m-1)$ существует ровно r возможностей добавить одну букву в слово. В итоге получаем слова длины m, число которых равно $r^{m-1}\cdot r=r^{m-1+1}=r^m$. *Доказательство завершено.*

Тогда по лемме 6.1 существует точно $r^m = 2^{2^n}$ различных n-местных булевых функций.

При $n = 1$ получаем $2^{2^n} = 2^{2^1} = 4$ булевы функции.

При $n = 2$ получаем $2^{2^n} = 2^{2^2} = 16$ булевых функций.

Булева функция $f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ *существенно зависит* от переменной x_i, если существует такой набор значений $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n$, что

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

В этом случае x_i называют *существенной переменной*, в противном случае x_i называют *несущественной*, или *фиктивной переменной*.

Пример. Пусть булевы функции $f_1(x_1,x_2), f_2(x_1,x_2)$ заданы следующей таблицей истинности (табл. 6.9)

Функции $f_1(x_1,x_2), f_2(x_1,x_2)$. Таблица 6.9

x_1	x_2	$f_1(x_1,x_2)$	$f_2(x_1,x_2)$
0	0	1	0
0	1	0	1
1	0	1	0
1	1	0	1

x_2 - существенная, а x_1 – фиктивная. $f_1(x_1,x_2)=\bar{x}_2$, $f_2(x_1,x_2)=x_2$.

Булевы функции от одной переменной. Таблица 6.10

	Переменная x	0	1	
Название	Обозначение			Фиктивная
нуль	0	0	0	x
тождественная	x	0	1	
отрицание	$\bar{x}$	1	0	
единица	1	1	1	x

Введем обозначение

$$x^{\sigma} = x\sigma \vee \bar{x}\bar{\sigma},$$

где σ – параметр, равный либо 0, либо 1. Тогда

$$x^{\sigma} = \begin{cases} x, & \sigma = 1, \\ \bar{x}, & \sigma = 0. \end{cases}$$

И при этом, $x^{\sigma} = 1 \Leftrightarrow x = \sigma$, т.е. значение «основания» равно значению «показателя».

Теорема 6.9 (о разложении функции по переменным). Каждую булеву функцию $f(x_1, \ldots, x_n)$ при любом k $(1 \le k \le n)$ можно представить в следующей форме

$$f(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_k)} x_1^{\sigma_1} \wedge \ldots \wedge x_k^{\sigma_k} \wedge f(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n), \quad (6.7)$$

где дизъюнкция берется по всевозможным наборам значений переменных $x_1, \ldots, x_k$.

Доказательство. Рассмотрим произвольный набор значений переменных $(\alpha_1, \ldots, \alpha_n)$ и покажем, что левая и правая части соотношения (6.7) принимают на нем одно и то же значение.

Левая часть

$$f(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) = f(\alpha_1, \ldots, \alpha_n).$$

Правая часть

$$\bigvee_{(\sigma_1,\ldots,\sigma_k)} x_1^{\sigma_1} \wedge \ldots \wedge x_k^{\sigma_k} \wedge f(\sigma_1,\ldots,\sigma_k,x_{k+1},\ldots,x_n) =$$

как только хотя бы один из сомножителей будет равен нулю, вся конъюнкция обратится в нуль. Таким образом, из ненулевых конъюнкций останется лишь та, в которой $\alpha_i = \sigma_i$ и

$$= 0 \vee \ldots \vee 0 \vee \alpha_1^{\alpha_1} \wedge \ldots \wedge \alpha_k^{\alpha_k} \wedge f(\alpha_1,\ldots,\alpha_n) =$$

в силу того, что $\alpha^{\alpha} = 1$, получаем

$$= f(\alpha_1,\ldots,\alpha_n).$$

Доказательство завершено.

Следствие 6.1. Разложение произвольной булевой функции по одной переменной имеет вид

$$f(x_1,x_2,\ldots,x_n) = \bar{x}_1 \wedge f(0,x_2,\ldots,x_n) \vee x_1 \wedge f(1,x_2,\ldots,x_n).$$

Функции $f(0,x_2,\ldots,x_n)$ и $f(1,x_2,\ldots,x_n)$ называются *компонентами разложения*.

Теорема 6.10 (о СДНФ булевой функции). Для любой булевой функции $f(x_1,\ldots,x_n)$, отличной от константы 0, справедливо следующее представление

$$f(x_1,\ldots,x_n)=\bigvee_{\substack{(\sigma_1,\ldots,\sigma_n)\\ f(\sigma_1,\ldots,\sigma_n)=1}} x_1^{\sigma_1}\wedge\ldots\wedge x_n^{\sigma_n}.$$

Доказательство.

...

Такое разложение носит название *совершенной дизъюнктивной нормальной формы булевой функции*..

Теорема 6.11 (о СКНФ булевой функции). Для любой булевой функции $f(x_1, \ldots, x_n)$, отличной от константы 1, справедливо следующее представление

$$f(x_1, \ldots, x_n) = \bigwedge_{\substack{(\sigma_1, \ldots, \sigma_n) \\ f(\sigma_1, \ldots, \sigma_n)=0}} (x_1^{\overline{\sigma_1}} \vee \ldots \vee x_n^{\overline{\sigma_n}}).$$

Доказательство.

Такое разложение носит название *совершенной конъюнктивной нормальной формы булевой функции*.

<u>Пример.</u> Построить СДНФ и СКНФ для $f(x,y)=x\,|\,y$.

СДНФ:

$$f(x,y)=x\,|\,y=(x^0\wedge y^0)\vee(x^0\wedge y^1)\vee(x^1\wedge y^0)=(\bar{x}\wedge\bar{y})\vee(\bar{x}\wedge y)\vee(x\wedge\bar{y}).$$

СКНФ: $f(x,y)=x\,|\,y=x^{\bar{1}}\vee y^{\bar{1}}=x^0\vee y^0=\bar{x}\vee\bar{y}$.

6.2.2. Алгебра Жегалкина

Алгеброй Жегалкина называют алгебру на множестве булевых функций с двумя заданными операциями: конъюнкцией ($\wedge$) и суммой по mod 2 ($\oplus$).

В алгебре Жегалкина выполняются следующие равносильности:

1) $x \wedge y = y \wedge x$ (коммутативность $\wedge$);

2) $x \oplus y = y \oplus x$ (коммутативность $\oplus$);

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

4) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ (ассоциативность $\oplus$);

5) $x \wedge (y \oplus z) = (x \wedge y) \oplus (x \wedge z)$ (дистрибутивность $\wedge$ относительно $\oplus$);

6) $x \wedge x = x$ (идемпотентность $\wedge$);

7) $x \oplus x = 0$;

8) $0 \wedge x = 0$;

9) $0 \oplus x = x$;

10) $1 \wedge x = x$;

11) $\overline{x} = x \oplus 1$;

12) $x \vee y = \overline{(\overline{x} \wedge \overline{y})} = (x \oplus 1) \wedge (y \oplus 1) \oplus 1 = x \wedge y \oplus x \oplus y$.

Многочленом Жегалкина функции $f(x_1, \ldots, x_n)$ называется многочлен вида

$$P(x_1, \ldots, x_n) = a_0 \oplus \sum_{i=1}^{n} a_i \wedge x_i \oplus \sum_{\substack{i,j=1 \\ i \neq j}}^{n} a_{ij} \wedge x_i \wedge x_j \oplus \ldots \oplus a_{12\ldots n} \wedge x_1 \wedge x_2 \wedge \ldots \wedge x_n,$$

где коэффициенты $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n}$ принимают значение 0 или 1.

Теорема 6.12 (теорема Жегалкина). Каждая булева функция $f(x_1, \ldots, x_n)$ может быть представлена в виде многочлена Жегалкина и притом единственным образом, с точностью до порядка слагаемых.

Пример. Пусть дана функция $f(x, y, z) = (\overline{y} \sim x) \vee \overline{z}$. Рассмотрим два способа получения многочлена Жегалкина.

1 способ.

$$
\begin{aligned}
& f(x, y, z) = (\overline{y} \sim x) \vee \overline{z} = [(\bar{y} \wedge x) \vee (\bar{\bar{y}} \wedge \bar{x})] \vee \bar{z} = \\
& = [(\bar{y} \wedge x) \vee (y \wedge \bar{x})] \vee \bar{z} = \\
& \ldots \\
& = (x \oplus y) \vee \bar{z} == (x \oplus y) \wedge \bar{z} \oplus x \oplus y \oplus \bar{z} = \\
& = (x \wedge \bar{z}) \oplus (y \wedge \bar{z}) \oplus x \oplus y \oplus \bar{z} = \\
& \ldots \\
& = x \wedge z \oplus x \oplus y \wedge z \oplus y \oplus x \oplus y \oplus z \oplus 1 = \\
& = 1 \oplus z \oplus xz \oplus yz = P(x, y, z).
\end{aligned}
$$

2 способ.

$$P(x,y,z) = a_0 \oplus a_1 x \oplus a_2 y \oplus a_3 z \oplus a_{12} xy \oplus a_{13} xz \oplus a_{23} yz \oplus a_{123} xyz \qquad (6.8)$$

$f(x,y,z) = (\bar{y} \sim x) \vee \bar{z}$ Таблица 6.12

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

$P(0,0,0) = a_0 = 1 \Rightarrow a_0 = 1,$

$P(0,0,1) = a_0 \oplus a_3 = 0, \quad 1 \oplus a_3 = 0 \Rightarrow a_3 = 1,$

$P(0,1,0) = a_0 \oplus a_2 = 1, \quad 1 \oplus a_2 = 1 \Rightarrow a_2 = 0,$

$P(0,1,1) = a_0 \oplus a_2 \oplus a_3 \oplus a_{23} = 1, \quad 1 \oplus 0 \oplus 1 \oplus a_{23} = 1 \Rightarrow a_{23} = 1,$

$P(1,0,0) = a_0 \oplus a_1 = 1, \quad 1 \oplus a_1 = 1 \Rightarrow a_1 = 0,$

$P(1,0,1) = a_0 \oplus a_1 \oplus a_3 \oplus a_{13} = 1, \quad 1 \oplus 0 \oplus 1 \oplus a_{13} = 1 \Rightarrow a_{13} = 1,$

$P(1,1,0) = a_0 \oplus a_1 \oplus a_2 \oplus a_{12} = 1, \quad 1 \oplus 0 \oplus 0 \oplus a_{12} = 1 \Rightarrow a_{12} = 0,$

$$P(1,1,1) = a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{12} \oplus a_{13} \oplus a_{23} \oplus a_{123} = 0,$$

$$1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus a_{123} = 0 \Rightarrow a_{123} = 0,$$

Таким образом, $P(x, y, z) = 1 \oplus z \oplus xz \oplus yz$.

Функция $f(x_1, \ldots, x_n)$ называется *линейной*, если ее многочлен Жегалкина имеет вид

$$P(x_1, \ldots, x_n) = a_0 \oplus \sum_{i=1}^{n} a_i \wedge x_i . \qquad (6.9)$$

Пример.

1. Константа 0 и константа 1 являются линейными функциями

2. $f_1(x, y) = x \oplus y$ – линейная функция, так как $P_1(x, y) = x \oplus y$;

$f_2(x, y) = x \sim y$ – линейная функция, так как

$P_2(x, y) = P_1^*(x, y) = \overline{(\overline{x} \oplus \overline{y})} = (x \oplus 1) \oplus (y \oplus 1) \oplus 1 = 1 \oplus x \oplus y$.

3. $f_3(x, y) = xy$ – нелинейная функция, так как $P_3(x, y) = xy$;

$f_4(x, y) = x \vee y$ – нелинейная функция, так как

$P_4(x, y) = P_3^*(x, y) = \overline{(\overline{x} \wedge \overline{y})} = (x \oplus 1) \wedge (y \oplus 1) \oplus 1 = xy \oplus x \oplus y \oplus 1 \oplus 1 = x \oplus y \oplus xy$.