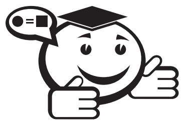
Модули 3.4–3.5. Тавтологии и равносильности

Определим несколько важных видов формул.



Формула называется ***выполнимой****, если существует интерпретация, в которой эта формула истинна.*

Формула называется ***опровержимой****, если существует интерпретация, в которой эта формула ложна.*

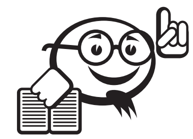
Формула A *называется* ***тавтологией*** *(или* ***тождественно истинной****), если формула истинна во всех интерпретациях, в этом случае мы будем использовать обозначение* $\vDash A$.

Формула называется ***противоречием*** *(или* ***тождественно ложной****), если формула ложна во всех интерпретациях.*

Конечно, каждое из этих определений можно эквивалентным образом сформулировать, используя понятие набора истинностных значений. Например, формула является противоречием, если она ложна независимо от того, какие значения принимают встречающиеся в ней пропозициональные переменные.

Приведем утверждения, которые являются очевидными следствиями данных определений:

- A — тавтология тогда и только тогда, когда A не является опровержимой;
- A — тождественно ложна тогда и только тогда, когда A не является выполнимой;
- A — тавтология тогда и только тогда, когда $\neg A$ — тождественно ложна;
- A — тождественно ложна тогда и только тогда, когда $\neg A$ — тавтология.



Теорема 1. Подстановка вместо пропозициональных переменных. Пусть A — формула, в которую входят только пропозициональные переменные $X_1, X_2, \ldots, X_n$, а B — формула, полученная из A одновременной подстановкой формул C_1, $C_2, \ldots$, C_n вместо $X_1, X_2, \ldots, X_n$ соответственно. Если A — тавтология (противоречие), то B — тавтология (противоречие соответственно).

Доказательство. Рассмотрим произвольную интерпретацию φ, определенную для всех переменных Y_1, $Y_2, \ldots$, Y_k, содержащихся в формулах C_1, $C_2, \ldots$, C_n. Если A — тавтология, то докажем, что B — тавтология. От противного. Пусть Y_1, $Y_2, \ldots$, Y_k — все переменные, содержащиеся в формулах C_1, $C_2, \ldots$, C_n. Только эти переменные являются пропозициональными переменными, присутствующими в формуле B. Рассмотрим интерпретацию φ, определенную для всех переменных Y_1, $Y_2, \ldots$, Y_k, и предположим, что формула B ложна в этой интерпретации. Тогда $\varphi(C_1)$, $\varphi(C_2), \ldots$, $\varphi(C_n)$ — некоторый набор истинностных значений для переменных $X_1, X_2, \ldots, X_n$ соответственно, при которых формула A ложна (так как формула B построена из подформул $C_1, C_2, \ldots, C_n$ таким же образом, как A построена из $X_1, X_2, \ldots, X_n$). Получили противоречие. Случай, когда A — противоречие, доказывается аналогично.

Пусть имеется некоторая тавтология A. В силу теоремы 1 любая подстановка произвольных формул в формулу A вместо пропозициональных переменных дает тавтологию. Поэтому тавтологии являются схемами истинных высказываний, в которых выражаются ***логические законы***.

Пример 1

Перечислим некоторые важные тавтологии (A, B, C — произвольные формулы):

1. $\vDash A \vee \neg A$ (***закон исключенного третьего*** или ***tertium nondatur***);
2. $\vDash A \supset A$;
3. $\vDash A \supset (B \supset A)$;
4. $\vDash (A \supset B) \supset \big((B \supset C) \supset (A \supset C)\big)$ (***цепное рассуждение***);
5. $\vDash \big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$;
6. $\vDash (A \& B) \supset A$; $(A \& B) \supset B$;
7. $\vDash A \supset \big(B \supset (A \& B)\big)$;
8. $\vDash A \supset (A \vee B)$; $B \supset (A \supset B)$;
9. $\vDash (\neg B \supset \neg A) \supset \big((\neg B \supset A) \supset B\big)$;
10. $\vDash \big((A \supset B) \supset A\big) \supset A$ (***закон Пирса***);
11. $\vDash \neg(B \& \neg B)$ (***закон противоречия***);
12. $\vDash (A \supset B) \vee (B \supset A)$.

Тавтология 12 выражает на первый взгляд парадоксальный закон: для любых высказываний A и B хотя бы одна из импликаций $A \supset B$ и $B \supset A$ является истинной.

Каждую из этих тавтологий можно обосновать, например, составив таблицу и вычислив по ней значение формулы, считая A, B и C — пропозициональными переменными.

Использование таблиц истинности является универсальным способом для установления того, является ли формула выполнимой, опровержимой, тавтологией или противоречием. Но если в формуле более трех переменных, то по мере увеличения количества переменных построение таблицы человеком становится очень трудоемким и невозможным. Использование компьютерных программ позволяет увеличить количество переменных в рассматриваемых формулах, но тоже до некоторого предела.

Тавтологичность формул некоторого вида можно установить с помощью доказательства от противного. Подробно метод доказательства от противного описан в параграфе 7.3 главы 7.

Покажем, как использовать доказательство от противного для некоторых формул $A = B \supset C$. Вы предполагаете, что формула A ложна и, делая отсюда выводы об истинном значении подформул формулы A, приходите к противоречию или определяете значения переменных, при которых формула ложна. Для формул указанного вида ложность $B \supset C$ однозначно определяет: B — истинна, а C — ложна. Этот метод эффективней, чем построение таблицы истинности, в том случае, когда истинностный анализ подформул можно произвести однозначно или с небольшим перебором.

Задача 1. Является ли формула $\big((P \supset Q)\&P\big) \supset Q$ тавтологией?

Решение. Предположим, что $\big((P \supset Q)\&P\big) \supset Q$ ложна при некоторых значениях пропозициональных переменных P и Q. Представим наши рассуждения в виде таблицы. Каждая следующая строчка таблицы есть логическое следствие предыдущей строки.

$\big((P \supset Q)\&P\big) \supset Q =$ **Л**	
$(P \supset Q)\&P =$ **И**	$Q =$ **Л**
$P \supset Q =$ **И**, $P =$ **И**	
И $\supset Q =$ **И** (подставили в формулу **И** вместо P)	
$\boldsymbol{Q} =$ **И**	

Получили противоречие (Q = **И** и Q = **Л** одновременно), следовательно, исходное предположение о ложности $\big((P \supset Q)\&P\big) \supset Q$ неверно, и получаем $\vDash \big((P \supset Q)\&P\big) \supset Q$.

Задача 2. Является ли тавтологией формула

$$\big((P \supset Q)\&(\neg R \supset \neg Q)\&(T \supset \neg R)\big) \supset (P \supset \neg T)?$$

Решение. Предположим, что формула ложна при некоторых значениях пропозициональных переменных P, Q, R и T.

$\big((P \supset Q)\&(\neg R \supset \neg Q)\&(T \supset \neg R)\big) \supset (P \supset \neg T) =$ **Л**	
$(P \supset Q)\&(\neg R \supset \neg Q)\&(T \supset \neg R) =$ **И**	$P \supset \neg T =$ **Л**
$P \supset Q =$ **И**, $\neg R \supset \neg Q =$ **И**, $T \supset \neg R =$ **И**	$P =$ **И**, $\neg T =$ **Л**
И $\supset Q =$ **И**, $\neg R \supset \neg Q =$ **И**, **И** $\supset \neg R =$ **И** (подставили в формулы **И** вместо P и T)	
$Q =$ **И**, $\neg R =$ **И**, $\neg R \supset \neg Q =$ **И**	
И $\supset \neg$**И** $=$ **И** (подставили в формулы **И** вместо Q и $\neg R$)	
И $\supset$ **Л** $=$ **И**. Но это невозможно!	

Пришли к противоречию, следовательно, исходная формула — тавтология.

Задача 3. Является ли формула $\big((P \supset Q)\&P\big) \supset (Q \supset \neg P)$ тавтологией?

Решение. Предположим, что формула $\big((P \supset Q)\&P\big) \supset (Q \supset \neg P)$ ложна при некоторых значениях пропозициональных переменных P и Q.

Получили значения переменных Q = **И** и P = **И**, при которых формула ложна:

$$\big((P \supset Q)\&P\big) \supset (Q \supset \neg P) = \textbf{Л},$$

следовательно, эта формула не является тавтологией.

$\big((P \supset Q)\&P\big) \supset (Q \supset \neg P)$ = **Л**	
$(P \supset Q)\&P$ = **И**	$Q \supset \neg P$ = **Л**
$P \supset Q$ = **И**, P = **И**	Q = **И**, $\neg P$ = **Л**
И $\supset Q$ = **И** (подставили в формулу **И** вместо P)	
Q = **И**	

На множестве пропозициональных формул определим отношение эквивалентности.

Формулы A и B называются ***равносильными****, если эти формулы принимают одинаковые истинностные значения в любой интерпретации. Равносильность формул обозначается как $A \equiv B$.*

Установить, равносильные формулы или нет, мы можем с помощью таблицы истинности, построенной сразу для двух формул.

Пример 2

Рассмотрим формулы $\neg X \vee \neg Y$ и $\neg(X\&Y)$.

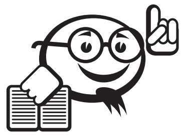
X	Y	$\neg X$	$\neg Y$	$\neg X \vee \neg Y$	$X\&Y$	$\neg(X\&Y)$
И	**И**	**Л**	**Л**	**Л**	**И**	**Л**
И	**Л**	**Л**	**И**	**И**	**Л**	**И**
Л	**И**	**И**	**Л**	**И**	**Л**	**И**
Л	**Л**	**И**	**И**	**И**	**Л**	**И**

Столбцы пятый и седьмой совпадают, поэтому $\neg X \vee \neg Y \equiv \neg(X\&Y)$.

Замечание 1. Из определений тавтологии и равносильности сразу следует, что $A \equiv B$ тогда и только тогда, когда $\models A \sim B$.

Теорема 2. Пусть формулы A и B равносильны, причем $X_1, X_2, \ldots, X_n$ — список всех переменных, входящих в A или в B. Пусть формулы D и E получены из A и B одновременной подстановкой формул $C_1, C_2, \ldots, C_n$ вместо $X_1, X_2, \ldots, X_n$ соответственно. Тогда $D \equiv E$.

Доказательство следует из предыдущего замечания и теоремы 1.



Теорема 3. Основные равносильности. Для любых формул A, B, C справедливы следующие равносильности:

1. $A\&B \equiv B\&A$ (коммутативность &);
2. $A\&A \equiv A$ (идемпотентность &);
3. $A\&(B\&C) \equiv (A\&B)\&C$ (ассоциативность &);
4. $A \vee B \equiv B \vee A$ (коммутативность $\vee$);
5. $A \vee A \equiv A$ (идемпотентность $\vee$);
6. $A \vee (B \vee C) \equiv (A \vee B) \vee C$ (ассоциативность $\vee$);
7. $A \vee (B\&C) \equiv (A \vee B)\&(A \vee C)$ (дистрибутивность $\vee$ относительно &);
8. $A\&(B \vee C) \equiv (A\&B) \vee (A\&C)$ (дистрибутивность & относительно $\vee$);
9. $A\&(A \vee B) \equiv A$ (первый закон поглощения);
10. $A \vee (A\&B) \equiv A$ (второй закон поглощения);
11. $\neg\neg A \equiv A$ (снятие двойного отрицания);
12. $\neg(A\&B) \equiv \neg A \vee \neg B$ (первый закон де Моргана);
13. $\neg(A \vee B) \equiv \neg A\&\neg B$ (второй закон де Моргана);
14. $A \equiv (A\&B) \vee (A\&\neg B)$ (первый закон расщепления);
15. $A \equiv (A \vee B)\&(A \vee \neg B)$ (второй закон расщепления).
16. $A \sim B \equiv (A \supset B)\&(B \supset A) \equiv (A\&B) \vee (\neg A\&\neg B)$;
17. $A \supset B \equiv \neg A \vee B \equiv \neg(A\&\neg B)$;
18. $A \vee B \equiv \neg A \supset B \equiv \neg(\neg A\&\neg B)$;
19. $A\&B \equiv \neg(A \supset \neg B) \equiv \neg(\neg A \vee \neg B)$;
20. $A \supset B \equiv \neg B \supset \neg A$ (закон контрапозиции).

Равносильности 16–19 показывают, что одни связки могут быть выражены через другие.

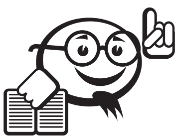
Все равносильности теоремы 3 легко доказываются либо с помощью таблиц истинности, либо без них. В качестве примера докажем 7 с помощью таблицы истинности.

Докажем равносильность 12 без таблицы истинности. Пусть на некотором наборе истинностных значений переменных формула $\neg(A\&B)$ принимает значение **Л**. Тогда формула $A\&B$ принимает значение **И**, а поэтому обе формулы A и B принимают значение **И**. Но в этом случае, очевидно, и правая часть равносильности 12 принимает значение **Л**. И наоборот, пусть формула $\neg A \vee \neg B$ принимает значение **Л**. Тогда формулы $\neg A$, $\neg B$ принимают значение **Л**, а формулы A, B — значение **И**. Очевидно, что и левая часть равносильности 12 принимает значение **Л**.

A	B	C	$B\&C$	$A \vee (B\&C)$	$A \vee B$	$A \vee C$	$(A \vee B)\&(A \vee C)$
И	**И**	**И**	**И**	**И**	**И**	**И**	**И**
И	**И**	**Л**	**Л**	**И**	**И**	**И**	**И**
И	**Л**	**И**	**Л**	**И**	**И**	**И**	**И**
И	**Л**	**Л**	**Л**	**И**	**И**	**И**	**И**
Л	**И**	**И**	**И**	**И**	**И**	**И**	**И**
Л	**И**	**Л**	**Л**	**Л**	**И**	**Л**	**Л**
Л	**Л**	**И**	**Л**	**Л**	**Л**	**И**	**Л**
Л	**Л**	**Л**	**Л**	**Л**	**Л**	**Л**	**Л**

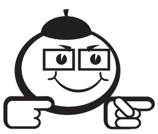
Замечание 2. Пусть символ $\bullet$ обозначает бинарную операцию «исключительное или», которая выдает истину только в случае, когда один из операндов имеет значение истина. Тогда $A \bullet B \equiv (A\&\neg B) \vee (B\&\neg A)$, что можно проверить с помощью таблицы истинности.

Используя известные равносильности, можно получать новые. Об этом говорит следующая теорема.



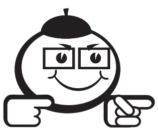
Теорема 4. Правило равносильных преобразований. Пусть C_A — формула, содержащая A в качестве своей подформулы. Пусть C_B получается из C_A заменой A в этом вхождении на B. Тогда, если $A \equiv B$, то $C_A \equiv C_B$.

Для доказательства нам потребуются две леммы.



Лемма 1. Пусть $A \equiv B$ и C — произвольная формула. Тогда $\neg A \equiv \neg B$, $A\&C \equiv B\&C$, $C\&A \equiv C\&B$, $A \vee C \equiv B \vee C$, $C \vee A \equiv C \vee B$, $A \supset C \equiv B \supset C$, $C \supset A \equiv C \supset B$, $A \sim C \equiv B \sim C$, $C \sim A \equiv C \sim B$.

Доказательство. Докажем, например, равносильность $A \supset C \equiv B \supset C$. Пусть на произвольном наборе истинностных значений пропозициональных переменных формулы A и B принимают одинаковое истинностное значение (скажем, s). Пусть t — значение C на этом распределении истинностных значений. Обе части рассматриваемой равносильности принимают одно и то же значение $s \supset t$.



Лемма 2. Пусть $A \equiv B$ и C — формула, в которой выделено одно вхождение некоторой переменной X. Пусть C_A получается из C заменой этого вхождения X на A, а C_B — из C заменой того же вхождения X на B. Тогда $C_A \equiv C_B$.

Доказательство леммы будет проведено в параграфе 7.2 главы 7 с помощью математической индукции по построению.

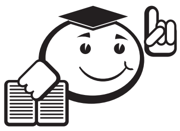
Доказательство теоремы 4. Рассмотрим произвольную переменную X и получим формулу C из C_A заменой A на X. Будем считать это вхождение X в C

выделенным. Тогда C, A, B, C_A, C_B удовлетворяют условиям леммы 2, а значит, $C_A \equiv C_B$.

Замечание 3. Из теоремы 4 мы сразу получаем несколько полезных следствий. Например, пусть имеется формула, содержащая только n штук операций конъюнкции. Если $n > 1$, то необходимо присутствие скобок в формуле, чтобы показать, в каком порядке выполняется бинарная операция конъюнкции. В силу ассоциативности & (равносильность 3 из теоремы 3) сразу получаем, что истинностное значение исходной n-кратной конъюнкции не зависит от расстановки скобок. Поэтому при записи такой формулы, скажем $A\&B\&C\&D\&E$, можно вообще не использовать скобки. Так как n-кратная дизъюнкция также ассоциативна, то мы можем использовать n-кратную дизъюнкцию также без скобок.

Замечание 4. Для каждой формулы можно указать равносильную ей формулу, не содержащую логических символов $\supset$ и $\sim$. В самом деле, опираясь на правило равносильных преобразований, можно в исходной формуле каждую подформулу вида $A \sim B$ заменить на $(A\&B) \vee (\neg A\&\neg B)$, а каждую подформулу вида $A \supset B$ — на $\neg A \vee B$ (см. равносильности 16 и 17 теоремы 3).

Замечание 5. Возможно, вы заметили, что основные равносильности логики высказываний и основные тождества алгебры множеств выражаются одними и теми же законами. Это не случайно: и алгебра высказываний, и алгебра множеств — это различные варианты математической структуры, называемой ***булевой алгеброй*** (см. например, [1] или любой учебник по дискретной математике).



Список литературы по модулям

[1] Игошин В. И. Математическая логика и теория алгоритмов / В. И. Игошин. — 2-е изд., стереотип. — М. : Академия, 2008. — 448 с.