Д. Д. Изаак

# МАТЕМАТИЧЕСКАЯ ЛОГИКА

Курс лекций

Орск, 2013

*УДК 510.6*
*ББК 22.12*
*И32*

**Научный редактор**
***Бонди И.Л.**, кандидат физико-математических наук*

**И32 Изаак, Д. Д. Математическая логика:** курс лекций / Д. Д. Изаак.– Орск: Типография «Бланк», 2013. – 78 с. – ISBN 978-5-9905230-1-2.

*Данный курс лекций предназначен, прежде всего, для студентов дневных отделений, изучающих математическую логику и теорию алгоритмов, но также может быть интересен и студентам заочной формы обучения. Кроме того, данный материал может заинтересовать аспирантов и преподавателей.*

*В первой и второй главах данного курса лекций приводится содержательное изложение основ математической логики. Третья и четвертая главы содержат формальное (аксиоматическое) изложение того же материала. Прикладное исчисление предикатов, рассмотренное в пятой главе, также излагается аксиоматически. Но в отличие от предыдущих разделов, где изучались только логические законы, прикладное исчисление предикатов позволяет наряду с логическими законами изучать и другие математические законы. В шестой главе приводится интуитивное понятие алгоритма, возникшее еще в Древней Греции, которым пользуются до сих пор. Кроме того, приводится два строгих уточнения этого понятия, одно из которых опирается на машину Тьюринга, появление которой послужило толчком к созданию первых ЭВМ.*

ISBN 978-5-9905230-1-2

# ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

Данный курс лекций предназначен, прежде всего, для студентов дневных отделений, изучающих математическую логику и теорию алгоритмов, но также может быть интересен и студентам заочной формы обучения. Кроме того, данный материал может заинтересовать аспирантов и преподавателей. Автором были рассмотрены следующие разделы: «***Алгебра высказываний***», «***Алгебра предикатов***», «***Исчисление высказываний***», «***Исчисление предикатов***», «***Прикладное исчисление предикатов***», «***Алгоритмы и рекурсивные функции***».

В первой и второй главах данного курса лекций приводится содержательное изложение основ математической логики. Третья и четвертая главы содержат формальное (аксиоматическое) изложение того же материала. Прикладное исчисление предикатов, рассмотренное в пятой главе, также излагается аксиоматически. Но в отличие от предыдущих разделов, где изучались только логические законы, прикладное исчисление предикатов позволяет наряду с логическими законами изучать и другие математические законы. В шестой главе приводится интуитивное понятие алгоритма, возникшее еще в Древней Греции, которым пользуются до сих пор. Кроме того, приводится два строгих уточнения этого понятия, одно из которых опирается на машину Тьюринга, появление которой послужило толчком к созданию первых ЭВМ.

Логика, наука о мышлении, зародилась еще в древней Греции. Основной вклад в ее изучение внес философ и ученый Аристотель. На границе XVII и XVIII веков у немецкого философа и математика Лейбница появилась идея заменить рассуждения вычислениями, то есть применить математические методы к изучению мышления.

В XIX веке оформился раздел математической логики «Алгебра высказываний». В нем элементарные высказывания обозначались буквами, союзы и отрицание – символами логических операций, а сложные высказывания – формулами. Законы логики изучались подобно алгебраическим законам. Большую роль в формировании этого раздела сыграл английский математик и логик Джордж Буль, отец известной писательницы Этель Войнич – автора романа «Овод».

Позже в язык математической логики были введены такие понятия как предметные переменные, предикаты, то есть утверждения о предметных переменных, а также кванторы $\forall$ и $\exists$, заменившие словесные выражения «для всех» и «существует». Так появился раздел формальной логики, названный «Алгеброй предикатов».

Немецкий математик Давид Гильберт (1862-1943) предложил другой подход к изучению законов логики. Некоторые законы логики, записанные формулами, принимались без доказательства, то есть объявлялись аксиомами. Постулировались также «правила вывода», которые позволяли из аксиом получать остальные «доказуемые формулы». Такой подход получил название аксиоматического. «Исчисление высказываний», «исчисление предикатов» и «прикладное исчисление предикатов» – разделы математической логики, изложенные аксиоматически.

Интуитивное понятие алгоритма было известно еще со времен Евклида. Алгоритм – это универсальный метод решения задач определенного типа. В начале XX века появилась необходимость уточнить понятие «алгоритм». Это было связано с тем, что не все массовые задачи имеют алгоритмическое решение. Было предложено несколько строгих подходов, один из которых опирается на понятие «машина Тьюринга». Это теоретическое понятие было предложено английским математиком Тьюрингом в 1937 году за 9 лет до появления первой ЭВМ.

# ГЛАВА 1
# АЛГЕБРА ВЫСКАЗЫВАНИЙ

## 1.1. Введение

**Определение 1.1.1.** Под высказыванием понимается любое предложение, о котором можно однозначно сказать, истинно оно или ложно.

**Примеры.**

«Закройте дверь», «$x > 3$», «$\sqrt{55}$» – не высказывания.

«Лондон – столица Англии», «$2 \geq 2$», «Заяц – хищное животное» – высказывания, первые два из которых истинны, последнее – ложно.

Элементарные высказывания обозначают большими латинскими буквами без индексов или с индексами внизу. Такие буквы называются пропозициональными. $A, B, C, \ldots, Z, A_1, B_1, \ldots Z_1, A_2, \ldots$ .

## 1.2. Логические операции алгебры высказываний

**Конъюнкция** соответствует союзам «и», «а», «но».

Ее обозначают: $A \wedge B$, $AB$ ($A$, $B$ – сомножители).

**Пример.** Мой брат работает в школе и учится заочно.

**Определение 1.2.1.** Конъюнкция двух высказываний истинна, если оба эти высказывания истинны, конъюнкция двух высказываний ложна, если хотя бы одно из этих высказываний ложно.

**Дизъюнкция** соответствует союзу «или», когда он понимается не разделительно.

Обозначается: $A \vee B$ ($A$, $B$ – слагаемые).

**Примеры.**

Я завтра пойду в кино или в театр (что-то одно, разделительный смысл).

Если завтра будет плохая погода или я заболею, то наша прогулка не состоится (не разделительный смысл).

**Определение 1.2.2.** Дизъюнкция двух высказываний истинна, если хотя бы одно из высказываний истинно, дизъюнкция ложна, если оба высказывания ложны.

**Импликация** соответствует двойному союзу «если…то…».

Обозначается: $A \to B$ ($A$ – посылка, $B$ – заключение.)

**Пример.** Если сдашь все экзамены, мы купим тебе велосипед.

**Определение 1.2.3.** Импликация двух высказываний истинна, если посылка ложна или заключение истинно. Импликация ложна, если посылка истинна, а заключение ложно.

**Эквиваленция** соответствует союзу «тогда и только тогда, когда».

Обозначается: $A \sim B$ .

**Пример.** Завтра будет пятница тогда и только тогда, когда вчера была среда.

**Определение 1.2.4.** Эквиваленция двух высказываний истинна, если высказывания принимают одинаковые значения, и ложна, если высказывания принимают различные значения.

**Отрицание** соответствует частице «не».

Обозначается: $\overline{A}$.

**Пример.** Я не живу в Орске.

**Определение 1.2.5.** Отрицание высказывания истинно, если само высказывание ложно, отрицание высказывания ложно, если само высказывание истинно.

Укажем все вышесказанное более компактно в виде таблицы истинностных значений.

| | | | | |
|---|---|---|---|---|
| $A$ | $И$ | $И$ | $Л$ | $Л$ |
| $B$ | $И$ | $Л$ | $И$ | $Л$ |
| $AB$ | $И$ | $Л$ | $Л$ | $Л$ |
| $A\vee B$ | $И$ | $И$ | $И$ | $Л$ |
| $A\to B$ | $И$ | $Л$ | $И$ | $И$ |
| $A\sim B$ | $И$ | $Л$ | $Л$ | $И$ |

| | | |
|---|---|---|
| $A$ | $И$ | $Л$ |
| $\overline{A}$ | $Л$ | $И$ |

## 1.3. Формулы алгебры высказываний

**Определение 1.3.1.** Элементарное высказывание или сложное высказывание, составленное из элементарных с помощью логических операций $\wedge$, $\vee$, $\to$, $\sim$, $-$, называется формулой алгебры высказываний.

Формула алгебры высказываний задает функцию, принимающую истинное или ложное значение в зависимости от значений, входящих в формулы букв. Если порядок выполнения операций не указан скобками, то операции выполняются в следующем порядке: $\wedge$, $\vee$, $\to$, $\sim$. Знак отрицания, стоящий над частью формулы, играет попутно и роль скобок.

**Пример.** Вычислить значение формулы $A \vee B \wedge C \to \overline{\overline{A} \sim B}$ при $A = Л$, $B = И$, $C = Л$.

$$A \vee B \wedge C \to \overline{\overline{A} \sim B} = Л \vee Л \to Л = Л \to Л = И .$$

**Определение 1.3.2.** Формула алгебры высказываний называется тождественно истинной, если она принимает значение «*И*» при любых значениях входящих в нее букв.

**Пример.** $X \vee \overline{X}$ – тождественно истинна.

**Определение 1.3.3.** Формула алгебры высказываний называется тождественно ложной, если она принимает значение ложь при всех значениях входящих в нее букв.

**Пример.** $X\overline{X}$ – тождественно ложна.

**Определение 1.3.4.** Формула алгебры высказываний называется выполнимой, если она принимает значение «*И*» хотя бы при некоторых значениях входящих в нее букв.

$\overline{X} \to \overline{Y}$ – выполнима, так как при $X = Л$, $Y = Л$, $\overline{X} \to \overline{Y} = И$.

**Определение 1.3.5.** Формула алгебры высказываний называется опровержимой, если она принимает значение «*Л*», хотя бы при некоторых значениях входящих в нее букв.

$\overline{X} \to \overline{Y}$ – опровержима, так как при $X = Л$, $Y = И$, $\overline{X} \to \overline{Y} = Л$.

**Определение 1.3.6.** Формула *U* сильнее формулы *V*, если всякий раз, когда формула *U* принимает значение «*И*», формула *V* также принимает значение «*И*».

Обозначение: $U \Rightarrow V$.

$U \Rightarrow V$ тогда и только тогда, когда $U \to V$ тождественно истинна.

**Пример.** $AB \Rightarrow A \vee B$.

**Определение 1.3.7.** Две формулы *U* и *V* равносильны, если эти формулы принимают одинаковые значения при любых значениях входящих в них букв.

Обозначение: $U \Leftrightarrow V$ или $U = V$.

$U \Leftrightarrow V$ тогда и только тогда, когда $U \Rightarrow V$ и $V \Rightarrow U$.

$U \Leftrightarrow V$ тогда и только тогда, когда $U \sim V$ тождественно истинна.

## 1.4. Основные равносильности алгебры высказываний

1. $X \vee Y = Y \vee X$ (коммутативность $\vee$)
2. $XY = YX$ (коммутативность $\wedge$)
3. $(X \vee Y) \vee Z = X \vee (Y \vee Z)$ (ассоциативность $\vee$)
4. $(XY)Z = X(YZ)$ (ассоциативность $\wedge$)
5. $X(Y \vee Z) = XY \vee XZ$ (дистрибутивность $\wedge$ относительно $\vee$)
6. $X \vee YZ = (X \vee Y)(X \vee Z)$ (дистрибутивность $\vee$ относительно $\wedge$)
7. $X \vee Л = X$ (ложное слагаемое можно опустить)
8. $XИ = X$ (истинный сомножитель можно опустить)
9. $X \vee И = И$ (если хотя бы 1 из слагаемых истинно, то дизъюнкция истинна)
10. $XЛ = Л$ (если хотя бы 1 из сомножителей ложен, то конъюнкция ложна)
11. $X \vee XY = X$ (закон поглощения)
12. $X(X \vee Y) = X$ (закон поглощения)
13. $X \vee X = X$ (идемпотентность $\vee$)
14. $XX = X$ (идемпотентность $\wedge$)
15. $X \vee \overline{X} = И$ (закон исключения третьего)
16. $X\overline{X} = Л$ (закон противоречия)
17. $\overline{\overline{X}} = X$ (закон двойного отрицания)
18. $\overline{XY} = \overline{X} \vee \overline{Y}$ (отрицание конъюнкции равносильно дизъюнкции отрицаний)
19. $\overline{X \vee Y} = \overline{X}\ \overline{Y}$ (отрицание дизъюнкции равносильно конъюнкции отрицаний) (законы де Моргана)

20. $X \to Y = \overline{X} \vee Y$ (избавление от →)
21. $\overline{X \to Y} = X\overline{Y}$ (избавление от отрицания →)
22. $X \sim Y = (X \to Y)(Y \to X)$ (избавление от ~)
23. $X \sim Y = XY \vee \overline{X}\ \overline{Y}$ (избавление от ~)

## 1.5. Способы доказательства равносильностей

1. Табличный способ. Чтобы доказать, что две формулы $U$ и $V$ равносильны, достаточно составить таблицы истинностных значений для этих формул и эти таблицы сравнить.

**Пример.**

18. $\overline{XY} = \overline{X} \vee \overline{Y}$

| | | | | |
|---|---|---|---|---|
| $X$ | *И* | *И* | *Л* | *Л* |
| $Y$ | *И* | *Л* | *И* | *Л* |
| $\overline{XY}$ | *Л* | *И* | *И* | *И* |
| $\overline{X} \vee \overline{Y}$ | *Л* | *И* | *И* | *И* |

2. Способ допущений. Чтобы доказать, что две формулы $U$ и $V$ равносильны, достаточно сперва предположить, что формула $U$ истинна (ложна) и доказать, что $V$ истинна (ложна). Затем мы должны предположить, что формула $V$ истинна (ложна) и доказать, что $U$ истинна (ложна).

**Примеры.**

19. $\overline{X \vee Y} = \overline{X}\ \overline{Y}$

I. Пусть $\overline{X \vee Y} = И$.
Тогда $X \vee Y = Л$;
$X = Л$, $Y = Л$;
$\overline{X}\ \overline{Y} = И$.

II. Пусть $\overline{X}\ \overline{Y} = И$.
Тогда $\overline{X} = И$; $\overline{Y} = И$;
$X = Л$, $Y = Л$;
$\overline{X \vee Y} = И$.

20. $X \to Y = \overline{X} \vee Y$

I. Пусть $X \to Y = Л$.
Тогда $X = И$, $Y = Л$;
$\overline{X} \vee Y = Л$.

II. Пусть $\overline{X} \vee Y = Л$.
Тогда $\overline{X} = Л$, $Y = Л$;
$X = И$;
$X \to Y = Л$.

6. $X \vee YZ = (X \vee Y)(X \vee Z)$

I. Пусть $X \vee YZ = Л$.
Тогда $X = Л$; $YZ = Л$;
а) $Y = Л$ или б) $Z = Л$
$\underbrace{(X \vee Y)}_{Л}(X \vee Z) = Л$ $\quad$ $(X \vee Y)\underbrace{(X \vee Z)}_{Л} = Л$

II. Пусть $(X \vee Y)(X \vee Z) = Л$.
а) $X \vee Y = Л$ или б) $X \vee Z = Л$
$X = Л$, $Y = Л$; $\quad$ $X = Л$, $Z = Л$;
$X \vee YZ = Л$. $\quad$ $X \vee YZ = Л$.

3. <u>Способ цепочки</u>. Чтобы доказать, что две формулы $U$ и $V$ равносильны, достаточно составить цепочку равносильных между собой формул, используя ранее доказанные равносильности, таким образом, чтобы первая и последняя формулы цепочки совпадали бы с данными формулами $U$ и $V$.

**Примеры.**

21. $\overline{X \to Y} = X\overline{Y}$

$$\overline{X \to Y} = \overline{\overline{X} \vee Y} = \overline{\overline{X}}\,\overline{Y} = X\overline{Y}$$

11. $X \vee XY = X$

$$X \vee XY = XИ \vee XY = X(И \vee Y) = X(Y \vee И) = XИ = X$$

## 1.6. Дизъюнктивные и конъюнктивные нормальные формы. (ДНФ и КНФ)

**Определение 1.6.1.** Элементарной конъюнкцией называют конъюнкцию элементарных высказываний или их отрицаний (в частности допускается элементарная конъюнкция с одним сомножителем).

**Пример.** $A\overline{B}$, $X\,\overline{Y}\,\overline{Z}$, $\overline{C}\,\overline{D}$, $E$.

**Определение 1.6.2.** Элементарной дизъюнкцией называют дизъюнкцию элементарных высказываний или их отрицаний (в частности допускается элементарная дизъюнкция с одним слагаемым).

**Пример.** $\overline{X} \vee \overline{Y} \vee Z$, $A \vee \overline{B}$, $\overline{C}$, $\overline{A} \vee B \vee C \vee \overline{D}$.

**Определение 1.6.3.** Дизъюнктивной нормальной формой формулы $U$ называется равносильная ей формула, представляющая собой дизъюнкцию элементарных конъюнкций.

**Пример.** $U = A\overline{B} \vee ABC \vee \overline{A}B\overline{C} \vee C$.

**Определение 1.6.4.** Конъюнктивной нормальной формой формулы $U$ называется равносильная ей формула, представляющая собой конъюнкцию элементарных дизъюнкций.

**Пример.** $U = (\overline{X} \vee \overline{Y} \vee Z)(X \vee \overline{Z})\overline{Y}$.

Каждая формула алгебры высказываний имеет как ДНФ, так и КНФ.

<u>*Способ нахождения ДНФ.*</u>

1. Избавляемся от $\to$ и $\sim$ с помощью основных равносильностей (20 – 23).
2. Переносим знак отрицания на элементарные высказывания с помощью законов де Моргана (18 – 19).
3. Избавляемся от двойных отрицаний с помощью соответствующего закона (17).
4. Используем первый дистрибутивный закон ($X(Y \vee Z) = XY \vee XZ$) в сочетании с коммутативным и ассоциативным законами (1 – 4).

**Пример.**

Найти и упростить ДНФ.

$$(\overline{X} \to Z)(X \to \overline{Y}Z) = (\overline{\overline{X}} \vee Z)(\overline{X} \vee \overline{Y}Z) = (X \vee Z)(\overline{X} \vee \overline{Y}Z) = X\overline{X} \vee X\overline{Y}Z \vee \overline{X}Z \vee Z\overline{Y}Z =$$
$$= X\overline{Y}Z \vee \overline{X}Z \vee \overline{Y}Z = \overline{X}Z \vee \overline{Y}Z$$

*Способ нахождения КНФ.*

1. Избавляемся от $\to$ и $\sim$.
2. Переносим знак отрицания на элементарные высказывания с помощью законов де Моргана.
3. Избавляемся от двойных отрицаний.
4. Используем второй дистрибутивный закон ($X \vee YZ = (X \vee Y)(X \vee Z)$) в сочетании с коммутативным и ассоциативным законами.

**Пример.**

Найти и упростить КНФ.

$$(\overline{X} \to Z)(X \to \overline{Y}Z) = (\overline{\overline{X}} \vee Z)(\overline{X} \vee \overline{Y}Z) = (X \vee Z)(\overline{X} \vee \overline{Y}Z) =$$
$$(X \vee Z)(\overline{X} \vee \overline{Y})(\overline{X} \vee Z) = (\overline{X} \vee \overline{Y})(Z \vee X\overline{X}) = (\overline{X} \vee \overline{Y})Z$$

*Критерии тождественной истинности*
*и тождественной ложности формул.*

**Теорема 1.6.1. (Критерий тождественной истинности.)**

Формула алгебры высказываний тождественно истинна тогда и только тогда, когда каждый сомножитель ее КНФ содержит некоторую букву одновременно с ее отрицанием.

Доказательство.

Необходимость. Дано: каждый сомножитель КНФ содержит некоторую букву, одновременно с ее отрицанием. Доказать: формула тождественно истинна. В силу закона исключения третьего каждый из сомножителей содержит по истинному слагаемому, значит, каждый сомножитель будет истинным, а, следовательно, вся КНФ истинна.

Например:

$$U = (A \vee \overline{B} \vee \overline{A} \vee C)(\overline{A} \vee B \vee \overline{B})(\overline{C} \vee C \vee \overline{B}) = И\,.$$

Достаточность. Дано: формула тождественно истинна. Доказать: каждый сомножитель КНФ содержит некоторую букву одновременно с ее отрицанием. Предположим, что некоторый сомножитель КНФ не содержат ни одной буквы одновременно с ее отрицанием. Тем буквам, которые входят в этот сомножитель без отрицания, мы придадим значение «*Л*», а тем буквам, которые входят в этот сомножитель со знаками отрицания, мы придадим значение «*И*». Тогда в этом сомножителе все слагаемые будут ложными, а, следовательно, этот сомножитель, а значит и вся КНФ примет значение «*Л*», что противоречит условию. Например:

$$U = (A \vee \overline{B} \vee B)(\overline{A} \vee B \vee C \vee \overline{D} \vee E)(A \vee B \vee \overline{C} \vee C) = Л\,,$$

при $A = И$, $B = Л$, $C = Л$, $D = И$, $E = Л$.

**Пример.**

Доказать тождественную истинность следующей формулы.

$$X \to \left(\overline{Y} \to X\overline{Y}\right) = \overline{X} \vee \left(\overline{\overline{Y}} \vee X\overline{Y}\right) = \overline{X} \vee \left(Y \vee X\overline{Y}\right) =$$
$$= \overline{X} \vee Y \vee X\overline{Y} = \left(\overline{X} \vee Y \vee X\right)\left(\overline{X} \vee Y \vee \overline{Y}\right)$$

Формула тождественно истинная.

**Теорема 1.6.2. (Критерий тождественной ложности.)**

Формула алгебры высказываний тождественно ложна тогда и только тогда, когда каждое слагаемое ее ДНФ содержит некоторую букву одновременно с ее отрицанием.

Доказательство.

Необходимость. Дано: каждое слагаемое ДНФ содержит некоторую букву, одновременно с ее отрицанием. Доказать: формула тождественно ложна. В силу закона противоречия каждое слагаемое ДНФ будет ложным, а, следовательно, и вся ДНФ будет ложной.

Например:

$$U = \overline{X}\,Y\,\overline{Z}\,Z \vee X\,\overline{X}\,\overline{Y} \vee X\,Z\,\overline{Z} = Л\,.$$

Достаточность. Дано: формула тождественно ложна. Доказать: каждое слагаемое ее ДНФ содержит некоторую букву одновременно с ее отрицанием. Предположим противное. Выделим то слагаемое, которое не содержит ни одной буквы одновременно с ее отрицанием. Тем буквам, которые входят в это слагаемое без отрицания, мы придадим значение «*И*», а тем буквам, которые входят в это слагаемое со знаком отрицания, мы придадим значение «*Л*». Тогда все сомножители в этом слагаемом примут значение «*И*», следовательно, все это слагаемое будет истинным, а значит и вся формула будет истинной при этих значениях букв. Мы получили противоречие с условием. Например:

$$U = A\,B\,\overline{B}\,\overline{C} \vee A\,B\,C\,\overline{C} \vee A\,\overline{B}\,C\,\overline{D} = И\,,$$

при $A = И$, $B = Л$, $C = И$, $D = Л$.

## 1.7. Совершенные дизъюнктивные и конъюнктивные нормальные формы. (СДНФ и СКНФ)

Среди всевозможных ДНФ выделим более узкий класс СДНФ.

**Определение 1.7.1.** ДНФ формулы *U*, составленной из пропозициональных букв $X_1$, $X_2$, …, $X_n$, называется совершенной, если выполнены следующие четыре условия:

1. каждая буква $X_i$ $(i = \overline{1,n})$ входит в каждое слагаемое или с отрицанием или без отрицания;
2. ни одна из букв $X_i$ $(i = \overline{1,n})$ не входит ни в одно из слагаемых одновременно с отрицанием и без отрицания;
3. ни в одном из слагаемых нет одинаковых сомножителей;
4. в ДНФ нет одинаковых слагаемых.

**Пример.** $U = A\overline{B}C \vee \overline{A}\,\overline{B}\,\overline{C} \vee A\overline{B}\,\overline{C}$ – СДНФ.

Тождественно ложные формулы не имеют СДНФ. Это следует из критерия тождественной ложности и пункта 2 данного определения. Каждая не тождественно ложная формула имеет СДНФ.

*Способ нахождения СДНФ.*

Пусть некоторая не тождественно ложная формула уже приведена к ДНФ.

1. Допустим, что некоторая буква $X_i$ $(i=\overline{1,n})$ не входит в некоторое слагаемое $S$ ни с отрицанием, ни без него. Тогда это слагаемое $S$ мы должны заменить на дизъюнкцию двух слагаемых $SX_i \vee S\overline{X}_i$. Докажем, что от этого равносильность формулы не нарушится: $SX_i \vee S\overline{X}_i = S(X_i \vee \overline{X}_i) = SИ = S$.

2. Допустим, что некоторая буква $X_i$ $(i=\overline{1,n})$ входит в некоторое слагаемое $S$ одновременно с ее отрицанием. Тогда в силу закона противоречия это слагаемое будет ложным и его можно опустить. Так как по условию формула $U$ не тождественно ложна, то не все слагаемые будут опущены.

3. Допустим, что в некотором слагаемом $S$ содержатся одинаковые сомножители. Тогда в силу идемпотентного закона ($XX$=$X$) повторные сомножители можно будет опустить.

4. Допустим, что ДНФ содержит одинаковые слагаемые. Тогда в силу идемпотентного закона ($X \vee X$=$X$) повторные слагаемые можно опустить.

**Пример.**

$$(A \to \overline{B}C)(A \to C) = (\overline{A} \vee \overline{B}C)(\overline{A} \vee C) =$$
$$= \overline{A}\,\overline{A} \vee \overline{A}C \vee \overline{A}\,\overline{B}C \vee \overline{B}CC = \overline{A} \vee \overline{A}C \vee \overline{A}\,\overline{B}C \vee \overline{B}C =$$
$$= \overline{A}B \vee \overline{A}\,\overline{B} \vee \overline{A}BC \vee \overline{A}\,\overline{B}C \vee \overline{A}\,\overline{B}C \vee A\overline{B}C \vee \overline{A}\,\overline{B}C =$$
$$= \overline{A}BC \vee \overline{A}B\overline{C} \vee \overline{A}\,\overline{B}C \vee \overline{A}\,\overline{B}\,\overline{C} \vee \overline{A}BC \vee \overline{A}\,\overline{B}C \vee A\overline{B}C =$$
$$= \overline{A}BC \vee \overline{A}B\overline{C} \vee \overline{A}\,\overline{B}C \vee \overline{A}\,\overline{B}\,\overline{C} \vee A\overline{B}C$$

Последняя формула является СДНФ.

Среди всевозможных КНФ выделим более узкий класс СКНФ.

**Определение 1.7.2.** КНФ формулы $U$, состоящей из пропозициональных букв $X_1$, $X_2$, …, $X_n$, называется совершенной, если выполняются следующие четыре условия:

1. каждая буква $X_i$ $(i=\overline{1,n})$ входит в каждый сомножитель или с отрицанием или без отрицания;
2. ни одна из букв $X_i$ $(i=\overline{1,n})$ не входит ни в один из сомножителей одновременно с отрицанием и без отрицания;
3. ни в одном из сомножителей нет одинаковых слагаемых;
4. в КНФ нет одинаковых сомножителей.

**Пример.** $U = (X \vee \overline{Y} \vee Z)(X \vee Y \vee Z)(\overline{X} \vee Y \vee \overline{Z})(X \vee \overline{Y} \vee \overline{Z})$ – СКНФ.

Тождественно истинные формулы не имеют СКНФ. Это следует из критерия тождественной истинности и пункта 2 данного определения. Каждая не тождественно истинная формула может быть приведена к СКНФ.

*Способ нахождения СКНФ.*

Пусть некоторая не тождественно истинная формула уже приведена к КНФ.

1. Пусть некоторая буква $X_i$ $(i=\overline{1,n})$ не входит в некоторый сомножитель $S$ ни с отрицанием, ни без него. Тогда этот сомножитель $S$ мы должны будем заменить на конъюнкцию двух сомножителей $(S \vee X_i)(S \vee \overline{X}_i)$. Докажем, что от этого равносильность формулы не нарушится: $(S \vee X_i)(S \vee \overline{X}_i) = S \vee X\overline{X}_i = S \vee Л = S$.

2. Пусть некоторая буква $X_i$ $(i=\overline{1,n})$ входит в некоторый сомножитель $S$ одновременно со своим отрицанием. Тогда в силу закона исключения третьего этот сомножитель является истинным и его можно опустить. Так как по условию формула не тождественно истина, то не все сомножители будут опущены.

3. Пусть некоторый сомножитель $S$ содержит одинаковые слагаемые. Тогда в силу идемпотентного закона $X \vee X = X$ повторные слагаемые можно опустить.

4. Пусть КНФ содержит одинаковые сомножители. Тогда в силу идемпотентного закона $XX=X$ повторные сомножители можно опустить.

**Пример.**

$$(A \to \overline{B}C)(A \to C) = (\overline{A} \vee \overline{B}C)(\overline{A} \vee C) =$$
$$= (\overline{A} \vee \overline{B})(\overline{A} \vee C)(\overline{A} \vee C) = (\overline{A} \vee \overline{B})(\overline{A} \vee C) =$$
$$= (\overline{A} \vee \overline{B} \vee C)(\overline{A} \vee \overline{B} \vee \overline{C})(\overline{A} \vee B \vee C)(\overline{A} \vee \overline{B} \vee C) =$$
$$= (\overline{A} \vee \overline{B} \vee C)(\overline{A} \vee \overline{B} \vee \overline{C})(\overline{A} \vee B \vee C)$$

Последняя формула является СКНФ.

## 1.8. Представление двузначных функций формулами алгебры высказываний

**Определение 1.8.1.** Функция $F(X_1, X_2, ..., X_n)$ называется двузначной, если сама функция и каждый из ее аргументов принимают только два значения: истина или ложь.

**Теорема 1.8.1.** Для каждой двузначной функции существует равносильная ей формула алгебры высказываний.

Доказательство.

I. Пусть $F(X_1, X_2, ..., X_n)$ не тождественно ложна. Рассмотрим всевозможные наборы длины $n$, составленные из букв «*И*» и «*Л*». Каждому такому набору мы поставим в соответствие элементарную конъюнкцию по следующему принципу: на место буквы «*И*» ставим соответствующую пропозициональную букву, а на место буквы «*Л*» ставим отрицание соответствующей буквы.

$$2^n \begin{cases} И, И, ..., И \leftrightarrow X_1 X_2 ... X_n \\ И, Л, ..., И \leftrightarrow X_1 \overline{X}_2 ... X_n \\ ... \\ Л, Л, ..., Л \leftrightarrow \overline{X}_1 \overline{X}_2 ... \overline{X}_n \end{cases}$$

Докажем равносильность:

$$F(X_1,X_2,...,X_n)=F(И,И,...,И)X_1X_2...X_n \vee F(И,Л,...,И)X_1\overline{X}_2...X_n \vee$$
$$\vee F(Л,Л,...,Л)\overline{X}_1\overline{X}_2...\overline{X}_n$$

Придадим пропозициональным буквам $X_1$, $X_2$, …, $X_n$ конкретные значения. Пусть, например, $X_1=И$, $X_2=Л$, …, $X_n=И$. Тогда левая часть равна $F(И,Л,...,И)$. Выделим в правой части то слагаемое, которое соответствует выбранным значениям пропозициональных букв. В этом слагаемом все сомножители, начиная со второго, принимают значения «*И*», и их можно опустить. В каждом из остальных слагаемых найдется хотя бы по одному ложному сомножителю. Следовательно, все остальные слагаемые будут ложными, и их можно опустить. Правая часть равна $F(И,Л,...,И)$. Итак, равносильность доказана.

Преобразуем правую часть этой равносильности в формулу алгебры высказываний. Для этого каждый из символов $F(И,И,...,И)$, $F(И,Л,...,И)$, …, $F(Л,Л,...,Л)$ заменим на его значение, то есть на «истину» или «ложь». Если значение функции на каком-то наборе есть «*И*», то в соответствующем слагаемом первый сомножитель будет истинным, и его можно опустить. Если значение функции на некотором наборе будет ложным, то в соответствующем слагаемом первый сомножитель будет ложным. Но тогда и все это слагаемое будет ложным и его можно опустить целиком. Так как по условию данная функция не тождественно ложна, то некоторые слагаемые останутся. В результате указанных преобразований мы получаем формулу алгебры высказываний, равносильную данной функции и стоящую в СДНФ.

II. Пусть $F(X_1,X_2,...,X_n)$ не тождественно истинна. Составим всевозможные наборы длины *n* из букв «*И*» и «*Л*». Каждому такому набору мы поставим в соответствие элементарную дизъюнкцию по принципу: на место буквы «*И*» мы поставим отрицание соответствующей пропозициональной буквы, а на место буквы «*Л*» поставим соответствующую пропозициональную букву.

$$2^n\begin{cases} И,И,...,И \leftrightarrow \overline{X}_1 \vee \overline{X}_2 \vee ... \vee \overline{X}_n \\ И,Л,...,И \leftrightarrow \overline{X}_1 \vee X_2 \vee ... \vee \overline{X}_n \\ ... \\ Л,Л,...,Л \leftrightarrow X_1 \vee X_2 \vee ... \vee X_n \end{cases}$$

Докажем равносильность:

$$F(X_1,X_2,...,X_n)=(F(И,И,...,И)\vee \overline{X}_1 \vee \overline{X}_2 \vee ... \vee \overline{X}_n)\wedge$$
$$\wedge(F(И,Л,...,И)\vee \overline{X}_1 \vee X_2 \vee ... \vee \overline{X}_n)\wedge ... \wedge (F(Л,Л,...,Л)\vee X_1 \vee X_2 \vee ... \vee X_n)$$

Придадим пропозициональным буквам $X_1$, $X_2$, …, $X_n$ конкретные значения, например, $X_1=И$, $X_2=Л$, …, $X_n=И$. Левая часть равна $F(И,Л,...,И)$. В правой части мы выделим тот сомножитель, который соответствует выбранным значениям пропозициональных букв. В этом сомножителе все слагаемые, начиная со второго, ложны, и их можно опустить. В каждом из остальных сомножителей будет хотя бы по одному истинному слагаемому. Тогда все остальные сомножители будут истинными, и их можно опустить. Правая часть равна $F(И,Л,...,И)$.

Далее мы должны преобразовать правую часть этой равносильности в формулу алгебры высказываний. Для этого каждый из символов $F(И,И,...,И)$, $F(И,Л,...,И)$, …, $F(Л,Л,...,Л)$ мы должны заменить на его значение, то есть на «истину» или «ложь». Если значение функции на некотором наборе есть «*И*», то в соответствующем сомножителе первое слагаемое будет истинным. Следовательно, весь соответствующий сомножитель будет истинным, и его можно опустить. Так как функция по условию не является тождественно истинной, не все сомножители будут опущены. Если значение функции на некотором наборе есть «*Л*», то в соответствующем сомножителе первое слагаемое будет ложно, и его можно опустить. В результате указанных преобразований мы получим формулу алгебры высказываний, равносильную данной функции и стоящую в СКНФ.

Теорема доказана.

**Замечание.** Если $F(X_1,X_2,...,X_n)$ не является ни тождественно истинной, ни тождественно ложной, то к ней применимы оба рассмотренных способа. Обозначим через $p$ число слагаемых в СДНФ, а через $q$ число сомножителей в СКНФ. Тогда $p+q=2^n$.

Например, пусть $F(X,Y,Z)=И$ тогда и только тогда, когда два аргумента ложны и один истинен.

$$F(X,Y,Z)=$$
$$=F(И,И,И)XYZ\vee F(И,И,Л)XY\overline{Z}\vee F(И,Л,И)X\overline{Y}Z\vee F(И,Л,Л)X\overline{Y}\,\overline{Z}\vee$$
$$\vee F(Л,И,И)\overline{X}YZ\vee F(Л,И,Л)\overline{X}Y\overline{Z}\vee F(Л,Л,И)\overline{X}\,\overline{Y}Z\vee F(Л,Л,Л)\overline{X}\,\overline{Y}\,\overline{Z}=$$
$$=ЛXYZ\vee ЛXY\overline{Z}\vee ЛX\overline{Y}Z\vee ИX\overline{Y}\,\overline{Z}\vee Л\overline{X}YZ\vee И\overline{X}Y\overline{Z}\vee И\overline{X}\,\overline{Y}Z\vee Л\overline{X}\,\overline{Y}\,\overline{Z}=$$
$$=X\overline{Y}\,\overline{Z}\vee\overline{X}Y\overline{Z}\vee\overline{X}\,\overline{Y}Z$$

$$F(X,Y,Z)=$$
$$=(F(И,И,И)\vee\overline{X}\vee\overline{Y}\vee\overline{Z})\wedge(F(И,И,Л)\vee\overline{X}\vee\overline{Y}\vee Z)\wedge$$
$$\wedge(F(И,Л,И)\vee\overline{X}\vee Y\vee\overline{Z})\wedge(F(И,Л,Л)\vee\overline{X}\vee Y\vee Z)\wedge$$
$$\wedge(F(Л,И,И)\vee X\vee\overline{Y}\vee\overline{Z})\wedge(F(Л,И,Л)\vee X\vee\overline{Y}\vee Z)\wedge$$
$$\wedge(F(Л,Л,И)\vee X\vee Y\vee\overline{Z})\wedge(F(Л,Л,Л)\vee X\vee Y\vee Z)=$$
$$=(Л\vee\overline{X}\vee\overline{Y}\vee\overline{Z})\wedge(Л\vee\overline{X}\vee\overline{Y}\vee Z)\wedge$$
$$\wedge(Л\vee\overline{X}\vee Y\vee\overline{Z})\wedge(И\vee\overline{X}\vee Y\vee Z)\wedge$$
$$\wedge(Л\vee X\vee\overline{Y}\vee\overline{Z})\wedge(И\vee X\vee\overline{Y}\vee Z)\wedge$$
$$\wedge(И\vee X\vee Y\vee\overline{Z})\wedge(Л\vee X\vee Y\vee Z)=$$
$$=(\overline{X}\vee\overline{Y}\vee\overline{Z})(\overline{X}\vee\overline{Y}\vee Z)(\overline{X}\vee Y\vee\overline{Z})(X\vee\overline{Y}\vee\overline{Z})(X\vee Y\vee Z)$$

# ГЛАВА 2
# АЛГЕБРА ПРЕДИКАТОВ
# (ЛОГИКА ПРЕДИКАТОВ)

## 2.1. Предикаты и кванторы

**Определение 2.1.1.** Предикатом называется логическая функция от одного или нескольких аргументов, определенная на произвольном множестве *M* и принимающая всего два значения: «истина» или «ложь» («*И*» или «*Л*»).

Предикаты обозначаются большими латинскими буквами (без индексов или с индексами внизу), а аргументы предикатов обозначаются малыми латинскими буквами (без индексов или с индексами внизу). Все предикаты подразделяются в зависимости от числа аргументов на одноместные, двухместные, трехместные и так далее: $P(a)$, $P(a,b)$, $P(a,b,c)$, … Элементарные высказывания можно рассматривать как частный случай предикатов, а именно как предикаты от нуля аргументов.

**Примеры.**

1. *M* – множество натуральных чисел.
   $P(a)$ = {*a* – простое число}.
   $P(1)$ = *Л*, $P(2)$ = *И*, $P(3)$ = *И*, $P(4)$ = *Л*.
2. *M* – множество людей.
   $R(a,b)$ = {*a* старше *b*}.
   *R*(Тьюринг, Гильберт) = *Л*.
3. *M* – множество целых чисел.
   $S(a,b,c) = \{\, a^2 + b^2 = c^2 \,\}$
   $S(2, 3, 4)$ = *Л*, $S(3, 4, 5)$ = *И*.

Одноместные предикаты выражают свойства предметов или понятий. Многоместные предикаты выражают отношения между предметами или понятиями.

Из элементарных предикатов можно получать сложные предикаты, при этом используются логические операции алгебры высказываний $\vee$, $\wedge$, $\to$, $\sim$, $\overline{\phantom{x}}$, а также кванторы.

**Пример.**

Пусть *M* – множество студентов II курса НФ МИСиС.

Пусть $P(a)$ = {студент *a* аккуратно посещает лекции по логике} – одноместный предикат.

«Все студенты II курса НФ МИСиС аккуратно посещает лекции по логике» – высказывание.

Пусть на множестве *M* задан предикат $P(a)$. Мы можем составить следующее высказывание: «для всех *x* справедливо $P(x)$» ($\forall x P(x)$).

**Определение 2.1.2.**

$$\forall x P(x) = \begin{cases} И, \text{ если для любого } a \ P(a) = И, \\ Л, \text{ если найдется такой элемент } a, \text{ что } P(a) = Л. \end{cases}$$

**Пример.**

«Имеется студент II курса НФ МИСиС, который аккуратно посещает лекции по логике» – высказывание.

Если на множестве $M$ задан предикат $P(a)$, то мы можем составить следующее высказывание: «существует такое $x$, что справедливо $P(x)$» ($\exists x P(x)$).

**Определение 2.1.3.**

$$\exists x P(x) = \begin{cases} И, \text{ если найдется такой элемент } a, \text{ что } P(a) = И, \\ Л, \text{ если для любого } a \ P(a) = Л. \end{cases}$$

**Замечание.** Если переменная не входит под знак ни одного из кванторов, то она называется свободной и обозначается малой латинской буквой из начала алфавита. Если переменная входит под знак одного из кванторов, то она называется связанной и обозначается малой латинской буквой из конца алфавита.

Кванторы можно использовать и в случае многоместных предикатов. Пусть, например, $P(a_1, a_2, ..., a_n)$ некоторый $n$-местный предикат. Тогда $\forall x_1 P(x_1, a_2, ..., a_n)$ – $(n-1)$-местный предикат, $\exists x_1 P(x_1, a_2, ..., a_n)$ – также $(n-1)$-местный предикат.

**Пример.** $M$ – множество целых чисел.

$P(a,b) = \{|a| > b\}$ – двухместный предикат.

$$Q(b) = \forall x P(x,b) = \forall x(|x| > b) = \begin{cases} И, & b < 0 \\ Л, & b \geq 0 \end{cases}.$$

$Q(b)$ – одноместный предикат.

**Пример.** $M$ – множество натуральных чисел.

$P(a,b) = \{a < b\}$ – двухместный предикат.

$$R(b) = \exists x P(x,b) = \exists x(x < b) = \begin{cases} И, & b \neq 1 \\ Л, & b = 1 \end{cases}.$$

$R(b)$ – одноместный предикат.

## 2.2. Формулы алгебры предикатов

**Определение 2.2.1.** Формулой алгебры предикатов называется элементарный предикат или сложный предикат, составленный из элементарных с помощью логических операций алгебры высказываний и кванторов.

**Замечание.** При записи формул алгебры предикатов принимают соглашение: если один квантор находится в области действия другого квантора, то переменные, связанные этими кванторами, обозначаются различными буквами.

**Примеры.**

1. $\forall x \exists y P(x,y) \vee \forall z(R(a) \to \forall x \exists z Q(x,z))$ – не формула.
2. $\forall x \exists y P(x,y) \vee \forall z(R(a) \to \forall x Q(x,z))$ – формула.
3. $\exists z(\overline{R(z)} \to \exists y \forall x S(x,y))$ – формула.

($a$ – свободная переменная, $x$, $y$, $z$ – связанные переменные).

Всякая формула алгебры предикатов сама является предикатом от входящих в нее свободных переменных. Если формула не содержит свободных переменных, то она является предикатом от нуля аргументов, то есть просто высказыванием.

**Определение 2.2.2.** Формула называется замкнутой, если она не содержит свободных предметных переменных.

**Определение 2.2.3.** Если формула алгебры предикатов $U(a_1, a_2, ..., a_n)$ содержит свободные переменные $a_1$, $a_2$, …, $a_n$, то формула

$$\forall x_1 \forall x_2 ... \forall x_n U(x_1, x_2, ..., x_n)$$

называется замыканием формулы $U(a_1, a_2, ..., a_n)$.

Замыкание любой формулы является замкнутой формулой. Значение формулы алгебры предикатов зависит от трех факторов.

1. От множества $M$, на котором эта формула рассматривается.
2. От выбора конкретных предикатов, определенных на этом множестве.
3. От выбора конкретных элементов этого множества, которые подставляются вместо свободных переменных.

**Пример.** $\exists x P(x,b)$

1. $M = N,\ P(a,b) = \{a < b\},\ b = 1,\ \exists x P(x,b) = \exists x(x < 1) = Л$.
2. $M = Z,\ P(a,b) = \{a < b\},\ b = 1,\ \exists x P(x,b) = \exists x(x < 1) = И$.
3. $M = N,\ P(a,b) = \{a > b\},\ b = 1,\ \exists x P(x,b) = \exists x(x > 1) = И$.
4. $M = N,\ P(a,b) = \{a < b\},\ b = 5,\ \exists x P(x,b) = \exists x(x < 5) = И$.

Значение замкнутой формулы алгебры предикатов зависит от двух факторов.

1. От множества $M$, на котором эта формула рассматривается.
2. От выбора конкретных предикатов, определенных на этом множестве.

**Определение 2.2.4.** Формула алгебры предикатов называется тождественно истинной, если она принимает значение «*И*» для всех множеств, для всех предикатов и для всех элементов.

**Определение 2.2.5.** Формула алгебры предикатов называется тождественно ложной, если она принимает значение «*Л*» для всех множеств, для всех предикатов и для всех элементов.

**Определение 2.2.6.** Формула алгебры предикатов называется выполнимой, если она принимает значение «*И*» хотя бы для некоторых множеств, предикатов и элементов.

**Определение 2.2.7.** Формула алгебры предикатов называется опровержимой, если она принимает значение «*Л*» хотя бы для некоторых множеств, предикатов и элементов.

**Пример.** $\forall x \forall y (P(x,y) \to \overline{P(y,x)})$ – замкнутая формула.

1. $U$ – выполнимая.

   $M$=$R$, $P(a, b)$ = $\{a > b\}$, $U = \forall x \forall y (x > y \to \overline{y > x}) = И$ .

2. $U$ – опровержимая.

   $M$=$R$, $P(a, b)$ = $\{a = b\}$, $U = \forall x \forall y (x = y \to \overline{y = x}) = Л$ .

**Определение 2.2.8.** Говорят, что формула $U$ сильнее формулы $V$, если всякий раз, когда формула $U$ принимает истинное значение, формула $V$ также принимает истинное значение.

**Пример.** $\forall x P(x) \Rightarrow \exists x P(x)$.

**Определение 2.2.9.** Две формулы $U$ и $V$ называются равносильными, если они принимают одинаковые значения для всех множеств, для всех предикатов и для всех элементов.

## 2.3. Основные равносильности алгебры предикатов

1. $\overline{\forall x P(x)} = \exists x \overline{P(x)}$
2. $\overline{\exists x P(x)} = \forall x \overline{P(x)}$

Знак отрицания можно внести под знак квантора, сменив квантор на двойственный.

3. $\forall x \forall y P(x,y) = \forall y \forall x P(x,y)$
4. $\exists x \exists y P(x,y) = \exists y \exists x P(x,y)$

Одинаковые кванторы можно переставлять.

**Замечание.** Двойственные кванторы переставлять нельзя:

$$\exists x \forall y P(x,y) \neq \forall y \exists x P(x,y).$$

**Пример.** $M$ – множество натуральных чисел.

$P(a,b) = \{a \vdots b\}$.

$\exists x \forall y P(x,y) = \exists x \forall y (x \vdots y) = Л$ ,

$\forall y \exists x P(x,y) = \forall y \exists x (x \vdots y) = И$ .

5. $\exists x (P(x) \vee Q(x)) = \exists x P(x) \vee \exists x Q(x)$ Квантор существования разбивается на два по дизъюнкции.

**Замечание.** Квантор всеобщности не разбивается по дизъюнкции:

$$\forall x (P(x) \vee Q(x)) \neq \forall x P(x) \vee \forall x Q(x).$$

**Пример.** $M$ – множество натуральных чисел.

$P(a)$ = $\{a$ – четное число$\}$, $Q(a)$ = $\{a$ – нечетное число$\}$.

$\forall x (P(x) \vee Q(x)) = И$ ,

$\underbrace{\forall x P(x)}_{Л} \vee \underbrace{\forall x Q(x)}_{Л} = Л$ .

6. $\forall x (P(x) \wedge Q(x)) = \forall x P(x) \wedge \forall x Q(x)$ Квантор всеобщности разбивается на два по конъюнкции.

**Замечание.** Квантор существования не разбивается по конъюнкции.

$$\exists x(P(x) \wedge Q(x)) \neq \exists xP(x) \wedge \exists xQ(x).$$

**Пример.** $M$ – множество действительных чисел.
$P(a)$ – $\{a$ – рациональное число$\}$,
$Q(a)$ – $\{a$ – иррациональное число$\}$.
$\exists x(P(x) \wedge Q(x)) = Л$,
$\underbrace{\exists xP(x)}_{И} \wedge \underbrace{\exists xQ(x)}_{И} = И$.

7. $\forall xP(x) = \forall yP(y)$
8. $\exists xP(x) = \exists yP(y)$

Связанные переменные можно переименовывать.

9. $\exists xP(x) \vee Q = \exists x(P(x) \vee Q)$
10. $\forall xP(x) \vee Q = \forall x(P(x) \vee Q)$
11. $\exists xP(x) \wedge Q = \exists x(P(x) \wedge Q)$
12. $\forall xP(x) \wedge Q = \forall x(P(x) \wedge Q)$

Если $Q$ не содержит буквы $x$, то можно переменить порядок выполнения таких операций как связывание квантором и дизъюнкции, а также связывание квантором и конъюнкции.

13. $\forall xP(x) \to Q = \exists x(P(x) \to Q)$
14. $\exists xP(x) \to Q = \forall x(P(x) \to Q)$
15. $Q \to \forall xP(x) = \forall x(Q \to P(x))$
16. $Q \to \exists xP(x) = \exists x(Q \to P(x))$

Если $Q$ не содержит буквы $x$, то при перемене порядка выполнения таких операций как связывание квантором и импликации квантор меняется на двойственный тогда и только тогда, когда он стоит в посылке.

## 2.4. Способы доказательства равносильностей в алгебре предикатов

В алгебре предикатов используются те же способы доказательства равносильности, что и в алгебре высказываний, кроме табличного.

**Примеры.**

1. $\overline{\forall xP(x)} = \exists x\overline{P(x)}$.

I. Пусть $\overline{\forall xP(x)} = И$. Тогда $\forall xP(x) = Л$, а, следовательно, существует такое $a$, что $P(a) = Л$, то есть существует такое $a$, что $\overline{P(a)} = И$, а значит $\exists x\overline{P(x)} = И$.

II. Пусть $\exists x\overline{P(x)} = И$. Тогда существует такое $a$, что $\overline{P(a)} = И$, то есть существует такое $a$, что $P(a) = Л$. Следовательно, $\forall xP(x) = Л$, а значит $\overline{\forall xP(x)} = И$.

9. $\exists xP(x) \vee Q = \exists x(P(x) \vee Q)$

I. Пусть $\exists xP(x) \vee Q = Л$. Тогда $\exists xP(x) = Л$ и $Q = Л$. То есть для любого $a$ $P(a) = Л$ и $Q = Л$. Следовательно, для любого $a$ $P(a) \vee Q = Л$, значит $\exists x(P(x) \vee Q) = Л$.

II. Пусть $\exists x(P(x) \vee Q) = Л$. Тогда для любого $a$ $P(a) \vee Q = Л$, значит, для любого $a$ $P(a) = Л$ и $Q = Л$, следовательно, $\exists x P(x) = Л$ и $Q = Л$, значит, $\exists x P(x) \vee Q = Л$.

13. $\forall x P(x) \to Q = \exists x(P(x) \to Q)$

$$\forall x P(x) \to Q = \overline{\forall x P(x)} \vee Q = \exists x \overline{P(x)} \vee Q = \exists x\left(\overline{P(x)} \vee Q\right) = \exists x\left(P(x) \to Q\right)$$

## 2.5. Ограниченные кванторы

Пусть дано произвольное непустое множество *M* и пусть $E \subseteq M$.

**Определение 2.5.1.** Характеристическим предикатом подмножества *E* называется предикат, определенный на всем множестве *M* и принимающий истинные значения на подмножестве *E*.

$$E(a) = \begin{cases} И, & a \in E \\ Л, & a \in M \setminus E \end{cases}$$

$E(a)$ – характеристический предикат.

Определим символы $\underset{x \in E}{\forall x} P(x)$ и $\underset{x \in E}{\exists x} P(x)$, где $P(a)$ есть произвольный предикат определенный на множестве *M*.

**Определение 2.5.2.**

$$\underset{x \in E}{\forall x} P(x) = \underset{E(x)}{\forall x} P(x) = \begin{cases} И, & \text{если для любого } a \in E \ \ P(a) = И, \\ Л, & \text{если существует такое } a \in E \text{, что } P(a) = Л. \end{cases}$$

**Определение 2.5.3.**

$$\underset{x \in E}{\exists x} P(x) = \underset{E(x)}{\exists x} P(x) = \begin{cases} И, & \text{если существует такое } a \in E \text{, что } P(a) = И, \\ Л, & \text{если для любого } a \in E \ \ P(a) = Л. \end{cases}$$

Эти кванторы называются ограниченными, так как область изменения аргумента ограниченна подмножеством *E*.

Докажем равносильности, связывающие ограниченные кванторы с обычными.

1. $\underset{x \in E}{\forall x} P(x) = \forall x(E(x) \to P(x))$

I. Пусть $\underset{x \in E}{\forall x} P(x) = Л$. Тогда существует $a \in E$, что $P(a) = Л$. Так как $a \in E$, то $E(a) = И$, $E(a) \to P(a) = И \to Л = Л$. Кроме того, так как $a \in E$ и $E \subseteq M$, следовательно, $a \in M$. Итак, существует $a \in M$, что $E(a) \to P(a) = Л$, а, значит, $\forall x(E(x) \to P(x)) = Л$.

II. Пусть $\forall x(E(x) \to P(x)) = Л$. Тогда найдется $a \in M$, что $E(a) \to P(a) = Л$, то есть $E(a) = И$ и $P(a) = Л$. Так как $E(a) = И$, то $a \in E$. Итак, найдется $a \in E$, что $P(a) = Л$. Значит, $\underset{x \in E}{\forall x} P(x) = Л$.

2. $\underset{x \in E}{\exists x} P(x) = \exists x(E(x) \wedge P(x))$

I. Пусть $\underset{x \in E}{\exists x} P(x) = И$. Тогда найдется $a \in E$, что $P(a) = И$. Так как $a \in E$, то $E(a) = И$, $E(a) \wedge P(a) = И$. Кроме того, $a \in E$ и $E \subseteq M$, значит,

$a \in M$. Итак, найдется $a \in M$, что $E(a) \wedge P(a) = И$. Значит, $\exists x(E(x) \wedge P(x)) = И$.

II. Пусть $\exists x(E(x) \wedge P(x)) = И$. Тогда найдется $a \in M$, что $E(a) \wedge P(a) = И$. Значит $E(a) = И$ и $P(a) = И$. $E(a) = И$, следовательно, $a \in E$. Итак, найдется $a \in E$, что $P(a) = И$. Следовательно, $\underset{x \in E}{\exists x}\, P(x) = И$.

**Замечание.** Основные равносильности, записанные выше для обычных кванторов, справедливы и для ограниченных кванторов.

**Пример.** $\overline{\underset{x \in E}{\forall x}\, P(x)} = \underset{x \in E}{\exists x}\, \overline{P(x)}$

$$\overline{\underset{x \in E}{\forall x}\, P(x)} = \overline{\forall x\big(E(x) \to P(x)\big)} = \exists x\Big(\overline{E(x) \to P(x)}\Big) = \exists x\Big(E(x) \wedge \overline{P(x)}\Big) = \underset{x \in E}{\exists x}\, \overline{P(x)}$$

## 2.6. Приведенные и нормальные формы

**Определение 2.6.1.** Формула алгебры предикатов называется приведенной, если она не содержит символов импликации и эквиваленции, а знак отрицания в ней встречается только над элементарными предикатами.

**Примеры.**

1. $\exists x\big(\overline{\forall y P(y)} \to \exists z Q(x,z)\big)$.

Это не приведенная формула, так как в ней есть знак импликации и знак отрицания стоит над квантором.

2. $\forall x \exists z \overline{Q(x,z)} \vee \forall y\big(\overline{S(a)} \vee R(y)\big)$ – приведенная формула.

**Определение 2.6.2.** Приведенная формула, равносильная данной формуле *U*, называется приведенной формой формулы *U*.

Каждая формула алгебры предикатов имеет приведенную форму.

*Способы нахождения приведенной формы.*

1. Избавляемся от $\to$ и $\sim$ с помощью основных равносильностей алгебры высказываний.
2. Переносим знак отрицания на элементарные предикаты с помощью равносильностей 1 и 2 алгебры предикатов и законов де Моргана.
3. Избавляемся от двойных отрицаний с помощью закона двойного отрицания.

**Пример.**

$$\overline{\exists x\big(P(a,x) \to \forall y \exists z Q(y,z)\big)} = \forall x \overline{P(a,x) \to \forall y \exists z Q(y,z)} =$$
$$= \forall x\Big(P(a,x) \wedge \overline{\forall y \exists z Q(y,z)}\Big) = \forall x\Big(P(a,x) \wedge \exists y \forall z \overline{Q(y,z)}\Big)$$

Среди всех приведенных формул мы можем выделить более узкий класс – класс нормальных формул.

**Определение 2.6.3.** Приведенная формула алгебры предикатов называется нормальной, если она или вовсе не содержит кванторов или если при образовании ее из элементарных формул операции связывания квантором выполняются после всех операций алгебры высказываний.

**Примеры.**

1. $\overline{P(a,b)} \wedge \left(S(a) \vee \overline{R(c)}\right)$ – нормальная формула.
2. $\forall x \exists z \left(\overline{R(a,z)} \wedge S(x)\right)$ – нормальная формула.
3. $\exists y \left(S(a,y) \vee \forall z \exists x \overline{R(x,z)}\right)$ – приведенная, но не нормальная формула.

**Определение 2.6.4.** Нормальная формула, равносильная данной формуле *U*, называется нормальной формой формулы *U*.

Каждая формула логики предикатов имеет нормальную форму.

*Способ нахождения нормальной формы.*

Если некоторая формула *U* уже находится в приведенной форме, но не является нормальной формулой, то мы должны переменить порядок выполнения таких операций как связывание квантором и дизъюнкция, а также связывание квантором и конъюнкция. Для этого мы можем использовать равносильности

$$\exists x P(x) \vee Q = \exists x (P(x) \vee Q),\ \exists x P(x) \wedge Q = \exists x (P(x) \wedge Q),$$
$$\forall x P(x) \vee Q = \forall x (P(x) \vee Q),\ \forall x P(x) \wedge Q = \forall x (P(x) \wedge Q).$$

Однако эти равносильности справедливы при условии, что формула *Q* не содержит буквы *x*. В противном случае мы должны будем переименовать связанную переменную *x* на новую букву, которая раньше не содержалась в нашей формуле. Для этого мы можем использовать равносильности

$$\forall x P(x) = \forall y P(y),\ \exists x P(x) = \exists y P(y).$$

**Пример.**

$$\exists x P(x) \sim \forall y Q(y) = \exists x P(x) \wedge \forall y Q(y) \vee \overline{\exists x P(x)} \vee \overline{\forall y Q(y)} =$$
$$= \exists x P(x) \wedge \forall y Q(y) \vee \forall x \overline{P(x)} \wedge \exists y \overline{Q(y)} =$$
$$= \exists x \forall y (P(x) \wedge Q(y)) \vee \forall x \exists y \left(\overline{P(x)} \wedge \overline{Q(y)}\right) =$$
$$= \exists x \forall y (P(x) \wedge Q(y)) \vee \forall z \exists u \left(\overline{P(z)} \wedge \overline{Q(u)}\right) =$$
$$= \exists x \forall y \forall z \exists u \left(P(x) \wedge Q(y) \vee \overline{P(z)} \wedge \overline{Q(u)}\right)$$

Последняя формула является нормальной.

# ГЛАВА 3
# ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

## 3.1. Основные понятия

В исчислении высказываний изучаются те же логические операции и законы, что и в алгебре высказываний. Однако, если логические операции задавались в алгебре высказываний с помощью таблиц истинностных значений, то в исчислении высказываний эти операции задаются аксиоматически. Если логические законы в алгебре высказываний задавались с помощью тождественно истинных формул, то в исчислении высказываний логические законы задаются с помощью формул, выводимых из аксиом с помощью определенных правил вывода.

**I. Перечисление символов.**

1. Пропозициональные буквы – большие латинские буквы с индексами внизу или без индексов.
2. Логические символы: $\wedge$, $\vee$, $\to$, –.
3. Вспомогательные символы: **(**, **)**.

**II. Определение формулы.**

1. Всякая пропозициональная буква есть формула.
2. Если $U$ – формула, то $\overline{U}$ – формула.
3. Если $U$ и $V$ – формулы, то $(U \wedge V)$, $(U \vee V)$, $(U \to V)$ – формулы.

Первый пункт является базисным, в нем указываются элементарные формулы. Пункты 2,3 являются индуктивными, в них даются правила, по которым из готовых формул можно получать новые формулы.

Например, $((A \to \overline{B}) \vee (A \wedge \overline{C}))$ – формула.

$A$, $B$, $C$ – формулы (следует из пункта 1).

$\overline{B}$, $\overline{C}$ – формулы (следует из пункта 2).

$(A \to \overline{B})$, $(A \wedge \overline{C})$ – формулы (следует из пункта 3).

$((A \to \overline{B}) \vee (A \wedge \overline{C}))$ – формула (следует из пункта 3).

Для упрощения записи формул принимаются следующие соглашения:

1. опускается знак конъюнкции;
2. опускаются внешние скобки;
3. опускаются скобки, стоящие под общим знаком отрицания;
4. опускаются те скобки, которые можно восстановить исходя из правил о порядке выполнения логических операций.

Так, $(A \to \overline{B}) \vee A\overline{C}$ – сокращенная запись формулы.

**III. Аксиомы исчисления высказываний.**

В исчислении высказываний аксиомы задаются следующими 11-ю схемами.

1. Схемы для импликации.

1a) $U \to (V \to U)$

Из справедливости заключения следует справедливость всей импликации.

1б) $(U \to (V \to Q)) \to ((U \to V) \to (U \to Q))$

Пусть из $U$ следует импликация. Тогда, если из $U$ следует посылка этой импликации, то из $U$ следует и заключение этой импликации.

2. Схемы для конъюнкции.

2а) $UV \to U$

Из справедливости конъюнкции следует справедливость первого сомножителя.

2б) $UV \to V$

Из справедливости конъюнкции следует справедливость второго сомножителя.

2в) $(U \to V) \to ((U \to Q) \to (U \to VQ))$

Пусть из $U$ следует некоторое высказывание. Тогда, если из $U$ следует второе высказывание, то из $U$ следует конъюнкция этих высказываний.

3. Схемы для дизъюнкции.

3а) $U \to U \vee V$

Из справедливости первого слагаемого следует справедливость дизъюнкции.

3б) $V \to U \vee V$

Из справедливости второго слагаемого следует справедливость дизъюнкции.

3в) $(U \to Q) \to ((V \to Q) \to (U \vee V \to Q))$

Пусть $Q$ следует из некоторого высказывания. Тогда, если $Q$ следует из второго высказывания, то $Q$ будет следовать из дизъюнкции этих высказываний.

4. Схемы для отрицания.

4а) $(U \to V) \to (\overline{V} \to \overline{U})$

Если справедлива импликация, то справедлива и импликация, противоположенная обратной.

4б) $U \to \overline{\overline{U}}$

Двойное отрицание можно навешивать.

4в) $\overline{\overline{U}} \to U$

Двойное отрицание можно снимать.

**Определение 3.1.1.** Аксиомой исчисления высказываний называется любая формула, записанная по одной из этих схем.

**Пример:** $(A \to \overline{C}) \to \overline{B} \vee (A \to \overline{C})$ – аксиома по схеме 3б.

**IV. Основное правило вывода.**

Все правила вывода подразделяются на основные и производные.

**Определение 3.1.2.** Правило вывода называется основным, если оно постулируется.

**Определение 3.1.3.** Правило вывода называется производным, если оно доказывается.

В исчислении высказываний имеется единственное основное правило вывода. Это правило заключения: $\dfrac{U \to V, U}{V}$. Если справедлива импликация и ее посылка, то справедливо и заключение.

**V. Определение формального доказательства и доказуемой формулы.**

**Определение 3.1.4.** Формальным доказательством называется конечная система формул, записанных друг под другом, каждая из которых либо аксиома, либо получается из вышестоящих формул по правилу заключения.

**Определение 3.1.5.** Формула исчисления предикатов называется доказуемой, если она стоит последней строчкой некоторого формального доказательства.

**Следствие 1.** Всякая аксиома исчисления высказываний является доказуемой формулой, причем ее доказательство состоит всего из одной строчки.

1. $(\overline{A} \to D)B \to B$ – аксиома по схеме 2б.

**Следствие 2.** Всякая строчка формального доказательства является доказуемой формулой. Действительно, каждый начальный отрезок формального доказательства сам является формальным доказательством.

**Следствие 3.** Если получена конечная система формул, причем каждая из этих формул будет либо доказуемой, либо будет получаться из вышестоящих формул по правилу заключения, то последняя строчка такой системы также будет доказуема. Хотя такая система не является формальным доказательством, однако она может быть преобразована в формальное доказательство, если каждую из встретившихся там доказуемых формул заменить на ее формальное доказательство.

## 3.2. Примеры доказуемых формул

1. $U \to U$

Доказательство.

1. $(U \to ((V \to U) \to U)) \to ((U \to (V \to U)) \to (U \to U))$

– аксиома по схеме 1б.

1б. $(U \to (V \to Q)) \to ((U \to V) \to (U \to Q))$

$U := U$, $Q := U$, $V := V \to U$.

2. $(U \to ((V \to U) \to U))$

– аксиома по схеме 1а.

1а. $U \to (V \to U)$

$U := U$, $V := V \to U$.

3. $(U \to (V \to U)) \to (U \to U)$

– правило заключения (1,2).

4. $U \to (V \to U)$ – аксиома по схеме 1а.
5. $U \to U$ – правило заключения (3,4).

2. $UV \to VU$

Доказательство.

1. $(UV \to V) \to ((UV \to U) \to (UV \to VU))$

– аксиома по схеме 2в.

2в. $(U \to V) \to ((U \to Q) \to (U \to VQ))$

$U := UV$, $V := V$, $Q := U$.

2. $UV \to V$ – аксиома по схеме 2б.
3. $(UV \to U) \to (UV \to VU)$

– правило заключения (1,2).

4. $UV \to U$ – аксиома по схеме 2а.
5. $UV \to VU$ – правило заключения (3,4).

3. $U \vee U \to U$

Доказательство.

1. $(U \to U) \to ((U \to U) \to (U \vee U \to U))$

– аксиома по схеме 3в.

3в. $(U \to Q) \to ((V \to Q) \to (U \vee V \to Q))$

$U := U$, $V := U$, $Q := U$.

2. $U \to U$ – доказуемая формула.
3. $(U \to U) \to (U \vee U \to U)$

– правило заключения (1,2).

4. $U \vee U \to U$ – правило заключения (3,2).

### 3.3. Формальный вывод и выводимые формулы

Пусть Г есть произвольное множество формул (или конечное, или бесконечное, или пустое).

**Определение 3.3.1.** Формальным выводом из Г называется конечная система формул, записанных друг под другом, каждая из которых либо является данной формулой, либо является доказуемой формулой, либо получается из двух вышестоящих формул по правилу заключения.

**Определение 3.3.2.** Формула исчисления высказываний называется выводимой из Г, если она стоит последней строчкой некоторого формального вывода из Г.

$\Gamma \vdash V$, «$\vdash$» – знак выводимости.

В частности, если Г конечное множество и $\Gamma = \{U_1, U_2, ..., U_n\}$, то записывают $U_1, U_2, ..., U_n \vdash V$, если Г есть пустое множество, то – $\vdash V$.

1. Понятие «выводимость из пустого множества» равносильно понятию «доказуемость»: $\{\vdash V\} \Leftrightarrow \{V - \textit{доказуема}\}$.

2. Каждая данная формула сама является выводимой, причем ее формальный вывод состоит всего из одной строчки: $V \in \Gamma \Rightarrow \Gamma \vdash V$.

3. Если формула $V$ выводима из некоторого множества Г, то она выводима из множества формул $\Gamma^{/}$, получаемого из Г:

а) добавлением произвольных формул;

б) удалением доказуемых формул.

4. Если из Г выводится несколько формул, а из этих формул выводится формула $V$, то из Г выводится эта формула $V$:

$$\Gamma \vdash U_1,\ \Gamma \vdash U_2,\ \ldots,\ \Gamma \vdash U_n \text{ и } U_1,\ U_2,\ \ldots,\ U_n \vdash V \Rightarrow \Gamma \vdash V.$$

5. Если формула $V$ выводима из бесконечного множества формул Г, то она выводима и из некоторого его конечного подмножества.

Пусть $\Gamma \vdash V$, $|\Gamma| = \infty$. Составим формальный вывод формулы $V$ из Г и обозначим через $\Gamma^{/}$ множество тех формул из Г, какие встречаются в этом формальном выводе. Тогда

1) $\Gamma^{/} \subseteq \Gamma$;

2) $\Gamma^{/}$ конечно;

3) $\Gamma^{/} \vdash V$.

6. Всякая строчка формального вывода является выводимой формулой. Действительно, всякий начальный отрезок формального вывода сам является формальным выводом.

**Пример.** $U \to (V \to Q),\ UV \vdash Q$.

1. $U \to (V \to Q)$ – первая данная формула;
2. $UV$ – вторая данная формула;
3. $UV \to U$ – аксиома по схеме 2а;
4. $U$ – правило заключения (3,2);
5. $V \to Q$ – правило заключения (1,4);
6. $UV \to V$ – аксиома по схеме 2б;
7. $V$ – правило заключения (6,2);
8. $Q$ – правило заключения (5,7).

**Пример.** $U,\ V \vdash UV$.

1. $U$ – первая данная формула;
2. $V$ – вторая данная формула;
3. $(U \to U) \to ((U \to V) \to (U \to UV))$ – аксиома по схеме 2в;
4. $U \to U$ – доказуемая формула;
5. $(U \to V) \to (U \to UV)$ – правило заключения (3,4);
6. $V \to (U \to V)$ – аксиома по схеме 1а;
7. $U \to V$ – правило заключения (6,2);
8. $U \to UV$ – правило заключения (5,7);
9. $UV$ – правило заключения (8,1).

## 3.4. Теорема дедукции

**Теорема 3.4.1.** Если Г, $R \vdash V$, то $\Gamma \vdash R \to V$.

Доказательство проведем методом математической индукции по числу строк $k$ данного вывода.

I. Пусть $k = 1$. Данный вывод состоит из одной строчки. Тогда единственной строчкой данного формального вывода стоит формула $V$. Формула $V$ может стоять первой строчкой данного вывода, если она или данная формула или доказуемая формула.

1.1. Пусть $V$ – данная формула. Тогда либо $V \in \Gamma$, либо $V$ совпадает с $R$.

1.1.1. Пусть $V \in \Gamma$.

1. $V$ – данная формула;
2. $V \to (R \to V)$ – аксиома по схеме 1а;
3. $R \to V$ – правило заключения (2,1).

Итак, $V \vdash R \to V$. Тогда $\Gamma \vdash R \to V$ по свойству 3.

1.1.2. Пусть $V = R$.

$$\{R \to R \text{ доказуема}\} \overset{1}{\Leftrightarrow} \{\vdash R \to R\} \overset{3}{\Leftrightarrow} \{\Gamma \vdash R \to R\} \Leftrightarrow \{\Gamma \vdash R \to V\}$$

1.2. Пусть $V$ – доказуемая формула.

1. $V$ – доказуемая формула;
2. $V \to (R \to V)$ – аксиома по схеме 1а;
3. $R \to V$ – правило заключения (2,1).

$$\{R \to V \text{ доказуемая}\} \overset{1}{\Leftrightarrow} \{\vdash R \to V\} \overset{3}{\Rightarrow} \{\Gamma \vdash R \to V\}$$

II. Пусть теорема дедукции доказана для всех $k \le m$. То есть теорема дедукции доказана в предположении, что данный формальный вывод состоит из числа строчек, не превосходящего $m$. Докажем теорему дедукции для $k = m + 1$. То есть докажем теорему в предположении, что число строк данного вывода равно $m + 1$.

Формула $V$ может стоять последней строчкой формального вывода, если

2.1. $V$ – данная формула;

2.2. $V$ – доказуемая формула;

2.3. $V$ получена по правилу заключения из двух вышестоящих формул.

В случаях 2.1, 2.2 доказательство аналогично предыдущему. Рассмотрим случай 2.3.

В этом случае в нашем формальном выводе выше формулы $V$ должны стоять формулы вида $U$ и $U \to V$.

$$(m+1)\ строка\begin{cases}\Gamma\\ R\\ \ldots\\ U\\ \ldots\\ U\to V\\ \ldots\\ V\end{cases}$$

Оборвем данный формальный вывод сразу после формулы $U$. Тогда мы получим новый формальный вывод, число строк которого не превосходит $m$. К нему мы можем применить теорему дедукции.

$$\Gamma,\ R\vdash U\Rightarrow\Gamma\vdash R\to U\,.$$

Если данный формальный вывод мы оборвем после формулы $U\to V$, то мы снова получим формальный вывод с числом строчек меньшим, либо равным $m$, и, следовательно, в этом случае мы снова сможем применить теорему дедукции.

$$\Gamma,\ R\vdash U\to V\Rightarrow\Gamma\vdash R\to(U\to V)\,.$$

Требуется доказать, что $\Gamma\vdash R\to V$. В силу свойства 4 остается доказать, что $R\to U$, $R\to(U\to V)\vdash R\to V$.

1. $R\to U$ – первая данная формула;
2. $R\to(U\to V)$ – вторая данная формула;
3. $(R\to(U\to V))\to((R\to U)\to(R\to V))$ – аксиома по схеме 1б;
4. $(R\to U)\to(R\to V)$ – правило заключения (3,2);
5. $R\to V$ – правило заключения (4,1).

Теорема доказана.

## 3.5. Метод вспомогательных гипотез

Пусть нам требуется вывести из $\Gamma$ некоторую формулу, содержащую одну или несколько посылок. То есть требуется доказать, что

$$\Gamma\vdash U_1\to(U_2\to\ldots(U_n\to V)\ldots)\,.$$

Для этого достаточно все эти посылки добавить к данному множеству формул $\Gamma$ и вывести последнее заключение:

$$\Gamma,\ U_1,\ U_2,\ldots,\ U_n\vdash V\,.$$

Действительно,

$$\Gamma,\ U_1,\ U_2,\ldots,\ U_n\vdash V\Rightarrow[\text{по теореме дедукции}]$$
$$\Gamma,\ U_1,\ U_2,\ldots,\ U_{n-1}\vdash U_n\to V\Rightarrow[\text{по теореме дедукции}]$$
$$\ldots$$
$$\Gamma,U_1\vdash U_2\to(\ldots(U_n\to V)\ldots)\Rightarrow[\text{по теореме дедукции}]$$
$$\Gamma\vdash U_1\to(U_2\to(\ldots(U_n\to V)\ldots))$$

**Пример.** Показать, что формула $\overline{U} \to (U \to V)$ доказуема.

Применим метод вспомогательных гипотез и предварительно докажем, что $\overline{U}, U \vdash V$.

1. $\overline{U}$ – первая данная формула;
2. $U$ – вторая данная формула;
3. $(\overline{V} \to U) \to (\overline{U} \to \overline{\overline{V}})$ – аксиома по схеме 4а;
4. $U \to (\overline{V} \to U)$ – аксиома по схеме 1а;
5. $\overline{V} \to U$ – правило заключения (4,2);
6. $\overline{U} \to \overline{\overline{V}}$ – правило заключения (3,5);
7. $\overline{\overline{V}}$ – правило заключения (6,1);
8. $\overline{\overline{V}} \to V$ – аксиома по схеме 4в;
9. $V$ – правило заключения (8,7).

Итак, $\overline{U},\ U \vdash V \Rightarrow$ [по теореме дедукции]

$\overline{U} \vdash U \to V \Rightarrow$ [по теореме дедукции]

$\vdash \overline{U} \to (U \to V) \overset{1}{\Rightarrow}$

$\{\overline{U} \to (U \to V)$ – доказуема$\}$.

## 3.6. Производные правила вывода

**1. Сложное правило заключения.**

$$U_1 \to (U_2 \to ...(U_n \to V)...),\ U_1,\ U_2, ...,\ U_n \vdash V$$

1. $U_1 \to (U_2 \to ...(U_n \to V)...)$
   – первая данная формула;
2. $U_1$ – вторая данная формула;
3. $U_2 \to (...(U_n \to V)...)$
   – правило заключения (1,2);
4. $U_2$ – третья данная формула;

…

$U_n \to V$ – правило заключения;

$U_n$ – $(n+1)$-я данная формула;

$V$ – правило заключения.

**2. Правило образования конъюнкции.**

$$U,\ V \vdash UV$$

Доказательство в примерах формальных выводов.

**3. Правило силлогизма.**

$$U \to V,\ V \to Q \vdash U \to Q$$

Применим метод вспомогательных гипотез и предварительно докажем, что $U \to V,\ V \to Q,\ U \vdash Q$.

1. $U \to V$ – первая данная формула;
2. $V \to Q$ – вторая данная формула;
3. $U$ – третья данная формула;
4. $V$ – правило заключения (1,3);
5. $Q$ – правило заключения (2,4).

$$U \to V,\ V \to Q,\ U \vdash Q \Rightarrow U \to V,\ V \to Q,\ \vdash U \to Q.$$

**4. Правило перестановки посылок.**

$$U \to (V \to Q) \vdash V \to (U \to Q)$$

Докажем, что $U \to (V \to Q),\ V,\ U \vdash Q$.

1. $U \to (V \to Q)$ – первая данная формула;
2. $V$ – вторая данная формула;
3. $U$ – третья данная формула;
4. $Q$ – сложное правило заключения (1,3,2).

$$U \to (V \to Q),\ V,\ U \vdash Q \Rightarrow \text{[по теореме дедукции]}$$

$$U \to (V \to Q),\ V \vdash U \to Q \Rightarrow \text{[по теореме дедукции]}$$

$$U \to (V \to Q) \vdash V \to (U \to Q).$$

**5. Правило соединения посылок.**

$$U \to (V \to Q) \vdash UV \to Q.$$

Ранее было доказано: $U \to (V \to Q)$, $UV \vdash Q$.

По теореме дедукции $U \to (V \to Q) \vdash UV \to Q$.

**6. Правило разъединения посылок (обратное правилу 5).**

$$UV \to Q \vdash U \to (V \to Q).$$

Предварительно докажем, что $UV \to Q,\ U,\ V \vdash Q$.

1. $UV \to Q$ – первая данная формула;
2. $U$ – вторая данная формула;
3. $V$ – третья данная формула;
4. $UV$ – правило образования конъюнкции (2,3);
5. $Q$ – правило заключения (1,4).

$$UV \to Q,\ U,\ V \vdash Q \Rightarrow \text{[по теореме дедукции]}$$

$$UV \to Q,\ U \vdash V \to Q \Rightarrow \text{[по теореме дедукции]}$$

$$UV \to Q \vdash U \to (V \to Q).$$

Приведем еще несколько примеров доказуемых формул.

**1. Закон де Моргана.**

$\overline{U \vee V} \to \overline{U}\ \overline{V}$ – доказуема.

Применим метод вспомогательных гипотез и предварительно докажем: $\overline{U \vee V} \vdash \overline{U}\ \overline{V}$.

1. $\overline{U \vee V}$ – данная формула;
2. $(U \to U \vee V) \to (\overline{U \vee V} \to \overline{U})$

   – аксиома по схеме 4а;
3. $U \to U \vee V$ – аксиома по схеме 3а;
4. $\overline{U}$ – сложное правило заключения (2,3,1);
5. $(V \to U \vee V) \to (\overline{U \vee V} \to \overline{V})$

   – аксиома по схеме 4а;
6. $V \to U \vee V$ – аксиома по схеме 3б;
7. $\overline{V}$ – сложное правило заключения (5,6,1);
8. $\overline{U}\ \overline{V}$ – правило образования конъюнкции (4,7).

$\overline{U \vee V} \vdash \overline{U}\ \overline{V} \Rightarrow\ \vdash \overline{U \vee V} \to \overline{U}\ \overline{V} \overset{1}{\Rightarrow} \{\overline{U \vee V} \to \overline{U}\ \overline{V}$ – доказуема$\}$

**2. Закон противоречия.**

$\overline{U\overline{U}}$ – доказуема.

1. $\overline{U} \to (U \to \overline{U \to U})$ – доказуема ($\overline{U} \to (U \to V)$ – доказуема);
2. $U \to (\overline{U} \to \overline{U \to U})$ – правило перестановки посылок (1);
3. $U\overline{U} \to \overline{U \to U}$ – правило соединения посылок (2);
4. $(U\overline{U} \to \overline{U \to U}) \to (\overline{\overline{U \to U}} \to \overline{U\overline{U}})$

   – аксиома по схеме 4а;
5. $U \to U$ – доказуемая формула;
6. $(U \to U) \to \overline{\overline{U \to U}}$ – аксиома по схеме 4б;
7. $\overline{\overline{U \to U}}$ – правило заключения (6,5);
8. $\overline{U\overline{U}}$ – сложное правило заключения (4,3,7).

**3. Закон исключения третьего.**

$U \vee \overline{U}$ – доказуема.

1. $\overline{U \vee \overline{U}} \to \overline{U}\ \overline{\overline{U}}$ – доказуема;
2. $(\overline{U \vee \overline{U}} \to \overline{U}\ \overline{\overline{U}}) \to (\overline{\overline{U}\ \overline{\overline{U}}} \to \overline{\overline{U \vee \overline{U}}})$

   – аксиома по схеме 4а;
3. $\overline{\overline{U}\ \overline{\overline{U}}}$ – доказуема;
4. $\overline{\overline{U \vee \overline{U}}}$ – сложное правило заключения (2,1,3);
5. $\overline{\overline{U \vee \overline{U}}} \to U \vee \overline{U}$ – аксиома по схеме 4в;
6. $U \vee \overline{U}$ – правило заключения (5,4).

## 3.7. Методы доказательства

Кроме метода вспомогательных гипотез рассмотрим еще три метода.

**1. Метод разбора случаев.**

**Лемма 3.7.1.** Если $\Gamma, P \vdash V$ и $\Gamma, Q \vdash V$, то $\Gamma,\ P \vee Q \vdash V$.

Пусть среди данных формул имеется дизъюнкция. Тогда нам достаточно вместо нужного нам вывода составить два формальных вывода. В первый раз вместо дизъюнкции в число данных формул включим первое слагаемое, а во втором случае мы вместо дизъюнкции в число данных формул включим второе слагаемое.

Доказательство.

По условию:

$$\Gamma, P \vdash V \overset{т.дед.}{\Rightarrow} \Gamma \vdash P \to V \overset{3а}{\Rightarrow} \Gamma,\ P \vee Q \vdash P \to V \ (1)$$

$$\Gamma, Q \vdash V \overset{т.дед.}{\Rightarrow} \Gamma \vdash Q \to V \overset{3а}{\Rightarrow} \Gamma,\ P \vee Q \vdash Q \to V \ (2)$$

По свойству 2: $\Gamma, P \vee Q \vdash P \vee Q$ (3)

По свойству 4 остается доказать, что $P \to V$, $Q \to V$, $P \vee Q \vdash V$.

1. $P \to V$ – первая данная формула;
2. $Q \to V$ – вторая данная формула;
3. $P \vee Q$ – третья данная формула;
4. $(P \to V) \to ((Q \to V) \to (P \vee Q \to V))$
 – аксиома по схеме 3в;
 $(U \to Q) \to ((V \to Q) \to (U \vee V \to Q))$
 $U := P$, $V := Q$, $Q := V$
5. $V$ – сложное правило заключения (4,1,2,3).

Лемма 3.7.1 доказана.

**2. Метод добавления противоположенных гипотез.**

**Лемма 3.7.2.** Если $\Gamma,\ P \vdash V$ и $\Gamma, \overline{P} \vdash V$, то $\Gamma \vdash V$.

Если формулу $V$ мы можем вывести добавляя к $\Gamma$ противоположенные гипотезы $P$ и $\overline{P}$, то мы можем вывести $V$ из $\Gamma$ и не добавляя этих гипотез.

Доказательство.

По условию $\left.\begin{matrix}\Gamma,\ P \vdash V \\ \Gamma, \overline{P} \vdash V\end{matrix}\right\} \overset{л.1}{\Rightarrow} \Gamma,\ P \vee \overline{P} \vdash V \overset{3б}{\Rightarrow} \Gamma \vdash V$ ($P \vee \overline{P}$ – доказуема).

Лемма 3.7.2 доказана.

**3. Метод сведения к противоречию.**

**Лемма 3.7.3.** Если $\Gamma,\ P \vdash V$ и $\Gamma, P \vdash \overline{V}$, то $\Gamma \vdash \overline{P}$.

Если мы должны вывести из $\Gamma$ формулу, стоящую под знаком отрицания, то мы можем эту формулу (без отрицания) добавить к числу данных формул и вывести два противоположенных утверждения.

Доказательство.

По условию $\Gamma,\ P \vdash V$ (1) и $\Gamma, P \vdash \overline{V}$ (2).

Докажем: $V, \overline{V} \vdash \overline{P}$ (3).

1. $V$ – первая данная формула;
2. $\overline{V}$ – вторая данная формула;
3. $\overline{V} \to (V \to \overline{P})$ – доказуемая формула;
4. $\overline{P}$ – сложное правило заключения (3,2,1).

Из (1), (2), (3) следует на основании свойства 4 что $\Gamma,\ P \vdash \overline{P}$, по свойству 2 $\Gamma, \overline{P} \vdash \overline{P}$, следовательно $\Gamma \vdash \overline{P}$.

Лемма 3.7.3 доказана.

**Примеры.**

1. $\overline{U}, \overline{V} \vdash \overline{U \vee V}$

1.1. Докажем, что $\overline{U}, \overline{V},\ U \vdash \overline{U \vee V}$.

1. $\overline{U}$ – первая данная формула;
2. $\overline{V}$ – вторая данная формула;
3. $U$ – третья данная формула;
4. $\overline{U} \to (U \to \overline{U \vee V})$ – доказуемая формула;
5. $\overline{U \vee V}$ – сложное правило заключения (4,1,3).

1.2. То, что $\overline{U}, \overline{V},\ V \vdash \overline{U \vee V}$ доказывается аналогично.

Из 1.1 и 1.2 следует, что $\overline{U}, \overline{V},\ U \vee V \vdash \overline{U \vee V}$.

По свойству 2 $\overline{U}, \overline{V}, \overline{U \vee V} \vdash \overline{U \vee V}$.

По лемме 3.7.2 $\overline{U}, \overline{V} \vdash \overline{U \vee V}$.

2. $U, \overline{V} \vdash \overline{U \to V}$.

2.1. Докажем, что $U, \overline{V},\ U \to V \vdash\ V$.

1. $U$ – первая данная формула;
2. $\overline{V}$ – вторая данная формула;
3. $U \to V$ – третья данная формула;
4. $V$ – правило заключения (3,1).

2.2. По свойству 2 $U, \overline{V},\ U \to V \vdash \overline{V}$.

Из 2.1 и 2.2 по лемме 3.7.3 $U, \overline{V} \vdash \overline{U \to V}$.

## 3.8. Связь между исчислением высказываний и алгеброй высказываний

**Теорема 3.8.1. (Непротиворечивость исчисления высказываний.)**

Если формула доказуема в исчислении высказываний, то она тождественно истинна в алгебре высказываний.

Доказательство.

1. Используя критерий тождественной истинности докажем, что каждая аксиома исчисления высказываний тождественно истинна в алгебре высказываний.

1а) $U \to (V \to U) = \overline{U} \vee (V \to U) = \overline{U} \vee \overline{V} \vee U$

1б) $(U \to (V \to Q)) \to ((U \to V) \to (U \to Q)) =$

$= \overline{U \to (V \to Q)} \vee ((U \to V) \to (U \to Q)) =$

$$= U\overline{V \to Q} \vee \overline{U \to V} \vee (U \to Q) =$$
$$= UV\overline{Q} \vee U\overline{V} \vee \overline{U} \vee Q = UV\overline{Q} \vee (U \vee \overline{U})(\overline{V} \vee \overline{U}) \vee Q = UV\overline{Q} \vee \overline{V} \vee \overline{U} \vee Q =$$
$$= (U \vee \overline{V} \vee \overline{U} \vee Q)(V \vee \overline{V} \vee \overline{U} \vee Q)(\overline{Q} \vee \overline{V} \vee \overline{U} \vee Q)$$

2в) $(U \to V) \to ((U \to Q) \to (U \to VQ)) = \overline{U \to V} \vee ((U \to Q) \to (U \to VQ)) =$
$$= U\overline{V} \vee \overline{U \to Q} \vee (U \to VQ) = U\overline{V} \vee U\overline{Q} \vee \overline{U} \vee VQ = U(\overline{V} \vee \overline{Q}) \vee \overline{U} \vee VQ =$$
$$= (U \vee \overline{U})(\overline{V} \vee \overline{Q} \vee \overline{U}) \vee VQ = \overline{V} \vee \overline{Q} \vee \overline{U} \vee VQ =$$
$$= (\overline{V} \vee \overline{Q} \vee \overline{U} \vee V)(\overline{V} \vee \overline{Q} \vee \overline{U} \vee Q)$$

3в) $(U \to Q) \to ((V \to Q) \to (U \vee V \to Q)) =$
$$= \overline{U \to Q} \vee ((V \to Q) \to (U \vee V \to Q)) =$$
$$= U\overline{Q} \vee \overline{V \to Q} \vee (U \vee V \to Q) =$$
$$= U\overline{Q} \vee V\overline{Q} \vee \overline{U \vee V} \vee Q =$$
$$= (U \vee V)\overline{Q} \vee Q \vee \overline{U \vee V} =$$
$$= (U \vee V \vee Q)(\overline{Q} \vee Q) \vee \overline{U \vee V} =$$
$$= U \vee V \vee Q \vee \overline{U}\,\overline{V} =$$
$$= (U \vee V \vee Q \vee \overline{U})(U \vee V \vee Q \vee \overline{V})$$

Аналогично проверяются все остальные аксиомы.

2. Докажем, что применение правила заключения к тождественно истинным формулам приводит к тождественно истинной формуле.

$\dfrac{U \to V, U}{V}$ – правило заключения.

Дано: $U \to V$ тождественно истинна и $U$ тождественно истинна.

Доказать: $V$ тождественно истинна.

Пусть $V$ не тождественно истинна, то есть пусть $V = Л$ хотя бы в одном случае. Тогда в этом случае $U \to V = И \to Л = Л$. Следовательно, формула $U \to V$ опровержима, что противоречит условию. Значит, $V$ тождественно истинна.

3. Всякая доказуемая формула исчисления высказываний тождественно истинна, так как она получается из аксиом с помощью конечного числа применений правила заключения.

Теорема доказана.

**Основная лемма.** Пусть формула $U$ составлена из пропозициональных букв $X_1$, $X_2$, …, $X_n$: $U(X_1, X_2, ..., X_n)$. Всякому набору $\alpha$ длины $n$, состоящему из букв $И$ и $Л$, мы поставим в соответствие набор $\alpha^*$ длины $n$, состоящий из пропозициональных букв или их отрицаний, по следующему принципу: букве $И$ соответствует пропозициональная буква, а букве $Л$ соответствует отрицание пропозициональной буквы. Если формула $U$ на некотором наборе $\alpha$ принимает значение $И$, то из соответствующего набора $\alpha^*$ выводима сама формула $U$. Если формула $U$ на некотором наборе $\alpha$ принимает значение $Л$, то из соответствующего набора $\alpha^*$ выводима формула $\overline{U}$.

**Пример.** $U = X \to \overline{Y}$, $n = 2$.

а) $\alpha = \{И, И\}$, $\alpha^* = \{X, Y\}$, $U(\alpha) = U(И, И) = И \to Л = Л$

$\alpha^* \vdash \overline{U} \Leftrightarrow X, Y \vdash \overline{X \to \overline{\overline{Y}}}$.

б) $\alpha = \{И, Л\}$, $\alpha^* = \{X, \overline{Y}\}$, $U(\alpha) = U(И, Л) = И$

$\alpha^* \vdash U \Leftrightarrow X, \overline{Y} \vdash X \to \overline{Y}$.

в) $\alpha = \{Л, И\}$, $\alpha^* = \{\overline{X}, Y\}$, $U(\alpha) = U(Л, И) = И$

$\alpha^* \vdash U \Leftrightarrow \overline{X}, Y \vdash X \to \overline{Y}$.

г) $\alpha = \{Л, Л\}$, $\alpha^* = \{\overline{X}, \overline{Y}\}$, $U(\alpha) = U(Л, Л) = И$

$\alpha^* \vdash U \Leftrightarrow \overline{X}, \overline{Y} \vdash X \to \overline{Y}$.

Доказательство.

Доказательство состоит из трех частей, соответствующих трем пунктам в определении формулы.

1 часть. Докажем основную лемму для случая, когда формула $U$ есть просто пропозициональная буква: $n = 1$, $U = X_1$.

а) $\alpha = \{И\}$, $\alpha^* = \{X_1\}$, $U(\alpha) = U(И) = И$.

Требуется доказать, что $\alpha^* \vdash U \Leftrightarrow X_1 \vdash X_1$ (по свойству 2).

б) $\alpha = \{Л\}$, $\alpha^* = \{\overline{X}_1\}$, $U(\alpha) = U(Л) = Л$.

Требуется доказать, что $\alpha^* \vdash \overline{U} \Leftrightarrow \overline{X}_1 \vdash \overline{X}_1$ (по свойству 2).

2 часть. Допустим, что основная лемма уже доказана для формулы $U$, докажем ее для формулы $\overline{U}$.

Пусть $\alpha$ есть произвольный набор длины $n$ из букв $И$ и $Л$. Возможны два случая:

а) $U(\alpha) = И$, б) $U(\alpha) = Л$.

а) $U(\alpha) = И \overset{осн.\ л.}{\Rightarrow} \alpha^* \vdash U$, $\overline{U(\alpha)} = Л$. Требуется доказать, что $\alpha^* \vdash \overline{\overline{U}}$. Остается доказать, что $U \vdash \overline{\overline{U}}$.

1. $U$ – данная формула;
2. $\overline{\overline{U}} \to \overline{\overline{U}}$ – аксиома по схеме 4б;
3. $\overline{\overline{U}}$ – правило заключения (2,1).

б) $U(\alpha) = Л \overset{осн.\ л.}{\Rightarrow} \alpha^* \vdash \overline{U}$, $\overline{U(\alpha)} = И$. Требуется доказать, что $\alpha^* \vdash \overline{U}$.

3 часть. Допустим, что основная лемма уже доказана для формул $U$ и $V$. Докажем ее для конъюнкции, дизъюнкции и импликации этих формул.

1. Рассмотрим конъюнкцию $UV$.

Пусть $\alpha$ набор длины $n$ из букв $И$ и $Л$. Возможны 4 случая.

а) $\left.\begin{array}{l} U(\alpha) = И \\ V(\alpha) = И \end{array}\right\} \overset{осн.\ л.}{\Rightarrow} \begin{array}{l} \alpha^* \vdash U \\ \alpha^* \vdash V \end{array}$

$UV(\alpha) = И$. Требуется доказать, что $\alpha^* \vdash UV$. По свойству 4 остается доказать, что $U$, $V \vdash UV$. А это было доказано выше.

б) $\left.\begin{array}{l} U(\alpha)=И \\ V(\alpha)=Л \end{array}\right\} \overset{осн.\ л.}{\Rightarrow} \begin{array}{l} \alpha^* \vdash U \\ \alpha^* \vdash \overline{V} \end{array}$

$UV(\alpha)=Л$. Требуется доказать, что $\alpha^* \vdash \overline{UV}$. По свойству 4 остается доказать, что $U, \overline{V} \vdash \overline{UV}$.

1. $U$ – первая данная формула;
2. $\overline{V}$ – вторая данная формула;
3. $(UV \to V) \to (\overline{V} \to \overline{UV})$
   – аксиома по схеме 4а;
4. $UV \to V$ – аксиома по схеме 2б;
5. $\overline{UV}$ – сложное правило заключения (3,4,2).

Случаи в) $U(\alpha)=Л$, $V(\alpha)=И$ и г) $U(\alpha)=Л$, $V(\alpha)=Л$ рассматриваются аналогично случаю б), только в случае в) вместо схемы 2б используется схема 2а.

2. Рассмотрим дизъюнкцию $U \vee V$.

а) $\left.\begin{array}{l} U(\alpha)=И \\ V(\alpha)=И \end{array}\right\} \overset{осн.\ л.}{\Rightarrow} \begin{array}{l} \alpha^* \vdash U \\ \alpha^* \vdash V \end{array}$

$(U \vee V)(\alpha)=И$. Требуется доказать, что $\alpha^* \vdash U \vee V$. По свойству 4 остается доказать, что $U,\ V \vdash U \vee V$.

1. $U$ – первая данная формула;
2. $V$ – вторая данная формула;
3. $U \to U \vee V$ – аксиома по схеме 3а;
4. $U \vee V$ – правило заключения (3,1).

Случаи б), в) рассматриваются аналогично случаю а), только в случае в) вместо схемы 3а используется схема 3б.

г) $\left.\begin{array}{l} U(\alpha)=Л \\ V(\alpha)=Л \end{array}\right\} \overset{осн.\ л.}{\Rightarrow} \begin{array}{l} \alpha^* \vdash \overline{U} \\ \alpha^* \vdash \overline{V} \end{array}$

$(U \vee V)(\alpha)=Л$. Требуется доказать, что $\alpha^* \vdash \overline{U \vee V}$. По свойству 4 остается доказать, что $\overline{U}, \overline{V} \vdash \overline{U \vee V}$, а это было доказано выше.

3. Рассмотрим импликацию $U \to V$.

а) $\left.\begin{array}{l} U(\alpha)=И \\ V(\alpha)=И \end{array}\right\} \overset{осн.\ л.}{\Rightarrow} \begin{array}{l} \alpha^* \vdash U \\ \alpha^* \vdash V \end{array}$

$(U \to V)(\alpha)=И$. Требуется доказать, что $\alpha^* \vdash U \to V$. Остается доказать, что $U,\ V \vdash U \to V$.

1. $U$ – первая данная формула;
2. $V$ – вторая данная формула;
3. $V \to (U \to V)$ – аксиома по схеме 1а;
4. $U \to V$ – правило заключения (3,2).

б) $\left.\begin{array}{l} U(\alpha)=И \\ V(\alpha)=Л \end{array}\right\} \overset{осн.\ л.}{\Rightarrow} \begin{array}{l} \alpha^* \vdash U \\ \alpha^* \vdash \overline{V} \end{array}$

$(U \to V)(\alpha)=Л$. Требуется доказать, что $\alpha^* \vdash \overline{U \to V}$. По свойству 4 остается доказать, что $U, \overline{V} \vdash \overline{U \to V}$, а это было доказано выше.

в) $\left.\begin{array}{l} U(\alpha)=Л \\ V(\alpha)=И \end{array}\right\}$ Этот случай аналогичен случаю а).

г) $\left.\begin{array}{l} U(\alpha)=Л \\ V(\alpha)=Л \end{array}\right\} \overset{осн.\ л.}{\Rightarrow} \begin{array}{l} \alpha^* \vdash \overline{U} \\ \alpha^* \vdash \overline{V} \end{array}$

$(U \to V)(\alpha)=И$. Требуется доказать, что $\alpha^* \vdash U \to V$. Остается доказать, что $\overline{U}, \overline{V} \vdash U \to V$.

1. $\overline{U}$ – первая данная формула;
2. $\overline{V}$ – вторая данная формула;
3. $\overline{U} \to (U \to V)$ – доказуемая формула;
4. $U \to V$ – правило заключения (3,1).

Основная лемма доказана.

**Теорема 3.8.2. (Полнота исчисления высказываний.)** Если формула тождественно истинна в алгебре высказываний, то она доказуема в исчислении высказываний.

Доказательство.

Обозначим через $n$ число пропозициональных букв, входящих в данную формулу $U$. Доказательство проведем для частного случая, когда $n=3$.

Дано: $U(X,Y,Z)$ – тождественно истинная.

Доказать: $U(X,Y,Z)$ – доказуема.

$$\left.\begin{array}{l} U(И,И,И)=И \\ U(И,И,Л)=И \\ U(И,Л,И)=И \\ U(И,Л,Л)=И \\ U(Л,И,И)=И \\ U(Л,И,Л)=И \\ U(Л,Л,И)=И \\ U(Л,Л,Л)=И \end{array}\right\} \overset{осн.\ л.}{\Rightarrow} \left.\begin{array}{l} \left.\begin{array}{l} \left.\begin{array}{l} X,Y,Z \vdash U \\ X,Y,\overline{Z} \vdash U \end{array}\right\} \overset{л.2}{\Rightarrow} X,Y \vdash U \\ \left.\begin{array}{l} X,\overline{Y},Z \vdash U \\ X,\overline{Y},\overline{Z} \vdash U \end{array}\right\} \overset{л.2}{\Rightarrow} X,\overline{Y} \vdash U \end{array}\right\} \overset{л.2}{\Rightarrow} X \vdash U \\ \left.\begin{array}{l} \left.\begin{array}{l} \overline{X},Y,Z \vdash U \\ \overline{X},Y,\overline{Z} \vdash U \end{array}\right\} \overset{л.2}{\Rightarrow} \overline{X},Y \vdash U \\ \left.\begin{array}{l} \overline{X},\overline{Y},Z \vdash U \\ \overline{X},\overline{Y},\overline{Z} \vdash U \end{array}\right\} \overset{л.2}{\Rightarrow} \overline{X},\overline{Y} \vdash U \end{array}\right\} \overset{л.2}{\Rightarrow} \overline{X} \vdash U \end{array}\right\} \overset{л.2}{\Rightarrow} \vdash U \overset{1}{\Leftrightarrow} \{U\ док.\}$$

Для остальных $n$ доказательство проводится аналогично, причем каждый раз приходится рассматривать $2^n$ случаев.

**Следствие.** Формула доказуема в исчислении высказываний тогда и только тогда, когда она тождественно истинна в алгебре высказываний.

# ГЛАВА 4
# ИСЧИСЛЕНИЕ ПРЕДИКАТОВ

## 4.1. Введение

В исчислении предикатов изучаются те же логические законы, что и в алгебре предикатов, но изучение их ведется аксиоматически.

**I. Перечисление символов.**

1. Буквенные символы.

a. Пропозициональные буквы – большие латинские буквы с индексами внизу или без индексов.

b. Предикатные буквы – большие латинские буквы с индексами вверху (без индексов внизу или с ними). $P^{(1)}$, $Q^{(1)}$, …, $P_1^{(1)}$, $Q_1^{(1)}$, …, $P_2^{(1)}$, $Q_2^{(1)}$, … – символы одноместных предикатов. $P^{(2)}$, $Q^{(2)}$, …, $P_1^{(2)}$, $Q_1^{(2)}$, …, $P_2^{(3)}$, $Q_2^{(3)}$, … – символы двухместных предикатов, и т. д.

c. Символы свободных переменных – малые латинские буквы из начала алфавита без индексов или с индексами внизу: $a$, $b$, …, $a_1$, $b_1$, …, $a_2$, $b_2$, … .

d. Символы связанных переменных – малые латинские буквы из конца алфавита без индексов или с индексами внизу: $x$, $y$, …, $x_1$, $y_1$, …, $x_2$, $y_2$, … .

2. Логические символы: $\wedge$, $\vee$, $\to$, $\overline{\phantom{x}}$, $\forall$, $\exists$.
3. Вспомогательные символы: **(**, **)**, **,** .

**II. Определение формулы.**

1. Всякая пропозициональная буква есть формула.
2. Если $P^{(m)}$ – предикатная буква, а $a_1$, $a_2$, …, $a_m$ – символы свободных переменных, то $P^{(m)}(a_1,a_2,...,a_m)$ есть формула.
3. Если $U$ – формула, то $\overline{U}$ – формула.
4. Если $U$ и $V$ – формулы, то $(U \wedge V)$, $(U \vee V)$, $(U \to V)$ – формулы.
5. Если $U(a)$ – формула, то $\forall x U(x)$ и $\exists x U(x)$ – формулы, где $x$ – любая связанная переменная, которая раньше не входила в $U(a)$.

Формулы, определенные в пунктах 1,2 называются элементарными. В пунктах 3,4,5 указываются правила, по которым из имеющихся формул можно получать новые формулы.

**Пример.**

$\left(\forall x P^{(2)}(a,x) \vee \exists z \overline{Q^{(1)}(z)}\right)$ – формула. Действительно, $P^{(2)}(a,b)$ и $Q^{(1)}(c)$ – формулы согласно пункту (2), $\overline{Q^{(1)}(c)}$ есть формула согласно пункту (3), $\forall x P^{(2)}(a,x)$ и $\exists z \overline{Q^{(1)}(z)}$ – формулы согласно пункту (5), $\left(\forall x P^{(2)}(a,x) \vee \exists z \overline{Q^{(1)}(z)}\right)$ есть формула согласно пункту (4).

Для упрощения записи формул исчисления предикатов примем все те же соглашения, что и в исчислении высказываний, и договоримся опускать верхние символы у предикатных букв.

**Пример.**

$\forall x P(a,x) \vee \exists z \overline{Q(z)}$ – сокращенная запись формулы.

**III. Аксиомы исчисления предикатов.**

Схемы аксиом для импликации, конъюнкции, дизъюнкции и отрицания остаются теми же. Добавляется пятая группа.

5. Схемы для кванторов.

5а) $\forall x U(x) \to U(a)$

Если утверждение $U$ справедливо для всех элементов, то оно справедливо и для элемента $a$.

5б) $U(a) \to \exists x U(x)$

Если утверждение $U$ справедливо для элемента $a$, то найдется такой элемент, для которого оно справедливо.

В схемах 5 выражение $U(a)$ получается из $U(x)$ путем замены всех вхождений $x$ на букву $a$.

**Определение 4.1.1.** Аксиомой исчисления предикатов называется любая формула, полученная по одной из перечисленных схем.

**IV. Основные правила вывода.**

1. Правило заключения: $\dfrac{U \to V, U}{V}$.

2. Правило для квантора всеобщности: $\dfrac{U \to V(a)}{U \to \forall x V(x)}$ ($U$ не содержит букву $a$). Если из справедливости $U$ следует справедливость $V(a)$, где $a$ произвольный элемент, то из справедливости $U$ следует, что утверждение $V$ справедливо для всех элементов.

3. Правило для квантора существования: $\dfrac{V(a) \to U}{\exists x V(x) \to U}$($U$ не содержит букву $a$). Если справедливость $U$ следует из справедливости $V(a)$, где $a$ произвольный элемент, то справедливость $U$ следует из существования такого элемента, для которого утверждение $V$ справедливо.

**Замечание.** В правилах 2, 3 $V(x)$ получается из $V(a)$ заменой всех вхождений $a$ на букву $x$.

**V. Определение формального доказательства и доказуемой формулы.**

**Определение 4.1.2.** Формальным доказательством называется конечная система формул, записанных друг под другом, каждая из которых либо аксиома, либо получается из вышестоящих формул по одному из основных правил вывода.

**Определение 4.1.3.** Формула исчисления предикатов называется доказуемой, если она стоит последней строчкой некоторого формального доказательства.

Справедливы следствия, аналогичные следствиям 1, 2, 3 из исчисления высказываний.

**Следствие 4.** Если формула $U(X_1, X_2, ..., X_n)$, где $X_i$ $(i=\overline{1,n})$ – пропозициональные буквы, доказуема в исчислении высказываний, то формула $U(V_1, V_2, ..., V_n)$, где $V_i$ $(i=\overline{1,n})$ – формулы исчисления предикатов, доказуема в исчислении предикатов.

Действительно, все схемы аксиом исчисления высказываний присутствуют и в исчислении предикатов. И, кроме того, правило заключения, которое было единственным основным правилом в исчислении высказываний, присутствует и в исчислении предикатов. Например, формула $X \to X$ доказуема в исчислении высказываний, значит, формула $\forall z P(z) \to \forall z P(z)$ доказуема в исчислении предикатов.

## 4.2. Примеры доказуемых формул

1. $\exists x \overline{U(x)} \to \overline{\forall x U(x)}$

Доказательство.

1. $\forall x U(x) \to U(a)$ – аксиома по схеме 5а;
2. $(\forall x U(x) \to U(a)) \to (\overline{U(a)} \to \overline{\forall x U(x)})$
   – аксиома по схеме 4а.
   4а. $(U \to V) \to (\overline{V} \to \overline{U})$
   $U := \forall x U(x)$; $V := U(a)$
3. $\overline{U(a)} \to \overline{\forall x U(x)}$ – правило заключения (2,1);
4. $\exists x \overline{U(x)} \to \overline{\forall x U(x)}$ – правило для квантора существования (3).

2. $\overline{\exists x U(x)} \to \forall x \overline{U(x)}$

Доказательство.

1. $U(a) \to \exists x U(x)$ – аксиома по схеме 5б;
2. $(U(a) \to \exists x U(x)) \to (\overline{\exists x U(x)} \to \overline{U(a)})$
   – аксиома по схеме 4а.
   4а. $(U \to V) \to (\overline{V} \to \overline{U})$
   $U := U(a)$; $V := \exists x U(x)$;
3. $\overline{\exists x U(x)} \to \overline{U(a)}$ – правило заключения (2,1);
4. $\overline{\exists x U(x)} \to \forall x \overline{U(x)}$ – правило для квантора всеобщности (3).

## 4.3. Определения формального вывода и выводимой формулы

Обозначим через Г произвольное множество формул исчисления предикатов.

**Определение 4.3.1.** Формальным выводом из Г называется конечная система формул, записанных друг под другом, каждая из которых является либо данной формулой, либо доказуемой формулой, либо получается из вышестоящих формул по одному из основных правил вывода.

**Определение 4.3.2.** Формула исчисления предикатов называется выводимой из Г, если она стоит последней строчкой некоторого формального вывода из Г.

## 4.4. Производные правила вывода

Сохраняются производные правила вывода, доказанные в исчислении высказываний.

**1. Правило обобщения:** $U(a) \vdash \forall x U(x)$.

1. $U(a)$ – данная формула;
2. $U(a) \to ((A \to A) \to U(a))$
   – аксиома по схеме 1а;
   1а. $U \to (V \to U)$; $U := U(a)$, $V := A \to A$;
3. $(A \to A) \to U(a)$ – правило заключения (2,1);
4. $(A \to A) \to \forall x U(x)$ – правило для квантора всеобщности (3);
5. $(A \to A)$ – доказуемая формула;
6. $\forall x U(x)$ – правило заключения (4,5).

**2. Правило навешивания кванторов всеобщности на члены импликации:** $U(a) \to V(a) \vdash \forall x U(x) \to \forall x V(x)$.

1. $U(a) \to V(a)$ – данная формула;
2. $\forall x U(x) \to U(a)$ – аксиома по схеме 5а;
3. $\forall x U(x) \to V(a)$ – правило силлогизма (2,1);
4. $\forall x U(x) \to \forall x V(x)$ – правило для квантора существования (3).

**3. Правило навешивания кванторов существования на члены импликации:** $U(a) \to V(a) \vdash \exists x U(x) \to \exists x V(x)$.

1. $U(a) \to V(a)$ – данная формула;
2. $V(a) \to \exists x V(x)$ – аксиома по схеме 5б;
3. $U(a) \to \exists x V(x)$ – правило силлогизма (1,2);
4. $\exists x U(x) \to \exists x V(x)$ – правило для квантора существования (3).

## 4.5. Теорема дедукции

**Теорема 4.5.1.** Если Г, $R \vdash V$ и $R$ – замкнутая формула, то $\Gamma \vdash R \to V$.

Проведем доказательство методом математической индукции по числу строк $k$ данного формального вывода.

I. Доказательство теоремы дедукции для $k = 1$ проводится аналогично предыдущему.

II. Пусть теорема доказана для всех $k \le m$, то есть теорема доказана в предположении, что число строк данного вывода не превосходит *m*. Докажем теорему для $k = m + 1$. То есть докажем теорему, предположив, что данный формальный вывод содержит $m + 1$ строчку. Последней строкой этого формального вывода стоит формула *V*. Формула *V* может стоять строкой формального вывода в силу следующих причин:

1) *V* – данная формула;
2) *V* – доказуемая формула;
3) *V* получена по правилу заключения;
4) *V* получена по правилу для квантора всеобщности;
5) *V* получена по правилу для квантора существования.

В первых трех случаях доказательство аналогично предыдущему.

4) Напомним правило для квантора всеобщности: $\dfrac{U \to V(a)}{U \to \forall x V(x)}$ (*U* не содержит *a*). В нашем случае формула *V* имеет вид $V = S \to \forall x T(x)$. Причем в нашем формальном выводе выше формулы *V* должна стоять формула вида $S \to T(a)$, где формула *S* не содержит буквы *a*.

$$m+1\begin{cases}\Gamma \\ R \\ \ldots \\ S \to T(a) \\ \ldots \\ S \to \forall x T(x)\end{cases}$$

Оборвем данный формальный вывод сразу после формулы $S \to T(a)$. Тогда мы получим новый формальный вывод, число строк которого не превосходит *m*. И, следовательно, к этому новому формальному выводу мы уже можем применить теорему дедукции.

$$\Gamma,\ R \vdash S \to T(a) \Rightarrow \Gamma \vdash R \to (S \to T(a))$$

Требуется доказать, что $\Gamma \vdash R \to (S \to \forall x T(x))$.

Остается доказать, что $R \to (S \to T(a)) \vdash R \to (S \to \forall x T(x))$.

1. $R \to (S \to T(a))$ – данная формула;
2. $RS \to T(a)$ – правило соединения посылок (1);
3. $RS \to \forall x T(x)$ – правило для квантора всеобщности (2);
4. $R \to (S \to \forall x T(x))$ – правило разъединения посылок (3).

Мы имели право ко второй строке применить правило для квантора всеобщности, так как посылка *RS* не содержит буквы *a*. Действительно, известно, что формула *S* не содержит буквы *a*, а формула *R* по условию замкнута, следовательно, она вовсе не содержит свободных переменных.

5) Напомним правило для квантора существования: $\dfrac{V(a) \to U}{\exists x V(x) \to U}$ ($U$ не содержит $a$). В нашем случае формула $V$ имеет вид $V = \exists x T(x) \to S$. Причем в нашем формальном выводе выше формулы $V$ стоит формула вида $T(a) \to S$ и формула $S$ не содержит буквы $a$.

$$m+1\begin{cases} \Gamma \\ R \\ \ldots \\ T(a) \to S \\ \ldots \\ \exists x T(x) \to S \end{cases}$$

Оборвем данный формальный вывод сразу после формулы $T(a) \to S$. Тогда мы получим новый формальный вывод с числом строк, меньшим либо равным $m$, к которому мы можем применить теорему дедукции.

$\Gamma,\ R \vdash T(a) \to S \Rightarrow \Gamma \vdash R \to (T(a) \to S)$

Требуется доказать, что $\Gamma \vdash R \to (\exists x T(x) \to S)$.

Остается доказать, что $R \to (T(a) \to S) \vdash R \to (\exists x T(x) \to S)$.

1. $R \to (T(a) \to S)$ – данная формула;
2. $T(a) \to (R \to S)$ – правило перестановки посылок (1);
3. $\exists x T(x) \to (R \to S)$ – правило для квантора существования (2);
4. $R \to (\exists x T(x) \to S)$ – правило перестановки посылок (3).

Применение правила для квантора существования ко второй строке было возможным, так как заключение $R \to S$ не содержит буквы $a$ ($S$ не содержит буквы $a$, а $R$ замкнута).

Теорема доказана.

**Лемма 4.5.1.** Если $\Gamma,\ P \vdash V$; $\Gamma,\ Q \vdash V$; $P$ и $Q$ – замкнуты; то $\Gamma,\ P \vee Q \vdash V$.

**Лемма 4.5.2.** Если $\Gamma,\ P \vdash V$; $\Gamma, \overline{P} \vdash V$; $P$ – замкнута; то $\Gamma \vdash V$.

**Лемма 4.5.3.** Если $\Gamma,\ P \vdash V$; $\Gamma,\ P \vdash \overline{V}$; $P$ – замкнута; то $\Gamma \vdash \overline{P}$.

В исчисление предикатов применимы методы вспомогательных гипотез, разбора случаев, противоположных гипотез и сведения к противоречию, так как эти методы опираются соответственно на теорему дедукции и леммы 4.5.1, 4.5.2, 4.5.3.

**Пример.**

$\left(\forall x P(x) \to \exists x P(x)\right) \to \exists x (P(x) \to Q(x))$ – доказуемая формула.

Применим метод вспомогательных гипотез и докажем, что

$\forall x P(x) \to \exists x P(x) \vdash \exists x (P(x) \to Q(x))$.

Применим метод противоположных гипотез и докажем два утверждения:

I. $\forall xP(x) \to \exists xQ(x)$, $\forall xP(x) \vdash \exists x(P(x) \to Q(x))$.

II. $\forall xP(x) \to \exists xQ(x)$, $\overline{\forall xP(x)} \vdash \exists x(P(x) \to Q(x))$.

I.

1. $\forall xP(x) \to \exists xQ(x)$ – первая данная формула;
2. $\forall xP(x)$ – вторая данная формула;
3. $\exists xQ(x)$ – правило заключения (1,2);
4. $Q(a) \to (P(a) \to Q(a))$
   – аксиома по схеме 1а;
   1а. $U \to (V \to U)$, $U := Q(a)$, $V := P(a)$.
5. $\exists xQ(x) \to \exists x(P(x) \to Q(x))$
   –правило навешивания кванторов существования на члены импликации (4);
6. $\exists x(P(x) \to Q(x))$ – правило заключения (5,3).

II.

1. $\forall xP(x) \to \exists xQ(x)$ – первая данная формула;
2. $\overline{\forall xP(x)}$ – вторая данная формула;
3. $\overline{\forall xP(x)} \to \exists x\overline{P(x)}$ – доказуемая формула;
4. $\exists x\overline{P(x)}$ – правило заключения (3,2);
5. $\overline{P(a)} \to (P(a) \to Q(a))$
   – доказуемая формула;
6. $\exists x\overline{P(x)} \to \exists x(P(x) \to Q(x))$
   –правило навешивания кванторов существования на члены импликации (5);
7. $\exists x(P(x) \to Q(x))$ – правило заключения (6,4).

Из I, II и из того, что $\forall xP(x)$ – замкнутая формула, по лемме 4.5.2 следует, что $\forall xP(x) \to \exists xP(x) \vdash \exists x(P(x) \to Q(x))$. Так как $\forall xP(x) \to \exists xQ(x)$ – замкнутая формула, то по теореме дедукции

$$\vdash \left(\forall xP(x) \to \exists xP(x)\right) \to \exists x(P(x) \to Q(x)).$$

По свойству 1 рассматриваемая формула является доказуемой.

## 4.6. Связь между исчислением предикатов и алгеброй предикатов

**Теорема 4.6.1. (Непротиворечивость исчисления предикатов.)** Если формула доказуема в исчислении предикатов, то она тождественно истинна в алгебре предикатов.

Доказательство.

I часть. Докажем, что каждая аксиома исчисления предикатов тождественно истинна в алгебре предикатов. Для схем I, II, III и IV групп доказательство аналогично тому, что было приведено в исчислении высказываний.

5а) Докажем, что формула $\forall x U(x) \to U(a)$ тождественно истинна. Пусть $\forall x U(x) \to U(a) = Л$ хотя бы в одном случае. Тогда $\forall x U(x) = И$ и $U(a) = Л$. Так как $U(a) = Л$, то $\forall x U(x) = Л$. Противоречие говорит о том, что формула $\forall x U(x) \to U(a)$ тождественно истинна.

5б) Докажем, что формула $U(a) \to \exists x U(x)$ тождественно истинна. Пусть $U(a) \to \exists x U(x) = Л$ хотя бы в одном случае. Тогда $U(a) = И$ и $\exists x U(x) = Л$. Так как $U(a) = И$, то $\exists x U(x) = И$. Противоречие говорит о том, что формула $U(a) \to \exists x U(x)$ тождественно истинна.

II часть. Докажем, что применение основных правил вывода к тождественно истинным формулам снова приводит к тождественно истинным формулам.

1. Для правила заключения это было доказано в предыдущей главе.

2. Рассмотрим правило для квантора всеобщности $\dfrac{U \to V(a)}{U \to \forall x V(x)}$, ($U$ не содержит $a$). Пусть $U \to V(a)$ – тождественно истинна. Докажем, что $U \to \forall x V(x)$ тождественно истинна. Проведем доказательство методом от противного. Пусть $U \to \forall x V(x) = Л$ хотя бы в одном случае. Тогда $U = И$, $\forall x V(x) = Л$. Так как $\forall x V(x) = Л$, то найдется такое $a$, что $V(a) = Л$. Следовательно, найдется такое $a$, что $U \to V(a) = Л$. Противоречие говорит о том, что $U \to \forall x V(x)$ тождественно истинна.

3. Рассмотрим правило для квантора существования $\dfrac{V(a) \to U}{\exists x V(x) \to U}$, ($U$ не содержит $a$). Пусть $V(a) \to U$ – тождественно истинна. Докажем, что $\exists x V(x) \to U$ тождественно истинна. Проведем доказательство методом от противного. Пусть $\exists x V(x) \to U = Л$ хотя бы в одном случае. Тогда $\exists x V(x) = И$ и $U = Л$. Так как $\exists x V(x) = И$, то найдется такое $a$, что $V(a) = И$. Следовательно, найдется такое $a$, что $V(a) \to U = Л$. Противоречие говорит о том, что $\exists x V(x) \to U$ тождественно истинна.

III часть. Так как всякая доказуемая формула получается из аксиом с помощью основных правил вывода, то всякая доказуемая формула тождественно истинна.

**Теорема 4.6.2. (Полнота исчисления предикатов.)** Если формула тождественно истинна в алгебре предикатов, то она доказуема в исчислении предикатов. (Принимаем без доказательства.)

Теорема доказана Гёделем.

**Следствие.** Формула доказуема в исчислении предикатов тогда и только тогда, когда она тождественно истинна в алгебре предикатов.

**Замечание.** В теореме дедукции мы не можем отбросить условие замкнутости формулы *R*. Покажем, что если предположить, что теорема дедукции справедлива без этого ограничения, то есть

$\Gamma,\ R \vdash V \Rightarrow \Gamma \vdash R \to V$, то мы придем к противоречию. По правилу обобщения $U(a) \vdash \forall x U(x)$, по теореме дедукции $\vdash U(a) \to \forall x U(x)$, по свойству 1 это равносильно тому, что формула $U(a) \to \forall x U(x)$ доказуема, следовательно по правилу для квантора существования формула $\exists x U(x) \to \forall x U(x)$ доказуема, следовательно, по теореме 4.6.1 формула $\exists x U(x) \to \forall x U(x)$ тождественно истинна. А это не так. Приведем контрпример, иллюстрирующий это: $M = N$, $U(a) = \{a$ – простое$\}$. Тогда $\exists x U(x) \to \forall x U(x) = И \to Л = Л$.

Аналогично можно показать, что в леммах 4.5.1, 4.5.2 и 4.5.3 ограничения также существенны.

# ГЛАВА 5
# ПРИКЛАДНОЕ ИСЧИСЛЕНИЕ ПРЕДИКАТОВ

## 5.1. Основные понятия

Прикладное исчисление предикатов так же, как и исчисление высказываний и исчисление предикатов, излагается в виде аксиоматической системы. В отличие от предыдущих разделов, где изучались только логические законы, прикладное исчисление предикатов позволяет наряду с логическими законами изучать и математические законы.

**I. Перечисление символов.**

1. Символы сигнатуры. Рассмотрим три множества: $\sigma_1 = \{\alpha_1, \alpha_2, ..., \alpha_p\}$ – множество символов индивидуальных объектов; $\sigma_2 = \{f_1^{(n_1)}, f_2^{(n_2)}, ..., f_q^{(n_q)}\}$ – множество функциональных символов; $\sigma_3 = \{p_1^{(m_1)}, p_2^{(m_2)}, ..., p_r^{(m_r)}\}$ – множество предикатных символов. Верхние индексы у функциональных и предикатных символов показывают число аргументов. В частных случаях $p$, $r$ и $q$ могут обращаться в нуль, то есть некоторые из перечисленных символов могут отсутствовать. Сигнатурой называется объединение этих трех множеств: $\sigma = \sigma_1 \bigcup \sigma_2 \bigcup \sigma_3$.
2. Символы переменных. а) Символы свободных переменных (малые латинские буквы из начала алфавита с индексами внизу или без индексов). б) Символы связанных переменных (малые латинские буквы из конца алфавита с индексами внизу или без индексов).
3. Логические символы: $\wedge$, $\vee$, $\rightarrow$, $-$, $\forall$, $\exists$.
4. Символ равенства: =.
5. Вспомогательные символы: (, ), ,.

**II. Определение терма и формулы.**

**Определение 5.1.1.**

1. Всякий символ индивидуального объекта из $\sigma_1$ есть терм.
2. Всякий символ свободной переменной есть терм.
3. Если $f^{(n)}$ есть функциональный символ из $\sigma_2$, а $t_1$, $t_2$, …, $t_n$ – термы, то $f^{(n)}(t_1, t_2, ..., t_n)$ – терм.

В пунктах 1 и 2 определяются элементарные термы, а в пункте 3 указано правило, позволяющее из имеющихся термов получать новые термы.

**Определение 5.1.2.**

1. Если $t_1$ и $t_2$ – термы, то $(t_1 = t_2)$ – формула.
2. Если $p^{(m)}$ – предикатный символ из $\sigma_3$, а $t_1$, $t_2$, …, $t_m$ – термы, то $P^{(m)}(t_1, t_2, ..., t_m)$ есть формула.
3. Если $U$ – формула, то $\overline{U}$ – формула.
4. Если $U$ и $V$ – формулы, то $(U \wedge V)$, $(U \vee V)$, $(U \rightarrow V)$ – формулы.

5. Если $U(a)$ – формула, содержащая свободную переменную $a$, то $\forall xU(x)$ и $\exists xU(x)$ также есть формулы, где $x$ – произвольная связанная переменная, не входящая раньше в формулу $U(a)$.

В пунктах 1 и 2 даются определения элементарных формул. В пунктах 3, 4, 5 даются правила, по которым из готовых формул можно получать новые формулы.

**Замечание.** Отметим, что определения терма и формулы зависят от выбора конкретной сигнатуры $\sigma$.

Замкнутую формулу сигнатуры $\sigma$ мы будем также называть предложением, совокупность всех предложений сигнатуры $\sigma$ будем обозначать $L_\sigma$. Все соглашения, касающиеся упрощения записи формул, сформулированные выше, остаются в силе. Кроме того, применим два новых соглашения.

1. Если $f^{(2)}$ – двухместных функциональный символ, то вместо терма $f^{(2)}(a,b)$ мы будем писать $a\,f\,b$. Например: $a+b$.
2. Если $P^{(2)}$ – двухместный предикатный символ, то вместо формулы $P^{(2)}(a,b)$ мы будем писать $a\;P\;b$. Например: $a<b$.

**Пример.**

В сигнатуре $\sigma=\{+^{(2)}\}$ $\forall x\forall y\exists z(x+y=z)$ есть формула в упрощенной записи. Действительно:

$a$, $b$, $c$ – термы согласно пункту (2);
$a+b$ – терм согласно пункту (3);
$(a+b=c)$ – формула согласно пункту (1);
$\exists z(a+b=z)$ – формула согласно пункту (5);
$\forall y\exists z(a+y=z)$ – формула согласно пункту (5);
$\forall x\forall y\exists z(x+y=z)$ – формула, согласно пункту (5).

**III. Аксиомы прикладного исчисление предикатов.**

Схемы для импликации, конъюнкции, дизъюнкции и отрицания остаются прежними.

5. Схемы для кванторов.

5а) $\forall xU(x)\to U(t)$, где $t$ – произвольный терм.

5б) $U(t)\to\exists xU(x)$, где $t$ – произвольный терм.

6. Аксиомы равенства.

6а) $\forall x(x=x)$ – аксиома рефлексивности.

6б) $\forall x\forall y(x=y\to y=x)$ – аксиома симметричности.

6в) $\forall x\forall y\forall z(x=y\wedge y=z\to x=z)$ – аксиома транзитивности.

Аксиомы 6а, 6б и 6в являются аксиомами эквивалентности.

6г) Для каждого функционального символа $f^{(n)}\in\sigma_2$ имеется аксиома замены

$$\forall x_1...\forall x_n\forall y_1...\forall y_n(x_1=y_1\wedge...\wedge x_n=y_n\to f^{(n)}(x_1,...,x_n)=f^{(n)}(y_1,...,y_n)).$$

6д) Для каждого предикатного символа $P^{(m)} \in \sigma_3$ имеется аксиома замены

$$\forall x_1 ... \forall x_m \forall y_1 ... \forall y_m (x_1 = y_1 \wedge ... \wedge x_m = y_m \to P^{(m)}(x_1,...,x_m) \to P^{(m)}(y_1,...,y_m)).$$

**IV. Основные правила вывода.**

1. Правило заключения: $\dfrac{U \to V, U}{V}$.
2. Правило для квантора всеобщности: $\dfrac{U \to V(a)}{U \to \forall x V(x)}$ ($U$ не содержит $a$).
3. Правило для квантора существования: $\dfrac{V(a) \to U}{\exists x V(x) \to U}$ ($U$ не содержит $a$).

**V. Определения формального доказательства и доказуемой формулы.**

Эти определения остаются прежними.

Также прежними остаются определения формального вывода и выводимой формулы. Аналогично формулируются теорема дедукции 4.5.1 и леммы 4.5.1, 4.5.2 и 4.5.3. Сохраняют силу и все доказанные ранее производные правила вывода.

## 5.2. Примеры

**Пример.**

$\sigma = \{+\}$.

$\forall x \forall y \exists z (x + y = z)$ – доказуемая формула.

1. $\forall x(x = x)$ – аксиома рефлексивности;
2. $\forall x(x = x) \to (a + b = a + b)$
   – аксиома по схеме 5а;
   5а. $\forall x U(x) \to U(t)$, $U(x) := x = x$, $t := a + b$;
3. $a + b = a + b$ – правило заключения (1,2);
4. $a + b = a + b \to \exists z(a + b = z)$
   – аксиома по схеме 5б.
   5б. $U(t) \to \exists x U(x)$,
   $U(x) := a + b = x$; $x := z$; $t := a + b$.
5. $\exists z(a + b = z)$ – правило заключения (4,3);
6. $\forall y \exists z(a + y = z)$ – правило обобщения (5);
7. $\forall x \forall y \exists z(x + y = z)$ – правило обобщения (6).

Рассмотрим некоторые новые производные правила вывода.

1. $\vdash t = t$ – рефлексивность.
2. $t_1 = t_2 \vdash t_2 = t_1$ – симметричность.

3. $t_1 = t_2,\ t_2 = t_3 \vdash t_1 = t_3$ – транзитивность.
4. $t_1 = s_1, ...,\ t_n = s_n \vdash f^{(n)}(t_1,...,t_n) = f^{(n)}(s_1,...s_n)$ – правило замены для функционального символа $f^{(n)}$.
5. $t_1 = s_1, ...,\ t_m = s_m,\ P^{(m)}(t_1,...,t_n) \vdash P^{(m)}(s_1,...s_n)$ – правило замены для предикатного символа $P^{(m)}$.

Все эти правила можно доказать используя схему 5а, аксиомы равенства, а также правило заключения и правило образования конъюнкции. Докажем, например, правило 3.

1. $t_1 = t_2$ – первая данная формула;
2. $t_2 = t_3$ – вторая данная формула;
3. $\forall x \forall y \forall z (x = y \wedge y = z \rightarrow x = z)$
   – аксиома транзитивности;
4. $\forall x \forall y \forall z (x = y \wedge y = z \rightarrow x = z) \rightarrow \forall y \forall z (t_1 = y \wedge y = z \rightarrow t_1 = z)$
   – аксиома по схеме 5а;
5. $\forall y \forall z (t_1 = y \wedge y = z \rightarrow t_1 = z)$
   – правило заключения (4,3);
6. $\forall y \forall z (t_1 = y \wedge y = z \rightarrow t_1 = z) \rightarrow \forall z (t_1 = t_2 \wedge t_2 = z \rightarrow t_1 = z)$
   – аксиома по схеме 5а;
7. $\forall z (t_1 = t_2 \wedge t_2 = z \rightarrow t_1 = z)$
   – правило заключения (6,5);
8. $\forall z (t_1 = t_2 \wedge t_2 = z \rightarrow t_1 = z) \rightarrow (t_1 = t_2 \wedge t_2 = t_3 \rightarrow t_1 = t_3)$
   – аксиома по схеме 5а;
9. $t_1 = t_2 \wedge t_2 = t_3$ – правило образования конъюнкции (1,2);
10. $t_1 = t_3$ – сложное правило заключения (8,7,9).

**Пример.**

$\sigma = \{\bigcup, \bigcap\}$.

$a \bigcap (a \bigcup b) = a,\ a \bigcup b = b \vdash a \bigcap b = a$.

1. $a \bigcap (a \bigcup b) = a$ – первая данная формула;
2. $a \bigcup b = b$ – вторая данная формула;
3. $a = a$ – доказуемая формула (рефлексивность);
4. $a \bigcap (a \bigcup b) = a \bigcap b$ – правило замены для пересечения (3,2);
5. $a \bigcap b = a \bigcap (a \bigcup b)$ – правило симметрии (4);
6. $a \bigcap b = a$ – правило транзитивности (5,1).

## 5.3. Структура, элементарная теория структуры. Элементарная эквивалентность структур

Пусть даны сигнатура $\sigma = \{\alpha_1,...,\alpha_p, f_1^{(n_1)},..., f_r^{(n_r)}, P_1^{(m_1)},..., P_q^{(m_q)}\}$ и множество *M*, отличное от пустого. Каждому символу $\alpha_i \in \sigma_1$ поставим в соответствие некоторый конкретный элемент из множества *M*. Каждому функциональному символу $f_i^{(n_i)} \in \sigma_2$ поставим в соответствие некоторую операцию, определенную на множестве *M*, причем число аргументов этой операции будет равно верхнему индексу $n_i$. Каждому предикатному символу $P_i^{(m_i)} \in \sigma_3$ мы поставим в соответствие предикат, определенный на множестве *M*, число аргументов которого равно $m_i$.

**Определение 5.3.1.** Непустое множество *M* с выделенными на нем элементами, с определенными на нем операциями и предикатами называется структурой.

$$M^* = < M, \alpha_1, ..., \alpha_p, f_1^{(n_1)}, ..., f_r^{(n_r)}, P_1^{(m_1)}, ..., P_q^{(m_q)} >,$$

$M$ – основное множество структуры $M^*$.

Отметим некоторые факты.

1. Каждому незамкнутому терму *t* сигнатуры $\sigma$ соответствует в структуре $M^*$ некоторая операция, число аргументов которой равно числу свободных переменных, входящих в терм *t*.

2. Каждому замкнутому терму *t* сигнатуры $\sigma$ соответствует в структуре $M^*$ некоторый конкретный элемент.

3. Всякой незамкнутой формуле *U* сигнатуры $\sigma$ соответствует в структуре $M^*$ некоторый предикат, число аргументов которого равно числу свободных переменных формулы *U*.

4. Любой замкнутой формуле *U* сигнатуры $\sigma$ соответствует в структуре $M^*$ некоторое высказывание, которое будет либо истинным, либо ложным.

**Пример 1.**

$\sigma = \{1, +, \cdot, <, \vdots\}$

$N^* =< N, 1, +, \cdot, <, \vdots >$

1. $a$, $b$, $a+b$, $(a+b)\cdot c$ – операции в $N^*$;
2. 1, $(1+1)\cdot(1+1)$ – конкретные элементы в $N^*$;
3. $a<b$, $a \vdots b \vee b \vdots a$, $\forall x(x<a)$ – предикаты в $N^*$;
4. $\forall x \forall y(x+y=y+x)$, $\forall x \forall y \exists z(x+z=y)$ – высказывания в $N^*$.

**Пример 2.**

$\sigma = \{\oslash, \bigcap, \bigcup, \subseteq\}$

$M^* =< M, \oslash, \bigcap, \bigcup, \subseteq >$, $M$ – множество всех множеств на плоскости.

1. $a$, $b$, $c$, $a \bigcap b$, $a \bigcup b$, $(a \bigcup b) \bigcap (a \bigcup c)$ – операции в $M^*$;
2. $\oslash$, $\oslash \bigcup \oslash$, $\oslash \bigcap \oslash$ – конкретные элементы в $M^*$;
3. $a \bigcap \oslash = b$, $a \subseteq b \bigcup c$ – предикаты в $M^*$;
4. $\forall x \exists y(y \subseteq x)$, $\forall x \forall y(x \bigcap y = x \bigcup y)$ – высказывания в $M^*$.

**Определение 5.3.2.** Элементарной теорией структуры $M^*$ называется совокупность всех предложений сигнатуры $\sigma$, истинных в этой структуре.

$$T(M^*) = \{U : U \in L_\sigma,\ U = И \ \ в\ M^*\}$$

**Пример 1.** $U = \forall x \exists y (y < x)$, $N^* =< N, < >$, $Z^* =< Z, < >$.

$U = Л$ в $N^* \Leftrightarrow U \bar{\in} T(N^*)$, $U = И$ в $Z^* \Leftrightarrow U \in T(Z^*)$.

**Пример 2.** $U = \exists x (x \cdot x = 1 + 1)$, $R^* =< R, 1, \cdot, + >$, $Q^* =< Q, 1, \cdot, + >$.

$U = И$ в $R^* \Leftrightarrow U \in T(R^*)$, $U = Л$ в $Q^* \Leftrightarrow U \bar{\in} T(Q^*)$.

**Определение 5.3.3.** Две структуры называются элементарно эквивалентными, если всякое предложение соответствующей сигнатуры будет принимать одно и то же значение в этих структурах.

**Пример.** $N^*$ не эквивалентна $Z^*$, $R^*$ не эквивалентна $Q^*$.

## 5.4. Элементарные системы аксиом

**Определение 5.4.1.** Элементарной системой аксиом сигнатуры σ называется конечное или бесконечное множество предложений этой сигнатуры.

$S = \{A_1, A_2, ..., A_n\}$ или $S = \{A_1, A_2, ...\}$, где $A_i \in L_\sigma$.

**Пример.**

$\sigma = \{0, +\}$

$A_1 = \forall x \forall y (x + y = y + x)$

$A_2 = \forall x \forall y \forall z ((x + y) + z = x + (y + z))$

$A_3 = \forall x (x + 0 = x)$

$A_4 = \forall x \exists y (x + y = 0)$

$S_1 = \{A_2, A_3, A_4\}$ – система аксиом группы;

$S_2 = \{A_1, A_2, A_3, A_4\}$ – система аксиом абелевой группы.

<u>*Непротиворечивость системы аксиом.*</u>

**Определение 5.4.2.** Система аксиом называется непротиворечивой, если не существует такого предложения, которое выводится из этой системы аксиом одновременно со своим отрицанием.

$$\{S \text{ – непротиворечива}\} \Leftrightarrow \overline{\underset{U \in L_\sigma}{\exists U} (S \vdash U \wedge S \vdash \overline{U})}$$

**Теорема 5.4.1.** Система аксиом $S$ непротиворечива тогда и только тогда, когда существует хотя бы одно предложение, не выводимое из этой системы аксиом.

Доказательство.

Необходимость. Дано: $S$ – непротиворечива. Доказать: $\underset{V \in L_\sigma}{\exists V} (S \overline{\vdash} V)$.

Пусть любое предложение выводимо из $S$. Тогда $S \vdash U$ и $S \vdash \overline{U}$. Следовательно, $S$ – противоречива, что противоречит условию.

Достаточность. Дано: $\underset{V \in L_\sigma}{\exists V} (S \overline{\vdash} V)$. Доказать: $S$ – непротиворечива.

Пусть $S$ – противоречива. Следовательно, существует предложение $U \in L_\sigma$ такое, что $S \vdash U$ и $S \vdash \overline{U}$. В 3.5 было доказано, что $\overline{U}, U \vdash V$. Следовательно, по свойству 4 $S \vdash V$, что противоречит условию.

**Теорема 5.4.2.** Если некоторое предложение $U$ не выводимо из системы аксиом $S$, то тогда новая система аксиом, полученная из $S$ добавлением формулы $\overline{U}$, будет непротиворечивой.

Доказательство.

Дано: $S \nvdash U$. Доказать: $S_0 = S \bigcup \{\overline{U}\}$ – непротиворечива.

Пусть $S_0$ – противоречива, то есть $\underset{V \in L_\sigma}{\exists V} (S_0 \vdash V \wedge S_0 \vdash \overline{V})$. Тогда

$$\left.\begin{array}{l} S_0 \vdash V \Leftrightarrow S,\overline{U} \vdash V \\ S_0 \vdash V \Leftrightarrow S,\overline{U} \vdash \overline{V} \end{array}\right\} \overset{\text{л.4.5.3}}{\Rightarrow} \left.\begin{array}{c} S \vdash \overline{\overline{U}} \\ \overline{\overline{U}} \vdash U \end{array}\right\} \Rightarrow S \vdash U,$$

что противоречит условию.

**Теорема 5.4.3.** Бесконечная система аксиом непротиворечива тогда и только тогда, когда непротиворечива любая ее конечная подсистема.

Доказательство.

Необходимость. Дано: бесконечная система аксиом $S$ – непротиворечива; $S_0$ – конечная подсистема системы $S$. Доказать: $S_0$ – непротиворечива.

Пусть $S_0$ – противоречива, то есть $\exists U \in L_\sigma$, что $S_0 \vdash U$ и $S_0 \vdash \overline{U}$.

$$\begin{array}{l} S_0 \vdash U \overset{\text{3а}}{\Rightarrow} S \vdash U \\ S_0 \vdash \overline{U} \Rightarrow S \vdash \overline{U} \end{array}.$$

Следовательно, $S$ – противоречива, что противоречит условию.

Достаточность. Дано: любая конечная подсистема системы $S$ непротиворечива. Доказать: $S$ – непротиворечива.

Пусть $S$ – противоречива. То есть $\exists U \in L_\sigma$, что $S \vdash U$ и $S \vdash \overline{U}$. Так как $S$ – бесконечная система аксиом, а $U$ выводима из $S$, то по свойству 5 существует конечная подсистема $S_1$ системы $S$ такая, что $S_1 \vdash U$. Аналогично существует конечная подсистема $S_2$ системы $S$ такая, что $S_2 \vdash U$. Обозначим через $S_0 = S_1 \bigcup S_2$. $S_0$ – конечная подсистема системы $S$. $S_1 \vdash U \overset{\text{3а}}{\Rightarrow} S_0 \vdash U$, $S_2 \vdash \overline{U} \overset{\text{3а}}{\Rightarrow} S_0 \vdash \overline{U}$, следовательно $S_0$ – противоречива, что противоречит условию.

<u>*Полнота системы аксиом.*</u>

**Определение 5.4.3.** Система аксиом $S$ называется полной, если какое бы предложение сигнатуры $\sigma$ мы бы ни взяли, или оно само, или его отрицание выводимо из $S$.

$$\{S \text{ – полна}\} \Leftrightarrow \underset{U \in L_\sigma}{\forall U} (S \vdash U \vee S \vdash \overline{U})$$

**Теорема 5.4.4.** Система аксиом $S$ является полной тогда и только тогда, когда добавление к $S$ любого предложения, не выводимого из $S$, приводит к противоречивой системе аксиом.

Доказательство.

Необходимость. Дано: $S$ – полна, $S \overline{\vdash} U$. Доказать: $S_0 = S \bigcup \{U\}$ – противоречива.

Так как $S$ – полна и $S \overline{\vdash} U$, то по определению полноты $S \vdash \overline{U} \overset{3a}{\Rightarrow} S_0 \vdash \overline{U}$. По свойству 2 $S,\ U \vdash U \Leftrightarrow S_0 \vdash U$. Следовательно, $S_0$ – противоречива.

Достаточность. Дано: $\underset{V \in L_\sigma}{\forall V}(S \overline{\vdash} V \Rightarrow S_0 = S \bigcup \{V\}$ – противоречива).

Доказать: $S$ – полна.

Пусть $S$ не полна, что равносильно

$$\overline{\underset{U \in L_\sigma}{\forall U}(S \vdash U \vee S \vdash \overline{U})}.$$

То есть $\exists U \in L_\sigma$, что 1) $S \overline{\vdash} U \overset{т.5.4.2}{\Rightarrow} S \bigcup \{\overline{U}\}$ – непротиворечива, 2) $S \overline{\vdash} \overline{U} \overset{усл.}{\Rightarrow} S \bigcup \{\overline{U}\}$ – противоречива. Полученное противоречие говорит о неверности предположения.

**Теорема 5.4.5.** Система аксиом непротиворечива и полна тогда и только тогда, когда невыводимость из $S$ произвольного предложения равносильно выводимости из $S$ его отрицания.

$$\{S \text{ – непротиворечива и полна}\} \Leftrightarrow \underset{U \in L_\sigma}{\forall U}(S \overline{\vdash} U \Leftrightarrow S \vdash \overline{U})$$

Доказательство.

Необходимость. Дано: $S$ – непротиворечива и полна. Доказать: $\underset{U \in L_\sigma}{\forall U}(S \overline{\vdash} U \Leftrightarrow S \vdash \overline{U})$.

Пусть $U$ – произвольное предложение из $L_\sigma$. Если $S \overline{\vdash} U$, то $S \vdash \overline{U}$, так как $S$ – полна. Если $S \vdash \overline{U}$, то $S \overline{\vdash} U$, так как $S$ – непротиворечива.

Достаточность. Дано: $\underset{U \in L_\sigma}{\forall U}(S \overline{\vdash} U \Leftrightarrow S \vdash \overline{U})$. Доказать: $S$ – непротиворечива и полна.

Докажем сначала, что $S$ – непротиворечива. Пусть $S$ – противоречива. Тогда $\exists U \in L_\sigma$, что $S \vdash U$, $S \vdash \overline{U} \Leftrightarrow S \overline{\vdash} U$. Получили противоречие.

Докажем теперь, что $S$ – полна. Пусть $S$ не полна. Тогда $\exists U \in L_\sigma$, что $S \overline{\vdash} U \Leftrightarrow S \vdash \overline{U}$, $S \overline{\vdash} \overline{U}$. Получили противоречие.

*Независимость системы аксиом.*

**Определение 5.4.4.** Аксиома $A_i \in S$ не зависит от остальных аксиом, если она не выводится из множества остальных аксиом.

$$\{A_i \in S \text{ не зависит от остальных аксиом}\} \Leftrightarrow \{S_i \overline{\vdash} A_i, \text{ где } S_i = S \setminus \{A_i\}\}$$

**Определение 5.4.5.** Система аксиом $S$ называется независимой, если каждая ее аксиома не зависит от остальных.

## 5.5. Модель системы аксиом.

**Определение 5.5.1.** Пусть $S$ – система аксиом сигнатуры $\sigma$. Моделью системы аксиом $S$ называется такая структура $M^*$ сигнатуры $\sigma$, в которой все аксиомы из $S$ истинны.

$$\{M^* - \text{модель системы аксиом S}\} \Leftrightarrow \underset{A_i \in S}{\forall A_i} \,(A_i = И \text{ в } M^*)$$

**Теорема 5.5.1.** Если предложение $U$ выводимо из системы аксиом $S$, то это предложение истинно в любой модели системы $S$.

Доказательство.

Дано: $S \vdash U$. Доказать: $\forall M^* (M^* - \text{модель S} \Rightarrow U = И \text{ в } M^*)$.

Пусть $M^*$ – модель S и пусть $U = Л$ в $M^*$. Докажем, что $U$ выводимо из некоторой конечной подсистемы $S_0$ системы $S$. Если $S$ – конечна, то $S_0 = S$. Пусть теперь $S$ – бесконечна. По свойству 5 раз $U$ выводима из бесконечного множества формул $S$, то $U$ будет выводима и из некоторого конечного подмножества этого множества. Тогда это конечное подмножество мы и обозначим через $S_0$.

$$S_0 \vdash U, \text{ где } S_0 = \{A_1, A_2, ..., A_n\},\ A_i \in S\ (i = \overline{1,n}).$$

Так как $A_1, A_2, ..., A_n \vdash U$ и формулы $A_1$, $A_2$, …, $A_n$ – замкнутые, то по теореме дедукции

$$A_1, A_2, ..., A_{n-1} \vdash A_n \to U \Rightarrow ... \Rightarrow A_1 \vdash A_2 \to (...(A_n \to U)) \Rightarrow$$
$$\Rightarrow\ \vdash A_1 \to (A_2 \to ...(A_n \to U))$$

Последнее утверждение по свойству 1 равносильно тому, что $V = A_1 \to (A_2 \to ...(A_n \to U)...)$ – доказуема, а, следовательно, $V$ – тождественно истинна. Так как $M^*$ – модель $S$, то $A_1 = И$ в $M^*$, …, $A_n = И$ в $M^*$.

$$V = A_1 \to (A_2 \to ...(A_n \to U)...) = И \to (И \to ...(И \to Л)...) = Л$$

Итак, $V = Л$ в $M^*$, что противоречит тому, что формула $V$ – тождественно истинна.

**Замечание.** Выше мы дали определения непротиворечивости, полноты и независимости системы аксиом. Эти определения иногда называют формальными определениями, так как они опираются на понятие «выводимость». Теперь мы дадим новые определения этим трем понятиям, которые мы назовем содержательными определениями. Содержательные определения будут использовать понятия «структура» и «модель».

**Определение 5.5.2.** Система аксиом $S$ называется непротиворечивой, если для нее существует хотя бы одна модель.

**Теорема 5.5.2.** Формальное и содержательное определения непротиворечивости равносильны.

Доказательство.

Необходимость примем без доказательства.

Достаточность. Дано: $S$ – непротиворечива содержательно, то есть для нее существует модель $M^*$. Доказать: $S$ – непротиворечива формально.

Пусть $S$ формально противоречива. Значит, найдется $U \in L_\sigma$ такое, что 1) $S \vdash U$, а, значит, по теореме 5.5.1 $U = И$ в $M^*$, 2) $S \vdash \overline{U}$, а, следовательно, по теореме 5.5.1 $\overline{U} = И$ в $M^*$, то есть $U = Л$ в $M^*$. Полученное противоречие доказывает теорему.

**Теорема 5.5.3 (обратная теореме 5.5.1.)** Если некоторое предложение истинно в любой модели системы аксиом $S$, то оно выводится из $S$.

Доказательство.

Дано: $\forall M^* (M^*$ – модель $S \Rightarrow U = И$ в $M^*)$. Доказать: $S \vdash U$.

Пусть $S \overline{\vdash} U$, тогда по теореме 5.4.2 $S_0 = S \bigcup \{\overline{U}\}$ – формально непротиворечива. По теореме 5.5.2 $S_0 = S \bigcup \{\overline{U}\}$ содержательно непротиворечива. Это утверждение по определению равносильно тому, что существует модель $M^*$ для $S_0 = S \bigcup \{\overline{U}\}$. Следовательно, в $M^*$ будут истинны все аксиомы из $S_0$. Но тогда, во-первых, все аксиомы из $S$ истинны в $M^*$, что равносильно тому, что $M^*$ – модель для $S$, во-вторых, $\overline{U} = И$ в $M^*$, что равносильно тому, что $U = Л$ в $M^*$. Это противоречит условию.

**Определение 5.5.3.** Система аксиом $S$ называется полной, если любые две ее модели элементарно эквивалентны между собой.

$\{S$ – полна$\} \Leftrightarrow \{\forall M^* \forall L^* (M^*$ – модель $S$, $L^*$ – модель $S \Rightarrow M^*$ элементарно эквивалентна $L^*)\}$

**Теорема 5.5.4.** Формальное и содержательное определения полноты равносильны.

Доказательство.

Необходимость. Дано: $S$ – формально полна. Доказать: $S$ – содержательно полна.

Пусть $M^*$ и $L^*$ – модели $S$. Докажем, что они элементарно эквивалентны. Предположим, что это не так. Тогда существует такое $U \in L_\sigma$, что оно в структурах $M^*$ и $L^*$ принимает различные значения. Пусть $U = Л$ в $M^*$ (следовательно по теореме 5.5.1 $S \overline{\vdash} U$) и $U = И$ в $L^*$, что равносильно тому, что $\overline{U} = Л$ в $L^*$ (следовательно по теореме 5.5.1 $S \overline{\vdash} \overline{U}$. Получили противоречие с условием.

Достаточность. Дано: $S$ – содержательно полна. Доказать: $S$ – формально полна.

Предположим, что это не так. Значит, существует $U \in L_\sigma$ такое, что:

1) $S \overline{\vdash} U$, следовательно, по теореме 5.5.3 найдется модель $M^*$ системы $S$ такая, что $U = Л$ в $M^*$;
2) $S \overline{\vdash} \overline{U}$, следовательно, по теореме 5.5.3 найдется модель $L^*$ системы $S$ такая, что $\overline{U} = Л$ в $L^*$, то есть $U = И$ в $L^*$.

Выводы в пунктах 1) и 2) говорят о том, что $M^*$ не элементарно эквивалентна $L^*$, что противоречит условию.

**Определение 5.5.4.** Аксиома $A_i \in S$ не зависит от остальных аксиом системы $S$, если существует такая структура, в которой эта аксиома ложна, а остальные аксиомы истинны.

{ $A_i \in S$ не зависит от остальных аксиом}$\Leftrightarrow \exists M^*$ ( $A_i = Л$ в $M^*$, а все остальные аксиомы истинны в $M^*$).

**Определение 5.5.5.** Система аксиом $S$ называется независимой, если любая ее аксиома не зависит от остальных.

**Теорема 5.5.5.** Формальное и содержательное определения независимости равносильны между собой.

Доказательство.

Необходимость. Дано: $A_i$ не зависит от остальных аксиом формально. Доказать: $A_i$ не зависит от остальных аксиом содержательно.

По условию $S_i \overline{\vdash} A_i$, где $S_i = S \setminus \{A_i\}$. Следовательно, по теореме 5.5.3 существует такая модель $M^*$ для $S_i$, что $A_i = Л$ в $M^*$. А то, что $M^*$ – модель для $S_i$, означает, что все аксиомы из $S_i$ истинны в $M^*$. Итак, аксиома $A_i$ не зависит от остальных аксиом содержательно.

Достаточность. Дано: аксиома $A_i$ не зависит от остальных содержательно. Доказать: аксиома $A_i$ не зависит от остальных формально. Фактически, требуется доказать, что $S_i \overline{\vdash} A_i$, где $S_i = S \setminus \{A_i\}$. Допустим, $S_i \vdash A_i$, тогда по теореме 5.5.1 $A_i = И$ в любой модели $M^*$ системы аксиом $S_i$. То есть, в любой структуре, где остальные аксиомы истинны, данная аксиома $A_i$ также должна быть истинной, что противоречит условию.

# ГЛАВА 6
# АЛГОРИТМЫ И РЕКУРСИВНЫЕ ФУНКЦИИ

## 6.1. Интуитивное понятие алгоритма

Интуитивное понятие алгоритма служило математикам, начиная со времён Евклида до 30-х годов 20-го века, до тех пор, пока не появилось строгое определение этого понятия.

**Определение 6.6.1.** Задача называется алгоритмически разрешимой, а метод ее решения называется алгоритмом, если выполняются следующие условия.

1. Массовость. Данная задача распадается на совокупность однотипных задач, причем указанный метод решения пригоден для каждой задачи из этой совокупности.
2. Счётность. Множество отдельных задач, на которые распадается наша основная задача, должно быть счетным. (Множество называется счётным, если можно установить взаимно однозначное соответствие между этим множеством и множеством натуральных чисел.)
3. Автоматичность. Алгоритм должен быть сформулирован таким образом, чтобы его можно было автоматически применять к решению любой задачи из данной совокупности. При решении отдельных задач этим методом не должно возникать никаких <u>принципиальных</u> трудностей. Все частные случаи, которые могут нам представиться, должны быть предусмотрены при формулировке алгоритма.
4. Выполнимость отдельных шагов. При применении алгоритма к решению отдельной задачи может возникнуть необходимость выполнить ряд шагов. Каждый шаг в каждой задаче должен быть принципиально выполним (если отвлечься от времени выполнения, от точности инструментов, от размеров бумаги).
5. Результативность. Процесс решения каждой отдельной задачи должен заканчиваться через <u>конечное</u> число шагов и давать определенный результат.
6. Обоснованность. Должно быть доказано, что результат, который мы получаем при применении алгоритма к каждой отдельной задаче, является решением этой задачи.

Можно заметить, однако, что это определение, может быть, не совсем соответствует сложившемуся у многих понятию алгоритма. Например, алгоритм игры в «преферанс» согласно этому определению таковым не является, так как число отдельных задач, на которые распадается основная задача при определении хода – конечно, а не счётно.

**Пример.**

Алгоритм Евклида для нахождения НОД.

Задача: Найти НОД натуральных чисел $a$ и $b$.

Описание метода. Если $a = b$, то $(a,b) = a$. Рассмотрим случай $a \neq b$.

1. Делим большее число на меньшее, находим частное и остаток.
2. Делим меньшее число на остаток, находим новое частное и новый остаток.
3. Делим предыдущий остаток на последующий, находим новое частное и новый остаток.
4. За НОД принимаем последний отличный от нуля остаток.

Покажем, что это действительно есть алгоритм.

1. Наша задача распадается на совокупность однотипных задач, которые получаются при конкретных значениях $a$ и $b$.
2. Множество отдельных задач является счетным, так как каждая отдельная задача задается указанием пары натуральных чисел, а множество пар натуральных чисел есть множество счетное. Докажем это.

   (1,1) (1,2) (1,3) (1,4) …
   (2,1) (2,2) (2,3) …
   (3,1) (3,2) …
   (4,1) ….
   …

   (1,1)↔1, (1,2)↔2, (2,1)↔3, (1,3)↔4, (2,2)↔5, (3,1)↔6, (4,1)↔7, … .
3. Указанный метод можно автоматически применить к любой паре натуральных чисел, причем для деления натуральных чисел можно применять известный нам метод деления углом, который также обладает свойством автоматичности.
4. Каждый отдельный шаг в каждой задаче принципиально выполним, так как деление с остатком всегда возможно.
5. Указанный метод нахождения НОД для любой пары натуральных чисел заканчивается через конечное число шагов. Действительно, остаток от деления всегда меньше делителя, следовательно, мы получаем убывающую последовательность натуральных чисел. Но убывающая последовательность натуральных чисел может быть только конечной. Следовательно, через конечное число шагов мы получим остаток, равный нулю.
6. Мы должны доказать, что последний отличный от нуля остаток действительно равен НОД.

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + r_2$$
$$\dots$$
$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1}$$

Докажем сначала, что $r_n$ – общий делитель $a$ и $b$.

$$r_{n-1} \vdots r_n$$
$$r_{n-2} \vdots r_n$$
$$\dots$$
$$r_2 \vdots r_n$$
$$r_1 \vdots r_n$$
$$b \vdots r_n$$
$$a \vdots r_n$$

Докажем теперь, что $r_n$ есть именно наибольший общий делитель чисел $a$ и $b$. Пусть существует для чисел $a$ и $b$ общий делитель $c$ такой, что $c > r_n$. То есть $a \vdots c$, $b \vdots c$, $c > r_n$.

$$a \vdots c$$
$$b \vdots c$$
$$r_1 \vdots c$$
$$r_2 \vdots c$$
$$\dots$$
$$r_{n-1} \vdots c$$
$$r_n \vdots c$$

Утверждение $r_n \vdots c$ противоречит $c > r_n$.

## 6.2. Необходимость уточнения понятия алгоритм

Вышеуказанное определение нельзя назвать строгим определением алгоритма. Однако, если счётная совокупность однотипных задач алгоритмически разрешима, то это можно доказать и с помощью интуитивного понятия алгоритма. Долгое время в математике господствовало мнение, что если имеется счётная совокупность однотипных задач, причём каждая задача в отдельности имеет решение, то обязательно существует алгоритм (то есть универсальный автоматический метод), который бы позволял решить каждую задачу из данной совокупности. Если же в некоторых случаях этот метод найти не удавалось, то предполагали, что со временем он будет найден. Это мнение оказалось ошибочным, но чтобы доказать, что данная счётная совокупность задач алгоритмически неразрешима, несмотря на то, что каждая задача имеет решение, невозможно без строгого определения понятия алгоритма.

В 30-х годах 20-го века рядом математиков было предложено строгое определение понятия алгоритма: Гёделем, Чёрчем, Клини, Постом, Тьюрингом, Колмогоровым, Марковым. Несмотря на различие формулировок, было доказано, что эти определения равносильны. После появления строгого определения появились доказательства алгоритмической неразрешимости ряда проблем. Так в 1936 году Чёрч доказал алгоритмическую неразрешимость проблемы разрешения для исчисления предикатов, которая формулируется следующим образом. «Для любой формулы исчисления предикатов определить, будет ли она доказуемой.» Отметим, что аналогичная проблема для исчисления высказываний алгоритмически разрешима. Действительно, формула доказуема в исчислении высказываний тогда и только тогда, когда она тождественно истинна в алгебре высказываний. Метод составления таблиц истинностных значений, а также метод, основанный на критерии тождественной истинности формул алгебры высказываний, являются алгоритмами.

### 6.3. Алфавит и слово

**Определение 6.3.1.** Алфавитом называется произвольный конечный набор отличных друг от друга символов: $A = \{a_1, a_2, ..., a_n\}$.

**Определение 6.3.2.** Словом алфавита называется произвольный конечный набор символов этого алфавита, причем один и тот же символ может повторяться в слове несколько раз: $\alpha = (a_{i_1} a_{i_2} ... a_{i_k})$, где $a_{i_1} \in A$, $a_{i_2} \in A$, …, $a_{i_k} \in A$. Длиной слова называется число входящих в него символов.

Хотя каждый алфавит конечен, и каждое слово алфавита конечно, но множество всех слов алфавита счётно. Действительно, мы можем составлять слова длины 1, 2, 3 и так далее.

**Пример.**

1. $A_1 = \{а, б, в, ..., я\}$
   $\alpha_1 = (корова)$
   $\alpha_2 = (вмлр)$
2. В алфавит $A_2$ включим все большие и маленькие русские буквы, знаки препинания и пустой символ.
   $\alpha = (\textit{Я живу в Орске.})$ – слово длины 15.
3. $A_3 = \{\mathrm{I}\}$. Этот алфавит можно использовать для записи натуральных чисел. Договоримся, что $N = \{0,1,2,...\}$ и I↔0, II↔1, III↔2, … .
4. $A_4 = \{0,1,2,3,4,5,6,7,8,9\}$. Этот алфавит также можно использовать для записи натуральных чисел.
5. $A_5 = \{0,1,2,...,9,(,),\text{'},-\}$. Этот алфавит можно использовать для записи произвольных рациональных чисел, так как каждое рациональное число представимо в виде десятичной дроби, конечной или бесконечной периодической. $\alpha_1 = (-0{,}35)$, $\alpha_2 = (3{,}7(4))$.

**Замечание.** Не существует алфавита, словами которого можно записать любое действительно число. Причина в том, что множество слов любого алфавита счётно, а множество действительных чисел имеет мощность континуума.

## 6.4. Нумерация слов алфавита

**Определение 6.4.1.** Говорят, что множество слов алфавита $A$ занумеровано, если существует взаимно однозначное соответствие между множеством всех слов этого алфавита и некоторым подмножеством множества натуральных чисел.

**Определение 6.4.2.** Нумерация слов алфавита называется эффективной, если существует алгоритм $\mu$, который для каждого слова находит его номер, и существует алгоритм $\lambda$, который для каждого натурального числа дает ответ на вопрос, является ли это число номером некоторого слова и в случае положительного ответа находит соответствующее слово.

Покажем, что слова любого алфавита можно эффективно занумеровать. Рассмотрим алфавит $A = \{a_1, a_2, ..., a_n\}$. Каждому символу алфавита поставим в соответствие номер места, на котором он стоит в алфавите: $a_1 \to 1$, $a_2 \to 2$, …, $a_n \to n$. Пусть $\alpha$ – произвольное слово этого алфавита: $\alpha = (a_{i_1} a_{i_2} ... a_{i_k})$. Номером слова $\alpha$ мы назовем следующее число: $p_1^{i_1} \cdot p_2^{i_2} \cdot ... \cdot p_k^{i_k}$, где $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, …, то есть $p_1$, $p_2$, $p_3$, … есть последовательность простых чисел. Можно показать, что эта нумерация эффективна.

**Пример.**

$A$={I, □}. I→1, □→2.

1) α=(I □ □ I I I)

$\mu(\alpha) = 2^1 \cdot 3^2 \cdot 5^2 \cdot 7^1 \cdot 11^1 \cdot 13^1$.

2) $n = 60$

3) $n = 2^2 \cdot 3^1 \cdot 5^1$

$\lambda(n)$=(□ I I)

4) $n = 32 = 2^5$, $5 \neq 1$, $5 \neq 2$, 32 не является номером никакого слова в данном алфавите.

5) $n = 35 = 5^1 \cdot 7^1$. Нет слова с таким номером ни в каком алфавите (нет множителей 2 и 3).

## 6.5. Алгоритмы и вычислимые функции. Критерий алгоритмической разрешимости

**Определение 6.5.1.** Натуральная функция от одного или нескольких натуральных аргументов $m = f(n_1, n_2, ..., n_p)$ называется вычислимой, если существует алгоритм, позволяющий вычислять значения этой функции.

**Замечание.** Это определение не является строгим, так как оно опирается на интуитивное понятие алгоритма, которое не является строгим.

**Пример.** Функция $f(n_1, n_2) = n_1 + n_2$ является вычислимой, так как метод сложения двух натуральных чисел столбиком является алгоритмом.

Покажем, что изучение любых алгоритмов можно свести к изучению вычислимых функций. Поэтому вместо того, чтобы уточнять понятие алгоритма, достаточно уточнить понятие вычислимой функции.

Пусть дана счётная совокупность однотипных задач, причем каждая отдельная задача имеет решение. Мы можем всегда подобрать такой алфавит $A$, что и сами задачи и решения этих задач записываются словами этого алфавита $A$. Действительно, в алфавит $A$ мы можем включить большие и маленькие русские буквы, знаки препинания, пустой символ, буквы латинского, греческого и любого другого алфавитов, кроме того, различные математические, логические и другие символы. Те слова алфавита, с помощью которых записываются отдельные задачи, мы назовем начальными. Пусть $U=\{u\}$ – множество всех начальных слов. Слова алфавита, с помощью которых записываются решения задач, мы назовем заключительными. Пусть $V=\{v\}$ – множество всех заключительных слов. Мы можем определить функцию, которая каждой задаче ставит в соответствие ее решение, то есть функцию $v=\varphi(u)$, которая каждому начальному слову ставит в соответствие соответствующее заключительное слово. Таким образом, $U$ – область определения этой функции, $V$ – область значений. Пусть слова алфавита $A$ эффективно занумерованы, то есть существует алгоритм $\mu$, который для каждого слова алфавита $A$ находит его номер, и существует алгоритм $\lambda$, который для каждого натурального числа дает ответ на вопрос, будет ли это число номером некоторого слова и в случае положительного ответа находит по номеру соответствующее слово. Если $n$ – номер начального слова $u$, $m$ – номер заключительного слова $v$, то $n=\mu(u)$, $m=\mu(v)$, $u=\lambda(n)$, $v=\lambda(m)$. Наряду с функцией $v=\varphi(u)$ мы можем рассмотреть функцию $m=f(n)$, которая номеру каждого начального слова ставит в соответствие номер соответствующего заключительного слова. Отметим, что $m=f(n)$ есть натуральная функция от натурального аргумента.

**Теорема 6.5.1.** Данная задача алгоритмически разрешима тогда и только тогда, когда соответствующая этой задаче функция $m=f(n)$ является вычислимой.

Доказательство.

Необходимость. Дано: задача алгоритмически разрешима, то есть существует алгоритм, вычисляющий $v=\varphi(u)$. Доказать: $m=f(n)$ вычислима, то есть существует алгоритм, вычисляющий $m=f(n)$.

$$\left.\begin{array}{l} m=\mu(v)=\mu(\varphi(u))=\mu(\varphi(\lambda(n))) \\ m=f(n) \end{array}\right\} \Rightarrow f(n)=\mu(\varphi(\lambda(n)))$$

Итак, существует алгоритм, вычисляющий функцию $f$, который является композицией трех алгоритмов $\lambda$, $\varphi$ и $\mu$.

Достаточность. Дано: $m=f(n)$ вычислимая функция, то есть существует алгоритм, вычисляющий функцию $m=f(n)$. Доказать: задача алгоритмически разрешима, то есть существует алгоритм, вычисляющий функцию $v = \varphi(u)$.

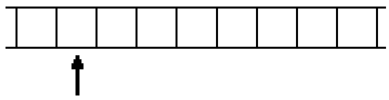
$$\left.\begin{array}{l} v = \lambda(m) = \lambda(f(n)) = \lambda(f(\mu(u))) \\ v = \varphi(u) \end{array}\right\} \Rightarrow \varphi(u) = \lambda(f(\mu(u)))$$

Итак, существует алгоритм, вычисляющий функцию $\varphi$, который является композицией алгоритмов $\mu, f, \lambda$.

Таким образом, мы показали, что изучение любых алгоритмов сводится к изучению вычислимых функций, а, следовательно, вместо того, чтобы уточнять понятие алгоритма, достаточно уточнить понятие вычислимой функции.

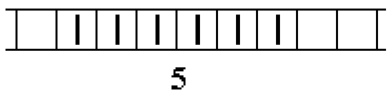
## 6.6. Машина Тьюринга

Машина Тьюринга – это не реально действующее устройство, а абстрактное математическое понятие. Машина состоит из бесконечной ленты, разделенной на клетки, и из указателя, направленного на одну из клеток. Клетка, на которую направлен указатель, называется обозреваемой.



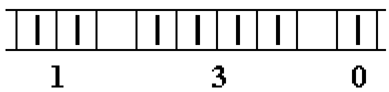
Для машины Тьюринга используется алфавит, который состоит из двух символов: палочки I и пустой клетки □. $A$={I, □}. На ленте могут записываться слова этого алфавита, причем в одной клетке записывается по одному символу, и соседние символы записываются на соседних клетках.

**Определение 6.6.1.** Слово называется заключительным, если это набор палочек.




Заключительное слово.

**Определение 6.6.2.** Слово называется начальным, если оно представляет собой или набор палочек, или несколько наборов палочек, разделенных пустыми клетками.




Начальное слово.

Машина Тьюринга может находиться в одном из следующих состояний: $q_1$, $q_2$, ..., $q_m$, $q_0$. Состояния $q_1$, $q_2$, ..., $q_m$ называются активными. Если машина Тьюринга находится в одном из активных состояний, то она может работать. Состояние $q_0$ – пассивное. Если машина Тьюринга переходит в состояние $q_0$, то она прекращает работу. Машина Тьюринга за один шаг работы может выполнить три элементарные операции.

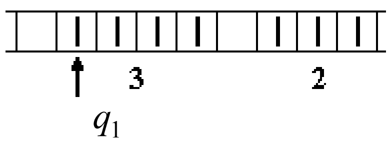
1. Стереть палочку в обозреваемой клетке или записать там палочку.
2. Может передвинуть указатель на одну клетку влево (Л), на одну клетку вправо (П) или оставить его на месте (М).
3. Машина может перейти из одного состояния в другое.

Работа машины Тьюринга задается программой. Программой называется произвольный конечный набор приказов. Приказом называется распоряжение следующего вида: если указатель направлен на символ $a_i$ (это палочка или пустая клетка), и машина находится в активном состоянии $q_j$, то машина вместо $a_i$ должна записать символ $a_k$, передвинуть определенным образом указатель и из состояния $q_j$ перейти в состояние $q_l$, $(a_i, q_j) \to (a_k, D, q_l)$ – запись приказа. Два приказа называются противоречивыми, если их посылки совпадают, а заключения не совпадают. Программа называется непротиворечивой, если она не содержит противоречивых приказов. Имеет смысл рассматривать только непротиворечивые программы.

Программы удобно записывать в виде таблицы. Вверху таблицы записывают все символы алфавита, а с левой стороны записывают все активные состояния. Если в программу входит приказ $(a_i, q_j) \to (a_k, D, q_l)$, то в таблице на пересечении *i*-го столбца и *j*-ой строки записывается заключение приказа (в конкретных приказах на месте движения *D* должно стоять Л, П или М). В таблице некоторые клетки могут оставаться незаполненными. Число занятых клеток равно числу приказов, входящих в программу.

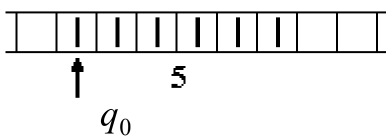
**Определение 6.6.3.** Говорят, что машина Тьюринга находится в начальной ситуации, если выполнены следующие три условия.

1. На ленте записано некоторое начальное слово.
2. Указатель направлен на самую левую палочку этого слова.
3. Машина находится в состоянии $q_1$.




**Определение 6.6.4.** Говорят, что машина Тьюринга находится в заключительной ситуации, если выполнены следующие три условия:

1. На ленте записано некоторое заключительное слово.
2. Указатель направлен на самую левую палочку этого слова.
3. Машина находится в пассивном состоянии $q_0$.




## 6.7. Простейшие примеры машин Тьюринга

Если конкретная машина Тьюринга находится в конкретной начальной ситуации, то возможны следующие 4 случая.

1. Машина Тьюринга вовсе не начнет работу.

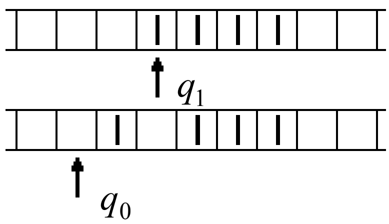
| | I | □ |
|---|---|---|
| $q_1$ | | I М $q_2$ |
| $q_2$ | □ П $q_1$ | I Л $q_0$ |

2. Машина Тьюринга начнет работу, но не остановится.

| | I | □ |
|---|---|---|
| $q_1$ | □ Л $q_1$ | I Л $q_1$ |

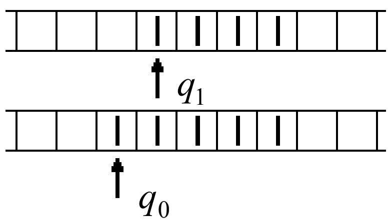
3. Машина Тьюринга начнет работу и через конечное число шагов остановится, но не в заключительной ситуации.

| | I | □ |
|---|---|---|
| $q_1$ | □ Л $q_1$ | I Л $q_0$ |




4. Машина Тьюринга начнет работу и через конечное число шагов остановится в заключительной ситуации.

| | I | □ |
|---|---|---|
| $q_1$ | I Л $q_1$ | I М $q_0$ |




### 6.8. Рекурсивные функции

**Определение 6.8.1.** Говорят, что машина Тьюринга перерабатывает набор натуральных чисел $n_1$, ..., $n_p$ в натуральное число $m$, если, находясь в начальной ситуации, в которой на ленте записан набор $n_1$, ..., $n_p$, машина Тьюринга начнет работать и через конечное число шагов остановится в заключительной ситуации, причем на ленте будет записано число $m$.

**Определение 6.8.2.** Говорят, что машина Тьюринга отказывается перерабатывать набор $n_1$, ..., $n_p$, если, находясь в начальной ситуации, в которой на ленте записан этот набор, машина или вовсе не начнет работать, или начнёт, но не остановится, или начнет работать и остановится, но не в заключительной ситуации.

Пусть дана натуральная функция от одного или нескольких аргументов $m = f(n_1,...,n_p)$. Эта функция может быть определенной не на всех наборах натуральных чисел. Если, в частности, данная функция определена на всех наборах натуральных чисел, то ее называют всюду определенной. Например, $m = n_1 \cdot n_2$ – всюду определенная функция, $m = \dfrac{n_1}{n_2}$ – нет. (Во-первых, здесь $m$ не всегда натуральное, во-вторых, если $n_2 = 0$, дробь не имеет смысла.)

**Определение 6.8.3.** Говорят, что машина Тьюринга вычисляет значения функции $m = f(n_1,...,n_p)$, если машина Тьюринга перерабатывает любой набор $n_1$, ..., $n_p$, входящий в область определения функции, в натуральное число $m$, равное значению данной функции на данном наборе, и отказывается перерабатывать любой набор $n_1$, ..., $n_p$, который не входит в область определения этой функции.

**Определение 6.8.4.** Натуральная функция от одного или нескольких натуральных аргументов называется рекурсивной (частично рекурсивной), если существует машина Тьюринга, вычисляющая ее значения.

**Определение 6.8.5.** Если рекурсивная функция является всюду определенной, то она называется общерекурсивной.

**Пример.** Функция $m = n_1 + n_2$ является общерекурсивной.

1. Функция всюду определена.
2. Определим машину Тьюринга, вычисляющую значения данной функции.

| | I | □ |
|---|---|---|
| $q_1$ | I П $q_1$ | I Л $q_2$ |
| $q_2$ | I Л $q_2$ | □ П $q_3$ |
| $q_3$ | □ П $q_4$ | |
| $q_4$ | □ П $q_0$ | |

Пояснение. Указатель двигается вправо, минуя первый набор палочек, затем машина записывает палочку в пустой клетке, разделяющей слагаемые, затем указатель двигается влево до первой пустой клетки, затем машина стирает две крайние левые палочки, и указатель останавливается против самой левой из оставшихся палочек.

$$(n_1 + 1) + (n_2 + 1) + 1 = n_1 + n_2 + 3 = (n_1 + n_2 + 1) + 2$$

**Пример.** Функция $f(n_1, n_2) = n_1 - n_2$ является рекурсивной.

1. Разность $n_1 - n_2$ определена при $n_1 \geq n_2$, следовательно функция не всюду определена.
2. Определим машину Тьюринга, вычисляющую значения данной функции.

| | I | □ |
|---|---|---|
| $q_1$ | I П $q_1$ | □ П $q_2$ |
| $q_2$ | I П $q_2$ | □ Л $q_3$ |
| $q_3$ | □ Л $q_4$ | □ Л $q_7$ |
| $q_4$ | I Л $q_4$ | □ Л $q_5$ |
| $q_5$ | I Л $q_5$ | □ П $q_6$ |
| $q_6$ | □ П $q_1$ | |
| $q_7$ | I Л $q_7$ | I М $q_0$ |

Пояснение. Указатель двигается вправо, минуя первый и второй наборы палочек, затем удаляет крайнюю правую палочку второго набора, затем указатель двигается влево, минуя второй и первый наборы палочек, затем машина удаляет крайнюю левую палочку первого набора. На этом заканчивается один цикл работы машины. Затем эти циклы повторяются до тех пор, пока остаются палочки в вычитаемом. Как только машина Тьюринга обнаружит, что в вычитаемом палочек не осталось, указатель начнет двигаться влево, минуя все оставшиеся палочки. Машина припишет слева недостающую палочку, и указатель остановится против нее.

$$(n_1+1)-(n_2+1)=n_1-n_2=(n_1-n_2+1)-1$$

## 6.9. Тезис Чёрча

Понятие рекурсивной функции является строгим, так как оно опирается на понятие машины Тьюринга, которое тоже является строгим. Понятие вычислимой функции не является строгим, так как оно опирается на интуитивное понятие алгоритма. Очевидно, что если функция рекурсивна, то она будет и вычислимой, так как, если можно вычислять значения функции с помощью некоторой машины Тьюринга, то тем более можно сказать, что существует алгоритм (т.е. универсальный автоматический метод) для вычисления значений этой функции. Возникает вопрос, будет ли справедливо обратное утверждение. Несмотря на то, что обратное утверждение вызывает сомнение, Чёрч высказал предположение, называемое тезисом Чёрча: «Всякая вычислимая функция является рекурсивной».

Тезис Чёрча нельзя в принципе строго доказать как теорему, так как в его формулировку входит нестрогое понятие. Опровергнуть тезис Чёрча было бы возможно, если бы удалось привести пример вычислимой функции, которая бы не была рекурсивной. Однако, несмотря на многочисленные попытки крупнейших математиков разных стран мира, такой пример привести не удалось, и в настоящее время тезис Чёрча является общепризнанным.

Принять тезис Чёрча – значит договориться признать строгое понятие рекурсивной функции за уточнение нестрогого понятия вычислимой функции.

Рассмотренное нами определение рекурсивной функции принадлежит Тьюрингу. Рассмотрим еще одно определение рекурсивной функции.

## 6.10. Примитивно рекурсивные функции

Договоримся рассматривать только натуральные функции от одного или нескольких натуральных аргументов. $N = \{0,1,2,3,...\}$.

Простейшими функциями мы назовем следующие функции:

1. $s(x) = x + 1$ «следовать за».
2. $C_0^{(1)}(x) = 0$ «одноместная константа 0».
3. $J_m^{(n)}(x_1,...,x_n) = x_m$ $\quad n = 1,2,3,...$ $\quad 1 \le m \le n$ «функция выбора определенного аргумента». Например: $J_2^{(3)}(x, y, z) = y$.

Заметим, что каждая из простейших функций всюду определена. Введем следующие операции над функциями.

**1. Суперпозиция.** Пусть дана функция *g*, зависящая от *n* аргументов, и даны функции $f_1$, …, $f_n$, зависящие от *m* аргументов. Тогда мы можем определить функцию *h*, зависящую от *m* аргументов, следующим образом

$$h(x_1, x_2,..., x_m) = g(f_1(x_1, x_2,..., x_m), f_2(x_1, x_2,..., x_m),..., f_n(x_1, x_2,..., x_m)).$$

Функцию *h* называют суперпозицией функций *g*, $f_1$, …, $f_n$.

$$h = S(g, f_1,..., f_n).$$

Функция *h* определена на наборе $x_1$, $x_2$, …, $x_m$ тогда и только тогда, когда каждая из функций $f_1$, …, $f_n$ определена на этом наборе и функция *g* определена на наборе $y_1$, $y_2$, …, $y_n$, где

$$y_1 = f_1(x_1, x_2,..., x_m),\ y_2 = f_2(x_1, x_2,..., x_m),\ …,\ y_n = f_n(x_1, x_2,..., x_m).$$

В частности, если каждая из данных функций *g*, $f_1$, …, $f_n$ будет всюду определена, то и функция *h*, являющаяся их суперпозицией, будет всюду определена.

**2. Примитивная рекурсия.** Пусть даны две функции: *g*, зависящая от *n* аргументов, и *h*, зависящая от $n + 2$ аргументов. Тогда можно определить функцию *f*, зависящую от $n + 1$ аргумента, следующим образом:

$$(*)\ \begin{cases} f(x_1, x_2,..., x_n, 0) = g(x_1, x_2,..., x_n), \\ f(x_1, x_2,..., x_n, y+1) = h(x_1, x_2,..., x_n, y, f(x_1, x_2,..., x_n, y)). \end{cases}$$

В силу данного определения мы можем последовательно находить значения функции *f*.

$$f(x_1, x_2,..., x_n, 0) = g(x_1, x_2,..., x_n),$$
$$f(x_1, x_2,..., x_n, 1) = h(x_1, x_2,..., x_n, 0, f(x_1, x_2,..., x_n, 0)),$$
$$f(x_1, x_2,..., x_n, 2) = h(x_1, x_2,..., x_n, 1, f(x_1, x_2,..., x_n, 1)),$$
$$\ldots$$

Если функция *f* получается из *g* и *h* с помощью системы (*), то говорят, что функция *f* получается из *g* и *h* примитивной рекурсией.

$$f = R(g, h)$$

**Замечание.** Функция $f$ определена на наборе $(x_1, x_2, ..., x_n, 0)$ тогда и только тогда, когда функция $g$ определена на наборе $(x_1, x_2, ..., x_n)$; функция $f$ определена на наборе $(x_1, x_2, ..., x_n, y+1)$ тогда и только тогда, когда функция $f$ определена на наборе $(x_1, x_2, ..., x_n, y)$ и функция $h$ определена на наборе $(x_1, x_2, ..., x_n, y, z)$, где $z = f(x_1, x_2, ..., x_n, y)$. Если данные функции $g$ и $h$ определены всюду, то и функция $f$ также является всюду определенной, если она получается из $g$ и $h$ примитивной рекурсией.

**Замечание.** Операцией «примитивная рекурсия» может быть получена и функция от одного аргумента $f$ из постоянного числа $q$ и функции $h$, зависящей от двух аргументов.

$$\begin{cases} f(0) = q, \\ f(x+1) = h(x, f(x)). \end{cases}$$

$$f = R(q, h).$$

**Определение 6.10.1.** Натуральная функция от одного или нескольких натуральных аргументов называется примитивно рекурсивной, если она может быть получена из простейших функций с помощью таких операций как суперпозиция и примитивная рекурсия.

**Следствие 1.** Всякая простейшая функция является примитивно рекурсивной.

**Следствие 2.** Если функция получена из примитивно рекурсивных функций с помощью операций суперпозиции и примитивной рекурсии, то эта функция также будет примитивно рекурсивной.

**Замечание.** Всякая примитивно рекурсивная функция всюду определена. Действительно, простейшие функции являются всюду определенными, кроме того, операции суперпозиции и примитивной рекурсии, будучи применены к всюду определенным функциям, снова дают всюду определенные функции.

## 6.11. Примеры примитивно рекурсивных функций

**Пример 1.** $n$-местная константа 0: $C_0^{(n)}(x_1, x_2, ..., x_n) = 0$.

$$C_0^{(n)}(x_1, x_2, ..., x_n) = C_0^{(1)}(J_1^{(n)}(x_1, x_2, ..., x_n)) = C_0^{(1)}(x_1) = 0$$

$C_0^{(n)} = S(C_0^{(1)}, J_1^{(n)})$ примитивно рекурсивна, так как $C_0^{(1)}$ и $J_1^{(n)}$ – простейшие.

**Пример 2.** Произвольная $n$-местная константа: $C_q^{(n)}(x_1, x_2, ..., x_n) = q$.

$q = 0$, $C_0^{(n)}(x_1, x_2, ..., x_n) = 0$ примитивно рекурсивна.

$q = 1$, $C_1^{(n)}(x_1, x_2, ..., x_n) = 1$.

$C_1^{(n)}(x_1, x_2, ..., x_n) = s(C_0^{(n)}(x_1, x_2, ..., x_n)) = s(0) = 0 + 1 = 1$.

$C_1^{(n)} = S(s, C_0^{(n)})$ – примитивно рекурсивная, так как $s$ – простейшая, а $C_0^{(n)}$ – примитивно рекурсивная.

$q = 2$, $C_2^{(n)}(x_1, x_2, ..., x_n) = 2$.

$C_2^{(n)}(x_1, x_2, ..., x_n) = s(C_1^{(n)}(x_1, x_2, ..., x_n)) = s(1) = 1 + 1 = 2$.

$C_2^{(n)} = S(s, C_1^{(n)})$ – примитивно рекурсивная, так как s – простейшая, а $C_1^{(n)}$ – примитивно рекурсивная.

И так далее.

**Пример 3.** $f(x, y) = x + y$. Запишем схему примитивной рекурсии для $n = 1$.

$$\begin{cases} f(x,0) = g(x) \\ f(x, y+1) = h(x, y, f(x, y)) \end{cases}$$

$$\begin{cases} f(x,0) = x + 0 = x \\ f(x, y+1) = x + (y+1) = (x + y) + 1 = f(x, y) + 1 = s(f(x, y)) \end{cases}$$

$g(x) = x$, $g = J_1^{(1)}$ – простейшая. $h(x, y, z) = s(z) = s(J_3^{(3)}(x, y, z))$. $h = S(s, J_3^{(3)})$ – примитивно рекурсивная, так как $s$ и $J_3^{(3)}$ – простейшие. $f = R(g, h)$ – примитивно рекурсивная.

**Пример 4.** $f(x, y) = x \cdot y$.

$$\begin{cases} f(x,0) = g(x) \\ f(x, y+1) = h(x, y, f(x, y)) \end{cases}$$

$$\begin{cases} f(x,0) = x \cdot 0 = 0 \\ f(x, y+1) = x(y+1) = xy + x = f(x, y) + x \end{cases}$$

$g(x) = 0$, $g = C_0^{(1)}$ – простейшая.

$$h(x, y, z) = z + x = J_3^{(3)}(x, y, z) + J_1^{(3)}(x, y, z)$$

$h = S(+, J_3^{(3)}, J_1^{(3)})$ – примитивно рекурсивная, так как «+» – примитивно рекурсивно, а $J_3^{(3)}$ и $J_1^{(3)}$ – простейшие. $f = R(g, h)$ – примитивно рекурсивная.

**Пример 5.** $f(x, y) = x^y = \exp(x, y)$.

$$\begin{cases} f(x,0) = x^0 = 1 \\ f(x, y+1) = x^{y+1} = x^y x = f(x, y) \cdot x \end{cases}$$

$g(x) = 1$, $g = C_1^{(1)}$ – примитивно рекурсивная.

$$h(x, y, z) = z \cdot x = J_3^{(3)}(x, y, z) \cdot J_1^{(3)}(x, y, z)$$

$h = S(\cdot, J_3^{(3)}, J_1^{(3)})$ – примитивно рекурсивная, так как «·» – примитивно рекурсивно, а $J_3^{(3)}$ и $J_1^{(3)}$ – простейшие. $f = R(g, h)$ – примитивно рекурсивная.

**Пример 6.** $f(x) = x!$

$$\begin{cases} f(0) = q \\ f(x+1) = h(x, f(x)) \end{cases}$$

$$\begin{cases} f(0) = 0! = 1 \\ f(x+1) = (x+1)! = x!(x+1) = x!s(x) = f(x)s(x) \end{cases}$$

$q = 1$, $h(x,y) = y \cdot s(x) = J_2^{(2)}(x,y) \cdot s(J_1^{(2)}(x,y))$. $h = S(\cdot, J_2^{(2)}, S(s, J_1^{(2)}))$ – примитивно рекурсивная, так как «$\cdot$» – примитивно рекурсивно, а $J_2^{(2)}$, $s$ и $J_1^{(2)}$ – простейшие. $f = R(q,h)$ – примитивно рекурсивная.

**Пример 7.** $f(x) = np.x$ – предшественник числа $x$.

$$f(x) = np.x = \begin{cases} x-1, & x > 0 \\ 0, & x = 0 \end{cases}.$$

$$\begin{cases} f(0) = q \\ f(x+1) = h(x, f(x)) \end{cases}$$

$$\begin{cases} f(0) = np.x = 0 \\ f(x+1) = x \end{cases}$$

$q = 0$, $h(x,y) = x$, $h = J_1^{(2)}$ – простейшая. $f = R(0,h)$ – примитивно рекурсивная.

**Пример 8.**

$f(x,y) = x \dot{-} y$ – усеченная разность.

$$f(x,y) = \begin{cases} x-y, & x \ge y \\ 0, & x < y \end{cases}$$

$$\begin{cases} f(x,0) = g(x) \\ f(x,y+1) = h(x,y,f(x,y)) \end{cases}$$

$$\begin{cases} f(x,0) = x \dot{-} 0 = x \\ f(x,y+1) = x \dot{-} (y+1) = np.(x \dot{-} y) = np.(f(x,y)) \end{cases}$$

$g(x) = x$, $g = J_1^{(1)}$ – простейшая функция.

$$h(x,y,z) = np.z = np.J_3^{(3)}(x,y,z)$$

$h = S(np., J_3^{(3)})$ – примитивно рекурсивная, так как $np.$ – примитивно рекурсивная, а $J_3^{(3)}$ – простейшая. $f = R(g,h)$ – примитивно рекурсивная.

**Пример 9.** $f(x,y) = |x-y| = \rho(x,y)$.

$$|x-y| = (x \dot{-} y) + (y \dot{-} x) = (x \dot{-} y) + \left( J_2^{(2)}(x,y) \dot{-} J_1^{(2)}(x,y) \right).$$

$|x-y| = S\left(+, \dot{-}, S\left(\dot{-}, J_2^{(2)}, J_1^{(2)}\right)\right)$ – примитивно рекурсивная, так как «+» и «$\dot{-}$» примитивно рекурсивные, а $J_2^{(2)}$ и $J_1^{(2)}$ – простейшие.

## 6.12. Операция минимизации. Рекурсивные функции

Пусть дана $n$-местная функция $f(x_1,...,x_{n-1},y)$, где $n \ge 1$. Определим $n$-местную функцию $g(x_1,...,x_n)$ следующим образом. Пусть $g(x_1,...,x_n)$ равно наименьшему натуральному значению $y$, при котором $f(x_1,...,x_{n-1},y)$ равно $x_n$:

$$g(x_1,...,x_n) = \mu_y\big(f(x_1,...,x_{n-1},y) = x_n\big)$$

Значение $g(x_1,...,x_n)$ определено во всех случаях, кроме следующих:

а) значение $f(x_1,...,x_{n-1},0)$ не определено;

б) значения $f(x_1,...,x_{n-1},y)$ определены для $y = 0, 1, ..., a-1$, но отличны от $x_n$, а значение $f(x_1,...,x_{n-1},a)$ не определено;

в) значения $f(x_1,...,x_{n-1},y)$ определены для всех $y = 0, 1, 2, ...$ и отличны от $x_n$.

Рассмотренную операцию называют операцией минимизации и обозначают через $M$.

$$g = M(f).$$

**Определение 6.12.1.** Натуральная функция от натуральных аргументов называется рекурсивной (частично рекурсивной), если она может быть получена из простейших функций с помощью таких операций как суперпозиция, примитивная рекурсия и минимизация.

Можно доказать, что это определение рекурсивной функции равносильно приведенному выше.

Заметим, что каждая примитивно рекурсивная функция рекурсивна, что непосредственно вытекает из определений. Так как каждая примитивно рекурсивная функция всюду определена, то она также и общерекурсивна. Заметим также, что всякая функция, которую можно получить из примитивно рекурсивных функций операциями суперпозиции, примитивной рекурсии и минимизации, является рекурсивной.

Приведем пример рекурсивной функции, которая не является примитивно рекурсивной.

**Пример.** $f(x,y) = x - y$. $x - y = \mu_z(y + z = x)$. Если обозначить через $g(y,x) = \mu_z(y + z = x)$, то $g = M(+)$. Следовательно,

$$f(x,y) = g(y,x) = g\left(J_2^{(2)}(x,y); J_1^{(2)}(x,y)\right),$$

то есть $f = S\left(g, J_2^{(2)}, J_1^{(2)}\right)$ или $f = S\left(M(+), J_2^{(2)}, J_1^{(2)}\right)$. Итак $f$ рекурсивна, но не примитивно рекурсивна, так как не всюду определена.

# ЛИТЕРАТУРА


1. Игошин В. И. Математическая логика и теория алгоритмов [Текст] : учеб. / В. И. Игошин. – Саратов. «Издательство Саратовского университета», 1991. – 256 с.
2. Клини С. К. Математическая логика [Текст] : учеб. / С. К. Клини. – М. «Мир», 1973. – 480 с.
3. Мальцев А. И. Алгоритмы и рекурсивные функции [Текст] : учеб. / А. И. Мальцев. – М. «Наука», «Главная редакция физико-математической литературы», 1965. – 392 с.
4. Мендельсон Э. Введение в математическую логику [Текст] : учеб. / Э. Мендельсон. – М. «Наука», «Главная редакция физико-математической литературы», 1971. – 320 с.
5. Новиков П. С. Элементы математической логики [Текст] : учеб. / П. С. Новиков. – М. «Наука», «Главная редакция физико-математической литературы», 1973. – 400 с.
6. Успенский В. А. Вводный курс математической логики [Текст] : учеб. / Н. К. Верещагин, В. Е. Плиско. – М. : «Физматлит», 2002. – 125 с.
7. Чёрч Л. Введение в математическую логику, том 1 [Текст] : учеб. / Л. Чёрч. – М. : «Издательство иностранной литературы», 1960. – 488с.

ISBN 978-5-9905230-1-2

***Дмитрий Давидович Изаак***

# МАТЕМАТИЧЕСКАЯ ЛОГИКА

***КУРС ЛЕКЦИЙ***

*Работа отпечатана с оригинала-макета,*
*предоставленного автором*