

Математическая логика, 2022



Содержание

Введение. Предмет математической логики	1
I. Логика высказываний	2
§1. Алгебра высказываний	2
1.1. Высказывания	2
1.2. Формулы алгебры высказываний	3
1.3. Тавтологии	4
§2. Формальные аксиоматические теории	5
2.1. Определение формальной теории	5
2.2. Доказательства и теоремы	5
§3. Аксиоматическая теория исчисления высказываний	6
3.1. Определение теории исчисления высказываний	6
3.2. Доказательства в исчислении высказываний	6
3.3. Теорема дедукции	9
3.4. Применение теоремы дедукции	9
3.5. Полнота и непротиворечивость ИВ	11
§4. Другие аксиоматические теории ИВ	12
4.1. Исчисление Гильберта–Аккермана	12
4.2. Исчисление Россера	12
4.3. Исчисление секвенций	12
4.4. Исчисление Клини	13
II. Логика предикатов первого порядка	15
§1. Кванторы и формулы логики предикатов первого порядка	15
§2. Интерпретации и метод моделей	16
§3. Теории первого порядка	16
§4. Теорема дедукции в теории ИП	17

Введение. Предмет математической логики

Математическая логика (символическая логика) — раздел фундаментальной математики, в котором математическими методами исследуются законы человеческого мышления.

Современная математическая логика занимается проблемами математических доказательств и оснований математики.

Разделы математической логики:

1. Логика высказываний;
2. Логика предикатов;
3. Теория доказательств;
4. Теория моделей;
5. Теория вычислимости.

I. Логика высказываний

§1. Алгебра высказываний

1.1. Высказывания

Высказывание — утверждение, о котором можно определённо сказать, истинно оно или ложно.

Высказывание может принимать только два истинностных значения: истина или ложь.

Высказывания делятся на *простые (элементарные)* и сложные (*составные*). Простые высказывания представляют собой одно утверждение, сложные составлены из простых с помощью *операций над высказываниями*.

Назначение логики высказываний — определение истинностных значений сложных высказываний только на основе их структуры, т.е. безотносительно смысла высказывания.

Пропозициональные связки Сложные высказывания строятся как истинностно-функциональные комбинации простых высказываний.

Простые высказывания будем обозначать строчными латинскими буквами: $a, b, c, \dots, a_1, a_2, \dots$, сложные — прописными латинскими буквами: $A, B, C, \dots, A_1, A_2, \dots$.

Операции над высказываниями:

1. Отрицание.

Определение. *Отрицанием* высказывания A называется высказывание $\neg A$, ложное тогда и только тогда, когда A истинно.

Истинностные значения высказываний удобно записывать в таблицы — *таблицы истинности (истинностные таблицы)*.

Таблица истинности для отрицания:

A	$\neg A$
И	Л
Л	И

И — истина, Л — ложь

2. Конъюнкция.

Определение. *Конъюнкцией* высказываний A и B называется высказывание $A \wedge B$, истинное тогда и только тогда, когда A и B истинны.

Таблица истинности для конъюнкции:

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

3. Дизъюнкция.

Определение. *Дизъюнкцией* высказываний A и B называется высказывание $A \vee B$, ложное тогда и только тогда, когда A и B ложны.

Таблица истинности для дизъюнкции:

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

4. Импликация.

Определение. Импликацией высказываний A и B называется высказывание $A \supset B$, ложное тогда и только тогда, когда A истинно, а B ложно.

Таблица истинности для импликации:

A	B	$A \supset B$
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

} Принцип материальной импликации

Определение. Высказывание A называется *антецедентом* (посылкой), B — *консеквентом* (следствием) импликации.

5. Эквиваленция.

Определение. Эквиваленцией высказываний A и B называется высказывание $A \equiv B$, истинное тогда и только тогда, когда A и B принимают одинаковые истинностные значения.

Таблица истинности для эквиваленции:

A	B	$A \equiv B$
И	И	И
Л	И	Л
И	Л	Л
Л	Л	И

Пропозициональными связками называются знаки операций \neg , \wedge , \vee , \supset , \equiv .

1.2. Формулы алгебры высказываний

Высказывания и операции над ними образуют *алгебру высказываний*. Для записи формул этой алгебры используем алфавит, состоящий из:

1. строчных латинских букв $a, b, c, \dots, a_1, a_2, \dots$ — *пропозициональных букв*;
2. пропозициональных связок;
3. специальных символов $(,)$.

Определение. Формулой алгебры высказываний (*пропозициональной формой*) называется слово в алфавите алгебры высказываний, построенное по правилам:

1. Любая пропозициональная буква есть формула.
2. Если A, B есть формулы, то слова $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \supset B)$, $(A \equiv B)$ также являются формулами.
3. Слово является формулой в том и только том случае, когда оно получено по правилам 1 и 2.

Определение. Подформулой формулы называется её часть, сама являющаяся формулой.

Правила удаления лишних скобок:

1. Внешние скобки можно опускать.
2. Если формула содержит вхождения только одной бинарной связки \wedge , \vee , \supset или \equiv , то для каждого вхождения можно опускать внешние скобки у подформулы слева.
3. Введём приоритет связок (по возрастанию): \equiv , \supset , \vee , \wedge , \neg . Можно опускать пары скобок, без которых возможно восстановление исходной формулы по следующим правилам. Каждое вхождение связки \neg относится к наименьшей следующей за ним подформуле. После расстановки скобок, относящихся к \neg каждое вхождение символа \wedge связывает наименьшие окружающие его подформулы. После расстановки скобок, относящихся к \wedge , каждое вхождение \vee относится к наименьшим подформулам слева и справа от него. Далее подобным образом расставляются скобки, относящиеся к символам \supset и \equiv . При применении этого правила к одинаковым связкам движение по формуле происходит слева направо.

Формулы представляют собой формализованную математическую запись реальных высказываний. Поэтому для обозначения формул будем использовать прописные латинские буквы.

Каждому распределению истинностных значений пропозициональных букв, входящих в формулу, соответствует некоторое истинностное значение этой формулы, полученное по таблицам истинности пропозициональных связок. Таким образом, любая пропозициональная форма (слово, последовательность символов) определяет некоторую истинностную функцию (математическую функцию, функцию алгебры логики). Эта функция может быть графически представлена истинностной таблицей формулы.

Пример таблицы для формулы $\neg(A \wedge \neg B) \supset C$:

A	B	C	$\neg B$	$A \wedge \neg B$	$\neg(A \wedge \neg B)$	$\neg(A \wedge \neg B) \supset C$
И	И	И	Л	Л	И	И
И	И	Л	Л	Л	И	Л
И	Л	И	И	И	Л	И
И	Л	Л	И	И	Л	И
Л	И	И	Л	Л	И	И
Л	И	Л	Л	Л	И	Л
Л	Л	И	И	Л	И	И
Л	Л	Л	И	Л	И	Л

1.3. Тавтологии

Далее будем отождествлять форму и соответствующую ей истинностную функцию (не забывая при этом в чём их различие).

Определение. Формула называется *тождественно истинной* (*тавтологией*), если она истинна при любых наборах истинностных значений входящих в неё букв.

Определение. Формула называется *тождественно ложной* (*противоречием*), если она ложна при любых наборах истинностных значений входящих в неё букв.

Определение. Формула называется *выполнимой* (*опровержимой*), если она истинна (ложна) при некотором наборе истинностных значений входящих в неё букв.

Очевидно следующее утверждение.

Лемма 1.1. Формула A является тавтологией тогда и только тогда, когда $\neg A$ является противоречием.

Следующие важные теоремы служат основаниями для фундаментальных правил логического вывода.

Теорема 1.1. Если $A, A \supset B$ — тавтологии, то B — также тавтология.

Доказательство. От противного. Предположим, что B не является тавтологией. Тогда существует набор истинностных значений входящих в B букв, который реализует ложность B . В силу того, что A — тавтология, на указанном наборе A будет истинно. С другой стороны, импликация $A \supset B$ ложна в связи с истинностью A и ложностью B на указанному наборе, что вступает в противоречие с тем, что $A \supset B$ — тавтология. Значит B является тавтологией. ■

Эта теорема обосновывает правило вывода по индукции *modus ponens*.

Теорема 1.2. Если A — тавтология, содержащая пропозициональные буквы a_1, a_2, \dots, a_n , формула B получена подстановкой в A формул A_1, A_2, \dots, A_n вместо всех вхождений букв a_1, a_2, \dots, a_n соответственно. Тогда B также является тавтологией.

Доказательство. От противного. Пусть B не является тавтологией, тогда существует набор истинностных значений входящих в B букв, реализующий ложность этой формулы. Пусть этот набор доставляет формулам A_1, A_2, \dots, A_n истинностные значения $\alpha_1, \alpha_2, \dots, \alpha_n$ соответственно. Присвоим буквам a_1, a_2, \dots, a_n формулы A истинностные значения $\alpha_1, \alpha_2, \dots, \alpha_n$ соответственно. Ясно, что полученное ранее истинностное значение B совпадает с истинностным значением A , полученным в предыдущей подстановке. Такое совпадение порождает противоречие, ибо B , как показано ранее, ложно, а A — тавтология по условию. Значит B является тавтологией. ■

Теорема 1.2 утверждает, что подстановка в тавтологию вместо всех вхождений букв (причём, не обязательно всех букв) произвольных формул даёт тавтологию. Таким образом, она обосновывает правило подстановки, используемое неявно в рассматриваемых далее исчислениях.

§2. Формальные аксиоматические теории

2.1. Определение формальной теории

Метод формальных теорий — другой, более мощный метод решения задачи логических исчислений. Но вместе с тем, это очень трудный метод.

Формальная аксиоматическая теория определена, если:

1. Задан *алфавит* теории (алфавит — не более чем счётное множество символов).
2. Задано подмножество слов в алфавите теории, которые считаются *формулами* теории.
3. Выделено некоторое подмножество формул — *аксиом* теории.
4. Задано конечное множество отношений между формулами теории, которые называются *правилами вывода*.

Введённые компоненты теории удовлетворяют следующим условиям:

1. Можно эффективно определить, является ли данная формула аксиомой теории или нет. Именно такие теории будем называть *аксиоматическими* (*аксиоматизируемыми*).
2. Правила вывода заданы эффективно. Это означает, что для каждого правила R_i существует такое число $j > 0$, что для любого набора j формул A_1, \dots, A_j и для любой формулы A можно эффективно определить, находятся ли эти формулы в отношении R_i с формулой A : $\langle A_1; \dots; A_j; A \rangle \in R_i$. Если находятся, то говорят, что формула A является непосредственным следствием формул A_1, \dots, A_j по правилу вывода R_i :

$$\frac{A_1, \dots, A_j}{A}.$$

2.2. Доказательства и теоремы

Определение. *Доказательством* (*выводом*) в теории называется такая последовательность формул A_1, \dots, A_m , что для любого $i > 0$ A_i — либо аксиома, либо непосредственное следствие каких-либо предыдущих формул по одному из правил вывода.

Определение. Формула называется *теоремой* теории, если существует вывод, в котором эта формула последняя. Такой вывод называется *доказательством* (*выводом*) теоремы.

Определение. Теория называется *разрешимой*, если для любой формулы существует эффективный алгоритм определения, является ли она теоремой теории или нет.

В разрешимой теории доказательство можно автоматизировать (механизировать). В неразрешимой теории поиск доказательств — творческий процесс, посильный только человеку.

Определение. Формула A называется *следствием* в теории множества формул Γ , если существует последовательность формул A_1, \dots, A_m , в которой A_m есть A , а для каждого $i > 0$ A_i — либо аксиома, либо непосредственное следствие каких-либо предыдущих формул по одному из правил вывода, либо формула из Γ . Такой вывод называется *доказательством* (*выводом*) формулы A из множества формул Γ . Формулы из множества Γ называются *гипотезами* (*посылками*).

Обозначается выводимость $\Gamma \vdash A$ или $A_1, \dots, A_s \vdash A$. Если $\Gamma = \emptyset$, то $\Gamma \vdash A$ равносильно тому, что A — теорема, поэтому тот факт, что A является теоремой, записывают $\vdash A$.

Свойства выводимости из посылок:

1. Если $\Gamma \subseteq \Delta$ и $\Gamma \vdash A$, то $\Delta \vdash A$ (в множество гипотез можно добавлять любые формулы).
2. $\Gamma \vdash A$ тогда и только тогда, когда в Γ имеется такое конечное подмножество Δ , что $\Delta \vdash A$ (некоторые формулы можно удалять из множества гипотез без потери выводимости).
3. Если $\Delta \vdash A$ и $\Gamma \vdash B$ для каждой формулы $B \in \Delta$, то $\Gamma \vdash A$.

§3. Аксиоматическая теория исчисления высказываний

3.1. Определение теории исчисления высказываний

Зададим теорию исчисления высказываний.

Алфавит теории:

1. пропозициональные буквы $A, B, C, \dots, A_1, A_2, \dots$;
2. пропозициональные связки \neg, \supset ;
3. специальные символы $(,)$.

Формулы теории определяются рекуррентно по правилам:

1. Любая пропозициональная буква есть формула.
2. Если A, B есть формулы, то слова $(\neg A), (A \supset B)$ также являются формулами.
3. Слово является формулой в том и только том случае, когда оно получено по правилам 1 и 2.

Используются те же правила удаления лишних скобок (см. п. 1.2.).

Аксиомы теории:

- (A1) $A \supset (B \supset A)$;
 (A2) $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$;
 (A3) $(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$.

Единственное правило вывода: B — непосредственное следствие формул $A, A \supset B$, или

$$\frac{A, A \supset B}{B}.$$

Это правило называется *modus ponens* (MP). Его правомерность обосновывается теоремой 1.1.

Замечание 1. Аксиомы на самом деле являются *схемами аксиом*. Это означает, что подстановка в схему любых формул вместо всех вхождений букв (все вхождения одной буквы заменяются одной и той же формулой) даёт аксиому в силу теоремы 1.2. Таким образом, множество аксиом в нашем исчислении бесконечно.

Замечание 2. Остальные пропозициональные связки используются для сокращения формул по эквивалентным заменам:

$$\begin{aligned} A \wedge B &\Longleftrightarrow \neg(A \supset \neg B); \\ A \vee B &\Longleftrightarrow \neg A \supset B; \\ A \equiv B &\Longleftrightarrow (A \supset B) \wedge (B \supset A). \end{aligned}$$

3.2. Доказательства в исчислении высказываний

Лемма 3.1. $\vdash A \supset A$.

Доказательство.

1. $(A \supset ((A \supset A) \supset A)) \supset ((A \supset (A \supset A)) \supset (A \supset A))$ (A2);
2. $A \supset ((A \supset A) \supset A)$ (A1);
3. $(A \supset (A \supset A)) \supset (A \supset A)$ (из 1, 2 по MP);
4. $A \supset (A \supset A)$ (A1);
5. $A \supset A$ (из 3, 4 по MP).



Лемма 3.2. $\vdash (\neg A \supset A) \supset A$.

Доказательство.

1. $\neg A \supset \neg A$ (лемма 3.1);
2. $(\neg A \supset \neg A) \supset ((\neg A \supset A) \supset A)$ (A3);
3. $(\neg A \supset A) \supset A$ (из 1, 2 по MP).

■

Лемма 3.3. $A \supset B, B \supset C \vdash A \supset C$.

Доказательство.

1. $B \supset C$ (гипотеза);
2. $(B \supset C) \supset (A \supset (B \supset C))$ (A1);
3. $A \supset (B \supset C)$ (из 1, 2 по MP);
4. $A \supset B$ (гипотеза);
5. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$ (A2);
6. $(A \supset B) \supset (A \supset C)$ (из 3, 5 по MP);
7. $A \supset C$ (из 4, 6 по MP).

■

Лемма 3.4. $\vdash A \supset (B \supset (A \supset B))$.

Доказательство.

1. $B \supset (A \supset B)$ (A1);
2. $(B \supset (A \supset B)) \supset (A \supset (B \supset (A \supset B)))$ (A1);
3. $A \supset (B \supset (A \supset B))$ (из 1, 2 по MP).

■

Лемма 3.5.

- 1) $\vdash A \supset (A \vee B)$;
- 2) $\vdash B \supset (A \vee B)$.

Доказательство.

- 1) Доказывается на основе $A, \neg A \vdash B$ (см. (1) в лемме 3.10) и применения теоремы дедукции (теорема 3.1):

$$A, \neg A \vdash B \implies A \vdash \neg A \supset B \iff A \vdash A \vee B.$$

- 2) Запись $B \supset (A \vee B)$ понимается как $B \supset (\neg A \supset B)$, что есть просто аксиома A1.

■

Лемма 3.6.

- 1) $A \wedge B \vdash A$;
- 2) $A \wedge B \vdash B$.

Доказательство.

- 1) Данная выводимость расшифровывается как $\neg(A \supset \neg B) \vdash A$. Для доказательства понадобятся результаты лемм 3.8 и 3.10, а также теорема дедукции. А именно,

$$\neg A, A \vdash \neg B \xrightarrow{\text{т. дедукции}} \neg A \vdash A \supset \neg B \xrightarrow{\text{контрапозиция}} \neg(A \supset \neg B) \vdash \neg\neg A \xrightarrow{\text{удаление } \neg\neg} \neg(A \supset \neg B) \vdash A.$$

- 2) Выводимость $\neg(A \supset \neg B) \vdash B$ поясняется аналогично на основе выводимости $\neg B \vdash A \supset \neg B$:

1. $\neg B$ (гипотеза);
2. $\neg B \supset (A \supset \neg B)$ (A1);
3. $A \supset \neg B$ (из 1, 2 по МР).

Далее получаем

$$\neg B \vdash A \supset \neg B \xrightarrow{\text{контрапозиция}} \neg(A \supset \neg B) \vdash \neg\neg B \xrightarrow{\text{удаление } \neg\neg} \neg(A \supset \neg B) \vdash B.$$

■

Лемма 3.7. $A \supset (B \supset C), B \vdash A \supset C$

Доказательство.

1. $A \supset (B \supset C)$ (гипотеза);
2. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$ (A2);
3. $(A \supset B) \supset (A \supset C)$ (из 1, 2 по МР);
4. $B \supset (A \supset B)$ (A1);
5. B (гипотеза);
6. $A \supset B$ (5, 4 по МР);
7. $A \supset C$ (из 6, 3 по МР).

■

Лемма 3.8.

- 1) $\vdash \neg\neg A \supset A$;
- 2) $\vdash A \supset \neg\neg A$;
- 3) $\neg\neg A \vdash A$;
- 4) $A \vdash \neg\neg A$.

Доказательство.

- 1)
 1. $(\neg A \supset \neg\neg A) \supset ((\neg A \supset \neg A) \supset A)$ (A3);
 2. $\neg A \supset \neg A$ (лемма 3.1);
 3. $(\neg A \supset \neg\neg A) \supset A$ (из 1, 2 по лемме 3.7);
 4. $\neg\neg A \supset (\neg A \supset \neg\neg A)$ (A1);

5. $\neg\neg A \supset A$ (из 4, 3 по лемме 3.3).
- 2) 1. $(\neg\neg\neg A \supset \neg A) \supset ((\neg\neg\neg A \supset A) \supset \neg\neg A)$ (A3);
 2. $\neg\neg\neg A \supset \neg A$ (формула $\neg\neg\neg A \supset A$ с подстановкой $A \Leftrightarrow \neg A$);
 3. $(\neg\neg\neg A \supset A) \supset \neg\neg A$ (из 2, 1 по МР);
 4. $A \supset (\neg\neg\neg A \supset A)$ (A1);
 5. $A \supset \neg\neg A$ (из 4, 3 по лемме 3.3).
- 3) 1. $\neg\neg A$ (гипотеза);
 2. $\neg\neg A \supset A$ (выведенная теорема в п. 1);
 3. A (из 1, 2 по МР).
- 4) 1. A (гипотеза);
 2. $A \supset \neg\neg A$ (выведенная теорема в п. 2);
 3. $\neg\neg A$ (из 1, 2 по МР).

■

3.3. Теорема дедукции

Теорема 3.1 (дедукция в ИВ). Если Γ — множество формул и $\Gamma, A \vdash B$, то $\Gamma \vdash A \supset B$.

Доказательство.

Пусть B_1, B_2, \dots, B_n — вывод $\Gamma, A \vdash B$. Тогда B_n совпадает с B .

Доказав индукцией по $i = 1, 2, \dots, n$, что $\Gamma \vdash A \supset B_i$, мы получим утверждение теоремы при $i = n$.

База: $i \leq 2$.

Проверим $\Gamma \vdash A \supset B_1$. Имеются следующие варианты: B_1 — либо аксиома, либо совпадает с A , либо входит в Γ . Если B_1 совпадает с A , то $\Gamma \vdash A \supset A$ — справедливое утверждение (лемма 3.1). Если B_1 есть аксиома или $B_1 \in \Gamma$, то, написав первую аксиому $B_1 \supset (A \supset B_1)$, из B_1 и написанной аксиомы по МР выводим требуемую формулу $A \supset B_1$.

Очевидно, что для $i = 2$ допускаются точно такие же варианты и рассуждения, ибо вывод B_2 по МР невозможен — перед B_2 в выводе должно идти по меньшей мере две формулы.

Индукционное предположение: Пусть $\Gamma \vdash A \supset B_j$ для всех $j = 1, 2, \dots, i - 1$.

Индукционный шаг: Докажем $\Gamma \vdash A \supset B_i$.

Снова имеются варианты: B_i — аксиома, либо B_i совпадает с A , либо входит в Γ , либо выводится из каких-то предыдущих формул B_r, B_q по МР ($r, q < i$). Проверка первых трёх случаев дословно повторяет проверку в базе индукции. Пусть $r < q$. Тогда B_q имеет вид $B_r \supset B_i$. По предположению индукции верны $\Gamma \vdash A \supset B_r$ и $\Gamma \vdash A \supset B_q$. Запишем аксиому A2: $(A \supset \underbrace{(B_r \supset B_i)}_{B_q}) \supset ((A \supset B_r) \supset (A \supset B_i))$. Дважды применяя МР ($A \supset B_q$ и написанная аксиома, а затем $A \supset B_r$ и $(A \supset B_r) \supset (A \supset B_i)$), получаем искомую формулу $A \supset B_i$.

Таким образом, по индукции доказано, что имеет место $\Gamma \vdash A \supset B_n$, то есть $\Gamma \vdash A \supset B$.

■

Следствие. Если $A \vdash B$, то $\vdash A \supset B$.

Замечание (от автора конспекта). Теорема дедукции верна и в обратную сторону: если $\Gamma \vdash A \supset B$, то справедливо $\Gamma, A \vdash B$.

Доказательство. Напишем вывод $\Gamma \vdash A \supset B$, состоящий из формул C_1, C_2, \dots, C_n , где C_n совпадает с $A \supset B$, а каждая из предыдущих формул либо аксиома, либо входит в Γ , либо выводится из некоторых предшествующих по МР. Далее допишем к написанному выводу формулу A как гипотезу (а это именно гипотеза для $\Gamma, A \vdash B$) и выведем B из A и C_n по МР.

■

3.4. Применение теоремы дедукции

Доказательство леммы 3.3.

Вывод $A \supset B, B \supset C, A \vdash C$:

1. $A \supset B$ (гипотеза);

2. A (гипотеза);
3. B (из 2, 1 по МР);
4. $B \supset C$ (гипотеза);
5. C (из 3, 4 по МР).

Теперь, применяя теорему дедукции, получаем $A \supset B, B \supset C \vdash A \supset C$. ■

Лемма 3.9. $A \supset (B \supset C) \vdash B \supset (A \supset C)$.

Доказательство.

Вывод $A \supset (B \supset C), B, A \vdash C$:

1. A (гипотеза);
2. $A \supset (B \supset C)$ (гипотеза);
3. $B \supset C$ (из 1, 2 по МР);
4. B (гипотеза);
5. C (из 4, 3 по МР).

Теперь, дважды применяя теорему дедукции, получаем требуемое: $A \supset (B \supset C) \vdash B \supset (A \supset C)$. ■

Лемма 3.10.

- 1) $\vdash \neg A \supset (A \supset B)$;
- 2) $\vdash (\neg B \supset \neg A) \supset (A \supset B)$ (*доказательство от противного*);
- 3) $\vdash (A \supset B) \supset (\neg B \supset \neg A)$ (*контрапозиция*);
- 4) $\vdash A \supset (\neg B \supset \neg(A \supset B))$;
- 5) $\vdash (A \supset B) \supset ((\neg A \supset B) \supset B)$.

Доказательство.

1) Доказательство $\neg A, A \vdash B$:

1. $\neg A$ (гипотеза);
2. A (гипотеза);
3. $A \supset (\neg B \supset A)$ (A1);
4. $\neg A \supset (\neg B \supset \neg A)$ (A1);
5. $\neg B \supset A$ (из 2, 3 по МР);
6. $\neg B \supset \neg A$ (из 1, 4 по МР);
7. $(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$ (A3);
8. $(\neg B \supset A) \supset B$ (из 6, 7 по МР);
9. B (из 5, 8 по МР).

Теперь дважды применяем теорему дедукции и получаем искомую выводимость.

2) Доказательство $\neg B \supset \neg A, A \supset B$:

1. $\neg B \supset \neg A$ (гипотеза);
2. A (гипотеза);
3. $(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$ (A3);
4. $A \supset (\neg B \supset A)$ (A1);

5. $(\neg B \supset A) \supset B$ (из 1, 3 по МР);
6. $A \supset B$ (из 4, 5 по лемме 3.3);
7. B (из 2, 6 по МР).

Теперь дважды применяем теорему дедукции и получаем искомую выводимость.

3) Доказательство $A \supset B, \neg\neg A \vdash B$:

1. $\neg\neg A$ (гипотеза);
2. A (согласно выведенному $\neg\neg A \vdash A$ в лемме 3.8);
3. $A \supset B$ (гипотеза);
4. B (из 2, 3 по МР).

Тогда по теореме дедукции справедливо $A \supset B \vdash \neg\neg A \supset B$. Далее докажем $A \supset B, \neg B \vdash \neg A$:

1. $\neg B \supset (\neg\neg A \supset \neg B)$ (A1);
2. $\neg B$ (гипотеза);
3. $\neg\neg A \supset \neg B$ (из 2, 1 по МР);
4. $(\neg\neg A \supset \neg B) \supset ((\neg\neg A \supset B) \supset \neg A)$ (A3);
5. $(\neg\neg A \supset B) \supset \neg A$ (из 3, 4 по МР);
6. $A \supset B$ (гипотеза);
7. $\neg\neg A \supset B$ (согласно доказанному $A \supset B \vdash \neg\neg A \supset B$);
8. $\neg A$ (из 7, 5 по МР).

Тогда, дважды применяя теорему дедукции, получаем требуемую выводимость: $\vdash (A \supset B) \supset (\neg B \supset \neg A)$.

4) Ясно, что $A, A \supset B \vdash B$. Дважды используя теорему дедукции, получаем $\vdash A \supset ((A \supset B) \supset B)$. Далее согласно 3) получаем $\vdash ((A \supset B) \supset B) \supset (\neg B \supset \neg(A \supset B))$. Наконец, задействуя лемму 3.3 на предыдущих двух выводимостях, получаем искомое $\vdash A \supset (\neg B \supset \neg(A \supset B))$.

5) Доказательство $A \supset B, \neg A \supset B \vdash B$:

1. $A \supset B$ (гипотеза);
2. $\neg A \supset B$ (гипотеза);
3. $(A \supset B) \supset (\neg B \supset \neg A)$ (доказанная формула контрапозиции);
4. $\neg B \supset \neg A$ (из 1, 3 по МР);
5. $(\neg A \supset B) \supset (\neg B \supset \neg\neg A)$ (доказанная формула контрапозиции);
6. $\neg B \supset \neg\neg A$ (из 2, 5 по МР);
7. $(\neg B \supset \neg\neg A) \supset ((\neg B \supset \neg A) \supset B)$ (A3);
8. $(\neg B \supset \neg A) \supset B$ (из 4, 7 по МР);
9. B (из 4, 8 по МР).

Теперь дважды применяем теорему дедукции и получаем искомую выводимость.

3.5. Полнота и непротиворечивость ИВ

Лемма 3.11 (корректность ИВ). Всякая теорема теории ИВ есть тавтология.

Доказательство. Пусть $\vdash A$ в теории ИВ. Тогда существует вывод B_1, B_2, \dots, B_n , где B_n совпадает с A . Первым делом нужно доказать, что все аксиомы теории ИВ являются тавтологиями. Это можно сделать с помощью составления таблиц истинности для соответствующих формул из схем аксиом, а затем применения теоремы 1.2.

Доказательство того, что B_n — тавтология, можно провести путём проверки по индукции по $j = 1, 2, \dots, n$, что B_j — тавтология. А именно, согласно определению вывода, B_1, B_2 — аксиомы, потому как эти формулы не могут быть выведены по МР из предшествующих (до них должно идти по крайней мере две формулы), а следующие формулы есть аксиомы (то есть тавтологии), либо выводятся из некоторых предшествующих по МР. Вспоминая теорему 1.1, получаем, что из тавтологичности B_j и $B_j \supset B_k$ ($j < k$) вытекает тавтологичность B_k .

Таким образом, доказано, что если A — теорема теории ИВ, то в любом выводе A все формулы — тавтологии, в том числе сама A .

Теорема 3.2 (*полнота ИВ*). Если формула в теории ИВ является тавтологией, то она является теоремой.

Следствие 1. Если слово \mathcal{B} в алфавите ИВ содержит пропозициональные связки $\neg, \supset, \wedge, \vee, \equiv$ и является сокращением некоторой формулы \mathcal{A} теории ИВ, то \mathcal{B} является тавтологией тогда и только тогда, когда \mathcal{A} есть теорема ИВ.

Определение. Теория называется *полной*, если для каждого её верного утверждения \mathcal{A} либо \mathcal{A} , либо отрицание \mathcal{A} есть теорема.

Таким образом, теорема 3.2 утверждает полноту теории ИВ.

Определение. Теория называется *противоречивой*, если в ней существует такое утверждение \mathcal{A} , что и \mathcal{A} , и отрицание \mathcal{A} есть теоремы. Теория называется *непротиворечивой*, если в ней не существует такого утверждения.

Следствие 2. Теория ИВ непротиворечива.

Из непротиворечивости ИВ следует существование формулы, не являющейся теоремой (например, отрицание любой теоремы). С другой стороны, в силу леммы 3.10 (1) из существования формулы, не являющейся теоремой, следует непротиворечивость ИВ. Вообще, непротиворечивость и существование формулы, не являющейся теоремой, эквивалентны для любой теории с правилом вывода МР, в которой выводимо утверждение леммы 3.10 (1).

Определение. Теория называется *абсолютно непротиворечивой*, если в ней не все формулы являются теоремами.

Выше было показано, что для ИВ непротиворечивость и абсолютная непротиворечивость эквивалентны.

§4. Другие аксиоматические теории ИВ

4.1. Исчисление Гильберта–Аккермана

Примитивные связки: \neg, \vee , а $A \supset B$ — сокращение $\neg A \vee B$.

Схемы аксиом:

- (A1) $A \vee A \supset A$;
- (A2) $A \supset (A \vee B)$;
- (A3) $(A \vee B) \supset (B \vee A)$;
- (A4) $(B \supset C) \supset ((A \vee B) \supset (A \vee C))$.

Правило вывода: МР.

4.2. Исчисление Россера

Примитивные связки: \neg, \wedge , а $A \supset B$ — сокращение $\neg(A \wedge \neg B)$.

Схемы аксиом:

- (A1) $A \supset A \wedge A$;
- (A2) $A \wedge B \supset A$;
- (A3) $(A \supset B) \supset (\neg(B \wedge C) \supset \neg(C \wedge A))$.

Правило вывода: МР.

4.3. Исчисление секвенций

Примитивные связки: $\neg, \vee, \wedge, \supset$.

Специальный символ: \vdash .

Секвенциями называются слова следующих трёх видов, где A_1, A_2, \dots, A_n, B — произвольные формулы:

1. $A_1, A_2, \dots, A_n \vdash B$ (из A_1, A_2, \dots, A_n следует B_n);
2. $\vdash B$ (B доказуема);

3. $A_1, A_2, \dots, A_n \vdash$ (система A_1, A_2, \dots, A_n противоречива).

Схема аксиом: $A \vdash A$.

Правила вывода, где $\Gamma, \Gamma_1, \Gamma_2, \Gamma_3$ — произвольные конечные (может быть, пустые) последовательности формул, а A, B, C — произвольные формулы:

- 1) $\frac{\Gamma_1 \vdash A; \Gamma_2 \vdash B}{\Gamma_1, \Gamma_2 \vdash A \wedge B}$ (введение \wedge);
- 2) $\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$ (удаление \wedge);
- 3) $\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$ (удаление \wedge);
- 4) $\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$ (введение \vee);
- 5) $\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$ (введение \vee);
- 6) $\frac{\Gamma_1 \vdash A \vee B; \Gamma_2, A \vdash C; \Gamma_3, B \vdash C}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash C}$ (удаление \vee);
- 7) $\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$ (введение \supset);
- 8) $\frac{\Gamma_1 \vdash A; \Gamma_2 \vdash A \supset B}{\Gamma_1, \Gamma_2 \vdash B}$ (удаление \supset);
- 9) $\frac{\Gamma, A \vdash}{\Gamma \vdash \neg A}$ (введение \neg);
- 10) $\frac{\Gamma_1 \vdash A; \Gamma_2 \vdash \neg A}{\Gamma_1, \Gamma_2 \vdash}$ (сведение к противоречию);
- 11) $\frac{\Gamma, \neg A \vdash}{\Gamma \vdash A}$ (удаление \neg);
- 12) $\frac{\Gamma \vdash}{\Gamma \vdash A}$ (уточнение);
- 13) $\frac{\Gamma \vdash A}{\Gamma, B \vdash A}$ (расширение);
- 14) $\frac{\Gamma_1, A, B, \Gamma_2 \vdash C}{\Gamma_1, B, A, \Gamma_2 \vdash C}$ (перестановка);
- 15) $\frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C}$ (сокращение).

4.4. Исчисление Клини

Примитивные связки: $\neg, \wedge, \vee, \supset$.

Схемы аксиом:

- (A1) $A \supset (B \supset A)$;
- (A2) $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;
- (A3) $A \wedge B \supset A$;
- (A4) $A \wedge B \supset B$;
- (A5) $(A \supset B) \supset ((A \supset C) \supset (A \supset B \wedge C))$;
- (A6) $A \supset (A \vee B)$;
- (A7) $B \supset (A \vee B)$;

$$(A8) (A \supset C) \supset ((B \supset C) \supset ((A \vee B) \supset C));$$

$$(A9) (A \supset \neg B) \supset (B \supset \neg A);$$

$$(A10) \neg\neg A \supset A.$$

Правило вывода: МР.

II. Логика предикатов первого порядка

§1. Кванторы и формулы логики предикатов первого порядка

Логика предикатов первого порядка представляет собой обобщение логики высказываний на такие логические рассуждения, которые не могут быть формализованы средствами последней.

Классический пример: все люди смертны, Сократ — человек, следовательно, Сократ смертен.

Пусть $P(x)$ означает, что объект x обладает свойством P (P — *предикат*). Посредством $\forall xP(x)$ будем обозначать утверждение «для всякого x выполнено свойство P », $\exists xP(x)$ — утверждение «существует x , для которого выполнено свойство P ». Символ \forall называется *квантором всеобщности*, а \exists — *квантором существования*.

Пусть константный символ S означает Сократа, предикат $M(x)$ — « x смертен», $H(x)$ — « x — человек». Тогда приведённое выше рассуждение формализуется так:

$$\frac{\forall x(H(x) \supset M(x)), H(S)}{M(S)}.$$

Ещё пример: все боятся Дракулы, Дракула боится только меня, следовательно, я Дракула. D — Дракула, $A(x, y)$ — « x боится y », I — я, $E(x, y)$ — « x есть y ». Тогда указанное выше утверждение формализуется так:

$$\frac{\forall xA(x, D), \forall y(A(D, y) \supset E(y, I))}{E(I, D)}$$

Алфавит теории ИП включает следующие символы:

1. предметные (индивидные) переменные: x_1, x_2, \dots ;
2. предметные (индивидные) константы: a_1, a_2, \dots ;
3. предикатные буквы $A_1^1, A_1^2, \dots, A_1^j, \dots$;
4. функциональные буквы $f_1^1, f_1^2, \dots, f_1^j, \dots$;
5. пропозициональные связки \neg, \supset ;
6. квантор всеобщности \forall ;
7. квантор существования \exists ;
8. специальные символы $(,), ,$.

Верхний индекс предикатных и функциональных букв указывает число аргументов буквы, а нижний служит номером соответствующей буквы.

Определение. *Термом* называется слово в алфавите ИП, построенное по правилам:

1. Всякая предметная переменная или предметная константа — терм;
2. Если f_i^j есть функциональная буква, а t_1, t_2, \dots, t_j — термы, то $f_i^j(t_1, t_2, \dots, t_j)$ — терм;
3. Слово является термом тогда и только тогда, когда оно может быть получено по правилам 1, 2.

Определение. Слово в алфавите ИП называется *элементарной формулой*, если оно имеет такой и только такой вид: $A_i^n(t_1, t_2, \dots, t_n)$, где A_i^n — предикатный символ n -арности, а t_1, t_2, \dots, t_n — термы.

Определение. Формулой теории ИП называется слово в алфавите ИП построенное по правилам:

1. Всякая элементарная формула является формулой;
2. Если A и B — формулы, а y — предметная переменная, то $(\neg A)$, $(A \supset B)$, $(\forall y A)$ также являются формулами. В последнем случае формула A называется *областью действия квантора* \forall .
3. Слово является формулой тогда и только тогда, когда оно может быть получено по правилам 1, 2.

Замечание.

1. Связки \equiv , \wedge , \vee могут использоваться как сокращения по эквивалентностям

$$A \wedge B \iff \neg(A \supset \neg B);$$

$$A \vee B \iff \neg A \supset B;$$

$$A \equiv B \iff (A \supset B) \wedge (B \supset A).$$

2. Квантор \exists можно использовать для сокращения по эквивалентности $\exists x A \iff \neg(\forall x(\neg A))$.
3. Можно опускать лишние скобки по тем же правилам, что и в ИВ с учётом того, что кванторы по приоритету находятся между \supset и \vee (сильнее \supset , но слабее \vee).
4. Можно опускать скобки в (под)формулах вида $Q_1(Q_2(\dots Q_{n-1}(Q_n A) \dots))$, где Q_i , $i = 1, 2, \dots, n$, есть кванторы, то есть допустимо писать $Q_1 Q_2 \dots Q_{n-1} Q_n A$.

Определение. Вхождение переменной x в формулу называется *связанным*, если x — переменная входящего в эту формулу квантора $\forall x$ или находится в области действия входящего в эту формулу квантора $\forall x$. В противном случае вхождение переменной x в формулу называется *свободным*.

Определение. Переменная x называется *свободной* (*связанной*) в формуле, если существует хотя бы одно её свободное (связанное) вхождение в эту формулу.

Вполне возможно, что одна и та же переменная может быть как связанной, так и свободной в одной и той же формуле.

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

§2. Интерпретации и метод моделей

Определение. *Интерпретацией* называется непустое множество D (*область интерпретации*) и соответствие, относящее каждой предикатной букве A_i^n некоторое n -арное отношение в D , каждой функциональной букве f_i^n — некоторую n -местную функцию $D^n \rightarrow D$, каждой предметной константе — некоторый элемент D . Предметные переменные принимают значения в D , связки \neg , \supset и квантор \forall имеют обычный смысл.

При заданной интерпретации замкнутая формула переходит в истинное или ложное высказывание, формула со свободными переменными — в некоторое отношение на D , которое может быть выполнено для одних значений переменных из D и не выполнено для других.

Определение. Формула называется *истинной в данной интерпретации*, если она *выполнена* для всех элементов из D .

Определение. Формула называется *ложной в данной интерпретации*, если она *не выполнена* ни для одного элемента из D .

Определение. Интерпретация называется *моделью* для множество формул Γ , если каждая формула из Γ истинна в ней.

Определение. Формула называется *логически общезначимой*, если она истинна в любой интерпретации.

Логически общезначимые формулы также называются *логическими законами*.

Определение. Формула A называется *противоречием*, если $\neg A$ логически общезначима.

Определение. Формула называется *выполнимой*, если существует интерпретация, в которой она выполнена хотя бы на одном подмножестве элементов из D .

Метод моделей установления общезначимости (противоречивости, выполнимости) формула заключается в подборе моделей (интерпретаций) или доказательстве общезначимости (противоречивости) с помощью интерпретаций.

§3. Теории первого порядка

Для построения теории используем введённый в §1. алфавит. При этом положим, что множества предикатных букв и предметных переменных не пусты, множества функциональных символов и предметных констант могут быть пустыми.

Термы, элементарные формулы и формулы определяются так же.

Определение. Терм t называется *свободным для переменной* x_i в формуле A , если никакое свободное вхождение x_i в A не лежит в области действия никакого квантора $\forall x_j$, где x_j — переменная, входящая в терм t .

Аксиомами теории будут следующие формулы:

$$(A1) \ A \supset (B \supset A);$$

$$(A2) \ (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C));$$

$$(A3) \ (\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B);$$

$$(A4) \ \forall x_i A(x_i) \supset A(t), \text{ где } t \text{ — терм, свободный для } x_i \text{ в формуле } A(x_i), \text{ а } A(t) \text{ — формула, в которой все вхождения переменной } x_i \text{ заменены на } t;$$

$$(A5) \ \forall x_i (A \supset B) \supset (A \supset \forall x_i B), \text{ где } A \text{ не содержит свободные вхождения переменной } x_i.$$

Различные конкретные теории исчисления предикатов могут содержать ещё аксиомы в дополнение к приведённым выше (*собственные аксиомы*). Теория первого порядка без собственных аксиом называется *исчислением предикатов первого порядка (ИП)*.

Первый порядок в названии выражается в том, что в предикаты можно подставлять исключительно термы, определённые в §1., а в кванторах могут записываться только индивидуальные переменные. В теориях более высокого порядка допускается взятие кванторов по предикатным символам, а так же подстановка в предикаты других предикатов.

Правила вывода:

1) МР

$$\frac{A, A \supset B}{B};$$

2) обобщение (Gen)

$$\frac{A}{\forall x_i A}.$$

Лемма 3.1. Если формула A произвольной теории первого порядка T есть частный случай тавтологии, то A есть теорема T и может быть выведена с применением одних только схем аксиом $A1, A2, A3$ и правила МР.

§4. Теорема дедукции в теории ИП

Теорема дедукции для пропозиционального ИВ не может быть перенесена без изменений на произвольные теории первого порядка. Однако некоторая ослабленная форма теоремы может быть доказана для них.

Пример: $A(x) \vdash \forall x A(x)$. Вывод состоит в применении к $A(x)$ правила Gen:

1. $A(x)$ (гипотеза);
2. $\forall x A(x)$ (из 1 по Gen).

Рассмотрим теперь интерпретацию $D = \{a, b\}$. Предикат A возьмём таким, что $A(a)$ истинно, а $A(b)$ ложно. Тогда формула $A(x) \supset \forall x A(x)$ не является верной, если положить свободную переменную $x = a$. Действительно, ясно, что $\forall x A(x)$ ложно, а с другой стороны, взяв значение свободной переменной $x = a$, получим, что посылка импликации будет истинной ($A(a)$ истинно), что влечёт ложность импликации.

Пусть A — формула из множества формул Γ , а B_1, B_2, \dots, B_n — некоторый вывод из Γ . Будем говорить, что формула B_i *зависит от A в этом выводе*, если для этой формулы выполнено какое-нибудь из условий:

1. формула B_i есть A ;
2. формула B_i есть непосредственное следствие по одному из правил вывода некоторых предшествующих в этом выводе формул, из которых хотя бы одна зависит от A .

Лемма 4.1. Если формула B не зависит от формулы A в выводе $\Gamma, A \vdash B$, то $\Gamma \vdash B$.

Доказательство. Пусть V_1, V_2, \dots, V_n — произвольный вывод V из $\Gamma \cup \{A\}$, в котором V независит от A . Ясно, что V_n совпадает с V .

Докажем по индукции по $n \in \mathbb{N}$ (то есть по длине вывода), что $\Gamma \vdash V_n$, то есть $\Gamma \vdash V$. Так мы докажем, что утверждение леммы верно, каков бы ни был вывод $\Gamma, A \vdash V$.

База: $n = 1$. Вывод состоит всего из одной формулы — формулы V . Ясно, что V в таком случае не совпадает с A , поскольку в противном случае имела бы место зависимость V от A , противоречащая условию леммы. В таком случае очевидно, что написанный вывод, состоящий из одной формулы, по совместительству является ещё и выводом $\Gamma \vdash V$, что доказывает базу индукции.

Индукционное предположение: пусть утверждение доказано для всех выводов $\Gamma, A \vdash V$ всех длин $k \leq n - 1$.

Индукционный шаг: докажем, что утверждение будет верно для вывода и длины n . Очевидно, что утверждение леммы будет верным, если окажется, что V входит в Γ или является одной из аксиом. Пусть теперь V_n в нашем произвольном выводе получено из каких-то предшествующих формул V_i и V_j ($i, j < n$) по одному из двух правил вывода. Ясно, что поскольку V_n (то есть V) не зависит от A , то ни одна из формул V_i и V_j не зависит от A . Тогда согласно индукционному предположению и произвольности формулы V в формулировке леммы, получаем, что имеют место выводы $\Gamma \vdash V_i$ и $\Gamma \vdash V_j$. Тогда по правилу сечения извлекаем искомым вывод: $\Gamma \vdash V_n$. ■

Теорема 4.1 (дедукция в ИП). Пусть $\Gamma, A \vdash V$ и существует вывод V из $\Gamma \cup \{A\}$, в котором ни при каком применении правила Gen к формулам, зависящим в этом выводе от A , не связывается квантором никакая свободная переменная формулы A . Тогда $\Gamma \vdash A \supset V$.

Следствие 1. Если $\Gamma, A \vdash V$ и существует вывод V из Γ, A , построенный без применения правила Gen к свободным переменным формулы A , то $\Gamma \vdash A \supset V$.

Следствие 2. Если формула A замкнута и $\Gamma, A \vdash V$, то $\Gamma \vdash A \supset V$.