Математическая логика, 2022

V. G.

Содержание

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.

1.2. Пропозициональные связки

Сложные высказывания строятся как истинностно-функциональные комбинации простых высказываний.

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

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 $\neg$, $\wedge$, $\vee$, $\supset$, $\equiv$.

1.3. Формулы алгебры высказываний

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

1. строчных латинских букв $a, b, c, \ldots, a_1, a_2, \ldots$ — *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

1.4. 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 $a_1, a_2, \ldots, a_n$, формула B получена подстановкой в A формул $A_1, A_2, \ldots, A_n$ вместо всех вхождений букв $a_1, a_2, \ldots, a_n$ 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 $A_1, A_2, \ldots, A_n$ истинностные значения $\alpha_1, \alpha_2, \ldots, \alpha_n$ соответственно. Присвоим буквам $a_1, a_2, \ldots, a_n$ формулы A истинностные значения $\alpha_1, \alpha_2, \ldots, \alpha_n$ 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 $\Gamma = \varnothing$, 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 $\mathsf{A}, \mathsf{B}, \mathsf{C}, \dots, \mathsf{A}_1, \mathsf{A}_2, \dots$;
2. пропозициональные связки $\neg, \supset$;
3. специальные символы (,).

Формулы теории определяются рекуррентно по правилам:

1. Любая пропозициональная буква есть формула.
2. Если $\mathcal{A}$, $\mathcal{B}$ есть формулы, то слова $(\neg\mathcal{A})$, $(\mathcal{A} \supset \mathcal{B})$ 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. 1.3.).

Аксиомы теории:

(A1) $\mathsf{A} \supset (\mathsf{B} \supset \mathsf{A})$;

(A2) $\Big(\mathsf{A} \supset (\mathsf{B} \supset \mathsf{C})\Big) \supset \Big((\mathsf{A} \supset \mathsf{B}) \supset (\mathsf{A} \supset \mathsf{C})\Big)$;

(A3) $(\neg\mathsf{B} \supset \neg\mathsf{A}) \supset \Big((\neg\mathsf{B} \supset \mathsf{A}) \supset \mathsf{B}\Big)$.

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

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

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:

- $\mathsf{A} \wedge \mathsf{B} \iff \neg(\mathsf{A} \supset \neg\mathsf{B})$;
- $\mathsf{A} \vee \mathsf{B} \iff \neg\mathsf{A} \supset \mathsf{B}$;
- $\mathsf{A} \equiv \mathsf{B} \iff (\mathsf{A} \supset \mathsf{B}) \wedge (\mathsf{B} \supset \mathsf{A})$.

3.2. Доказательства в исчислении высказываний

Лемма 3.1. $\vdash \mathsf{A} \supset \mathsf{A}$.

Доказательство.

1. $\Big(\mathsf{A} \supset \big((\mathsf{A} \supset \mathsf{A}) \supset \mathsf{A}\big)\Big) \supset \Big(\big(\mathsf{A} \supset (\mathsf{A} \supset \mathsf{A})\big) \supset (\mathsf{A} \supset \mathsf{A})\Big)$ (A2);
2. $\mathsf{A} \supset \big((\mathsf{A} \supset \mathsf{A}) \supset \mathsf{A}\big)$ (A1);
3. $\big(\mathsf{A} \supset (\mathsf{A} \supset \mathsf{A})\big) \supset (\mathsf{A} \supset \mathsf{A})$ (из 1, 2 по MP);
4. $\mathsf{A} \supset (\mathsf{A} \supset \mathsf{A})$ (A1);
5. $\mathsf{A} \supset \mathsf{A}$ (из 3, 4 по MP).

$\square$

Лемма 3.2. $\vdash (\neg\mathsf{A} \supset \mathsf{A}) \supset \mathsf{A}$.

Доказательство.

1. $\neg\mathsf{A} \supset \neg\mathsf{A}$ (лемма 3.1);

2. $(\neg A \supset \neg A) \supset \big((\neg A \supset A) \supset A\big)$ (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.

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

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

$A \supset (B \supset (A \supset B))$ (из 1, 2 по MP). □

Лемма 3.5.

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

Лемма 3.6.

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

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

□

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. Доказательство первого:

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. $(\neg A \supset \neg\neg A) \supset A$ (леммы);
4. $\neg\neg A \supset (\neg A \supset \neg\neg A)$ (A1);
5. $\neg\neg A \supset A$ (3, 4 по лемма 3.3).

□

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 $B_1, \ldots, B_n$ — вывод $\Gamma, A \vdash B$. Тогда B_n совпадает с B.

Доказываем индукцией по $i = 1, \ldots, n$, что $\Gamma \vdash A \supset B_i$. Тогда при $i = n$ получаем утверждение теоремы.

База: $i = 1$. То есть имеет место $\Gamma \vdash A \supset B_1$. Тогда 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. Если B_1 есть аксиома, то тогда, написав аксиому $B_1 \supset (A \supset B_1)$, по MP получаем вывод $A \supset B_1$.

Индукционное предположение: Пусть $\Gamma \vdash A \supset B_i$ для всех $i = 1, \ldots, m-1$.

Индукционный шаг: Докажем $\Gamma \vdash A \supset B_m$. Тогда либо B_m — аксиома, либо B_m совпадает с A, либо входит в Γ, либо выводится из каких-то предыдущих формул B_r, B_q по MP, $r, q < m$. Проверка первых трёх случаев дословно повторяет проверку в базе индукции. Пусть $r < q$. Тогда B_q имеет вид $B_r \supset B_m$. По предположению индукции $\Gamma \vdash A \supset B_r$ и $\Gamma \vdash A \supset B_q$ или $\Gamma \vdash A \supset (B_r \supset B_m)$. Запишем аксиому A2: $(A \supset (\underbrace{B_r \supset B_m}_{B_q})) \supset ((A \supset B_r) \supset (A \supset B_m))$.

Дважды применяя MP (написанная аксиома и $A \supset B_q$, а затем $A \supset B_r$ и $(A \supset B_r) \supset (A \supset B_m)$), получаем искомую импликацию $A \supset B_m$.

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