

Математическая логика и теория вычислимости

Лекция 3. Исчисление высказываний гильбертовского типа

Денис Николаевич Москвин

Кафедра математических и информационных технологий
Санкт-Петербургского академического университета

27.02.2017

- 1 Классическое исчисление высказываний
- 2 Правила естественного вывода
- 3 Полнота исчисления высказываний

- 1 Классическое исчисление высказываний
- 2 Правила естественного вывода
- 3 Полнота исчисления высказываний

- Говорят, что задано *исчисление* (или *формальная теория*) если определены:
 - правила построения формул;
 - *аксиомы* (или *схемы аксиом*), то есть формулы, которые считаются заведомо верными;
 - *правила вывода*, то есть правила, по которым из набора формул мы можем вывести новую формулу.
- Правила вывода обычно записывают в виде

$$\frac{A_1 \dots A_n}{A}$$

Элементы набора $A_1 \dots A_n$ называют *посылками*, а A — *заключением*.

- *Выводом* в некотором исчислении называется конечная последовательность формул, каждая из которых
 - является аксиомой;
 - получается из предыдущих по правилам вывода.
- Формула называется *выводимой* в исчислении (*теоремой* исчисления), если существует вывод, в котором эта формула является последней.
- Часто для удобства анализа аксиомы именуют, а формулы в последовательности нумеруют.

- В качестве формул берут пропозициональные формулы.
- Схемы аксиом:
 - 1 $A \rightarrow B \rightarrow A$
 - 2 $(A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$
 - 3 $A \wedge B \rightarrow A$
 - 4 $A \wedge B \rightarrow B$
 - 5 $A \rightarrow B \rightarrow A \wedge B$
 - 6 $A \rightarrow A \vee B$
 - 7 $B \rightarrow A \vee B$
 - 8 $(A \rightarrow C) \rightarrow (B \rightarrow C) \rightarrow A \vee B \rightarrow C$
 - 9 $\neg A \rightarrow A \rightarrow B$
 - 10 $(A \rightarrow B) \rightarrow (A \rightarrow \neg B) \rightarrow \neg A$
 - 11 $A \vee \neg A$
- Правило вывода (modus ponens, MP)

$$\frac{A \quad A \rightarrow B}{B}$$

Примеры вывода в исчислении высказываний

Пример вывода

- 1 $p \rightarrow q \rightarrow p$ (A1)
- 2 $(p \rightarrow q \rightarrow p) \rightarrow (p \rightarrow q) \rightarrow p \rightarrow p$ (A2)
- 3 $(p \rightarrow q) \rightarrow p \rightarrow p$ MP(1)(2)

Пример схемы вывода. Возьмем произвольную формулу A :

- 1 $A \rightarrow (A \rightarrow A) \rightarrow A$ (A1)
- 2 $(A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow (A \rightarrow (A \rightarrow A)) \rightarrow A \rightarrow A$ (A2)
- 3 $(A \rightarrow A \rightarrow A) \rightarrow A \rightarrow A$ MP(1)(2)
- 4 $A \rightarrow A \rightarrow A$ (A1)
- 5 $A \rightarrow A$ MP(4)(3)

Получили первую полезную теорему исчисления высказываний

$$A \rightarrow A$$

Теорема (корректность исчисления высказываний).

Всякая теорема исчисления высказываний есть тавтология.

Доказательство.

- Аксиомы являются тавтологиями (доказывается прямой проверкой).
- Правило MP тоже корректно: если A и $A \rightarrow B$ всегда истинны, то B тоже всегда истинно.



Выполнено ли для исчисления высказываний свойство полноты?

- Пусть имеется множество формул

$$\Gamma = A_1, \dots, A_n$$

- *Выводом из множества формул Γ* называется конечная последовательность формул, каждая из которых
 - является аксиомой;
 - принадлежит множеству формул Γ ;
 - получается из предыдущих по правилам вывода.
- Нотация для формулы A выводимой из Γ :

$$\Gamma \vdash A$$

- Нотация для расширения множества Γ формулой A :

$$\Gamma, A$$

- Очевидно, что расширение не «ухудшает» выводимость.

Лемма о дедукции. $\Gamma \vdash A \rightarrow B$ тогда и только тогда, когда $\Gamma, A \vdash B$.

Доказательство.

- Пусть $\Gamma \vdash A \rightarrow B$. Тогда и $\Gamma, A \vdash A \rightarrow B$, откуда из $\Gamma, A \vdash A$ по МР получаем искомый результат.
- Пусть $\Gamma, A \vdash B$. Рассмотрим вывод формулы B — последовательность формул

$$C_1, C_2, \dots, C_n$$

где C_n это B .

C_i может быть: (1) A , (2) из Γ , (3) аксиомой, (4) результатом применения МР к двум предыдущим C_k и $C_k \rightarrow C_i$.

Лемма о дедукции (продолжение доказательства)

Припишем ко всем формулам вывода посылку A

$$A \rightarrow C_1, A \rightarrow C_2, \dots, A \rightarrow C_n$$

и покажем, что эту цепочку можно расширить до вывода.

(1). $C_i = A$, в новой цепочке это будет $A \rightarrow A$, это выводимое утверждение, добавляем его вывод.

(2). $C_i \in \Gamma$. Вставляем C_i и $C_i \rightarrow A \rightarrow C_i$ (A1), MP даст искомое $A \rightarrow C_i$.

(3). C_i — аксиома. Аналогично.

(4). C_i выводится по MP из предыдущих C_k и $C_k \rightarrow C_i$. То есть новой цепочке имеются $A \rightarrow C_k$ и $A \rightarrow C_k \rightarrow C_i$.

Вставляем формулы

$$\begin{array}{ll} (A \rightarrow C_k \rightarrow C_i) \rightarrow (A \rightarrow C_k) \rightarrow A \rightarrow C_i & \text{(A2)} \\ (A \rightarrow C_k) \rightarrow A \rightarrow C_i & \text{MP} \\ A \rightarrow C_i & \text{MP} \end{array}$$



Лемма о дедукции: пример

- Доказать, что $\vdash (A \rightarrow B) \rightarrow (B \rightarrow C) \rightarrow A \rightarrow C$.
- Доказательство.** $A \rightarrow B, B \rightarrow C, A \vdash C$. Действительно

1	$A \rightarrow B, B \rightarrow C, A \vdash A$	
2	$A \rightarrow B, B \rightarrow C, A \vdash A \rightarrow B$	
3	$A \rightarrow B, B \rightarrow C, A \vdash B$	MP(1)(2)
4	$A \rightarrow B, B \rightarrow C, A \vdash B \rightarrow C$	
5	$A \rightarrow B, B \rightarrow C, A \vdash C$	MP(3)(4)

Применяем трижды лемму о дедукции

$A \rightarrow B, B \rightarrow C, A$	$\vdash C$
$A \rightarrow B, B \rightarrow C$	$\vdash A \rightarrow C$
$A \rightarrow B$	$\vdash (B \rightarrow C) \rightarrow A \rightarrow C$
	$\vdash (A \rightarrow B) \rightarrow (B \rightarrow C) \rightarrow A \rightarrow C$

Теорема. (Правило сечения.) Если $\Gamma \vdash A$ и $\Delta, A \vdash B$, то $\Gamma, \Delta \vdash B$.

Доказательство. Расширяем первое до $\Gamma, \Delta \vdash A$. Расширяем второе до $\Gamma, \Delta, A \vdash B$, затем ко второму применяем лемму о дедукции, получая $\Gamma, \Delta \vdash A \rightarrow B$. Искомый результат получается с помощью MP. ■

- 1 Классическое исчисление высказываний
- 2 Правила естественного вывода
- 3 Полнота исчисления высказываний

Правило введения импликации

- Вывод на основании одного лишь правила MP не очень удобен.
- Можно сформулировать дополнительные правила вывода и показать, что они *допустимы* в исчислении высказываний.
- Лемма о дедукции порождает *правило введения импликации*:

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \quad (\rightarrow \text{intro})$$

- Из MP можно получить *правило удаления импликации*

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A \rightarrow B}{\Gamma \vdash B} \quad (\rightarrow \text{elim})$$

Правило введения и удаления конъюнкции

- Аксиомы исчисления высказываний 3, 4 и 5 имеют вид
 - $A \wedge B \rightarrow A$
 - $A \wedge B \rightarrow B$
 - $A \rightarrow B \rightarrow A \wedge B$
- Из последней легко получить *правило введения конъюнкции*

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \quad (\wedge\text{intro})$$

$$1 \quad \Gamma \vdash A$$

$$2 \quad \Gamma \vdash B$$

$$3 \quad \Gamma \vdash A \rightarrow B \rightarrow A \wedge B \quad A5$$

$$4 \quad \Gamma \vdash B \rightarrow A \wedge B \quad \text{MP}(1)(3)$$

$$5 \quad \Gamma \vdash A \wedge B \quad \text{MP}(2)(4)$$

- Из аксиом 3 и 4 имеем *правила удаления конъюнкции*

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad (\wedge\text{elimI})$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \quad (\wedge\text{elimII})$$

- Доказать

$$\vdash (A \rightarrow B \rightarrow C) \rightarrow A \wedge B \rightarrow C$$

- Доказательство:

1	$A \rightarrow B \rightarrow C, A \wedge B \vdash A \wedge B$	
2	$A \rightarrow B \rightarrow C, A \wedge B \vdash A$	$\wedge\text{elimI (1)}$
3	$A \rightarrow B \rightarrow C, A \wedge B \vdash A \rightarrow B \rightarrow C$	
4	$A \rightarrow B \rightarrow C, A \wedge B \vdash B \rightarrow C$	MP(2)(3)
5	$A \rightarrow B \rightarrow C, A \wedge B \vdash B$	$\wedge\text{elimII (1)}$
6	$A \rightarrow B \rightarrow C, A \wedge B \vdash C$	MP(5)(4)
7	$A \rightarrow B \rightarrow C \vdash A \wedge B \rightarrow C$	$\rightarrow\text{intro (6)}$
8	$\vdash (A \rightarrow B \rightarrow C) \rightarrow A \wedge B \rightarrow C$	$\rightarrow\text{intro (7)}$

Правило введения и удаления дизъюнкции

- Аксиомы исчисления высказываний 6, 7 и 8 имеют вид
 - $A \rightarrow A \vee B$
 - $B \rightarrow A \vee B$
 - $(A \rightarrow C) \rightarrow (B \rightarrow C) \rightarrow A \vee B \rightarrow C$
- Из аксиом 6 и 7 имеем *правила введения дизъюнкции*

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \quad (\vee\text{introI}) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \quad (\vee\text{introII})$$

- Из аксиомы 8 имеем *правило разбора случаев*

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \quad (\text{case analysis})$$

откуда можно получить *правило удаления дизъюнкции*

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \quad (\vee\text{elim})$$

- Доказать

$$\vdash (A \vee B \rightarrow C) \rightarrow (A \rightarrow C) \wedge (B \rightarrow C)$$

- Доказательство:

- | | | |
|----|--|--------------------------------|
| 1 | $A \vee B \rightarrow C, A \vdash A$ | |
| 2 | $A \vee B \rightarrow C, A \vdash A \vee B$ | $\vee\text{introI (1)}$ |
| 3 | $A \vee B \rightarrow C, A \vdash A \vee B \rightarrow C$ | |
| 4 | $A \vee B \rightarrow C, A \vdash C$ | MP(2)(3) |
| 5 | $A \vee B \rightarrow C \vdash A \rightarrow C$ | $\rightarrow\text{intro (4)}$ |
| 6 | $A \vee B \rightarrow C, B \vdash B$ | |
| 7 | $A \vee B \rightarrow C, B \vdash A \vee B$ | $\vee\text{introII (6)}$ |
| 8 | $A \vee B \rightarrow C, B \vdash A \vee B \rightarrow C$ | |
| 9 | $A \vee B \rightarrow C, B \vdash C$ | MP(7)(8) |
| 10 | $A \vee B \rightarrow C \vdash B \rightarrow C$ | $\rightarrow\text{intro (9)}$ |
| 11 | $A \vee B \rightarrow C \vdash (A \rightarrow C) \wedge (B \rightarrow C)$ | $\wedge\text{intro (5)(10)}$ |
| 12 | $\vdash (A \vee B \rightarrow C) \rightarrow (A \rightarrow C) \wedge (B \rightarrow C)$ | $\rightarrow\text{intro (11)}$ |

- Аксиомы исчисления высказываний 9 и 10 имеют вид
 - $\neg A \rightarrow A \rightarrow B$
 - $(A \rightarrow B) \rightarrow (A \rightarrow \neg B) \rightarrow \neg A$
- Аксиома 9 позволяет вывести все что угодно из противоречивых посылок

$$\frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash B} \quad (\neg\text{-elim})$$

- Аксиома 10 описывает, как можно ввести отрицание

$$\frac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A} \quad (\neg\text{-intro})$$

- Доказать закон контрапозиции

$$\vdash (A \rightarrow B) \rightarrow \neg B \rightarrow \neg A$$

- Доказательство:

1	$A \rightarrow B, \neg B, A \vdash \neg B$	
2	$A \rightarrow B, \neg B, A \vdash A$	
3	$A \rightarrow B, \neg B, A \vdash A \rightarrow B$	
4	$A \rightarrow B, \neg B, A \vdash B$	MP(2)(3)
5	$A \rightarrow B, \neg B \vdash \neg A$	\neg -intro (1)(4)

- Общая идея: если формула кончается на $\neg C$, добавить C к посылкам и попытаться вывести два противоречивых результата.

Закон исключенного третьего

- Аксиома исчисления высказываний 11 имеет вид $A \vee \neg A$ и называется “*законом исключенного третьего*” (tertium non datur).
- Из нее можно вывести “*закон снятия двойного отрицания*”

$$\neg\neg A \rightarrow A$$

- Действительно

1	$A, \neg\neg A \vdash A$	
2	$\neg A, \neg\neg A \vdash A$	$\neg\text{-elim}$
3	$A \vee \neg A, \neg\neg A \vdash A$	case analysis (1)(2)
4	$A \vee \neg A \vdash \neg\neg A \rightarrow A$	$\rightarrow\text{-intro}(3)$

- Можно ли в предыдущем примере

$$A \vee \neg A \vdash \neg\neg A \rightarrow A$$

убрать аксиому слева от \vdash ?

- Можно ли в предыдущем примере

$$A \vee \neg A \vdash \neg\neg A \rightarrow A$$

убрать аксиому слева от \vdash ?

- Да, и это верно для любой аксиомы

$$\begin{array}{l} 1 \quad \Gamma, Ax \vdash B \\ 2 \quad \Gamma \vdash Ax \rightarrow B \quad \rightarrow \text{intro}(3) \\ 3 \quad \Gamma \vdash Ax \\ 4 \quad \Gamma \vdash B \quad \rightarrow \text{elim}(3)(2) \end{array}$$

- После доказательства полноты исчисления этим же методом можно будет убирать слева любую тавтологию.

- 1 Классическое исчисление высказываний
- 2 Правила естественного вывода
- 3 Полнота исчисления высказываний

Вспомогательные факты (1)

Лемма 1. Для любых формул A и B верны теоремы:

$$\begin{array}{lll} \neg A, \neg B \vdash \neg(A \wedge B) & \neg A, \neg B \vdash \neg(A \vee B) & \neg A, \neg B \vdash A \rightarrow B \\ \neg A, B \vdash \neg(A \wedge B) & \neg A, B \vdash A \vee B & \neg A, B \vdash A \rightarrow B \\ A, \neg B \vdash \neg(A \wedge B) & A, \neg B \vdash A \vee B & A, \neg B \vdash \neg(A \rightarrow B) \\ A, B \vdash A \wedge B & A, B \vdash A \vee B & A, B \vdash A \rightarrow B \end{array}$$

$$\neg A \vdash \neg A$$

$$A \vdash \neg\neg A$$

Доказательство. Несложный вывод. ■

Вспомогательные факты (2)

Лемма 2. Пусть B — формула, содержащая n переменных p_1, p_2, \dots, p_n . Тогда для каждой строки ее таблицы истинности

p_1	p_2	\dots	p_n	B
\dots	\dots	\dots	\dots	\dots
α_1	α_2	\dots	α_n	β
\dots	\dots	\dots	\dots	\dots

можно построить выводы

$$L_1, L_2, \dots, L_n \vdash B'$$

где

$$L_i = \begin{cases} p_i, & \alpha_i = 1, \\ \neg p_i, & \alpha_i = 0, \end{cases} \quad B' = \begin{cases} B, & \beta = 1, \\ \neg B, & \beta = 0. \end{cases}$$

Доказательство. Индукция по построению формулы с использованием Леммы 1. ■

Теорема (о полноте исчисления высказываний). Любая тавтология пропозициональной логики выводима в исчислении высказываний.

Доказательство. Пусть формула B — тавтология. Тогда для любого из 2^n наборов литералов выводится B , а не $\neg B$:

$$L_1, L_2, \dots, L_n \vdash B$$

Выберем переменную, например, p_n . Имеем

- 1 $L_1, \dots, L_{n-1}, p_n \vdash B$
- 2 $L_1, \dots, L_{n-1}, \neg p_n \vdash B$
- 3 $L_1, \dots, L_{n-1} \vdash p_n \vee \neg p_n$ (A11)
- 4 $L_1, \dots, L_{n-1} \vdash B$ $\vee\text{elim}(3)(1)(2)$
- ...
- $\vdash B$



- Множество формул Γ называют *совместным*, если существует такой набор значений переменных, на которых все формулы из Γ истинны. (Другой эквивалентный термин — множество формул *имеет модель*.)
- Множество формул Γ называют *противоречивым*, если из него одновременно можно вывести формулы A и $\neg A$. (В противном случае это множество формул *непротиворечиво*.)
- Если множество формул противоречиво, то, используя $\neg\text{elim}$, из него можно вывести любую формулу.

- **Теорема.** Всякое совместное множество формул Γ непротиворечиво.
- **Доказательство.** Пусть оно противоречиво, тогда из него выводится некоторая A и $\neg A$. Фиксируем набор переменных, обеспечивающий совместность. На этом наборе все формулы из Γ истинны, тогда A тоже должна быть истинна¹, как и $\neg A$. Противоречие. ■
- **Теорема.** Исчисление высказываний корректно.
- **Доказательство.** Если A — теорема исчисления высказываний, то множество $\{\neg A\}$ — противоречиво:

$$\neg A \vdash \neg A$$

$$\neg A \vdash A$$

Тогда оно несовместно, то есть $\neg A$ ложна на всех значениях переменных, а значит A — тавтология. ■

¹Индукцией по структуре вывода.

- Множество формул Γ называют *полным*, если для любой формулы A имеет место либо $\Gamma \vdash A$, либо $\Gamma \vdash \neg A$.
- **Лемма 1.** Всякое непротиворечивое множество Γ содержится в непротиворечивом полном множестве Δ .
- **Доказательство.** Пусть A произвольная формула. Рассмотрим Γ, A и $\Gamma, \neg A$. Одно из них непротиворечиво. Действительно, если противоречивы оба, то по \neg -intro $\Gamma \vdash \neg A$ и $\Gamma \vdash \neg\neg A$, что противоречит непротиворечивости Γ . Будем теперь перебирать все допустимые формулы, добавляя к Γ либо формулу, либо отрицание, сохраняя непротиворечивость. ■

- **Лемма 2.** Всякое непротиворечивое полное множество Δ совместно.

- **Доказательство.**

Из непротиворечивости и полноты следует, что для любой переменной p в Δ входит ровно одно: либо p , либо $\neg p$. Это формирует набор ν «выполняющих» значений переменных (модель):

$$\begin{aligned}\Delta \vdash p &\Rightarrow \nu : p \mapsto 1 \\ \Delta \vdash \neg p &\Rightarrow \nu : p \mapsto 0\end{aligned}$$

Индукцией по построению формулы A доказываем

$$\begin{aligned}A(\nu) = 1 &\Rightarrow \Delta \vdash A \\ A(\nu) = 0 &\Rightarrow \Delta \vdash \neg A\end{aligned}$$

База: Если формула A — переменная, то очевидно.

Шаг: делаем стандартный перебор связок

(самостоятельно). ■

- **Теорема.** Всякое непротиворечивое множество Γ совместно.
- **Доказательство.** Непосредственно из Лемм 1 и 2. ■
- **Теорема (о полноте).** Всякая тавтология есть теорема.
Доказательство. Пусть A — тавтология, тогда $\{\neg A\}$ несовместно, тогда из $\neg A$ выводится противоречие, тогда $\vdash \neg\neg A$, тогда $\vdash A$. ■

- **Теорема (о компактности для исчисления высказываний).** Множество формул, у которого всякое конечное подмножество совместно, само является совместным.
- **Доказательство.** Несовместность равносильна противоречивости, а вывод противоречия всегда конечен (как любой вывод). ■