Математическая логика и теория вычислимости Лекция 3. Исчисление высказываний гильбертовского типа

Денис Николаевич Москвин

Совместная магистратура JetBrains и ИТМО
Разработка ПО / Software Engineering

19.02.2020

План лекции

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

План лекции

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

Понятие исчисления

- 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

$$\frac{A_1 \quad \ldots \quad A_n}{A}$$

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

Понятие вывода

- *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.

Классическое исчисление высказываний

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

$$\frac{A \qquad A \to B}{B}$$

Пример вывода

$$\begin{array}{lll} 1 & p \to q \to p & (A1) \\ 2 & (p \to q \to p) \to (p \to q) \to p \to p & (A2) \\ 3 & (p \to q) \to p \to p & MP(1)(2) \end{array}$$

Пример схемы вывода. Возьмем произвольную формулу A:

$$\begin{array}{lll} 1 & A \to (A \to A) \to A & (A1) \\ 2 & (A \to (A \to A) \to A) \to (A \to (A \to A)) \to A \to A & (A2) \\ 3 & (A \to A \to A) \to A \to A & MP(1)(2) \\ 4 & A \to A \to A & (A1) \\ 5 & A \to A & MP(4)(3) \end{array}$$

Получили первую полезную теорему исчисления высказываний

$$A \to A$$

Корректность исчисления высказываний

Теорема (soundness). Всякая теорема исчисления высказываний есть тавтология.

Доказательство.

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

■

Выполнено ли для исчисления высказываний свойство полноты (completeness)?

Вывод из формул

- Пусть имеется множество формул

$$\Gamma = A_1, \ldots, A_n$$

- *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. $\Gamma \vdash A \to B$ тогда и только тогда, когда $\Gamma, A \vdash B$.

Доказательство.

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

$$C_1, C_2, \ldots, C_n$$

где C_n это B.
C_i может быть: (1) A, (2) из Γ, (3) аксиомой, (4) результатом применения MP к двум предыдущим C_k и $C_k \to C_i$.

Лемма о дедукции (продолжение доказательства)

Припишем ко всем формулам вывода посылку A

$$A \to C_1, A \to C_2, \ldots, A \to C_n$$

и покажем, что эту цепочку можно расширить до вывода.
(1). $C_i = A$, в новой цепочке это будет $A \to A$, это выводимое утверждение, добавляем его вывод.
(2). $C_i \in \Gamma$. Вставляем C_i и $C_i \to A \to C_i$ (A1), MP даст искомое $A \to C_i$.
(3). C_i — аксиома. Аналогично.
(4). C_i выводится по MP из предыдущих C_k и $C_k \to C_i$. То есть новой цепочке имеются $A \to C_k$ и $A \to C_k \to C_i$.
Вставляем формулы

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

■

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

$$
\begin{array}{lll}
1 & A \to B, B \to C, A \vdash A & \\
2 & A \to B, B \to C, A \vdash A \to B & \\
3 & A \to B, B \to C, A \vdash B & MP(1)(2) \\
4 & A \to B, B \to C, A \vdash B \to C & \\
5 & A \to B, B \to C, A \vdash C & MP(3)(4)
\end{array}
$$

Применяем трижды лемму о дедукции

$$
\begin{array}{lcl}
A \to B, B \to C, A & \vdash & C \\
A \to B, B \to C & \vdash & A \to C \\
A \to B & \vdash & (B \to C) \to A \to C \\
 & \vdash & (A \to B) \to (B \to C) \to A \to C
\end{array}
$$

Правило сечения

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 $\Gamma, \Delta \vdash A \to B$. Искомый результат получается с помощью MP. ∎

План лекции

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* (admissible $\approx$ derivable) в исчислении высказываний.
- Лемма о дедукции порождает *правило введения импликации*:
$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \quad (\to \text{intro})$$
- Из MP можно получить *правило удаления импликации*
$$\frac{\Gamma \vdash A \qquad \Gamma \vdash A \to B}{\Gamma \vdash B} \quad (\to \text{elim})$$

Правило введения и удаления конъюнкции

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

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

$$\begin{array}{lll} 1 & \Gamma \vdash A & \\ 2 & \Gamma \vdash B & \\ 3 & \Gamma \vdash A \to B \to A \wedge B & \mathrm{A5} \\ 4 & \Gamma \vdash B \to A \wedge B & \mathrm{MP}(1)(3) \\ 5 & \Gamma \vdash A \wedge B & \mathrm{MP}(2)(4) \end{array}$$

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

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

Пример

- Доказать
$$\vdash (A \to B \to C) \to A \land B \to C$$
- Доказательство:

1	$A \to B \to C, A \land B \vdash A \land B$	
2	$A \to B \to C, A \land B \vdash A$	$\land$elimI (1)
3	$A \to B \to C, A \land B \vdash A \to B \to C$	
4	$A \to B \to C, A \land B \vdash B \to C$	MP(2)(3)
5	$A \to B \to C, A \land B \vdash B$	$\land$elimII (1)
6	$A \to B \to C, A \land B \vdash C$	MP(5)(4)
7	$A \to B \to C \vdash A \land B \to C$	$\to$ intro (6)
8	$\vdash (A \to B \to C) \to A \land B \to C$	$\to$ intro (7)

Правило введения и удаления дизъюнкции

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

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

- Из аксиомы 8 имеем *правило разбора случаев*

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

откуда можно получить *правило удаления дизъюнкциии*

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ (\vee\mathrm{elim})$$

Пример

- Доказать

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

- Доказательство:

1	$A \vee B \to C, A \vdash A$	
2	$A \vee B \to C, A \vdash A \vee B$	$\vee$introI (1)
3	$A \vee B \to C, A \vdash A \vee B \to C$	
4	$A \vee B \to C, A \vdash C$	MP(2)(3)
5	$A \vee B \to C \vdash A \to C$	$\to$ intro (4)
6	$A \vee B \to C, B \vdash B$	
7	$A \vee B \to C, B \vdash A \vee B$	$\vee$introII (6)
8	$A \vee B \to C, B \vdash A \vee B \to C$	
9	$A \vee B \to C, B \vdash C$	MP(7)(8)
10	$A \vee B \to C \vdash B \to C$	$\to$ intro (9)
11	$A \vee B \to C \vdash (A \to C) \wedge (B \to C)$	$\wedge$intro (5)(10)
12	$\vdash (A \vee B \to C) \to (A \to C) \wedge (B \to C)$	$\to$ intro (11)

Правило введения и удаления отрицания

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

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

- Аксиома 10 описывает, как можно ввести отрицание

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

Пример

- Доказать закон контрапозиции

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

- Доказательство:

$$\begin{array}{lll}
1 & A \to B, \neg B, A \vdash \neg B & \\
2 & A \to B, \neg B, A \vdash A & \\
3 & A \to B, \neg B, A \vdash A \to B & \\
4 & A \to B, \neg B, A \vdash B & \mathrm{MP}(2)(3) \\
5 & A \to B, \neg B \vdash \neg A & \neg\mathrm{intro}\ (1)(4)
\end{array}$$

- 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*" (tetrium non datur).
- Из нее можно вывести "*закон снятия двойного отрицания*"

$$\neg\neg A \to A$$

- Действительно

$$\begin{array}{lll}
1 & A, \neg\neg A \vdash A & \\
2 & \neg A, \neg\neg A \vdash A & \neg\mathrm{elim} \\
3 & A \vee \neg A, \neg\neg A \vdash A & \text{case analysis } (1)(2) \\
4 & A \vee \neg A \vdash \neg\neg A \to A & \to \mathrm{intro}(3)
\end{array}$$

Аксиома в множестве формул

- Можно ли в предыдущем примере

$$A \vee \neg A \vdash \neg\neg A \to A$$

убрать аксиому слева от $\vdash$?

Аксиома в множестве формул

- Можно ли в предыдущем примере

$$A \vee \neg A \vdash \neg\neg A \to A$$

убрать аксиому слева от $\vdash$?

- Да, и это верно для любой аксиомы

$$\begin{array}{lll} 1 & \Gamma, Ax \vdash B & \\ 2 & \Gamma \vdash Ax \to B & \to \mathrm{intro}(3) \\ 3 & \Gamma \vdash Ax & \\ 4 & \Gamma \vdash B & \to \mathrm{elim}(3)(2) \end{array}$$

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

План лекции

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

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

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

$$
\begin{array}{l}
\neg A \vdash \neg A \\
A \vdash \neg\neg A
\end{array}
$$

Доказательство. Несложный вывод. ■

Вспомогательные факты (2)

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

p_1	p_2	$\ldots$	p_n	B
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
α_1	α_2	$\ldots$	α_n	β
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$

можно построить выводы

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

где

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

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

Теорема о полноте исчисления высказываний

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 $\neg B$:

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

Выберем переменную, например, p_n. Имеем

$$\begin{array}{lll}
1 & L_1, \ldots, L_{n-1}, p_n \vdash B & \\
2 & L_1, \ldots, L_{n-1}, \neg p_n \vdash B & \\
3 & L_1, \ldots, L_{n-1} \vdash p_n \vee \neg p_n & (A11) \\
4 & L_1, \ldots, L_{n-1} \vdash B & \vee elim(3)(1)(2) \\
 & \ldots & \\
 & \vdash B &
\end{array}$$

■

Более универсальный подход к корректности и полноте

- 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 $\neg\mathrm{elim}$, из него можно вывести любую формулу.

Корректность, дубль 2

- **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 истинна[1], 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. ■

[1] Индукцией по структуре вывода.

Полнота множества формул

- 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. ■

Совместность непротиворечивого полного множества

- **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):

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

  Индукцией по построению для произвольной формулы A из Δ доказываем

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

  База: Если формула A — переменная, то очевидно.
  Шаг: делаем стандартный перебор связок (самостоятельно). ■

Полнота, дубль 2

- **Теорема.** Всякое непротиворечивое множество Γ совместно.
- **Доказательство.** Непосредственно из Лемм 1 и 2.$\blacksquare$
- **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 $\vdash A$. $\blacksquare$

Компактность

- **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).■