Введение в математическую логику
(осень 2018)

В.Б. Шехтман

Лекция 4

Теорема 4.1. *Для любой нетривиальной булевой алгебры $\mathcal{B}$ и формулы A*

$$\mathcal{B} \vDash A \Rightarrow \mathit{2} \vDash A.$$

Доказательство Пусть $\mathcal{B} \vDash A$. Возьмем оценку $f : Var \longrightarrow \mathit{2}$, и рассмотрим "такую же" оценку в $\mathcal{B}$, т.е. $F : Var \longrightarrow \mathcal{B}$, где

$$F(P_i) = \mathbf{1} \Leftrightarrow f(P_i) = 1$$

для каждого i. Из свойств булевых алгебр получаем:

$$\mathbf{0} \sqcup \mathbf{1} = \mathbf{1} \sqcup \mathbf{0} = \mathbf{1},\ \mathbf{0} \sqcup \mathbf{0} = \mathbf{0},\ \mathbf{1} \sqcup \mathbf{1} = \mathbf{1},$$

и аналогично для $\sqcap$.

Кроме того,
$-\mathbf{0} = \mathbf{1}$, т.к. $\mathbf{1} = \mathbf{0} \sqcup -\mathbf{0} = -\mathbf{0}$,
$-\mathbf{1} = \mathbf{0}$, т.к. $\mathbf{0} = \mathbf{1} \sqcap -\mathbf{1} = -\mathbf{1}$.

Отсюда мы видим, что $\mathbf{0}, \mathbf{1}$ образуют подалгебру в $\mathcal{B}$, изоморфную $\mathit{2}$. Обозначим этот изоморфизм через $\approx$, т.е. пусть

$$\mathbf{1} \approx 1,\ \mathbf{0} \approx 0.$$

Тогда для всех i

$$F(P_i) \approx f(P_i),$$

откуда по индукции имеем для любой формулы B

$$F(B) \approx f(B).$$

Здесь надо разбирать все случаи построения B, но это — рутинная проверка. Например, пусть $B = C \vee D$. Тогда $F(B) = F(C) \sqcup F(D)$, $f(B) = \max(f(C), f(D))$, и если $F(C) \approx f(C),\ F(D) \approx f(D)$, то $F(C) \sqcup F(D) \approx \max(f(C), f(D))$. Это получается из равенств

$$\mathbf{0} \sqcup \mathbf{1} = \mathbf{1} \sqcup \mathbf{0} = \mathbf{1},\ \mathbf{0} \sqcup \mathbf{0} = \mathbf{0},\ \mathbf{1} \sqcup \mathbf{1} = \mathbf{1}.$$

Теперь для исходной формулы A получаем $f(A) = 1$, поскольку $F(A) = \mathbf{1}$.

Таким образом, $2 \vDash A$. ■

Исчисление высказываний

Различные тавтологии можно получать как теоремы в некоторой аксиоматической системе — исчислении высказываний. Имеются разные варианты таких исчислений. Мы будем рассматривать исчисление *гильбертовского типа*. Оно задается множеством *аксиом* и *правил вывода*; *теоремы* выводятся из аксиом с помощью правил. В процессе вывода возникает *доказательство* — некоторая последовательность формул.

Приведем одну из формулировок исчисления высказываний (CL).

Схемы аксиом

(1) $A \to (B \to A)$

(2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

(3) $A \wedge B \to A$

(4) $A \wedge B \to B$

(5) $A \to (B \to A \wedge B)$

(6) $A \to A \vee B$

(7) $B \to A \vee B$

(8) $(A \to C) \to ((B \to C) \to (A \vee B \to C))$

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

(10) $\neg\neg A \to A$

Здесь A, B, C — произвольные формулы. Поэтому каждая из схем (1)–(10) порождает бесконечную серию аксиом. Например, схема (1) задает аксиомы вида $A \to (B \to A)$ и т.д.

Единственное правило вывода — Modus Ponens (MP), которое записывается так:

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

Эта запись означает, что если доказаны формулы A и $A \to B$, то можно доказать B.

Формальное понятие доказательства определяется следующим образом.

Определение 1. Доказательство *(или* вывод*) формулы A в CL — это конечная последовательность формул, каждая из которых — аксиома или получается из предыдущих по правилу MP и которая заканчивается формулой A.*

Точнее: доказательство — это такая последовательность формул $A_1, \ldots, A_n = A$, что для всех k $(1 \le k \le n)$ A_k — аксиома или существуют $i, j < k$, для которых $A_j = A_i \to A_k$.

Действительно, из A_i и $A_i \to A_k$ по MP получается как раз A_k.

Любое математическое доказательство можно организовать аналогичным образом, если включить в него все промежуточные доказательства и выбрать подходящую систему аксиом и правил вывода (исчисления высказываний здесь уже не хватит). Однако на практике так не происходит, потому что доказательства упрощаются и сокращаются.

Формула A, для которой существует доказательство в CL, называется *теоремой* CL, или *выводимой* в CL; это записывается так: $\vdash_{CL} A$. Индекс CL не пишем, если ясно, что речь идет об этой системе.

Пример 1 $\vdash A \vee B \to B \vee A$.

Приведем доказательство (с комментариями). Для удобства обозначим формулу $B \vee A$ через C.

1. $A \to C$ (аксиома 7)

2. $B \to C$ (аксиома 6)

3. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$ (аксиома 8)

4. $(B \to C) \to (A \vee B \to C)$ (2,4, MP)

5. $A \vee B \to C$ (1,3, MP)

Формула 5 и есть нужная теорема.

Пример 2 $\vdash A \to A$. Обозначим эту формулу B.

1. $A \to B$ (аксиома 1)

2. $A \to (B \to A)$ (аксиома 1)

3. $(A \to (B \to A)) \to ((A \to B) \to (A \to A))$ (аксиома 2)

4. $(A \to B) \to (A \to A)$ (2,3, MP)

5. $A \to A$ (1,4, MP)

Расширим теперь определение вывода 1.

Определение 2. *Пусть* Γ *— какое-то множество пропозициональных формул.* Вывод из Γ *формулы* A *в* CL *— это конечная последовательность формул, каждая из которых — аксиома или принадлежит* Γ *или получается из предыдущих по правилу MP и которая заканчивается формулой* A.

Т.е. это последовательность формул $A_1, \ldots, A_n$, *где для всех* k A_k *— аксиома или* $A_k \in \Gamma$ *или существуют* $i, j < k$, *для которых* $A_j = A_i \to A_k$.

Формула A выводима из Γ, *если существует вывод из* Γ, *содержащий* A; *обозначение:* $\Gamma \vdash_{CL} A$.

Если рассматриваются выводы из Γ, то формулы из Γ называются *гипотезами*. В математике (и в практической жизни) такие выводы часто встречаются: мы делаем какие-то предположения (временно считая их аксиомами), и получаем из них различные следствия.

Очевидно, что если $\Gamma = \varnothing$, то вывод из Γ — это обычный вывод из заданных аксиом (в CL).

Лемма 4.2.

(1) Если $\Delta \subseteq \Gamma$ *и* $\Delta \vdash A$*, то* $\Gamma \vdash A$*.*

(2) Если $\Gamma \vdash A$*, то существует конечное* $\Delta \subseteq \Gamma$*, для которого* $\Delta \vdash A$*.*

(3) ("транзитивность выводимости", или "сечение")
Если $\Gamma \vdash A$*, и* $\Delta \vdash B$ *для всех* $B \in \Gamma$*, то* $\Delta \vdash A$*.*

Если условие $\Delta \vdash B$ для всех $B \in \Gamma$ обозначить как $\Delta \vdash \Gamma$, то утверждение (3) запишется так:

$$\text{Если } \Delta \vdash \Gamma \text{ и } \Gamma \vdash A, \text{ то } \Delta \vdash A.$$

Отсюда название "транзитивность".

Доказательство (1) очевидно.

(2) также очевидно: можно составить Δ из тех гипотез, которые встречаются в выводе A; их конечное число.

(3) Предположим, что $\Delta \vdash \Gamma$ и $\Gamma \vdash A$. Из (2) следует, что можно заменить Γ на его конечное подмножество Γ_1, т.е. мы имеем

$$\Delta \vdash \Gamma_1,\ \Gamma_1 \vdash A.$$

Пусть $\Gamma_1 = \{B_1, \ldots, B_n\}$. Пусть Π_i —- вывод B_i из Δ. Возьмем вывод A из Γ_1; в нем встречаются какие-то гипотезы B_i:

$$\ldots B_{i_1}, \ldots, B_{i_2}, \ldots, A.$$

Заменим в этом выводе каждую B_i на ее вывод Π_i:

$$\ldots \Pi_{i_1}, \ldots, \Pi_{i_2}, \ldots, A.$$

Получится вывод A из из Δ. Действительно, все формулы из исходного вывода, кроме гипотез B_i, — аксиомы CL или получаются из предыдущих по MP. А в каждом вставном выводе Π_i все формулы — аксиомы CL или входят в Δ или получаются по MP из предыдущих (внутри того же вывода).

■

Вместо $\{A_1, \ldots, A_n\} \vdash_{CL} B$ обычно пишут $A_1, \ldots, A_n \vdash_{CL} B$. Говорят также, что $\dfrac{A_1, \ldots, A_n}{B}$ — *производное правило* CL.

Если из выводимости формул $A_1, \ldots, A_n$ следует выводимость B, то говорят, что $\dfrac{A_1, \ldots, A_n}{B}$ — *допустимое правило* CL.

Лемма 4.3. *Всякое производное правило CL допустимо.*[1]

Доказательство Пусть $\Gamma = \{A_1, \ldots, A_n\} \vdash B$. Тогда, если $\varnothing \vdash \Gamma$, то $\varnothing \vdash B$ — по транзитивности выводимости: ■

Транзитивность выводимости означает, что уже доказанные теоремы можно использовать в новых выводах, не повторяя из доказательств. Полученные допустимые правила также можно применять для сокращения доказательств.

Пример 3 Допустимо правило введения конъюнкции

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

Действительно, $A, B \vdash A \wedge B$:

1. A (гипотеза)
2. B (гипотеза)
3. $A \to (B \to A \wedge B)$ (аксиома 5)
4. $B \to A \wedge B$ (1,3, MP)
5. $A \wedge B$ (2,4, MP)

Теорема о дедукции для исчисления высказываний

Теорема 4.4. *(теорема[2] о дедукции)*

$$\Gamma, A \vdash_{CL} B \Leftrightarrow \Gamma \vdash_{CL} A \to B.$$

Здесь Γ, A обозначает множество $\Gamma \cup \{A\}$.

Доказательство Утверждение ($\Leftarrow$) почти очевидно. Действительно, пусть $\Gamma \vdash A \to B$. Тогда имеем $\Gamma, A \vdash A, A \to B$ и $A, A \to B \vdash B$ (MP). Отсюда по транзитивности $\Gamma, A \vdash B$.

Утверждение ($\Rightarrow$) доказывается индукцией по длине вывода B из Γ, A.

(1) Если этот вывод — длины 1, то B — аксиома или гипотеза. Если B — аксиома, то имеем вывод $A \to B$ (из $\varnothing$):

[1] Обратное утверждение (при некотором уточнении понятия “правило вывода ”) тоже верно, но в этом курсе мы его не доказываем.

[2] Конечно, это — не теорема нашего формального исчисления, а утверждение о его свойствах (“метатеорема”).

1. B (аксиома)

2. $B \to (A \to B)$ (аксиома 1)

3. $A \to B$ (1,2, MP)

(2) Если $B \in \Gamma$, то имеем такой же вывод $A \to B$ из Γ:

1. B (гипотеза)

2. $B \to (A \to B)$ (аксиома 1)

3. $A \to B$ (1,2, MP)

(3) Если $B = A$, то $A \to B = A \to A$. Но $\vdash A \to A$ (пример 2 выше).

(4) Предположим теперь, что $\Gamma, A \vdash B$ и утверждение ($\Rightarrow$) верно для всех более коротких выводов, т.е.
для всех C, если $\Gamma, A \vdash C$ и вывод C из Γ, A короче, чем вывод B, то $\Gamma \vdash A \to C$.

Докажем, что $\Gamma \vdash A \to B$.

Рассмотрим вывод из Γ, A, который заканчивается формулой B. При этом B может оказаться аксиомой или гипотезой (тогда все предыдущие формулы для доказательства B не нужны). Но в этом случае $\Gamma \vdash A \to B$ по (1)–(3).

Остается случай, когда B получается по MP из формул $C, C \to B$, причем $\Gamma, A \vdash C$ и $\Gamma, A \vdash C \to B$ с более короткими доказательствами. По предположению индукции имеем

(*) $\Gamma \vdash A \to C,\ A \to (C \to B)$.

С другой стороны,

(**) $A \to C,\ A \to (C \to B) \vdash A \to B$:

1. $A \to C$ (гипотеза)

2. $A \to (C \to B)$ (гипотеза)

3. $(A \to (C \to B)) \to ((A \to C) \to (A \to B))$ (аксиома 2)

4. $(A \to C) \to (A \to B)$ (2,3, MP)

5. $A \to B$ (1,4, MP)

Из (*), (**) по транзитивности получаем $\Gamma \vdash A \to B$. ■

Отметим частный случай теоремы о дедукции для $\Gamma = \varnothing$:

$$A \vdash B \ \Leftrightarrow \vdash A \to B.$$

Пример 4 Допустимо *правило силлогизма*

$$\frac{A \to B, B \to C}{A \to C}.$$

Покажем, что это — производное правило, т.е.

$$A \to B,\ B \to C \vdash A \to C.$$

По теореме дедукции это равносильно

$$A \to B,\ B \to C, A \vdash C.$$

Последнее утверждение очевидно: надо два раза применить MP.

Корректность исчисления высказываний для булевых алгебр

Теорема 4.5. *Если $\vdash_{CL} A$, то $\mathcal{B} \vDash A$ для любой булевой алгебры $\mathcal{B}$.*

Доказательство

Доказываем теорему индукцией по длине вывода A. Имеется 2 случая:

(I) A — аксиома.

(II) A получается по MP из формул B, $B \to A$ с более короткими выводами.

Начнем с более простого случая (II). По предположению индукции, $\mathcal{B} \vDash B, B \to A$. Рассмотрим произвольную оценку f в $\mathcal{B}$; пусть $f(A) = a$. Докажем, что $a = \mathbf{1}$.

Поскольку $\mathcal{B} \vDash B, B \to A$, имеем: $f(B) = f(B \to A) = \mathbf{1}$. Тогда

$$\mathbf{1} = f(B \to A) = f(B) \oplus f(A) = \mathbf{1} \oplus a.$$

По лемме 3.4 $\mathbf{1} \leq a$, и значит, $a = \mathbf{1}$, т.к. $\mathbf{1}$ — наибольший элемент.

В случае (I) надо доказывать общезначимость всех 10 аксиом. Это мы рассмотрим на следующей лекции. ■