

2. Исчисление высказываний

Напомним, что тавтологии — это пропозициональные формулы, истинные при всех значениях переменных. Оказывается, что все тавтологии можно получить из некоторого набора «аксиом» с помощью «правил вывода», которые имеют чисто синтаксический характер и никак не апеллируют к смыслу формулы, её истинности и т. д. Эту задачу решает так называемое *исчисление высказываний*. В этой главе мы перечислим аксиомы и правила вывода этого исчисления, и приведём несколько доказательств *теоремы о полноте* (которая утверждает, что всякая тавтология выводима в исчислении высказываний).

2.1. Исчисление высказываний (ИВ)

Каковы бы ни были формулы A, B, C , следующие формулы называют *аксиомами исчисления высказываний*:

- (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) $A \vee \neg A$.

Как говорят, мы имеем здесь одиннадцать «схем аксиом»; из каждой схемы можно получить различные конкретные аксиомы, заменяя входящие в неё буквы на пропозициональные формулы.

Единственным правилом вывода исчисления высказываний является правило со средневековым названием «modus ponens» (MP). Это правило разрешает получить (вывести) из формул A и $(A \rightarrow B)$ формулу B .

Выводом в исчислении высказываний называется конечная последовательность формул, каждая из которых есть аксиома или получается из предыдущих по правилу modus ponens.

Вот пример вывода (в нём первая формула является частным случаем схемы (1), вторая — схемы (2), а последняя получается из

двух предыдущих по правилу *modus ponens*):

$$\begin{aligned}(p \rightarrow (q \rightarrow p)), \\ (p \rightarrow (q \rightarrow p)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow p)), \\ ((p \rightarrow q) \rightarrow (p \rightarrow p)).\end{aligned}$$

Пропозициональная формула A называется *выводимой* в исчислении высказываний, или *теоремой* исчисления высказываний, если существует вывод, в котором последняя формула равна A . Такой вывод называют выводом формулы A . (В принципе можно было бы и не требовать, чтобы формула A была последней — все дальнейшие формулы можно просто вычеркнуть.)

Как мы уже говорили, в исчислении высказываний выводятся все тавтологии и только они. Обычно это утверждение разбивают на две части: простую и сложную. Начнём с простой:

Теорема 17 (о корректности ИВ). Всякая теорема исчисления высказываний есть тавтология.

◁ Несложно проверить, что все аксиомы — тавтологии. Для примера проделаем это для самой длинной аксиомы (точнее, схемы аксиом) — для второй. В каком случае формула

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

(где A, B, C — некоторые формулы) могла бы быть ложной? Для этого посылка $A \rightarrow (B \rightarrow C)$ должна быть истинной, а заключение $(A \rightarrow B) \rightarrow (A \rightarrow C)$ — ложным. Чтобы заключение было ложным, формула $A \rightarrow B$ должна быть истинной, а формула $A \rightarrow C$ — ложной. Последнее означает, что A истинна, а C ложна. Таким образом, мы знаем, что A , $(A \rightarrow B)$ и $(A \rightarrow (B \rightarrow C))$ истинны. Отсюда следует, что B и $(B \rightarrow C)$ истинны, и потому C истинна — противоречие. Значит, наша формула не бывает ложной.

Корректность правила МР также ясна: если формулы $(A \rightarrow B)$ и A всегда истинны, то по определению импликации формула B также всегда истинна. Таким образом, все формулы, входящие в выводы (все теоремы) являются тавтологиями. ▷

Гораздо сложнее доказать обратное утверждение.

Теорема 18 (о полноте ИВ). Всякая тавтология есть теорема исчисления высказываний.

◁ Мы предложим несколько альтернативных доказательств этой теоремы. Но прежде всего мы должны приобрести некоторый опыт построения выводов и использования аксиом.

Лемма 1. Какова бы ни была формула D , формула $(D \rightarrow D)$ является теоремой.

Докажем лемму, предъявив вывод формулы $(D \rightarrow D)$ в исчислении высказываний.

1. $(D \rightarrow ((D \rightarrow D) \rightarrow D)) \rightarrow ((D \rightarrow (D \rightarrow D)) \rightarrow (D \rightarrow D))$
[аксиома 2 при $A = D$, $B = (D \rightarrow D)$, $C = D$];
2. $D \rightarrow ((D \rightarrow D) \rightarrow D)$ [аксиома 1];
3. $(D \rightarrow (D \rightarrow D)) \rightarrow (D \rightarrow D)$ [из 1 и 2 по правилу MP];
4. $D \rightarrow (D \rightarrow D)$ [аксиома 1];
5. $(D \rightarrow D)$ [из 3 и 4 по правилу MP].

Как видно, вывод даже такой простой тавтологии, как $(D \rightarrow D)$, требует некоторой изобретательности. Мы облегчим себе жизнь, доказав некоторое общее утверждение о выводимости.

Часто мы рассуждаем так: предполагаем, что выполнено какое-то утверждение A , и выводим различные следствия. После того как другое утверждение B доказано, мы вспоминаем, что использовали предположение A , и заключаем, что мы доказали утверждение $A \rightarrow B$. Следующая лемма, называемая иногда «леммой о дедукции», показывает, что этот подход правомерен и для исчисления высказываний.

Пусть Γ — некоторое множество формул. *Выводом из Γ* называется конечная последовательность формул, каждая из которых является аксиомой, принадлежит Γ или получается из предыдущих по правилу MP. (Другими словами, мы как бы добавляем формулы из Γ к аксиомам исчисления высказываний — именно как формулы, а не как схемы аксиом.) Формула A *выводима из Γ* , если существует вывод из Γ , в котором она является последней формулой. В этом случае мы пишем $\Gamma \vdash A$. Если Γ пусто, то речь идёт о выводимости в исчислении высказываний, и вместо $\emptyset \vdash A$ пишут просто $\vdash A$.

Лемма 2 (о дедукции). $\Gamma \vdash A \rightarrow B$ тогда и только тогда, когда $\Gamma \cup \{A\} \vdash B$.

В одну сторону утверждение почти очевидно: пусть $\Gamma \vdash (A \rightarrow B)$. Тогда и $\Gamma, A \vdash (A \rightarrow B)$. (Для краткости мы опускаем фигурные скобки и заменяем знак объединения запятой.) Согласно определению, $\Gamma, A \vdash A$, откуда по MP получаем $\Gamma, A \vdash B$.

Пусть теперь $\Gamma, A \vdash B$. Нам надо построить вывод формулы $A \rightarrow B$ из Γ . Возьмём вывод C_1, C_2, \dots, C_n формулы $B = C_n$ из Γ, A . Припишем ко всем формулам этого вывода слева посылку A :

$$(A \rightarrow C_1), (A \rightarrow C_2), \dots, (A \rightarrow C_n).$$

Эта последовательность оканчивается на $(A \rightarrow B)$. Сама по себе она не будет выводом из Γ , но из неё можно получить такой вывод, добавив недостающие формулы, и тем самым доказать лемму о дедукции.

Будем добавлять эти формулы, двигаясь слева направо. Пусть мы подошли к формуле $(A \rightarrow C_i)$. По предположению формула C_i либо совпадает с A , либо принадлежит Γ , либо является аксиомой, либо получается из двух предыдущих по правилу МР. Рассмотрим все эти случаи по очереди.

(1) Если C_i есть A , то очередная формула имеет вид $(A \rightarrow A)$. По лемме 1 она выводима, так что перед ней мы добавляем её вывод.

(2) Пусть C_i принадлежит Γ . Тогда мы вставляем формулы C_i и $C_i \rightarrow (A \rightarrow C_i)$ (аксиома 1). Применение правила МР к этим формулам даёт $(A \rightarrow C_i)$, что и требовалось.

(3) Те же формулы можно добавить, если C_i является аксиомой исчисления высказываний.

(4) Пусть, наконец, формула C_i получается из двух предыдущих формул по правилу МР. Это значит, что в исходном выводе ей предшествовали формулы C_j и $(C_j \rightarrow C_i)$. Тогда в новой последовательности (с добавленной посылкой A) уже были формулы $(A \rightarrow C_j)$ и $(A \rightarrow (C_j \rightarrow C_i))$. Поэтому мы можем продолжить наш Γ -вывод, написав формулы

$((A \rightarrow (C_j \rightarrow C_i)) \rightarrow ((A \rightarrow C_j) \rightarrow (A \rightarrow C_i)))$ (аксиома 2);

$((A \rightarrow C_j) \rightarrow (A \rightarrow C_i))$ (modus ponens);

$(A \rightarrow C_i)$ (modus ponens).

Итак, во всех четырёх случаях мы научились дополнять последовательность до вывода из Γ , так что лемма о дедукции доказана.

20. Докажите, что для любых формул A, B, C формула

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

выводима в исчислении высказываний. (Указание: используйте лемму о дедукции и тот факт, что $A \rightarrow B, B \rightarrow C, A \vdash C$.)

21. Докажите, что если $\Gamma_1 \vdash A$ и $\Gamma_2, A \vdash B$, то $\Gamma_1 \cup \Gamma_2 \vdash B$. (Это свойство иногда называют «правилом сечения» (cut); говорят, что формула A «отсекается» или «высекается». Сходные правила играют центральную роль в теории доказательств, где формулируется и доказывается «теорема об устранении сечения» для различных логических систем.)

22. Добавим к исчислению высказываний, помимо правила МР, ещё одно правило, называемое *правилом подстановки*. Оно разрешает заменить в выведенной формуле все переменные на произвольные формулы

(естественно, вхождения одной переменной должны заменяться на одну и ту же формулу). Покажите, что после добавления такого правила класс выводимых формул не изменится, но лемма о дедукции перестанет быть верной.

Заметим, что мы пока что использовали только две первые аксиомы исчисления высказываний. Видно, кстати, что они специально подобраны так, чтобы прошло доказательство леммы о дедукции.

Другие аксиомы описывают свойства логических связок. Аксиомы 3 и 4 говорят, какие следствия можно вывести из конъюнкции ($A \wedge B \vdash A$ и $A \wedge B \vdash B$). Напротив, аксиома 5 говорит, как можно вывести конъюнкцию. Из неё легко следует такое правило: если $\Gamma \vdash A$ и $\Gamma \vdash B$, то $\Gamma \vdash (A \wedge B)$ (применяем эту аксиому и дважды правило МР). Часто подобные правила записывают так:

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

(над чертой пишут «посылки» правила, а снизу — его «заключение», вытекающее из посылок).

23. Докажите, что формула $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \wedge B) \rightarrow C)$, так же как и обратная к ней формула (в которой посылка и заключение переставлены), являются теоремами исчисления высказываний. Докажите аналогичное утверждение про формулы $(A \wedge B) \rightarrow (B \wedge A)$ и $((A \wedge B) \wedge C) \rightarrow (A \wedge (B \wedge C))$.

Аксиомы 6–7 позволяют утверждать, что $A \vdash A \vee B$ и $B \vdash A \vee B$. Аксиома 8 обеспечивает такое правило:

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$$

Оно соответствует такой схеме рассуждения: «Предположим, что $A \vee B$. Разберём два случая. Если выполнено A , то $\langle \dots \rangle$ и потому C . Если выполнено B , то $\langle \dots \rangle$ и потому C . В обоих случаях верно C . Значит, $A \vee B$ влечёт C .»

Обоснование: дважды воспользуемся леммой о дедукции, получив $\Gamma \vdash (A \rightarrow C)$ и $\Gamma \vdash (B \rightarrow C)$, а затем дважды применим правило МР к этим формулам и аксиоме $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C))$. Получив формулу $(A \vee B) \rightarrow C$, опять применим правило МР к ней и формуле $A \vee B$.

24. Докажите, что следующие формулы, а также обратные к ним (меняем местами посылку и заключение) являются теоремами исчисления

высказываний:

$$\begin{aligned} & ((A \vee B) \rightarrow C) \rightarrow ((A \rightarrow C) \wedge (B \rightarrow C)), \\ & ((A \wedge C) \vee (B \wedge C)) \rightarrow ((A \vee B) \wedge C), \\ & ((A \vee C) \wedge (B \vee C)) \rightarrow ((A \wedge B) \vee C). \end{aligned}$$

У нас остались ещё три аксиомы, касающиеся отрицания. Аксиома 9 гарантирует, что из противоречивого набора посылок можно вывести что угодно: если $\Gamma \vdash A$ и $\Gamma \vdash \neg A$, то $\Gamma \vdash B$ для любого B . Аксиома 10, напротив, объясняет, как можно вывести отрицание некоторой формулы A : надо допустить A и вывести два противоположных заключения B и $\neg B$. Точнее говоря, имеет место такое правило:

$$\frac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$$

(в самом деле, дважды применяем лемму о дедукции, а затем правило МР с аксиомой 10).

Аксиомы 9 и 10 позволяют вывести некоторые логические законы, связанные с отрицанием. Докажем, например, что (для любых формул A и B) формула

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

(«закон контрапозиции») является теоремой исчисления высказываний. В самом деле, по лемме о дедукции достаточно установить, что

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

Для этого, в свою очередь, достаточно вывести из трёх посылок $(A \rightarrow B)$, $\neg B$, A какую-либо формулу и её отрицание (в данном случае формулы B и $\neg B$).

25. Выведите формулы $A \rightarrow \neg\neg A$ и $\neg\neg\neg A \rightarrow \neg A$ с помощью аналогичных рассуждений.

Последняя аксиома, называемая «законом исключённого третьего», и иногда читаемая как «третьего не дано» (*tertium non datur* в латинском оригинале), вызвала в первой половине века большое количество споров. (См. раздел 2.4 об интуиционистской логике, в которой этой аксиомы нет.)

Из неё можно вывести закон «снятия двойного отрицания», формулу $\neg\neg A \rightarrow A$. Достаточно показать, что $A \vee \neg A, \neg\neg A \vdash A$. По правилу разбора случаев, достаточно установить, что $A, \neg\neg A \vdash A$

(это очевидно) и что $\neg A, \neg\neg A \vdash A$ (а это верно, так как из двух противоречащих друг другу формул выводится что угодно с помощью аксиомы 9).

26. Докажите, что формула $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$ является теоремой исчисления высказываний. (Указание: используйте закон исключённого третьего.)

27. Исключим из числа аксиом исчисления высказываний закон исключённого третьего, заменив его на закон снятия двойного отрицания. Покажите, что от этого класс выводимых формул не изменится.

28. Докажите, что при наличии аксиомы исключённого третьего (11) аксиома (10) является лишней — её (точнее следовало бы сказать: любой частный случай этой схемы аксиом) можно вывести из остальных аксиом.

Теперь уже можно доказать теорему о полноте: всякая тавтология выводима в исчислении высказываний. Идея доказательства состоит в разборе случаев. Поясним её на примере. Пусть A — произвольная формула, содержащая переменные p, q, r . Предположим, что A истинна, когда все три переменные истинны. Тогда, как мы докажем, $p, q, r \vdash A$. Вообще каждой строке таблицы истинности для формулы A соответствует утверждение о выводимости. Например, если A ложна, когда p и q ложны, а r истинно, то $\neg p, \neg q, r \vdash \neg A$. Если формула A является тавтологией, то окажется, что она выводима из всех восьми возможных вариантов посылок. Пользуясь законом исключённого третьего, можно постепенно избавляться от посылок. Например, из $p, q, r \vdash A$ и $p, q, \neg r \vdash A$ можно получить $p, q, (r \vee \neg r) \vdash A$, то есть $p, q \vdash A$ (поскольку $(r \vee \neg r)$ является аксиомой).

Проведём это рассуждение подробно. Начнём с такой леммы:

Лемма 3. Для произвольных формул P и Q

$$\begin{array}{ll}
 P, Q \vdash (P \wedge Q); & P, Q \vdash (P \vee Q); \\
 P, \neg Q \vdash \neg(P \wedge Q); & P, \neg Q \vdash (P \vee Q); \\
 \neg P, Q \vdash \neg(P \wedge Q); & \neg P, Q \vdash (P \vee Q); \\
 \neg P, \neg Q \vdash \neg(P \wedge Q) & \neg P, \neg Q \vdash \neg(P \vee Q); \\
 \\
 P, Q \vdash (P \rightarrow Q); & \\
 P, \neg Q \vdash \neg(P \rightarrow Q); & P \vdash \neg(\neg P); \\
 \neg P, Q \vdash (P \rightarrow Q); & \neg P \vdash \neg P. \\
 \neg P, \neg Q \vdash (P \rightarrow Q); &
 \end{array}$$

Эта лемма говорит, что если принять в качестве гипотез истин-

ность или ложность формул P и Q , являющихся частями конъюнкции, дизъюнкции или импликации, то можно будет доказать или опровергнуть всю формулу (в зависимости от того, истинна она или ложна). Последняя часть содержит аналогичное утверждение про отрицание.

После предпринятой нами тренировки доказать эти утверждения несложно. Например, убедимся, что $\neg P \vdash \neg(P \wedge Q)$. Для этого достаточно вывести два противоположных утверждения из $\neg P, (P \wedge Q)$; ими будут утверждения P и $\neg P$.

Проверим ещё одно утверждение: $\neg P, \neg Q \vdash \neg(P \vee Q)$. Нам надо вывести два противоположных утверждения из $\neg P, \neg Q, (P \vee Q)$. Покажем, что из $\neg P, \neg Q, (P \vee Q)$ следует всё, что угодно. По правилу разбора случаев достаточно убедиться, что из $\neg P, \neg Q, P$ и из $\neg P, \neg Q, Q$ следует всё, что угодно — но это мы знаем.

Утверждения, касающиеся импликации, просты: в самом деле, мы знаем, что $Q \vdash (P \rightarrow Q)$ благодаря аксиоме 1, а $\neg P \vdash (P \rightarrow Q)$ благодаря аксиоме 9.

Остальные утверждения леммы столь же просты.

Теперь мы можем сформулировать утверждение о разборе случаев для произвольной формулы.

Лемма 4. Пусть A — произвольная формула, составленная из переменных p_1, \dots, p_n . Тогда для каждой строки таблицы истинности формулы A имеет место соответствующее утверждение о выводимости: если $\varepsilon_1, \dots, \varepsilon_n, \varepsilon \in \{0, 1\}$, и значение формулы A есть ε при $p_1 = \varepsilon_1, \dots, p_n = \varepsilon_n$, то

$$\neg_{\varepsilon_1} p_1, \dots, \neg_{\varepsilon_n} p_n \vdash \neg_{\varepsilon} A,$$

где $\neg_u \varphi$ обозначает φ при $u = 1$ и $\neg \varphi$ при $u = 0$ (напомним, что 1 обозначает истину, а 0 — ложь).

Лемма очевидно доказывается индукцией по построению формулы A . Мы имеем посылки, утверждающие истинность или ложность переменных, и для всех подформул (начиная с переменных и идя ко всей формуле) выводим их или их отрицания с помощью леммы 3.

Если формула A является тавтологией, то из всех 2^n вариантов посылок выводится именно она, а не её отрицание. Тогда правило разбора случаев и закон исключённого третьего позволяют избавиться от посылок: сгруппируем их в пары, отличающиеся в позиции p_1 (в одном наборе посылок стоит p_1 , в другом $\neg p_1$), по правилу разбора случаев заменим их на посылку $(p_1 \vee \neg p_1)$, которую можно выбросить (она является аксиомой). Сделав так для всех пар, получим

2^{n-1} выводов, в посылках которых нет p_1 ; повторим этот процесс с посылками $p_2, \neg p_2$ и т. д. В конце концов мы убедимся, что формула A выводима без посылок, как и утверждает теорема о полноте. \triangleright

2.2. Второе доказательство теоремы о полноте

Это доказательство, в отличие от предыдущего, обобщается на более сложные случаи (исчисление предикатов, интуиционистское исчисление высказываний).

Начнём с такого определения: множество формул Γ называется *совместным*, если существует набор значений переменных, при которых все формулы из Γ истинны. Заметим, что формула φ является тавтологией тогда и только тогда, когда множество, состоящее из единственной формулы $\neg\varphi$, не является совместным. Для случая одной формулы есть специальный термин: формула τ *выполнима*, если существуют значения переменных, при которых она истинна, то есть если множество $\{\tau\}$ совместно. Тавтологии — это формулы, отрицания которых не выполнимы.

Множество формул Γ называется *противоречивым*, если из него одновременно выводятся формулы A и $\neg A$. Мы знаем, что в этом случае из него выводятся вообще все формулы. (В противном случае Γ называется *непротиворечивым*.)

Теорема 19 (корректность исчисления высказываний, вторая форма). Всякое совместное множество формул непротиворечиво.

\triangleleft В самом деле, пусть совместное множество Γ противоречиво. Так как оно совместно, существуют значения переменных, при которых все формулы из Γ истинны. С другой стороны, из Γ выводится некоторая формула B и её отрицание. Может ли так быть?

Оказывается, что нет. Мы уже видели, что всякая выводимая формула истинна при всех значениях переменных (является тавтологией). Справедливо и несколько более общее утверждение: если $\Gamma \vdash A$ и при некоторых значениях переменных все формулы из Γ истинны, то и формула A истинна при этих значениях переменных. (Как и раньше, это легко доказывается индукцией по построению вывода A из Γ .)

В нашей ситуации это приводит к тому, что на выполняющем наборе значений переменных для Γ должны быть истинны обе формулы B и $\neg B$, что, разумеется, невозможно. \triangleright

Мы называем это утверждение другой формой теоремы о корректности исчисления высказываний, поскольку из него формально