Московский физико-технический институт
Физтех-школа прикладной математики и информатики
Математическая логика и теория алгоритмов, осень 2021
Лекции 5–7: исчисление высказываний и теорема о компактности

Краткое содержание

Зачем нужно исчисление высказываний. Общие понятия аксиом, правил вывода, вывода, выводимой формулы. Гильбертовский и генценовский подходы к построению исчисления. Список аксиом и правил вывода в гильбертовской системе. Теорема о корректности исчисления высказываний. Вывод коммутативности дизъюнкции. Вывод эквивалентного определения импликации. Вывод закона тождества. Выводимость из посылок. Лемма о дедукции. Вывод силлогизма. Вывод ассоциативности дизъюнкции. Дополнительные правила вывода. Другие примеры выводов: коммутативность конъюнкции, две дистрибутивности, закон непротиворечия, закон двойного отрицания, контрапозиция, законы де Моргана. Использование закона исключённого третьего в выводах. Лемма о выводимости из литералов. Теорема о полноте исчисления высказываний. Совместные и непротиворечивые системы формул. Непротиворечивость любой совместной системы, связь с теоремой о корректности. Совместность любой непротиворечивой системы: связь с теоремой о полноте, пополнение непротиворечивых систем, совместность любой полной непротиворечивой системы. Теорема о компактности для исчисления высказываний. Применения теоремы о компактности: раскраска обобщённых графов, определимость присваиваний, лемма Кёнига, замощения плоскости.

1 Формальные системы рассуждений

Становление логики как математической дисциплины началось с попыток аксиоматизации и формализации математических рассуждений, после того как обнаружилось, что рассуждения на естественном языке могут приводить к парадоксам. Фундаментом любой формальной математической системы являются логические правила, позволяющие из одних истинных утверждений получать другие истинные утверждения. В обычных математических текстах эти правила считаются самоочевидными и не специфицируются. Но в логике изучаются именно они. Более того, изучаются различные варианты, в которых список этих правил существенно меняется: например, помимо классической логики существует интуиционистская.

В этой лекции мы изучаем *исчисление высказываний* (propositional calculus), т. е. наши формулы будут что-то говорить лишь об истинности или ложности утверждений, от которых они зависят, не обращая внимания на смысл этих утверждений. Более конкретно, мы будем рассматривать пропозициональные формулы на некотором наборе переменных с использованием связок $\neg$, $\wedge$, $\vee$ и $\to$. Формальная система будет задаваться списком *аксиом* (axioms), т. е. утверждений, истинность которых постулируется, и *правил вывода* (inference rules), т. е. процедур, позволяющих из одних истинных утверждений получать другие. Понятия вывода и выводимой формулы определяются так:

Определение 1. *Выводом* (derivation) называется конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из ранее встретившихся по правилам вывода. Формула называется *выводимой* (derivable), если она встречается в некотором выводе.

Из определения очевидно следует, что начало любого вывода также будет выводом. Поэтому мы не требуем, чтобы выводимая формула встретилась именно на последнем месте вывода.

Разные конкретные системы отличаются набором аксиом и правил вывода, в которых так или иначе нужно описать суть всех четырёх логических связок. Описанные выше исчисления называют исчислениями *гильбертовского типа*. Обычно в них много аксиом и небольшое число правил вывода. Альтернативный подход — *генценовский*, или исчисление секвенций: в качестве базового элемента вывода используется не пропозициональная формула, а *секвенция* (sequent), т. е. утверждение, которое говорит, что из одного множества пропозициональных формул выводится другое множество. Выводом будет последовательность секвенций, каждая из которых будет либо аксиомой, либо получаться из ранее встретившихся по одному из правил вывода. Формула будет выводимой, если она встретилась в некотором выводе в правой части некоторой секвенции с пустой левой частью. Обычно в генценовских системах мало аксиом и много правил вывода.

2 Аксиомы и правила вывода

В этом разделе мы зафиксируем список аксиом и правил вывода, с которыми будем работать. Точнее говоря, мы перечислим не аксиомы, а *схемы аксиом* (axiom schema, во мн. ч. axiom schemas или axiom schemata), т. е. выражения, которые становятся аксиомами после подстановки в них конкретных формул вместо входящих в них символов A, B, C. Каждую аксиому мы снабдим пояснением, что она означает. Сначала идут две аксиомы про импликацию:

1) $A \to (B \to A)$: истина следует из чего угодно.

2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$: левая дистрибутивность импликации относительно самой себя.

Обычно смысл этой формулы не сразу ясен, так что остановимся на ней подробнее. Посмотрим на подформулу $A \to (B \to C)$. Она означает, что из двух посылок A и B следует заключение C. Действительно, если A верна, то должна быть верна и импликация $B \to C$. А тогда, если и B верна, то должна быть верна C. Подобные конструкции участвуют в нескольких следующих аксиомах. А вся текущая аксиома означает следующее: если из двух посылок следует заключение, и при этом из первой посылки следует вторая, то заключение следует из одной первой посылки.

Затем идут три аксиомы про конъюнкцию:

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

4) $(A \wedge B) \to B$: из конъюнкции двух формул следует каждая из этих формул;

5) $A \to (B \to (A \wedge B))$: если выполнены обе формулы, то выполнена их конъюнкция.

Затем — три аксиомы про дизъюнкцию:

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

7) $B \to (A \vee B)$: дизъюнкция двух формул следует из каждой из них;

8) $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$: если формула C следует из каждой из формул A и B, то она следует и из их дизъюнкции.

Последняя формула называется правилом разбора случаев и часто используется в математических рассуждениях. Например, некоторое утверждение может по-разному доказываться для остроугольных и тупоугольных треугольников, или для чётных и нечётных чисел, и т. д. Если для каждого случая утверждение доказано, то оно доказано и в целом, когда хотя бы один из случаев верен.

Наконец, последние три аксиомы говорят про отрицание:

9) $\neg A \to (A \to B)$: из лжи следует всё, что угодно;

10) $(A \to B) \to ((A \to \neg B) \to \neg A)$: правило рассуждения от противного. Если из A следуют два противоречивых утверждения, т. е. и B, и $\neg B$, то само A обязано быть неверным;

Заметим, что на практике чаще испольщуется другая схема: предполагается, что A неверно, из этого выводится противоречие и делается вывод, что A верно. Это соответствует формуле $(\neg A \to B) \to ((\neg A \to \neg B) \to A)$, однако это более сильное правило, чем настоящая аксиома.

11) $A \vee \neg A$: закон исключённого третьего.

Как мы уже упоминали, правомерность использования закона исключённого третьего подвергалась сомнению среди некоторых логиков XX века. В результате была создана альтернатива — интуиционстиская логика. Лежащая в её основе система вывода, интуиционистское исчисление высказываний, отличается как раз отсутствием последней аксиомы.

В качестве единственного правила вывода выступает modus ponens (Правило Вывода с большой буквы, правило отделения, исключение импликации, гипотетический силлогизм):

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

Понимается оно так: если ранее уже выведены формулы A и $A \to B$, то в вывод можно приписать B.[1] Как и прежде, буквами A и B могут быть обозначены любые пропозициональные формулы.

Утверждение о том, что формула φ выводима в исчислении высказываний (ИВ), записывается так: $\vdash \varphi$. (Символ $\vdash$ в русском языке называется «штопор», а в английском — “turnstile”, т. е. «турникет»). Сразу можно доказать теорему о корректности ИВ (soundness theorem):

[1] Не следует путать modus ponens с логическим законом $A \to ((A \to B) \to B)$. Ведь тогда для вывода B нужно добавить правило $\frac{A \quad A\to B \quad A\to((A\to B)\to B)}{B}$, а если и его преобразовать в формулу, то ещё более сложное правило, и так без конца. Подобная ситуация описана в заметке Льюиса Кэрролла «Что черепаха сказала Ахиллесу».

Теорема 2. *Если* $\vdash \varphi$*, то* φ *— тавтология.*

Доказательство. Любая аксиома является тавтологией. Это можно проверить непосредственно по таблице истинности. Если A и $A \to B$ являются тавтологиями, то B также является тавтологией, ведь только при $A = B = 1$ верны и формула A, и импликация $A \to B$. Индукцией по номеру формулы в выводе доказывается, что все формулы в выводе тавтологичны, что и требовалось. □

Нашей следующей целью будет доказательство обратного утверждения, которое называется *теоремой о полноте* (completeness theorem): все тавтологии выводимы. Вначале мы потренируемся на конкретных примерах и познакомимся с различными приёмами вывода. Затем мы докажем эту теорему двумя способами. Наконец, мы изучим интересное следствие теорем о корректности и полноте: теорему о компактности.

3 Приёмы и примеры выводов

Наша цель — доказать теорему о полноте ИВ. В этом разделе мы приведём много конкретных примеров и познакомимся с различными общими приёмами доказательства выводимости.

3.1 Выводы по определению

Некоторые формулы легко вывести непосредственно по определению. Например:

Утверждение 3. *Коммутативность дизъюнкции выводима, т. е.* $\vdash (A \vee B) \to (B \vee A)$*.*

Доказательство. Вывод состоит из пяти формул:

1. $A \to (B \vee A)$ — аксиома 7)
2. $B \to (B \vee A)$ — аксиома 6)
3. $(A \to (B \vee A)) \to ((B \to (B \vee A)) \to ((A \vee B) \to (B \vee A)))$ — аксиома 8)
4. $(B \to (B \vee A)) \to ((A \vee B) \to (B \vee A))$ — modus ponens из 1 и 3;
5. $(A \vee B) \to (B \vee A)$ — modus ponens из 2 и 4.

□

Утверждение 4. *Выводимо альтернативное определение импликации:* $\vdash (\neg A \vee B) \to (A \to B)$*.*

Доказательство. Вывод также состоит из пяти формул и очень похож на предыдущий:

1. $\neg A \to (A \to B)$ — аксиома 9)
2. $B \to (A \to B)$ — аксиома 1)
3. $(\neg A \to (A \to B)) \to ((B \to (A \to B)) \to ((\neg A \vee B) \to (A \to B)))$ — аксиома 8)
4. $(B \to (A \to B)) \to ((\neg A \vee B) \to (A \to B))$ — modus ponens из 1 и 3;
5. $(\neg A \vee B) \to (A \to B)$ — modus ponens из 2 и 4.

□

Теорема 5. *Закон тождества выводим, т. е.* $\vdash A \to A$*.*

Доказательство. И тут вывод состоит из 5 формул, но выглядит уже иначе:

1. $A \to ((A \to A) \to A)$	аксиома 1)
2. $A \to (A \to A)$	аксиома 1)
3. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$	аксиома 2)
4. $(A \to (A \to A)) \to (A \to A)$	modus ponens из 1 и 3;
5. $A \to A$	modus ponens из 2 и 4.

□

3.2 Теорема о дедукции

Для многих других формул выводы по определению будут слишком длинными. Нужны более мощные инструменты, облегчающие вывод. Первой из них будет теорема о дедукции (deduction theorem).[2] Для этого нужно сначала ввести понятие *выводимости из посылок*.

Определение 6. Пусть Γ («Гамма») есть некоторое множество формул. Тогда *выводом из множества посылок* Γ называется последовательность формул, каждая из которых является либо аксиомой, либо элементом Γ, либо выводится из более ранних по правилу modus ponens. Если формула A встречается в некотором выводе из Γ, то она называется *выводимой из* Γ. Обозначение: $\Gamma \vdash A$.

Теорема 7 (о дедукции)**.** *Из множества посылок выводится импликация* $A \to B$ *тогда и только тогда, когда при добавлении* A *к списку посылок выводится* B*. Иначе говоря,* $\Gamma \vdash A \to B \Leftrightarrow \Gamma \cup \{A\} \vdash B$*.*

Доказательство. Слева направо теорема очень проста. Действительно, если к выводу импликации $A \to B$ из Γ добавить формулы A и B, то получится вывод B из $\Gamma \cup \{A\}$: формулу A можно написать как посылку, а B — по modus ponens.

Справа налево мы будем доказывать по индукции такое утверждение: если $C_1, \ldots, C_n$ есть вывод из $\Gamma \cup \{A\}$, то для всех i импликация $A \to C_i$ выводима из Γ. Рассуждение по индукции будет опираться на такой принцип, объединяющий в себе и базу, и переход: если импликации $A \to C_1, \ldots, A \to C_{i-1}$ выводимы, то и $A \to C_i$ тоже выводима. Разберём несколько случаев:

- C_i является аксиомой. В таком случае импликация выводится в три шага: C_i; $C_i \to (A \to C_i)$ (аксиома 1); $A \to C_i$ (по modus ponens из двух предыдущих).

- C_i является посылкой, т. е. элементом $\Gamma \cup \{A\}$.

  – $C_i \in \Gamma$. Годится тот же вывод, что и для аксиомы.

  – $C_i = A$. Импликация $A \to A$ выводится по теореме 5.

[2] Термин «дедукция» происходит из работ по философии. Им обозначают способ рассуждения от общего к частному, в противоположность индукции, а зачастую понимают как синоним логического вывода вообще. Ведь при логическом выводе делаются конкретные заключения из общих логических законов.

- C_i выводится по правилу modus ponens из формул C_j и C_k для некоторых $j, k < i$. В этом случае C_k обязательно имеет вид $C_j \to C_i$, иначе modus ponens не применить. По предположению индукции $\Gamma \vdash (A \to C_j)$ и $\Gamma \vdash (A \to C_k)$, т. е. $\Gamma \vdash (A \to (C_j \to C_i))$. Далее добавим в вывод вторую аксиому: $(A \to (C_j \to C_i)) \to ((A \to C_j) \to (A \to C_i))$ — и двумя применениями modus ponens получим $A \to C_i$, что и требовалось.

Все случаи разобраны, поэтому индукционный принцип установлен и теорема доказана. □

Покажем, как теорема о дедукции применяется для доказательства выводимости формул.

Утверждение 8. *Выводим закон силлогизма, т. е.* $\vdash (A \to B) \to ((B \to C) \to (A \to C))$.

Доказательство. По теореме о дедукции утверждение $\vdash (A \to B) \to ((B \to C) \to (A \to C))$ эквивалентно $A \to B \vdash ((B \to C) \to (A \to C))$ (для краткости мы опускаем фигурные скобки в перечислении формул из Γ). В свою очередь, это эквивалентно $A \to B, B \to C \vdash A \to C$. Наконец, последнее эквивалентно $A \to B, B \to C, A \vdash C$. А для последнего вывод очень простой: A; $A \to B$; B; $B \to C$; C. □

Сравните это рассуждение с непосредственным выводом:

1. $(B \to C) \to (A \to (B \to C))$;
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$;
3. $((A \to (B \to C)) \to ((A \to B) \to (A \to C))) \to ((B \to C) \to ((A \to (B \to C)) \to ((A \to B) \to (A \to C))))$;
4. $(B \to C) \to ((A \to (B \to C)) \to ((A \to B) \to (A \to C)))$;
5. $((B \to C) \to ((A \to (B \to C)) \to ((A \to B) \to (A \to C)))) \to (((B \to C) \to (A \to (B \to C))) \to ((B \to C) \to ((A \to B) \to (A \to C))))$;
6. $((B \to C) \to (A \to (B \to C))) \to ((B \to C) \to ((A \to B) \to (A \to C)))$;
7. $(B \to C) \to ((A \to B) \to (A \to C))$ (похоже на то, что нужно, но ещё не то!);
8. $((B \to C) \to ((A \to B) \to (A \to C))) \to (((B \to C) \to (A \to B)) \to ((B \to C) \to (A \to C)))$;
9. $((B \to C) \to (A \to B)) \to ((B \to C) \to (A \to C))$;
10. $(((B \to C) \to (A \to B)) \to ((B \to C) \to (A \to C))) \to ((A \to B) \to (((B \to C) \to (A \to B)) \to ((B \to C) \to (A \to C))))$;
11. $(A \to B) \to (((B \to C) \to (A \to B)) \to ((B \to C) \to (A \to C)))$;
12. $((A \to B) \to (((B \to C) \to (A \to B)) \to ((B \to C) \to (A \to C)))) \to (((A \to B) \to ((B \to C) \to (A \to B))) \to ((A \to B) \to ((B \to C) \to (A \to C))))$;
13. $((A \to B) \to ((B \to C) \to (A \to B))) \to ((A \to B) \to ((B \to C) \to (A \to C)))$;
14. $(A \to B) \to ((B \to C) \to (A \to B))$;
15. $(A \to B) \to ((B \to C) \to (A \to C))$.

Ещё один пример показывает, что в импликации с двумя посылками можно менять порядок посылок:

Утверждение 9. *Выводима формула* $(A \to (B \to C)) \to (B \to (A \to C))$.

Доказательство. По теореме о дедукции утверждение $\vdash (A \to (B \to C)) \to (B \to (A \to C))$ эквивалентно $A \to (B \to C) \vdash B \to (A \to C)$, это эквивалентно $A \to (B \to C), B \vdash A \to C$, а это — $A \to (B \to C), B, A \vdash C$. Последний вывод очень простой: A; $A \to (B \to C)$; $B \to C$; B; C. □

3.3 Дополнительные правила вывода

Теорему о дедукции можно переформулировать как правило вывода: $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$. Такие записи означают, что если верна верхняя выводимость, то верна и нижняя. Можно получить различные другие подобные правила, либо применяя лемму о дедукции к разным аксиомам, либо непосредственно. Изучим различные правила и способы их применения к выводам.

Теорема 10. *Справедливо правило сечения (cut rule):* $\dfrac{\Gamma \vdash A \quad \Delta, A \vdash B}{\Gamma, \Delta \vdash B}$. *В общем виде:*

$$\frac{\Gamma \vdash A_1 \quad \ldots \quad \Gamma \vdash A_k \quad \Delta, A_1, \ldots, A_k \vdash B}{\Gamma, \Delta \vdash B};$$

Доказательство. Достаточно написать все выводы подряд. Тогда в последнем выводе формулы A_i будут использоваться не как посылки, а как уже выведенные формулы. □

Теорема 11. *Справедливы следующие правила про конъюнкцию:*

1) *Правило вывода конъюнкции:* $\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$;

2) *Правила сокращения конъюнкции:* $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$ *и* $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$;

3) *Правило добавления конъюнкции:* $\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}$;

4) *Правило разбиения конъюнкциия:* $\dfrac{\Gamma, A \wedge B \vdash C}{\Gamma, A, B \vdash C}$;

Доказательство. Все эти свойства следуют из аксиом 3–5. Более подробно:

1) Нужно записать выводы A и B подряд и добавить в конец цепочку формул $A \to (B \to (A \wedge B))$; $B \to (A \wedge B)$; $A \wedge B$.

2) Нужно к выводу добавить две формулы $(A \wedge B) \to A$; A.

3) Нужно в начало вывода дописать цепочку формул $A \wedge B$; $(A \wedge B) \to A$; $(A \wedge B) \to B$; A; B.

4) Нужно в начало вывода дописать цепочку формул A; B; $A \to (B \to (A \wedge B))$; $B \to (A \wedge B)$; $A \wedge B$.

□

Покажем, как можно применять эти правила:

Утверждение 12. *Выводима коммутативность конъюнкции:* $(A \wedge B) \to (B \wedge A)$.

Доказательство. Очевидно, что $A, B \vdash B$ и $A, B \vdash A$. Отсюда по правилу вывода конъюнкции $A, B \vdash B \wedge A$, затем по правилу добавления конъюнкции $A \wedge B \vdash B \wedge A$. По теореме о дедукции получаем то, что нужно. □

Утверждение 13. *Выводима эквивалентность между импликацией с двумя посылками и импликацией из конъюнкции посылок:* $(A \to (B \to C)) \leftrightarrow ((A \wedge B) \to C)$.

Доказательство. Эквиваленция здесь означает просто две импликации. Докажем их по очереди. Выводимость прямой импликации по дважды применённой лемме о дедукции эквивалентна $(A \to (B \to C)), A \wedge B \vdash C$. По правилу добавления конъюнкции для этого нужно доказать $(A \to (B \to C)), A, B \vdash C$, а это мы уже выводили.

Выводимость обратной импликации эквивалентна $(A \wedge B) \to C, A, B \vdash C$. По правилу разбиения[3] конъюнкции для этого нужно доказать $(A \wedge B) \to C, A \wedge B \vdash C$, а это делается однократным применением modus ponens. $\square$

Теперь обратимся к правилам, облегчающим работу с дизъюнкцией.

Теорема 14. *Справедливы правила добавления дизъюнкции* $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$ *и* $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$.

Доказательство. Правила напрямую следуют из аксиом 6 и 7. $\square$

Теорема 15. *Справедливо правило разбора случаев* $\dfrac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$.

Доказательство. По теореме о дедукции из $\Gamma, A \vdash C$ следует $\Gamma \vdash A \to C$, а из $\Gamma, B \vdash C$ следует $\Gamma \vdash B \to C$. Далее добавляем восьмую аксиому: $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$ — и после двух применений modus ponens получаем $\Gamma \vdash (A \vee B) \to C$. Применив лемму о дедукции в обратную сторону, получаем $\Gamma, A \vee B \vdash C$, что и требовалось. $\square$

Покажем, как можно применить правило разбора случаев вместе с правилом сечения.

Утверждение 16. *Выводима ассоциативность дизъюнкции:* $\vdash ((A \vee B) \vee C) \to (A \vee (B \vee C))$.

Доказательство. Из 6-й и 7-й аксиом по лемме о дедукции имеем $A \vdash A \vee (B \vee C)$, $B \vdash B \vee C$, $C \vdash B \vee C$, $B \vee C \vdash A \vee (B \vee C)$. По правилу сечения получаем $B \vdash A \vee (B \vee C)$ и $C \vdash A \vee (B \vee C)$. далее по правилу разбора случаев получаем $A \vee B \vdash A \vee (B \vee C)$, а затем и $(A \vee B) \vee C \vdash A \vee (B \vee C)$. Применив теорему о дедукции, получаем требуемую формулу. $\square$

Теперь покажем, как правило разбора случаев взаимодействует с правилами для конъюнкции.

Утверждение 17. *Выводима дистрибутивность конъюнкции относительно дизъюнкции и наоборот:* $\vdash (A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$ *и* $\vdash (A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$.

[3] Может показаться, что тут перепутаны названия правил добавления и разбиения. На самом деле всё правильно, просто мы записываем вывод в обратном порядке.

Доказательство. Здесь нужно вывести целых 4 импликации. К каждой из них мы применим теорему о дедукции. Вначале докажем $A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$. По правилу добавления конъюнкции достаточно доказать $A, B \vee C \vdash (A \wedge B) \vee (A \wedge C)$. Для этого по правилу разбора случаев достаточно доказать $A, B \vdash (A \wedge B) \vee (A \wedge C)$ и $A, C \vdash (A \wedge B) \vee (A \wedge C)$. По правилу разбиения дизъюнкции для этого достаточно $A \wedge B \vdash (A \wedge B) \vee (A \wedge C)$ и $A \wedge C \vdash (A \wedge B) \vee (A \wedge C)$, а обе эти выводимости получаются из 6-й и 7-й аксиом по теореме о дедукции.

Перейдём к утверждению $(A \wedge B) \vee (A \wedge C) \vdash A \wedge (B \vee C)$. По правилам разбора случаев и добавления конъюнкции достаточно доказать $A, B \vdash A \wedge (B \vee C)$ и $A, C \vdash A \wedge (B \vee C)$. В обоих случаях по шестой (или седьмой) аксиоме выводится $B \vee C$, A получается как посылка, и $A \wedge (B \vee C)$ выводится по правилу вывода конъюнкции.

Теперь на очереди утверждение $A \vee (B \wedge C) \vdash (A \vee B) \wedge (A \vee C)$. По правилам разбора случаев и добавления конъюнкции достаточно доказать $A \vdash (A \vee B) \wedge (A \vee C)$ и $B, C \vdash (A \vee B) \wedge (A \vee C)$. В каждом варианте по шестой (или седьмой) аксиоме получаются обе дизъюнкции, которые комбинируются по правилу вывода конъюнкции.

Наконец, осталось утверждение $(A \vee B) \wedge (A \vee C) \vdash A \vee (B \wedge C)$. По правилам разбора случаев и добавления конъюнкции достаточно вывести $A \vee (B \wedge C)$ из каждого набора посылок: A; A, C; B, A; B, C. В первых трёх случаях это делается по шестой аксиоме, в последнем по пятой и седьмой. □

Перейдём к правилам, говорящим об отрицании.

Теорема 18. *Справедливы следующие правила вывода*

1) *Правило рассуждения от противного (reductio ad absurdum —* лат. *сведение к абсурду):* $\dfrac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$*;*

2) *Правило вывода из противоречия (principle of explosion, ex falso [sequitur] quodlibet —* лат. *из лжи [следует] что угодно):* $\Gamma, A, \neg A \vdash B$*;*

Доказательство. 1) Аналогично правилу разбора случаев имеем $\Gamma \vdash A \to B$ и $\Gamma \vdash A \to \neg B$. После добавления десятой аксиомы: $(A \to B) \to ((A \to \neg B) \to \neg A)$ — и двойного применения modus ponens получаем $\Gamma \vdash \neg A$, что и требовалось.

2) По теореме о дедукции из 9-й аксиомы $\neg A \to (A \to B)$ следует, что $\neg A, A \vdash B$. Добавление Γ в посылки не повлияет на выводимость.

□

Правило рассуждения от противного удобно понимать так: чтобы вывести отрицание какой-то формулы, надо саму эту формулу добавить в список посылок и из получившегося множества вывести противоречие. Покажем, как работает этот принцип.

Утверждение 19. *Выводим закон непротиворечия:* $\vdash \neg(A \wedge \neg A)$.

Доказательство. По правилу рассуждения от противного достаточно доказать, что из $A \wedge \neg A$ выводятся две противоречивые формулы. Это верно по третьей и четвёртой аксиомам: из $A \wedge \neg A$ следуют и A, и $\neg A$. □

Утверждение 20. *Выводим закон добавления двойного отрицания:* $\vdash A \to \neg\neg A$.

Доказательство. По теореме о дедукции достаточно доказать $A \vdash \neg\neg A$, а для этого по правилу рассуждения от противного достаточно доказать, что из A и $\neg A$ выводятся две противоречивые формулы. Но это очевидно: сами A и $\neg A$ и будут такими формулами. $\square$

Утверждение 21. *Выводим закон снятия двух отрицаний из трёх:* $\vdash \neg\neg\neg A \to \neg A$.

Доказательство. Аналогично предыдущему, достаточно вывести противоречие из $\neg\neg\neg A$ и A. По предыдущему из A можно вывести $\neg\neg A$, т. е. мы вывели B и $\neg B$ для $B = \neg\neg A$. $\square$

Утверждение 22. *Выводим закон контрапозиции:* $\vdash (A \to B) \to (\neg B \to \neg A)$.

Доказательство. Двойным применением теоремы о дедукции получаем, что нам нужно доказать $A \to B, \neg B \vdash \neg A$. По правилу рассуждения от противного нужно вывести противоречие из $A \to B$, $\neg B$ и A. Это верно: можно вывести $\neg B$ как посылку и B по modus ponens. $\square$

Заметим, что если понимать отрицание как импликацию в тождественную ложь, то закон контрапозиции является следствием из силлогизма: $(A \to B) \to ((B \to \bot) \to (A \to \bot))$. Кроме того, закон можно преобразовать в правило: $\dfrac{\Gamma, A \vdash B}{\Gamma, \neg B \vdash \neg A}$.

Утверждение 23. *Выводим закон де Моргана про отрицание дизъюнкции:* $\vdash \neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$.

Доказательство. Здесь нужно вывести отдельно две импликации. Применив закон контрапозиции к шестой и седьмой аксиомам, получим $\vdash \neg(A \vee B) \to \neg A$ и $\vdash \neg(A \vee B) \to \neg B$. По теореме о дедукции получаем $\neg(A \vee B) \vdash \neg A$ и $\neg(A \vee B) \vdash \neg B$, затем по правилу вывода конъюнкции $\neg(A \vee B) \vdash (\neg A \wedge \neg B)$ и вновь по теореме о дедукции $\vdash \neg(A \vee B) \to (\neg A \wedge \neg B)$.

В обратную сторону нужно вывести противоречие из $\neg A \wedge \neg B$ и $A \vee B$. По правилу добавления конъюнкции достаточно вывести противоречие из $\neg A$, $\neg B$ и $A \vee B$. По правилу разбора случаев достаточно вывести противоречие отдельно из $\neg A, \neg B, A$ и из $\neg A, \neg B, B$. В каждом из вариантов противоречие уже есть среди посылок, и одно и то же противоречие (C и $\neg C$) получается по правилу вывода из противоречия. $\square$

До сих пор мы ни разу не использовали закон исключённого третьего. Для вывода многих формул без него обойтись невозможно. Мы будем использовать не закон в чистом виде, а правило из следующей теоремы:

Теорема 24. *Справедливо правило исчерпывающего разбора случаев:* $\dfrac{\Gamma, A \vdash C \quad \Gamma, \neg A \vdash C}{\Gamma \vdash C}$*;*

Доказательство. По правилу разбора случаев получаем $\Gamma, A \vee \neg A \vdash C$. Но $A \vee \neg A$ является аксиомой, поэтому её можно исключить из посылок. Действительно, та же самая цепочка формул будет выводом не только из $\Gamma \cup \{A \vee \neg A\}$, но и из Γ. Отметим, что тут можно сослаться и на правило сечения, ведь $\Gamma \vdash A \vee \neg A$. $\square$

Трудностью в применении правила исчерпывающего разбора случаев является то, что заранее не всегда ясно, какую формулу нужно взять, чтобы нужное утверждение выводилось и из неё, и из её отрицания. К счастью, как мы увидимо позже, можно просто перебирать значения всех переменных в формуле. Покажем, как это работает на примерах.

Утверждение 25. *Выводим закон снятия двойного отрицания:* $\vdash \neg\neg A \to A$.

Доказательство. По теореме о дедукции достаточно доказать $\neg\neg A \vdash A$. Добавим в список посылок поочерёдно A и $\neg A$. Тогда $\neg\neg A, A \vdash A$, т. к. A есть в списке посылок, а $\neg\neg A, \neg A \vdash A$ по правилу вывода из противоречия. По правилу исчерпывающего разбора случаев получаем $\neg\neg A \vdash A$, что и требовалось. □

Утверждение 26. *Выводима обратная контрапозиция:* $\vdash (\neg B \to \neg A) \to (A \to B)$.

Доказательство. По теореме о дедукции достаточно доказать $\neg B \to \neg A, A \vdash B$. Добавим в список посылок поочерёдно B и $\neg B$. Тогда $\neg B \to \neg A, A, B \vdash B$, т. к. B есть в списке посылок, а $\neg B \to \neg A, A, \neg B \vdash B$ по modus ponens и закону вывода из противоречия. По правилу исчерпывающего разбора случаев получаем $\neg B \to \neg A, A \vdash B$, что и требовалось. □

Утверждение 27. *Выводим закон де Моргана про отрицание конъюнкции:* $\vdash \neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$.

Доказательство. Справа налево закон выводится аналогично первому: нужно взять контрапозицию к третьей аксиоме $(A \wedge B) \to A$: $\neg A \to \neg(A \wedge B)$, аналогично получить $\neg B \to \neg(A \wedge B)$ и по правилу разбора случаев сделать вывод $(\neg A \vee \neg B) \to \neg(A \wedge B)$, что и требовалось.

В другую сторону без закона исключённого третьго не обойтись. По теореме о дедукции требуется доказать, что $\neg(A \wedge B) \vdash \neg A \vee \neg B$. Мы выведем из $\neg(A \wedge B)$ формулу $\neg\neg(\neg A \vee \neg B)$, а затем воспользуемся законом снятия двойного отрицания. Для этого нужно вывести противоречие из $\neg(A \wedge B)$ и $\neg(\neg A \vee \neg B)$. Применив закон контрапозиции к шестой и седьмой аксиомам, получим, что из $\neg(\neg A \vee \neg B)$ можно вывести $\neg\neg A$ и $\neg\neg B$. После снятия двойного отрицания получим A и B, откуда выведем конъюнкцию $A \wedge B$. Вместе с посылкой $\neg(A \wedge B)$ получим противоречие, что и требовалось. □

3.4 Вариации списка аксиом

Точный набор аксиом можно варьировать. Например, 10-я аксиома на самом деле выводится из остальных. Действительно, в теореме о дедукции она не используется, поэтому она эквивалентна такой выводимости: $A \to B, A \to \neg B \vdash \neg A$. А это получается по правилу исчерпывающего разбора случаев: вывод $\neg A, A \to B, A \to \neg B \vdash \neg A$ тривиален, а вывод $A, A \to B, A \to \neg B \vdash \neg A$ происходит так: по modus ponens получаем B и $\neg B$, откуда выводим $\neg A$ по правилу вывода из противоречия. Мы включили 10-ю аксиомы в список, потому что без 11-й аксиомы она не выводится, но и из неё самой нельзя вывести 11-ю. В частности, она нужна для интуиционистского исчисления высказываний. Исчисление, в котором нет ни 10-й, ни 11-й аксиомы, называется *минимальным*.

Чаще всего на какую-нибудь другую аксиому заменяют как раз 11-ю, т. е. закон исключённого третьего. Например, верны такие утверждения:

Утверждение 28. *Закон исключённого третьего можно вывести из аксиом 1–10 и закона снятия двойного отрицания.*

Доказательство. Как уже было замечено, из аксиом 1–10 можно вывести закон де Моргана $\neg(A\vee\neg A) \to (\neg A\wedge\neg\neg A)$. По правилу контрапозиции получаем $\neg(\neg A\wedge\neg\neg A) \to \neg\neg(A\vee\neg A)$. При помощи закона непротиворечия и modus ponens получаем $\neg\neg(A\vee\neg A)$. Сняв двойное отрицание, получаем то, что нужно. $\square$

Утверждение 29. *Закон снятия двойного отрицания можно вывести из аксиом 1–10 и закона обратной контрапозиции.*

Доказательство. Достаточно применить обратную контрапозицию к формуле $\neg A \to \neg\neg\neg A$, которая есть закон навешивания двойного отрицания. $\square$

Утверждение 30. *Закон исключённого третьего можно вывести из аксиом 1–10 и формулы* $(\neg A \to A) \to A$.

Доказательство. Подставим закон исключённого третьего вместо A: $(\neg(A \vee \neg A) \to (A\vee\neg A)) \to (A\vee\neg A)$. По закону де Моргана выполнено $\neg(A\vee\neg A) \to (\neg A\wedge\neg\neg A)$. Также по теореме о дедукции, девятой аксиоме и правилу разбиения конъюнкции выводимо $(\neg A\wedge\neg\neg A) \to B$, в частности, $(\neg A\wedge\neg\neg A) \to (A\vee\neg A)$. По правилу силлогизма получаем $\neg(A \vee \neg A) \to (A \vee \neg A)$. Применив modus ponens к последней и исходной формулам, получаем $A \vee \neg A$, что и требовалось. $\square$

Утверждение 31. *Закон исключённого третьего можно вывести из аксиом 1–10 и* закона Пирса $((A \to B) \to A) \to A$.

Доказательство. Идея доказательства такова: если взять в качестве B тождественную ложь, то закон Пирса сведётся к предыдущей формуле, ведь формулы $\neg A$ и $A \to \perp$ эквивалентны. Однако в нашем языке нет константы $\perp$, так что мы её заменим на $A \wedge \neg A$: $(((A \vee \neg A) \to (A \wedge \neg A)) \to (A \vee \neg A)) \to (A \vee \neg A)$. При помощи десятой аксиомы выводим $((A \vee \neg A) \to (A \wedge \neg A)) \to \neg(A \vee \neg A)$: из $(A \vee \neg A) \to (A \wedge \neg A)$ и $A \vee \neg A$ выводятся A и $\neg A$. Поскольку $\neg(A \vee \neg A) \to (A \vee \neg A)$ уже выведено, по правилу силлогизма получаем $(((A \vee \neg A) \to (A \wedge \neg A)) \to (A \vee \neg A))$. Теперь получаем $A \vee \neg A$ вновь по modus ponens. $\square$

Закон Пирса важен, поскольку он использует только импликацию, но при этом эквивалентен закону исключённого третьего (при наличии остальных аксиом). Можно доказать, что любую тавтологию, состоящую только из импликаций, можно вывести из первых двух аксиом и закона Пирса. Это будет теоремой о полноте импликативного исчисления высказываний. Мы её доказывать не будем, вместо этого докажем полноту для обычного исчисления высказываний.

4 Полнота исчисления высказываний

В этом разделе мы докажем теорему о полноте: все тавтологии выводимы. Мы начнём с леммы, в которой 14 утверждений, но все либо простые, либо очень простые. В дальнейшем будем называть эту лемму базовой.

Лемма 32 (базовая)**.** *Имеют место следующие выводимости:*

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

Поясним смысл леммы. Слева от знака выводимости стоят либо формулы A и B, либо их отрицания. Справа стоит более сложная формула, либо её отрицание в зависимости от того, что из двух верно, когда верны обе посылки. Можно сказать, что лемма моделирует вычисление значения по таблице истинности через выводимость.

Доказательство. Первая выводимость про конъюнкцию следует из пятой аксиомы, остальные получаются контрапозицией из третьей или четвёртой аксиом.

Первые три выводимости про дизъюнкцию следуют из шестой и седьмой аксиом. Последняя выводится так: добавим в список посылок $A \vee B$, далее по правилу разбора случаев нужно вывести противоречие и из $\neg A, \neg B, A$, и из $\neg A, \neg B, B$. В каждом из случаев противоречие есть прямо в списке посылок.

Первая, третья и четвёртая выводимости про импликацию следуют из первой и девятой аксиом. Вторая выводится так: добавим в список посылок $A \to B$, по modus ponens выводится B, а $\neg B$ уже есть в списке посылок. Значит, противоречие выведено, что и требовалось.

Первая выводимость про отрицание уже доказана, вторая тривиальна. □

Следующая лемма обобщает предыдущую.

Лемма 33 (основная)**.** *Пусть A — формула, $x \in \{0,1\}$. Через A^x обозначим формулу A, если $x = 1$, и формулу $\neg A$, если $x = 0$. Далее, пусть φ — формула от n переменных, выражающая функцию f. Тогда для всех формул $A_1, \ldots, A_n$ и значений $x_1, \ldots, x_n$ выполнено*

$$A_1^{x_1}, \ldots, A_n^{x_n} \vdash \varphi(A_1, \ldots, A_n)^{f(x_1,\ldots,x_n)}.$$

Доказательство. Будем доказывать утверждение индукцией по построению формулы. В качестве базы можно было бы взять базовую лемму, но мы сделаем ещё один шаг назад. Пусть φ — переменная, т. е. $\varphi(A_1, \ldots, A_n) = A_i$. В таком случае f — проектор, т. е. $f(x_1, \ldots, x_n) = x_i$ и в правой части стоит просто одна из посылок.

Теперь докажем переход. Для разных связок он делается одинаково, возьмём для примера конъюнкцию. Таким образом, формула φ есть конъюнкция $\gamma \wedge \eta$, а функция f есть также конъюнкция функций g и h, но уже в смысле булевой функции, а не синтаксической связки. По предположению индукции имеем $A_1^{x_1}, \ldots, A_n^{x_n} \vdash \gamma(A_1, \ldots, A_n)^{g(x_1,\ldots,x_n)}$ и $A_1^{x_1}, \ldots, A_n^{x_n} \vdash \eta(A_1, \ldots, A_n)^{h(x_1,\ldots,x_n)}$. Далее, по базовой лемме имеем

$$\gamma(A_1, \ldots, A_n)^{g(x_1,\ldots,x_n)}, \eta(A_1, \ldots, A_n)^{h(x_1,\ldots,x_n)} \vdash (\gamma \wedge \eta)(A_1, \ldots, A_n)^{(g \wedge h)(x_1,\ldots,x_n)}.$$

Последняя формула есть $\varphi(A_1, \ldots, A_n)^{f(x_1,\ldots,x_n)}$. По правилу сечения получаем, что $A_1^{x_1}, \ldots, A_n^{x_n} \vdash \varphi(A_1, \ldots, A_n)^{f(x_1,\ldots,x_n)}$, что и требовалось. Переходы для остальных связок доказываются аналогично. Таким образом, индуктивное утверждение доказано. □

Теперь мы докажем теорему о полноте.

Теорема 34 (о полноте исчисления высказываний)**.** *Пусть формула φ, зависящая от переменных $p_1, \ldots, p_n$, является тавтологией. Тогда $\vdash \varphi$.*

Доказательство. Поскольку формула φ является тавтологией, она выражает функцию f, тождественно равную единице. По основной лемме для любого набора $(x_1, \ldots, x_n) \in \{0,1\}^n$ выполнено $p_1^{x_1}, \ldots, p_n^{x_n} \vdash \varphi$. При помощи обратной индукции мы докажем, что для каждого k от n до 0 выполнено $p_1^{x_1}, \ldots, p_k^{x_k} \vdash \varphi$. Начальное утверждение (для $k = n$) у нас уже есть. Конечное (для $k = 0$) утверждает $\vdash \varphi$, что и требуется. Осталось доказать переход.

Пусть для некоторого k утверждение уже доказано. Докажем для $k-1$. Из полученного имеем, что $p_1^{x_1}, \ldots, p_{k-1}^{x_{k-1}}, p_k \vdash \varphi$ и $p_1^{x_1}, \ldots, p_{k-1}^{x_{k-1}}, \neg p_k \vdash \varphi$. По правилу исчерпывающего разбора случаев получаем $p_1^{x_1}, \ldots, p_{k-1}^{x_{k-1}} \vdash \varphi$, что и требовалось. Таким образом, теорема о полноте доказана. □

5 Непротиворечивость и совместность

Доказательство теоремы о полноте в предыдущем параграфе существенно опиралось на интерпретацию тавтологий через таблицы истинности. Поэтому оно не обобщается на другие разделы, такие как логика предикатов, интуиционистская логика, модальные логики и т. п. В этом разделе мы изучим другой способ доказательства, который обобщается на эти случаи, но также интересен и сам по себе. Начнём с определений.

Определение 35. Множество пропозициональных формул Γ называется *совместным* (satisfiable, semantically consistent), если все формулы из Γ могут быть одновременно истинными на некотором наборе.

Определение 36. Множество пропозициональных формул Γ называется *противоречивым* (inconsistent), если из него выводится некоторая формула B и её отрицание, и *непротиворечивым* (consistent) в противном случае.

Заметим, что первое из этих определений семантическое, т. е. говорит о значениях формул — таблицах истинности, а второе — синтаксическое, т. е. говорит о самих формулах и их последовательностях. Мы докажем, что эти понятия тесно друг с другом связаны:

Теорема 37. *Множество Γ непротиворечиво тогда и только тогда, когда оно совместно.*

Прежде, чем доказывать эту теорему, покажем, как из неё следуют теоремы о корректности и полноте.

Утверждение 38. *Из теоремы 37 следуют теоремы о корректности и о полноте.*

Доказательство. Пусть формула φ выводима. В таком случае множество $\{\neg\varphi\}$ противоречиво: из него выводится как сама φ (она выводится из любого множества), так и $\neg\varphi$ (она есть в списке посылок). По контрапозиции к теореме 37 множество $\{\neg\varphi\}$ несовместно. Это означает, что ни на каком наборе $\neg\varphi$ не будет истинным. Поэтому φ, напротив, всюду истинно, т. е. φ — тавтология.

Пусть теперь φ — тавтология. В таком случае множество $\{\neg\varphi\}$ несовместно. По контрапозиции к теореме 37 оно будет противоречивым. Отсюда по правилу рассуждения от противного выводится $\neg\neg\varphi$, а по закону снятия двойного отрицания выводится и сама φ, что и требовалось. □

Перейдём к доказательству самой теоремы.

Доказательство теоремы 37. Доказательство будет состоять из нескольких лемм.

Лемма 39. *Если $\Gamma \vdash A$ и на некотором наборе значений $\mathbf{x}$ все формулы из Γ истинны, то и формула A на этом наборе истинна.*

Доказательство. Эта лемма аналогична теореме о корректности. Посмотрим на вывод формулы A. Каждая его формула либо является аксиомой и потому истинна на любом наборе, в том числе на $\mathbf{x}$, либо принадлежит Γ, и потому тоже истинна на $\mathbf{x}$, либо получена из двух более ранних по правилу modus ponens. В этом случае эти формулы истинны на $\mathbf{x}$ по предположению индукции, и потому новая формула также истинна. □

Теперь мы уже можем доказать, что любое совместное множество непротиворечиво. Действительно, пусть Γ совместно, но противоречиво. Тогда все формулы из Γ истинны на некотором наборе $\mathbf{x}$, но при этом $\Gamma \vdash B$ и $\Gamma \vdash \neg B$. По предыдущей лемме и B, и $\neg B$ должны быть истинны на наборе $\mathbf{x}$. Но это невозможно, поэтому совместное Γ противоречивым быть не может.

В обратную сторону доказательство посложнее. Идея его такова: сначала расширим произвольное непротиворечивое множество Γ до полного непротиворечивого множества Δ, а затем докажем, что Δ совместно.

Определение 40. Непротиворечивое множество Δ называется *полным* (complete), если для любой формулы φ выполнено либо $\Delta \vdash \varphi$, либо $\Delta \vdash \neg\varphi$.

Доказанная нами основная лемма позволяет упростить определение:

Лемма 41. *Непротиворечивое множество Δ полно тогда и только тогда, когда для любой переменной p выполнено либо $\Delta \vdash p$, либо $\Delta \vdash \neg p$.*

Доказательство. В одну сторону это верно, т. к. переменная является формулой. В другую сторону: для каждой переменной, входящей в формулу, выводится либо она, либо её отрицание. По основной лемме из этих литералов выводится либо φ, либо $\neg\varphi$. По правилу сечения получаем, что φ или $\neg\varphi$ выводится из Δ, что и требовалось. □

Перейдём к основной линии доказательства.

Лемма 42. *Для любого непротиворечивого множества Γ найдётся полное непротиворечивое множество $\Delta \supset \Gamma$.*

Доказательство. Доказательство проведём для конечного или счётного числа переменных $p_1, p_2, p_3, \ldots$. Доказательство для произвольного множества переменных также возможно, но лишь с использованием леммы Цорна.

Будем рассматривать все переменные по очереди. Если уже верно $\Gamma \vdash p_i$ или $\Gamma \vdash \neg p_i$, то ничего менять не будем. Иначе добавим в Γ переменную p_i в качестве формулы. Таким образом, получим семейство $\Gamma_0 \subset \Gamma_1 \subset \Gamma_2 \subset \ldots$, где $\Gamma_0 = \Gamma$, а далее

$$\Gamma_k = \begin{cases} \Gamma_{k-1}, & \text{если } \Gamma_{k-1} \vdash p_i \text{ или } \Gamma_{k-1} \vdash \neg p_i, \\ \Gamma_{k-1} \cup \{p_k\}, & \text{иначе.} \end{cases}$$

Положим $\Delta = \bigcup_{k=0}^{\infty} \Gamma_k$. Покажем, что Δ искомое. Сначала докажем по индукции, что все Γ_k непротиворечивы. Действительно, Γ_0 непротиворечиво по определению. Далее, множество Γ_{k+1} либо совпадает с Γ_k и потому непротиворечиво, либо равно $\Gamma_k \cup \{p_{k+1}\}$. Если оно противоречиво, то по правилу рассуждения от противного $\Gamma \vdash \neg p_{k+1}$, но в этом случае Γ_{k+1} совпало бы с Γ_k. Значит, Γ_{k+1} непротиворечиво и переход индукции доказан.

Теперь покажем, что и само Δ непротиворечиво. Действительно, если бы противоречие выводилось, то в выводе было бы задействовано конечное число формул, ведь сам вывод — конечная последовательность формул. Но тогда все эти формулы содержались бы уже в Γ_k при достаточно большом k. А тогда само Γ_k было бы противоречивым, но это не так, как мы уже убедились.

Полнота Δ получается из того, что для каждой переменной выводится либо она, либо её отрицание. Таким образом, Δ непротиворечивое и полное, что и требовалось. $\square$

Лемма 43. *Всякое полное непротиворечивое множество Δ совместно.*

Доказательство. Найдём выполняющий набор следующим образом: для каждой переменной p, если $\Delta \vdash p$, положим $p = 1$, а если $\Delta \vdash \neg p$, положим $p = 0$. Покажем, что он в самом деле выполняющий. Действительно, пусть $\varphi \in \Delta$, но $\varphi = 0$ на этом наборе. В таком случае по основной лемме $\Delta \vdash \neg\varphi$. Но тогда Δ противоречиво: оно содержит φ, и из него выводится $\neg\varphi$. Поскольку Δ непротиворечиво, формула φ должна быть истинной на построенном наборе, что и требовалось. $\square$

Итак, произвольное непротиворечивое множество Γ расширено до Δ, которое оказалось совместным. Значит, исходное Γ также было совместным, что и требовалось в теореме о полноте. $\square$

6 Семантическое следование

Мы доказали, что выводимость формулы эквивалентна её тавтологичности. Но это верно только для простой выводимости. Для выводимости из посылок также есть аналог, который называется семантическим следованием (semantic consequence).

Определение 44. Из множества формул Γ семантически следует φ, если на любом наборе $\mathbf{x}$, на котором верны все формулы из Γ, φ также верна. Обозначение: $\Gamma \vDash \varphi$.

Таким образом, тавтологичность эквивалентна семантическому следованию из пустого множества и потому обозначается $\vDash \varphi$. Лемма 39 фактически гласит, что из $\Gamma \vdash \varphi$ следует $\Gamma \vDash \varphi$. Рассуждения из предыдущего раздела позволяют доказать и обратное.

Теорема 45. *Если* $\Gamma \vDash \varphi$, *то* $\Gamma \vdash \varphi$.

Доказательство. Если $\Gamma \vDash \varphi$, то $\Gamma \cup \{\neg\varphi\}$ не совместно. Действительно, если все формулы из Γ выполнены, то $\neg\varphi$ выполнить не получится. По контрапозиции к теореме 37 $\Gamma \cup \{\neg\varphi\}$ будет противоречивым. В таком случае, как и раньше, $\Gamma \vdash \neg\neg\varphi$, откуда $\Gamma \vdash \varphi$, что и требовалось. □

7 Теорема о компактности и её применения

В математическом анализе известно понятие *компактности* (compactness) множества: из любого покрытия этого множества открытыми множествами можно выбрать конечное подпокрытие. Похожую ситуацию мы увидели в исчислении высказываний: из любого противоречивого множества можно выбрать конечное противоречивое подмножество. Эквивалентность противоречивости и несовместности позволяет доказать такую теорему:

Теорема 46 (о компактности для исчисления высказываний)**.** *Пусть любое конечное подмножество множества* Γ *совместно. Тогда и всё множество* Γ *совместно.*

Доказательство. Если всё множество Γ несовместно, то оно противоречиво. Но тогда в нём есть конечное противоречивое подмножество. Но тогда оно несовместно, что противоречит условию. □

Теорема о компактности позволяет доказать разнообразные результаты для бесконечных объектов. Главное требование заключается в том, чтобы свойства этих объектов можно было записать пропозициональными формулами. Приведём несколько примеров.

7.1 Раскраска обобщённых графов

Определение 47. *Обобщённым неориентированным графом* назовём пару (V, E), где V — произвольное множество, а E — симметричное антирефлексивное отношение на V. Элементы множества V называются *вершинами*, элементы множества E — рёбрами.

Заметим, что термин «обобщённый граф» (generalized graph) используется в самых разных смыслах. У нас обобщение в сторону бесконечного числа вершин, но также могут добавляться веса рёбер, гиперрёбра из более, чем двух вершин, и т. д.

Определение 48. Правильной раскраской обобщённого графа (V, E) в два цвета называется функция $c\colon V \to \{0, 1\}$, такая что у любого ребра $e = (x, y) \in E$ вершины покрашены в разные цвета, т. е. $c(x) \neq c(y)$.

Раскрашиваемость в два цвета также естественно называть *двудольностью* (bipartiteness). В одну долю соберём все вершины одного цвета, в другую — все вершины другого. Получим, что рёбра идут только между долями, а не внутри них. Как и для обычных графов, для обобщённых верна такая теорема:

Теорема 49. *Обобщённый граф можно правильно раскрасить в два цвета тогда и только тогда, когда он не содержит циклов нечётной длины.*

Доказательство. Для конечных графов будем считать теорему известной. Для обобщённого графа сделаем следующее: каждой вершине сопоставим переменную p, а каждой паре вершин — формулу $(p \wedge \neg q) \vee (\neg p \wedge q)$. Значение переменной будем интерпретировать как цвет, в который покрашена вершина. Формула означает, что соседние вершины покрашены в разные цвета. Совместность конечного подмножества этих формул соответствует раскрашиваемости конечного подграфа. Поскольку во всём графе нет нечётных циклов, то и в любом конечном подграфе их тем более нет. Значит, любой конечный граф раскрашивается, т. е. любое конечное подмножество формул совместно. Значит, все формулы совместны, т. е. весь граф раскрашивается. $\square$

Аналогичную теорему можно доказать для раскрашивания в несколько цветов: если любой конечный подграф можно покрасить в k цветов, то и весь граф можно раскрасить. Важный пример из комбинаторики — подсчёт хроматических чисел пространств. Это число — минимальное количество цветов, в которое можно покрасить точки евклидова пространства, так чтобы точки одного цвета не отстояли друг от друга на расстояние 1. Фактически это задача о раскраске дистанционного графа, в котором рёбрами соединены все пары точек на расстоянии 1. Теорема о компактности показывает, что достаточно решить задачу только для конечных графов. Тем не менее, задача не решена даже для плоскости: хроматическое число лежит в диапазоне от 5 до 7, причём пример для 5 цветов был построен только в 2018 году.

7.2 Определимость наборов присваиваний

Теперь поговорим об определимости. Неформально вопрос такой: можно ли бесконечную таблицу истинности выразить пропозициональными формулами? Формальное определение такое:

Определение 50. Пусть $\mathcal{V}$ — некоторое множество пропозициональных переменных. *Присваиванием* (assignment) называется произвольное отображение из $\mathcal{V}$ в $\{0, 1\}$. Множество присваиваний A называется *определимым* (definable), если существует такое множество (конечных) пропозициональных формул Γ, что $x \in A$ тогда и только тогда, когда все формулы из Γ истинны на x.

Мы будем интерпретировать присваивание f как строку в таблице истинности: если $f(p) = 1$, то переменная истинна, иначе ложна. Можно считать, что присваивание записывает единицу в эту строку. Ну а множество присваиваний записывает единицы во все строки, которые оно содержит.

Если переменных конечное число, то любое множество присваиваний определимо. Действительно, при нашей интерпретации множество присваиваний определяет таблицу истинности. Её можно задать некоторой формулой, которая и определит наше множество.

Если переменных счётное число, то из соображений мощности определимо уже не любое множество присваиваний. Дело в том, что всех присваиваний в этом случае континуум, а потому всех множеств присваиваний больше континуума. С другой стороны, всех формул счётное число, поэтому всех множеств формул континуум. Поскольку каждое множество формул задаёт только одно множество присваиваний, на все множества присваиваний множеств формул не хватит.

Тем не менее, любое конечное множество присваиваний определимо и для счётного числа переменных. Действительно, одно присваивание определимо: достаточно для каждой переменной взять p, если p в этом присваивании истинна, и $\neg p$, если ложна (получится счётное множество формул, каждая из которых будет литералом). Конечное число присваиваний определимо по следующей причине: если заранее известно, что присваивание лежит в этом множестве, то значения некоторого конечного числа переменных (например, $p_1, \ldots, p_n$) определят значения всех остальных. Например, два присваивания должны отличаться в значениях некоторой переменной, и одна эта переменная их и отличит. Можно написать одну формулу, которая определит допустимые значения этих переменных, а далее для каждого присваивания f и каждой последующей переменной q написать формулу, которая будет означать, что из $f(p_1), \ldots, f(p_n)$ следует $f(q)$.

С другой стороны, счётное множество присваиваний уже может быть неопределимо (и это не выводится из соображений мощности). Например, рассмотрим множество $\{100000\ldots, 110000\ldots, 111000\ldots, \ldots\}$ Пусть оно определяется множеством формул Γ. Любое его конечное подмножество использует лишь конечное число переменных, а значит, все его формулы должны быть истинными на наборе из всех единиц. Но тогда по теореме о компактности и все формулы множества будут истинными на наборе из всех единиц. Но такого присваивания не было в исходном множестве, значит, исходное множество неопределимо.

7.3 Лемма Кёнига

Теорему о компактности часто неудобно применять непосредственно. Есть эквивалентный инструмент, который гораздо удобнее применять. Это лемма Кёнига: в любом бесконечном дереве с конечным ветвлением есть бесконечная ветвь. Мы формализуем все эти понятия, сформулируем лемму, а затем докажем эквивалентность.

Определение 51. Пусть задан некоторый алфавит Σ (не обязательно конечный и даже не обязательно счётный). *Деревом* (tree) называется подмножество T множества Σ^*, такое что если некоторое слово x принадлежит T, то и все префиксы x принадлежат T. Дерево имеет *конечное ветвление* (finite branching), если для любого $x \in T$ лишь для конечного числа $a \in \Sigma$ выполнено $xa \in T$. *Бесконечной ветвью* (infinite branch) в дереве T называется последовательность $\omega \in \Sigma^\infty$, такая что любой конечный префикс ω лежит в T.

Интерпретация множества T в виде дерева такова: в корне дерева стоит пустое слово, дальше идут все возможные однобуквенные слова из T, дальше от каждого однобуквенного все возможные двухбуквенные продолжения, и так далее. В каждой вершине ветвление конечно, однако общего ограничение на число ветвей может не быть, поэтому нужен счётный алфавит. Несчётный алфавит по сути не нужен: при конечном ветвлении всё равно общее число вершин и, как следствие, используемых символов будет счётным.

Теорема 52 (Лемма Кёнига)**.** *Если дерево T бесконечно (как множество) и имеет конечное ветвление, то в нём найдётся бесконечная ветвь.*

Из соображений мощности легко вытекает, что в бесконечном дереве с конечным ветвлением есть сколь угодно длинные ветви. Однако объяснить, почему они образуют общую бесконечную, не так легко.

Доказательство. Введём булеву переменную p_x для каждой вершины x дерева T, которая предполагается истинной, если данная вершина входит в бесконечную ветвь, и ложной, если не входит. Далее запишем два семейства формул: первое будет говорить, что на каждом уровне дерева лежит ровно одна вершина, второе — что эти вершины образуют ветвь. Первое семейство будет состоять из строгих дизъюнкций всех переменных на одном уровне, т. е. формул вида $\bigvee_{x \in T \cap \Sigma^n} (p_x \wedge \bigwedge_{y \in (T \cap \Sigma^n) \setminus \{x\}} \neg p_y)$. Формула из второго семейства будет выглядеть так: $p_x \to \bigvee_{a \in \Sigma, xa \in T} p_{xa}$, т. е. если некоторая вершина лежит на ветви, то один из её непосредственных потомков также лежит.

Из конечного ветвления следует, что на каждом уровне лежит лишь конечное число вершин. Как следствие, на каждом уровне есть хотя бы одна вершина: иначе все вершины были бы на предыдущих уровнях, и потому их было бы конечное число. Значит, любое конечное подмножество построенных формул совместно: нужно взять максимальный уровень, переменная с которого встречается в этих формулах, найти вершину x из T на этом уровне, сделать истинными переменные, соответствующие всем её префиксам, а остальные сделать ложными. Все формулы из первого семейства будут говорить про этот или меньшие уровни и потому будут верны: есть ровно один префикс x данной длины. Все формулы из второго семейства будут также верны: если посылка будет истинна, то данная вершина будет префиксом x (причём собственным). Префикс x на единицу большей длины будет непосредственным потомком данной вершины. А переменная, ему соответствующая, будет также истинна.

Таким образом, любое конечное подмножество и правда совместно. Значит, и всё множество совместно. Покажем, что слова, которым соответствуют истинные переменные, образуют бесконечную ветвь. Действительно, докажем по индукции, что на k-м месте у всех таких слов, которые не короче k, стоит один и тот же символ. Для длины k это следует из единственности слова на k-м уровне. Если это верно для длин $k, \dots, m$, то верно и для длины $m+1$: в этой длине также есть единственное слово, причём оно должно быть продолжением уже полученного слова длины m. Значит, на k-м месте в нём стоит тот же символ. Значит, все слова будут префиксами одной и той же бесконечной последовательности. А поскольку в каждой длине есть ровно одно слово, эта последовательность и будет бесконечной ветвью. □

Можно провести и обратное рассуждение: вывести теорему о компактности из леммы Кёнига.

Доказательство теоремы о компактности через лемму Кёнига. Изначально в множестве Γ может быть несколько (и даже бесконечное число) формул, выражающих одну и ту же функцию. Ясно, что достаточно для каждой функции оставить только одну формулу и доказывать теорему для уменьшенного множества. Включим в дерево T все кортежи булевых значений $(a_1, \dots, a_k)$, такие что все формулы из Γ, зависящие только от переменных $p_1, \dots, p_k$, истинны на этих наборах. Обозначим множество таких формул через Γ_k. Поскольку после уменьшения Γ множество Γ_k будет конечным, оно будет совместным по предположению теоремы о компактности. Иными словами, хотя бы один такой кортеж найдётся.

Все указанные кортежи действительно образуют дерево: если все формулы из Γ_m верны на кортеже $(a_1, \dots, a_m)$, то и все формулы из $\Gamma_k \subset \Gamma_m$ $(k < m)$ верны на том же кортеже, а значит, и на кортеже $(a_1, \dots, a_k)$. Поскольку для каждой длины найдётся хотя бы один кортеж, это дерево будет бесконечным. По лемме Кёнига в нём найдётся бесконечная ветвь $(a_1, a_2, \dots)$. Эта ветвь задаст выполняющий набор для всех формул из Γ. Действительно, каждая формула зависит только от конечного числа переменных, т. е. входит в некоторое Γ_k. По построению она должна быть верна на значениях $(a_1, \dots, a_k)$, т. е. и на нашем бесконечном наборе. Таким образом, на нём верны все формулы, т. е. Γ совместно, что и требовалось. □

Для полноты изложения приведём непосредственное доказательство леммы Кёнига.

Непосредственное доказательство леммы Кёнига. Будем строить последовательность ω по индукции. Будем поддерживать такое условие: для префикса ω_k длины k в дереве T найдётся бесконечное число слов, продолжающих этот префикс. Для $k = 0$ это следует из бесконечности всего дерева. Далее, пусть для ω_k условие установлено. Из конечности ветвления есть только конечное число символов $a \in \Sigma$, таких что $\omega_k a \in T$. Любой элемент T длиннее k, продолжающий ω_k, должен начинаться с одного из таких слов. Значит, хотя бы одно из слов $\omega_k a$ будет продолжаться бесконечным числом разных элементов T. Именно его мы и возьмём в качестве ω_{k+1}. □

Заметим напоследок, что в больших мощностях лемма Кёнига может быть неверна. Например, доказано существование *деревьев Ароншайна* (Aronszajn tree), т. е. несчётных деревьев, не имеющих несчётных ветвей. Для конкретных мощностей существование или несуществование таких деревьев может быть независимо от других аксиом теории множеств и вытекать из континуум-гипотезы и более сложных дополнительных предположений. Впрочем, даже строгое определение понятия дерева в общем случае требует инструментария вполне упорядоченных множеств, которые мы пока не изучили.

7.4 Замощения плоскости

Известно множество способов замостить плоскость копиями одной или нескольких фигур. Самые интересные замощения — непериодические. Их существование доказывается так: с одной стороны, по каким-то соображениям периодического замощения быть не может. С другой стороны, какое-то замощение есть. Существование замощения может доказываться при помощи самоподобия: несколько фигур вместе образуют бóльшие фигуры, которые друг с другом стыкуются так же, как и маленькие. Это позволяет доказать, что сколь угодно большой кусок плоскости замостить можно. Теорема о компактности позволяет сделать вывод, что и всю плоскость можно замостить. Мы проведём это рассуждение для квадратных плиток с раскрашенными сторонами, а затем распространим его на произвольные многоугольники.

Определение 53. Пусть задано некоторое конечное множество цветов $\mathcal{C}$. *Плиткой* (tile) назовём квадрат с заданными цветами сторон. Формально это просто четвёрка $(c_t, c_b, c_l, c_r) \in \mathcal{C}^4$ (заданы цвета верхней, нижней, левой и правой сторон соответственно).

Определение 54. Пусть задано множество плиток $C \subset \mathcal{C}^4$. *Замощением* (tiling) плоскости называется отображение $F\colon \mathbb{N}^2 \to C$. Замощение называется *правильным*, если для всех x, y выполнено $F(x,y)_t = F(x, y+1)_b$ и $F(x.y)_r = F(x+1, y)_l$. Неформально плитки стыкуются по сторонам одинаковыми цветами. Аналогично определяются замощение и правильное замощение квадрата $\{0, 1, \ldots, n\}^2$. Разумеется, в этом случае цвета должны совпадать только вдоль границ внутри квадрата.

Обратите внимание, что при таком определении плитки нельзя вращать или переворачивать.

Теорема 55. *Если существуют правильные замощения сколь угодно больших квадратов, то существует правильное замощение и всей плоскости.*

Доказательство. Введём переменные $p_{x,y,c}$ для всех $x, y \in \mathbb{N}$ и $c \in C$. Истинность этой переменной будет означать, что в клетке (x, y) стоит плитка c. Правильность замощения будет гарантирована следующими формулами. Во-первых, в каждой клетке должна стоять ровно одна плитка. Для этого для каждой пары (x, y) пишется формула $\bigvee_{c \in C} \left(p_{x,y,c} \wedge \bigwedge_{d \neq c} \neg p_{x,y,d}\right)$. Во вторых, клетки должны стыковаться. Для этого пишутся формулы $\bigvee_{c,d \in C\colon c_t = d_b} (p_{x,y,c} \wedge p_{x,y+1,d})$ и $\bigvee_{c,d \in C\colon c_r = d_l} (p_{x,y,c} \wedge p_{x+1,y,d})$. Любое конечное множество этих формул совместно: все клетки, о которых идёт речь, можно заключить в один большой квадрат. Поскольку его можно замостить, соответствующие значения будут выполняющим набором. Значит, и все формулы сразу совместны. Значит, всю плоскость можно замостить. □

Раскрашенные плитки можно заменить на многоугольники: каждому цвету нужно сопоставить уникальный центрально симметричный рисунок границы. Принцип «достаточно замостить сколь угодно большой квадрат» верен и для произвольных многоугольников.

Теорема 56. *Если набором многоугольников можно замостить любой квадрат (без перекрытий, но с возможными выходами за пределы квадрата), то ими можно замостить и всю плоскость.*

Идея доказательства. Проблема заключается в том, что многоугольники можно сдвигать на произвольные вектора и поворачивать на произвольные углы. Поэтому положений для каждого многоугольника, вообще говоря, континуум. В том числе и возможных положений одного многоугольника относительно другого. Но вариантов корректно «обложить» один многоугольник лишь конечное число. Таким образом от замощения можно перейти к графу, описывающему взаимное расположение многоугольников. Требуется записать формулами корректность этого графа. □