Глава 1

Введение в логику

Эта глава является базовой. В ней вводятся основные логические понятия: высказывания, предикаты, логические связки и кванторы. После неформального обсуждения необходимости формализации математики, напоминаются основные факты из теории множеств. Затем подробно разбираются свойства логических связок и понятие логического следствия. Различные тождества, которые мы докажем, будут активно использоваться на протяжении всей книги.

Последние три раздела более формальные. В них определяются сигнатура теории, понятие интерпретации и языка на котором задано исчисление, позволяющее выводить новые формулы.

Важную роль играют задачи. Некоторые из них приведены в тексте и помечены символом $\lessdot\mathrm{H}_n$, где $n \in \mathbb{N}_+$ – номер решения в приложении "Помощь", стр. 185. Остальные задачи собраны в конце главы.

Логика, физика и искусственный разум

Сергей С. Степанов

Книга находится в процессе создания. Её последняя версия и другие материалы выкладываются на сайт: http://synset.com. Замеченные ошибки и вопросы просьба присылать по адресу: steps137, затем собачка и gmail.com.

1.1 Формализация математики

• В математике аксиомы *определяют* объекты и их свойства. Новые утверждения (теоремы) *доказываются* при помощи логических рассуждений. Подобная схема впервые проявилась в книгах Евклида, в частности, при описании геометрии.

Пятая аксиома о параллельных прямых (не имеющих общей точки) выглядела сложнее остальных аксиом: "через всякую точку, не лежащую на данной прямой, проходит только одна, параллельная ей прямая". На протяжении более двух тысячелетий длилась безрезультатная борьба за её доказательство (вывод из остальных аксиом). Пятая аксиома оказалась всё же независимой, однако попытки построить её доказательство привели к неевклидовым геометриям и более глубокому пониманию как структуры математического здания, так и возможных свойств физического пространства.

Впрочем, на самом деле "доказательств" было множество. Внешне они выглядели безупречными, однако при более внимательном рассмотрении выяснялось, что в них неявно используется то или иное очень "естественное" допущение. Например, что может быть "очевиднее" существования треугольников со сколь угодно большой площадью? Однако нет ничего более неочевидного, чем очевидные истины.

Со временем возникла потребность так формализовать теории и методы доказательств, чтобы ни какие незаметно привнесённые "очевидности" не портили её логической стройности. В частности, по-возможности необходимо отказаться от естественного языка с присущей ему неоднозначностью. Блестящим примером подобного подхода явились "Основания геометрии" и последующие работы Давида Гильберта.

Геометрия на плоскости родилась из построений при помощи линейки и циркуля. С формальной точки зрения это теория о точках и прямых. Эти сущности или *предметы* не наделяются образными свойствами ("не имеет ширины" и т.п). Просто рассматриваются объекты двух видов. Первые обозначаются латинскими буквами x, y,... и называются точками, а вторые – греческими α, β,... и называются прямыми.

Предметы вступают в определённые отношения, которые в геометрии соответствуют словам "лежать", "параллельны", "между" и т.д. Чтобы избежать неоднозначности естественного языка, эти отношения записывают при помощи формальных обозначений. Например, фразы "точка x лежит на прямой α" или "прямая α проходит через точку x" кодируются функцией с именем "$\in$". Она имеет два аргумента. Первый – имя точки, а второй – имя прямой: $\in(x, \alpha)$.

Для данных x и α такая функция считается либо истинным утверждением (если x действительно принадлежит α), либо ложным (в противном случае). Подобные логические функции, значения которых бинарны (истина/ложь) называются *предикатами*. Их аргументы – это *предметные* величины, т.е. сущности с которыми оперирует теория.

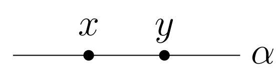
Предикаты с двумя аргументами часто записывают в *операционном* виде, когда имя предиката помещается между его аргументами как операция. Так, $x \in \alpha$ – это то-же, что и $\in (x, \alpha)$.

При помощи одних предикатов (отношений между объектами = логических функций = высказываний об объектах) можно определять другие. Для этого вводятся формальные замещения слов “И”, “ИЛИ”, “НЕ”:

$A \,\&\, B$	:	“И”	(и A, и B, т.е. оба);
$A \vee B$	:	“ИЛИ”	(или A, или B, или оба, т.е. хотя бы одно);
$\neg A$	:	“НЕ”	(не A; если A истинно, то $\neg A$ – ложно).

Например, предикат от трёх сущностей: “прямая α проходит через две точки x и y” можно *определить* следующим образом:

$$L(x,\, y,\, \alpha) \quad : \qquad (x \in \alpha) \,\&\, (y \in \alpha).$$



Двоеточие означает, что везде, где встречается $L(x,\, y,\, \alpha)$, его необходимо *заменить* на строку $(x \in \alpha) \,\&\, (y \in \alpha)$.

Введём ещё два символа – заменители слов:

$\forall$	:	“любой” = “каждый” = “для всех”	= квантор всеобщности
$\exists$	:	“существует по крайней мере один”	= квантор существования

Теперь можно записывать различные геометрические утверждения. Например, фраза “для любых точек x и y существует по крайней мере одна прямая α, которая через них проходит” имеет вид:

$$\forall_x \forall_y \exists_\alpha \, L(x,\, y,\, \alpha),$$

а предикат параллельности прямых α и β определим как:

$$\alpha || \beta : \qquad \neg \exists_x \, (x \in \alpha \;\&\; x \in \beta).$$

Подобным образом записываются все аксиомы геометрии. Затем с ними проделываются формальные манипуляции для вывода новых формул. После перечисления аксиом и правил вывода, содержательная составляющая теории отходит на второй план. Построение доказательств и их проверка может быть проведена компьютером или марсианином, ничего не знающим о смысле букв x, y, α, β, предиката $x \in \alpha$, и ему подобных. Довнесение “очевидных” суждений, не заложенных в исходные аксиомы, при таком подходе уже практически невозможно.

• В каждой формальной теории фиксируется множество символов, при помощи которых записывают все утверждения. Так, для формулировки большинства фактов из теории натуральных чисел достаточно такого “*алфавита*”:

$$0 \quad 1 \quad x \quad + \quad \cdot \quad = \quad (\ ) \quad \neg \quad \& \quad \vee \quad \forall \quad \exists$$

Символы “0”, “1” являются предметными *константами*, обозначающими числа “ноль” и “один”, “x” – *переменная* (произвольное число). Дополнительные переменные можно ввести при помощи повторений xx, xxx, и т.д., которые для краткости обозначают как $x, y, ...$ или $x_1, x_2, ...$.

Сложение “+” – это *предметная функция* двух переменных. Каждым двум числам она ставит в соответствие третье число: $+(x, y)$ или $(x + y)$. При помощи константы “1” и функции “+” определяется множество других констант: 2: (1+1), 3: ((1+1)+1), и т.д. Аналогично, точка – это ещё одна функция $x \cdot y$, имеющая смысл умножения чисел.

Символ “=” – это *предикат*, истинный или ложный, в зависимости от того, равны числа или нет: 2=2 – это истина, 1=2 – это ложь.

Скобки, логические функции “¬ & ∨” (НЕ, И, ИЛИ) и кванторы - заменители слов “все” (∀) и “существует” (∃) - позволяют записывать произвольные формулы. Таким образом, математическое утверждение представляется строкой символов из данного алфавита.

Существуют простые способы (алгоритмы) отличить правильно построенную формулу: “$\neg(x = y) \vee (x + 1 = y)$” от неправильной: “$\vee)\neg\&x$”. Правильность понимается в смысле “синтаксически верно”, а не в смысле истинно! Так, компилятор распознает синтаксическую ошибку, сделанную при записи программы, хотя синтаксически верная программа может работать и не правильно, например, никогда не останавливаться.

Через предикат $x = y$ определяются предикаты “не равно” и “меньше”:

$$\begin{aligned} &x \neq y: \quad \neg(x = y), \\ &x < y: \quad \exists_z \big(z \neq 0 \ \& \ z + x = y\big). \end{aligned}$$

В последнем случае предикат $x < y$ истинен, если существует отличное от нуля число z, добавление которого к x, даёт y. Двоеточием везде обозначается определение формулы или утверждения.

Аналогично можно определить предикаты Even(x): “x – чётное число” и Odd(x): “x – нечётное число”:

$$\text{Even}(x) \ : \ \exists_y\big(x = y + y\big), \qquad \text{Odd}(x) \ : \ \exists_y\big(x = (y + y) + 1\big),$$

т.е. число чётное, *если* существует y, который при сложении с собой даёт x. В этом определении не указывается как искать y. Однако, если такой y находится (хотя бы один), предикат Even(x) считается истинным.

• Предметные функции и предикаты *определяются* при помощи аксиом – формул, которым они должны удовлетворять (быть истинными).

◇ Сложение в арифметике определяют аксиомы:

$$\forall_x \big[\, x+1 \neq 0 \,\big], \qquad \forall_x \forall_y \big[\, x+1 \neq y+1 \;\;\vee\;\; x = y \,\big],$$
$$\forall_x \big[\, x+0 = x \,\big], \qquad \forall_x \forall_y \big[\, x+(y+1) = (x+y)+1 \,\big],$$

а умножение:

$$\forall_x \big[\, x \cdot 0 = 0 \,\big], \qquad \forall_x \forall_y \big[\, x \cdot (y+1) = (x \cdot y) + x \,\big].$$

Предикат, утверждающий что число x является простым, имеет вид:

$$\mathrm{Prime}(x): \quad \neg\exists_y \exists_z \big[\, y \neq 1 \;\&\; z \neq 1 \;\&\; x = y \cdot z \big].$$

Это уже определение, использующее функцию умножения. □

В формулах необходимо различать свободные и связанные предметные переменные. Связанная переменная стоит под действием квантора "$\exists_x$" или "$\forall_x$". Если рассматривается конечная предметная область, состоящая только из трех предметных констант $x = \{1, 2, 3\}$, то:

$$\exists_x A(x) = A(1) \vee A(2) \vee A(3), \qquad \forall_x A(x) = A(1) \,\&\, A(2) \,\&\, A(3).$$

Первое выражение утверждает, что "существует такой x, что некий предикат $A(x)$ истинен". Это значит, что истинно или $A(1)$, или $A(2)$, или $A(3)$ (хотя бы что-то одно из $\{1, 2, 3\}$, которое и "существует"). Аналогично для квантора "любой" истинными должны быть и $A(1)$, и $A(2)$, и $A(3)$, т.е. все. Таким образом, наличие в формуле переменной, связанной с квантором, аналогично индексу суммирования и выражение (после явной записи "суммы") от нее не зависит. Как и суммационный индекс, связанную переменную можно обозначить любой буквой, которой еще нет в выражении.

Формулы без свободных переменных считаются либо истинными, либо ложными. Например, утверждение об отсутствии самого большого простого числа:

$$\neg\exists_x \forall_y \big[\, \mathrm{Prime}(x) \;\&\; \mathrm{Prime}(y) \;\&\; y \leqslant x \,\big]$$

истинно, а его отрицание (наибольшее число x существует) – ложно.

Кроме аксиом, задаются *правила вывода* – формальные способы получения одних формул из других. Такие правила сохраняют истинность выражений, так что из истинной формулы может быть выведена только истинная формула.

Прежде чем подробнее изучать введенные понятия, напомним основные факты из теории множеств.

1.2 Множества

• Размышления о совокупностях объектов создало математику и стало её основой. *Множество* – это фундаментальное понятие, обобщающее интуитивное представление об объединении объектов по некоторому признаку. Множества состоят из *элементов*. Все элементы данного множества *различны* и *порядок* их перечисления *не важен*.

◇ Примеры: множество целых чисел, множество прямых, множество симпатичных девушек, множество этих трёх множеств. □

Множество определено, когда задан способ, позволяющий выяснить содержит ли оно данный элемент. Если элемент a *принадлежит* множеству $\mathcal{A}$ (содержится в нём), то это обозначается следующим образом: $a \in \mathcal{A}$ (предикат с двумя аргументами a, $\mathcal{A}$, который истинен, если a принадлежит $\mathcal{A}$ и ложен, в противном случае). Если элемент a не принадлежит множеству $\mathcal{A}$, то это обозначается так: $a \notin \mathcal{A}$ или $\neg(a \in \mathcal{A})$. Два множества $\mathcal{A}$ и $\mathcal{B}$, состоящие из одних и тех же элементов, равны: $\mathcal{A} = \mathcal{B}$ (предикат *равенства*).

Конечные множества можно описать, перечислив их элементы. В общем случае множество задаётся при помощи условия: $\mathcal{A} = \{x|\text{ условие}\}$.

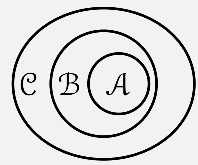
◇ $\mathcal{A} = \{3, 2, 1, 5, 4\}$ – множество *натуральных чисел* $\mathbb{N}$ от 1 до 5.
$\mathcal{A} = \{x|x \in \mathbb{N},\ 0 < x < 6\}$ – это снова натуральные числа от 1 до 5. □

Если каждый a, принадлежащий множеству $\mathcal{A}$ ($a \in \mathcal{A}$) также принадлежит и множеству $\mathcal{B}$ ($a \in \mathcal{B}$), то говорят, что $\mathcal{A}$ является *подмножеством* (частью) множества $\mathcal{B}$. Для выражения этого вводится третий предикат: $\mathcal{A} \subseteq \mathcal{B}$ со свойствами:

$\mathcal{A} \subseteq \mathcal{A}$, само себе подмножество,

Если $(\mathcal{A} \subseteq \mathcal{B})\,\&\,(\mathcal{B} \subseteq \mathcal{A})$ то $\mathcal{A} = \mathcal{B}$,

Если $(\mathcal{A} \subseteq \mathcal{B})\,\&\,(\mathcal{B} \subseteq \mathcal{C})$ то $\mathcal{A} \subseteq \mathcal{C}$.



Элементами множества могут выступать другие множества. Для избежания противоречий считают, что множество не может быть своим элементом: $\mathcal{A} \notin \mathcal{A}$.

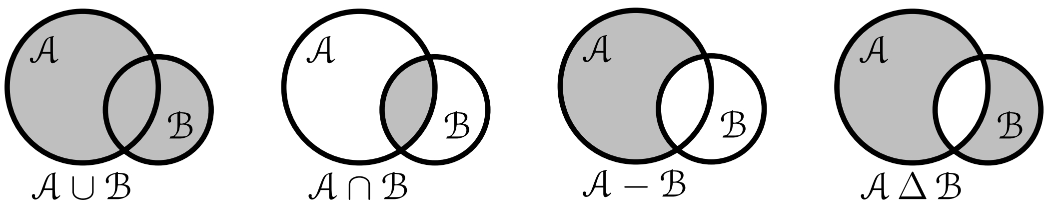
◇ Элементами множества $\mathcal{Z} = \{\,\{a, b\},\ \{a\}\,\}$ выступают два множества $\mathcal{X} = \{a, b\}$ и $\mathcal{Y} = \{a\}$. Не стоит путать $a \in \mathcal{X}$ или $\{a\} \in \mathcal{Z}$ (элементы) и $\{a\} \subseteq \mathcal{X}$ или $\{\{a\}\} \subseteq \mathcal{Z}$ (подмножества), где $\{\{a\}\}$ – множество из одного элемента $\{a\}$, который есть множество с элементом a. □

Множество $\varnothing = \{\}$, не содержащее элементов, называется *пустым*. Пустое множество является подмножеством любого множества: $\varnothing \subseteq \mathcal{A}$. У множества $\mathcal{A}$ с n элементами 2^n подмножеств $\lessdot$ H_1, включая $\mathcal{A}$ и $\varnothing$.

• Для образования новых множеств вводится три *функции* (операции), ставящие в соответствие двум множествам, третье:

объединение:	$\mathcal{A}\cup\mathcal{B} = \{x \mid (x\in\mathcal{A}) \vee (x\in\mathcal{B})\}$,
пересечение:	$\mathcal{A}\cap\mathcal{B} = \{x \mid (x\in\mathcal{A}) \,\&\, (x\in\mathcal{B})\}$,
дополнение:	$\mathcal{A}-\mathcal{B} = \{x \mid (x\in\mathcal{A}) \,\&\, (x\notin\mathcal{B})\}$,
симметричная разность:	$\mathcal{A}\,\Delta\,\mathcal{B} = (\mathcal{A}-\mathcal{B})\cup(\mathcal{B}-\mathcal{A})$.

В объединённое множество попадают все элементы из обоих множеств. В пересечение – только общие для множеств элементы, а в дополнение $\mathcal{A}-\mathcal{B}$ только те элементы $\mathcal{A}$, которые не принадлежат $\mathcal{B}$. Эти базовые функции наглядно представляются при помощи *диаграмм Эйлера-Венна*, в которых замкнутая область обозначает некоторое множество. Область геометрического пересечения двух множеств будет множественным пересечением $\mathcal{A}\cap\mathcal{B}$ (она закрашена), и т.д.:



Ясно, что $\mathcal{A}\cup\mathcal{A}=\mathcal{A}$, $\mathcal{A}\cap\mathcal{A}=\mathcal{A}$ и если $\mathcal{A}\subseteq\mathcal{B}$, то $\mathcal{A}\cap\mathcal{B}=\mathcal{A}$. Результатом действия функций может быть пустое множество. Например: $(\mathcal{A}-\mathcal{B})\cap\mathcal{B}=\varnothing$. Отметим мнемонику: значок $\cup$ – это чашка в которую “сливаются” (объединяясь) оба множества.

При помощи диаграмм Эйлера-Венна, несложно мотивировать различные тождества для введенных операций. Например, в качестве простого упражнения, предлагается проверить свойства *коммутативности* и *ассоциативности* для объединения множеств:

$$\mathcal{A}\cup\mathcal{B}=\mathcal{B}\cup\mathcal{A}, \qquad\qquad (\mathcal{A}\cup\mathcal{B})\cup\mathcal{C}=\mathcal{A}\cup(\mathcal{B}\cup\mathcal{C}).$$

и такое же для пересечения $\cap$. Затем доказать ($\lessdot$ H_2) их *дистрибутивность*, которая также верна, если заменить $\cup$ на $\cap$ и наоборот (поменять объединение и пересечение местами):

$$(\mathcal{A}\cup\mathcal{B})\cap\mathcal{C}=(\mathcal{A}\cap\mathcal{C})\cup(\mathcal{B}\cap\mathcal{C}).$$

Ещё два тождества с операцией дополнения:

$$\mathcal{A}\cap(\mathcal{B}-\mathcal{C})=(\mathcal{A}\cap\mathcal{B})-(\mathcal{A}\cap\mathcal{C}),$$

$$(\mathcal{A}-\mathcal{B})\cup(\mathcal{B}-\mathcal{A})=(\mathcal{A}\cup\mathcal{B})-(\mathcal{A}\cap\mathcal{B})$$

также несложно доказать, пользуясь этими диаграммами ($\lessdot$ H_3).

• Теория множеств позволяет определять предикаты. Например, на множестве $\mathcal{X} = \{x_1, x_2, x_3, x_4\}$ из четырёх элементов, зададим предикат $A(x)$ с одним аргументом. Пусть $A(x_1) = \mathbb{1}$, $A(x_2) = \mathbb{O}$, $A(x_3) = \mathbb{1}$, $A(x_4) = \mathbb{O}$, где $\mathbb{1}$ – это истина, а $\mathbb{O}$ – ложь. Эквивалентно, его можно считать равным *подмножеству* элементов $\mathcal{A} \subseteq \mathcal{X}$, для которых $A(x)$ истинно:

$$\mathcal{A} = \{x_1, x_3\}$$

x_1	x_2	x_3	x_4
•		•	

Определим теперь предикат $B(x, y)$ с первым аргументом из множества $\mathcal{X} = \{x_1, x_2, x_3\}$, а со вторым – из множества $\mathcal{Y} = \{y_1, y_2, y_3, y_4, y_5, y_6\}$. Они могут иметь разный смысл ($\mathcal{X}$ – это точки, $\mathcal{Y}$ – прямые), или одинаковый (и $\mathcal{X}$, и $\mathcal{Y}$ – натуральные числа). Составим множество всех *упорядоченных* пар которое называют *прямым произведением*:

$$\mathcal{X} \times \mathcal{Y} = \{(x_1, y_1), ..., (x_1, y_6),\ (x_2, y_1), ..., (x_2, y_6),\ (x_3, y_6), ..., (x_3, y_6)\}.$$

Предикат зададим подмножеством $\mathcal{B} \subseteq \mathcal{X} \times \mathcal{Y}$ на котором он истинный:

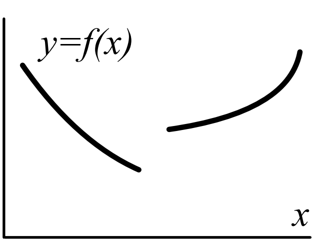
$$\begin{aligned} \mathcal{B} : \{ \ & (x_1, y_2), (x_1, y_3), (x_1, y_4), (x_1, y_5), (x_1, y_6), \\ & (x_2, y_4), (x_2, y_6), \\ & (x_3, y_6)\ \} \end{aligned}$$

	y_1	y_2	y_3	y_4	y_5	y_6
x_1		•	•	•	•	•
x_2				•		•
x_3						•

Таблица соответствует всем $18 = 3 \cdot 6$ упорядоченным парам и 8 точек стоит там, где $B(x, y)$ истинен. Предикат $B(x, y)$ может обозначать “число x – собственный делитель y” ($x \neq y$), если $\mathcal{X} = \{1, 2, 3\}$, а $\mathcal{Y} = \{1, ..., 6\}$. Например $B(2, 4)$ истинно, а $B(3, 4)$ – ложно.

Точно также определяются предикаты с тремя аргументами (между тремя объектами): $C(x, y, z) :\ \mathcal{C} \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ и т.д.

• Если бинарный (с двумя аргументами) предикат $F(x, y)$ для каждого $x \in \mathcal{X}$ истинен для *не более одного* $y \in \mathcal{Y}$, его называют *функциональным.* Он определяет *функцию* $y = f(x)$, которая элементу x ставит в соответствие единственный элемент y:



	$\mathcal{Y}$		
	•		
$\mathcal{X}$	•		
			•

x	x_1	x_2	x_3	x_4
$y = f(x)$	y_1		y_1	y_3

Если в таблице предиката есть пустые строчки, то это *частично определённая* (не при всех значениях x) функция. Аналогично, предикат $F(x, y, z)$ может определять функцию $z = f(x, y)$ и т.д.

• Конечные множества (имеющие конечное число элементов) являются очень конструктивными математическими объектами. Их можно (по крайней мере в принципе) "изобразить" на бумаге или в памяти компьютера. Иначе обстоит дело с множествами бесконечными. Например, не существует "самого большого" натурального числа и множество $\mathcal{N} = \{0, 1, 2, ...\}$ бесконечно.

Различают *потенциальную* и *актуальную* бесконечности. Первая подразумевает, что конкретное число $x \in \mathcal{N}$ может быть сколь угодно большим. Актуальная бесконечность представляет совокупность *всех* натуральных чисел или всех точек отрезка $[0...1]$, как самостоятельный математический объект (*законченную совокупность*). С актуальными бесконечностями связаны определённые проблемы, однако сейчас мы их обсуждать не будем, а введём понятие счётного множества.

Множество называется *счётным*, если все его элементы можно пронумеровать, т.е. каждому элементу поставить в соответствие *уникальное* натуральное число.

◇ Любое подмножество натуральных чисел $\mathcal{N} = \{0, 1, 2, ...\}$ счётно. Например, упорядоченные по возрастанию чётные числа можно пронумеровать, перечислив их как $\{0, 2, 4, ...\}$ или при помощи функции соответствия $f(n) = 2n$ такой, что $f(0) = 0$, $f(1) = 2$, $f(2) = 4$,....

◇ Счётны целые числа, которых кажется "больше", чем натуральных. Их перечисление такое: $\{0, -1, 1, -2, 2, -3, 3, ...\}$ или при помощи функции $f(n)$, равной $n/2$ при чётных n и $-(n+1)/2$ – при нечётных.

◇ Множество рациональных чисел $\mathcal{Q}$ – это все несократимые дроби p/q, где $p, q \in \mathcal{N}$ и $q \neq 0$. Каждому числу p/q можно присвоить уникальный номер $n = 2^p \cdot 3^q$, поэтому множество $\mathcal{Q}$ счётно. Так как любое число *единственным* образом раскладывается на множители, то по данному n можно получить p, q и наоборот. Заметим, что рациональные числа (как и целые) нельзя перечислить по возрастанию и введенная нумерация даёт последовательность $\{0,\ 1,\ 2,\ 1/2,\ 3,\ 4,\ 1/3,\ 3/2,\ ...\}$.

◇ Счётно множество всех строк конечной длины, состоящих из букв конечного алфавита. Такие строки можно упорядочить сначала по длине (строки из одного символа, строки из двух символов и т.д.), а строки одинаковой длины отсортировать по алфавиту (*лексографический порядок*). Каждая строка в таком списке имеет свой порядковый номер.

◇ Любые определения, формулы, доказательства и алгоритмы счётны, т.к. являются конечными строками из букв конечного алфавита. □

1.3 Алгебра логики

• В *бинарной* (двоичной) *логике* каждому утверждению приписывается одно из двух значений: истина ($\mathbb{1}$) или ложь ($\mathbb{O}$). Константное утверждение (A : "сейчас идет дождь") называется *высказыванием*. Утверждение может зависеть от переменных $P(x):\ x>0$. Такие переменные утверждения (=*предикаты*) истинны при одних x и ложны при других.

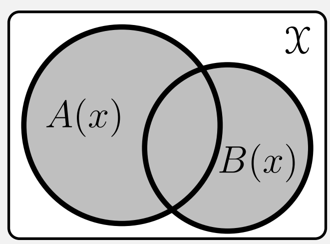
Это очень ограниченная модель "человеческой логики". Высказывание "сейчас идёт дождь" истинно или ложно, и третьего не дано. Хотя для многих "одна дождинка – ещё не дождь". Тем не менее, в формальных теориях, таких как математика, бинарной логики вполне достаточно.

Простые утверждения (высказывания, предикаты) объединяют в более сложные при помощи логических связок (=операций) $\neg$, $\&$, $\vee$, $\equiv$. Эти связки являются функциями, аргументы и значения которых принадлежат множеству $\{\mathbb{1}, \mathbb{O}\}$.

Логическое "ИЛИ" $A \vee B$ истинно, если истинно или A или B или оба (хотя бы одно). Представим это утверждение при помощи *таблицы истинности*, где в колонках A и B перечисленны все варианты значений истинности высказываний A и B, а под символом $\vee$ находится результат логической операции $A \vee B$ (она называется также *дизъюнкцией*):

$A \vee B$ "ИЛИ", дизъюнкция

A	$\vee$	B
$\mathbb{O}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{O}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

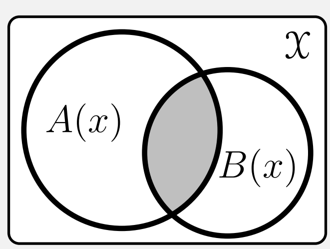


Так $\mathbb{O} \vee \mathbb{O}$ – это $\mathbb{O}$, а $\mathbb{O} \vee \mathbb{1}$ – это $\mathbb{1}$. Справа кругами изображены области истинности предикатов $A(x)$ и $B(x)$ на плоскости всех значений $x \in \mathfrak{X}$. Заштрихованная область – это *результирующий предикат* $A(x) \vee B(x)$.

Логическое "И" или *конъюнкция* истинно, только если истинны оба высказывания:

$A \,\&\, B$ "И", конъюнкция

A	$\&$	B
$\mathbb{O}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{O}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

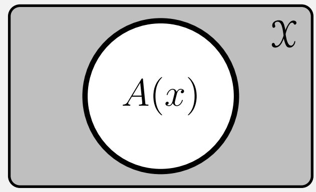


Предикат конъюнкции $A(x) \,\&\, B(x)$ истинен в области пересечения множеств истинности $A(x)$ и $B(x)$.

Операция *логического отрицания* меняет истину на ложь и наоборот, т.е. $\neg\,\mathbb{1}$ это $\mathbb{O}$, а $\neg\,\mathbb{O}$ – это $\mathbb{1}$. Кроме символа $\neg$, часто будет использоваться черта сверху ($\bar{A}$ – тоже, что и $\neg A$):

$\neg A,\ \bar{A}$ отрицание

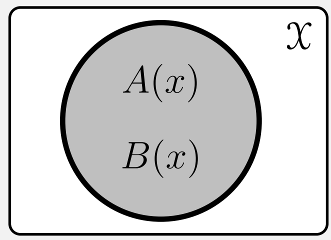
$\neg$	A
$\mathbb{1}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{1}$



Если два логических выражения имеют одинаковые значения истинности или лжи, то говорят, что они эквивалентны:

$A \equiv B$ тождество, эквивалентность

A	$\equiv$	B
$\mathbb{O}$	$\mathbb{1}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{O}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$



Эквивалентность $A \equiv B$ похожа на равенство $x = y$, однако мы будем их различать. Например, в арифметике $(x = y) \;\equiv\; (y = x)$, где $x, y \in \mathbb{N}$, а $x = y$ – это предикат равенства (истинный или ложный).

Логическая функция двух аргументов определяется последовательностью из $4 = 2^2$ символов $\mathbb{1}$ или $\mathbb{O}$. Для логического ИЛИ эта последовательность имеет вид $\mathbb{O}\,\mathbb{1}\,\mathbb{1}\,\mathbb{1}$, а для эквивалентности $\mathbb{1}\,\mathbb{O}\,\mathbb{O}\,\mathbb{1}$. Возможно $16 = 2^4$ подобных последовательностей (двоичных чисел с 4-мя разрядами) $\lessdot\,\mathrm{H}_1$. Как мы увидим дальше, любую логическую функцию можно выразить через связки $\&, \vee, \neg$.

В качестве примера рассмотрим *разделительное* “ИЛИ” $A \oplus B$: “она любит или Колю или Васю” (но не обоих). Оно отлично от объединяющего “ИЛИ” $A \vee B$, которое истинно и когда истинны оба высказывания.

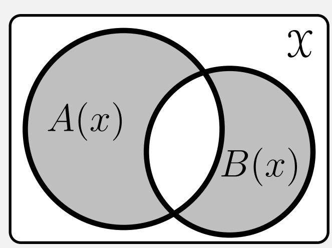
разделительное ИЛИ :

$(A \,\&\, \bar{B}) \vee (\bar{A} \,\&\, B)$,

а можно и так:

$(A \vee B) \,\&\, (\bar{A} \vee \bar{B})$.

A	$\oplus$	B
$\mathbb{O}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{O}$
$\mathbb{1}$	$\mathbb{O}$	$\mathbb{1}$



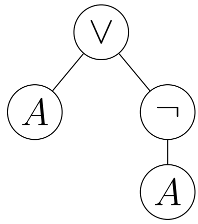
Так, подстановка последней строки в таблице истинности во вторую формулу даёт: $(\mathbb{1} \vee \mathbb{1})\,\&\,(\bar{\mathbb{1}} \vee \bar{\mathbb{1}}) \equiv \mathbb{1}\;\&\,(\mathbb{O} \vee \mathbb{O}) \equiv \mathbb{1}\;\&\;\mathbb{O} \equiv \mathbb{O}$. Отметим, что:

$$A \vee B \equiv A \oplus B \oplus (A \,\&\, B), \qquad \neg A \equiv A \oplus \mathbb{1},$$

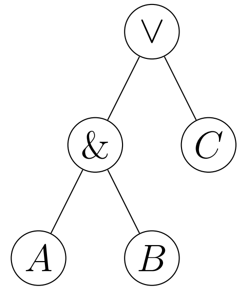
т.е. все связки выражаются через $\oplus$, $\&$ и $\mathbb{1}$ (т.н. полиномы Жегалкина).

• Любую логическую формулу (=выражение) можно представить в виде дерева, задающего последовательность вычислений:

$A \vee \neg A$:



$(A \,\&\, B) \vee C$:



В вершине дерева стоит последняя вычисляющаяся функция, а внизу, на “листьях” – высказывания. Вычисление выражения идёт снизу-вверх.

Введём соглашение о приоритетах логических функций:

> самый высокий приоритет у отрицания “$\neg$”, чуть ниже у “&” и ещё ниже у “$\vee$”; самый низкий приоритет у эквивалентности “$\equiv$”.

Если на приоритеты не полагаются, то используют скобки. Например, формула $A \,\&\, B \vee \neg C \,\&\, D$ – это тоже, что и $(A \,\&\, B) \vee ((\neg C) \,\&\, D)$, а формула $A \vee B \equiv C \,\&\, D$ – это $(A \vee B) \equiv (C \,\&\, D)$.

• Логическое выражение, истинное при любых значениях входящих в него высказываний, называется *общезначимым* или *тавтологией*. Докажем, например, общезначимость следующей формулы:

$$A \,\&\, (A \vee B) \;\equiv\; A.$$

Для этого запишем её таблицу истинности. Высказывания принимают значение $\mathbb{0}$ и $\mathbb{1}$. Если $A \equiv \mathbb{0}$, то B может быть равно $\mathbb{0}$ или $\mathbb{1}$. Аналогично для $A \equiv \mathbb{1}$. Это даёт четыре варианта, которые подпишем под высказываниями, входящими в формулу. Затем под каждой логической связкой (сначала $\vee$, затем &) будем подписывать её результат:

A	&	$(A$	$\vee$	$B)$	$\equiv$	A
$\mathbb{0}$		$\mathbb{0}$		$\mathbb{0}$		$\mathbb{0}$
$\mathbb{0}$		$\mathbb{0}$		$\mathbb{1}$		$\mathbb{0}$
$\mathbb{1}$		$\mathbb{1}$		$\mathbb{0}$		$\mathbb{1}$
$\mathbb{1}$		$\mathbb{1}$		$\mathbb{1}$		$\mathbb{1}$

A	&	$(A$	$\vee$	$B)$	$\equiv$	A
$\mathbb{0}$	$\underline{\mathbb{0}}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$		$\underline{\mathbb{0}}$
$\mathbb{0}$	$\underline{\mathbb{0}}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$		$\underline{\mathbb{0}}$
$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$		$\underline{\mathbb{1}}$
$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$		$\underline{\mathbb{1}}$

Осталось сравнить подчёркнутые значения. Так как они совпадают, в колонке $\equiv$ везде необходимо поставить $\mathbb{1}$, т.е. это тавтология.

В качестве простого упражнения ($\lessdot$ H$_4$) предлагается доказать, что формула $A \vee \neg A$ также является тавтологией. Она имеет смысл закона исключения третьего (“или A или не A”). На месте A может стоять как константное высказывание “сейчас идет дождь”, так и предикат. Например: $(x = y) \vee \neg(x = y)$, т.е. x или равно или не равно y.

• Существует множество формул, имеющих одинаковые таблицы истинности. Соединение их символом эквивалентности "≡" приводит к тавтологиям. Часть из них составляет *булеву алгебру*.
Так, логические "И", "ИЛИ" – *симметричны* и *ассоциативны*:

$$\begin{array}{lcl} A\,\&\,B & \equiv & B\,\&\,A, \qquad A\,\&\,(B\,\&\,C) \equiv (A\,\&\,B)\,\&\,C, \\ A\vee B & \equiv & B\vee A, \qquad A\vee(B\vee C) \equiv (A\vee B)\vee C. \end{array}$$

Для них выполняются законы *дистрибутивности*:

$$\begin{array}{lcl} A\,\&\,(B\vee C) & \equiv & (A\,\&\,B)\vee(A\,\&\,C), \\ A\vee(B\,\&\,C) & \equiv & (A\vee B)\,\&\,(A\vee C) \end{array}$$

и более специфические свойства *поглощения*:

$$\begin{array}{lcl} A\,\&\,A \equiv A, & & A\,\&\,(A\vee B) \equiv A, \\ A\vee A \equiv A, & & A\vee(A\,\&\,B) \equiv A. \end{array}$$

Справедлив закон двойного отрицания и *правила де-Моргана*:

$$\begin{array}{lcl} \neg(\neg A) \equiv A, & & \neg(A\,\&\,B) \equiv \neg A\vee\neg B, \\ & & \neg(A\vee B) \equiv \neg A\,\&\,\neg B. \end{array}$$

В алгебру можно ввести константы: "$\mathbb{1}$" (истина), "$\mathbb{0}$" (ложь) и записать *закон исключения третьего* в двух формах:

$$A\,\&\,\neg A \equiv \mathbb{0}, \qquad A\vee\neg A \equiv \mathbb{1},$$

а также следующие очевидные соотношения:

$$A\,\&\,\mathbb{0} \equiv \mathbb{0}, \qquad A\,\&\,\mathbb{1} \equiv A, \qquad A\vee\mathbb{1} \equiv \mathbb{1}, \qquad A\vee\mathbb{0} \equiv A.$$

Стоит обратить внимание на симметричность всех формул относительно перестановки & и ∨, с одновременной заменой $\mathbb{0}$ на $\mathbb{1}$ и наоборот.

◇ Проведём при помощи этих тождеств упрощение следующего логического выражения:

$$A\,\&\,(\bar{A}\vee B) \equiv (A\,\&\,\bar{A})\vee(A\,\&\,B) \equiv \mathbb{0}\vee(A\,\&\,B) \equiv A\,\&\,B,$$

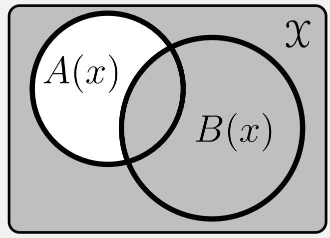
где сначала использовано свойство дистрибутивности конъюнкции (&), затем закон исключения третьего и тождество $\mathbb{0}\vee A \equiv A$. Непрерывная цепочка эквивалентностей основана на свойстве *транзитивности*: если $A \equiv B$ и $B \equiv C$, то $A \equiv C$, что записывается как $A \equiv B \equiv C$. Аналогично стоит доказать, что $A\vee(\bar{A}\,\&\,B) \equiv A\vee B$. □

1.4 Импликация и логическое следование

• Важна также связка $A \to B$, называемая *импликацией*. Она ложна только для комбинации $\mathbb{1} \to \mathbb{O}$, что интерпретируется как "из истины нельзя получить ложь". В остальных случаях она истинна:

$A \to B$ импликация

A	$\to$	B
$\mathbb{O}$	$\mathbb{1}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$



Из истины "следует" истина, поэтому $\mathbb{1} \to \mathbb{1}$ это $\mathbb{1}$. Из лжи можно вывести что угодно, поэтому $\mathbb{O} \to \mathbb{O}$ и $\mathbb{O} \to \mathbb{1}$ считаются истинными. Аргументы импликации называются *посылкой* и *следствием*.

Для высказываний интерпретация импликации, как следования выглядит странной. Так $(2 \cdot 2 = 4) \;\to\;$ "Солнце это звезда" – истинная формула, хотя посылка и следствие между собой ни как не связаны.

Лучше ситуация для предикатов. Например, в арифметике при любом x истинно утверждение: "если $x < 2$, то $x < 4$", или $(x < 2) \to (x < 4)$. Когда посылка истинна $(x = 1)$, истинно и следствие. Если же посылка ложна, то следствие может быть как истинным (при $x = 3$), так и ложным (при $x = 5$). Эти случаи соответствуют строчкам таблицы истинности, где стоит $\mathbb{1}$. "Менее правильное" утверждение $(x > 2) \to (x < 4)$ ложно при $x = 5$.

Стоит графически проверить, что если область истинности предиката $A(x)$ является подмножеством $B(x)$, то их импликация $A(x) \to B(x)$ всегда истинна и наоборот. Так обстоит дело для "$(x < 2) \to (x < 4)$". Именно в этом случае функция импликации имеет смысл следования.

При помощи таблиц истинности можно показать ($\lessdot$ H$_5$), что импликация выражается через остальные логические связки (приоритет "$\to$" считаем большим, чем у "$\equiv$" и меньшим, чем у "$\vee$, & $\neg$"):

$$A \to B \;\equiv\; \neg A \vee B.$$

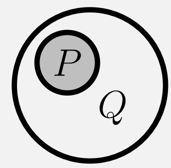
В свою очередь, эквивалентность $A \equiv B$ имеет такую же таблицу истинности, как и $(A \to B) \,\&\, (B \to A)$, что интерпретируется как следование в обе стороны. В частности формула

$$(A \equiv B) \equiv (A \to B) \,\&\, (B \to A)$$

всегда истинная (общезначимая), т.е. она является тавтологией.

• Пусть $P = P(A, B(x), ...)$ и $Q = Q(A, C(x, y), ...)$ формулы, зависящие от высказываний и предикатов. Эти формулы равны $\mathbb{1}$ или $\mathbb{O}$ при определённых значениях, входящих в них элементарных утверждений.

Если всегда, когда P истинно, истинно и Q, то говорят, что из утверждения P логически следует утверждение Q. Это обозначается так: $P \Rightarrow Q$.



Например:

$$A \;\Rightarrow\; A \vee B, \qquad\qquad A \,\&\, B \;\Rightarrow\; A.$$

Так, первое следование означает, что *если* A истинно, то для любого B, дизъюнкция $A \vee B$ будет истинной. Справедлива теорема ($\lessdot$ H$_6$):

Если $P \Rightarrow Q$, то формула $P \to Q$ – это тавтология и наоборот.

Например, формула $A \to (A \vee B)$ – общезначима. Импликация $P \to Q$ (бинарная функция), в отличие от следования $P \Rightarrow Q$, определена и когда P ложно. При логическом же следовании подразумевается истинность посылки. В частности, справедливо правило *modus ponens*:

(MP) $\qquad P, \quad P \to Q \quad \Rightarrow \quad Q,$

означающее, что если *обе* посылки P и $P \to Q$ истинны, то истинна и формула Q. Если $P \equiv \mathbb{O}$, то Q – это $\mathbb{1}$ или $\mathbb{O}$. Стоит проверить ($\lessdot$ H$_7$) общезначимость формулы $P \,\&\, (P \to Q) \to Q$.

Следствие обладает *транзитивностью*:

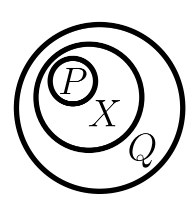
$$\text{если } P \Rightarrow X \text{ и } X \Rightarrow Q, \text{ то } P \Rightarrow Q.$$

Следствие в общем случае не симметрично. Так, $A \;\Rightarrow\; A \vee B$ справедливо только в одну сторону и из $A \vee B$ не следует A (поэтому $A \vee B \to A$ не тавтология $\lessdot$ H$_8$). Тем не менее, существуют и следования в обе стороны: $\Leftrightarrow$. Например: $A \vee B \;\Leftrightarrow B \vee A$ или двухстороннее правило:

$$A \,\&\, B \;\Leftrightarrow A, \quad B.$$

Вправо, это $A \,\&\, B \Rightarrow A$, влево оно означает: когда обе посылки A и B истинны, истинна и их конъюнкция.

Двухсторонний вывод $P \Leftrightarrow Q$ аналогичен функции эквивалентности $P \equiv Q$. Утверждения: "если P, то Q и наоборот", "P *тогда и только тогда*, когда Q" означают $P \Leftrightarrow Q$.



Если $P \Rightarrow X \Rightarrow Q$, то P называют *достаточным* условием, а Q – *необходимым* условием для X. Когда необходимое и достаточное условия совпадают, то они совпадают и с X: $P \equiv Q \equiv X$.

• Большинство рассуждений в математике можно разделить на прямые и обратные. Получение по (**MP**) из двух формул P и $P \to Q$ третей формулы Q является примером *прямого логического следования*. Ещё одно, более мощное, правило прямого следования называется *резолюцией*:

$$\text{(}\mathbf{Res}\text{)} \qquad P \vee S, \quad \neg P \vee Q \quad \Rightarrow \quad S \vee Q.$$

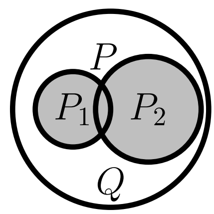
Действительно: так как P и $\neg P$ не могут быть одновременно истинными, а посылки $P \vee S$ и $\neg P \vee Q$ истинны по определению, то истинно S или Q. Если S — ложно, получается частный случай (**MP**). Стоит также проверить ($\lessdot$ H$_9$), что $(P \vee S) \,\&\, (\neg P \vee Q) \;\to\; S \vee Q$ – это тавтология.

Вариантом резолюции является *метод цепочек импликаций*:

$$P \to S, \quad S \to Q \quad \Rightarrow \quad P \to Q.$$

Если в каждой формуле выразить импликацию через дизъюнкцию (заменить $P \to S$ на $\neg P \vee S$), то получится следование, совпадающее с резолюцией точностью до переобозначений: $\neg P \vee \underline{S}, \;\; \neg \underline{S} \vee Q \;\; \stackrel{\mathbf{Res}}{\Rightarrow} \;\; \neg P \vee Q$.

Метод разбора случаев – ещё один пример прямых рассуждений. Пусть из P необходимо вывести Q. Рассмотрим несколько утверждений, например, P_1 и P_2, объединение которых равно P. Говорят, что P_1 и P_2 покрывают все возможные случаи. Если из каждого утверждения P_i следует Q, то оно следует и из $P = P_1 \vee P_2$:



$$P_1 \vee P_2, \quad P_1 \to Q, \quad P_2 \to Q \quad \Rightarrow \quad Q.$$

◁ Докажем это правило при помощи резолюции:

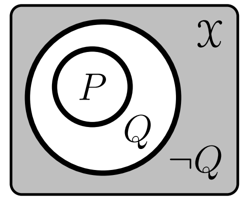
$$\underline{P_1} \vee P_2, \quad \neg \underline{P_1} \vee Q, \quad \neg P_2 \vee Q \quad \stackrel{\mathbf{Res}}{\Rightarrow} \quad \underline{\underline{P_2}} \vee Q, \quad \neg \underline{\underline{P_2}} \vee Q \quad \stackrel{\mathbf{Res}}{\Rightarrow} \quad Q.$$

Формула и её отрицание подчёркнуты. В первом выводе это P_1 и из формул $P_1 \vee P_2$ и $\neg P_1 \vee Q$ следует $P_2 \vee Q$. Во втором выводе формула и её отрицание – это P_2, а резолюция приводит к $Q \vee Q \;\Leftrightarrow\; Q$. □

Приведём в качестве неформального примера простую теорему:

Если числа $x, y \in \mathbb{N}$ имеют одинаковую чётность, то $x + y$ – чётно.

◁ Рассмотрим два случая: $P_1 : \mathrm{Even}(x) \,\&\, \mathrm{Even}(y)$ и $P_2 : \mathrm{Odd}(x) \,\&\, \mathrm{Odd}(y)$.
По условию теоремы $P_1 \vee P_2$ является посылкой.
По определению $\mathrm{Even}(x)$ и P_1, существуют такие $n, m \in \mathbb{N}$, что $x = 2n$ и $y = 2m$. Тогда $x + y = 2(n + m)$ – чётно (Q). Во втором случае P_2 : $x = 2n + 1$, $y = 2m + 1$ и $x + y = 2(n + m + 1)$ также чётно (снова Q). Поэтому теорема истинна. □



• *Доказательство от противного* – исключительно важный обратный метод. В нём, вместо прямого заключения $P \Rightarrow Q$, показывают, что P и *отрицание* Q противоречивы, т.е. из них следует всегда ложное утверждение, подобное $A \,\&\, \neg A \equiv \mathbb{O}$:

$$P \,\&\, \neg Q \;\to\; \mathbb{O} \qquad\Leftrightarrow\qquad P \;\to\; Q.$$

На рисунке область истинности формулы P является подмножеством области истинности Q, поэтому отрицание Q (серый цвет) и P не пересекаются ($P \,\&\, \neg Q \equiv \mathbb{O}$). Несложно видеть, что $\neg(P \,\&\, \neg Q) \;\equiv\; P \to Q$. Дадим также формальное доказательство метода от противного.

◁ Пусть $P \,\&\, \neg Q \;\to\; \mathbb{O}$ истинно. Тогда по определению импликации $P \,\&\, \neg Q$ ложно. Для $\{P, Q\}$ возможно 3 варианта $\{\mathbb{O}, \mathbb{O}\}$, $\{\mathbb{O}, \mathbb{1}\}$ и $\{\mathbb{1}, \mathbb{1}\}$. Для всех них $P \to Q$ истинно. Аналогично для логического следования в обратную сторону. □

Доказательство от противного это очень мощный метод. Существует множество математических утверждений, для которых известно только доказательство от противного.

Косвенное доказательство – это частный случай метода от противного. В нём, вместо $P \to Q$, выясняется, что $\neg Q \to \neg P$. Если это так, то значит справедливо и $P \to Q$:

$$\neg Q \;\to\; \neg P \qquad\Leftrightarrow\qquad P \;\to\; Q.$$

Фактически $\neg Q \to \neg P$ равно $Q \vee \neg P$, что эквивалентно $P \to Q$.

Подобный метод вывода может показаться тривиальной тавтологией. Однако это не так. На практике берут отрицание $\neg Q$. Из этой формулы логически выводят (иногда довольно сложным образом) формулу $\neg P$. Если построен вывод $\neg Q \;\Rightarrow\; \neg P$, то, как мы видели выше, формула $\neg Q \to \neg P$ оказывается тавтологией. Именно на этом этапе, при помощи косвенного доказательства, выводится $P \to Q$. Наконец, если посылка P считается истинной, то по правилу (**MP**) из P и $P \to Q$ выводится Q.

Классический пример рассуждения от противного, доказательство, что

$\sqrt{2}$ – иррационально, т.е. не представимо в виде n/m, где $n, m \in \mathbb{N}$.

◁ В качестве P выступают стандартные аксиомы арифметики.
Необходимо доказать $Q: \;\; \sqrt{2} \neq n/m$, где n/m *несократимая* дробь. Пусть $\neg Q: \;\sqrt{2} = n/m$. Тогда $n^2 = 2m^2$ и следовательно n – чётно, т.е. $n = 2k$. Но тогда $(2k)^2 = 2m^2$ или $m^2 = 2k^2$, т.е. m – также чётно, а это противоречит несократимости дроби n/m. Поэтому Q истинно. □

1.5 Кванторы

• *Исчисление предикатов* начинается, когда в предметную теорию с бесконечным числом сущностей вводятся кванторы существования $\exists$ и всеобщности $\forall$. В ограниченной предметной области, они служат лишь сокращением для конечной цепочки логических связок "$\vee$" и "&". В общем же случае кванторы превращаются в бесконечные конструкции вида:

$$\begin{aligned} \exists_x A(x) \quad &\equiv \quad A(x_1) \vee A(x_2) \vee A(x_3) \vee ..., \\ \forall_x A(x) \quad &\equiv \quad A(x_1) \,\&\, A(x_2) \,\&\, A(x_3) \,\&\, ..., \end{aligned}$$

где $\{x_1, x_2, x_3, ...\}$ – множество значений предметной переменной x (все предметные сущности). Выражение $\exists_x A(x)$ истинно, если существует *хотя бы один* предмет x_i для которого предикат $A(x_i)$ истинен. Аналогично выражение $\forall_x A(x)$ истинно, если предикат $A(x)$ истинен для всех предметов (и для первого, и для второго, и т.д.)

Определить истинность или ложность подобных выражений при помощи таблиц истинности проблематично.

Иногда, соответствующий подтверждающий или опровергающий пример находится быстро. Например, если все $A(x_i)$ при $i < 100000$ истины, а $A(x_{1000000})$ ложен, то и выражение $\forall_x A(x)$ будет ложно. И наоборот, первое же истинное $A(x_i)$ сделает истинным утверждение $\exists_x A(x)$.

Однако, часто перебор предметных констант не приводит к опровергающему для $\forall_x A(x)$ или подтверждающему для $\exists_x A(x)$ примеру. В результате, *опровергнуть* высказывание типа $\forall_x A(x)$, при помощи таблиц истинности можно, а вот *доказать* его таким образом – нельзя (*полуразрешимость* теории предикатов). Никто не способен *бесконечно* долго оценивать предикаты и понятие истинности, основанное на соответствующих таблицах, может оказаться не применимым к подобным формулам.

◇ Например, по теореме Ферма, для всех $n > 2$ нельзя найти таких $x, y, z \in \mathbb{N}$, чтобы выполнялась обобщенная формула Пифагора:

$$\forall_n \forall_x \forall_y \forall_z \big((n > 2) \,\&\, (x > 0) \,\&\, (y > 0) \;\to\; (x^n + y^n \neq z^n)\big).$$

Можно выяснить истинность или ложность каждого предиката: $n > 2$, $x > 0$, $x^n + y^n = z^n$ при данных n, x, y, z. Однако этого нельзя сделать для всей формулы в целом так как пришлось бы просмотреть бесконечное множество чисел. Убедится в правильности такой формулы можно, только построив её вывод из аксиом арифметики (стр. 38). □

• Различные кванторы не перестановочны: "для любого x существует y" не тоже, что "некий y существует для любого x":

$$\forall_x \exists_y A(x,y) \quad \not\equiv \quad \exists_y \forall_x A(x,y).$$

В обыденной жизни подобная неэквивалентность вполне естественна. Пусть $A(x,y)$: "x имеет мать y". Тогда очевидно, что для "любого x существует мать y", тогда как утверждение "некая y является матерью всех людей x" истинно только в очень специфическом мире. Чтобы доказать не общезначимость формулы (т.е. что она не тавтология) достаточно придумать пример где она ложна.

◇ Пусть предметная область – это натуральные числа: $0, 1, ...$, а предикат $A(x,y): \; x < y$. Утверждение $\forall_x \exists_y (x < y)$ истинно ("для каждого x существует y, который его больше"). Утверждение же $\exists_y \forall_x (x < y)$ ложно, так как нет числа, большего *любого* натурального. Пример с матерями и детьми – это также опровергающий пример. □

Тем не менее, далее (стр. 31) мы докажем, что следующая формула является тавтологией:

$$\exists_y \forall_x A(x,y) \quad \to \quad \forall_x \exists_y A(x,y).$$

Стоит её проверить, для $A(x,y)$: "x имеет мать y". Заметим, что в этой и предыдущей формулах область действия кванторов ограничивается только предикатом (кванторы имеют *наивысший приоритет*). В частности, можно было бы написать $\exists_y \forall_x A(x,y) \to \forall_u \exists_v A(u,v)$.

Разберём неперестановочность $\forall_x$ и $\exists_y$ с других позиций. Всеобщность $\forall_x A(x,y)$ связывает переменную x и выражение зависит только от y:

$$\exists_y \forall_x A(x,y) \;\equiv\; \exists_y \big(A(x_1,y) \,\&\, A(x_2,y) \,\&\, A(x_3,y) \,\&\, ...\big),$$

где x_i – все предметы теории, множеству $\mathcal{X} = \{x_1, x_2, ...\}$ которых принадлежит первый аргумент предиката $A(x,y)$. Эта формула истинна, если существует такая константа $\bar{y}$ (одна или несколько), для которой $A(x,\bar{y})$ истинно при *каждом* $x \in \mathcal{X}$, т.е. $\bar{y}$ одинаков для всех x. Связывание сначала квантором существования допускает больше произвола:

$$\forall_x \exists_y A(x,y) \;\equiv\; \forall_x \big(A(x,y_1) \vee A(x,y_2) \vee A(x,y_2) \vee ...\big).$$

Выражение истинно, если для каждого x есть такое y_i, что $A(x,y_i)$ истинно. Следовательно, существует одна или несколько функций $y = f(x)$, для которых $\forall_x \exists_y A(x,y)$ можно заменить на $\forall_x A(x, f(x))$, где $f(x)$ даёт при данном x существующий y. Понятно, что если $A(x,\bar{y})$ истинно для константы $\bar{y}$, то оно будет истинно и для некоторых функций $A(x, f(x))$, по крайней мере константных $f(x) = \bar{y}$ (но, возможно, не только).

- *Однотипные* кванторы, можно переставлять местами:

$$\forall_x \forall_y A(x,y) \equiv \forall_y \forall_x A(x,y),$$
$$\exists_x \exists_y A(x,y) \equiv \exists_y \exists_x A(x,y).$$

В таких формулах иногда будет использоваться сокращение $\forall_{x,y}$: $\forall_x\forall_y$ и аналогично для $\exists$. Таким образом $\forall_{x,y} \equiv \forall_{y,x}$ и $\exists_{x,y} \equiv \exists_{y,x}$. Число аргументов предикатов, входящих в формулу, произвольно. Например, справедливо: $\forall_x \forall_y A(w,x,v,y,z) \equiv \forall_y \forall_x A(w,x,v,y,z)$.

Отрицание можно “проносить” через квантор, меняя его:

$$\neg\forall_x A(x) \equiv \exists_x \neg A(x),$$
$$\neg\exists_x A(x) \equiv \forall_x \neg A(x).$$

(“если не верно для всех x, то есть x для которого ложно”).

Действие *любого* квантора ($\mathcal{Q} = \exists$ или $\forall$) можно расширять, вынося за дизъюнкцию или конъюнкцию (*правила расширения действвия*):

$$\mathcal{Q}_x A(x) \,\&\, B \equiv \mathcal{Q}_x \big(A(x) \,\&\, B\big),$$
$$\mathcal{Q}_x A(x) \vee B \equiv \mathcal{Q}_x \big(A(x) \vee B\big),$$

где отсутствие явного указания у предиката B аргумента x означает, что он от x не зависит, а при отсутствии скобок *приоритет кванторов* считается *максимальным*, т.е. $\forall_x A(x) \,\&\, \dots$ – это $(\forall_x A(x)) \,\&\, \dots$ и т.д.

Наконец, для родственных операций ($\&$ для $\forall$ и $\vee$ для $\exists$) можно объединять кванторы (*правила объединения*):

$$\forall_x \forall_y \big(A(x) \,\&\, B(y)\big) \equiv \forall_x \big(A(x) \,\&\, B(x)\big),$$
$$\exists_x \exists_y \big(A(x) \vee B(y)\big) \equiv \exists_x \big(A(x) \vee B(x)\big).$$

Полезны также *тождества разбиения*:

$$\forall_x \forall_y A(x,y) \equiv \forall_x A(x,x) \,\&\, \forall_x\forall_y \big(x \neq y \to A(x,y)\big),$$
$$\exists_x \exists_y A(x,y) \equiv \exists_x A(x,x) \vee \exists_x\exists_y \big(x \neq y \;\&\; A(x,y)\big).$$

Для конечных предметных областей все эти тождества несложно доказать при помощи алгебры логики, записав квантор всеобщности как цепочку логических И, а квантор существования как цепочку логических ИЛИ. Постулируется, что все эти тождества справедливы не только для конечных, но и для *бесконечных* множеств.

• Перестановочность кванторов непосредственно следует из коммутативности $A \,\&\, B \equiv B \,\&\, A$ и правил поглощения $A \,\&\, A \equiv A$.

Тождества с отрицанием следуют из правил $\neg(A \,\&\, B) \;\equiv\; \neg A \vee \neg B$:

$$\neg\forall_x A(x) \;\;\equiv\;\; \neg(A_1 \,\&\, A_2 \,\&\, ...) \;\;\equiv\;\; \neg A_1 \vee \neg A_2 \vee ... \;\;\equiv\;\; \exists_x \neg A(x),$$

где $A_i = A(x_i)$. Также легко доказываются правила расширения для родственных операций. Например $\forall_x A(x) \,\&\, B \;\equiv\; \forall_x \big(A(x) \,\&\, B\big)$ это

$$(A_1 \,\&\, A_2 \,\&\, ...) \,\&\, B \equiv (A_1 \,\&\, B) \,\&\, (A_2 \,\&\, B) \,\&\, ...,$$

где учтена ассоциативность, коммутативность и поглощение $B \,\&\, B \equiv B$. Для неродственных операций используется свойство дистрибутивности. Так $\forall_x A(x) \vee B \;\equiv\; \forall_x \big(A(x) \vee B\big)$ это

$$(A_1 \,\&\, A_2 \,\&\, ...) \vee B \equiv (A_1 \vee B) \,\&\, (A_2 \vee B) \,\&\, ...$$

Чтобы обосновать правила объединения кванторов с родственными операциями, распишем в $\forall_x\forall_y \big(A(x) \,\&\, B(y)\big)$ сначала $\forall_y$, а затем $\forall_x$:

$$(A_1 \& B_1) \,\&\, (A_1 \& B_2) \,\&\, (A_1 \& B_3) \,\&\, ...(A_2 \,\&\, B_1) \,\&\, (A_2 \& B_2) \,\&\, (A_2 \,\&\, B_3) \,\&\, ...$$

По свойству поглощения это: $(A_1 \,\&\, B_1) \,\&\, (A_2 \,\&\, B_2) \,\&\, ... \equiv \forall_x\, (A_x \,\&\, B_x)$. Аналогично доказываются тождества разбиения.

• Пусть в теории определён предикат равенства $x = y$, позволяющий выяснять одинаковы ли две сущности x и y. С его помощью можно детализировать количество существующих объектов. Например:

Не более одного объекта $\{0, 1\}$ *обладает свойством* A:

$$\forall_{x,y}\, [A(x) \,\&\, A(y) \to x = y].$$

Один и только один объект $\{1\}$ *обладает свойством* A:

$$\exists_x A(x) \;\;\&\;\; \forall_{x,y}\, [A(x) \,\&\, A(y) \to x = y].$$

Последний вид существования в единственном экземпляре иногда обозначают при помощи квантора с восклицательным знаком: $\exists_x^! A(x)$. Аналогично строятся формулы относительно двух сущностей:

По меньшей мере два объекта $\{2, 3, ...\}$ *обладают свойством* A:

$$\exists_{x,y}\, [A(x) \,\&\, A(y) \,\&\, x \neq y].$$

Не более двух объектов $\{0, 1, 2\}$ *обладают свойством* A:

$$\forall_{x,y,z}\, [A(x) \,\&\, A(y) \,\&\, A(z) \;\to\; (x = y \;\vee\; x = z \;\vee\; y = z)].$$

Объединение двух последних формул логическим "И" приведёт к фразе: "в точности два объекта обладают свойством A". Подобным образом можно говорить о трёх сущностях, и т.д.

1.6 Логическое следование и кванторы

Любой логический вывод должен начинаться с некоторых формул. Их принято называть *гипотезами* или *посылками* вывода. Если в теории есть аксиомы, то они также являются посылками вывода (хотя и не выписываемыми явно). Рассмотрим как из гипотез можно выводить формулы, истинные всегда, когда истинны *все* гипотезы.

Базовой является следующая, достаточно очевидная, цепочка приведения примеров (examples):

$$(\mathbf{Ex}) \qquad \forall_x P(x) \quad \Rightarrow \quad P(x) \quad \Rightarrow \quad \exists_x P(x) \quad \Leftrightarrow \quad P(a).$$

Первое правило *опускания квантора всеобщности* $\forall_x P(x) \;\Rightarrow\; P(x)$ означает, что если утверждение $P(x)$ истинно при любом x, то формула $P(x)$ будет истинна, какое бы значение x в неё не подставили. Обратное следование, вообще говоря, не верно. В частности $P(x) \;\to\; \forall_y P(y)$ не является тавтологией, например, для $P(x_1) \equiv \mathbb{1}$, $P(x_2) \equiv \mathbb{O}$ при $x = x_1$.

Далее идёт одностороннее следование $P(x) \;\Rightarrow\; \exists_x P(x)$, т.е. если $P(x)$ истинно при данном x, то он (по крайней мере) и существует. В обратную сторону такое следствие, в общем случае, также неверно. Наконец, последнее двухстороннее следование означает, что если некий x существует, то для него можно ввести константу a, записав константное высказывание $P(a)$. Это правило необходимо использовать осторожно и константа a не должна совпадать с уже введенными константами (хотя в процессе рассуждений такое совпадение может оказаться и справедливым).

Выводу $\forall_x P(x) \;\Rightarrow\; \exists_x P(x)$ "если $P(x)$ справедливо для всех x, то оно справедливо хотя бы для одного x" соответствует тавтология:

$$\forall_x P(x) \;\to\; \exists_x P(x).$$

$\lhd$ Переименуем связанную переменную в следствии импликации на y. Обозначим для краткости $P_x = P(x)$. Выразим импликацию $X \to Y$ через дизъюнкцию $\neg X \vee Y$ и пронесём отрицание $\neg$ через квантор:

$$\neg(\forall_x P_x) \vee \exists_y P_y \;\Leftrightarrow\; \big(\exists_x \neg P_x\big) \vee \big(\exists_y P_y\big) \;\Leftrightarrow\; \exists_{x,y}(\bar{P}_x \vee P_y) \;\Leftrightarrow\; \exists_x(\bar{P}_x \vee P_x),$$

где в конце учтены правила расширения и объединения (стр. 26). По закону $\bar{P} \vee P \equiv \mathbb{1}$ (стр. 19), эта формула истинна. $\square$

Обратная импликация $\exists_x P_x \to \forall_x P_x$ – это не тавтология. Например, пусть множество имеет два элемента: $\mathcal{X} = \{x_1, x_2\}$ и на нём предикат определён так: $P_1 \equiv \mathbb{O}$, $P_2 \equiv \mathbb{1}$. Понятно, что $\exists_x P_x$ истинно, а $\forall_x P_x$ – ложно, поэтому $\mathbb{1} \to \mathbb{O}$ также ложно.

• Напомним, что переменная x в формуле $P(x)$ является *свободной* если она не связана квантором (не находится под действием $\forall_x$ или $\exists_x$). Формула без свободных переменных называется *замкнутой*. Аксиомы предметных теорий всегда замкнуты.

Пусть в посылках вывода есть формула $P(x)$ со свободной переменной. Она означает некоторую *фиксированную* предметную сущность (одну или несколько) для которой $P(x)$ истинно. Пусть по-мимо $P(x)$ есть ещё замкнутая формула $\forall_x G(x)$. Чтобы при выводе не возникало ошибок, необходимо избегать *коллизии переменных*. Это означает, что имена связанных переменных должны отличаться от имён свободных переменных. Таким образом, если в посылках уже есть $P(x)$, то вместо $\forall_x G(x)$ стоит написать $\forall_y G(y)$.

В замкнутой формуле по правилу (**Ex**) можно опустить квантор всеобщности. Затем в такие формулы вместо переменных *можно* подставлять любые *термы* (константы, переменные, функции), например:

$$\forall_y G(y) \ \stackrel{\mathbf{Ex}}{\Rightarrow} \ G(y) \ \Rightarrow \ G(f(y,z)),$$

где $f(y,z)$ – *всюду определённая* функция (имеет значение при любых y,z). Такую подстановку часто обозначают как $\{f(y,z)/y\}$.

Если в формуле есть связанные переменные, то их не должно быть в подставляемом терме, когда он попадает в область действия квантора. Например, в $\forall_z G(y,z)$ нельзя подставить $\{f(y,z)/y\}$, т.к. z не свободная переменная. Говорят, что терм $t = t(x_1, x_2, ...)$ при подстановке $\{t/x\}$ в формулу $F(x)$ *свободен для* x, если ни какое свободное вхождение x не находится под действием кванторов по переменным x_i, входящим в t. Абсолютно аналогична ситуация в анализе с формулами, содержащими индексы суммирования или переменные интегрирования.

Иначе обстоит дело с переменными, которые в посылках были свободными. В процессе вывода их *нельзя* менять или замещать термами, т.к. при этом есть риск попасть в область значений, где $P(x)$ ложен. Подобные переменные мы будем называть *фиксированными*.

Ко всем не фиксированным переменным можно применять *правило обобщения*, связывая их квантором всеобщности:

(**Gen**) Если x нефиксирован, то $F(x) \ \Rightarrow \ \forall_x F(x)$.

Например, возможен следующий вывод:

$$P(x),\ \forall_y G(y) \ \stackrel{\mathbf{Ex}}{\Rightarrow} \ P(x),\ G(y) \ \Rightarrow \ ... \Rightarrow \ F(x,y) \ \stackrel{\mathbf{Gen}}{\Rightarrow} \ \forall_y F(x,y).$$

При этом квантор $\forall_x$ в финальной формуле поставить нельзя, так как переменная x фиксированна. А вот для "любого" y это сделать можно.

◇ Рассмотрим простой пример применения правил (**Ex**) и (**Gen**). Пусть для *предиката порядка* $x < y$ задана *аксиома транзитивности*:

$$\forall_{x,y,z}\Big[(x<y)\ \&\ (y<z)\ \to\ (x<z)\Big].$$

Докажем, что из $x < 1$ следует формула $\forall_u\big[(1 < u) \to (x < u)\big]$. Посылкой (гипотезой) выступает формула $x < 1$, в которой переменная x фиксирована. Для устранения коллизии, переименуем переменные в аксиоме и по правилу (**Ex**) опустим кванторы всеобщности:

$$(s<t)\ \&\ (t<u)\ \to\ (s<u)\quad\Rightarrow\quad (x<1)\ \&\ (1<u)\ \to\ (x<u),$$

где проведены подстановки в нефиксированные переменные: $\{x/s,\ 1/t\}$. Выразим импликацию через дизъюнкцию и воспользуемся выводом по резолюции (стр. 22), с посылкой $x < 1$:

$$\underline{x<1},\quad \neg(\underline{x<1})\vee\neg(1<u)\vee(x<u)\quad\overset{\mathbf{Res}}{\Rightarrow}\quad\neg(1<u)\vee(x<u).$$

Теперь к не фиксированной переменной u можно применить правило (**Gen**), поставив квантор всеобщности $\forall_u$. Опуская в посылках аксиому (но подразумевая её наличие), окончательно имеем:

$$x<1\quad\Rightarrow\quad\forall_u\big[(1<u)\to(x<u)\big].$$

Заметим, что если бы правило (**Gen**) было применено к фиксированной переменной x, мы бы получили неверную (в арифметике) формулу. □

◇ Ещё одним, исключительно важным примером, является *правило математической индукции*. Пусть есть некоторая формула $P_x = P(x)$, зависящая от натурального числа $x \in \mathbb{N}$. Тогда справедлив вывод:

$$(\mathbf{Ind})\qquad P_0,\quad \forall_x\big[P_x\ \to\ P_{x+1}\big]\quad\Rightarrow\quad\forall_x P_x.$$

Он означает, что если удалось доказать P_x для $x = 0$ (так называемая *база вывода*) и для любого x из P_x следует P_{x+1}, то формула P_x справедлива при всех x.

Обычно, формулу $\forall_x\big[P_x \to P_{x+1}\big]$ получают, строя вывод $P_x \Rightarrow P_{x+1}$. В этом выводе нельзя делать подстановки (x – фиксирован), иначе из любой формулы P_x всегда следовало бы P_{x+1}. Напомним (стр. 21), что если справедлив вывод $P(x) \Rightarrow Q(x)$, то формула $P(x) \to Q(x)$ общезначима при всех x, даже при тех, для которых $P(x)$ ложна. Поэтому, построив вывод $P_x \Rightarrow P_{x+1}$, мы имеем тавтологию $\forall_x(P_x \to P_{x+1})$. Затем, по правилу индукции (**Ind**) можно (если также доказана база P_0) вывести формулу $\forall_x P_x$. Правило (**Ind**) будет многократно применяться при рассмотрении арифметики (стр. 148) и не только. □

• Приведём несколько тавтологий, лежащих в основе *односторонних* правил логического следования. Напомним (стр. 21), что если $A \to B$ – тавтология, то $A \Rightarrow B$ и наоборот.

Кванторы всеобщности можно объединять и для не родственной дизъюнкции, но “в одну сторону”:

$$\forall_x \forall_y \big(A_x \vee B_y\big) \quad \to \quad \forall_x \big(A_x \vee B_x\big).$$

$\lhd$ Неформально: пусть $\forall_x \forall_y \big(A_x \vee B_y\big) \equiv \mathbb{1}$. В бесконечной конъюнкции пар x, y будут диагональные члены $\big(A_1 \vee B_1\big) \,\&\, \big(A_2 \vee B_2\big) \,\&\, ...$ Поэтому следствие также истинно. В остальных случаях импликация равна $\mathbb{1}$. $\Box$

$\lhd$ Формально, от противного. Отрицание этой формулы равно:

$$\neg\big(\neg\forall_{x,y}\,(A_x \vee B_y)\ \vee\ \forall_z\,(A_z \vee B_z)\big) \quad \Leftrightarrow \quad \forall_{x,y}\,\big(A_x \vee B_y\big) \,\&\, \neg\forall_z\,\big(A_z \vee B_z\big).$$

Учтём правило $P \,\&\, Q \Leftrightarrow P,\ Q$ (стр. 21), пронесём $\neg$ через квантор $\forall_z$, а для существующего z, введём константу a:

$$\Leftrightarrow \quad \forall_{x,y}\,\big(A_x \vee B_y\big), \quad \exists_z\,\big(\bar{A}_z \,\&\, \bar{B}_z\big) \quad \overset{\mathbf{Ex}}{\Rightarrow} \quad A_x \vee B_y, \quad \bar{A}_a \,\&\, \bar{B}_a.$$

Сделаем теперь замену $\{a/x,\ a/y\}$ и применим вывод по резолюции:

$$\Rightarrow \quad \underline{A_a} \vee B_a, \quad \underline{\bar{A}_a}, \quad \bar{B}_a \quad \Rightarrow \quad \bar{B}_a, \quad B_a \quad \Leftrightarrow \quad \bar{B}_a \,\&\, B_a \quad \Leftrightarrow \quad \mathbb{O}\,.$$

Получилось противоречие. Поэтому отрицание доказываемой формулы ложно а, сама формула истинна. $\Box$

Похожая формула для существования $\exists_x \exists_y \big(A_x \,\&\, B_y\big) \to \exists_x \big(A_x \,\&\, B_x\big)$ *не является* тавтологией (приведите контрпример $\lessdot\, \mathrm{H}_{10}$). В обратную сторону (разъединение кванторов существования) тождество верно:

$$\exists_x \big[A_x \,\&\, B_x\big] \quad \to \quad \exists_x A_x \ \&\ \exists_y B_y.$$

(если существует такой x, что A_x и B_x одновременно истинны, то понятно, что будет истинно и следствие импликации).

Следующую формулу предлагается самостоятельно доказать при помощи формальных рассуждений ($\lessdot\, \mathrm{H}_{11}$):

$$\exists_x \exists_y\ \big(A_x \,\&\, B_y\big) \quad \to \quad \exists_x A_x.$$

Также доказывается ($\lessdot\, \mathrm{H}_{12}$) и одностороннее правило перестановки кванторов, которое обсуждалось в предыдущем разделе:

$$\exists_y \forall_x A(x,y) \quad \to \quad \forall_x \exists_y A(x,y).$$

В обоих формулах формальные доказательства строятся от противного.

1.7 Силлогизмы

• Кванторы в логике очень древнее изобретение. Достаточно вспомнить аристотелевское:

Все люди бессмертны. Сократ – человек.
Следовательно, Сократ бессмертен.

Введем предметное множество различных существ и предметную константу "s" для идентификации Сократа. Потребуется также два предиката $M(x)$: "x является человеком" и $I(x)$: "x – бессмертен". Тогда в рамках формальной теории этот *силлогизм* (логическое следствие) можно записать так:

$$\forall_x \big(M(x) \to I(x)\big), \qquad M(s) \qquad\quad \Rightarrow \qquad\quad I(s).$$

Из двух посылок (логических утверждений) вводится третья. В такой формальной записи содержательный смысл предикатов не играет роли и этот вывод общезначим (справедлив в любой теории).

Приведём ещё один пример силлогизма:

Всякая блондинка умна. Мэри не умна.
Следовательно, Мэри не является блондинкой.

Введём предикаты $B(x)$: "x – блондинка" и $W(x)$: "x – умна", а также константу m для обозначения бедной Мэри. Формализация рассуждения тогда будет иметь следующую запись:

$$\forall_x (B(x) \to W(x)), \qquad \neg W(m) \qquad \Rightarrow \qquad \neg B(m).$$

Оба вывода обосновываются следующим образом. Квантор всеобщности говорит о всех сущностях и, в частности, о Сократе или Мэри. Поэтому, по правилу (**Ex**), стр. 28, его можно опустить, заменив x на константу: $\forall_x A(x) \Rightarrow A(a)$. В результате получатся обычные формулы из алгебры высказываний, например, $B(m) \to W(m)$. Соответствующие заключения теперь не сложно сделать по резолюции (стр. 22):

$$\neg B(m) \vee \underline{W(m)}, \quad \neg\underline{W(m)} \qquad \Rightarrow \qquad \neg B(m).$$

Важно понимать, что истинность или ложность каждой посылки в силлогизме может быть различной в различных интерпретациях. Понятно, что существует мир (к сожалению, по-видимому наш), в котором утверждение $\forall_x \big(M(x) \to I(x)\big)$ ложно, в прочем, к счастью, также как и утверждение $\forall_x (B(x) \to W(x))$. Однако, *если* посылки истинны, то и следствие будет обязательно истинным. Поэтому из исходных истинных утверждений (аксиом) всегда будут следовать истинные результаты (теоремы).

• Аристотель выделял четыре типа утверждений **A**, **E**, **O**, **I** о двух предикатах $P(x)$, $Q(x)$:

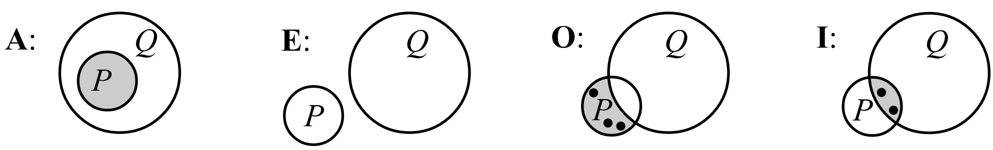
$$
\begin{array}{lcll}
\mathbf{A}(P,Q) & : & \text{все } P \text{ есть } Q & : \ \forall_x\,[P(x)\to\ \ Q(x)],\\
\mathbf{E}(P,Q) & : & \text{все } P \text{ не } Q & : \ \forall_x\,[P(x)\to\neg Q(x)]
\end{array}
$$

Примеры: "все квадраты – прямоугольники", "все млекопитающие – живородящие"; "нет ни одного летающего крокодила", "нет круглых квадратов" (любой x, если он квадрат, то он не круглый). В этих утверждениях важна импликация. Так, мы не говорим "любой является квадратом и прямоугольником", а именно "любой, *если* он квадрат, *то* он будет прямоугольником". К тому же $\forall_x\,[P(x)\,\&\,Q(x)]$ эквивалентно двум утверждениям $\forall_x\,P(x)$ и $\forall_x\,Q(x)$, которые обычно ложны.

$$
\begin{array}{lcll}
\mathbf{O}(P,Q) & : & \text{некоторые } P \text{ не } Q & : \ \exists_x\,[P(x)\,\&\,\neg Q(x)],\\
\mathbf{I}(P,Q) & : & \text{некоторые } P \text{ есть } Q & : \ \exists_x\,[P(x)\,\&\ \ Q(x)].
\end{array}
$$

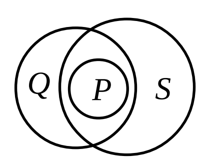
Примеры: "некоторые блондинки умны", "некоторые эллипсы – это окружности", "некоторые грибы не съедобны". В данных случаях не уместна импликация. Мы не скажем "нечто является эллипсом, следовательно это окружность", а именно "бывает нечто являющееся и эллипсом и окружностью". Заметим, что $\neg\mathbf{O}\ \equiv\ \mathbf{A}$, а $\neg\mathbf{I}\ \equiv\ \mathbf{E}$.

Утверждения **A**, **E**, **O**, **I** можно представить, как и множества, при помощи диаграмм Эйлера-Венна на плоскости возможных значений x:



Два утверждения относительно трёх свойств могут логически влечь третье утверждение: $\mathbf{A}(P,Q),\mathbf{A}(Q,S)\Rightarrow\mathbf{A}(P,S)$ ("*если P суть Q, а Q суть S, то P суть S*"). Подобный вывод и называется силлогизмом. Аристотель установил, что логически приемлемыми является 19 таких комбинаций. Правда в последствии оказалось, что 4 из них неявно подразумевают обязательную истинность одного из свойств. Например, т.н. силлогизм Darapti: $\mathbf{A}(P,Q),\ \ \mathbf{A}(P,S)\Rightarrow\mathbf{I}(Q,S)$ или:

$$
\forall_x\,[P(x)\to Q(x)],\ \ \forall_x\,[P(x)\to S(x)]\ \Rightarrow\ \exists_x\,[Q(x)\,\&\,S(x)]
$$



корректен, если дополнительно $\exists_x\,P(x)$. В противном случае, если P пустое множество, то оно принадлежит Q и S, но они могут не пересекаться. Это приводит к тому, что из $\forall_x\,[P(x)\to Q(x)]$, $\forall_x\,[P(x)\to S(x)]$ следует $\exists_x\,[Q(x)\,\&\,S(x)]$, *только* если добавить ещё и $\exists_x\,P(x)$, что стоит формально доказать ($\lessdot\,\mathrm{H}_{13}$) при помощи резолюции.

1.8 Нормальные формы

• Для доказательства истинности некоторого выражения, его можно привести к *конъюнктивной нормальной форме* (КНФ). Чтобы это сделать, сначала избавляются от связок эквивалентности и импликации:

$$A \equiv B \quad \Leftrightarrow \quad (A \to B)\,\&\,(B \to A), \qquad\qquad A \to B \quad \Leftrightarrow \quad \neg A \vee B.$$

Затем, применяя несколько раз правила де-Моргана:

$$\neg(A\,\&\,B) \quad \Leftrightarrow \quad \neg A \vee \neg B, \qquad\qquad \neg(A \vee B) \quad \Leftrightarrow \quad \neg A\,\&\,\neg B$$

и закон двойного отрицания $\neg(\neg A) \quad \Leftrightarrow \quad A$, прижимают символ "$\neg$" к высказываниям, Наконец, при помощи дистрибутивности:

$$A \vee (B\,\&\,C) \quad \Leftrightarrow \quad (A \vee B)\,\&\,(A \vee C),$$

логическому выражению придаётся следующий вид:

$$\boxed{(A_1 \vee A_2 \vee ...)\,\&\,(B_1 \vee B_2 \vee ...)\,\&\,(C_1 \vee C_2 \vee ...)\,\&\,...}$$

Входящие в формулу буквы, являются простыми высказываниями (или предикатами), перед которыми, возможно, стоит отрицание "$\neg$". Это и есть конъюнктивная нормальная форма. Название происходит от соединения при помощи конъюнкций (логических "И") выражений, состоящих только из логических "ИЛИ". Так как операция $\vee$ ассоциативна, скобки внутри *дизъюнктов* ("сумма" $\vee$ в круглых скобках) можно не ставить.

Если формула тождественно истинна (=общезначима=тавтология), то каждый дизъюнкт также должен быть истинным. Поэтому выражение распадается на более *элементарные*:

$$A_1 \vee A_2 \vee ..., \qquad B_1 \vee B_2 \vee ..., \qquad C_1 \vee C_2 \vee ...,$$

каждое из которых должно быть истинным. Произойдёт это, если в каждом из них встретится некоторая буква и её отрицание (*закон исключения третьего* $A \vee \neg A$).

◇ Докажем, что $(A \to B) \to (\neg B \to \neg A)$ – тавтология. Сначала избавимся от импликации "$\to$" и прижмём отрицание к высказываниям:

$$\neg(\neg A \vee B) \vee (\neg\neg B \vee \neg A) \qquad \Leftrightarrow \qquad (A\,\&\,\neg B) \vee (B \vee \neg A).$$

Теперь воспользуемся дистрибутивностью:

$$\Leftrightarrow \qquad (\underline{A} \vee B \vee \neg \underline{A})\,\&\,(\neg \underline{\underline{B}} \vee \underline{\underline{B}} \vee \neg A).$$

Каждая формула соединённая "&", в силу закона "исключения третьего", – истинна. Первая содержит $A \vee \neg A$, а вторая – $B \vee \neg B$. □

• Конъюнктивные нормальные формы играют важную роль при аксиоматическом построении теории, т.к. формулу, записанную в КНФ, можно разбить на более элементарные.

Если формула содержит кванторы всеобщности и существования, перед переводом её в КНФ, кванторы необходимо устранить. Для этого, при помощи кванторных тождеств (стр. 26), их действие распространяется на всю формулу. Запись $\mathcal{Q}_x\mathcal{Q}_y\mathcal{Q}_z...F$, где $\mathcal{Q}$ это $\exists$ или $\forall$, а формула F не содержит кванторов, называется *предварённой нормальной формулой*.

Кванторы существования дают новые предметные константы и функции. Например, формула $\exists_z \forall_x \exists_y A(x, y, z)$ заменяется на $\forall_x A(x,\ f(x),\ a)$, где a – предметная константа (значение "существующего" z) и функция $f(x)$ обозначает тот y, который существует при каждом x. После ликвидации кванторов $\exists$, кванторы $\forall$ опускаются: $\forall_x A(x) \quad \Rightarrow \quad A(x)$ (если справедливо при любом x, то справедливо и в каждом частном случае).

◇ Пусть множество предметов $\mathcal{X}$ состоит из людей и неодушевлённых сущностей. Введем предикат $H(x)$: "x – человек" и $M(x, y)$: "x является матерью для y". Сформулируем утверждение: "каждый человек имеет мать, которая также человек":

$$\forall_x \big[H(x) \to \exists_y \big(H(y) \,\&\, M(y, x)\big)\big].$$

Выразим импликацию через дизъюнкцию и расширим действие $\exists_y$ на всю формулу:

$$\forall_x \exists_y \big[\neg H(x) \vee \big(H(y) \,\&\, M(y, x)\big)\big].$$

Для каждого x существует y, поэтому введём предметную функцию $m(x)$, дающую мать для сущности x и опустим квантор $\exists_y$:

$$\forall_x \big[\neg H(x) \vee \big(H(m(x)) \,\&\, M(m(x), x)\big)\big].$$

Воспользуемся дистрибутивностью:

$$\forall_x \big[\big(\neg H(x) \vee H(m(x))\big) \,\&\, \big(\neg H(x) \vee M(m(x), x)\big)\big].$$

По правилу объединения, можно написать $\forall_x (A_x \,\&\, B_x) \equiv \forall_x A_x \,\&\, \forall_y B_y$, т.е. формула является конъюнкцией двух утверждений. Так она считается истинной, то независимо истинно и каждое утверждение. Поэтому получается две аксиомы предметной теории о людях и их матерях:

$$\neg H(x) \vee H(m(x)), \qquad\qquad \neg H(y) \vee M(m(y), y).$$

Такое представление исходной аксиомы называют *стандартной формой*. Заметим, что в этом примере введение функции $m(x)$ оправдано, так как предполагается, что мать у человека (в этой модели) может быть одна (хотя, это, вообще говоря, самостоятельная аксиома). □

• Иногда необходимо доказать совпадение таблиц истинности двух выражений, не перебирая значения всех переменных. Каждое из выражений можно записать в конъюнктивной нормальной форме. Однако в таком виде их ещё рано сравнивать, т.к. одна и та же формула может иметь различные КНФ. Например, $A \,\&\, B$ эквивалентно $A \,\&\, (A \vee B) \,\&\, (\bar{A} \vee B)$.

Для подобных задач, формулу, записанную в КНФ, представляют в *совершенной конъюнктивной нормальной форме* (СКНФ). Под этим подразумевается следующее. Если формула зависит, например, от трёх высказываний A, B и C, то *каждая* из этих букв *должна* встречаться один раз в каждой из скобок, соединённых логическим "И". Когда в дизъюнкте нет, скажем, буквы B, то при помощи "ИЛИ" в него добавляется всегда ложная формула $B \,\&\, \bar{B}$, не меняющая истинности выражения.

◇ Например: $A \,\&\, B \;\; \Leftrightarrow \; \big(A \vee (B \,\&\, \bar{B})\big) \,\&\, \big(B \vee (A \,\&\, \bar{A})\big)$. Дважды выполним преобразование дистрибутивности: $(A \vee B) \,\&\, (A \vee \bar{B}) \,\&\, (\bar{A} \vee B)$ (второй дизъюнкт $A \vee B$ опущен, т.к. он уже есть). □

Если в СКНФ упорядочить все высказывания, например, по алфавиту, то получится *однозначное выражение*. Число переменных в сравниваемых выражениях должно совпадать. Поэтому перед построением СКНФ применяют правила поглощения, для исключения высказываний, значения которых не влияют на истинность выражения.

◇ Например: $A \,\&\, (A \vee B)$ по описанному алгоритму приводит к формуле $(A \vee B) \,\&\, (A \vee \bar{B})$, хотя и равно A (стр. 19). □

• По таблице истинности можно построить СКНФ, тем самым получив соответствующее ей логическое выражение. Для этого необходимо:

1) отобрать все строки, равные $\mathbb{O}$;
2) перед высказыванием, равным $\mathbb{1}$, поставить отрицание;
3) все высказывания в строке соединить логическим "ИЛИ";
4) строки (равные $\mathbb{O}$) соединить логическим "И":

A	B	F
$\mathbb{O}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{1}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{1}$	$\mathbb{O}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

$$\Leftrightarrow \qquad F = (A \vee B) \,\&\, (\bar{A} \vee B) \,\&\, (A \vee \bar{B}).$$

Такая формула правильно воспроизводит все строчки, дающие $\mathbb{O}$ и автоматически истинна в остальных случаях.

Тавтология в СКНФ от высказываний не зависит (всегда равна $\mathbb{1}$), а ложная формула от n высказываний будет иметь 2^n дизъюнктов.

• Аналогично КНФ или СКНФ можно строить *дизъюнктивную нормальную форму* (ДНФ), и соответствующий ей совершенный вариант (СДНФ). При этом ДНФ определяется как выражение вида:

$$(A_1 \,\&\, A_2 \,\&\, ...) \vee (B_1 \,\&\, B_2 \,\&\, ...) \vee (C_1 \,\&\, C_2 \,\&\, ...) \vee ...,$$

где каждая буква является либо простым высказыванием (предикатом), либо его отрицанием. Таким образом, конъюнкция ("&") и дизъюнкция ("∨") меняются ролями. Преобразование к ДНФ проводится также как и к КНФ, но на финальном этапе используется другой закон дистрибутивности:

$$A \,\&\, (B \vee C) \quad \Leftrightarrow \quad (A \,\&\, B) \vee (A \,\&\, C)$$

Соответственно, для построения СДНФ из ДНФ необходимо добавлять истинное выражение $... \,\&\, (A \vee \neg A)$, которое не изменит истинностного значение конъюнкта, т.к. $B \,\&\, \mathbb{1} \equiv B$.

ДНФ можно использовать для доказательства ложности некоторого выражения. Для этого должны быть ложными все конъюнкты, соединённые логическим "ИЛИ": $(A_1 \,\&\, A_2 \,\&\, ...)$ – ложно, $(B_1 \,\&\, B_2 \,\&\, ...)$ – ложно и т.д. Это, в свою очередь, происходит, когда в каждом из этих выражений встречается некоторая буква и её отрицание. Действительно, $A \,\&\, \neg A$ ложно, а $\mathbb{0} \,\&\, A \equiv \mathbb{0}$.

Алгоритм построения СДНФ по таблице аналогичен СКНФ: отбираются все строки равные $\mathbb{1}$, а перед элементарными высказываниями ставится отрицание, если их значение равно $\mathbb{0}$. Они соединяются при помощи &, а строки при помощи ∨.

• Приведение формулы к КНФ или ДНФ иногда позволяет получить более простое выражение.

◇ Рассмотрим в качестве примера: $A \vee \big((A \to B) \,\&\, C\big)$. Выразим импликацию через дизъюнкцию:

$$A \vee \big((\bar{A} \vee B) \,\&\, C\big) \quad \Leftrightarrow \quad (A \vee \bar{A} \vee B) \,\&\, (A \vee C) \quad \Leftrightarrow \quad A \vee C,$$

где сначала применён закон дистрибутивности. Первый дизъюнкт содержит $A \vee \bar{A}$, поэтому всегда истинен, и без изменения таблицы истинности первую скобку в выражении можно отбросить. В результате, исходная формула равна $A \vee C$ и не зависит от B. Это можно также проверить перебором значений в таблице истинности. □

Иногда выражение сильнее упрощается в КНФ, а иногда в ДНФ, поэтому стоит строить оба представления. В примере с таблицей на предыдущей странице $F = A \,\&\, B$ (СДНФ по последней строке).

1.9 Сигнатура и интерпретация

• При построении формальной теории сначала фиксируется её *сигнатура.* Для этого необходимо задать:

1. *Разновидности* предметных сущностей. В арифметике все предметы одного вида (числа). В геометрии на плоскости может быть два вида предметов – точки $\mathcal{P} = \{x, y, ...\}$ и прямые $\mathcal{L} = \{\alpha, \beta, ...\}$. Если предметы одного вида, то для обозначения произвольного, но фиксированного предмета, обычно, используются латинские буквы из конца алфавита: x, y, z. Они называются *предметными переменными.*

2. *Предметные константы* обозначают выделенные предметы с уникальными именами. В арифметике достаточно двух таких констант: 0 и 1. В геометрии Евклида выделенных констант нет. Константы часто обозначаются буквами из начала алфавита: a, b, c, или специальными символами типа 0 или $\varnothing$.

3. *Предметные функции* – третий и не обязательный элемент сигнатуры. Они ставят в соответствие одним предметам – другие. Если $\mathcal{X}$ множество предметов, то унарная функция $f(x)$ – это отображение $\mathcal{X} \mapsto \mathcal{X}$, бинарная функция $g(x, y)$ – отображение $\mathcal{X} \times \mathcal{X} \mapsto \mathcal{X}$ и т.д. Часто для бинарных функций используется операционная форма: $x + y$, $x \cdot y$. Переменные, константы и функции называются *термами.* Примеры термов: $\varnothing$, x, $f(1, g(z))$.

4. *Предикаты* (отношения в которые вступают сущности) – четвёртый и обязательный элемент сигнатуры. Они зависят от термов и равны истине или лжи. Предикаты обозначаются большими буквами: $A(x)$, $B(x, y)$ или в операционном виде: $x = y$, $\mathcal{A} \subseteq \mathcal{B}$ и т.д. В геометрии есть предикат принадлежности $x \in \alpha$: “точка x лежит на прямой α” и совпадения $\alpha = \beta$. Первый предикат – это отображение $\mathcal{P} \times \mathcal{L} \mapsto \{\mathbb{O}, \mathbb{1}\}$, а второй – $\mathcal{L} \times \mathcal{L} \mapsto \{\mathbb{O}, \mathbb{1}\}$, см. также стр.14.

Если t_i – термы, а $P(x_1, x_2, ...)$ – предикат сигнатуры, то $P(t_1, t_2, ...)$ называется *атомарной формулой.* Из атомарных формул при помощи логических связок и кванторов строиться любая формула.

Одну и ту же теорию можно формулировать в различных сигнатурах. Так, вместо функций можно использовать предикаты (скажем, в арифметике считать истинным $A(x, y, z)$, если $x+y = z$). Предметная область (множество всех сущностей) на этом этапе не фиксируется. Сигнатура только вводит *обозначения* с которыми оперирует теория.

• *Интерпретация* теории – это придание всем символам сигнатуры содержательного (конструктивного) смысла. Для этого необходимо задать *не пустое* множество $\mathfrak{X} = \{a_1, a_2, ...\}$ (конечное или бесконечное, одно или несколько), называемое *носителем интерпретации.* На нём определяется действие функций (например, $f(a_1) = a_2$, $f(a_2) = a_8$, и т.д.). Затем предикатам приписываются истинностные значения (для $E(x, y)$ определить, что $E(a_1, a_1) = \mathbb{1}$, а $E(a_1, a_2) = \mathbb{O}$, и т.д.).

Формула называется *общезначимой* или *тавтологией*, если она истинна на *любой* интерпретации при любой оценке свободных переменных (придании им конкретных значений). Например $\neg A(x) \vee A(x)$ – тавтология. Отметим, что если формула истинна на всех конечных интерпретациях (конечных множествах), она может оказаться ложной для бесконечных множеств (пример: существование максимального элемента в упорядоченных множествах, стр. 120).

Формула называется *невыполнимой* (= противоречивой), если она ложна в любой интерпретации. Пример: $\neg A(x) \,\&\, A(x)$.

Формула называется *выполнимой* (= непротиворечивой), если существует (хотя бы одна) интерпретация, где она истинна. Пример: $A \vee B$.

• Система аксиом любой формальной теории разбивается на две группы – общелогические и предметные аксиомы. *Общелогические аксиомы* – это тавтологии. Например $P \,\&\, Q \equiv Q \,\&\, P$ или $P \to (P \vee Q)$ справедливы в любой теории. В этих аксиомах символы P, Q обозначают любые формулы.

Общелогические аксиомы дополняются *правилами* получения новых формул. К ним относятся правила с кванторами ($\forall_x P_x \;\Rightarrow \exists_x P_x$) или без них ($\neg P \vee Q,\; P \vee S \;\Rightarrow\; Q \vee S$). Понятие истинности при этом отходит на второй план и выведенные формулы считаются верными, даже если их истинность невозможно проверить при помощи таблиц.

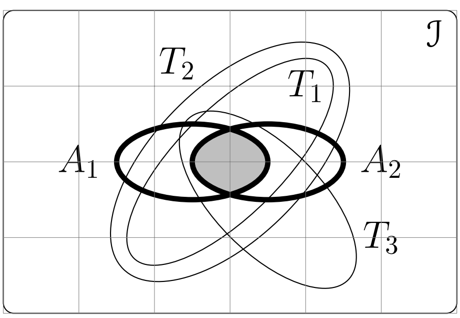
Предметные аксиомы связаны с конкретной сигнатурой (теория чисел, геометрия и т.д.). Они накладывают ограничения на предикаты и функции, *определяя* тем самым их свойства. Общелогические аксиомы и правила вывода создаются "один раз", тогда как предметные аксиомы для каждой новой теории необходимо придумывать заново. Если предикаты зависят только от термов, но не зависят от других предикатов, такая сигнатура называется теорией *предикатов первого порядка.* Например, в арифметике выражение $(x < y) = z$ бессмысленно.

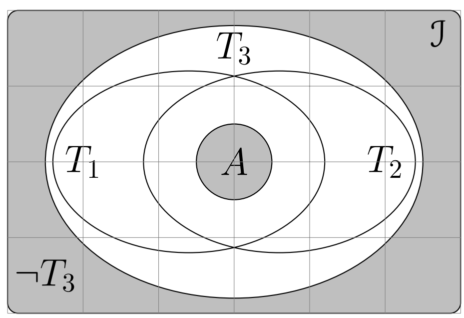
Для одной и той же системы аксиом можно построить различные интерпретации. И наоборот, на некоторых интерпретациях часть аксиом будет выполняться, а часть – нет.

1.10 Множество интерпретаций

• Пусть задана сигнатура предметной теории. Представим (если сможем) *множество интерпретаций* $\mathcal{I}$, элементами которого являются различные интерпретации. Два одинаковых предметных множества, на которых по-разному определены функции и предикаты, являются различными элементами множества интерпретаций. Будем считать, что любая формула, *не содержащая* свободных переменных, в данной интерпретации или истинна или ложна. Тогда на множестве $\mathcal{I}$ существует *подмножество истинности* такой формулы.

Теория, предметные аксиомы A_1, A_2, ... которой пересекаются на множестве $\mathcal{I}$, является *непротиворечивой* (существуют интерпретации на которых аксиомы одновременно выполнимы). Формулы теории $T_1, T_2, T_3, ...$, логически следующие из аксиом, содержат в себе область пересечения аксиом в качестве подмножества. Ниже на левом рисунке приведена теория в которой $A_1, A_2 \Rightarrow T_1, T_2, T_3$. Кроме этого $T_1 \Rightarrow T_2$, однако из T_1 или T_2 не следует T_3:





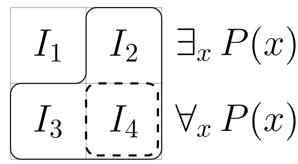
На правом рисунке условно изображён прямой вывод из аксиомы A формулы T_3, с предварительным получением формул T_1 и T_2, которые покрывают бо́льшую область множества интерпретаций, чем A. Затем из них получается T_3: $A \Rightarrow T_1, T_2 \Rightarrow T_3$. Если формул, подобных T_1 и T_2 не существует, то приходится использовать метод от противного.

Не стоит путать множество интерпретаций и носитель интерпретации $\mathcal{X}$, на диаграммах которого ранее иллюстрировались логические функции для предикатов и логическое следование. Любая подобная диаграмма является одной из возможной интерпретаций, т.е. элементом множества всех интерпретаций. Общелогические аксиомы покрывают всё множество интерпретаций.

Множество интерпретаций очень "большое" множество и допущение его существования является достаточно нетривиальным утверждением, требующим доказательства его непротиворечивости. Но даже использование его конечного подмножества часто оказывается эффективным методом установления возможных взаимоотношений между формулами.

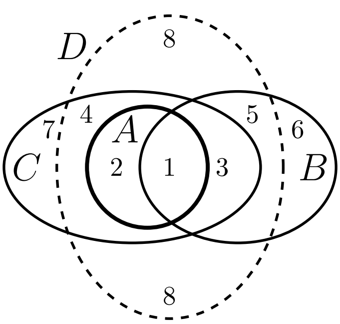
Любой нетривиальный логический вывод увеличивает множество истинности. Рассмотрим, например, вывод $\forall_x P(x) \ \Rightarrow \ \exists_x P(x)$ на множестве из двух элементов $\mathcal{X} = \{a, b\}$. На таком множестве возможно 4 интерпретации, т.е. 4 способа задания истинности $P(a)$ и $P(b)$:

	$P(a)$	$P(b)$	$\forall_x P(x)$	$\exists_x P(x)$
I_1	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$
I_2	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{1}$
I_3	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$
I_4	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

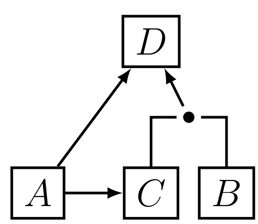


Так, в интерпретации I_2 считаем, что $P(a) \equiv \mathbb{1}$, $P(b) \equiv \mathbb{0}$ и т.д. Посылка вывода (формула $\forall_x P(x)$) истинна только в интерпретации I_4 (пунктир на рисунке), тогда как следствие (формула $\exists_x P(x)$) – в трёх интерпретациях (сплошная линия).

В реальной предметной теории множества истинности формул достаточно затейливо пересекаются. При этом возникают различные взаимосвязи между формулами (возможность логического вывода одних формул из других). Эти взаимосвязи можно отражать на *графе логических следствий*. Рассмотрим модельный пример с четырьмя формулами A, B, C, D, множества истинности которых изображены ниже на рисунке:



	1	2	3	4	5	6	7	8
A	•	•						
B	•		•		•	•		
C	•	•	•	•			•	
D	•	•	•	•	•			•



Объединение множеств A, B, C, D состоит из 8-и непересекающихся областей, номера которых приведены на рисунке. В таблице точками помечены формулы, множества истинности которых попали в ту или иную область. Так, в области 1 пересекаются все четыре формулы.

Последним нарисован граф логических следствий. Множество истинности формулы A является подмножеством C, поэтому $A \Rightarrow C$, что на графе помечено стрелкой от A к C. Пересечение B и C – подмножество D, поэтому $B \,\&\, C \ \Rightarrow D$. На графе это соответствует соединению в узле в виде точки линий от B и C с дальнейшей стрелкой от точки к D.

Несложно видеть, что в этом примере в качестве системы независимых аксиом могут быть выбраны формулы A и B, из которых выводятся C и D. В общем случае систем аксиом может быть более одной.

• В качестве двух примеров, использования интерпретаций, рассмотрим геометрию на плоскости и теорию групп.

▷ Запишем 2 аксиомы геометрии на языке с сигнатурой из множеств $\mathcal{P}$ (точки), $\mathcal{L}$ (прямые) и предикатов $x \in \alpha$ (принадлежность), $x = y$:

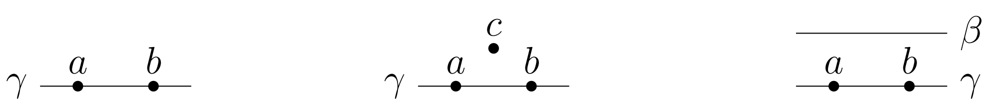
$(\mathbf{A_1})$: $\quad \forall_{x,y}\, \exists_{\alpha}\, (x \in \alpha \;\&\; y \in \alpha)$

Через любые две точки проходит прямая.

$(\mathbf{A_2})$: $\quad \forall_{\alpha}\, \exists_{x,y}\, (x \in \alpha \;\&\; y \in \alpha \;\&\; x \neq y)$

На каждой прямой лежат две различные точки.

Для доказательства *непротиворечивости* аксиом, достаточно найти интерпретацию, где они обе истинны (т.е. их области истинности пересекаются). Это так ($\lessdot$H$_{14}$), когда в $\mathcal{P} = \{a, b\}$ два элемента, а в $\mathcal{L} = \{\gamma\}$ – один и задано $(a \in \gamma) \equiv \mathbb{1}$, $\;(b \in \gamma) \equiv \mathbb{1}$ (ниже 1-й рисунок):



$\mathbf{A_1} \equiv \mathbb{1}$, $\mathbf{A_2} \equiv \mathbb{1}$ $\qquad$ $\mathbf{A_1} \equiv \mathbb{0}$, $\mathbf{A_2} \equiv \mathbb{1}$ $\qquad$ $\mathbf{A_1} \equiv \mathbb{1}$, $\mathbf{A_2} \equiv \mathbb{0}$

На 2-м и 3-ем рисунках даны интерпретации, доказывающие *независимость* аксиом (одна истинна, вторая – ложна, т.е. ни одна не является подмножеством другой). При этом, рисунки не имеют "геометрического смысла" и служат лишь для перечисления элементов множеств и значений предикатов. Например 3-й – это множество $\mathcal{P} = \{a, b\}$, $\mathcal{L} = \{\beta, \gamma\}$, где задано $(a \in \beta) \equiv (b \in \beta) \equiv \mathbb{0}$, $(a \in \gamma) \equiv (b \in \gamma) \equiv \mathbb{1}$. □

◇ Пусть определён предикат равенства $x = y$. Введём функцию $f(x, y)$, которую будем записывать как $x \cdot y$. Зададим аксиомы, определяющие свойства этой функции:

$(\mathbf{D})$: $\quad \forall_{x,y}\, \exists_z\, [x \cdot y = z]$, $\qquad$ определённость,

$(\mathbf{A})$: $\quad \forall_{x,y,z}\; \big[(x \cdot y) \cdot z = x \cdot (y \cdot z)\big]$, $\qquad$ асоциативность.

Интерпретации (множества на которых задана функция $x \cdot y$), где эти аксиомы выполняются (истинны), называют *полугруппами.*

Введём предметную константу e (выделенный единичный элемент) и добавим ещё две аксиомы:

$(\mathbf{E})$: $\quad \forall_x\; [(x \cdot e = x) \;\&\; (e \cdot x = x)]$, $\qquad$ единичный элемент,

$(\mathbf{I})$: $\quad \forall_x \exists_y\, [(x \cdot y = e) \;\&\; (y \cdot x = e)]$, $\qquad$ обратный элемент.

Число интерпретаций, удовлетворяющих такой расширенной системе аксиом, *уменьшается.* Изучением их свойств занимается *теория групп.* Наконец, если добавить ещё одну аксиому:

$(\mathbf{S})$: $\quad \forall_{x,y}\, [x \cdot y = y \cdot x]$, $\qquad$ функция симметрична,

подходящих интерпретаций станет ещё меньше (*абелевы группы*). □

• Рассмотрим примеры интерпретаций аксиом теории групп и докажем их независимость. Предикат равенства $x = y$ будем считать истинным, если x и y – это один и тот же элемент множества $\mathcal{X}$. При таком определении, для задания интерпретации остаётся только перечислить значения функции группового умножения и выбрать единичный элемент. Для одноэлементного множества $\mathcal{X} = \{e\}$ единственная и тривиальная интерпретация, удовлетворяющая всем аксиомам – это: $e \cdot e = e$. Для двухэлементного множества $\mathcal{X} = \{e, a\}$, существует 16 таблиц, определяющих функцию $x \cdot y$ (считаем, что $(\mathbf{D})$ выполняется). С точностью до переобозначения элементов, различных таблиц 10. Три из них приведены ниже:

$$
\begin{array}{c|cc|}
 & e & a \\ \hline
e & e & a \\
a & a & e \\ \hline
\end{array}
\qquad
\begin{array}{c|cc|}
 & e & a \\ \hline
e & e & a \\
a & a & a \\ \hline
\end{array}
\qquad
\begin{array}{c|cc|}
 & e & a \\ \hline
e & e & e \\
a & e & e \\ \hline
\end{array}
\qquad
\begin{array}{c|ccc|}
 & e & a & b \\ \hline
e & e & a & b \\
a & a & e & e \\
b & b & e & e \\ \hline
\end{array}
\qquad
\begin{array}{|cccccc|}
\hline
e & a & b & c & d & f \\
a & b & e & d & f & c \\
b & e & a & f & c & d \\
c & f & d & e & b & a \\
d & c & f & a & e & b \\
f & d & c & b & a & e \\ \hline
\end{array}
$$

1: **A**,**E**,**I**,**S** 2: **A**,**E**,–,**S** 3: **A**,–,**I**,**S** 4: –,**E**,**I**,**S** 5: **A**,**E**,**I**,–

Строчки в таблицах соответствуют первому аргументу функции $x \cdot y$, а колонки – второму. На пересечении строки и колонки, внутри рамки стоит значение функции. Например, первая таблица определяет функцию следующим образом: $e \cdot e = a \cdot a = e$ и $e \cdot a = a \cdot e = a$. Везде выделенный (единичный) элемент обозначен как e.

Первая таблица удовлетворяет всем четырём аксиомам $(\mathbf{A}, \mathbf{E}, \mathbf{I}, \mathbf{S})$, что доказывает их непротиворечивость (интерпретация $\mathcal{X} = \{e\}$, $e \cdot e = e$ – также это доказывает). Для следующей таблицы не выполняется аксиома $(\mathbf{I})$, так как у a нет обратного элемента. Остальные аксиомы выполняются, поэтому $(\mathbf{I})$ независима от $(\mathbf{A}, \mathbf{E}, \mathbf{S})$. Аналогично, третья таблица доказывает независимость аксиомы $(\mathbf{E})$.

Для доказательства независимости аксиомы ассоциативности $(\mathbf{A})$ необходимо уже взять трехэлементное множество $\mathcal{X} = \{e, a, b\}$ с функцией группового умножения, приведенной в четвёртой таблице. Для неё, например $(b \cdot a) \cdot a \neq b \cdot (a \cdot a)$. Остальные же три аксиомы истинны.

Чтобы доказать независимость аксиомы симметричности $(\mathbf{S})$, необходимо множество $\mathcal{X}$ с 6-ю элементами, которое допускает первую, самую маленькую неабелеву группу $\mathbf{D_3}$ (последняя таблица группового умножения с опущенными подписями у строк и столбцов). В этой группе (интерпретации), например, $f \cdot d = a$ и $d \cdot f = b$, т.е. $(\mathbf{S})$ не выполняется.

1.11 Языки и исчисления

Развитие математики идёт по пути придумывания новых символов и правил получения слов, состоящих из этих символов. По большому счёту, математики постоянно играют в различные разновидности одной и той же игры. Эта игра называется “Игрой в слова”. Символы и правила Игры меняются, но часто оказываются причудливо связанными с предыдущими вариантами игры. Иногда выясняется, что целое множество, ранее не связанных между собой игр, можно объединить в одну с очень простыми правилами. Придумывание подобных суперигр доставляет математику наибольшее удовольствие. Любая формальная теория является некоторым языком со своим алфавитом, словами и способами получения (вывода) новых слов. Определим детальнее эти понятия.

Алфавит – непустое, конечное множество Σ символов. *Символом* может быть что угодно, лишь бы мы могли однозначно отличать один символ от другого. Понятие символа не столь тривиально, как кажется на первый взгляд. Один и тот же символ в различных местах “текста” может иметь несколько различное ”написание”. Например, в тексте $ababa$, третья буква чуть отличается от первой и последней. Однако мы, можем договориться считать их одним и тем же символом. Ещё большее разнообразие начертаний символов возникает в рукописных текстах. Таким образом, должен быть способ не только различать, но и надёжно отождествлять символы. Игры в которых символы слов имеют вероятностное значение, обычно не рассматриваются, хотя и очень любопытны. Например, в микромире существуют тождественные частицы, при помощи которых можно кодировать символы. Однако их положение в “тексте” иногда принципиально вероятностное.

Слово – конечная цепочка (упорядоченная последовательность) символов. Число символов в слове называется его длиной. Слово может быть и пустым (нулевой длины). Такое слово часто обозначается как ε. Из двух слов можно получить третье при помощи *конкатенации*. Так, если a_i и b_i – символы, а $\alpha = a_1a_2...a_n$ и $\beta = b_1b_2...b_m$ – слова, то их конкатенация равна $\alpha\beta = a_1a_2...a_nb_1b_2...b_m$. Слово α – это *префикс* (начало) слова $\alpha\beta$, а β – его *суффикс* (окончание). Обращение слова α^R – это слово с обратным порядком букв: $a_n...a_2a_1$. При этом $(\alpha\beta)^R = \beta^R\alpha^R$ и если $\alpha^R = \alpha$, то такое симметричное слово называется *палиндромом*.

Множество всех слов из алфавита Σ обозначают Σ^*. К этому множеству принадлежит и пустое слово ε. Так как алфавит – это конечное множество и слова имеют конечную длину, множество Σ^* счётно (стр. 15).

Язык – это некоторое подмножество $\mathcal{L}$ множества всех слов: $\mathcal{L} \subseteq \Sigma^*$. Пустое слово ε может как присутствовать в языке, так и отсутствовать. Язык, не содержащий слов, как обычно, обозначается символом $\varnothing$ или пустыми скобками $\{\}$. Язык из одного пустого слова – это $\{\varepsilon\}$ и т.д. Предполагается, что существуют правила, которые позволяют отличать слово, входящее в язык, от не принадлежащего ему слова.

◇ В качестве примера, приведём язык $\mathcal{L}_P$ правильно построенных формул логики высказываний (propositions). Его алфавит – это множество символов:

$$\Sigma = \{\neg,\ \&,\ \vee,\ \to,\ \equiv,\ (,\ ),\ X\}.$$

Запятая не является символом, а служит только разделителем. Слово, принадлежащее языку, будем называть *формулой* и зададим по индукции:

- слова (X), (XX), (XXX), ... являются формулами;
- если P и Q формулы, то
  $(\neg P)$, $(P \,\&\, Q)$, $(P \vee Q)$, $(P \to Q)$, $(P \equiv Q)$ – также формулы.

Слова (X), (XX),... – это элементарные высказывания (не содержащие логических связок). Обычно их обозначают отдельными буквами A, B,... из начала алфавита. Впрочем, для введения счётного числа высказываний достаточно одного символа X. Произвольные формулы в книге обозначаются буквами из конца алфавита: $P, Q, R, \ldots$ Они состоят из элементарных высказываний и логических связок. □

Так как языки являются множествами слов, к ними можно применять стандартные множественные операции (объединение, пересечение, вычитание и т.п.) для получения новых языков. Кроме этого возможны и специфические операции. Например, *конкатенация* языков $\mathcal{A}$ и $\mathcal{B}$ – это язык $\mathcal{L} = \mathcal{A} \cdot \mathcal{B} = \{\alpha\beta \mid \alpha \in \mathcal{A},\quad \beta \in \mathcal{B}\}$, т.е. множество всех конкатенаций слов обоих языков.

◇ Пусть есть два *конечных* языка, содержащих по 2 не пустых слова: $\mathcal{A} = \{0,\ 01\}$ и $\mathcal{B} = \{1,\ 11\}$. Тогда $\mathcal{A} \cdot \mathcal{B} = \{01,\ 011,\ 0111\}$. При этом слово $011 \in \mathcal{A} \cdot \mathcal{B}$ получается двумя способами: $0 \cdot 11$ и $01 \cdot 1$ □.

Несложно проверить, что конкатенация языков удовлетворяет следующим тождествам:

$$(\mathcal{A} \cdot \mathcal{B}) \cdot \mathcal{C} = \mathcal{A} \cdot (\mathcal{B} \cdot \mathcal{C}), \qquad \mathcal{A} \cdot \{\varepsilon\} = \{\varepsilon\} \cdot \mathcal{A} = \mathcal{A}.$$

Считается, что конкатенация с пустым множеством $\varnothing$ равна $\varnothing$. Степень языка $\mathcal{L}^n$ это n конкатенаций $\mathcal{L} \cdot \ldots \cdot \mathcal{L}$ и $\mathcal{L}^0 = \{\varepsilon\}$ *Замыканием Клини* $\mathcal{L}^*$ называют объединение всех степеней языка $\mathcal{L}^* = \mathcal{L}^0 \cup \mathcal{L}^1 \cup \mathcal{L}^2 \cup \ldots$

Модель языка – это отображение $\mathcal{L} \mapsto \mathcal{M}$ всех слов языка $\mathcal{L}$, на некоторое множество $\mathcal{M}$, т.е. с каждым словом связывается некоторый элемент множества $\mathcal{M}$. Если задана модель, то говорят, что введена *семантика* ("смысл") слов языка. Обычно элементов в множестве $\mathcal{M}$ существенно меньше, чем слов в языке (хотя это и не обязательно). Бинарной моделью является отображение на множество из двух элементов, которые можно, например, обозначать как $\mathbb{O}$ и $\mathbb{1}$.

$\lhd$ Примером бинарной модели является бинарная логика, изученная в этой главе. Для построения такой модели, необходимо каждому элементарному высказыванию из счётного множества $\mathcal{V} = \{(X), (XX), ...\}$ "присвоить" значение $\mathbb{O}$ или $\mathbb{1}$. Затем задать таблицы истинности для каждой логической связки (стр. 16). В результате будет определено отображение любого слова языка $\mathcal{L}_P$ (правильно построенной формулы) на множество $\mathcal{M} = \{\mathbb{O}, \mathbb{1}\}$. $\square$

В принципе, для языка $\mathcal{L}_P$ можно построить модель с множеством $\mathcal{M}$, состоящим из любого числа элементов. Так, *многозначные логики* предполагают, что значение высказывания может принимать, например, три значения (нет, возможно, да). Могут быть *нечёткие логики* с непрерывным значением истинности в интервале $[0...1]$ и т.д. Всё это различные модели языка $\mathcal{L}_P$. Далее, в соответствии с данным на стр. 39 определением, мы будем называть бинарную модель *интерпретацией* языка.

Если формула (слово $\mathcal{L}_P$) в данной интерпретации $\mathcal{L}_P \mapsto \mathcal{M} = \{\mathbb{O}, \mathbb{1}\}$ соответствует $\mathbb{1}$, то говорят, что она *истинная*. Это обозначается таким образом: $\Rightarrow_{\mathcal{M}} F$. *Тавтология* истинна в *любой* интерпретации: $\Rightarrow F$.

Формула F *логически следует* из формул $\Gamma = \{\Gamma_1, \Gamma_2, ...\}$, т.е. $\Gamma \Rightarrow F$, если для *всякой* интерпретации $\mathcal{M}$, когда *любая* Γ_i истинна: $\Rightarrow_{\mathcal{M}} \Gamma_i$, то истинна и формула: $\Rightarrow_{\mathcal{M}} F$. Вместо символа $\Rightarrow$ часто также используют символ $\models$. Ранее (стр. 21) было показано, что

$$\Gamma_1, ..., \Gamma_n \;\Rightarrow\; F \quad \text{тогда и только тогда, когда} \quad \Rightarrow\; \Gamma_1 \,\&\, ... \,\&\, \Gamma_n \;\to\; F,$$

т.е. логическое следствие F из *посылок* $\Gamma_1, ..., \Gamma_n$ эквивалентно общезначимости формулы $\Gamma_1 \,\&\, ... \,\&\, \Gamma_n \;\to\; F$.

Кроме логического следствия (определяемого при помощи интерпретаций), важную роль играет формальный *вывод*, который будет обозначаться символом $\vdash$. В выводе из одних формул $\Gamma_1, ..., \Gamma_n$ по некоторым *правилам* получаются другие формулы: $\Gamma_1, ..., \Gamma_n \vdash F$. При этом логическая интерпретация формул роли не играет. Вывод – это просто алгоритм получения одних слов из других, чтобы эти слова не обозначали. Дадим соответствующие определения.

Исчислением называют язык $\mathcal{L}$, на алфавите Σ, в котором задано множество слов (формул) $\mathcal{A} = \{A_1, ..., A_m\}$, называемых *аксиомами* и правила вывода $\mathcal{R}$ (получения) новых формул. Правило вывода – это предписание, при помощи которого из n формул определённого вида получается новая формула. Формально, *правило вывода* с n *посылками*, это $n+1$-местное отношение $\mathcal{R} \subseteq \mathcal{L} \times \mathcal{L} \times ... \times \mathcal{L}$ ($n+1$ раз):

$$\Gamma_1, ..., \Gamma_n \ \vdash \ F.$$

Обычно последовательность *посылок* $\Gamma_1, ..., \Gamma_n$ в правиле роли не играет.

Выводом (доказательством) формулы F в данном исчислении называется последовательность формул F_1 , ..., F_m, в которой каждая формула является либо аксиомой, либо получена по некоторому правилу вывода из предшествующих формул, а последняя формула F_m – это F.

◇ Пусть есть алфавит $\Sigma = \{a\ b\}$ из двух символов. Определим исчисление с четырьмя аксиомами:

$$(\mathbf{A_1}):\ a, \qquad (\mathbf{A_2}):\ b, \qquad (\mathbf{A_3}):\ aa, \qquad (\mathbf{A_4}):\ bb$$

и двумя правилами вывода:

$$(\mathbf{R_a}):\ W\ \vdash\ aWa, \qquad (\mathbf{R_b}):\ W\ \vdash\ bWb,$$

где W – любое, ранее выведенное, слово. Выведем, например, в этом исчислении слово $babbab$:

$$\underbrace{bb}_{1:\ \mathbf{A_4}}, \quad \underbrace{abba}_{2:\ \mathbf{R_a}(1)}, \quad \underbrace{babbab}_{3:\ \mathbf{R_b}(2)}.$$

Первое слово вывода (номера стоят под чертой) – это аксиома $(\mathbf{A_4})$. Для получения второго слова, применено правило $(\mathbf{R_a})$, в котором в качестве W взято первое выведенное слово. Аналогично, в конце применяется правило $(\mathbf{R_b})$. Предлагается проверить ($\lessdot$ H_{15}), что в этом языке выводятся только *палиндромы* (слова одинаково читающиеся слева-направо и справа-налево). Зачем нужны $(\mathbf{A_3})$ и $(\mathbf{A_4})$? □

Исчисления делают математические рассуждения формальными на столько, на сколько это по-видимому вообще возможно. Подобные цепочки слов (в $\mathcal{L}_P$ формул) можно загружать в компьютер и он, "не понимая" смысла символов и слов, может проверить корректность вывода и даже самостоятельно такие выводы находить. Следующая глава посвящена построению исчисления высказываний (язык $\mathcal{L}_P$).

1.12 Задачи

∘ $\lessdot$ H$_{16}$: Истинны или ложны высказывания:
"Париж находится в Америке", "1+1=10"?

∘ $\lessdot$ H$_{17}$: Выделить в составных высказываниях элементарные и записать их в формальных обозначениях:

- ∘ Она не любит кошек, но любит собак.
- ∘ Если он выпьет виски, то будет пьян.
- ∘ Вечером они посетят ресторан или останутся дома.

∘ $\lessdot$ H$_{18}$: Перечислить все значения трёх высказываний A, B, C. Сколько комбинаций будет в формуле с 8 различными высказываниями?

∘ $\lessdot$ H$_{19}$: Поставить скобки в: $A \vee B \,\&\, C \to D \vee \neg A$ и $\forall_x A_x \,\&\, \neg \forall_x B_x \to C$.

∘ $\lessdot$ H$_{20}$: Нарисовать деревья формул: $A \to A \vee B$ и $\neg A \vee B \to C$.

∘ $\lessdot$ H$_{21}$: Записать таблицы истинности формул из предыдущей задачи.

∘ При помощи алгебры логики доказать, что следующие формулы являются тавтологиями:

- ∘ H$_{22}$: $(A \vee B) \,\&\, A \equiv A \vee (A \,\&\, B)$,
- ∘ H$_{23}$: $(A \to B) \vee (B \to A)$,
- ∘ H$_{24}$: $A \to (B \to (A \,\&\, B))$,
- ∘ H$_{25}$: $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$.

∘ Используя метод опровержений (см. $\lessdot$ H$_7$) доказать, что следующие формулы являются тавтологиями:

- ∘ $\lessdot$H$_{26}$: $A \to (B \to A)$,
- ∘ $\lessdot$H$_{27}$: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
- ∘ $\lessdot$H$_{28}$: $(\bar{A} \to \bar{B}) \to (B \to A)$,

∘ Записать КНФ формул:

- ∘ $\lessdot$ H$_{29}$: $(A \vee B) \to (A \,\&\, B)$,
- ∘ $\lessdot$ H$_{30}$: $\neg(A \equiv B) \,\&\, A$.

∘ Выразить отрицание, конъюнкцию и дизъюнкцию через:

- ∘ $\lessdot$ H$_{31}$ штрих Шеффера: $A \,|\, B \equiv \neg(A \,\&\, B)$,
- ∘ $\lessdot$ H$_{32}$ стрелку Пирса: $A \uparrow B \equiv \neg(A \vee B)$.

◦ При помощи резолюции доказать следующие логические выводы:.

- ◦ $\lessdot$ Н$_{33}$ $P \to Q, \quad P \vee R \quad \Rightarrow \quad Q \vee R$,
- ◦ $\lessdot$ Н$_{34}$ $P \to Q, \quad P \,\&\, R \quad \Rightarrow \quad Q \,\&\, R$.

◦ $\lessdot$ Н$_{35}$ Доказать от противного: $\forall_n \big(n \in \mathbb{N} \ \& \ \mathrm{Even}(n^2) \quad \to \quad \mathrm{Even}(n)\big)$.

◦ Нарисовать области истинности предикатов на предметном множестве и записать соответствующие формулы:

- ◦ $\lessdot$Н$_{36}$: Не все птицы летают.
- ◦ $\lessdot$Н$_{37}$: Если есть читающие и если каждый читающий умён и любой кто читает – блондинка, то существуют умные блондинки.

◦ Доказать тождества:

- ◦ $\lessdot$Н$_{38}$: $\forall_x (A_x \to B) \ \equiv \ \exists_x A_x \to B$,
- ◦ $\lessdot$Н$_{39}$: $\forall_x (B \to A_x) \ \equiv \ B \to \forall_x A_x$,
- ◦ $\lessdot$Н$_{40}$: $\exists_x (A_x \to B) \ \equiv \ \forall_x A_x \to B$,
- ◦ $\lessdot$Н$_{41}$: $\exists_x (B \to A_x) \ \equiv \ B \to \exists_x A_x$,
- ◦ $\lessdot$Н$_{42}$: $\exists_x (A_x \to B_x) \ \equiv \ \forall_x A_x \to \exists_x B_x$.

◦ Доказать, что эти формулы являются тавтологиями:

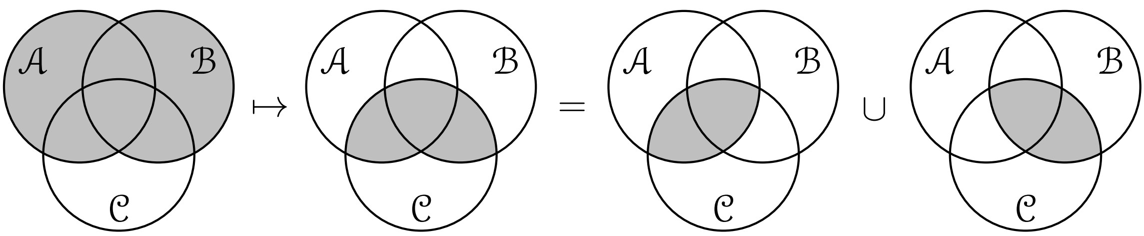
- ◦ $\lessdot$Н$_{43}$: $(\forall_x A_x \to \forall_x B_x) \to \exists_x (A_x \to B_x)$,
- ◦ $\lessdot$Н$_{44}$: $(\exists_x A_x \to \exists_x B_x) \to \exists_x (A_x \to B_x)$,
- ◦ $\lessdot$Н$_{45}$: $(\exists_x A_x \to \forall_x B_x) \to \forall_x (A_x \to B_x)$,
- ◦ $\lessdot$Н$_{46}$: $(\forall_x A_x \vee \forall_x B_x) \ \to \ \forall_x (A_x \vee B_x)$.
- ◦ $\lessdot$Н$_{47}$: $\forall_x (A_x \to B_x) \ \to \ (\forall_x A_x \to \forall_x B_x)$,

◦ ($\lessdot$Н$_{48}$) Напишите аксиомы и правила для исчисления, порождающего палиндромы (стр. 47) с алфавитом $\Sigma = \{a, b, c\}$

Введение в логику

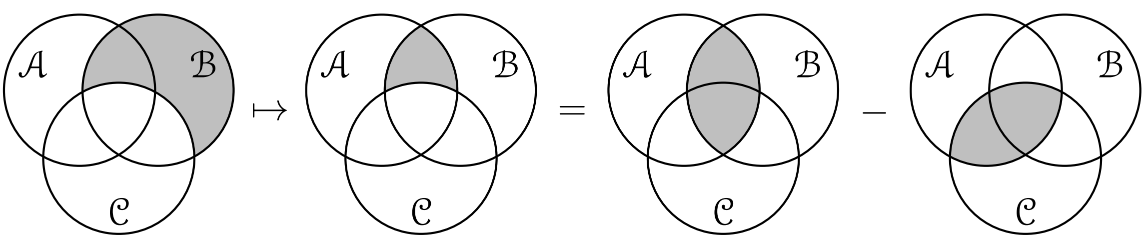
• **H**$_1$ *Число подмножеств множества с n элементами* (стр. 12,17) Если в множестве n элементов, то каждое его подмножество можно закодировать n-значным двоичным числом, где 1 – соответствует наличию элемента, а 0 – его отсутствию. Например, код для $X = \{a, b, c\}$ равен 111, для $\{a, c\}$ – 101, а пустое множество $\{\}$ – это 000. В n-значном двоичном числе на первом месте может стоять 0 или 1 (две возможности). Для *каждой* из этих возможностей, на втором месте снова может стоять 0 или 1 (это уже 4 возможности). Аналогично получается 2^n для вариантов для последовательности, состоящей из n нулей и единиц.

• **H**$_2$ $(\mathcal{A} \cup \mathcal{B}) \cap \mathcal{C} = (\mathcal{A} \cap \mathcal{C}) \cup (\mathcal{B} \cap \mathcal{C})$ (стр. 13)
Для 3-х множеств $\mathcal{A}, \mathcal{B}, \mathcal{C}$ существует 8 возможностей: для $a \in \mathcal{A}$ имеем: $a \notin \mathcal{B}$ и $a \notin \mathcal{C}$ или $a \in \mathcal{B}$ и $a \notin \mathcal{C}$, или $a \in \mathcal{B}$ и $a \in \mathcal{C}$, ... Эти возможности удобно перечислять на диаграммах Эйлера-Венна, нарисовав три пересекающихся круга. На самом деле это лишь наглядное изображение формального перебора возможностей.



$\mathcal{A} \cup \mathcal{B}$ $\quad$ $(\mathcal{A} \cup \mathcal{B}) \cap \mathcal{C}$ $\quad$ $\mathcal{A} \cap \mathcal{C}$ $\quad$ $\mathcal{B} \cap \mathcal{C}$

• **H**$_3$ $\mathcal{A} \cap (\mathcal{B} - \mathcal{C}) = (\mathcal{A} \cap \mathcal{B}) - (\mathcal{A} \cap \mathcal{C})$ (стр. 13)



$\mathcal{B} - \mathcal{C}$ $\quad$ $\mathcal{A} \cap (\mathcal{B} - \mathcal{C})$ $\quad$ $\mathcal{A} \cap \mathcal{B}$ $\quad$ $\mathcal{B} \cap \mathcal{C}$

• **H**$_4$ *Тавтология* $A \vee \neg A$ (стр. 18)

A	$\vee$	$\neg$	A
$\mathbb{0}$			$\mathbb{0}$
$\mathbb{1}$			$\mathbb{1}$

A	$\vee$	$\neg$	A
$\mathbb{0}$		$\mathbb{1}$	$\mathbb{0}$
$\mathbb{1}$		$\mathbb{0}$	$\mathbb{1}$

A	$\vee$	$\neg$	A
$\mathbb{0}$	$\underline{\mathbb{1}}$	$\mathbb{1}$	$\mathbb{0}$
$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{0}$	$\mathbb{1}$

Результирующие значения подчёркнуты и стоят под дизъюнкцией “$\vee$”.

- $\mathbf{H}_5$ $A \to B \;\equiv\; \neg A \vee B$ (стр. 20)

A	$\to$	B	$\equiv$	$\neg$	A	$\vee$	B
$\mathbb{O}$	$\mathbb{1}$	$\mathbb{O}$	$\underline{\mathbb{1}}$	$\mathbb{1}$	$\mathbb{O}$	$\mathbb{1}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{1}$	$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{1}$	$\mathbb{O}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{O}$	$\mathbb{O}$	$\underline{\mathbb{1}}$	$\mathbb{O}$	$\mathbb{1}$	$\mathbb{O}$	$\mathbb{O}$
$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{O}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

- $\mathbf{H}_6$ *Если $P \Rightarrow Q$, то $P \to Q$ – тавтология* (стр. 21)

Импликация $P \to Q$ будет тавтологией, если мы исключим единственную возможность её ложности, когда: $P \equiv \mathbb{1}$ и $Q \equiv \mathbb{O}$. Однако, по определению логического вывода $P \Rightarrow Q$ этого и не может быть (всегда, когда P истинно, должно быть истинно и Q).

- $\mathbf{H}_7$ *Тавтология:* $P \,\&\, (P \to Q) \to Q$ (стр. 21)

Докажем это двумя способами: при помощи булевой алгебры и методом опровержения. В первом способе подставляем определение импликации $P \to Q$: $\neg P \vee Q$ и прижимаем отрицание к формулам P и Q при помощи законов де-Моргана:

$$\neg(P \,\&\, (\neg P \vee Q)) \vee Q \;\;\equiv\;\; \neg P \vee (P \,\&\, \neg Q) \vee Q.$$

Теперь воспользуемся дистрибутивностью $\neg P$ с круглыми скобками и отбросим тождественно истинную формулу $\neg P \vee P \equiv \mathbb{1}$ (так $\mathbb{1} \,\&\, P \equiv P$). Аналогичны и дальнейшие вычисления:

$$\equiv\;\; (\neg P \vee P) \,\&\, (\neg P \vee \neg Q) \vee Q \;\;\equiv\;\; (\neg P \vee \neg Q) \vee Q \;\;\equiv\;\; \neg P \vee \mathbb{1} \;\;\equiv\;\; \mathbb{1}\,.$$

В *методе опровержения* мы пытаемся сделать формулу ложной. Если это не получается, значит она тавтология. Финальная операция в формуле – это вторая импликация. Подписываем под ней $\mathbb{O}$ (подчёркнуто). Импликация ложна, только для $\mathbb{1} \to \mathbb{O}$:

$$\begin{array}{ccccccc} P & \& & (P & \to & Q) & \to & Q. \\ & \mathbb{1} & & & & \underline{\mathbb{O}} & \mathbb{O} \end{array}$$

Продолжаем рассуждения. Конъюнкция будет истинной, если истинны оба её аргумента – подписываем под ними $\mathbb{1}$:

$$\begin{array}{ccccccc} P & \& & (P & \to & Q) & \to & Q. \\ \mathbb{1} & \mathbb{1} & & \mathbb{1} & & \underline{\mathbb{O}} & \mathbb{O} \end{array}$$

Нам уже известно, что $P \equiv \mathbb{1}$ и $Q \equiv \mathbb{O}$. Но в последней импликации это невозможно, т.к. она равна $\mathbb{1}$. Мы пришли к противоречию, следовательно формула не может быть ложной.

• $\mathbf{H}_8$ *Не тавтология:* $A \vee B \to A$ (стр. 21)
Пример: $(\mathbb{O} \vee \mathbb{1}) \to \mathbb{O}$ это $\mathbb{1} \to \mathbb{O}$, что равно $\mathbb{O}$.

• $\mathbf{H}_9$ *Тавтология:* $(P \vee S)\,\&\,(\neg P \vee Q) \;\to\; S \vee Q$ (стр. 22)

$$\neg\big((P \vee S)\,\&\,(\neg P \vee Q)\big) \vee S \vee Q \quad\equiv\quad (\neg P\,\&\,\neg S) \vee (P\,\&\,\neg Q) \vee S \vee Q.$$

Применим дистрибутивность 1-го члена с 3-м и 2-го с 4-м:

$$\equiv\!\big((\neg P \vee S)\,\&\,(\neg S \vee S)\big)\!\vee\!\big((P \vee Q)\,\&\,(\neg Q \vee Q)\big) \equiv \neg P \vee S \vee P \vee Q \equiv \mathbb{1}\,.$$

• $\mathbf{H}_{10}$ *Контрпример для* $\exists_{x,\,y}\big(A_x\,\&\,B_y\big) \to \exists_x\big(A_x\,\&\,B_x\big)$ (стр. 31)
Пусть $\mathcal{X}$ состоит из двух элементов и $A_1 = \mathbb{O}$, $A_2 = \mathbb{1}$, $B_1 = \mathbb{1}$, $B_2 = \mathbb{O}$. Следствие $\exists_x(A_x\,\&\,B_x) \equiv (A_1\,\&\,B_1) \vee (A_2\,\&\,B_2)$ ложно, а посылка $\exists_{x,y}\big(A_x\,\&\,B_y\big)$ – истинна (при $A_2\,\&\,B_1$), т.е. $\mathbb{1} \to \mathbb{O} \equiv \mathbb{O}$.

• $\mathbf{H}_{11}$ $\exists_x\exists_y\,(A_x\,\&\,B_y) \;\to\; \exists_x\,A_x$ (стр. 31)
Доказываем от противного, взяв отрицание формулы:

$$\neg\big(\neg\exists_{x,y}\,(A_x\,\&\,B_y) \vee \exists_x\,A_x\big) \quad\Leftrightarrow\quad \exists_{x,y}\,(A_x\,\&\,B_y)\,\&\,\forall_x\,\neg A_x$$

Применим для $\exists$ правило расширения и вводя две константы, имеем:

$$\Leftrightarrow\quad A_a,\quad B_b,\quad \neg A_x,\quad\Rightarrow\quad A_a,\quad B_b,\quad \neg A_a,\quad\Leftrightarrow\quad \mathbb{O}\,.$$

• $\mathbf{H}_{12}$ $\exists_y\,\forall_x\,A(x,y) \quad\to\quad \forall_x\,\exists_y\,A(x,y).$ (стр. 31)
Доказываем от противного, взяв отрицание формулы:

$$\neg\big(\neg\exists_y\,\forall_x\,A_{x,y} \;\vee\; \forall_x\,\exists_y\,A_{x,y}\big) \quad\Leftrightarrow\quad \exists_y\,\forall_x\,A_{x,y}\;\&\;\exists_x\,\forall_y\,\neg A_{x,y}.$$

Вводя для существований константы a, b, опуская кванторы всеобщности и разбивая на две формулы $(P\,\&\,Q \Leftrightarrow P,\ Q)$, имеем:

$$\Leftrightarrow\quad A_{x,b},\quad \neg A_{a,y}\quad\Rightarrow\quad A_{a,b},\quad \neg A_{a,b}\quad\Leftrightarrow\quad \mathbb{O},$$

где в одностороннем выводе сделаны подстановки $\{x/a,\ y/b\}$.

• $\mathbf{H}_{13}$ *Силлогизм Darapti* (стр. 33)
Покажем справедливость вывода:

$$\exists_x\,P(x),\quad \forall_x\,[P(x) \to Q(x)],\quad \forall_x\,[P(x) \to S(x)] \quad\Rightarrow\quad \exists_x\,[Q(x)\,\&\,S(x)].$$

Вводя для первой посылки существующую константу a и опуская кванторы всеобщности $(\forall_x A(x) \Rightarrow A(x))$, имеем:

$$P(a),\ \neg P(x)\vee Q(x),\ \neg P(y)\vee S(y) \;\;\Rightarrow\;\; P(a),\ \neg P(a)\vee Q(a),\ \neg P(a)\vee S(a),$$

где по правилу $P(x) \Rightarrow P(a)$ для аргументов второй и третей посылки подставлена константа a. Теперь по резолюции первая посылка со второй даёт $Q(a)$, а с третей – $S(a)$. Окончательно:

$$Q(a),\ S(a) \quad\Leftrightarrow\quad Q(a)\,\&\,S(a) \quad\Leftrightarrow\quad \exists_x[Q(x)\,\&\,S(x)].$$

• $\mathbf{H}_{14}$ *Непротиворечивость аксиом геометрии* $(\mathbf{A_1})$ *и* $(\mathbf{A_2})$ (стр. 42)
Так как прямая одна ($\mathcal{P} = \{a, b\}$, $\mathcal{L} = \{\gamma\}$), в аксиоме $(\mathbf{A_1})$ можно опустить квантор существования, положив переменную α равную константе γ, что даёт $\forall_{x,y}\,(x \in \gamma\ \&\ y \in \gamma)$. Распишем кванторы всеобщности:

$$(a \in \gamma\ \&\ a \in \gamma)\,\&\,(a \in \gamma\ \&\ b \in \gamma)\,\&\,(b \in \gamma\ \&\ a \in \gamma)\,\&\,(b \in \gamma\ \&\ b \in \gamma).$$

Это выражение истинно по заданным значениям предиката $x \in \alpha$. Аналогично для аксиомы $(\mathbf{A_2})$.

• $\mathbf{H}_{15}$ *Исчисление палиндромов* (стр. 47)
Аксиомы являются палиндромами. Правила сохраняют свойства слова быть палиндромом. Поэтому все выводимые в исчислении слова – палиндромы.

Если бы не было аксиом $(\mathbf{A_3})$ и $(\mathbf{A_4})$, то центральная часть палиндрома всегда содержала бы нечётное число букв. Благодаря им можно выводить слова $abba$, $baaaab$ и т.п.

• $\mathbf{H}_{16}$ *Париж находится в Америке* (стр. 48)
Истинность высказывания зависит от определения входящих в него понятий.

◦ Если Париж – столица Франции, то это утверждение ложно. Для американского города, расположенного в штате Техас (США), это высказывание истинно.

◦ $1 + 1 = 10$ в десятичной системе ложно, а в двоичной – истинно.

• $\mathbf{H}_{17}$ *Выделение элементарных высказываний* (стр. 48)

◦ Если $(x \heartsuit y)$ – означает "x любит y", то $\neg$(Она$\heartsuit$кошек) & (Она$\heartsuit$собак).

◦ (Он выпил виски)$\to$(Он пьяный).

◦ $(R \,\&\, \neg H) \vee (\neg R \,\&\, H)$, где R: "будут в ресторане", H: "будут дома".

• $\mathbf{H}_{18}$ *Значения трёх высказываний* A, B, C (стр. 48)

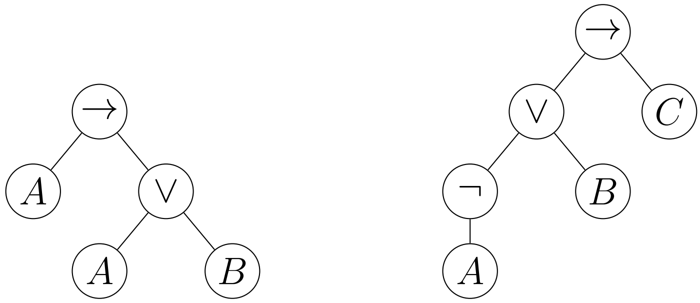
$$\mathbb{O}\,\mathbb{O}\,\mathbb{O},\quad \mathbb{O}\,\mathbb{O}\,\mathbb{1},\quad \mathbb{O}\,\mathbb{1}\,\mathbb{O},\quad \mathbb{O}\,\mathbb{1}\,\mathbb{1},\quad \mathbb{1}\,\mathbb{O}\,\mathbb{O},\quad \mathbb{1}\,\mathbb{O}\,\mathbb{1},\quad \mathbb{1}\,\mathbb{1}\,\mathbb{O},\quad \mathbb{1}\,\mathbb{1}\,\mathbb{1},$$

где, например, комбинация $\mathbb{O}\,\mathbb{1}\,\mathbb{1}$ обозначает $A = \mathbb{O}$, $B = \mathbb{1}$, $C = \mathbb{1}$. Если в формулу входит 8 различных высказываний, то потребуется уже перебрать $256 = 2^8$ комбинаций.

• $\mathbf{H}_{19}$ *Скобки в формулах* (стр. 48)

$$\big(A \vee (B \,\&\, C)\big) \to (D \vee \neg A), \qquad \big((\forall_x A_x) \,\&\, \neg(\forall_y B_y)\big) \to C.$$

- $\mathbf{H}_{20}$ *Деревья формул* (стр. 48)



- $\mathbf{H}_{21}$ *Таблицы истинности* (стр. 48)

A	$\to$	$(A$	$\vee$	$B)$
$\mathbb{0}$	$\underline{\mathbb{1}}$	$\mathbb{0}$	$\mathbb{0}$	$\mathbb{0}$
$\mathbb{0}$	$\underline{\mathbb{1}}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$
$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{0}$
$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

,

$(\neg$	A	$\vee$	$B)$	$\to$	C
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\underline{\mathbb{0}}$	$\mathbb{0}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\underline{\mathbb{1}}$	$\mathbb{1}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\underline{\mathbb{0}}$	$\mathbb{0}$
$\mathbb{1}$	$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\underline{\mathbb{1}}$	$\mathbb{0}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{0}$	$\mathbb{0}$	$\underline{\mathbb{1}}$	$\mathbb{1}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\underline{\mathbb{0}}$	$\mathbb{0}$
$\mathbb{0}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\underline{\mathbb{1}}$	$\mathbb{1}$

- $\mathbf{H}_{22}$ *Тавтология:* $(A \vee B) \,\&\, A \equiv A \vee (A \,\&\, B)$ (стр. 48)

$$(A \vee B) \,\&\, A \quad \Leftrightarrow \quad (A \,\&\, A) \vee (A \,\&\, B) \quad \Leftrightarrow \quad A \vee (A \,\&\, B).$$

- $\mathbf{H}_{23}$ *Тавтология:* $(A \to B) \vee (B \to A)$ (стр. 48)

$$(\bar{A} \vee B) \vee (\bar{B} \vee A) \quad \Leftrightarrow \quad (\bar{A} \vee A) \vee (B \vee \bar{B}) \quad \Leftrightarrow \quad \mathbb{1} \vee \mathbb{1} \quad \Leftrightarrow \quad \mathbb{1}\,.$$

- $\mathbf{H}_{24}$ *Тавтология:* $A \to (B \to (A \,\&\, B))$ (стр. 48)

$$\bar{A} \vee (\bar{B} \vee (A \,\&\, B)) \;\Leftrightarrow\; (\bar{A} \vee \bar{B} \vee A) \,\&\, (\bar{A} \vee \bar{B} \vee B) \;\Leftrightarrow\; (\bar{B} \vee \mathbb{1}) \,\&\, (\bar{A} \vee \mathbb{1}) \;\Leftrightarrow\; \mathbb{1}\,.$$

- $\mathbf{H}_{25}$ $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$ (стр. 48)

$$\neg(\bar{A} \vee B) \vee (\neg(\bar{A} \vee (\bar{B} \vee C)) \vee (\bar{A} \vee C)) \;\Leftrightarrow\; (A \,\&\, \bar{B}) \vee (A \,\&\, B \,\&\, \bar{C}) \vee \bar{A} \vee C$$

$$\Leftrightarrow\; (A \vee \bar{A} \vee C) \,\&\, (\bar{B} \vee \bar{A} \vee C) \vee (A \,\&\, B \,\&\, \bar{C}) \;\Leftrightarrow\; \bar{B} \vee \bar{A} \vee C \vee (A \,\&\, B \,\&\, \bar{C})$$

$$\Leftrightarrow\; (\bar{B} \vee \bar{A} \vee C \vee A) \,\&\, (\bar{B} \vee \bar{A} \vee C \vee B) \,\&\, (\bar{B} \vee \bar{A} \vee C \vee \bar{C}) \;\Leftrightarrow\; \mathbb{1} \,\&\, \mathbb{1} \,\&\, \mathbb{1}\,.$$

- $\mathbf{H}_{26}$ *Тавтология:* $A \to (B \to A)$ *(метод опровержения)* (стр. 48)

A	$\to$	$(B$	$\to$	$A)$
$\mathbb{1}$	$\underline{\mathbb{0}}$	?	$\mathbb{0}$	$\mathbb{1}$

- $\mathbf{H}_{27}$ *Тавтология:* $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

Последовательность рассуждений приведена в строках под формулой:

$$
\begin{array}{ccccccccccccccccc}
(& A & \to & (B & \to & C) &) & \to & (& (A & \to & B) & \to & (A & \to & C) &) \\
 & & \mathbb{1} & & & & & \underline{\mathbb{O}} & & & & & \mathbb{O} & & & & \\
 & & \mathbb{1} & & & & & \underline{\mathbb{O}} & & & \mathbb{1} & & \mathbb{O} & & \mathbb{O} & & \\
 & & \mathbb{1} & & & & & \underline{\mathbb{O}} & & & \mathbb{1} & & \mathbb{O} & \mathbb{1} & \mathbb{O} & \mathbb{O} & \\
 & \mathbb{1} & \mathbb{1} & & & \mathbb{O} & & \underline{\mathbb{O}} & & \mathbb{1} & \mathbb{1} & & \mathbb{O} & \mathbb{1} & \mathbb{O} & \mathbb{O} & \\
 & \mathbb{1} & \mathbb{1} & & & \mathbb{O} & & \underline{\mathbb{O}} & & \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{O} & \mathbb{1} & \mathbb{O} & \mathbb{O} & \\
 & \mathbb{1} & \mathbb{1} & \mathbb{1} & ? & \mathbb{O} & & \underline{\mathbb{O}} & & \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{O} & \mathbb{1} & \mathbb{O} & \mathbb{O} &
\end{array}
$$

- $\mathbf{H}_{28}$ *Тавтология:* $(\bar{A} \to \bar{B}) \to (B \to A)$ *(опровержением)* (стр. 48)

$$
\begin{array}{cccccccccc}
(& \bar{A} & \to & \bar{B} &) & \to & (& B & \to & A &) \\
 & & \mathbb{1} & & & \underline{\mathbb{O}} & & & \mathbb{O} & & \\
 & & \mathbb{1} & & & \underline{\mathbb{O}} & & \mathbb{1} & \mathbb{O} & \mathbb{O} & \\
 & \mathbb{1} & \mathbb{1} & \mathbb{O}? & & \underline{\mathbb{O}} & & \mathbb{1} & \mathbb{O} & \mathbb{O} &
\end{array}
$$

- $\mathbf{H}_{29}$ *КНФ формулы* $(A \vee B) \to (A \,\&\, B)$ (стр. 48)

$$(A \vee \bar{B}) \,\&\, (\bar{A} \vee B).$$

- $\mathbf{H}_{30}$ *КНФ формулы* $\neg(A \equiv B) \,\&\, A$ (стр. 48)

$$[(A \,\&\, \bar{B}) \vee (B \,\&\, \bar{A})] \,\&\, A \quad \Leftrightarrow \quad A \,\&\, \bar{B}.$$

- $\mathbf{H}_{31}$ *Штрих Шеффера* $A|B \equiv \neg(A \,\&\, B)$ (стр. 48)

$$\neg A \equiv A|A, \qquad A \vee B \equiv (A|A)|(B|B), \qquad A \,\&\, B \equiv (A|B)|(A|B).$$

- $\mathbf{H}_{32}$ *Стрелка Пирса* $A \uparrow B \equiv \neg(A \vee B)$ (стр. 48)

$$\neg A \equiv A \uparrow A, \; A \,\&\, B \equiv (A \uparrow A) \uparrow (B \uparrow B), \; A \vee B \equiv (A \uparrow B) \uparrow (A \uparrow B).$$

- $\mathbf{H}_{33}$ $P \to Q, \quad P \vee R \quad \Rightarrow \quad Q \vee R$ (стр. 49)

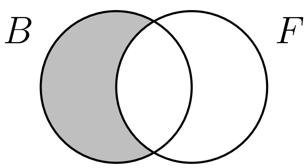
$$\neg \underline{P} \vee Q, \quad \underline{P} \vee R \quad \Rightarrow \quad Q \vee R.$$

- $\mathbf{H}_{34}$ $P \to Q, \quad P \,\&\, R \quad \Rightarrow \quad Q \,\&\, R$ (стр. 49)

$$\neg P \vee Q, \quad P \,\&\, R \quad \Leftrightarrow \quad \neg \underline{P} \vee Q, \quad \underline{P}, \quad R \quad \Rightarrow \quad Q, \quad R \quad \Rightarrow \quad Q \,\&\, R.$$

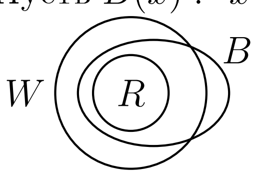
• **H**$_{35}$ $\mathrm{Even}(n^2) \quad \to \quad \mathrm{Even}(n)$ (стр. 49)
От обратного. Пусть n^2 чётно, а n – нечётно. Тогда существует такое k, что $n = 2k+1$, и следовательно $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$. Таким образом n^2 – нечётно. Пришли к противоречию.

• **H**$_{36}$ *Не все птицы летают* (стр. 49)
Пусть $B(x)$: "x является птицей", $F(x)$: "x умеет летать". Тогда "не любой x, если птица, то летает" $\equiv$ "существует x, который птица и не летает".



$$\neg\forall_x(B_x \to F_x) \quad \Leftrightarrow \quad \exists_x(B_x \,\&\, \neg F_x).$$

• **H**$_{37}$ *Блондинки и книжки* (стр. 49)
Пусть $B(x)$: "x – блондинка", $R(x)$: "x умеет читать", $W(x)$: "x – умен".



$$\exists_x R_x \,\&\, \forall_x \big((R_x \to W_x) \,\&\, (R_x \to B_x)\big) \;\to\; \exists_x (B_x \,\&\, W_x).$$

• **H**$_{38}$ $\forall_x (A_x \to B) \;\equiv\; \exists_x A_x \to B$ (стр. 49)
После подстановки определения импликации, используем правило расширения действия квантора в обратную сторону (сужаем действие) и затем проносим отрицание через квантор:

$$\forall_x (A_x \to B) \;\Leftrightarrow\; \forall_x (\neg A_x \vee B) \;\Leftrightarrow\; (\forall_x \neg A_x) \vee B \;\Leftrightarrow\; \neg(\exists_x A_x) \vee B.$$

• **H**$_{39}$ $\forall_x (B \to A_x) \;\equiv\; B \to \forall_x A_x$ (стр. 49)

$$\forall_x (B \to A_x) \;\Leftrightarrow\; \forall_x (\neg B \vee A_x) \;\Leftrightarrow\; \neg B \vee (\forall_x A_x) \;\Leftrightarrow\; B \to \forall_x A_x.$$

• **H**$_{40}$ $\exists_x (A_x \to B) \;\equiv\; \forall_x A_x \to B$ (стр. 49)

$$\exists_x (A_x \to B) \;\Leftrightarrow\; \exists_x (\neg A_x \vee B) \;\Leftrightarrow\; (\exists_x \neg A_x) \vee B \;\Leftrightarrow\; \neg(\forall_x A_x) \vee B.$$

• **H**$_{41}$ $\exists_x (B \to A_x) \;\equiv\; B \to \exists_x A_x$ (стр. 49)

$$\exists_x (B \to A_x) \;\Leftrightarrow\; \exists_x (\neg B \vee A_x) \;\Leftrightarrow\; \neg B \vee (\exists_x A_x) \;\Leftrightarrow\; B \to \exists_x A_x.$$

• **H**$_{42}$ $\exists_x (A_x \to B_x) \;\equiv\; \forall_x A_x \to \exists_x B_x$ (стр. 49)
Используем правило объединения $\exists$ с родственной операцией $\vee$ и расширения в обратную сторону:

$$\exists_x (\neg A_x \vee B_x) \Leftrightarrow \exists_{x,y} (\neg A_x \vee B_y) \Leftrightarrow (\exists_x \neg A_x) \vee (\exists_y B_y) \Leftrightarrow \neg(\forall_x A_x) \vee (\exists_y B_y).$$

• **H**$_{43}$ $(\forall_x A_x \to \forall_x B_x) \to \exists_x (A_x \to B_x)$ (стр. 49)
Так как, если $P \Rightarrow Q$, то $P \to Q$ – тавтология, выведем в формуле следствие из посылки импликации. Переименовываем вторую немую переменную в y, затем проносим отрицание. В одностороннем следовании учитываем правило $\forall_x P_x \Rightarrow \exists_x P_x$ (стр. 28) и правило (H$_{33}$):

$$\neg\forall_x A_x \vee \forall_y B_y \;\Leftrightarrow\; \exists_x \neg A_x \vee \forall_y B_y \;\Rightarrow\; \exists_x \neg A_x \vee \exists_y B_y \;\Leftrightarrow\; \exists_x (\neg A_x \vee B_x).$$

• **H**$_{44}$ $(\exists_x A_x \to \exists_x B_x) \to \exists_x (A_x \to B_x)$ (стр. 49)

$$\neg\exists_x A_x \vee \exists_y B_y \;\Leftrightarrow\; \forall_x \neg A_x \vee \exists_y B_y \;\Rightarrow\; \exists_x \neg A_x \vee \exists_y B_y \;\Leftrightarrow\; \exists_x (\neg A_x \vee B_x).$$

• **H**$_{45}$ $(\exists_x A_x \to \forall_x B_x) \to \forall_x (A_x \to B_x)$ (стр. 49)

$$\neg\exists_x A_x \vee \forall_y B_y \;\Leftrightarrow\; \forall_x \neg A_x \vee \forall_y B_y \;\Rightarrow\; \forall_x (\neg A_x \vee B_y).$$

• **H**$_{46}$ $(\forall_x A_x \vee \forall_x B_x) \to \forall_x (A_x \vee B_x)$ (стр. 49)

$$\forall_x A_x \vee \forall_x B_x \;\Leftrightarrow\; \forall_{x,y} (A_x \vee B_y) \;\Rightarrow\; \forall_x (A_x \vee B_x).$$

• **H**$_{47}$ $\forall_x (A_x \to B_x) \to (\forall_x A_x \to \forall_x B_x)$ (стр. 49)

$$\neg\forall_x (\bar{A}_x \vee B_x) \vee \neg\forall_y A_y \vee \forall_z B_z \;\Leftrightarrow\; \exists_x (A_x \,\&\, \bar{B}_x) \vee \exists_y \bar{A}_y \vee \forall_z B_z$$
$$\Leftrightarrow\; \exists_x ((A_x \,\&\, \bar{B}_x) \vee \bar{A}_x) \vee \forall_z B_z \;\Leftrightarrow\; \exists_x (\bar{A}_x \vee \bar{B}_x) \vee \forall_z B_z$$
$$\Leftrightarrow\; \exists_x \bar{A}_x \vee \neg\forall_z B_z \vee \forall_z B_z \;\Leftrightarrow\; \exists_x \bar{A}_x \vee \mathbb{1} \;\Leftrightarrow\; \mathbb{1}\,.$$

• **H**$_{48}$ *Палиндромы с тремя буквами* (стр. 49)
Аксиомы: a, aa, b, bb, c, cc.
Правила: $W \vdash aWa$, $W \vdash bWb$, $W \vdash cWc$.
