Математическая логика

КТ ИТМО, осень 2023 года

Что такое «правильное рассуждение»?

Логика. Аристотель: 384-322 гг. до н.э.

Математический анализ

Формализация матанализа

- Ньютон, Лейбниц — неформальная идея
- Коши — последовательности вместо бесконечно-малых, пределы
- Вейерштрасс — вещественные числа
- Кантор — теория множеств

Наивная теория множеств

Парадокс брадобрея (Рассела)

- На некотором острове живёт брадобрей, который бреет всех, кто не бреется сам. Бреется ли сам брадобрей?
- Если

$$X = \{x \mid x \notin x\}$$

то что можно сказать про

$$X \in X$$

- - Пусть $X \in X$. Тогда $X : X \notin X$
  - Пусть $X \notin X$. Тогда X должен принадлежать X
- Не совсем парадокс: откуда мы знаем, что X существует? А откуда мы знаем, что вещественные числа существуют?

Программа Гильберта

Высказывание

Высказывание — это строка, сформированная по следующим правилам.

- Атомарное высказывание — пропозициональная переменная: A, B', C_{1234}
- Составное высказывание: если α и β — высказывания, то высказываниями являются:
  - Отрицание: $(\neg\alpha)$
  - Конъюнкция: $(\alpha \,\&\, \beta)$ *или* $(\alpha \wedge \beta)$
  - Дизъюнкция: $(\alpha \vee \beta)$
  - Импликация: $(\alpha \to \beta)$ *или* $(\alpha \supset \beta)$

Пример:

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

Соглашения о записи (метаязык)

- Метапеременные:

$$\alpha, \beta, \gamma, \ldots$$

  Если α — высказывание, то $(\neg\alpha)$ — высказывание

- Метапеременные для пропозициональных переменных:

$$X, Y_n, Z'$$

  Пусть дана пропозициональная переменная X, тогда $(X \,\&\, (\neg X))$ — высказывание

Способы упростить запись

- Приоритет связок: отрицание, конъюнкция, дизъюнкция, импликация
- Ассоциативность: левая для конъюнкции и дизъюнкции, правая для импликации

Пример:

$$((((A \to B)\,\&\,Q) \vee (((\neg B) \to B) \to C)) \vee (C \to (C \to A)))$$

можем записать так:

$$(A \to B)\,\&\,Q \vee ((\neg B \to B) \to C) \vee (C \to C \to A)$$

Теория моделей

Оценка высказываний: как их понимать?

Неформальный пример: $(A \to B) \to (B \to A)$

Давайте попробуем оценить высказывание $(A \to B) \to (B \to A)$.

Если из A следует B, то из B следует A.

Наверное, в общем случае это неверно. Например, пусть:

1. A означает «у меня есть кот»;
2. B означает «у меня есть животное».

Тогда:

1. $A \to B$ выполнена всегда;
2. $B \to A$ может не выполняться: скажем, у меня есть собака, но нет кота.

Оценка высказываний

Высказывание $(A \to B) \to (B \to A)$ ложно, если, например:

- A — «у меня есть кот»;
- B — «у меня есть животное»;
- у меня есть собака, но нет кота.

Иначе: A ложно, B истинно, тогда высказывание ложно.

Чтобы задать оценку высказываний:

- Зафиксируем множество истинностных значений $V = \{И, Л\}$
- Определим функцию оценки переменных (*интерпретацию*) $f : P \to V$
  (P — множество пропозициональных переменных).

Если $[\![A]\!] = Л$ и $[\![B]\!] = И$, то $[\![(A \to B) \to (B \to A)]\!] = Л$

Указание функции оценки (метаязык)

- Синтаксис для указания функции оценки переменных

$$[\![\alpha]\!]^{X_1:=v_1,\ ...,\ X_n:=v_n}$$

- Это всё метаязык — потому полагаемся на здравый смысл

$$[\![A \,\&\, B \,\&\, (C \to C)]\!]^{A:=И,\ B:=[\![\neg A]\!]}$$

Оценим высказывания рекурсивно

- Переменные

$$[\![X]\!] = f(X) \qquad [\![X]\!]^{X:=a} = a$$

- Отрицание

$$[\![\neg\alpha]\!] = \begin{cases} Л, & \text{если } [\![\alpha]\!] = И \\ И, & \text{иначе} \end{cases}$$

- Конъюнкция

$$[\![\alpha \,\&\, \beta]\!] = \begin{cases} И, & \text{если } [\![\alpha]\!] = [\![\beta]\!] = И \\ Л, & \text{иначе} \end{cases}$$

- Дизъюнкция

$$[\![\alpha \vee \beta]\!] = \begin{cases} Л, & \text{если } [\![\alpha]\!] = [\![\beta]\!] = Л \\ И, & \text{иначе} \end{cases}$$

- Импликация

$$[\![\alpha \to \beta]\!] = \begin{cases} Л, & \text{если } [\![\alpha]\!] = И,\ [\![\beta]\!] = Л \\ И, & \text{иначе} \end{cases}$$

Тавтологии

Если α истинна при любой оценке переменных, то она *общезначима* (является *тавтологией*):

$$\models \alpha$$

Выражение $A \to A$ — тавтология. Переберём все возможные значения единственной переменной A:

$$[\![A \to A]\!]^{A:=И} = И$$
$$[\![A \to A]\!]^{A:=Л} = И$$

Выражение $A \to \neg A$ тавтологией не является:

$$[\![A \to \neg A]\!]^{A:=И} = Л$$

Ещё определения

- Если α истинна при любой оценке переменных, при которой истинны высказывания $\gamma_1, \ldots, \gamma_n$, будем говорить, что α — *следствие* этих высказываний:

$$\gamma_1, \ldots, \gamma_n \models \alpha$$

- Истинна при какой-нибудь оценке — *выполнима*.
- Не истинна ни при какой оценке — *невыполнима*.
- Не истинна при какой-нибудь оценке — *опровержима*.

Теория доказательств

- Из чего состоит доказательство (неформально):
  1. Аксиомы — утверждения, от которых отталкиваемся.
  2. Правила вывода — способы делать умозаключения, переходить от одних утверждений к другим.
- Давайте определим формально, что такое аксиомы и правила вывода, и затем дадим формальное определение доказательству как таковому.

Схемы высказываний: определение

Определение (схема высказывания)

Строка, строящаяся по правилам для построения высказываний, с одним отличием — вместо пропозициональных переменных можно указывать маленькие греческие буквы.

По-простому: схемы высказываний — высказывания с метапеременными

Пример

- $(A \to \alpha) \vee (\beta \to B)$
- $(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$
- $A \vee B \,\&\, A$

Схемы высказываний: определение

Определение

Будем говорить, что высказывание σ строится (иначе: задаётся) по схеме Ш, если существует такая замена метапеременных $ч_1$, $ч_2$, ..., $ч_n$ в высказывании на какие-либо выражения φ_1, φ_2, ..., φ_n, что после её проведения получается высказывание σ:

$$\sigma = Ш[ч_1 := \varphi_1][ч_2 := \varphi_2]...[ч_n := \varphi_n]$$

Заметьте, здесь $ч_i$ — мета-метапеременные для метапеременных, а Ш — мета-метапеременная для схем.

Схемы высказываний: примеры

Схема

$$A \to \alpha \vee B \vee \alpha$$

задаёт, к примеру, следующие высказывания:

- $A \to X \vee B \vee X$, при $\alpha := X$.
- $A \to (M \to N) \vee B \vee (M \to N)$, при $\alpha := M \to N$.

и НЕ задаёт следующие высказывания:

- $A \to X \vee B \vee Y$ — все вхождения α должны заменяться одинаково во всём выражении.
- $(A \to (M \to N) \vee B \vee M) \to N$ — структура скобок должна сохраняться.

Аксиомы исчисления высказываний

Определение

Назовём следующие схемы высказываний схемами аксиом исчисления высказываний:

(1) $\alpha \to \beta \to \alpha$

(2) $(\alpha \to \beta) \to (\alpha \to \beta \to \gamma) \to (\alpha \to \gamma)$

(3) $\alpha \to \beta \to \alpha\&\beta$

(4) $\alpha\&\beta \to \alpha$

(5) $\alpha\&\beta \to \beta$

(6) $\alpha \to \alpha \vee \beta$

(7) $\beta \to \alpha \vee \beta$

(8) $(\alpha \to \gamma) \to (\beta \to \gamma) \to (\alpha \vee \beta \to \gamma)$

(9) $(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$

(10) $\neg\neg\alpha \to \alpha$

Все высказывания, которые задаются схемами аксиом, назовём аксиомами исчисления высказываний.

Правило вывода Modus Ponens

Первый, упомянувший правило — Теофраст (древнегреческий философ, IV-III век до н.э.).

Переход по следствию: «сейчас сентябрь; если сейчас сентябрь, то сейчас осень; следовательно, сейчас осень».

Если имеет место α и $\alpha \to \beta$, то имеет место β.

$$\frac{\alpha \quad \alpha \to \beta}{\beta}$$

Доказательство

Определение (доказательство в исчислении высказываний)

Доказательством (выводом) назовём конечную последовательность высказываний $\delta_1, \delta_2, \ldots, \delta_n$, причём каждое δ_i либо:

- *является аксиомой — существует замена метапеременных для какой-либо схемы аксиом, позволяющая получить формулу δ_i, либо*
- *получается из $\delta_1, \ldots, \delta_{i-1}$ по правилу Modus Ponens — существуют такие индексы $j < i$ и $k < i$, что $\delta_k \equiv \delta_j \to \delta_i$.*

Пример:

$A \to (A \to A)$,
$(A \to (A \to A)) \to (A \to ((A \to A) \to A)) \to (A \to A)$,
$(A \to ((A \to A) \to A)) \to (A \to A)$,
$A \to ((A \to A) \to A)$,
$A \to A$

Доказательство подробнее

Почему это доказательство? То же подробнее:

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

$\alpha \to \beta \to \alpha \ [\alpha, \beta := A]$

(2) $(A \to (A \to A)) \to (A \to ((A \to A) \to A)) \to (A \to A)$

$(\alpha \to \beta) \to (\alpha \to \beta \to \gamma) \to (\alpha \to \gamma) \ [\alpha, \gamma := A; \beta := A \to A]$

(3) $(A \to ((A \to A) \to A)) \to (A \to A)$

$$\frac{A \to (A \to A) \quad (A \to (A \to A)) \to (A \to ((A \to A) \to A)) \to (A \to}{(A \to ((A \to A) \to A)) \to (A \to A)}$$

(4) $A \to ((A \to A) \to A)$

$\alpha \to \beta \to \alpha \ [\alpha := A, \beta := A \to A]$

(5) $A \to A$

$$\frac{A \to ((A \to A) \to A) \quad (A \to ((A \to A) \to A)) \to (A \to A)}{A \to A}$$

Дополнительные определения

Определение (доказательство формулы α)

— такое доказательство (вывод) $\delta_1, \delta_2, \ldots, \delta_n$, что $\alpha \equiv \delta_n$. Формула α доказуема (выводима), если существует её доказательство. Обозначение:

$$\vdash \alpha$$

Определение (вывод формулы α из гипотез $\gamma_1, \ldots, \gamma_k$)

— такая последовательность $\delta_1, \ldots, \delta_n$, причём каждое δ_i либо:

- *является аксиомой;*
- *либо получается по правилу Modus Ponens из предыдущих;*
- *либо является одной из гипотез: существует $t : \delta_i \equiv \gamma_t$.*

Формула α выводима из гипотез $\gamma_1, \ldots, \gamma_k$, если существует её вывод. Обозначение:

$$\gamma_1, \ldots, \gamma_k \vdash \alpha$$

Корректность и полнота

Определение (корректность теории)

Теория корректна, если любое доказуемое в ней утверждение общезначимо. То есть, $\vdash \alpha$ *влечёт* $\models \alpha$.

Определение (полнота теории)

Теория полна, если любое общезначимое в ней утверждение доказуемо. То есть, $\models \alpha$ *влечёт* $\vdash \alpha$.

Корректность исчисления высказываний

Лемма (корректность)

Если $\vdash \alpha$, *то* $\models \alpha$

Доказательство.

Индукция по длине вывода n. Для каждого высказывания δ_n из вывода разбор случаев:

1. Аксиома — убедиться, что все аксиомы общезначимы.
2. Modus Ponens j, k — убедиться, что если $\models \delta_j$ и $\models \delta_j \to \delta_n$, то $\models \delta_n$.

$\square$

Общезначимость схемы аксиом №9

Общезначимость схемы аксиом — истинность каждой аксиомы, задаваемой данной схемой, при любой оценке:

$$[\![(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha]\!] = \text{И}$$

Построим таблицу истинности формулы в зависимости от оценки α и β:

$[\![\alpha]\!]$	$[\![\beta]\!]$	$[\![\neg\alpha]\!]$	$[\![\alpha \to \beta]\!]$	$[\![\alpha \to \neg\beta]\!]$	$[\![(\alpha \to \neg\beta) \to \neg\alpha]\!]$	$[\![(\alpha \to \beta) \to (\alpha$
Л	Л	И	И	И	И	И
Л	И	И	И	И	И	И
И	Л	Л	Л	И	Л	И
И	И	Л	И	Л	И	И

Общезначимость заключения правила Modus Ponens

Пусть в выводе есть формулы δ_j, $\delta_k = \delta_j \to \delta_n$, δ_n (причём $j < n$ и $k < n$).

Фиксируем какую-нибудь оценку. По индукционному предположению, δ_j и $\delta_j \to \delta_n$ общезначимы. Поэтому при данной оценке $[\![\delta_j]\!] = \text{И}$ и $[\![\delta_j \to \delta_n]\!] = \text{И}$.

Построим таблицу истинности для импликации:

$[\![\delta_j]\!]$	$[\![\delta_n]\!]$	$[\![\delta_j \to \delta_n]\!]$
Л	Л	И
Л	И	И
И	Л	Л
И	И	И

Из таблицы видно, что $[\![\delta_n]\!] = \text{Л}$ только если $[\![\delta_j \to \delta_n]\!] = \text{Л}$ или $[\![\delta_j]\!] = \text{Л}$. Значит, это невозможно, и $[\![\delta_n]\!] = \text{И}$

Теоремы об исчислении высказываний.

Напоминание: истинность

- Если α истинна при любой оценке переменных, то α общезначима:

$$\models \alpha$$

- Если α истинна при любой оценке переменных, при которой истинны высказывания $\gamma_1, \ldots, \gamma_n$, будем говорить, что α — *следствие* этих высказываний:

$$\gamma_1, \ldots, \gamma_n \models \alpha$$

- Истинна при какой-нибудь оценке — *выполнима*.
- Не истинна ни при какой оценке — *невыполнима*.
- Не истинна при какой-нибудь оценке — *опровержима*.

Выводимость из гипотез

Определение (доказательство формулы α)

— такое доказательство (вывод) $\delta_1, \delta_2, \ldots, \delta_n$, что $\alpha \equiv \delta_n$. Формула α доказуема (выводима), если существует её доказательство. Обозначение:

$$\vdash \alpha$$

Определение (вывод формулы α из гипотез $\gamma_1, \ldots, \gamma_k$)

— такая последовательность $\delta_1, \ldots, \delta_n$, причём каждое δ_i либо:

- *является аксиомой;*
- *либо получается по правилу Modus Ponens из предыдущих;*
- *либо является одной из гипотез: существует $t : \delta_i \equiv \gamma_t$.*

Формула α выводима из гипотез $\gamma_1, \ldots, \gamma_k$, если существует её вывод. Обозначение:

$$\gamma_1, \ldots, \gamma_k \vdash \alpha$$

Корректность и полнота

Определение (корректность теории)

Теория корректна, если любое доказуемое в ней утверждение общезначимо. То есть, $\vdash \alpha$ *влечёт* $\models \alpha$.

Определение (полнота теории)

Теория семантически полна, если любое общезначимое в ней утверждение доказуемо. То есть, $\models \alpha$ *влечёт* $\vdash \alpha$.

Корректность исчисления высказываний

Теорема (корректность)

Если $\vdash \alpha$, *то* $\models \alpha$

Доказательство.

Индукция по длине вывода n.

- База, $n = 1$ — частный случай перехода (без правила Modus Ponens)
- Переход. Пусть для любого доказательства длины n формула δ_n общезначима. Тогда рассмотрим обоснование δ_{n+1} и разберём случаи:
  1. Аксиома — убедиться, что все аксиомы общезначимы.
  2. Modus Ponens j, k — убедиться, что если $\models \delta_j$ и $\models \delta_j \to \delta_{n+1}$, то $\models \delta_{n+1}$.

Общезначимость схемы аксиом №9

Общезначимость схемы аксиом — истинность каждой аксиомы, задаваемой данной схемой, при любой оценке:

$$[\![(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha]\!] = \text{И}$$

Построим таблицу истинности формулы в зависимости от оценки α и β:

$[\![\alpha]\!]$	$[\![\beta]\!]$	$[\![\neg\alpha]\!]$	$[\![\alpha \to \beta]\!]$	$[\![\alpha \to \neg\beta]\!]$	$[\![(\alpha \to \neg\beta) \to \neg\alpha]\!]$	$[\![(\alpha \to \beta) \to (\alpha$
Л	Л	И	И	И	И	И
Л	И	И	И	И	И	И
И	Л	Л	Л	И	Л	И
И	И	Л	И	Л	И	И

Общезначимость заключения правила Modus Ponens

Пусть в выводе есть формулы δ_j, $\delta_k \equiv \delta_j \to \delta_{n+1}$, δ_{n+1} (причём $j < n+1$ и $k < n+1$).

Фиксируем какую-нибудь оценку. По индукционному предположению, δ_j и $\delta_j \to \delta_{n+1}$ общезначимы. Поэтому при данной оценке $[\![\delta_j]\!] \equiv$ И и $[\![\delta_j \to \delta_{n+1}]\!] \equiv$ И.

Построим таблицу истинности для импликации:

$[\![\delta_j]\!]$	$[\![\delta_{n+1}]\!]$	$[\![\delta_j \to \delta_{n+1}]\!]$
Л	Л	И
Л	И	И
И	Л	Л
И	И	И

Из таблицы видно, что $[\![\delta_{n+1}]\!] =$ Л только если $[\![\delta_j \to \delta_{n+1}]\!] =$ Л или $[\![\delta_j]\!] =$ Л. Значит, это невозможно, и $[\![\delta_{n+1}]\!] =$ И

Контекст, метаязык

Будем обозначать большими греческими буквами середины алфавита, возможно с индексами, (Γ, Δ_1, ...) списки формул. Будем использовать, где удобно:

$$\Gamma \vdash \alpha$$

Списки можно указывать через запятую:

$$\Gamma, \Delta, \zeta \vdash \alpha$$

это означает то же, что и

$$\gamma_1, \gamma_2, \ldots, \gamma_n, \delta_1, \delta_2, \ldots, \delta_m, \zeta \vdash \alpha$$

если

$$\Gamma := \{\gamma_1, \gamma_2, \ldots, \gamma_n\}, \quad \Delta := \{\delta_1, \delta_2, \ldots, \delta_m\}$$

Теорема о дедукции

Theorem (О дедукции, Жак Эрбран, 1930)

$\Gamma, \alpha \vdash \beta$ *выполнено тогда и только тогда, когда выполнено* $\Gamma \vdash \alpha \to \beta$

Доказательство «в две стороны», сперва «справа налево».
Пусть $\Gamma \vdash \alpha \to \beta$, покажем $\Gamma, \alpha \vdash \beta$

То есть по условию существует вывод:

$$\delta_1, \delta_2, \ldots, \delta_{n-1}, \alpha \to \beta$$

Тогда следующая последовательность — тоже вывод:

$$\delta_1, \delta_2, \ldots, \delta_{n-1}, \alpha \to \beta, \alpha, \beta$$

Доказательство: $\Gamma \vdash \alpha \to \beta$ влечёт $\Gamma, \alpha \vdash \beta$

№ п/п	формула	пояснение
(1)	δ_1	в соответствии с исходным доказательством
	$\dots$	
$(n-1)$	δ_{n-1}	в соответствии с исходным доказательством
(n)	$\alpha \to \beta$	в соответствии с исходным доказательством
$(n+1)$	α	гипотеза
$(n+2)$	β	Modus Ponens n+1, n

Вывод $\Gamma, \alpha \vdash \beta$ предоставлен, первая часть теоремы доказана.

Доказательство: $\Gamma, \alpha \vdash \beta$ влечёт $\Gamma \vdash \alpha \to \beta$

Пусть даны формулы вывода

$$\delta_1, \delta_2, \ldots, \delta_{n-1}, \beta$$

Аналогично предыдущему пункту, перестроим вывод. Построим «черновик» вывода, приписав α слева к каждой формуле:

$$\alpha \to \delta_1, \alpha \to \delta_2, \ldots, \alpha \to \delta_{n-1}, \alpha \to \beta$$

Данная последовательность формул не обязательно вывод: $\Gamma := \varnothing$, $\alpha := A$

$$\delta_1 := A \to B \to A$$

припишем A слева — вывод не получим:

$$\alpha \to \delta_1 \equiv A \to (A \to B \to A)$$

Последовательности, странная нумерация

Определение (конечная последовательность)

Функция $\delta : 1 \ldots n \to \mathcal{F}$

Определение (конечная последовательность, индексированная дробными числами)

Функция $\zeta : I \to \mathcal{F}$, *где* $I \subset \mathbb{Q}$ *и* $|I| \in \mathbb{N}$

Пример (странный мотивационный пример: язык Фокал)

Программа		*Вывод*
`10.1`	`t n,!`	`= 0.0000`
`10.15`	`s n = n+1`	`= 1.0000`
`10.17`	`i (n-3) 10.1,11.0,11.0`	`= 2.0000`
`11.0`	`t "That's all"`	`That's all`

Доказательство: $\Gamma, \alpha \vdash \beta$ влечёт $\Gamma \vdash \alpha \to \beta$

Доказательство.

(индукция по длине вывода). Если $\delta_1, \ldots, \delta_n$ — вывод $\Gamma, \alpha \vdash \beta$, то найдётся вывод ζ_k для $\Gamma \vdash \alpha \to \beta$, причём $\zeta_1 \equiv \alpha \to \delta_1, \ldots, \zeta_n \equiv \alpha \to \delta_n$.

- База ($n = 1$): частный случай перехода (без М.Р.).
- Переход. Пусть $\delta_1, \ldots, \delta_{n+1}$ — исходный вывод. И пусть (по индукционному предположению) уже по начальному фрагменту $\delta_1, \ldots, \delta_n$ построен вывод ζ_k утверждения $\Gamma \vdash \alpha \to \delta_n$.
  Но δ_{n+1} как-то был обоснован — разберём случаи:
  1. δ_{n+1} — аксиома или $\delta_{n+1} \in \Gamma$
  2. $\delta_{n+1} \equiv \alpha$
  3. δ_{n+1} — Modus Ponens из δ_j и $\delta_k \equiv \delta_j \to \delta_{n+1}$.

  В каждом из случаев можно дополнить черновик до полноценного вывода.

□

Доказательство: $\Gamma, \alpha \vdash \beta$ влечёт $\Gamma \vdash \alpha \to \beta$, случай аксиомы

№ п/п	новый вывод	пояснение
	$\dots$	
(1)	$\alpha \to \delta_1$	
	$\dots$	
(2)	$\alpha \to \delta_2$	
	$\dots$	
(n)	$\alpha \to \delta_n$	
	$\alpha \to \delta_{n+1}$	δ_{n+1} — аксиома, либо $\delta_{n+1} \in \Gamma$

Доказательство: $\Gamma, \alpha \vdash \beta$ влечёт $\Gamma \vdash \alpha \to \beta$, случай аксиомы

№ п/п	новый вывод	пояснение
	$\dots$	
(1)	$\alpha \to \delta_1$	
	$\dots$	
(2)	$\alpha \to \delta_2$	
	$\dots$	
$(n+0.3)$	$\delta_{n+1} \to \alpha \to \delta_{n+1}$	схема аксиом 1
$(n+0.6)$	δ_{n+1}	аксиома, либо $\delta_{n+1} \in \Gamma$
$(n+1)$	$\alpha \to \delta_{n+1}$	M.P. $n+0.6$, $n+0.3$

Доказательство: $\Gamma, \alpha \vdash \beta$ влечёт $\Gamma \vdash \alpha \to \beta$, случай $\delta_i \equiv \alpha$

№ п/п	новый вывод	пояс
	$\dots$	
(1)	$\alpha \to \delta_1$	
	$\dots$	
(2)	$\alpha \to \delta_2$	
	$\dots$	
$(n+0.2)$	$\alpha \to (\alpha \to \alpha)$	Сх. а
$(n+0.4)$	$(\alpha \to (\alpha \to \alpha)) \to (\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to \alpha)$	Сх. а
$(n+0.6)$	$(\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to \alpha)$	M.P.
$(n+0.8)$	$\alpha \to (\alpha \to \alpha) \to \alpha$	Сх. а
$(n+1)$	$\alpha \to \alpha$	M.P.

Доказательство: $\Gamma, \alpha \vdash \beta$ влечёт $\Gamma \vdash \alpha \to \beta$, случай Modus Ponens

№ п/п	новый вывод	пояснение
	$\dots$	
(1)	$\alpha \to \delta_1$	
	$\dots$	
(2)	$\alpha \to \delta_2$	
	$\dots$	
(j)	$\alpha \to \delta_j$	
	$\dots$	
(k)	$\alpha \to \delta_j \to \delta_{n+1}$	
	$\dots$	
$(n+0.3)$	$(\alpha \to \delta_j) \to (\alpha \to \delta_j \to \delta_{n+1}) \to (\alpha \to \delta_{n+1})$	Сх. акс. 2
$(n+0.6)$	$(\alpha \to \delta_j \to \delta_{n+1}) \to (\alpha \to \delta_{n+1})$	M.P. j, $n+$
$(n+1)$	$\alpha \to \delta_{n+1}$	M.P. k, $n+$

Некоторые полезные правила

Лемма (Правило контрапозиции)

Каковы бы ни были формулы α *и* β*, справедливо, что* $\vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$.

Лемма (правило исключённого третьего)

Какова бы ни была формула α, $\vdash \alpha \vee \neg\alpha$.

Лемма (об исключении допущения)

Пусть справедливо $\Gamma, \rho \vdash \alpha$ *и* $\Gamma, \neg\rho \vdash \alpha$*. Тогда также справедливо* $\Gamma \vdash \alpha$.

Доказательство.

Доказывается с использованием лемм, указанных выше. $\square$

Теорема о полноте исчисления высказываний

Теорема

Если $\models \alpha$, *то* $\vdash \alpha$.

Специальное обозначение

Определение (условное отрицание)

Зададим некоторую оценку переменных, такую, что $[\![\alpha]\!] = x$. *Тогда условным отрицанием формулы* α *назовём следующую формулу* $(\!|\alpha|\!)$*:*

$$(\!|\alpha|\!) = \begin{cases} \alpha, & x = \text{И} \\ \neg\alpha, & x = \text{Л} \end{cases}$$

Аналогично записи для оценок, будем указывать оценку переменных, если это потребуется / будет неочевидно из контекста:

$$(\!|\neg X|\!)^{X:=\text{Л}} = \neg X \qquad (\!|\neg X|\!)^{X:=\text{И}} = \neg\neg X$$

Также, если $\Gamma := \gamma_1, \gamma_2, \ldots, \gamma_n$, то за $(\!|\Gamma|\!)$ обозначим $(\!|\gamma_1|\!), (\!|\gamma_2|\!), \ldots (\!|\gamma_n|\!)$.

Таблицы истинности и высказывания

Рассмотрим связку «импликация» и её таблицу истинности:

$[\![A]\!]$	$[\![B]\!]$	$[\![A \to B]\!]$	формула
Л	Л	И	$\neg A, \neg B \vdash A \to B$
Л	И	И	$\neg A, B \vdash A \to B$
И	Л	Л	$A, \neg B \vdash \neg(A \to B)$
И	И	И	$A, B \vdash A \to B$

Заметим, что с помощью условного отрицания данную таблицу можно записать в одну строку:

$$(\!|A|\!), (\!|B|\!) \vdash (\!|A \to B|\!)$$

Полнота исчисления высказываний

Теорема (О полноте исчисления высказываний)

Если $\models \alpha$, *то* $\vdash \alpha$

1. Построим таблицы истинности для каждой связки $(\star)$ и докажем в них каждую строку:

$$(\!|\varphi|\!), (\!|\psi|\!) \vdash (\!|\varphi \star \psi|\!)$$

2. Построим таблицу истинности для α и докажем в ней каждую строку:

$$(\!|\Xi|\!) \vdash (\!|\alpha|\!)$$

3. Если формула общезначима, то в ней все строки будут иметь вид $(\!|\Xi|\!) \vdash \alpha$, потому от гипотез мы сможем избавиться и получить требуемое $\vdash \alpha$.

Шаг 1. Лемма о связках

Запись

$$(\!|\varphi|\!), (\!|\psi|\!) \vdash (\!|\varphi \star \psi|\!)$$

сводится к 14 утверждениям:

$$\begin{array}{rcl}
\neg\varphi, \neg\psi & \vdash & \neg(\varphi \,\&\, \psi) \\
\neg\varphi, \psi & \vdash & \neg(\varphi \,\&\, \psi) \\
\varphi, \neg\psi & \vdash & \neg(\varphi \,\&\, \psi) \\
\varphi, \psi & \vdash & (\varphi \,\&\, \psi) \\
\neg\varphi, \neg\psi & \vdash & \neg(\varphi \vee \psi) \\
\neg\varphi, \psi & \vdash & (\varphi \vee \psi) \\
\varphi, \neg\psi & \vdash & (\varphi \vee \psi) \\
\varphi, \psi & \vdash & (\varphi \vee \psi)
\end{array}$$

$$\begin{array}{rcl}
\neg\varphi, \neg\psi & \vdash & (\varphi \to \psi) \\
\neg\varphi, \psi & \vdash & (\varphi \to \psi) \\
\varphi, \neg\psi & \vdash & \neg(\varphi \to \psi) \\
\varphi, \psi & \vdash & (\varphi \to \psi) \\
\varphi & \vdash & \neg\neg\varphi \\
\neg\varphi & \vdash & \neg\varphi
\end{array}$$

Шаг 2. Обобщение на любую формулу

Лемма (Условное отрицание формул)

Пусть пропозициональные переменные $\Xi := \{X_1, \ldots, X_n\}$ — *все переменные, которые используются в формуле* α. *И пусть задана некоторая оценка переменных.*
Тогда, $(\!|\Xi|\!) \vdash (\!|\alpha|\!)$

Доказательство.

Индукция по длине формулы α.

- База: формула α — атомарная, т.е. $\alpha \equiv X_i$. Тогда при любом Ξ выполнено $(\!|\Xi|\!)^{X_i:=\text{И}} \vdash X_i$ и $(\!|\Xi|\!)^{X_i:=\text{Л}} \vdash \neg X_i$.
- Переход: $\alpha \equiv \varphi \star \psi$, причём $(\!|\Xi|\!) \vdash (\!|\varphi|\!)$ и $(\!|\Xi|\!) \vdash (\!|\psi|\!)$
  Тогда построим вывод:

$(1)\ldots(n)$	$(\!|\varphi|\!)$	индукционное предположение
$(n+1)\ldots(k)$	$(\!|\psi|\!)$	индукционное предположение
$(k+1)\ldots(l)$	$(\!|\varphi \star \psi|\!)$	лемма о связках: $(\!|\varphi|\!)$ и $(\!|\psi|\!)$ доказаны в значит, их можно использовать как ги

□

Шаг 3. Избавляемся от гипотез

Лемма

Пусть при всех оценках переменных $(\!|\Xi|\!) \vdash \alpha$, *тогда* $\vdash \alpha$.

Доказательство.

Индукция по количеству переменных n.

- База: $n = 0$. Тогда $\vdash \alpha$ есть из условия.
- Переход: пусть $(\!|X_1, X_2, \ldots X_{n+1}|\!) \vdash \alpha$. Рассмотрим 2^n пар выводов:

$$\frac{(\!|X_1, X_2, \ldots X_n|\!), \neg X_{n+1} \vdash \alpha \qquad (\!|X_1, X_2, \ldots X_n|\!), X_{n+1} \vdash \alpha}{(\!|X_1, X_2, \ldots X_n|\!) \vdash \alpha}$$

При этом, $(\!|X_1, X_2, \ldots X_n|\!) \vdash \alpha$ при всех оценках переменных $X_1, \ldots X_n$. Значит, $\vdash \alpha$ по индукционному предположению. $\square$

Заключительные замечания

Теорема о полноте — конструктивна. Получающийся вывод — экспоненциальный по длине.
Несложно по изложенному доказательству разработать программу, строящую вывод.
Вывод для формулы с 3 переменными — порядка 3 тысяч строк.

О равенствах

С целью уменьшения нагрузки на символ (=) договоримся об альтернативных символах:

символ	использование
(=)	▶ равенство в предметных языках ▶ равенство чисел, значений в метаязыке (при наличии традиции): $$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$
(:=)	▶ введение обозначений: *пусть* $\Xi := \{x_1, x_2, x_3\}$ ▶ указание значений для модели: $[\![A \to A]\!]^{A:=И}$
(≡)	▶ Равенство строк после подстановки метапеременных: *пусть дано доказательство* $\delta_1, \ldots, \delta_n$, *причём* $\delta_n \equiv \alpha \to \beta$

Интуиционистская логика

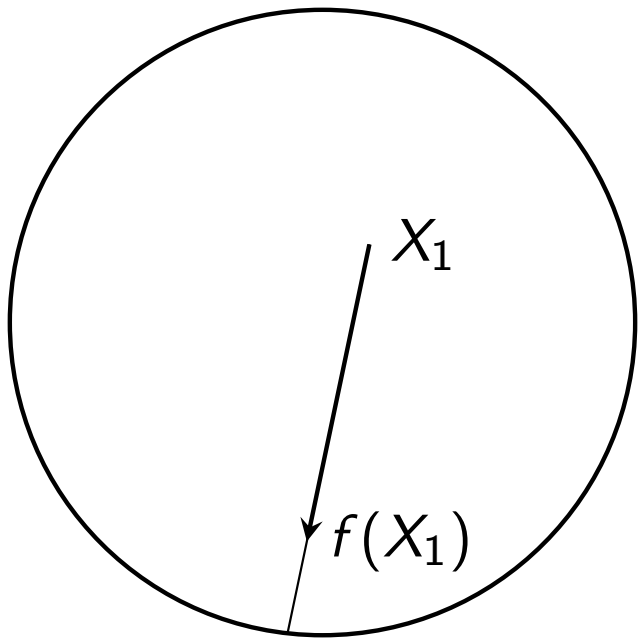
Доказательства чистого существования

Теорема (Брауэра о неподвижной точке)

Любое непрерывное отображение f шара в $\mathbb{R}^n$ на себя имеет неподвижную точку

Доказательство.

Не существует непрерывного отображения шара на границу (без доказательства), однако:



□

Один из примеров подробно

Теорема

Существует пара иррациональных чисел a и b, такая, что a^b — рационально.

- 2^5, 3^3, 7^{10}, $\sqrt{2}^2$ — рациональны;
- $2^{\sqrt{2}}$, e^{π} — иррациональны (как это доказать?);

Один из примеров подробно

Теорема

Существует пара иррациональных чисел a и b, такая, что a^b — рационально.

Доказательство.

Рассмотрим $a = b = \sqrt{2}$ и рассмотрим a^b. Возможны два варианта:

1. $a^b = \sqrt{2}^{\sqrt{2}}$ — рационально;
2. $a^b = \sqrt{2}^{\sqrt{2}}$ — иррационально; отлично, тогда возьмём $a_1 = \sqrt{2}^{\sqrt{2}}$ и получим

$$a_1^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

□

Интуиционизм

“Over de Grondslagen der Wiskunde” (Брауэр, 1907 г.)
Основные положения:

1. Математика не формальна.
2. Математика независима от окружающего мира.
3. Математика не зависит от логики — это логика зависит от математики.

BHK-интерпретация логических связок

BHK — это сокращение трёх фамилий: Брауэр, Гейтинг, Колмогоров.

Пусть α, β — некоторые конструкции, тогда:

- α & β построено, если построены α и β
- $\alpha \vee \beta$ построено, если построено α или β, и мы знаем, что именно
- $\alpha \to \beta$ построено, если есть способ перестроения α в β
- $\bot$ — конструкция, не имеющая построения
- $\neg\alpha$ построено, если построено $\alpha \to \bot$

Дизъюнкция

Конструкция $\alpha \vee \neg\alpha$ не имеет построения в общем случае. Что может быть построено: α или $\neg\alpha$?

Возьмём за α нерешённую проблему, например, $P = NP$

Авторам в данный момент не известно, выполнено $P = NP$ или же $P \neq NP$.

Отличия импликации

Высказывание общезначимо в И.В. и не выполнено в ВНК-интерпретации:

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

Давайте дадим следующий смысл пропозициональным переменным:

- A — 16.09.2023 в Санкт-Петербурге идёт дождь;
- B — 16.09.2023 в Санкт-Петербурге светит солнце;
- C — во 2 семестре староста группы 3239 получил «отлично» по матанализу.

Импликацию можно понимать как «формальную» и как «материальную».

- Материальная импликация $A \to B$ — надо посмотреть в окно.
- Формальная импликация $A \to B$ места не имеет (причинно-следственной связи нет).

Формализация

Формализация интуиционистской логики возможна, но интуитивное понимание — основное.

Определение

Аксиоматика интуиционистского исчисления высказываний в гильбертовском стиле: аксиоматика КИВ, в которой 10 схема аксиом

$$\textit{(10)} \quad \neg\neg\alpha \to \alpha$$

заменена на

$$\textit{(10и)} \quad \alpha \to \neg\alpha \to \beta$$

Немного об общей топологии.

Топологическое пространство

Определение

Топологическим пространством называется упорядоченная пара $\langle X, \Omega \rangle$, *где* X — *некоторое множество, а* $\Omega \subseteq \mathcal{P}(X)$, *причём:*

1. $\varnothing, X \in \Omega$
2. *если* $A_1, \ldots, A_n \in \Omega$, *то* $A_1 \cap A_2 \cap \cdots \cap A_n \in \Omega$;
3. *если* $\{A_\alpha\}$ — *семейство множеств из* Ω, *то и* $\bigcup_\alpha A_\alpha \in \Omega$.

Множество Ω *называется топологией. Элементы* Ω *называются открытыми множествами.*

Определение

$\mathcal{B}$ — *база топологического пространства* $\langle X, \Omega \rangle$ ($\mathcal{B} \subseteq \Omega$), *если всевозможные объединения множеств (в т.ч. пустые) из* $\mathcal{B}$ *дают* Ω.

Примеры топологических пространств

Определение

Евклидово пространство (евклидова топология) на $\mathbb{R}$*: база топологии* $\{(x, y) \mid x, y \in \mathbb{R}\}$.

Определение

Дискретная топология: $\langle X, \mathcal{P}(X) \rangle$ *— все множества открыты.*

Определение

Топология стрелки: $\langle \mathbb{R}, \{(x, +\infty) \mid x \in \mathbb{R}\} \cup \{\varnothing, \mathbb{R}\} \rangle$ *— открыты все положительные лучи.*

Метрические пространства

Определение

Метрикой на X назовём множество, на котором определена функция расстояния $d : X^2 \to \mathbb{R}^+$, удовлетворяющая следующим свойствам:

1. $d(x, y) = 0$ *тогда и только тогда, когда* $x = y$
2. $d(x, y) = d(y, x)$
3. $d(x, z) \leq d(x, y) + d(y, z)$ *(неравенство треугольника)*

Определение

Открытым ε-шаром с центром в точке $x \in X$ назовём $O_\varepsilon(x) = \{t \in X \mid d(x, t) < \varepsilon\}$.

Определение

Если X — некоторое множество и d — метрика на X, то будем говорить, что топологическое пространство, задаваемое базой $\mathcal{B} = \{O_\varepsilon(x) \mid \varepsilon \in \mathbb{R}^+, x \in X\}$, *порождено метрикой d.*

Непрерывность

Определение

Функция $f : X \to Y$ непрерывна, если прообраз любого открытого множества открыт.

Пример

Функция $f : \mathbb{N} \to \mathbb{R}$ всегда непрерывна (при дискретной топологии на $\mathbb{N}$), поскольку любое множество в $\mathbb{N}$ открыто.

Компактность

Определение

Будем говорить, что множество компактно, если из любого его открытого покрытия можно выбрать конечное подпокрытие

Пример

Множество $\{0, 1\}$ *в дискретной топологии компактно.*

Пример

Интервал $(0, 1)$ *в* $\mathbb{R}$ *не компактен — например, рассмотрим покрытие* $\{(\varepsilon, 1) \mid \varepsilon \in (0, 1)\}$

Подпространства и связные множества

Определение

Пространство $\langle X_1, \Omega_1 \rangle$ *— подпространство пространства* $\langle X, \Omega \rangle$, *если* $X_1 \subseteq X$ *и* $\Omega_1 = \{A \cap X_1 | A \in \Omega\}$.

Пример

$[0, 1]$ *с евклидовой топологией на отрезке — подпространство* $\mathbb{R}$. $[0, 0.5)$ *открыто в* $[0, 1]$, *так как* $[0, 0.5) = (-0.5, 0.5) \cap [0, 1]$.

Определение

Пространство $\langle X, \Omega \rangle$ *связно, если нет* $A, B \in \Omega$, *что* $A \cup B = X$, $A \cap B = \varnothing$ *и* $A, B \neq \varnothing$.

Пример

Пространство $(0, 1] \cup [2, 3)$ *в* $\mathbb{R}$ *несвязно: возьмём* $A = (0, 1]$ *и* $B = [2, 3)$.

Дискретное топологическое пространство $\langle X, \mathcal{P}(X) \rangle$ *несвязно при* $|X| > 1$: *пусть* $a \in X$, *тогда* $A = \{a\}$ *и* $B = X \setminus A$.

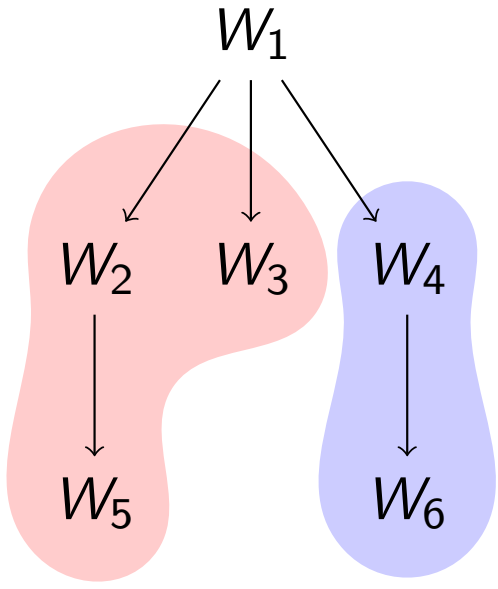
Топология на деревьях

Определение

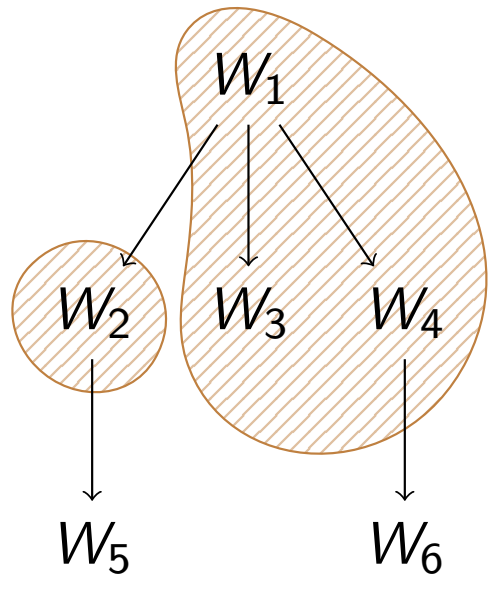
Пусть некоторый лес задан конечным множеством вершин V и отношением $(\preceq)$, связывающим предков и потомков ($a \preceq b$, если b — потомок a). Тогда подмножество его вершин $X \subseteq V$ назовём открытым, если из $a \in X$ и $a \preceq b$ следует, что $b \in X$.

Пример

Открыты



Не открыты



Связность деревьев

Лемма

Лес связен (является одним деревом) тогда и только тогда, когда соответствующее ему топологическое пространство связно.

Доказательство.

1. Лес связен: пусть не так и найдутся открытые непустые A,B, что $A \cup B = V$ и $A \cap B = \varnothing$. Пусть $v \in V$ — корень дерева и пусть $v \in A$ (для определённости). Тогда $A = \{x \mid v \preceq x\}$ и $B = \varnothing$.
2. Пусть лес топологически связен, но есть несколько разных корней $v_1, v_2, \ldots, v_k$. Возьмём $A_i = \{x \mid v_i \preceq x\}$. Тогда все A_i открыты, непусты, дизъюнктны и $V = \cup A_i$.

Пишем скобки или нет?

Вы как пишете: $\sin x$ или $\sin(x)$?

```
int main () {
    return sizeof 0;
}
```

Соглашение о записи:

$$\text{sizeof } \varnothing = \text{sizeof}(\varnothing) = 0$$

но:

$$\text{sizeof}\{\varnothing\} = \text{sizeof}(\{\varnothing\}) = 1$$

Минимальные и максимальные элементы

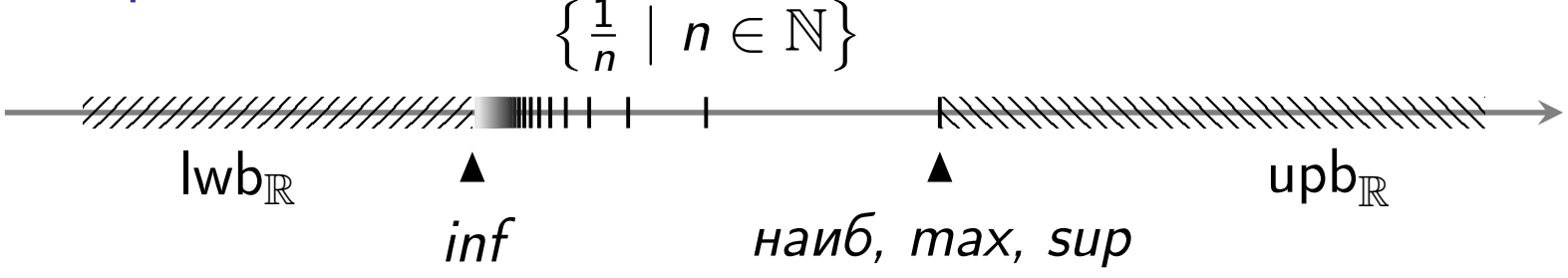
Определение

Множество нижних граней $X \subseteq \mathcal{U}$*:*
$\mathsf{lwb}_{\mathcal{U}} X = \{y \in \mathcal{U} \mid y \preceq x$ *при всех* $x \in X\}$. *Множество верхних граней* $X \subseteq \mathcal{U}$*:* $\mathsf{upb}_{\mathcal{U}} X = \{y \in \mathcal{U} \mid x \preceq y$ *при всех* $x \in X\}$.

Определение

минимальный $(m \in X)$*: нет меньшего*	*при всех* $y \in X$, $y \preceq m$ *влеч*
максимальный $(m \in X)$*: нет большего*	*при всех* $y \in X$, $m \preceq y$ *влеч*
наименьший $(m \in X)$*: меньше всех*	*при всех* $y \in X$ *выполнено* m
наибольший $(m \in X)$*: больше всех*	*при всех* $y \in X$ *выполнено* y
инфимум: наибольшая нижняя грань	$\inf_{\mathcal{U}} X = \mathsf{наиб}(\mathsf{lwb}_{\mathcal{U}} X)$
супремум: наименьшая верхняя грань	$\sup_{\mathcal{U}} X = \mathsf{наим}(\mathsf{upb}_{\mathcal{U}} X)$

Пример



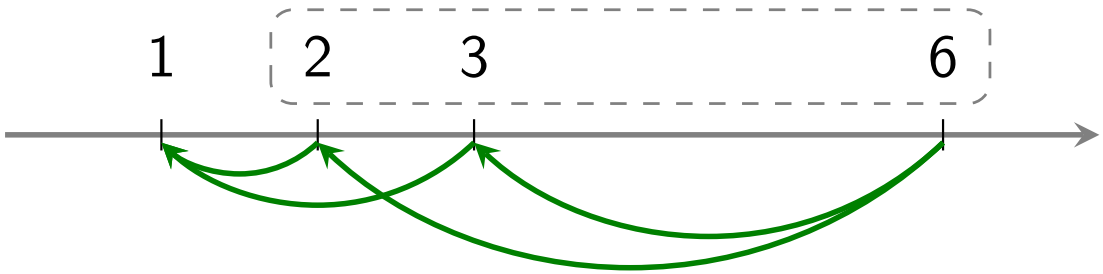
Пример: делимость

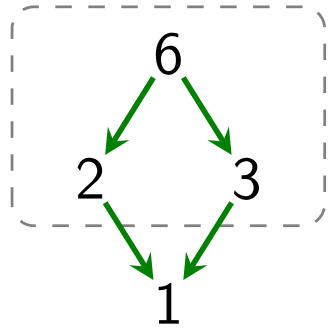
На $\mathbb{N}$ положим $a \preceq b$, если $b \vdots a$.

Пример

Множество $\{2, 3, 6\}$

Минимальные:	*2,3*	$2 \vdots x$ *влечёт* $x = 1$ *или* $x = 2$, *то же п*
Наименьший:	*отсутствует*	$2 \not\preceq 3$ *и* $3 \not\preceq 2$
Инфимум:	*1*	$1 \preceq x$ *при всех* $x \in \mathbb{N}$





Пример

Рассмотрим $X = \{1; 1.4; 1.41; 1.414; 1.4142; \ldots\}$ — *множество десятичных приближений* $\sqrt{2}$, $\preceq = \leqslant$. *Тогда* $\mathrm{upb}_{\mathbb{Q}} X$ *состоит из рациональных чисел, бóльших* $\sqrt{2}$. *При этом* $\sqrt{2} \notin \mathrm{upb}_{\mathbb{Q}} X$, *а значит* $\sup_{\mathbb{Q}} X$ *не определён.*

Пример: внутренность множества

Определение (внутренность множества)

Рассмотрим $\langle X, \Omega \rangle$ *и возьмём* $(\subseteq)$ *как отношение частичного порядка на* $\mathcal{P}(X)$*. Тогда* $A^\circ := \inf_\Omega(\{A\})$*.*

Теорема

A° *определена для любого* A*.*

Доказательство.

Пусть $V = \mathrm{lwb}_\Omega\{A\} = \{Q \in \Omega \mid Q \subseteq A\}$. Тогда $\inf_\Omega\{A\} = \bigcup V$.
Напомним, $\inf_{\mathcal{U}} T = \text{наиб}(\mathrm{lwb}_{\mathcal{U}} T)$.

1. Покажем принадлежность: $\bigcup V \subseteq A$ и $\bigcup V \in \Omega$ как объединение открытых.
2. Покажем, что все из V меньше или равны: пусть $X \in V$, то есть $V = \{X, \dots\}$, тогда $X \subseteq X \cup \dots$, тогда $X \subseteq \bigcup V$

□

Решётка

Определение

Решёткой называется упорядоченная пара: $\langle X, (\preceq)\rangle$, *где* X — *некоторое множество, а* $(\preceq)$ — *частичный порядок на* X, *такой, что для любых* $a, b \in X$ *определены* $a + b = \sup\{a, b\}$ *и* $a \cdot b = \inf\{a, b\}$.

То есть, $a + b$ — наименьший элемент c, что $a \preceq c$ и $b \preceq c$.

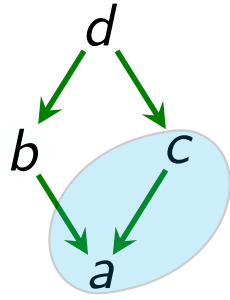
Пример

$\langle \Omega, (\subseteq)\rangle$ — *решётка.* $\langle \mathbb{N} \setminus \{1\}, (\vdots)\rangle$ — *не решётка.*

Псевдодополнение

Псевдодополнением $a \to b$ называется наибольший из $\{x \mid a \cdot x \preceq b\}$.

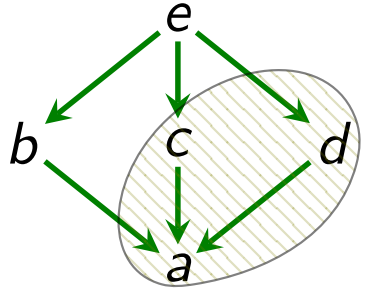
Пример



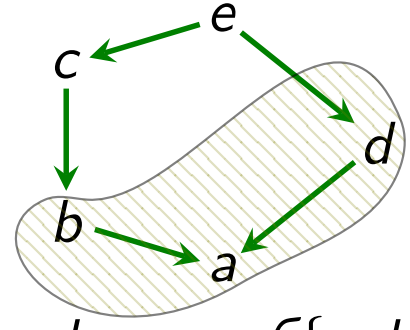
$$a \cdot b = a$$
$$b \cdot b = b$$
$$c \cdot b = a$$
$$d \cdot b = b$$

Здесь $b \to c = \textit{наиб}\{x \mid b \cdot x \preceq c\} = \textit{наиб}\{a, c\} = c$

Пример (нет псевдодополнения: диамант и пентагон)



$b \to c = \textit{наиб}\{a, c, d\}$



$c \to b = \textit{наиб}\{a, b, d\}$

Особые решётки

Определение

Дистрибутивной решёткой называется такая, что для любых a, b, c *выполнено* $a \cdot (b + c) = a \cdot b + a \cdot c$.

Определение

Импликативная решётка — такая, в которой для любых элементов есть псевдодополнение.

Лемма

Любая импликативная решётка — дистрибутивна.

Ноль и один

Определение

0 — наименьший элемент решётки, а 1 — наибольший элемент решётки

Лемма

В любой импликативной решётке $\langle X, (\preceq)\rangle$ есть 1

Доказательство.

Рассмотрим $a \to a$, тогда
$a \to a = \text{наиб}\{c \mid a \cdot c \preceq a\} = \text{наиб} X = 1.$ □

Определение

Импликативная решётка с 0 — псевдобулева алгебра (алгебра Гейтинга). В такой решётке определено $\sim a := a \to 0$

Определение

Булева алгебра — псевдобулева алгебра, в которой $a + \sim a = 1$ для всех a.

Булева алгебра является булевой алгеброй в смысле решёток

Доказательство.

Символы булевой алгебры: $(\&), (\vee), (\neg), \text{Л}, \text{И}$.
Символы решёток: $(+), (\cdot), (\to), (\sim), 0, 1$
Упорядочивание: $\text{Л} \leq \text{И}$.

1. $a \,\&\, b = \min(a, b)$, $a \vee b = \max(a, b)$ (анализ таблицы истинности), отсюда $a \cdot b = a \,\&\, b$ и $a + b = a \vee b$.
2. $a \to b = \neg a \vee b$, так как:

$$a \to b = \text{наиб}\{c | c \,\&\, a \leq b\} = \begin{cases} \neg a, & b = \text{Л} \\ \text{И}, & b = \text{И} \end{cases}$$

3. $0 = \min\{\text{И}, \text{Л}\} = \text{Л}$, $1 = \max\{\text{И}, \text{Л}\} = \text{И}$,
   $\sim a = a \to 0 = \neg a \vee \text{Л} = \neg a$. Заметим, что
   $a + \sim a = a \vee \neg a = \text{И}$.

Итого: булева алгебра — импликативная решётка с 0 и с $a + \sim a = 1$.

Множества и топологии как решётки

Лемма
$\langle \mathcal{P}(X), (\subseteq) \rangle$ — *булева алгебра.*

Доказательство.
$a \to b = \text{наиб}\{c \subseteq X \mid a \cap c \subseteq b\}$. Т.е. наибольшее, не содержащее точек из $a \setminus b$. Т.е. $X \setminus (a \setminus b)$. То есть $(X \setminus a) \cup b$.
$a + \sim a = a \cup (X \setminus a) \cup \varnothing = X$ □

Лемма
$\langle \Omega, (\subseteq) \rangle$ — *псевдобулева алгебра.*

Доказательство.
$a \to b = \text{наиб}\{c \in \Omega \mid a \cap c \subseteq b\}$. Т.е. наибольшее открытое, не содержащее точек из $a \setminus b$. То есть, $(X \setminus (a \setminus b))^\circ$. То есть, $((X \setminus a) \cup b)^\circ$. □

Решётки и исчисление высказываний

Определение

Пусть некоторое исчисление высказываний оценивается значениями из некоторой решётки. Назовём оценку согласованной с исчислением, если $[\![\alpha \,\&\, \beta]\!] = [\![\alpha]\!] \cdot [\![\beta]\!]$, $[\![\alpha \vee \beta]\!] = [\![\alpha]\!] + [\![\beta]\!]$, $[\![\alpha \to \beta]\!] = [\![\alpha]\!] \to [\![\beta]\!]$, $[\![\neg\alpha]\!] = \sim [\![\alpha]\!]$, $[\![A \,\&\, \neg A]\!] = 0$, $[\![A \to A]\!] = 1$.

Теорема

Любая псевдобулева алгебра, являющаяся согласованной оценкой интуиционистского исчисления высказываний, является его корректной моделью: если $\vdash \alpha$, *то* $[\![\alpha]\!] = 1$.

Теорема

Любая булева алгебра, являющаяся согласованной оценкой классического исчисления высказываний, является его корректной моделью: если $\vdash \alpha$, *то* $[\![\alpha]\!] = 1$

Теоремы об интуиционистском исчислении высказываний

Общие результаты об исчислениях высказываний

	К.И.В.	И.И.В. + алгебры Гейтинга
корректность	да (лекция 1)	да (ДЗ III.10)
непротиворечивость	да (очев.)	да (из непр. КИВ)
полнота	да (лекция 2)	да
разрешимость	да (лекция 2)	да

Алгебра Линденбаума

Определение

Определим предпорядок на высказываниях: $\alpha \preceq \beta := \alpha \vdash \beta$ *в интуиционистском исчислении высказываний. Также* $\alpha \approx \beta$, *если* $\alpha \preceq \beta$ *и* $\beta \preceq \alpha$.

Определение

Пусть L *— множество всех высказываний. Тогда алгебра Линденбаума* $\mathcal{L} = L/_{\approx}$.

Теорема

$\mathcal{L}$ *— псевдобулева алгебра.*

Схема доказательства.

Надо показать, что $(\preceq)$ есть отношение порядка на $\mathcal{L}$, что $[\alpha \vee \beta]_{\mathcal{L}} = [\alpha]_{\mathcal{L}} + [\beta]_{\mathcal{L}}$, $[\alpha \,\&\, \beta]_{\mathcal{L}} = [\alpha]_{\mathcal{L}} \cdot [\beta]_{\mathcal{L}}$, импликация есть псевдодополнение, $[A \,\&\, \neg A]_{\mathcal{L}} = 0$, $[\alpha]_{\mathcal{L}} \to 0 = [\neg\alpha]_{\mathcal{L}}$. $\square$

Полнота псевдобулевых алгебр

Теорема

Пусть $[\![\alpha]\!] = [\alpha]_{\mathcal{L}}$. Такая оценка интуиционистского исчисления высказываний алгеброй Линденбаума является согласованной.

Теорема

Интуиционистское исчисление высказываний полно в псевдобулевых алгебрах: если $\models \alpha$ во всех псевдобулевых алгебрах, то $\vdash \alpha$.

Доказательство.

Возьмём в качестве модели исчисления алгебру Линденбаума: $[\![\alpha]\!] = [\alpha]_{\mathcal{L}}$.
Пусть $\models \alpha$. Тогда $[\![\alpha]\!] = 1$ во всех псевдобулевых алгебрах, в том числе и $[\![\alpha]\!] = 1_{\mathcal{L}}$. То есть $[\alpha]_{\mathcal{L}} = [A \to A]_{\mathcal{L}}$. То есть $A \to A \approx \alpha$. Значит, в частности, $A \to A \vdash \alpha$. Значит, $\vdash \alpha$. $\square$

Модели Крипке

Определение

Модель Крипке $\langle \mathcal{W}, \preceq, (\Vdash) \rangle$*:*

- $\mathcal{W}$ *— множество миров,* $(\preceq)$ *— нестрогий частичный порядок на* $\mathcal{W}$*;*
- $(\Vdash) \subseteq \mathcal{W} \times P$ *— отношение вынуждения между мирами и переменными, причём, если* $W_i \preceq W_j$ *и* $W_i \Vdash X$*, то* $W_j \Vdash X$*.*

Доопределим вынужденность:

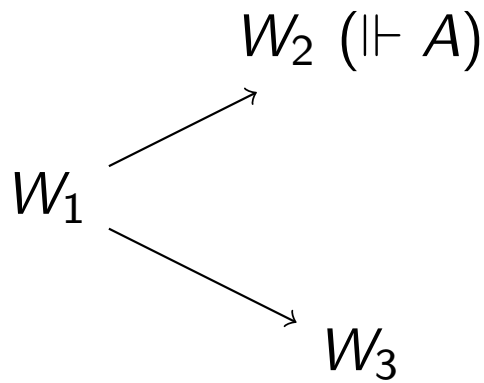
- $W \Vdash \alpha \,\&\, \beta$, если $W \Vdash \alpha$ и $W \Vdash \beta$;
- $W \Vdash \alpha \vee \beta$, если $W \Vdash \alpha$ или $W \Vdash \beta$;
- $W \Vdash \alpha \to \beta$, если всегда при $W \preceq W_1$ и $W_1 \Vdash \alpha$ выполнено $W_1 \Vdash \beta$
- $W \Vdash \neg\alpha$, если всегда при $W \preceq W_1$ выполнено $W_1 \nVdash \alpha$.

Будем говорить, что $\Vdash \alpha$, если $W \Vdash \alpha$ при всех $W \in \mathcal{W}$. Будем говорить, что $\models_\kappa \alpha$, если $\Vdash \alpha$ во всех моделях Крипке.

Исключённое третье

Пример

Покажем, что $\not\models_\kappa A \vee \neg A$.



Тогда, $W_3 \Vdash \neg A$, *но* $W_1 \nVdash A$ *(по определению) и* $W_1 \nVdash \neg A$ *(так как* $W_1 \preceq W_2$ *и* $W_2 \Vdash A$*). Значит,* $W_1 \nVdash A \vee \neg A$.

Корректность моделей Крипке

Лемма

Если $W_1 \Vdash \alpha$ *и* $W_1 \preceq W_2$, *то* $W_2 \Vdash \alpha$

Теорема

Пусть $\langle \mathcal{W}, (\preceq), (\Vdash) \rangle$ — *некоторая модель Крипке. Тогда она есть корректная модель интуиционистского исчисления высказываний.*

Доказательство.

Доказательство для древовидного $(\preceq)$, обобщение на произвольный порядок легко построить.
Заметим, что $V(\alpha) := \{w \in \mathcal{W} \mid w \Vdash \alpha\}$ открыто в топологии для деревьев. Значит, положив
$V = \{\ S \mid S \subseteq \mathcal{W}\ \ \&\ \ S$ — открыто $\}$ и $[\![\alpha]\!] = V(\alpha)$, получим алгебру Гейтинга. □

Табличные модели

Определение

Пусть задано V, значение $T \in V$ («истина»), функция $f_P : P \to V$, функции $f_\&, f_\vee, f_\to : V \times V \to V$, функция $f_\neg : V \to V$.
Тогда оценка $[\![X]\!] = f_P(X)$, $[\![\alpha \star \beta]\!] = f_\star([\![\alpha]\!], [\![\beta]\!])$, $[\![\neg\alpha]\!] = f_\neg([\![\alpha]\!])$ — табличная.
Если $\vdash \alpha$ влечёт $[\![\alpha]\!] = T$ при всех оценках пропозициональных переменных f_P, то $\mathcal{M} := \langle V, T, f_\&, f_\vee, f_\to, f_\neg \rangle$ — табличная модель.

Определение

Табличная модель конечна, если V конечно.

Теорема

Не существует полной конечной табличной модели для интуиционистского исчисления высказываний

Доказательство нетабличности: α_n

Пусть существует полная конечная табличная модель $\mathcal{M}$, $V = \{v_1, v_2, \ldots, v_n\}$. То есть, если $\models_{\mathcal{M}} \alpha$, то $\vdash \alpha$.
Рассмотрим

$$\alpha_n = \bigvee_{1 \le p < q \le n+1} A_p \to A_q$$

Рассмотрим оценку $f_P : \{A_1 \ldots A_{n+1}\} \to \{v_1 \ldots v_n\}$. По принципу Дирихле существуют $p \neq q$, что $[\![A_p]\!] = [\![A_q]\!]$. Значит,

$$[\![A_p \to A_q]\!] = f_{\to}([\![A_p]\!], [\![A_q]\!]) = f_{\to}(v, v)$$

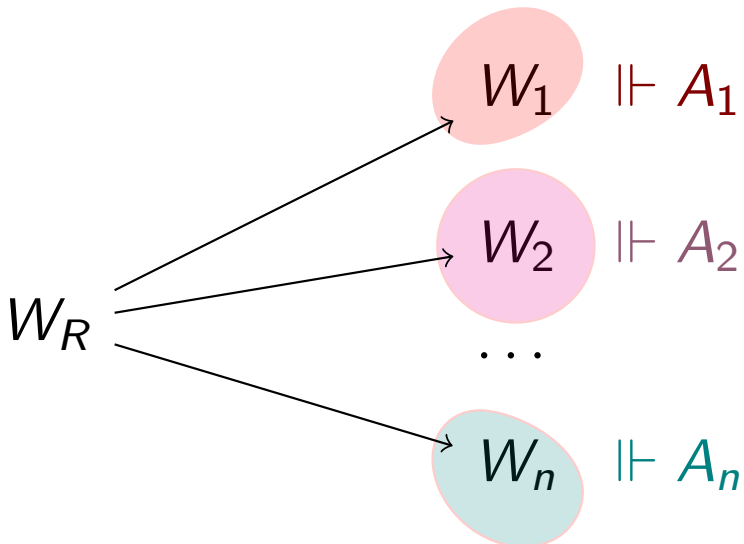
С другой стороны, $\vdash X \to X$ — поэтому $f_{\to}([\![X]\!], [\![X]\!]) = T$, значит,

$$[\![A_p \to A_q]\!] = f_{\to}(v, v) = f_{\to}([\![X]\!], [\![X]\!]) = T$$

Аналогично, $\vdash \sigma \vee (X \to X) \vee \tau$, отсюда
$[\![\alpha_n]\!] = [\![\sigma \vee (X \to X) \vee \tau]\!] = T$.

Доказательство нетабличности: противоречие

Однако, в такой модели $\nVdash \alpha_n$:



Если $q > 1$, то $W_1 \nVdash A_q$ и $W_1 \Vdash$

Если $q > 2$, то $W_2 \nVdash A_q$ и $W_2 \Vdash$

$W_n \nVdash A_{n+1}$; W_n

Если $p < q$, то $W_p \nVdash A_q$ и W_p

Если $p < q$, то $W_p \nVdash A_p \to A_q$, то есть $W_R \nVdash A_p \to A_q$.
Отсюда: $W_R \nVdash \bigvee_{p<q} A_p \to A_q$, $W_R \nVdash \alpha_n$, потому $\nvDash \alpha_n$ и $\nvdash \alpha_n$.

Дизъюнктивность ИИВ

Определение

Исчисление дизъюнктивно, если при любых α *и* β *из* $\vdash \alpha \vee \beta$ *следует* $\vdash \alpha$ *или* $\vdash \beta$.

Определение

Решётка гёделева, если $a + b = 1$ *влечёт* $a = 1$ *или* $b = 1$.

Теорема

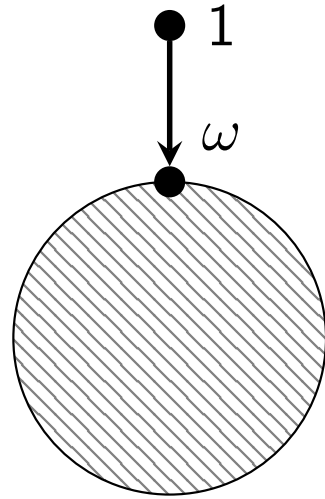
Интуиционистское исчисление высказываний дизъюнктивно

«Гёделевизация» (операция $\Gamma(\mathcal{A})$)

Определение

Для алгебры Гейтинга $\mathcal{A} = \langle A, (\preceq)\rangle$ *определим операцию «гёделевизации»:* $\Gamma(\mathcal{A}) = \langle A \cup \{\omega\}, (\preceq_{\Gamma(\mathcal{A})})\rangle$, *где отношение* $(\preceq_{\Gamma(\mathcal{A})})$ — *минимальное отношение порядка, удовлетворяющее условиям:*

- $a \preceq_{\Gamma(\mathcal{A})} b$, *если* $a \preceq_{\mathcal{A}} b$ *и* $a, b \notin \{\omega, 1\}$;
- $a \preceq_{\Gamma(\mathcal{A})} \omega$, *если* $a \neq 1$;
- $\omega \preceq_{\Gamma(\mathcal{A})} 1$



Теорема

$\Gamma(\mathcal{A})$ — *гёделева алгебра.*

Доказательство.

Проверка определения алгебры Гейтинга и наблюдение: если $a \preceq \omega$ и $b \preceq \omega$, то $a + b \preceq \omega$. □

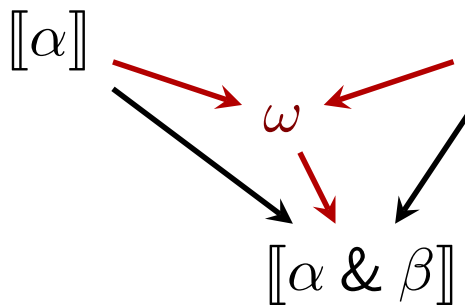
Оценка $\Gamma(\mathcal{L})$

Теорема

Рассмотрим оценку $[\![\alpha]\!]_{\Gamma(\mathcal{L})} = [\![\alpha]\!]_{\mathcal{L}}$. Тогда она является согласованной с ИИВ.

Индукция по структуре формулы и перебор операций.
Рассмотрим (&). Неформально: почти везде
$[\![\alpha]\!]_{\Gamma(\mathcal{L})} \cdot [\![\beta]\!]_{\Gamma(\mathcal{L})} = [\![\alpha]\!]_{\mathcal{L}} \cdot [\![\beta]\!]_{\mathcal{L}}$, поскольку $[\![\sigma]\!]_{\Gamma(\mathcal{L})} \neq \omega$,

... но нет ли случаев, когда
$\omega = \text{наиб}\{x \mid x \preceq [\![\alpha]\!]_{\Gamma(\mathcal{L})} \,\&\, x \preceq [\![\beta]\!]_{\Gamma(\mathcal{L})}\}$?



Чтобы убедиться, что всегда $[\![\alpha \,\&\, \beta]\!]_{\Gamma(\mathcal{L})} = [\![\alpha]\!]_{\Gamma(\mathcal{L})} \cdot [\![\beta]\!]_{\Gamma(\mathcal{L})}$,
надо показать:

- $[\alpha \,\&\, \beta]$ — из множества нижних граней: $\alpha \,\&\, \beta \vdash \alpha$ и $\alpha \,\&\, \beta \vdash \beta$;
- $[\alpha \,\&\, \beta]$ — наибольшая нижняя грань: $x \preceq [\alpha]$ и $x \preceq [\beta]$ влечёт $x \preceq [\alpha \,\&\, \beta]$

Гомоморфизм алгебр

Определение

Пусть $\mathcal{A}, \mathcal{B}$ *— алгебры Гейтинга. Тогда* $g : \mathcal{A} \to \mathcal{B}$ *— гомоморфизм, если* $g(a \star b) = g(a) \star g(b)$, $g(0_{\mathcal{A}}) = 0_{\mathcal{B}}$ *и* $g(1_{\mathcal{A}}) = 1_{\mathcal{B}}$.

Определение

Будем говорить, что оценка $[\![\cdot]\!]_{\mathcal{A}}$ *согласована с* $[\![\cdot]\!]_{\mathcal{B}}$ *и гомоморфизмом* g, *если* $g(\mathcal{A}) = \mathcal{B}$ *и* $g([\![\alpha]\!]_{\mathcal{A}}) = [\![\alpha]\!]_{\mathcal{B}}$.

Доказательство дизъюнктивности ИИВ

Определение ($\mathcal{G} : \Gamma(\mathcal{L}) \to \mathcal{L}$)

$$\mathcal{G}(a) = \begin{cases} a, & a \neq \omega \\ 1, & a = \omega \end{cases}$$

Лемма

$\mathcal{G}$ — гомоморфизм $\Gamma(\mathcal{L})$ и $\mathcal{L}$, причём оценка $[\![\cdot]\!]_{\Gamma(\mathcal{L})}$ согласована с $\mathcal{G}$ и $[\![\cdot]\!]_{\mathcal{L}}$.

Теорема

Если $\vdash \alpha \vee \beta$, то либо $\vdash \alpha$, либо $\vdash \beta$.

Доказательство.

Пусть $\vdash \alpha \vee \beta$. Тогда $[\![\alpha \vee \beta]\!]_{\Gamma(\mathcal{L})} = 1$ (так как данная оценка согласована с ИИВ). Тогда $[\![\alpha]\!]_{\Gamma(\mathcal{L})} = 1$ или $[\![\beta]\!]_{\Gamma(\mathcal{L})} = 1$ (так как $\Gamma(\mathcal{L})$ гёделева).
Пусть $[\![\alpha]\!]_{\Gamma(\mathcal{L})} = 1$, тогда $\mathcal{G}([\![\alpha]\!]_{\Gamma(\mathcal{L})}) = [\![\alpha]\!]_{\mathcal{L}} = 1$, тогда $\vdash \alpha$ (по полноте $\mathcal{L}$). □

Построение дистрибутивных подрешёток

Определение

Решётка $\mathcal{L}' = \langle L', \preceq \rangle$ *— подрешётка решётки* $\mathcal{L} = \langle L, \preceq \rangle$, *если* $L' \subseteq L$, $(\preceq') \subseteq (\preceq)$ *и при* $a, b \in L'$ *выполнено* $a +_{\mathcal{L}'} b = a +_{\mathcal{L}} b$ *и* $a \cdot_{\mathcal{L}'} b = a \cdot_{\mathcal{L}} b$.

Лемма

Существует дистрибутивная подрешётка $\mathcal{L}'$, *содержащая* $a_1, \ldots, a_n$, *что* $|L'| \leq 2^{2^n}$.

Доказательство.

Пусть $\mathcal{L}' = \langle \{\varphi(a_1, \ldots, a_n) \mid \varphi \text{ составлено из } (+) \text{ и } (\cdot)\}, (\preceq) \rangle$. Заметим, что если $p, q \in L'$, то $p \star_{\mathcal{L}} q \in L'$ (так как $\varphi_p(\overrightarrow{a}) \star \varphi_q(\overrightarrow{a}) = \psi(\overrightarrow{a})$). Также ясно, что если $\sup_L\{p, q\} \in L'$ (или $\inf_L\{p, q\} \in L'$), то $p \star_{\mathcal{L}} q = p \star_{\mathcal{L}'} q$. Значит, $\mathcal{L}'$ также дистрибутивна. Построим «ДНФ»:

$$\varphi(a_1, \ldots, a_n) = \sum_{\text{Кн} \in \text{ДНФ}(\varphi)} \prod_{i \in \text{Кн}} a_i$$

Разрешимость ИИВ

Теорема

Если $\nvdash \alpha$ в ИИВ, то существует $\mathcal{G}$, что $\mathcal{G} \not\models \alpha$, причём $|\mathcal{G}| \leq 2^{2^{|\alpha|+2}}$.

Доказательство.

Если $\nvdash \alpha$, то по полноте найдётся алгебра Гейтинга $\mathcal{H}$, что $\mathcal{H} \not\models \alpha$.

Пусть $\varphi_1, \ldots, \varphi_n$ — подформулы α. Пусть $\mathcal{G}$ — дистрибутивная подрешётка $\mathcal{H}$, построенная по $[\![\varphi_1]\!], \ldots, [\![\varphi_n]\!]$, 0 и 1.

Очевидно, что $\mathcal{G}$ — алгебра Гейтинга, и можно показать, что $\mathcal{G} \not\models \alpha$ (псевдодополнения не обязаны сохраниться). Тогда по лемме, $|\mathcal{G}| \leq 2^{2^{n+2}}$. □

Теорема

ИИВ разрешимо.

Доказательство.

По формуле α построим все возможные алгебры Гейтинга $\mathcal{G}$ размера не больше $2^{2^{|\alpha|+2}}$, если $\mathcal{G} \models \alpha$, то $\vdash \alpha$. □

Алгебра Линденбаума

Теорема

Пусть $\alpha \approx \beta$, *если* $\alpha \vdash \beta$ *и* $\beta \vdash \alpha$. *Тогда* $(\approx)$ — *отношение эквивалентности.*

Доказательство.

Надо доказать, что для любых α, β, γ:

1. $\alpha \approx \alpha$ (очевидно, $\alpha \vdash \alpha$);
2. $\alpha \approx \beta$ влечёт $\beta \approx \alpha$ (очевидно из определения);
3. $\alpha \approx \beta$ и $\beta \approx \gamma$ влечёт $\alpha \approx \gamma$:
   из посылок следует $\alpha \vdash \beta$ и $\beta \vdash \gamma$, соединив доказательства, получим $\alpha \vdash \gamma$.

□

$L/_{\approx}$ — частично-упорядоченное множество. Элементы будем обозначать $[\alpha]$.

Теорема

$\alpha \vdash \beta$ *тогда и только тогда, когда* $[\alpha] \leq [\beta]$.

$\mathcal{L}$ — решётка.

Покажем $[\alpha] \cdot [\beta] = [\alpha \,\&\, \beta]$. То есть, $[\alpha \,\&\, \beta]$ — наибольшая нижняя грань α и β.

- *(... нижняя грань)* $[\alpha \,\&\, \beta] \leq [\alpha]$: заметим, что $\alpha \,\&\, \beta \vdash \alpha$.
- *(наибольшая ...)* Если $[\sigma] \leq [\alpha]$ и $[\sigma] \leq [\beta]$, то $[\sigma] \leq [\alpha \,\&\, \beta]$:
  Рассмотрим вывод в контексте σ:

$(1..a)$	α	из $[\sigma] \leq [\alpha]$
$(a+1..b)$	β	из $[\sigma] \leq [\beta]$
$(b+1)$	$\alpha \to \beta \to \alpha \,\&\, \beta$	Сх. акс
$(b+2)$	$\beta \to \alpha \,\&\, \beta$	M.P. a, $b+1$
$(b+3)$	$\alpha \,\&\, \beta$	M.P. b, $b+2$

  Отсюда $\sigma \vdash \alpha \,\&\, \beta$.

Утверждение $[\alpha] + [\beta] = [\alpha \vee \beta]$ показывается аналогично.

$\mathcal{L}$ — импликативная решётка с 0, согласованная с ИИВ

- *(импликативная ...)* Покажем $[\alpha] \to [\beta] = [\alpha \to \beta]$:
  в самом деле, $[\alpha] \to [\beta] =$ наиб $\{[\sigma] \mid [\alpha \,\&\, \sigma] \leq [\beta]\}$.
  Покажем требуемое двумя включениями:
  1. $\alpha \,\&\, (\alpha \to \beta) \vdash \beta$ (карринг + транзитивность импликации)
  2. Если $\alpha \,\&\, \sigma \vdash \beta$, то $\sigma \vdash \alpha \to \beta$ (карринг + теорема о дедукции)
- *(... с нулём ...)* Покажем, что $0 = [A \,\&\, \neg A]$:
  в самом деле, $A \,\&\, \neg A \vdash \sigma$ при любом σ.
- *(... согласованная с ИИВ)*
  1. Из доказательства видно, что $[\alpha \,\&\, \beta] = [\alpha] \cdot [\beta]$, $[\alpha \vee \beta] = [\alpha] + [\beta]$, $[\alpha \to \beta] = [\alpha] \to [\beta]$, $[A \,\&\, \neg A] = 0$.
  2. $[A \to A] = [A] \to [A] = 1$ по свойствам алгебры Гейтинга
  3. $[\neg\alpha] = [\alpha \to A \,\&\, \neg A] = [\alpha] \to 0 = {\sim}\,[\alpha]$

$\Gamma(\mathscr{L})$ — алгебра Гейтинга, согласованная с ИИВ.

Надо учитывать существование нового элемента ω.
Например, импликация/псевдодополнение:
$[\alpha] \to [\beta] =$ наиб $\{s \mid [\alpha] \cdot s \leq [\beta]\}$.

- *(... нижняя грань)* $[\alpha] \cdot [\alpha \to \beta] \leq [\beta]$ — аналогично случаю для $\mathscr{L}$
- *(наибольшая ...)* Если $[\alpha] \cdot s \leq [\beta]$, то
  - $s = [\sigma]$, то есть $s \neq \omega$ — аналогично случаю для $\mathscr{L}$;
  - $s = \omega$, тогда $[\alpha] \cdot \omega \leq [\beta]$. Но $[\alpha] \neq \omega$ — либо $[\alpha] < \omega$, либо $[\alpha] = 1$. В обоих случаях $[\alpha] \cdot 1 \leq [\beta]$. Отсюда s не наибольший.

Исчисление предикатов

Ограничения языка исчисления высказываний

$$\frac{\text{Каждый человек смертен} \qquad \text{Сократ есть человек}}{\text{Сократ смертен}}$$

Цель: увеличить формализованную часть метаязыка.

Мы неформально знакомы с предикатами ($P : D \to V$) и кванторами ($\forall x.H(x) \to S(x)$).

$$\frac{\forall x.H(x) \to S(x) \qquad H(\text{Сократ})}{S(\text{Сократ})}$$

Начнём с примера

$$\forall x.\sin x = 0 \vee (\sin x)^2 + 1 > 1$$

1. Предметные (здесь: числовые) выражения
   - 1.1 Предметные переменные (x).
   - 1.2 Одно- и двухместные функциональные символы «синус», «возведение в квадрат» и «сложение».
   - 1.3 Нульместные функциональные символы «ноль» (0) и «один» (1).
2. Логические выражения
   - 2.1 Предикатные символы «равно» и «больше»

Язык исчисления предикатов

1. Два типа: предметные и логические выражения.
2. Предметные выражения: метапеременная θ.
   - Предметные переменные: a, b, c, ..., метапеременные x, y.
   - Функциональные выражения: $f(\theta_1, \ldots, \theta_n)$, метапеременные f, g, ...
   - Примеры: r, $q(p(x, s), r)$.
3. Логические выражения: метапеременные α, β, γ, ...
   - Предикатные выражения: $P(\theta_1, \ldots, \theta_n)$, метапеременная P. Имена: A, B, C, ...
   - Связки: $(\varphi \vee \psi)$, $(\varphi \,\&\, \psi)$, $(\varphi \to \psi)$, $(\neg\varphi)$.
   - Кванторы: $(\forall x.\varphi)$ и $(\exists x.\varphi)$.

Сокращения записи, метаязык

1. Метапеременные:
   - ψ, ϕ, π, ... — формулы
   - P, Q, ... — предикатные символы
   - θ, ... — термы
   - f, g, ... — функциональные символы
   - x, y, ... — предметные переменные
2. Скобки — как в И.В.; квантор — жадный:

$$\underbrace{(\forall a.\, A \vee B \vee C \to \exists b.\, \underbrace{D \,\&\, \neg E}_{\exists b....})}_{\forall a....} \,\&\, F$$

3. Дополнительные обозначения при необходимости:
   - $(\theta_1 = \theta_2)$ вместо $E(\theta_1, \theta_2)$
   - $(\theta_1 + \theta_2)$ вместо $p(\theta_1, \theta_2)$
   - 0 вместо z
   - ...

Теория моделей: два типа значений

Напомним формулу:

$$\forall x.\, \sin x = 0 \vee (\sin x)^2 + 1 > 1$$

Без синтаксического сахара:

$$\forall x.E(f(x), z) \;\vee\; G(p(q(s(x)), o), o)$$

$$\forall x.E(f(x), z) \;\vee\; G(p(q(s(x)), o), o)$$

$$\forall x.E(f(x), z) \vee G(p(q(s(x)), o), o)$$

$$\forall x.E(f(x), z) \vee G(p(q(s(x)), o), o)$$

$$\forall x.E(f(x), z) \vee G(p(q(s(x)), o), o)$$

1. Истинностные (логические) значения:
   - 1.1 предикаты (в том числе пропозициональные переменные = нульместные предикаты);
   - 1.2 логические связки и кванторы.
2. Предметные значения:
   - 2.1 предметные переменные;
   - 2.2 функциональные символы (в том числе константы = нульместные функциональные символы)

Оценка исчисления предикатов

Определение

Оценка — упорядоченная четвёрка $\langle D, F, P, E \rangle$, *где:*

1. D — *предметное множество;*
2. F — *оценка для функциональных символов; пусть* f_n — n*-местный функциональный символ:*

$$F_{f_n} : D^n \to D$$

3. P — *оценка для предикатных символов; пусть* T_n — n*-местный предикатный символ:*

$$P_{T_n} : D^n \to V \qquad V = \{И, Л\}$$

4. E — *оценка для предметных переменных.*

$$E(x) \in D$$

Оценка формулы

Запись и сокращения записи подобны исчислению высказываний:

$$[\![\phi]\!] \in V, \quad [\![Q(x, f(x)) \vee R]\!]^{x:=1, f(t):=t^2, R:=\text{И}} = \text{И}$$

1. Правила для связок $\vee$, $\&$, $\neg$, $\to$ остаются прежние;
2. $[\![f_n(\theta_1, \theta_2, \ldots, \theta_n)]\!] = F_{f_n}([\![\theta_1]\!], [\![\theta_2]\!], \ldots, [\![\theta_n]\!])$
3. $[\![P_n(\theta_1, \theta_2, \ldots, \theta_n)]\!] = P_{T_n}([\![\theta_1]\!], [\![\theta_2]\!], \ldots, [\![\theta_n]\!])$
4. $$[\![\forall x.\phi]\!] = \begin{cases} \text{И}, & \text{если } [\![\phi]\!]^{x:=t} = \text{И} \text{ при всех } t \in D \\ \text{Л}, & \text{если найдётся } t \in D, \text{ что } [\![\phi]\!]^{x:=t} = \text{Л} \end{cases}$$
5. $$[\![\exists x.\phi]\!] = \begin{cases} \text{И}, & \text{если найдётся } t \in D, \text{ что } [\![\phi]\!]^{x:=t} = \text{И} \\ \text{Л}, & \text{если } [\![\phi]\!]^{x:=t} = \text{Л} \text{ при всех } t \in D \end{cases}$$

Пример (очевидная интерпретация)

Оценим:

$$[\![\forall a.\exists b.\neg a + 1 = b]\!]$$

Зададим оценку:

- $D := \mathbb{N}$;
- $F_1 := 1$, $F_{(+)}$ — сложение в $\mathbb{N}$;
- $P_{(=)}$ – равенство в $\mathbb{N}$.

Фиксируем $a \in \mathbb{N}$. Тогда:

$$[\![a + 1 = b]\!]^{b:=a} = \text{Л}$$

поэтому при любом $a \in \mathbb{N}$:

$$[\![\exists b.\neg a + 1 = b]\!] = \text{И}$$

Итого:

$$[\![\forall a.\exists b.\neg a + 1 = b]\!] = \text{И}$$

Пример (странная интерпретация)

$$[\![\forall a.\exists b.\neg a + 1 = b]\!]$$

Зададим интерпретацию:

- $D := \{\square\}$;
- $F_{(1)} := \square$, $F_{(+)}(a, b) := \square$;
- $P_{(=)}(a, b) := \text{И}$.

Тогда:

$$[\![a + 1 = b]\!]^{a \in D, b \in D} = \text{И}$$

Итого:

$$[\![\forall a.\exists b.\neg a + 1 = b]\!] = \text{Л}$$

Общезначимость

Определение

Формула исчисления предикатов общезначима, если истинна при любой оценке:

$$\models \phi$$

То есть истинна при любых D, F, P и E.

Пример: общезначимая формула

Теорема

$$[\![\forall x.Q(f(x)) \vee \neg Q(f(x))]\!]$$

Доказательство.

Фиксируем D, F, P, E. Пусть $x \in D$. Обозначим $P_Q(F_f(E_x))$ за t. Ясно, что $t \in V$. Разберём случаи.

- Если $t = \text{И}$, то $[\![Q(f(x))]\!]^{Q(f(x)):=t} = \text{И}$, потому $[\![Q(f(x)) \vee \neg Q(f(x))]\!]^{Q(f(x)):=t} = \text{И}$
- Если $t = \text{Л}$, то $[\![\neg Q(f(x))]\!]^{Q(f(x)):=t} = \text{И}$, потому всё равно $[\![Q(f(x)) \vee \neg Q(f(x))]\!]^{Q(f(x)):=t} = \text{И}$

□

Свободные вхождения

Определение

Вхождение подформулы в формулу — это позиция первого символа этой подформулы в формуле.

Вхождения x в формулу: $(\forall x.A(x) \vee \exists x.B(x)) \vee C(x)$

Определение

Рассмотрим формулу $\forall x.\psi$ (или $\exists x.\psi$). Здесь переменная x связана в ψ. Все вхождения переменной x в ψ — связанные.

Определение

Вхождение x в ψ свободное, если не находится в области действия никакого квантора по x. Переменная входит свободно в ψ, если имеет хотя бы одно свободное вхождение.
$FV(\psi), FV(\Gamma)$ — множества свободных переменных в ψ, в Γ

Пример

$\exists y.(\forall x.P(x)) \vee P(x) \vee Q(y)$

Подстановка, свобода для подстановки

$$\psi[x := \theta] := \begin{cases} \psi, & \psi \equiv y, y \not\equiv x \\ \psi, & \psi \equiv \forall x.\pi \text{ или } \psi \equiv \exists x.\pi \\ \pi[x := \theta] \star \rho[x := \theta], & \psi \equiv \pi \star \rho \\ \theta, & \psi \equiv x \\ \forall y.\pi[x := \theta], & \psi \equiv \forall y.\pi \text{ и } y \not\equiv x \\ \exists y.\pi[x := \theta], & \psi \equiv \exists y.\pi \text{ и } y \not\equiv x \end{cases}$$

Определение

Терм θ свободен для подстановки вместо x в ψ ($\psi[x := \theta]$), если ни одно свободное вхождение переменных в θ не станет связанным после подстановки.

Свобода есть	Свободы нет
$(\forall x.P(y))[y := z]$	$(\forall x.P(y))[y := x]$
$(\forall y.\forall x.P(x))[x := y]$	$(\forall y.\forall x.P(t))[t := y]$

Теория доказательств

Рассмотрим язык исчисления предикатов. Возьмём все схемы аксиом классического исчисления высказываний и добавим ещё две схемы аксиом (здесь везде θ свободен для подстановки вместо x в φ):

11. $(\forall x.\varphi) \to \varphi[x := \theta]$
12. $\varphi[x := \theta] \to \exists x.\varphi$

Добавим ещё два правила вывода (здесь везде x не входит свободно в φ):

$$\frac{\varphi \to \psi}{\varphi \to \forall x.\psi}$$ Правило для $\forall$

$$\frac{\psi \to \varphi}{(\exists x.\psi) \to \varphi}$$ Правило для $\exists$

Определение

Доказуемость, выводимость, полнота, корректность — аналогично исчислению высказываний.

Важность ограничений на схемы аксиом и правила вывода

- Рассмотрим формулу
  $(\forall x.\exists y.\neg x = y) \to ((\exists y.\neg x = y)[x := y])$
- Соответствует 11 схеме

$$(\forall x.\varphi) \to \varphi[x := \theta] \qquad \varphi \equiv \exists y.\neg x = y \qquad \theta \equiv y$$

- Но нарушается свобода для подстановки

$$(\exists y.\neg x = y)[x := y] \equiv (\exists y.\neg y = y)$$

- Пусть $D = \mathbb{N}$ и $(=)$ есть равенство на $\mathbb{N}$. Тогда

$$[\![\exists y.\neg x = y]\!] = \text{И} \qquad [\![(\exists y.\neg x = y)[x := y]]\!] = \text{Л}$$

- $\not\models (\forall x.\exists y.\neg x = y) \to ((\exists y.\neg x = y)[x := y])$

Теорема о дедукции для исчисления предикатов

Теорема

Если $\Gamma \vdash \alpha \to \beta$*, то* $\Gamma, \alpha \vdash \beta$*. Если* $\Gamma, \alpha \vdash \beta$ *и в доказательстве не применяются правила для кванторов по свободным переменным из* α*, то* $\Gamma \vdash \alpha \to \beta$*.*

Доказательство.

($\Rightarrow$) — как в КИВ ($\Leftarrow$) — та же схема, два новых случая.
Перестроим: $\delta_1, \delta_2, \ldots, \delta_n \equiv \beta$ в $\alpha \to \delta_1, \alpha \to \delta_2, \ldots, \alpha \to \delta_n$.
Дополним: обоснуем $\alpha \to \delta_n$, если предыдущие уже обоснованы.
Два новых похожих случая: правила для $\forall$ и $\exists$. Рассмотрим $\forall$.
Доказываем (n) $\alpha \to \psi \to \forall x.\varphi$ (правило для $\forall$), значит, доказано (k) $\alpha \to \psi \to \varphi$.

$(n-0.9)\ldots(n-0.8)$	$(\alpha \to \psi \to \varphi) \to (\alpha \,\&\, \psi) \to \varphi$	Т. о п
$(n-0.6)$	$(\alpha \,\&\, \psi) \to \varphi$	М.Р.
$(n-0.4)$	$(\alpha \,\&\, \psi) \to \forall x.\varphi$	Прав
$(n-0.3)\ldots(n-0.2)$	$((\alpha \,\&\, \psi) \to \forall x.\varphi) \to (\alpha \to \psi \to \forall x.\varphi)$	Т. о п
(n)	$\alpha \to \psi \to \forall x.\varphi$	М.Р.

Следование

Определение

$\gamma_1, \gamma_2, \ldots, \gamma_n \models \alpha$, *если выполнено два условия:*

1. α *выполнено всегда, когда выполнено* $\gamma_1, \gamma_2, \ldots, \gamma_n$;
2. α *не использует кванторов по переменным, входящим свободно в* $\gamma_1, \gamma_2, \ldots, \gamma_n$.

Теорема

Если $\Gamma \vdash \alpha$ *и в доказательстве не используются кванторы по свободным переменным из* Γ, *то* $\Gamma \models \alpha$

Важность второго условия

Пример

Покажем, что $\Gamma \models \alpha$ *ведёт себя неестественно, если в* α *используются кванторы по переменным, входящим свободно в* Γ.

Легко показать, что $P(x) \vdash \forall x.P(x)$.

(1)	$P(x)$	*Гипотеза*
(2)	$P(x) \to (A \to A \to A) \to P(x)$	*Сх. акс. 1*
(3)	$(A \to A \to A) \to P(x)$	*M.P. 1, 2*
(4)	$(A \to A \to A) \to \forall x.P(x)$	*Правило для* $\forall$*, 3*
(5)	$(A \to A \to A)$	*Сх. акс. 1*
(6)	$\forall x.P(x)$	*M.P. 5, 4*

Пусть $D = \mathbb{Z}$ *и* $P(x) = x > 0$. *Тогда не будет выполнено* $P(x) \models \forall x.P(x)$.

Корректность

Теорема

Если θ свободен для подстановки вместо x в φ, то $[\![\varphi]\!]^{x:=[\![\theta]\!]} = [\![\varphi[x := \theta]]\!]$

Доказательство (индукция по структуре φ).

- База: φ не имеет кванторов. Очевидно.
- Переход: пусть справедливо для ψ. Покажем для $\varphi = \forall y.\psi$.
  - $x = y$ либо $x \notin FV(\psi)$. Тогда: $[\![\forall y.\psi]\!]^{x:=[\![\theta]\!]} = [\![\forall y.\psi]\!] = [\![(\forall y.\psi)[x := \theta]]\!]$
  - $x \neq y$. Тогда: $[\![\forall y.\psi]\!]^{x:=[\![\theta]\!]} = [\![\psi]\!]^{y\in D;x:=[\![\theta]\!]} = \ldots$

    Свобода для подстановки: $y \notin \theta$.

    $$\ldots = [\![\psi]\!]^{x:=[\![\theta]\!];y\in D} = \ldots$$

    Индукционное предположение.

    $$\ldots = [\![\psi[x := \theta]]\!]^{y\in D} = [\![\forall y.(\psi[x := \theta])]\!] = \ldots$$

    Но $\forall y.(\psi[x := \theta]) \equiv (\forall y.\psi)[x := \theta]$ (как текст). Отсюда:

    $$\ldots = [\![(\forall y.\psi)[x := \theta]]\!]$$

□

Корректность

Теорема

Если $\Gamma \vdash \alpha$ *и в доказательстве не используются кванторы по свободным переменным из* $FV(\Gamma)$, *то* $\Gamma \models \alpha$

Доказательство.

Фиксируем D, F, P. Индукция по длине доказательства α: при любом E выполнено $\Gamma \models \alpha$ при длине доказательства n, покажем для $n+1$.

- Схемы аксиом (1)..(10), правило М.Р.: аналогично И.В.
- Схемы (11) и (12), например, схема $(\forall x.\varphi) \to \varphi[x := \theta]$:

  $$[\![(\forall x.\varphi) \to \varphi[x := \theta]]\!] = [\![((\forall x.\varphi) \to \varphi)[x := \theta]]\!] = [\![((\forall x.\varphi) \to \varphi]\!]^{x:=}$$

- Правила для кванторов: например, введение $\forall$:
  Пусть $[\![\psi \to \varphi]\!] = \text{И}$. Причём $x \notin FV(\Gamma)$ и $x \notin FV(\psi)$. То есть, при любом x выполнено $[\![\psi \to \varphi]\!]^{x:=x} = \text{И}$. Тогда $[\![\psi \to (\forall x.\varphi)]\!] = \text{И}$.

□

Теорема о полноте исчисления предикатов

Общая идея доказательства

1. Надо справиться со слишком большим количеством вариантов. Модель задаётся как $\langle D, F, P, X \rangle$.
2. Для оценки в модели важно только какие формулы истинны. Модели $\mathcal{M}_1$ и $\mathcal{M}_2$ «похожи», если $[\![\varphi]\!]_{\mathcal{M}_1} = [\![\varphi]\!]_{\mathcal{M}_2}$ при всех φ.
3. Поступим так:
   - 3.1 построим эталонное множество моделей $\mathfrak{M}$, каждая модель соответствует списку истинных формул, *но им не является*;
   - 3.2 докажем полноту $\mathfrak{M}$: если каждая $\mathcal{M} \in \mathfrak{M}$ предполагает $\mathcal{M} \models \varphi$, то $\vdash \varphi$;
   - 3.3 заметим, что если $\models \varphi$, то каждая $\mathcal{M} \in \mathfrak{M}$ предполагает $\mathcal{M} \models \varphi$.
4. В ходе доказательства нас ждёт множество технических препятствий.

Непротиворечивое множество формул

Определение

Γ — *непротиворечивое множество формул, если* $\Gamma \nvdash \alpha \,\&\, \neg\alpha$ *для любого* α

Примеры:

- непротиворечиво:
  - $\Gamma = \{A \to B \to A\}$
  - $\Gamma = \{P(x, y) \to \neg P(x, y), \forall x.\forall y.\neg P(x, y)\}$;
- противоречиво:
  - $\Gamma = \{P \to \neg P, \neg P \to P\}$
    так как $P \to \neg P, \neg P \to P \vdash \neg P \,\&\, \neg\neg P$
- пусть $D = \mathbb{Z}$ и $P(x) \equiv (x > 0)$, аналогом для этой модели будет $\Gamma = \{P(1), P(2), P(3), \dots\}$

Полное непротиворечивое множество формул

Определение

Γ — *полное непротиворечивое множество замкнутых бескванторных формул, если:*

1. Γ *содержит только замкнутые бескванторные формулы;*
2. *если* α — *некоторая замкнутая бескванторная формула, то либо* $\alpha \in \Gamma$, *либо* $\neg\alpha \in \Gamma$.

Определение

Γ — *полное непротиворечивое множество замкнутых формул, если:*

1. Γ *содержит только замкнутые формулы;*
2. *если* α — *некоторая замкнутая формула, то либо* $\alpha \in \Gamma$, *либо* $\neg\alpha \in \Gamma$.

Пополнение непротиворечивого множества формул

Теорема

Пусть Γ *— непротиворечивое множество замкнутых (бесквантворных) формул. Тогда, какова бы ни была замкнутая (бесквантворная) формула* φ*, хотя бы* $\Gamma \cup \{\varphi\}$ *или* $\Gamma \cup \{\neg\varphi\}$ *— непротиворечиво*

Доказательство.

Пусть это не так и найдутся такие Γ, φ и α, что

$$\begin{aligned} \Gamma, \varphi &\vdash \alpha \,\&\, \neg\alpha \\ \Gamma, \neg\varphi &\vdash \alpha \,\&\, \neg\alpha \end{aligned}$$

Тогда по лемме об исключении гипотезы

$$\Gamma \vdash \alpha \,\&\, \neg\alpha$$

То есть Γ не является непротиворечивым. Противоречие. $\square$

Дополнение непротиворечивого множества формул до полного

Теорема

Пусть Γ *— непротиворечивое множество замкнутых (бесквантворных) формул. Тогда найдётся полное непротиворечивое множество замкнутых (бесквантворных) формул* Δ*, что* $\Gamma \subseteq \Delta$

Доказательство.

1. Занумеруем все формулы (их счётное количество): $\varphi_1, \varphi_2, \dots$
2. Построим семейство множеств $\{\Gamma_i\}$:

$$\Gamma_0 = \Gamma \qquad \Gamma_{i+1} = \begin{cases} \Gamma_i \cup \{\varphi_i\}, & \text{если } \Gamma_i \cup \{\varphi_i\} \text{ непротив} \\ \Gamma_i \cup \{\neg\varphi_i\}, & \text{иначе} \end{cases}$$

3. Итоговое множество

$$\Delta = \bigcup_i \Gamma_i$$

Дополнение. . . (завершение доказательства)

4. Δ непротиворечиво:

4.1 Пусть Δ противоречиво, то есть

$$\Delta \vdash \alpha \,\&\, \neg\alpha$$

4.2 Доказательство конечной длины и использует конечное количество гипотез $\{\delta_1, \delta_2, \ldots, \delta_n\} \subset \Delta$, то есть

$$\delta_1, \delta_2, \ldots, \delta_n \vdash \alpha \,\&\, \neg\alpha$$

4.3 Пусть $\delta_i \in \Gamma_{d_i}$, тогда

$$\Gamma_{d_1} \cup \Gamma_{d_2} \cup \cdots \cup \Gamma_{d_n} \vdash \alpha \,\&\, \neg\alpha$$

4.4 Но $\Gamma_{d_1} \cup \Gamma_{d_2} \cup \cdots \cup \Gamma_{d_n} = \Gamma_{\max(d_1, d_2, \ldots, d_n)}$, которое непротиворечиво, и потому

$$\Gamma_{d_1} \cup \Gamma_{d_2} \cup \cdots \cup \Gamma_{d_n} \nvdash \alpha \,\&\, \neg\alpha$$

Модель для множества формул

Определение

Моделью для множества формул F назовём такую модель $\mathcal{M}$, что при всяком $\varphi \in F$ выполнено $[\![\varphi]\!]_{\mathcal{M}} = И$.
Альтернативное обозначение: $\mathcal{M} \models \varphi$.

Модели для непротиворечивых множеств замкнутых бескванторных формул

Теорема

Любое непротиворечивое множество замкнутых бескванторных формул имеет модель.

Конструкция для модели

Определение

Пусть M — полное непротиворечивое множество замкнутых бескванторных формул. Тогда модель $\mathcal{M}$ задаётся так:

1. *D — множество всевозможных предметных выражений без предметных переменных и дополнительная строка “ошибка!”*
2. $[\![f(\theta_1, \ldots, \theta_n)]\!] = \text{“}f(\text{”} + [\![\theta_1]\!] + \text{“,”} + \ldots + \text{“,”} + [\![\theta_n]\!] + \text{“)”}$
3. $[\![P(\theta_1, \ldots, \theta_n)]\!] = \begin{cases} И, & \text{если } P(\theta_1, \ldots, \theta_n) \in M \\ Л, & \text{иначе} \end{cases}$
4. $[\![x]\!] = \text{“ошибка!”}$, *так как формулы замкнуты.*

Доказательство корректности

Лемма

Пусть φ — бескванторная формула, тогда $\mathcal{M} \models \varphi$ тогда и только тогда, когда $\varphi \in M$.

Доказательство (индукция по длине формулы φ).

1. База. φ — предикат. Требуемое очевидно по определению $\mathcal{M}$.
2. Переход. Пусть $\varphi = \alpha \star \beta$ (или $\varphi = \neg\alpha$), причём $\mathcal{M} \models \alpha$ ($\mathcal{M} \models \beta$) тогда и только тогда, когда $\alpha \in M$ ($\beta \in M$). Тогда покажем требуемое для каждой связки в отдельности. А именно, для каждой связки покажем два утверждения:
   - 2.1 если $\mathcal{M} \models \alpha \star \beta$, то $\alpha \star \beta \in M$.
   - 2.2 если $\mathcal{M} \not\models \alpha \star \beta$, то $\alpha \star \beta \notin M$.

Доказательство утверждений для связок

Если $\varphi = \alpha \to \beta$ и для любой формулы ζ, более короткой, чем φ, выполнено $\mathcal{M} \models \zeta$ тогда и только тогда, когда $\zeta \in M$, тогда:

1. если $\mathcal{M} \models \alpha \to \beta$, то $\alpha \to \beta \in M$;
2. если $\mathcal{M} \not\models \alpha \to \beta$, то $\alpha \to \beta \notin M$.

Доказательство (разбором случаев).

1. $\mathcal{M} \models \alpha \to \beta$: $[\![\alpha]\!] =$ Л. Тогда по предположению $\alpha \notin M$, потому по полноте $\neg\alpha \in M$. И, поскольку в ИВ $\neg\alpha \vdash \alpha \to \beta$, то $M \vdash \alpha \to \beta$. Значит, $\alpha \to \beta \in M$, иначе по полноте $\neg(\alpha \to \beta) \in M$, что делает M противоречивым.
2. $\mathcal{M} \models \alpha \to \beta$: $[\![\alpha]\!] =$ И и $[\![\beta]\!] =$ И. Рассуждая аналогично, используя $\alpha, \beta \vdash \alpha \to \beta$, приходим к $\alpha \to \beta \in M$.
3. $\mathcal{M} \not\models \alpha \to \beta$. Тогда $[\![\alpha]\!] =$ И, $[\![\beta]\!] =$ Л, то есть $\alpha \in M$ и $\neg\beta \in M$. Также, $\alpha, \neg\beta \vdash \neg(\alpha \to \beta)$, отсюда $M \vdash \neg(\alpha \to \beta)$. Предположим, что $\alpha \to \beta \in M$, то $M \vdash \alpha \to \beta$ — отсюда $\alpha \to \beta \notin M$.

Доказательство теоремы о существовании модели

Доказательство.

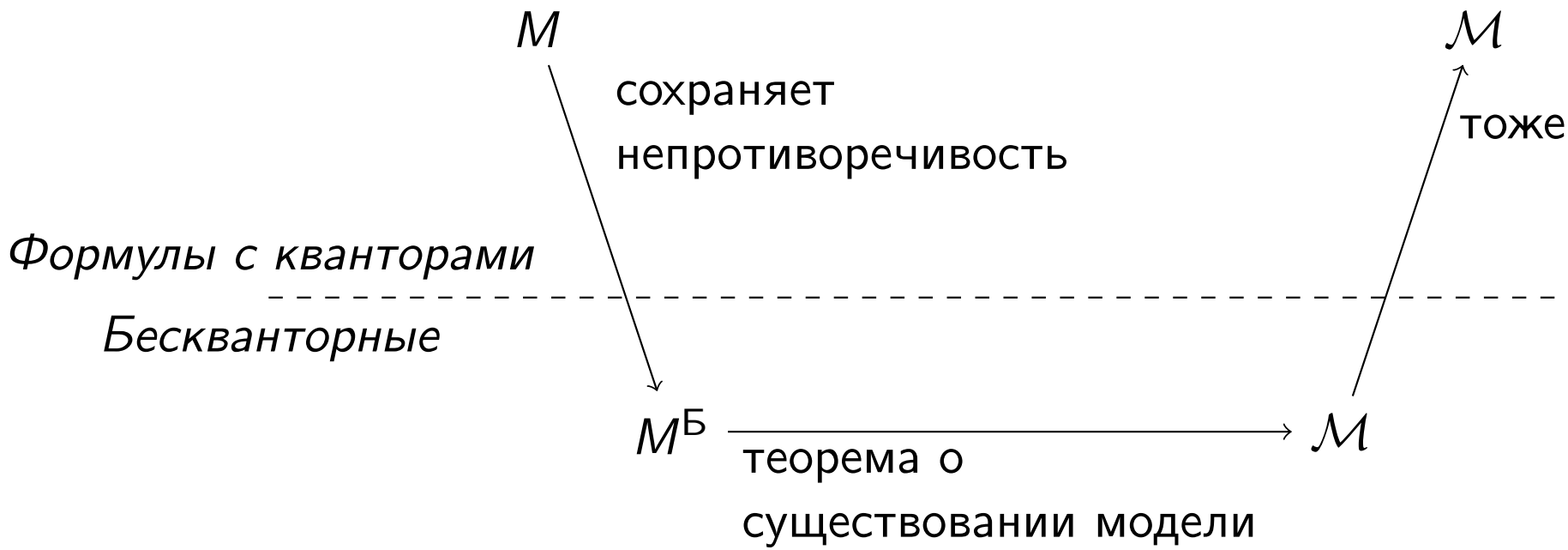
Пусть M — непротиворечивое множество замкнутых бескванторных формул.
По теореме о пополнении существует M' — полное непротиворечивое множество замкнутых бескванторных формул, что $M \subseteq M'$.
По лемме M' имеет модель, эта модель подойдёт для M. $\square$

Формулировка и схема доказательства теоремы Гёделя о полноте

Теорема (Гёделя о полноте исчисления предикатов)

Если M — непротиворечивое множество замкнутых формул, то оно имеет модель.

Схема доказательства.



□

Поверхностные кванторы (предварённая форма)

Определение

Формула φ имеет поверхностные кванторы (находится в предварённой форме), если соответствует грамматике

$$\varphi ::= \forall x.\varphi \mid \exists x.\varphi \mid \tau$$

где τ — формула без кванторов

Теорема

Для любой замкнутой формулы ψ найдётся такая формула φ с поверхностными кванторами, что $\vdash \psi \to \varphi$ и $\vdash \varphi \to \psi$

Доказательство.

Индукция по структуре, применение теорем о перемещении кванторов. $\square$

Построение M^*

- Пусть M — полное непротиворечивое множество замкнутых формул с поверхностными кванторами (очевидно, счётное). Построим семейство непротиворечивых множеств замкнутых формул M_k.
- Пусть d_i^k — семейство *свежих* констант, в M не встречающихся.
- Индуктивно построим M_k:
  - База: $M_0 = M$
  - Переход: положим $M_{k+1} = M_k \cup S$, где множество S получается перебором всех формул $\varphi_i \in M_k$.
    1. φ_i — формула без кванторов, пропустим;
    2. $\varphi_i = \forall x.\psi$ — добавим к S все формулы вида $\psi[x := \theta]$, где θ — всевозможные замкнутые термы, использующие символы из M_k;
    3. $\varphi_i = \exists x.\psi$ — добавим к S формулу $\psi[x := d_i^{k+1}]$, где d_i^{k+1} — некоторая свежая, ранее не использовавшаяся в M_k, константа.

Непротиворечивость M_k

Лемма

Если M непротиворечиво, то каждое множество из M_k — непротиворечиво

Доказательство.

Доказательство по индукции, база очевидна ($M_0 = M$).
Переход:

- пусть M_k непротиворечиво, но M_{k+1} — противоречиво: $M_k, M_{k+1} \setminus M_k \vdash A \,\&\, \neg A$.
- Тогда (т.к. доказательство конечной длины): $M_k, \gamma_1, \gamma_2, \ldots, \gamma_n \vdash A \,\&\, \neg A$, где $\gamma_i \in M_{k+1} \setminus M_k$.
- По теореме о дедукции: $M_k \vdash \gamma_1 \to \gamma_2 \to \cdots \to \gamma_n \to A \,\&\, \neg A$.
- Научимся выкидывать первую посылку: $M_k \vdash \gamma_2 \to \cdots \to \gamma_n \to A \,\&\, \neg A$.
- И по индукции придём к противоречию: $M_k \vdash A \,\&\, \neg A$.

Устранение посылки

Лемма

Если $M_k \vdash \gamma \to W$ *и* $\gamma \in M_{k+1} \setminus M_k$, *то* $M_k \vdash W$.

Доказательство.

Покажем, как дополнить доказательство до $M_k \vdash W$, в зависимости от происхождения γ:

- Случай $\forall x.\varphi$: $\gamma = \varphi[x := \theta]$. Допишем в конец доказательства:

$\forall x.\varphi$	(гипотеза)
$(\forall x.\varphi) \to (\varphi[x := \theta])$	(сх. акс. 11)
γ	(M.P.)
W	(M.P.)

□

Случай $\exists x.\varphi$

- $\gamma = \varphi[x := d_i^{k+1}]$
- Перестроим доказательство $M_k \vdash \gamma \to W$: заменим во всём доказательстве d_i^{k+1} на y. Коллизий нет: под квантором d_i^{k+1} не стоит, переменной не является.
- Получим доказательство $M_k \vdash \gamma[d_i^{k+1} := y] \to W$ и дополним его:

$\varphi[x := y] \to W$	$\varphi[x := d_i^{k+1}][d_i^{k+1} := y]$
$(\exists y.\varphi[x := y]) \to W$	y не входит в W
$(\exists x.\varphi) \to (\exists y.\varphi[x := y])$	доказуемо (упражнение)
$\ldots$	
$(\exists x.\varphi) \to W$	доказуемо как $(\alpha \to \beta) \to (\beta \to \gamma) \vdash$
$\exists x.\varphi$	гипотеза
W	

□

Построение $M^{Б}$

Определение

$M^* = \bigcup_k M_k$

Теорема

M^* непротиворечиво.

Доказательство.

От противного: доказательство противоречия конечной длины, гипотезы лежат в максимальном M_k, тогда M_k противоречив. □

Определение

$M^{Б}$ — множество всех бескванторных формул из M^*.

По непротиворечивому множеству M можем построить $M^{Б}$ и для него построить модель $\mathcal{M}$. Покажем, что эта модель годится для M^* (и для M, так как $M \subset M^*$).

Модель для M^*

Лемма

$\mathcal{M}$ есть модель для M^*.

Доказательство.

Покажем, что при $\varphi \in M^*$ выполнено $\mathcal{M} \models \varphi$. Докажем индукцией по количеству кванторов в φ.

- База: φ без кванторов. Тогда $\varphi \in M^{\text{Б}}$, отсюда $\mathcal{M} \models \varphi$ по построению $\mathcal{M}$.
- Переход: пусть утверждение выполнено для всех формул с n кванторами. Покажем, что это выполнено и для $n+1$ кванторов.
  - Рассмотрим $\varphi = \exists x.\psi$, случай квантор всеобщности — аналогично.
  - Раз $\exists x.\psi \in M^*$, то существует k, что $\exists x.\psi \in M_k$.
  - Значит, $\psi[x := d_i^{k+1}] \in M_{k+1}$.
  - По индукционному предположению, $\mathcal{M} \models \psi[x := d_i^{k+1}]$ — в формуле n кванторов.
  - Но тогда $[\![\psi]\!]^{x:=[\![d_i^{k+1}]\!]} = \text{И}$.
  - Отсюда $\mathcal{M} \models \exists x.\psi$.

Теорема Гёделя о полноте исчисления предикатов

Теорема (Гёделя о полноте исчисления предикатов)

Если M — замкнутое непротиворечивое множество формул, то оно имеет модель.

Доказательство.

- Построим по M множество формул с поверхностными кванторами M'.
- По M' построим непротиворечивое множество замкнутых бескванторных формул $M^{\text{Б}}$ ($M^{\text{Б}} \subseteq M^*$, теорема о непротиворечивости M^*).
- Дополним его до полного, построим для него модель $\mathcal{M}$ (теорема о существовании модели).
- $\mathcal{M}$ будет моделью и для M' ($M' \subseteq M^*$, лемма о модели для M^*), и, очевидно, для M.

Полнота исчисления предикатов

Следствие (из теоремы Гёделя о полноте)

Исчисление предикатов полно.

Доказательство.

- Пусть это не так, и существует формула φ, что $\models \varphi$, но $\nvdash \varphi$.
- Тогда рассмотрим $M = \{\neg\varphi\}$.
- M непротиворечиво: если $\neg\varphi \vdash A \,\&\, \neg A$, то $\vdash \varphi$ (упражнение).
- Значит, у M есть модель $\mathcal{M}$, и $\mathcal{M} \models \neg\varphi$.
- Значит, $[\![\neg\varphi]\!] = \text{И}$, поэтому $[\![\varphi]\!] = \text{Л}$, поэтому $\not\models \varphi$. Противоречие.

$\square$

Непротиворечивость исчисления предикатов

Теорема

Если у множества формул M есть модель $\mathcal{M}$, оно непротиворечиво.

Доказательство.

Пусть противоречиво: $M \vdash A \,\&\, \neg A$, в доказательстве использованы гипотезы $\delta_1, \delta_2, \ldots, \delta_n$. Тогда $\vdash \delta_1 \to \delta_2 \to \cdots \to \delta_n \to A \,\&\, \neg A$, то есть $[\![\delta_1 \to \delta_2 \to \cdots \to \delta_n \to A \,\&\, \neg A]\!] = \text{И}$ (корректность). Поскольку все $[\![\delta_i]\!]_{\mathcal{M}} = \text{И}$, то и $[\![A \,\&\, \neg A]\!]_{\mathcal{M}} = \text{И}$ (анализ таблицы истинности импликации). Однако $[\![A \,\&\, \neg A]\!] = \text{Л}$. Противоречие. □

Следствие

Исчисление предикатов непротиворечиво

Доказательство.

Рассмотрим $M = \varnothing$ и любую классическую модель. □

Доказательства опираются на непротиворечивость метатеории.

Лекция 7

Неразрешимость исчисления предикатов
Аксиоматика Пеано и формальная арифметика

Общие результаты об исчислениях

	К.И.В.	И.И.В.	К.И.П.
корректность	да (лекция 1)	да (ДЗ IV.10)	да (лекци
непротиворечивость	да (очев.)	да (из непр. КИВ)	да (лекци
полнота	да (лекция 2)	да (лекция 4)	да (лекци
разрешимость	да (лекция 2)	да (лекция 4)	Нет (сейч

Машина Тьюринга

Определение

Машина Тьюринга:

1. *Внешний алфавит* $q_1, \ldots, q_n$, *выделенный символ-заполнитель* q_ε
2. *Внутренний алфавит (состояний)* $s_1, \ldots, s_k$; s_s — *начальное,* s_f — *допускающее,* s_r — *отвергающее.*
3. *Таблица переходов* $\langle k, s \rangle \Rightarrow \langle k', s', \leftrightarrow \rangle$

Определение

Состояние машины Тьюринга:

1. *Бесконечная лента с символом-заполнителем* q_ε, *текст конечной длины.*
2. *Головка над определённым символом.*
3. *Символ состояния (состояние в узком смысле) — символ внутреннего алфавита.*

Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

	ε	0	1
s_s	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
s_f	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

Пример

Головка — на первом символе 011, *состояние* s_s.

$\underline{0}11 \Rightarrow 1\underline{1}1 \Rightarrow 10\underline{1} \Rightarrow 100\underline{\varepsilon}$

Состояние s_f, *допускающее.*

Разрешимость

Определение

Язык — множество строк

Определение

Язык L разрешим, если существует машина Тьюринга, которая для любого слова w переходит в допускающее состояние, если $w \in L$, и в отвергающее, если $w \notin L$.

Неразрешимость задачи останова

Определение

Рассмотрим все возможные описания машин Тьюринга. Составим упорядоченные пары: описание машины Тьюринга и входная строка. Из них выделим язык останавливающихся на данном входе машин Тьюринга.

Теорема

Язык всех останавливающихся машин Тьюринга неразрешим

Доказательство.

От противного. Пусть $S(x, y)$ — машина Тьюринга, определяющая, остановится ли машина x, примененная к строке y.

W(x) = if (S(x,x)) { while (true); return 0; } else { return 1; }

Что вернёт $S(code(W), code(W))$? □

Кодируем состояние

1. внешний алфавит: n 0-местных функциональных символов $q_1, \ldots, q_n$; q_ε — символ-заполнитель.
2. список: ε и $c(l, s)$; «abc» представим как $c(q_a, c(q_b, c(q_c, \varepsilon)))$.
3. положение головки: «$ab\underline{p}q$» как $(c(q_b, c(q_a, \varepsilon)), c(q_p, c(q_q, \varepsilon)))$.
4. внутренний алфавит: k 0-местных функциональных символов $s_1, \ldots, s_k$. Из них выделенные s_s — начальное и s_f — допускающее состояние.

Достижимые состояния

Предикатный символ $F_{x,y}(w_l, w_r, s)$: если у машины x с начальной строкой y состояние s достижимо на строке $rev(w_l)@w_r$. Будем накладывать условия: семейство формул C_m. Очевидно, начальное состояние достижимо:

$$C_0 := F_{x,y}(\varepsilon, y, s_s)$$

Кодируем переходы

1. Занумеруем переходы.
2. Закодируем переход m:

$$\langle k, s\rangle \Rightarrow \langle k', s', \rightarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

$C_m = \forall w_l.\forall w_r.F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow$
$F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'})$
(здесь требуется, чтобы под головкой находился непустой символ q_k, потому мы обязательно требуем, чтобы лента была непуста)

3. Переход посложнее:

$$\langle k, s\rangle \Rightarrow \langle k', s', \leftarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

$C_m = \forall w_l.\forall w_r.\forall t.F_{x,y}(c(t, w_l), c(q_k, w_r), s_s) \rightarrow$
$F_{x,y}(w_l, c(t, c(q_{k'}, w_r)), s_{s'}) \,\&\, \forall w_l.\forall w_r.F_{x,y}(\varepsilon, c(q_k, w_r), s_s) \rightarrow$
$F_{x,y}(\varepsilon, c(q_\varepsilon, c(q_{k'}, w_r)), s_{s'})$

4. и т.п.

Итоговая формула

$$C = C_0 \,\&\, C_1 \,\&\, \cdots \,\&\, C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

Теорема

Состояние s со строкой $rev(w_l)@w_r$ достижимо тогда и только тогда, когда $C \vdash F_{x,y}(w_l, w_r, s)$

Доказательство.

($\Leftarrow$) Рассмотрим модель: предикат $F_{x,y}(w_l, w_r, s)$ положим истинным, если состояние достижимо. Это — модель для C (по построению C_m). Значит, доказуемость влечёт истинность (по корректности).

($\Rightarrow$) Индукция по длине лога исполнения. $\square$

Неразрешимость исчисления предикатов: доказательство

Теорема

Язык всех доказуемых формул исчисления предикатов неразрешим

Т.е. нет машины Тьюринга, которая бы по любой формуле α определяла, доказуема ли она.

Доказательство.

Пусть существует машина Тьюринга, разрешающая любую формулу. На её основе тогда несложно построить некоторую машину Тьюринга, перестраивающую любую машину S (с допускающим состоянием s_f и входом y) в её ограничения C и разрешающую формулу ИП $C \to \exists w_l . \exists w_r . F_{S,y}(w_l, w_r, s_f)$. Эта машина разрешит задачу останова. $\square$

Аксиоматика Пеано и формальная арифметика

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:
   2.1 $A \cup B = \mathbb{Q}$
   2.2 Если $a \in A$, $x \in \mathbb{Q}$ и $x \leq a$, то $x \in A$
   2.3 Если $b \in B$, $x \in \mathbb{Q}$ и $b \leq x$, то $x \in B$
   2.4 A не содержит наибольшего.

   $\mathbb{R}$ — множество всех возможных дедекиндовых сечений.
   $\sqrt{2} = \{\{x \in \mathbb{Q} \mid x < 0 \vee x^2 < 2\}, \{x \in \mathbb{Q} \mid x > 0 \ \& \ x^2 > 2\}\}$

Целые числа тоже попробуем определить

$$\mathbb{Z} : \cdots -3, -2, -1, 0, 1, 2, 3, \ldots$$

- $Z = \{\langle x, y\rangle \mid x, y \in \mathbb{N}_0\}$
- Интуиция: $\langle x, y\rangle = x - y$
- $$\begin{aligned} \langle a, b\rangle + \langle c, d\rangle &= \langle a + c, b + d\rangle \\ \langle a, b\rangle - \langle c, d\rangle &= \langle a + d, b + c\rangle \end{aligned}$$
- Пусть $\langle a, b\rangle \equiv \langle c, d\rangle$, если $a + d = b + c$. Тогда $\mathbb{Z} = Z/_{\equiv}$
- $0 = [\langle 0, 0\rangle]$, $1 = [\langle 1, 0\rangle]$, $-7 = [\langle 0, 7\rangle]$

Натуральные числа: аксиоматика Пеано, 1889

$\mathbb{N} : 1, 2, \ldots$ или $\mathbb{N}_0 : 0, 1, 2, \ldots$

Определение

N (или, более точно, $\langle N, 0, (') \rangle$) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. *Операция «штрих» $(') : N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$.*
   Если $x = y'$, то x назовём следующим за y, а y — предшествующим x.
2. *Константа $0 \in N$: нет $x \in N$, что $x' = 0$.*
3. *Индукция. Каково бы ни было свойство («предикат») $P : N \to V$, если:*
   - 3.1 *$P(0)$*
   - 3.2 *При любом $x \in N$ из $P(x)$ следует $P(x')$*

   то при любом $x \in N$ выполнено $P(x)$.

Как построить? Например, в стиле алгебры Линденбаума:

1. N — язык, порождённый грамматикой $\nu ::= 0 \mid \nu$«’»
2. 0 — это «0», x' — это $x +\!\!+$ «’»

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$
2. Кольцо вычетов $\mathbb{Z}/7\mathbb{Z}$, где $x' = x + 1$
   $6' = 0$, что нарушает свойства 0
3. $\mathbb{R}^+ \cup \{0\}$, где $x' = x + 1$
   Пусть $P(x)$ означает «$x \in \mathbb{Z}$»:
   - 3.1 $P(0)$ выполнено: $0 \in \mathbb{Z}$.
   - 3.2 Если $P(x)$, то есть $x \in \mathbb{Z}$, то и $x + 1 \in \mathbb{Z}$ — так что и $P(x')$ выполнено.

   Однако $P(0.5)$ ложно.

Пример доказательства

Теорема

0 единственен: если t таков, что при любом y выполнено $y' \neq t$, то $t = 0$.

Доказательство.

- Определим $P(x)$ как «либо $x = 0$, либо $x = y'$ для некоторого $y \in N$».
  1. $P(0)$ выполнено, так как $0 = 0$.
  2. Если $P(x)$ выполнено, то возьмём x в качестве y: тогда для $P(x')$ будет выполнено $x' = y'$.

  Значит, $P(x)$ для любого $x \in N$.
- Рассмотрим $P(t)$: «либо $t = 0$, либо $t = y'$ для некоторого $y \in N$». Но так как такого y нет, то неизбежно $t = 0$.

□

Обозначения и определения

Определение

$1 = 0'$, $2 = 0''$, $3 = 0'''$, $4 = 0''''$, $5 = 0'''''$, $6 = 0''''''$, $7 = 0'''''''$, $8 = 0''''''''$, $9 = 0'''''''''$

Определение

$$a + b = \begin{cases} a, & \textit{если } b = 0 \\ (a + c)', & \textit{если } b = c' \end{cases}$$

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' = ((0'' + 0)')' = ((0'')')' = 0'''' = 4$$

Определение

$$a \cdot b = \begin{cases} 0, & \textit{если } b = 0 \\ a \cdot c + a, & \textit{если } b = c' \end{cases}$$

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

$$a+b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$
2. Покажем, что если $P(x)$, то $P(x')$. Покажем $P(x')$, то есть $x' + 0 = \ldots$

$$\begin{array}{lll} \cdots = x' & a = x', b = 0: & x' + 0 \Rightarrow x' \\ \cdots = (x)' & & \\ \cdots = (x + 0)' & a = x, b = 0: & (x + 0) \Leftarrow (x) \\ \cdots = (0 + x)' & P(x): & (x + 0) \Rightarrow (0 + x) \\ \cdots = 0 + x' & a = 0, b = x': & 0 + x' \Leftarrow (0 + x)' \end{array}$$

Значит, $P(a)$ выполнено для любого $a \in N$. □

Пример: коммутативность сложения (завершение)

Лемма (2)

$a + b' = a' + b$

Доказательство.

$P(x)$ — это $a + x' = a' + x$

1. $a + 0' = (a + 0)' = (a)' = a' = a' + 0$
2. Покажем, что $P(x')$ следует из $P(x)$:
   $a + x'' = (a + x')' = (a' + x)' = a' + x'$

□

Теорема

$a + b = b + a$

Доказательство индукцией по b: $P(x)$ — это $a + x = x + a$.

1. $a + 0 = 0 + a$ (лемма 1)
2. $a + x' = (a + x)' = (x + a)' = x + a' = x' + a$

□

Уточнение исчисления предикатов

- Пусть требуется доказывать утверждения про равенство. Введём $E(p, q)$ — предикат «равенство».
- Однако $\nvdash \forall E(p, q) \to E(q, p)$: если $D = \{0, 1\}$ и $E(p, q) ::= (p > q)$, то $\not\models E(p, q) \to E(q, p)$.
- Конечно, можем указывать $\forall p.\forall q.E(p, q) \to E(q, p) \vdash \varphi$.
- Но лучше добавим аксиому $\forall p.\forall q.E(p, q) \to E(q, p)$.
- Добавив необходимые аксиомы, получим *теорию первого порядка*.

Теория первого порядка

Определение

Теорией первого порядка назовём исчисление предикатов с дополнительными («нелогическими» или «математическими»):

- *предикатными и функциональными символами;*
- *аксиомами.*

Сущности, взятые из исходного исчисления предикатов, назовём логическими

Порядок логики/теории

Порядок	Кванторы	Формализует суждения...
нулевой	запрещены	об отдельных значениях
первый	по предметным переменным	о множествах
	$\{2,3,5,7,\dots\} = \{t \mid \forall p.\forall q.(p \neq 1 \,\&\, q \neq 1) \to (t \neq p \cdot q)\}$	
второй	по предикатным переменным	о множествах множеств
	$S = \{\{t \mid P(t)\} \mid \varphi[p := P]\}$	
	...	

Пример (логики 2 порядка)

$\alpha \to \beta \to \alpha$ (сх. акс. 1) $\quad \forall a.\forall b.a \to b \to a$

```
let rec map f l = match l with
| [] -> []
| l1::ls -> f l1 :: map f l1
```

$map : \forall a.\forall b.(a \to b) \to a$ `list`

```
map ((+) 1) [1;2;3] = [2;3;4]
```

Формальная арифметика

Определение

Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими . . .

- *двухместными функциональными символами* $(+)$, $(\cdot)$; *одноместным функциональным символом* $(')$, *нульместным функциональным символом* 0;
- *двухместным предикатным символом* $(=)$;
- *восемью нелогическими аксиомами:*

  (A1) $a = b \to a = c \to b = c$
  (A2) $a = b \to a' = b'$
  (A3) $a' = b' \to a = b$
  (A4) $\neg a' = 0$
  (A5) $a + 0 = a$
  (A6) $a + b' = (a + b)'$
  (A7) $a \cdot 0 = 0$
  (A8) $a \cdot b' = a \cdot b + a$

- *нелогической схемой аксиом индукции* $\psi[x := 0]\ \&\ (\forall x.\psi \to \psi[x := x']) \to \psi$ *с метапеременными* x *и* ψ.

Докажем, что $a = a$

Пусть $\top ::= 0 = 0 \to 0 = 0 \to 0 = 0$, тогда:

(1)	$a = b \to a = c \to b = c$	(Акс. А
(2)	$(a = b \to a = c \to b = c) \to \top \to (a = b \to a = c \to b = c)$	(Сх. ак
(3)	$\top \to (a = b \to a = c \to b = c)$	(M.P. 1
(4)	$\top \to (\forall c.a = b \to a = c \to b = c)$	(Введ.
(5)	$\top \to (\forall b.\forall c.a = b \to a = c \to b = c)$	(Введ.
(6)	$\top \to (\forall a.\forall b.\forall c.a = b \to a = c \to b = c)$	(Введ.
(7)	$\top$	(Сх. ак
(8)	$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c)$	(M.P. 7
(9)	$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c) \to$ $\to (\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c)$	(Сх. ак
(10)	$\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c$	(M.P. 8
(12)	$\forall c.a + 0 = a \to a + 0 = c \to a = c$	(M.P. 1
(14)	$a + 0 = a \to a + 0 = a \to a = a$	(M.P. 1
(15)	$a + 0 = a$	(Акс. А
(16)	$a + 0 = a \to a = a$	(M.P. 1
(17)	$a = a$	(M.P. 1

Арифметизация логики

Общие замечания

- Рассматриваем функции $\mathbb{N}_0^n \to \mathbb{N}_0$.
- Обозначим вектор $\langle x_1, x_2, \ldots, x_n \rangle$ как $\overrightarrow{x}$.

Примитивно-рекурсивные функции

Определение (Примитивы Z, N, U, S)

1. *Примитив «Ноль» (Z)*
$$Z : \mathbb{N}_0 \to \mathbb{N}_0, \qquad Z(x_1) = 0$$

2. *Примитив «Инкремент» (N)*
$$N : \mathbb{N}_0 \to \mathbb{N}_0, \qquad N(x_1) = x_1 + 1$$

3. *Примитив «Проекция» (U) — семейство функций; пусть* $k, n \in \mathbb{N}_0, k \leq n$
$$U_n^k : \mathbb{N}_0^n \to \mathbb{N}_0, \qquad U_n^k(\overrightarrow{x}) = x_k$$

4. *Примитив «Подстановка» (S) — семейство функций; пусть* $g : \mathbb{N}_0^k \to \mathbb{N}_0, \quad f_1, \ldots, f_k : \mathbb{N}_0^n \to \mathbb{N}_0$
$$S\langle g, f_1, f_2, \ldots, f_k\rangle(\overrightarrow{x}) = g(f_1(\overrightarrow{x}), \ldots, f_k(\overrightarrow{x}))$$

Примитивная рекурсия

Определение (примитив «примитивная рекурсия», R)

Пусть $f : \mathbb{N}_0^n \to \mathbb{N}_0$ *и* $g : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$. *Тогда* $R\langle f, g\rangle : \mathbb{N}_0^{n+1} \to \mathbb{N}_0$, *причём*

$$R\langle f, g\rangle(\overrightarrow{x}, y) = \begin{cases} f(\overrightarrow{x}), & y = 0 \\ g(\overrightarrow{x}, y-1, R\langle f, g\rangle(\overrightarrow{x}, y-1)), & y > 0 \end{cases}$$

Пояснение

```
res := f(x1...xn);
for yi = 0 to y-1 do
    res := g(x1...xn,yi,res);
```

Пример

$$\begin{aligned} R\langle f, g\rangle(\overrightarrow{x}, 3) &= g(\overrightarrow{x}, 2, R\langle f, g\rangle(\overrightarrow{x}, 2)) \\ &= g(\overrightarrow{x}, 2, g(\overrightarrow{x}, 1, R\langle f, g\rangle(\overrightarrow{x}, 1))) \\ &= g(\overrightarrow{x}, 2, g(\overrightarrow{x}, 1, g(\overrightarrow{x}, 0, R\langle f, g\rangle(\overrightarrow{x}, 0)))) \\ &= g(\overrightarrow{x}, 2, g(\overrightarrow{x}, 1, g(\overrightarrow{x}, 0, f(\overrightarrow{x})))) \end{aligned}$$

Примитивно-рекурсивные функции

Определение

Функция f — примитивно-рекурсивна, если может быть выражена как композиция примитивов Z, N, U, S и R.

Теорема

$f(x) = x + 2$ *примитивно-рекурсивна*

Доказательство.

$f = S\langle N, N\rangle$

$N(x) = x + 1$
$S\langle g, f\rangle(x) = g(f(x))$

$f, g = N$
$S\langle N, N\rangle(x) = N(N(x)) = (x + 1) + 1$ □

Примитивно-рекурсивные функции: $x + y$

Лемма

$f(a, b) = a + b$ *примитивно-рекурсивна*

Доказательство.

$f = R\langle U_1^1, S\langle N, U_3^3\rangle\rangle$:

$$R\langle f, g\rangle(x, y) = \begin{cases} f(x), & y = 0 \\ g(x, y-1, R\langle f, g\rangle(x, y-1)), & y > 0 \end{cases}$$

- База. $R\langle U_1^1, S\langle N, U_3^3\rangle\rangle(x, 0) = U_1^1(x) = x$
- Переход. $R\langle U_1^1, S\langle N, U_3^3\rangle\rangle(x, y+1) =$
  $\ldots = S\langle N, U_3^3\rangle(x, y, R\langle U_1^1(x), S\langle N, U_3^3\rangle\rangle(x, y)) =$
  $\ldots = S\langle N, U_3^3\rangle(x, y, x + y) =$
  $\ldots = N(x + y) = x + y + 1$

□

Какие функции примитивно-рекурсивные?

1. Сложение, вычитание
2. Умножение, деление
3. Вычисление простых чисел
4. Неформально: все функции, вычисляемые конечным числом вложенных циклов `for`:

```
for (int i1 = 0; i1 < g1(x1...xn); i1++) {
    for (int i2 = 0; i2 < g2(x1...xn,i1); i2++) {
        ...
            for (int ik = 0; ik < gk(x1...xn,i1,i2...); i
                // выражение без циклов
            }
        ...
    }
}
```

Общерекурсивные функции

Определение

Функция — общерекурсивная, если может быть построена при помощи примитивов Z, N, U, S, R и примитива минимизации:

$$M\langle f\rangle(x_1, x_2, \ldots, x_n) = \min\{y : f(x_1, x_2, \ldots, x_n, y) = 0\}$$

Если $f(x_1, x_2, \ldots, x_n, y) > 0$ при любом y, результат не определён.

Пример:
Пусть $f(x, y) = x - y^2$, тогда $\lceil\sqrt{x}\rceil = M\langle f\rangle(x)$

```
int sqrt(int x) {
    int y = 0;
    while (x-y*y > 0) y++;
    return y;
}
```

Выразительная сила

Определение

Функция Аккермана:

$$A(m,n) = \begin{cases} n+1, & m = 0 \\ A(m-1,1), & m > 0, n = 0 \\ A(m-1, A(m,n-1)), & m > 0, n > 0 \end{cases}$$

Пример

n	0	1	2	3	4	...
0	1	2	3	5	13	
1	2	3	5	13	65533	
2	3	4	7	29	$2^{65536} - 3$	
n	$n+1$	$n+2$	$2n+3$	$2^{n+3} - 3$	$\underbrace{2^{2^{2^{\cdots^{2}}}}}_{n+3} - 3$	

Лемма о росте функции Аккермана

Определение

$$A^{(p)}(k,x) = \underbrace{A(k,A(k,A(k,\ldots,A(k,x))))}_{p \text{ раз}}$$

$$A(m,n) = \begin{cases} n+1, & m = 0 \\ A(m-1,1), & m > 0 \\ A(m-1,A(m,n-1)), & m > 0 \end{cases}$$

Лемма

1. $A(p,q) = A^{(q+1)}(p-1,1)$
2. $A^{(x+2)}(k,x) < A(k+2,x)$

$A(0,n) = n+1$
$A(2,n) = 2n+3$

Доказательство.

1. $A(p,q) = A(p-1,A(p,q-1)) = \cdots = A(p-1,A(p-1,\ldots A(p,0)) = A^{(q)}(p-1,A(p,0)) = A^{(q+1)}(p-1,1)$
2. $A(k+2,x) = A(k+1,A(k+2,x-1)) = A^{(A(k+2,x-1)+1)}(k,1) \geq A^{(A(2,x-1)+1)}(k,1) = A^{(2(x-1)+3+1)}(k,1) = A^{(2x+2)}(k,1) = A^{(x+2)}(k,A^{(x)}(k,1)) \geq A^{(x+2)}(k,A^{(x)}(0,1)) = A^{(x+2)}(k,x+1) > A^{(x+2)}(k,x)$

Функция Аккермана не примитивно-рекурсивна

Теорема

Пусть $f(\overrightarrow{x})$ *— примитивно-рекурсивная. Тогда найдётся* k*, что* $f(\overrightarrow{x}) < A(k, \max(\overrightarrow{x}))$

Доказательство.

Индукция по структуре f.

1. $f = Z$, тогда $k = 0$, т.к. $A(0, x) = x + 1 > Z(x) = 0$;
2. $f = N$, тогда $k = 1$, т.к. $A(1, x) = x + 2 > N(x) = x + 1$;
3. $f = U_s^n$, тогда $k = 0$, т.к. $f(\overrightarrow{x}) \leq \max(\overrightarrow{x}) < A(0, \max(\overrightarrow{x}))$;
4. $f = S\langle g, h_1, \ldots, h_n \rangle$, тогда $k = k_g + \max(k_{h_1}, \ldots, k_{h_n}) + 2$;
5. $f = R\langle g, h \rangle$, тогда $k = \max(k_g, k_h) + 2$.

□

Доказательство оценки для R

Лемма

Пусть $f = R\langle g, h\rangle$. *Тогда при* $k = \max(k_g, k_h) + 2$ *выполнено* $f(\overrightarrow{x}, y) \leq A^{(y+1)}(k-2, \max(\overrightarrow{x}, y))$.

Доказательство.

Индукция по y.

- База: $y = 0$. Тогда:
  $f(\overrightarrow{x}, 0) = g(\overrightarrow{x}) \leq A(k_g, \max(\overrightarrow{x})) \leq A^{(1)}(k-2, \max(\overrightarrow{x}, 0))$.
- Переход: пусть $f(\overrightarrow{x}, y) \leq A^{(y+1)}(k-2, \max(\overrightarrow{x}, y))$. Тогда
  $f(\overrightarrow{x}, y+1) = h(\overrightarrow{x}, y, f(\overrightarrow{x}, y)) \leq$
  $A(k_h, \max(\overrightarrow{x}, y, f(\overrightarrow{x}, y))) \leq A(k_h, \max(\overrightarrow{x}, y, A^{(y+1)}(k-2, \max(\overrightarrow{x}, y)))) = A(k_h, A^{(y+1)}(k-2, \max(\overrightarrow{x}, y))) \leq$
  $A^{(y+2)}(k-2, \max(\overrightarrow{x}, y+1))$

□

Заметим, что
$A^{(y+1)}(k-2, \max(\overrightarrow{x}, y)) \leq A^{(\max(\overrightarrow{x}, y)+1)}(k-2, \max(\overrightarrow{x}, y)) \leq$
$A^{(\max(\overrightarrow{x}, y)+2)}(k-2, \max(\overrightarrow{x}, y)) < A(k, \max(\overrightarrow{x}, y))$

Тезис Чёрча

Определение

Тезис Чёрча для общерекурсивных функций: любая эффективно-вычислимая функция $\mathbb{N}_0^k \to \mathbb{N}_0$ *является общерекурсивной.*

Новые обозначения

Определение

Запись вида $\psi(\theta_1, \ldots, \theta_n)$ *означает* $\psi[x_1 := \theta_1, \ldots, x_n := \theta_n]$

Определение (Литерал числа)

$$\overline{a} = \begin{cases} 0, & \text{если } a = 0 \\ (\overline{b})', & \text{если } a = b + 1 \end{cases}$$

Пример: пусть $\psi := x_1 = 0$. Тогда $\psi(\overline{3})$ соответствует формуле $0''' = 0$

Выразимость отношений в Ф.А.

Определение

Будем говорить, что отношение $R \subseteq \mathbb{N}_0^n$ *выразимо в ФА, если существует формула* ρ*, что:*

1. *если* $\langle a_1, \ldots, a_n \rangle \in R$*, то* $\vdash \rho(\overline{a_1}, \ldots, \overline{a_n})$
2. *если* $\langle a_1, \ldots, a_n \rangle \notin R$*, то* $\vdash \neg\rho(\overline{a_1}, \ldots, \overline{a_n})$

Теорема

отношение «равно» выразимо в Ф.А.: $R = \{\langle x, x \rangle \mid x \in \mathbb{N}_0\}$

Доказательство.

Пусть $\rho := x_1 = x_2$. Тогда:

- $\vdash p = p$ при $p := \overline{k}$ при всех $k \in \mathbb{N}_0$: $\vdash 0 = 0$, $\vdash 0' = 0'$, $\vdash 0'' = 0''$, ...
- $\vdash \neg p = q$ при $p := \overline{k}$, $q := \overline{s}$ при всех $k, s \in \mathbb{N}_0$ и $k \neq s$. $\vdash \neg 0 = 0'$, $\vdash \neg 0 = 0''$, $\vdash \neg 0''' = 0'$, ...

Представимость функций в Ф.А.

Определение

Будем говорить, что функция $f : \mathbb{N}_0^n \to \mathbb{N}_0$ *представима в ФА, если существует формула* φ*, что:*

1. *если* $f(a_1, \ldots, a_n) = u$*, то* $\vdash \varphi(\overline{a_1}, \ldots, \overline{a_n}, \overline{u})$
2. *если* $f(a_1, \ldots, a_n) \neq u$*, то* $\vdash \neg\varphi(\overline{a_1}, \ldots, \overline{a_n}, \overline{u})$
3. *для всех* $a_i \in \mathbb{N}_0$ *выполнено* $\vdash (\exists x.\varphi(\overline{a_1}, \ldots, \overline{a_n}, x))\ \&$ $(\forall p.\forall q.\varphi(\overline{a_1}, \ldots, \overline{a_n}, p)\ \&\ \varphi(\overline{a_1}, \ldots, \overline{a_n}, q) \to p = q)$

Соответствие рекурсивных и представимых функций

Теорема

Любая рекурсивная функция представима в Ф.А.

Теорема

Любая представимая в Ф.А. функция рекурсивна.

Примитивы Z, N, U представимы в Ф.А.

Теорема

Примитивы Z, N и U_n^k представимы в Ф.А.

Доказательство.

- $\zeta(x_1, x_2) := x_2 = 0$, формальнее:
  $\zeta(x_1, x_2) := x_1 = x_1 \,\&\, x_2 = 0$
- $\nu(x_1, x_2) := x_2 = x_1'$
- $\upsilon(x_1, \ldots, x_n, x_{n+1}) := x_k = x_{n+1}$

  формальнее:
  $\upsilon(x_1, \ldots, x_n, x_{n+1}) := (\underset{i \neq k, n+1}{\&} x_i = x_i) \,\&\, x_k = x_{n+1}$

□

Примитив S представим в Ф.А.

$$S\langle f, g_1, \ldots, g_k\rangle(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n))$$

Теорема

Пусть функции $f, g_1, \ldots, g_k$ представимы в Ф.А. Тогда $S\langle f, g_1, \ldots, g_k\rangle$ представима в Ф.А.

Доказательство.

Пусть f, g_1, ..., g_k представляются формулами φ, γ_1, ..., γ_k.
Тогда $S\langle f, g_1, \ldots, g_k\rangle$ будет представлена формулой

$$\exists g_1 \ldots . \exists g_k . \varphi(g_1, \ldots, g_k, x_{n+1}) \& \gamma_1(x_1, \ldots, x_n, g_1) \& \cdots \& \gamma_k(x_1, \ldots, x_n, g_k$$

□

β-функция Гёделя

Задача: закодировать последовательность натуральных чисел произвольной длины.

Определение

β-функция Гёделя: $\beta(b, c, i) := b\%(1 + (i + 1) \cdot c)$
Здесь (%) — остаток от деления.

Теорема

β-функция Гёделя представима в Ф.А. формулой

$$\hat{\beta}(b, c, i, d) := \exists q.(b = q \cdot (1 + c \cdot (i + 1)) + d)\&(d < 1 + c \cdot (i + 1))$$

Деление b на x с остатком: найдутся частное (q) и остаток (d), что $b = q \cdot x + d$ и $0 \leq d < x$.

Теорема

Если $a_0, \ldots, a_n \in \mathbb{N}_0$, то найдутся такие $b, c \in \mathbb{N}_0$, что
$a_i = \beta(b, c, i)$

Доказательство свойства β-функции

Теорема

Китайская теорема об остатках (вариант формулировки): если $u_0, \ldots, u_n$ *— попарно взаимно просты, и* $0 \leq a_i < u_i$*, то существует такой* b*, что* $a_i = b\%u_i$*.*

Положим $c = \max(a_0, \ldots, a_n, n)!$ и $u_i = 1 + c \cdot (i + 1)$.

- НОД$(u_i, u_j) = 1$, если $i \neq j$.

  Пусть p — простое, $u_i \vdots p$ и $u_j \vdots p$ $(i < j)$. Заметим, что $u_j - u_i = c \cdot (j - i)$. Значит, $c \vdots p$ или $(j - i) \vdots p$. Так как $j - i \leq n$, то $c \vdots (j - i)$, потому если и $(j - i) \vdots p$, всё равно $c \vdots p$. Но и $(1 + c \cdot (i + 1)) \vdots p$, отсюда $1 \vdots p$ — что невозможно.
- $0 \leq a_i < u_i$.

Условия китайской теоремы об остатках выполнены и найдётся b, что

$$a_i = b\%(1 + c \cdot (i + 1)) = \beta(b, c, i)$$

□

Примитив «примитивная рекурсия» представим в Ф.А.

Пусть $f : \mathbb{N}_0^n \to \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$ представлены формулами φ и γ.

Зафиксируем $x_1, \ldots, x_n, y \in \mathbb{N}_0$.

Шаг вычисления	Об.	Утверждение
$R\langle f, g\rangle(x_1, \ldots, x_n, 0) = f(x_1, \ldots, x_n)$	a_0	$\vdash \varphi(\overline{x_1}, \ldots, \overline{x_n}$
$R\langle f, g\rangle(x_1, \ldots, x_n, 1) = g(x_1, \ldots, x_n, 0, a_0)$	a_1	$\vdash \gamma(\overline{x_1}, \ldots, \overline{x_n}$
$\ldots$		
$R\langle f, g\rangle(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y-1, a_{y-1})$	a_y	$\vdash \gamma(\overline{x_1}, \ldots, \overline{x_n}$

По свойству β-функции, найдутся b и c, что $\beta(b, c, i) = a_i$ для $0 \leq i \leq y$.

Теорема

Примитив $R\langle f, g\rangle$ представим в Ф.А. формулой $\rho(x_1, \ldots, x_n, y, a)$:

$$\begin{aligned}
&\exists b.\exists c.(\exists a_0.\hat{\beta}(b, c, 0, a_0)\&\varphi(x_1, \ldots x_n, a_0)) \\
\& \quad &\forall k.k < y \to \exists d.\exists e.\hat{\beta}(b, c, k, d)\&\hat{\beta}(b, c, k', e)\&\gamma(x_1, \ldots x_n, k, d, e) \\
\& \quad &\hat{\beta}(b, c, y, a)
\end{aligned}$$

Представимость рекурсивных функций в Ф.А.

Теорема

Пусть функция $f : \mathbb{N}_0^{n+1} \to \mathbb{N}_0$ *представима в Ф.А. формулой* $\varphi(x_1, \ldots, x_n, y, r)$. *Тогда примитив* $M\langle f \rangle$ *представим в Ф.А. формулой*

$$\mu(x_1, \ldots, x_n, y) := \varphi(x_1, \ldots, x_n, y, 0) \& \forall u.u < y \to \neg\varphi(x_1, \ldots, x_n, u, 0)$$

Теорема

Если f *— рекурсивная функция, то она представима в Ф.А.*

Доказательство.

Индукция по структуре f. □

Рекурсивность представимых функций в Ф.А.

Фиксируем f и $x_1, x_2, \ldots, x_n$. Обозначим $y = f(x_1, x_2, \ldots, x_n)$.
По представимости нам известна φ, что $\vdash \varphi(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}, \overline{y})$.
Давайте просто переберём все результаты и доказательства!

1. Закодируем доказательства натуральными числами.
2. Напишем рекурсивную функцию, проверяющую доказательства на корректность.
3. Параллельный перебор значений и доказательств:
   $s = 2^y \cdot 3^p$. Переберём все s, по s получим y и p. Проверим, что p — код доказательства $\vdash \varphi(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}, \overline{y})$.

Гёделева нумерация

1. Отдельный символ.

Номер	Символ	Номер	Символ	Имя	k, n	Гёдел
3	$($	17	$\&$	0	$0, 0$	$27+6$
5	$)$	19	$\forall$	$(')$	$0, 1$	$27+6$
7	$,$	21	$\exists$	$(+)$	$0, 2$	$27+6$
9	$.$	23	$\vdash$	$(\cdot)$	$1, 2$	$27+6$
11	$\neg$	$25+6\cdot k$	x_k	$(=)$	$0, 2$	$29+6$
13	$\to$	$27+6\cdot 2^k\cdot 3^n$	f_k^n			
15	$\vee$	$29+6\cdot 2^k\cdot 3^n$	P_k^n			

2. Формула. $\phi \equiv s_0 s_1 \dots s_{n-1}$. Гёделев номер:
$\ulcorner \phi \urcorner = 2^{\ulcorner s_0 \urcorner} \cdot 3^{\ulcorner s_1 \urcorner} \cdot \dots \cdot p_{n-1}^{\ulcorner s_{n-1} \urcorner}$.
3. Доказательство. $\Pi = \delta_0 \delta_1 \dots \delta_{k-1}$, его гёделев номер:
$\ulcorner \Pi \urcorner = 2^{\ulcorner \delta_0 \urcorner} \cdot 3^{\ulcorner \delta_1 \urcorner} \cdot \dots \cdot p_{k-1}^{\ulcorner \delta_{k-1} \urcorner}$

Проверка доказательства на корректность

Теорема

Следующая функция рекурсивна:

$$proof(f, x_1, x_2, \ldots, x_n, y, p) = \begin{cases} 1, & \text{если} \vdash \phi(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}, \overline{y}), \\ & p \text{ — гёделев номер вывода}, f = \ulcorner \phi \\ 0, & \text{иначе} \end{cases}$$

Идея доказательства.

1. Проверка доказательства вычислима.
2. Согласно тезису Чёрча, любая вычислимая функция вычислима с помощью рекурсивных функций.

□

Перебор доказательств

Лемма

Следующие функции рекурсивны:

1. *Функции* $plog_k(n) = \max\{p : n \vdots k^p\}$, $fst(x) = plog_2(x)$ *и* $snd(x) = plog_3(x)$.
2. *Числовые литералы:* $\overline{k} : \mathbb{N}_0 \to \mathbb{N}_0$, $\overline{k}(x) = k$.

Теорема

Если $f : \mathbb{N}_0^n \to \mathbb{N}_0$, *и* f *представима в Ф.А. формулой* φ, *то* f — *рекурсивна.*

Доказательство.

Пусть заданы $x_1, x_2, \ldots, x_n$. Ищем $\langle y, p\rangle$, что
$\text{proof}(\ulcorner\varphi\urcorner, x_1, x_2, \ldots, x_n, y, p) = 1$, напомним:
$y = f(x_1, x_2, \ldots, x_n)$, $p = \ulcorner\Pi\urcorner$, Π — доказательство
$\varphi(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}, \overline{y})$.

$f = S\langle \text{fst}, M\langle S\langle \text{proof}, \overline{\ulcorner\varphi\urcorner}, U^1_{n+1}, U^2_{n+1}, \ldots, U^n_{n+1}, S\langle \text{fst}, U^{n+1}_{n+1}\rangle, S\langle \text{snd}, U^n_{n+1}\rangle, S\langle \text{snd}, U^{n+1}_{n+1}\rangle\rangle\rangle\rangle$

Теоремы Гёделя о неполноте арифметики

Основные свойства исчислений: Ф.А.

	К.И.В.	И.И.В.	К.И.П.	Ф.А. + кл.
корректность	да	да	да (лекция 5)	да (сейчас)
непротиворечивость	да	да	да (лекция 6)	верим (т. Г
полнота	да	да	да (лекция 6)	нет (т. Гёде
разрешимость	да	да	нет (лекция 7)	нет (док-во

Классическая модель Ф.А.

А как определять «нестандартные» предикаты и функции (Q_1', $c(p,q)$ и т.п.)? Для простоты разрешим только нелогические функциональные и предикатные символы ($=$, $+$, $\cdot$, 0, $'$).

Определение

Классическая модель формальной арифметики: $D = \mathbb{N}_0$, оценки предикатных и функциональных символов — естественные.

Теорема

Формальная арифметика корректна

Доказательство.

Свойства аксиом $A1 \ldots A8$ очевидны.
Доказательство схемы аксиом индукции:

$$\psi(0) \,\&\, (\forall x.\psi(x) \to \psi(x')) \to \psi(x)$$

Индукция по структуре формулы ψ, затем математическая индукция по x. □

Схема аксиом индукции чуть подробнее

Индукция по структуре формулы ψ в

$$\psi(0)\ \&\ (\forall x.\psi(x) \to \psi(x')) \to \psi(x)$$

Для примера база:

$$\theta_0(0) = \theta_1(0)\&(\forall x.\theta_0(x) = \theta_1(x) \to \theta_0(x') = \theta_1(x')) \to \theta_0(x) = \theta_1(x)$$

Докажем индукцией по x.

1. $x := 0$. Тогда либо $[\![\theta_0(0) = \theta_1(0)]\!] = \text{Л}$, либо $[\![\theta_0(x) = \theta_1(x)]\!]^{x:=0} = \text{И}$
2. $x := s$. Тогда s раз применяем переход

$$[\![\theta_0(x) = \theta_1(x) \to \theta_0(x') = \theta_1(x')]\!]^{x:=\overline{0\ldots s}} = \text{И}$$

отсюда

$$[\![\theta_0(x') = \theta_1(x')]\!]^{x:=s} = [\![\theta_0(x) = \theta_1(x)]\!]^{x:=s+1} = \text{И}$$

Можно ли верить этому доказательству (доказываем индукцию через индукцию)?

Самоприменимость

Определение

Пусть ξ — формула с единственной свободной переменной x_1. Тогда: $\langle \ulcorner \xi \urcorner, p \rangle \in W_1$, если $\vdash \xi(\overline{\ulcorner \xi \urcorner})$ и p — номер доказательства.

Определение

Отношение W_1 рекурсивно, поэтому выражено в Ф.А. формулой ω_1 со свободными переменными x_1 и x_2, причём:

1. $\vdash \omega_1(\overline{\ulcorner \varphi \urcorner}, \overline{p})$, *если p — гёделев номер доказательства самоприменения φ;*
2. $\vdash \neg\omega_1(\overline{\ulcorner \varphi \urcorner}, \overline{p})$ *иначе.*

Определение

Определим формулу $\sigma(x_1) := \forall p.\neg\omega_1(x_1, p)$.

Первая теорема Гёделя о неполноте арифметики

Определение

Если для любой формулы $\phi(x)$ из $\vdash \phi(0), \vdash \phi(\overline{1}), \vdash \phi(\overline{2}), \ldots$ выполнено $\nvdash \exists x.\neg\phi(x)$, то теория омега-непротиворечива.

Теорема

Первая теорема Гёделя о неполноте арифметики

- *Если формальная арифметика непротиворечива, то $\nvdash \sigma(\overline{\ulcorner\sigma\urcorner})$.*
- *Если формальная арифметика ω-непротиворечива, то $\nvdash \neg\sigma(\overline{\ulcorner\sigma\urcorner})$.*

Доказательство теоремы Гёделя

Напомним: $\sigma(x_1) := \forall p.\neg\omega_1(x_1, p)$. $W_1(\ulcorner\xi\urcorner, p)$ — p есть доказательство самоприменения ξ.

Доказательство.

- Пусть $\vdash \sigma(\overline{\ulcorner\sigma\urcorner})$. Значит, p — номер доказательства. Тогда $\langle\ulcorner\sigma\urcorner, p\rangle \in W_1$. Тогда $\vdash \omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{p})$. Тогда $\vdash \exists p.\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$. То есть $\vdash \neg\forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$. То есть $\vdash \neg\sigma(\overline{\ulcorner\sigma\urcorner})$. Противоречие.
- Пусть $\vdash \neg\sigma(\overline{\ulcorner\sigma\urcorner})$. То есть $\vdash \exists p.\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$.
  - Но найдётся ли натуральное число p, что $\vdash \omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{p})$? Пусть нет. То есть $\vdash \neg\omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{0})$, $\vdash \neg\omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{1})$, ... По ω-непротиворечивости $\nvdash \exists p.\neg\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$.

  Значит, найдётся натуральное p, что $\vdash \omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{p})$. То есть, $\langle\ulcorner\sigma\urcorner, p\rangle \in W_1$. То есть, p — доказательство самоприменения W_1: $\vdash \sigma(\overline{\ulcorner\sigma\urcorner})$. Противоречие.

□

Почему теорема о неполноте?

Определение

Семантически полная теория — теория, в которой любая общезначимая формула доказуема.
Синтаксически полная теория — теория, в которой для каждой формулы α выполнено $\vdash \alpha$ или $\vdash \neg\alpha$.

Теорема

Формальная арифметика с классической моделью семантически неполна.

Доказательство.

Рассмотрим Ф.А. с классической моделью. Из теоремы Гёделя имеем $\nvdash \sigma(\overline{\ulcorner\sigma\urcorner})$. Рассмотрим $\sigma(\overline{\ulcorner\sigma\urcorner}) \equiv \forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$: нет числа p, что p — номер доказательства $\sigma(\overline{\ulcorner\sigma\urcorner})$. То есть, $[\![\forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}), p)]\!] =$ И. То есть, $\models \sigma(\overline{\ulcorner\sigma\urcorner})$. $\square$

Первая теорема Гёделя о неполноте в форме Россера

Определение

$\theta_1 \leq \theta_2 \equiv \exists p.p + \theta_1 = \theta_2 \qquad \theta_1 < \theta_2 \equiv \theta_1 \leq \theta_2 \,\&\, \neg\theta_1 = \theta_2$

Определение

Пусть $\langle \ulcorner \xi \urcorner, p\rangle \in W_2$, *если* $\vdash \neg\xi(\overline{\ulcorner \xi \urcorner})$. *Пусть* ω_2 *выражает* W_2 *в формальной арифметике.*

Теорема

Рассмотрим $\rho(x_1) = \forall p.\omega_1(x_1, p) \to \exists q.q \leq p \,\&\, \omega_2(x_1, q)$. *Тогда* $\nvdash \rho(\overline{\ulcorner \rho \urcorner})$ *и* $\nvdash \neg\rho(\overline{\ulcorner \rho \urcorner})$. $\rho(\overline{\ulcorner \rho \urcorner})$: *«Меня легче опровергнуть, чем доказать»*

Формальное доказательство

Неполнота варианта теории, изложенной выше, формально доказана на Coq, Russell O'Connor, 2005:

"My proof, excluding standard libraries and the library for Pocklington's criterion, consists of 46 source files, 7 036 lines of specifications, 37 906 lines of proof, and 1 267 747 total characters. The size of the gzipped tarball (gzip -9) of all the source files is 146 008 bytes, which is an estimate of the information content of my proof."

```
Theorem Incompleteness : forall T : System,
   Included Formula NN T ->
   RepresentsInSelf T ->
   DecidableSet Formula T ->
   exists f : Formula,
   Sentence f/\(SysPrf T f \/ SysPrf T (notH f) ->
Inconsistent LNN T).
```

Consis

Лемма

$\vdash 1 = 0$ *тогда и только тогда, когда* $\vdash \alpha$ *при любом* α.

Определение

Обозначим за $\psi(x, p)$ *формулу, выражающую в формальной арифметике рекурсивное отношение Proof:* $\langle \ulcorner \xi \urcorner, p \rangle \in Proof$, *если* p *— гёделев номер доказательства* ξ.
Обозначим $\pi(x) \equiv \exists p.\psi(x, p)$

Определение

Формулой Consis назовём формулу $\neg\pi(\overline{\ulcorner 1 = 0 \urcorner})$

Неформальный смысл: «формальная арифметика непротиворечива»

Вторая теорема Гёделя о неполноте арифметики

Теорема

Если Consis доказуем, то формальная арифметика противоречива.

Доказательство.

(неформально) Формулировка 1 теоремы Гёделя о неполноте арифметики: «если Ф.А. непротиворечива, то недоказуемо $\sigma(\overline{\ulcorner\sigma\urcorner})$». То есть, $\forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$. То есть, если Consis, то $\sigma(\overline{\ulcorner\sigma\urcorner})$. То есть, если Consis, то $\sigma(\overline{\ulcorner\sigma\urcorner})$, — и это можно доказать, то есть $\vdash$ Consis $\to \sigma(\overline{\ulcorner\sigma\urcorner})$. Однако если формальная арифметика непротиворечива, то $\nvdash \sigma(\overline{\ulcorner\sigma\urcorner})$. $\square$

Слишком много неформальности

Рассмотрим такой особый Consis′:

$$\pi'(x) := \exists p.\psi(x,p)\ \&\ \neg\psi(\overline{\ulcorner 1=0 \urcorner}, p)$$
$$\text{Consis}' := \pi'(\overline{\ulcorner 1=0 \urcorner})$$

Заметим:

1. Если ФА непротиворечива, то $[\![\pi'(x)]\!] = [\![\pi(x)]\!]$:
   - если $x \neq \ulcorner 1=0 \urcorner$ и $[\![\psi(x,p)]\!] = \text{И}$, то $[\![\psi(\overline{\ulcorner 1=0 \urcorner}, p)]\!] = \text{Л}$
   - если $x = \ulcorner 1=0 \urcorner$, то $\psi(\overline{\ulcorner 1=0 \urcorner}, p) = \text{Л}$ при любом p.
2. Но $\vdash \text{Consis}'$.

Условия выводимости Гильберта-Бернайса-Лёба

Определение

Будем говорить, что формула ψ, выражающая отношение Proof, формула π и формула Consis соответствуют условиям Гильберта-Бернайса-Лёба, если следующие условия выполнены для любой формулы α:

1. $\vdash \alpha$ *влечет* $\vdash \pi(\overline{\ulcorner \alpha \urcorner})$
2. $\vdash \pi(\overline{\ulcorner \alpha \urcorner}) \to \pi(\overline{\ulcorner \pi(\overline{\ulcorner \alpha \urcorner}) \urcorner})$
3. $\vdash \pi(\overline{\ulcorner \alpha \to \beta \urcorner}) \to \pi(\overline{\ulcorner \alpha \urcorner}) \to \pi(\overline{\ulcorner \beta \urcorner})$

Первая теорема Гёделя о неполноте ещё раз

Лемма

Лемма об автоссылках. Для любой формулы $\phi(x_1)$ можно построить такую замкнутую формулу α (не использующую неаксиоматических предикатных и функциональных символов), что $\vdash \phi(\overline{\ulcorner \alpha \urcorner}) \leftrightarrow \alpha$.

Теорема

Существует такая замкнутая формула γ, что если Ф.А. непротиворечива, то $\nvdash \gamma$, а если Ф.А. ω-непротиворечива, то и $\nvdash \neg\gamma$.

Доказательство.

Рассмотрим $\phi(x_1) \equiv \neg\pi(x_1)$. Тогда по лемме об автоссылках существует γ, что $\vdash \gamma \leftrightarrow \neg\pi(\overline{\ulcorner \gamma \urcorner})$.

- Предположим, что $\vdash \gamma$. Тогда $\vdash \gamma \rightarrow \neg\pi(\overline{\ulcorner \gamma \urcorner})$, то есть $\nvdash \gamma$
- Предположим, что $\vdash \neg\gamma$. Тогда $\vdash \pi(\overline{\ulcorner \gamma \urcorner})$, то есть $\vdash \exists p.\psi(\overline{\ulcorner \gamma \urcorner}, p)$. Тогда по ω-непротиворечивости найдётся p, что $\vdash \psi(\overline{\ulcorner \gamma \urcorner}, \overline{p})$, то есть $\vdash \gamma$.

Доказательство второй теоремы Гёделя

1. Пусть γ таково, что $\vdash \gamma \leftrightarrow \neg\pi(\overline{\ulcorner\gamma\urcorner})$.
2. Покажем $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner 1 = 0\urcorner})$.
   - 2.1 По условию 2, $\vdash \pi(\overline{\ulcorner\gamma\urcorner}) \to \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner})$. По теореме о дедукции $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner})$;
   - 2.2 Так как $\vdash \pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma$, то по условию 1 $\vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma\urcorner})$;
   - 2.3 По условию 3, $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner}) \to \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma\urcorner}) \to \pi(\overline{\ulcorner\neg\gamma\urcorner})$;
   - 2.4 Таким образом, $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\neg\gamma\urcorner})$;
   - 2.5 Однако $\vdash \gamma \to \neg\gamma \to 1 = 0$. Условие 3 (применить два раза) даст $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner 1 = 0\urcorner})$.
3. $\neg\pi(\overline{\ulcorner 1 = 0\urcorner}) \to \neg\pi(\overline{\ulcorner\gamma\urcorner})$ (т. о дедукции, контрапозиция).
4. $\vdash \neg\pi(\overline{\ulcorner 1 = 0\urcorner}) \to \gamma$ (определение γ).

Расширение на другие теории

Определение

Теория $\mathcal{S}$ — расширение теории $\mathcal{T}$, если из $\vdash_{\mathcal{T}} \alpha$ следует $\vdash_{\mathcal{S}} \alpha$

Определение

Теория $\mathcal{S}$ — рекурсивно-аксиоматизируемая, если найдётся теория $\mathcal{S}'$ с тем же языком, что:

1. $\vdash_{\mathcal{S}} \alpha$ *тогда и только тогда, когда* $\vdash_{\mathcal{S}'} \alpha$;
2. *Множество аксиом теории $\mathcal{S}'$ рекурсивно.*

Теорема

Если $\mathcal{S}$ — непротиворечивое рекурсивно-аксиоматизируемое расширение формальной арифметики, то в ней можно доказать аналоги теорем Гёделя о неполноте арифметики.

Сужение: система Робинсона

Определение

Теория первого порядка, использующая нелогические функциональные символы 0, $(+)$ *и* $(\cdot)$, *нелогический предикатный символ* $(=)$ *и следующие нелогические аксиомы, называется системой Робинсона.*

$a = a$

$a = b \to b = c \to a = c$

$a' = b' \to a = b$

$a = b \to a + c = b + c \,\&\, c + a = c + b$

$\neg a = 0 \to \exists b.a = b'$

$a + b' = (a + b)'$

$a \cdot b' = a \cdot b + a$

$a = b \to b = a$

$a = b \to a' = b'$

$\neg 0 = a'$

$a = b \to a \cdot c = b \cdot c \,\&\, c \cdot a =$

$a + 0 = a$

$a \cdot 0 = 0$

Система Робинсона неполна: аксиомы — в точности утверждения, необходимые для доказательства теорем Гёделя. Система Робинсона не имеет схем аксиом.

Арифметика Пресбургера

Определение

Теория первого порядка, использующая нелогические функциональные символы 0, 1, $(+)$, *нелогический предикатный символ* $(=)$ *и следующие нелогические аксиомы, называется арифметикой Пресбургера.*

$$\neg(0 = x + 1)$$
$$x + 1 = y + 1 \to x = y$$
$$x + 0 = x$$
$$x + (y + 1) = (x + y) + 1$$
$$(\varphi(0) \,\&\, \forall x.\varphi(x) \to \varphi(x + 1)) \to \forall y.\varphi(y)$$

Теорема

Арифметика Пресбургера разрешима и синтаксически и семантически полна.

Невыразимость доказуемости

Определение

$Th_{\mathcal{S}} = \{\ulcorner\alpha\urcorner \mid \vdash_{\mathcal{S}} \alpha\}$; $Tr_{\mathcal{S}} = \{\ulcorner\alpha\urcorner \mid [\![\alpha]\!]_{\mathcal{S}} = И\}$

Лемма

Пусть $D(\ulcorner\alpha\urcorner) = \ulcorner\alpha(\overline{\ulcorner\alpha\urcorner})\urcorner$ *для любой формулы* $\alpha(x)$. *Тогда* D *представима в формальной арифметике.*

Теорема

Если расширение Ф.А. $\mathcal{S}$ *непротиворечиво и* D *представима в нём, то* $Th_{\mathcal{S}}$ *невыразимо в* $\mathcal{S}$

Доказательство.

Пусть $\delta(a, p)$ представляет D, и пусть $\sigma(x)$ выражает множество $\mathsf{Th}_{\mathcal{S}}$ (рассматриваемое как одноместное отношение). Пусть $\alpha(x) := \forall p.\delta(x, p) \to \neg\sigma(p)$. Верно ли, что $\ulcorner\alpha\urcorner \in \mathsf{Th}$? $\square$

Неразрешимость формальной арифметики

Теорема

Если формальная арифметика непротиворечива, то формальная арифметика неразрешима

Доказательство.

Пусть формальная арифметика разрешима. Значит, есть рекурсивная функция $f(x)$: $f(x) = 1$ тогда и только тогда, когда $x \in \mathrm{Th}_{\Phi.\mathrm{A}.}$. То есть, $\mathrm{Th}_{\Phi.\mathrm{A}.}$ выразимо в формальной арифметике.
По теореме о невыразимости доказуемости, $\mathrm{Th}_{\Phi.\mathrm{A}.}$ невыразимо в формальной арифметике. Противоречие. $\square$

Теорема Тарского

Теорема (Тарского о невыразимости истины)

Не существует формулы $\varphi(x)$, что $[\![\varphi(x)]\!] = И$ (в стандартной интерпретации) тогда и только тогда, когда $x \in Tr_{ФА}$.

Доказательство.

Пусть теория $\mathcal{S}$ — формальная арифметика + аксиомы: все истинные в стандартной интерпретации формулы. Очевидно, что $\mathrm{Th}_{\mathcal{S}} = \mathrm{Tr}_{\mathcal{S}} = \mathrm{Tr}_{\Phi\mathrm{A}}$. То есть $\mathrm{Tr}_{\Phi\mathrm{A}}$ невыразимо в $\mathcal{S}$.
Пусть φ таково, что $[\![\varphi(x)]\!] = И$ при $x \in \mathrm{Tr}$. Тогда $\vdash \varphi(x)$, если $x \in \mathrm{Tr}$ и $\vdash \neg\varphi(x)$, если $x \notin \mathrm{Tr}$.
Тогда Tr выразимо в $\mathcal{S}$. Противоречие. □

Однако, если взять $D = \mathbb{R}$, истина становится выразима (алгоритм Тарского).

Лямбда-исчисление

Лямбда-исчисление, синтаксис

$$\Lambda ::= (\lambda x.\Lambda)|(\Lambda\ \Lambda)|x$$

Мета-язык:

- Мета-переменные:
  - $A \ldots Z$ — мета-переменные для термов.
  - x, y, z — мета-переменные для переменных.
- Правила расстановки скобок аналогичны правилам для кванторов:
  - Лямбда-выражение ест всё до конца строки
  - Аппликация левоассоциативна

Пример

- $a\ b\ c\ (\lambda d.e\ f\ \lambda g.h)\ i \equiv \Big(\big(((a\ b)\ c)\ \big(\lambda d.((e\ f)\ (\lambda g.h))\big)\big)\ i\Big)$
- $0 := \lambda f.\lambda x.x; \quad (+1) := \lambda n.\lambda f.\lambda x.n\ f\ (f\ x); \quad (+2) := \lambda x.(+1)\ ((+1)\ x)$

Альфа-эквивалентность

$$FV(A) = \begin{cases} \{x\}, & A \equiv x \\ FV(P) \cup FV(Q), & A \equiv P\ Q \\ FV(P) \setminus \{x\}, & A \equiv \lambda x.P \end{cases}$$

Примеры:

- $M := \lambda b.\lambda c.a\ c\ (b\ c)$; $FV(M) = \{a\}$
- $N := x\ (\lambda x.(x\ (\lambda y.x)))$; $FV(N) = \{x\}$

Определение

$A =_\alpha B$, если и только если выполнено одно из трёх:

1. $A \equiv x$, $B \equiv y$, $x \equiv y$;
2. $A \equiv P_a Q_a$, $B \equiv P_b Q_b$ *и* $P_a =_\alpha P_b$, $Q_a =_\alpha Q_b$;
3. $A \equiv (\lambda x.P)$, $B \equiv (\lambda y.Q)$, $P[x := t] =_\alpha Q[y := t]$, *где* t *не входит в* A *и* B.

Определение

$L = \Lambda / =_\alpha$

Альфа-эквивалентность, пример

1. $A \equiv x$, $B \equiv y$, $x \equiv y$;
2. $A \equiv P_a Q_a$, $B \equiv P_b Q_b$ и $P_a =_\alpha P_b$, $Q_a =_\alpha Q_b$;
3. $A \equiv (\lambda x.P)$, $B \equiv (\lambda y.Q)$, $P[x := t] =_\alpha Q[y := t]$, где t не входит в A и B.

Лемма

$$\lambda a.\lambda b.a\ b =_\alpha \lambda b.\lambda a.b\ a$$

Доказательство.

$$\begin{array}{rcll} t & =_\alpha & t & \text{Правило 1} \\ s & =_\alpha & s & \text{Правило 1} \\ t\ s & =_\alpha & t\ s & \text{Правило 2} \\ \lambda b.(t\ b) & =_\alpha & \lambda a.(t\ a) & \text{Правило 3} \\ \lambda a.\lambda b.(a\ b) & =_\alpha & \lambda b.\lambda a.(b\ a) & \text{Правило 3} \end{array}$$

Бета-редукция

Интуиция: вызов функции.

λ-выражение	Python
$\lambda f.\lambda x.f\ x$	`def one(f,x): return f(x)`
$(\lambda x.x\ x)\ (\lambda x.x\ x)$	`(lambda x: x x) (lambda x: x x)`
	`def omega(x): return x(x); omega(omega)`

Определение

Терм вида $(\lambda x.P)\ Q$ *— бета-редекс.*

Определение

$A \to_\beta B$, *если:*

1. $A \equiv (\lambda x.P)\ Q$, $B \equiv P\ [x := Q]$, *при условии свободы для подстановки;*
2. $A \equiv (P\ Q)$, $B \equiv (P'\ Q')$, *при этом* $P \to_\beta P'$ *и* $Q = Q'$, *либо* $P = P'$ *и* $Q \to_\beta Q'$;
3. $A \equiv (\lambda x.P)$, $B \equiv (\lambda x.P')$, *и* $P \to_\beta P'$.

Бета-редукция, пример

Пример

$(\lambda x.x\ x)\ (\lambda n.n) \to_\beta (\lambda n.n)\ (\lambda n.n) \to_\beta \lambda n.n$

Пример

$(\lambda x.x\ x)\ (\lambda x.x\ x) \to_\beta (\lambda x.x\ x)\ (\lambda x.x\ x)$

Нормальная форма

Определение

Лямбда-терм N находится в нормальной форме, если нет Q: $N \to_\beta Q$.

Пример

В нормальной форме:
$\lambda f.\lambda x.x\ (f\ (f\ \lambda g.x))$

Пример

Не в нормальной форме (редексы подчёркнуты):
$\lambda f.\lambda x.\underline{(\lambda g.x)\ (f\ (f\ x))}$
$(\underline{(\lambda x.x)\ (\lambda x.x)})\ (\underline{(\lambda x.x)\ (\lambda x.x)})$

Определение

$(\twoheadrightarrow_\beta)$ *— транзитивное и рефлексивное замыкание* $(\to_\beta)$.

Булевские значения

$T := \lambda x.\lambda y.x$ $F := \lambda x.\lambda y.y$

Тогда: $Or := \lambda a.\lambda b.a\ T\ b$:

$Or\ F\ T = \underline{((\lambda a.\lambda b.a\ T\ b)\ F)}\ T \to_\beta (\lambda b.F\ T\ b)\ T \to_\beta F\ T\ T =$

$= (\lambda x.\lambda y.y)\ T\ T \to_\beta (\lambda y.y)\ T \to_\beta T$

Чёрчевские нумералы

$$f^{(n)}(x) = \begin{cases} x, & n = 0 \\ f(f^{(n-1)}(x)), & n > 0 \end{cases}$$

Определение

Чёрчевский нумерал $\overline{n} = \lambda f.\lambda x.f^{(n)}(x)$

Пример

$\overline{3} = \lambda f.\lambda x.f(f(f(x)))$

Инкремент: $Inc = \lambda n.\lambda f.\lambda x.n\ f\ (f\ x)$

$$(\lambda n.\lambda f.\lambda x.n\ f\ (f\ x))\ \overline{0} = (\lambda n.\lambda f.\lambda x.n\ f\ (f\ x))\ (\lambda f'.\lambda x'.x') \to_\beta$$
$$\ldots \lambda f.\lambda x.(\lambda f'.\lambda x'.x')\ f\ (f\ x) \to_\beta$$
$$\ldots \lambda f.\lambda x.(\lambda x'.x')\ (f\ x) \to_\beta$$
$$\ldots \lambda f.\lambda x.f\ x = \overline{1}$$

Декремент: $Dec = \lambda n.\lambda f.\lambda x.n\ (\lambda g.\lambda h.h\ (g\ f))\ (\lambda u.x)\ (\lambda u.u)$

Упорядоченная пара и алгебраический тип

Определение

$Pair(a, b) := \lambda s.s\ a\ b$
$Fst := \lambda p.p\ T$
$Snd := \lambda p.p\ F$

Пример

$Fst(Pair(a, b)) = (\lambda p.p\ T)\ \lambda s.s\ a\ b \twoheadrightarrow_\beta (\lambda s.s\ a\ b)\ T \twoheadrightarrow_\beta a$

Определение

$InL\ L := \lambda p.\lambda q.p\ L$
$InR\ R := \lambda p.\lambda q.q\ R$
$Case\ t\ f\ g := t\ f\ g$

Теорема Чёрча-Россера

Теорема (Чёрча-Россера)

Для любых термов N, P, Q, если $N \twoheadrightarrow_\beta P$, $N \twoheadrightarrow_\beta Q$, и $P \neq Q$, то найдётся T: $P \twoheadrightarrow_\beta T$ и $Q \twoheadrightarrow_\beta T$.

Теорема

Если у терма N существует нормальная форма, то она единственна

Доказательство.

Пусть не так и $N \twoheadrightarrow_\beta P$ вместе с $N \twoheadrightarrow_\beta Q$, $P \neq Q$. Тогда по теореме Чёрча-Россера существует T: $P \twoheadrightarrow_\beta T$ и $Q \twoheadrightarrow_\beta T$, причём $T \neq P$ или $T \neq Q$ в силу транзитивности $(\twoheadrightarrow_\beta)$ $\square$

Бета-эквивалентность, неподвижная точка

Пример

$\Omega = (\lambda x.x\ x)\ (\lambda x.x\ x)$ *не имеет нормальной формы:* $\Omega \to_\beta \Omega$

Определение

$(=_\beta)$ — *транзитивное, рефлексивное и симметричное замыкание* $(\to_\beta)$.

Теорема

Для любого терма N *найдётся такой терм* R, *что* $R =_\beta N\ R$.

Доказательство.

Пусть $Y = \lambda f.(\lambda x.f\ (x\ x))\ (\lambda x.f\ (x\ x))$. Тогда $R := Y\ N$:

$$Y\ N =_\beta (\lambda x.N\ (x\ x))\ (\lambda x.N\ (x\ x)) =_\beta N\ ((\lambda x.N\ (x\ x))\ (\lambda x.N\ (x\ x)))$$

□

Интуиционистское И.В. (натуральный, естественный вывод)

- Формулы языка (секвенции) имеют вид: $\Gamma \vdash \alpha$. Правила вывода:
- Аксиома: $\dfrac{\text{посылка 1} \qquad \text{посылка 2} \qquad \dots}{\text{заключение}}$ (аннотация)

  $\dfrac{}{\Gamma, \alpha \vdash \alpha}$ (акс.)
- Правила введения связок:

  $\dfrac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \to \beta} \qquad \dfrac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta}, \dfrac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta} \qquad \dfrac{\Gamma \vdash \alpha \qquad \Gamma \vdash \beta}{\Gamma \vdash \alpha \,\&\, \beta}$
- Правила удаления связок:

  $\dfrac{\Gamma \vdash \alpha \quad \Gamma \vdash \alpha \to \beta}{\Gamma \vdash \beta} \qquad \dfrac{\Gamma \vdash \alpha \to \gamma \quad \Gamma \vdash \beta \to \gamma \quad \Gamma \vdash \alpha \vee \beta}{\Gamma \vdash \gamma}$

  $\dfrac{\Gamma \vdash \alpha \,\&\, \beta}{\Gamma \vdash \alpha} \qquad \dfrac{\Gamma \vdash \alpha \,\&\, \beta}{\Gamma \vdash \beta} \qquad \dfrac{\Gamma \vdash \bot}{\Gamma \vdash \alpha}$
- Пример доказательства:

$$\dfrac{\dfrac{\dfrac{}{A \,\&\, B \vdash A \,\&\, B}\ (\text{акс.})}{A \,\&\, B \vdash B}\ (\text{удал\&}) \qquad \dfrac{\dfrac{}{A \,\&\, B \vdash A \,\&\, B}\ (\text{акс.})}{A \,\&\, B \vdash A}\ (\text{удал\&})}{A \,\&\, B \vdash B \,\&\, A}\ (\text{введ\&})$$

Эквивалентность натурального и гильбертовского выводов

Определение

$$|\alpha|_{\bot} = \begin{cases} X, & \alpha \equiv X \\ |\sigma|_{\bot} \star |\tau|_{\bot}, & \alpha \equiv \sigma \star \tau \\ |\sigma|_{\bot} \to \bot, & \alpha \equiv \neg\sigma \end{cases} \qquad |\alpha|_{\neg} = \begin{cases} X, & \alpha \equiv X \\ |\sigma|_{\neg} \star |\tau|_{\neg}, & \alpha \equiv \sigma \star \\ A \,\&\, \neg A, & \alpha \equiv \bot \end{cases}$$

Теорема

1. $\Gamma \vdash_n \alpha$ *тогда и только тогда, когда* $|\Gamma|_{\neg} \vdash_h |\alpha|_{\neg}$.
2. $\Gamma \vdash_h \alpha$ *тогда и только тогда, когда* $|\Gamma|_{\bot} \vdash_n |\alpha|_{\bot}$.

Доказательство.

Индукция по структуре $\square$

Просто-типизированное лямбда-исчисление

Определение

Импликационный фрагмент интуиционистской логики:

$$\frac{}{\Gamma, \varphi \vdash_{\to} \varphi} \qquad \frac{\Gamma, \varphi \vdash_{\to} \psi}{\Gamma \vdash_{\to} \varphi \to \psi} \qquad \frac{\Gamma \vdash_{\to} \varphi \qquad \Gamma \vdash_{\to} \varphi \to \psi}{\Gamma \vdash_{\to} \psi}$$

Теорема

Если $\Gamma \vdash \alpha$, *то* $\Gamma \vdash_{\to} \alpha$.

Доказательство.

Определим модель Крипке:

- миры — замкнутые множества формул: $\alpha \in \Gamma$ т.и.т.т. $\Gamma \vdash_{\to} \alpha$,
- порядок — $(\subseteq)$,
- $\Gamma \Vdash X$ т.и.т.т. $X \in \Gamma$.

Из корректности моделей Крипке следует, что что если $\Gamma \vdash \alpha$, то $\Gamma \Vdash \alpha$. Требуемое следует из того, что $\Gamma \Vdash \alpha$ влечёт

$\Gamma \Vdash \alpha$ т.и.т.т. $\Gamma \vdash_{\to} \alpha$

Индукция по структуре α.

- $\alpha \equiv X$. Утверждение следует из определения;
- $\alpha \equiv \varphi \to \psi$.
  - Пусть $\Gamma \Vdash \varphi \to \psi$. То есть, $\Gamma \subseteq \Delta$ и $\Delta \Vdash \varphi$ влечёт $\Delta \Vdash \psi$. Возьмём Δ как замыкание $\Gamma \cup \{\varphi\}$. Значит, $\Gamma \vdash_{\to} \varphi$ и, по индукционному предположению, $\Delta \Vdash \varphi$. Тогда $\Delta \Vdash \psi$. По индукционному предположению, $\Delta \vdash_{\to} \psi$. То есть, $\Gamma, \varphi \vdash_{\to} \psi$, откуда

$$\frac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \to \beta}$$

  - Пусть $\Gamma \vdash_{\to} \varphi \to \psi$. Проверим $\Gamma \Vdash \varphi \to \psi$. Пусть $\Gamma \subseteq \Delta$ и пусть $\Delta \Vdash \varphi$.
    По индукционному предположению, $\varphi \in \Delta$. То есть, $\Delta \vdash_{\to} \varphi$ и $\Delta \vdash_{\to} \varphi \to \psi$. Тогда

$$\frac{\Delta \vdash_{\to} \varphi \quad \Delta \vdash_{\to} \varphi \to \psi}{\Delta \vdash_{\to} \psi}$$

    По индукционному предположению, $\Delta \Vdash \psi$, отчего $\Gamma \Vdash \varphi \to \psi$.

Просто-типизированное лямбда-исчисление

Определение

Просто-типизированное лямбда-исчисление (по Карри). Типы: $\tau ::= \alpha | (\tau \to \tau)$. *Язык:* $\Gamma \vdash A : \varphi$

$$\frac{}{\Gamma, x : \varphi \vdash x : \varphi}\ x \notin \Gamma \qquad \frac{\Gamma, x : \varphi \vdash A : \psi}{\Gamma \vdash \lambda x.A : \varphi \to \psi}\ x \notin \Gamma \qquad \frac{\Gamma \vdash A : \varphi \qquad \Gamma \vdash}{\Gamma \vdash BA :}$$

Пример: тип чёрчевских нумералов

Пусть $\Gamma = f : \alpha \to \alpha, x : \alpha$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash x : \alpha}\,Ax \qquad \dfrac{}{\Gamma \vdash f : \alpha \to \alpha}\,Ax}{\Gamma \vdash f\ x : \alpha}\,App \qquad \dfrac{}{\Gamma \vdash f : \alpha \to \alpha}\,Ax}{\{f : \alpha \to \alpha, x : \alpha\}\ \Gamma \vdash f\ (f\ x) : \alpha}\,App}{f : \alpha \to \alpha \vdash \lambda x.f\ (f\ x) : (\alpha \to \alpha)}\,\lambda}{\vdash \lambda f.\lambda x.f\ (f\ x) : (\alpha \to \alpha) \to (\alpha \to \alpha)}\,\lambda$$

Изоморфизм Карри-Ховарда

λ-исчисление	исчисление высказываний
Выражение	доказательство
Тип выражения	высказывание
Тип функции	импликация
Упорядоченная пара	Конъюнкция
Алгебраический тип	Дизъюнкция
Необитаемый тип	Ложь

Изоморфизм Карри-Ховарда: отрицание

Определение

Ложь ($\bot$) — *необитаемый тип;*

$\mathit{failwith/raise/throw} : \alpha \to \bot$; $\neg\varphi \equiv \varphi \to \bot$

Например, контрапозиция: $(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Phi \vdash a : \alpha}\,Ax \quad \dfrac{}{\Phi \vdash f : \alpha \to \beta}\,Ax}{\Phi \vdash f\ a : \beta}\,App \quad \dfrac{}{\Phi \vdash n : \beta \to \bot}\,Ax}{f : \alpha \to \beta, n : \beta \to \bot, a : \alpha \vdash n\ (f\ a) : \bot}\,App}{f : \alpha \to \beta, n : \beta \to \bot \vdash \lambda a^{\alpha}.n\ (f\ a) : \neg\alpha}\,\lambda}{f : \alpha \to \beta \vdash \lambda n^{\beta\to\bot}.\lambda a^{\alpha}.n\ (f\ a) : \neg\beta \to \neg\alpha}\,\lambda}{\lambda f^{\alpha\to\beta}.\lambda n^{\beta\to\bot}.\lambda a^{\alpha}.n\ (f\ a) : (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)}\,\lambda$$

Снятие двойного отрицания: $((\alpha \to \bot) \to \bot) \to \alpha$, то есть $\lambda f^{(\alpha\to\bot)\to\bot}.? : \alpha$.

f угадывает, что передать $x : \alpha \to \bot$. Тогда надо по f угадать, что передать x.

Исчисление по Чёрчу и по Карри

Определение

Просто-типизированное лямбда-исчисление по Карри.

$$\frac{}{\Gamma, x:\varphi \vdash x:\varphi}\ x \notin \Gamma \qquad \frac{\Gamma, x:\varphi \vdash A:\psi}{\Gamma \vdash \lambda x.A:\varphi \to \psi}\ x \notin \Gamma \qquad \frac{\Gamma \vdash A:\varphi \qquad \Gamma \vdash}{\Gamma \vdash BA:}$$

Просто-типизированное лямбда-исчисление по Чёрчу.

$$\frac{}{\Gamma, x:\varphi \vdash x:\varphi}\ x \notin \Gamma \qquad \frac{\Gamma, x:\varphi \vdash A:\psi}{\Gamma \vdash \lambda x^{\varphi}.A:\varphi \to \psi}\ x \notin \Gamma \qquad \frac{\Gamma \vdash A:\varphi \qquad \Gamma \vdash}{\Gamma \vdash BA}$$

Пример

По Карри	*По Чёрчу*
$\lambda f.\lambda x.f\ (f\ x) : (\alpha \to \alpha) \to (\alpha \to \alpha)$	$\lambda f^{\alpha\to\alpha}.\lambda x^{\alpha}.f\ (f\ x) : (\alpha \to \alpha) \to$
$\lambda f.\lambda x.f\ (f\ x) : (\beta \to \beta) \to (\beta \to \beta)$	$\lambda f^{\beta\to\beta}.\lambda x^{\beta}.f\ (f\ x) : (\beta \to \beta) \to$

Комбинаторы S,K

Определение

Комбинатор — лямбда-терм без свободных переменных

Определение

$S := \lambda x.\lambda y.\lambda z.x\ z\ (y\ z)$, $K := \lambda x.\lambda y.x$, $I := \lambda x.x$

Теорема

Пусть N — некоторый замкнутый лямбда-терм. Тогда найдётся выражение C, состоящее из комбинаторов S,K, что $N =_\beta C$

Пример

$K := \lambda x^{\alpha}.\lambda y^{\beta}.x$ $\quad \alpha \to \beta \to \alpha$

$S := \lambda x^{\alpha\to\beta\to\gamma}.\lambda y^{\alpha\to\beta}.\lambda z^{\alpha}.x\ z\ (y\ z)$ $\quad (\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha$

$$I =_\beta S\ K\ K$$

Дальнейшее развитие: изоморфизм Карри-Ховарда и вокруг него

Исчисление второго порядка

- Напомним о порядках:

Порядок	Объекты	Пример
0 (И.В.)	Атомарные	P
1 (И.П. 1)	Множества	$\{x \mid P(x)\}$
2 (И.П. 2)	Множества множеств	$\{P \mid \forall t.t > 0 \to P(t)\}$

- Можно заменить схемы аксиом на аксиомы:
  $\forall a.\forall b.a \to b \to a$
- Острый угол: импредикативность (формулы могут говорить о себе). Что такое «предикат»? Произвольное выражение, а подстановка — буквальная замена текста? Тогда каково $[\![p(p)]\!]$ при $p(x) = x(x) \to \bot$?
  Нужна точная формализация.
- Самый простой вариант: переменные второго порядка — только булевские пропозициональные переменные.

$$[\![\forall p.Q]\!] = \begin{cases} \text{И}, & [\![Q]\!]^{p:=\text{И}} = [\![Q]\!]^{p:=\text{Л}} = \text{И} \\ \text{Л}, & \text{иначе} \end{cases}$$

Изоморфизм Карри-Ховарда для логики второго порядка

Типы и значения, зависящие от типов.

- Что такое $T : \forall x.x \to x$?
  `template <class x> class T { x f (x); }`
- Что такое $T : \exists x.\tau(x)$?
  Абстрактный тип данных: `interface T {`τ`}; f(T x)`

Зависимые типы

- Рассмотрим код
  `int n; cin >> n; int arr[n];`
  Каков тип `arr`?
- `sizeof(arr)` $= n \cdot$ `sizeof(int)`
- $arr = \Pi n^{\texttt{int}}.\texttt{int}[n]$
- Аналогично, `printf(const char*, ...)` — капитуляция.
- Есть языки, где тип выписывается (например, Идрис).

Прямолинейное: доказательства в коде

- `Div2: (l: int) -> (even l) -> int`
- `even l` — что это?
- $$even(x) ::= \begin{cases} EZ, & x = 0 \\ EP(even(y)), & x = y'' \end{cases}$$
- `Div2 10 (EP (EP (EP (EP (EP EZ)))))`
- А если `Div2 p`? В общем случае сложно.
  `Plus2: (l: int) -> (p: even l) -> (l+2, even (l+2)) = (l+2, EP p)`

Интереснее: доказательства утверждений

Натуральные числа: $\texttt{Nat} ::= 0 | \texttt{suc Nat}$,

$$a + b = \begin{cases} a, & b = 0 \\ \texttt{suc } (a + c), & b = \texttt{suc } c \end{cases}$$

```
func pmap A B :
(f : A -> B) {a a' : A} (p : a = a') : f a = f a' =>
...

func +-comm (n m : Nat) : n + m = m + n
| 0, 0 => idp
| suc n, 0 => pmap suc (+-comm n 0)
| 0, suc m => pmap suc (+-comm 0 m)
| suc n, suc m => pmap suc (+-comm (suc n) m *>
pmap suc (inv (+-comm n m)) *> +-comm n (suc m))
```

Что ещё

- Гомотопическая теория типов...
- Метод резолюций и рядом — Prolog, SMT-солверы,...
- Можно пытаться совмещать (F*, ...)

Теория множеств

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».
2. Неограниченный принцип абстракции $\{x \mid P(x)\}$
3. Парадокс Бурали-Форте (1895, Кантор). Парадокс Рассела: $X := \{x \mid x \notin x\}$; $X \in X$?
4. Вариант решения парадокса: а, может, запретить все «опасные» ситуации?
5. Аксиоматика Цермело — 1908 год, оставим только то, что используют математики.
6. Что такое множество? Неформально мы понимаем, формально:

Определение

Теория множеств — теория первого порядка, с дополнительным нелогическим двухместным функциональным символом $\in$, и следующими дополнительными нелогическими аксиомами и схемами аксиом

Аксиоматика ZF, равенство

Определение

Равенство «по Лейбницу»: объекты равны, если неразличимы.

Если нечто ходит как утка, выглядит как утка и крякает как утка, то это утка.

Определение

Принцип объёмности: объекты равны, если состоят из одинаковых частей

Определение

$A \subseteq B \equiv \forall x.x \in A \to x \in B$
$A = B \equiv A \subseteq B \,\&\, B \subseteq A$

Определение

Аксиома равенства: равные множества содержатся в одних и тех же множествах. $\forall x.\forall y.\forall z.x = y \,\&\, x \in z \to y \in z.$

Аксиоматика ZF, конструктивные аксиомы

Определение

Аксиома пустого. Существует пустое множество $\varnothing$.

$$\exists s.\forall t.\neg t \in s$$

Определение

Аксиома пары. Существует $\{a, b\}$. *Каковы бы ни были два множества* a *и* b, *существует множество, состоящее в точности из них.*

$$\forall a.\forall b.\exists s.a \in s \,\&\, b \in s \,\&\, \forall c.c \in s \to c = a \vee c = b$$

Аксиоматика ZF, конструктивные аксиомы 2

Определение

Аксиома объединения: существует $\cup x$. Для любого непустого множества x найдется такое множество, состоящее в точности из тех элементов, из которых состоят элементы x.

$$\forall x.(\exists y.y \in x) \to \exists p.\forall y.y \in p \leftrightarrow \exists s.y \in s \,\&\, s \in x$$

Определение

Аксиома степени: существует $\mathcal{P}(x)$. Каково бы ни было множество x, существует множество, содержащее в точности все возможные подмножества множества x.

$$\forall x.\exists p.\forall y.y \in p \leftrightarrow y \subseteq x$$

Аксиоматика ZF. Схема аксиом выделения

Определение

Схема аксиом выделения: существует $\{t \in x \mid \varphi(t)\}$. *Для любого множества* x *и любой формулы от одного аргумента* $\varphi(y)$ *(*b *не входит свободно в* φ*), найдется* b*, в которое входят те и только те элементы из множества* x*, что* $\varphi(y)$ *истинно.*

$$\forall x.\exists b.\forall y.y \in b \leftrightarrow (y \in x \,\&\, \varphi(y))$$

Немного теорем

Теорема

Для любого множества X существует множество $\{X\}$, содержащее в точности X.

Доказательство.

Воспользуемся аксиомой пары: $\{X, X\}$ □

Теорема

Пустое множество единственно.

Доказательство.

Пусть $\forall p.\neg p \in s$ и $\forall p.\neg p \in t$. Тогда $s \subseteq t$ и $t \subseteq s$. □

Теорема

Для двух множеств s и t существует множество, являющееся их пересечением.

Доказательство.

$s \cap t = \{x \in s \mid x \in t\}$ □

Упорядоченная пара

Определение

Упорядоченная пара. Упорядоченной парой двух множеств a и b назовём $\{\{a\}, \{a, b\}\}$, или $\langle a, b\rangle$

Теорема

Упорядоченную пару можно построить для любых множеств.

Доказательство.

Применить аксиому пары, теорему о существовании $\{X\}$, аксиому пары. □

Теорема

$\langle a, b\rangle = \langle c, d\rangle$ *тогда и только тогда, когда* $a = c$ *и* $b = d$.

Аксиома бесконечности

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует
$N : \varnothing \in N \,\&\, \forall x.x \in N \to x' \in N$

В N есть всевозможные множества вида $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, ...

(неформально) $\omega = \{\varnothing, \varnothing', \varnothing'', \dots\}$. Тогда
$N_1 = \omega \cup \{\omega, \omega', \omega'', \dots\}$ подходит.

Полный порядок (вполне упорядоченные множества)

1. Частичный: рефлексивность ($a \preceq a$), антисимметричность ($a \preceq b \to b \preceq a \to a = b$), транзитивность ($a \preceq b \to b \preceq c \to a \preceq c$).
2. Линейный: частичный + $\forall a. \forall b. a \preceq b \vee b \preceq a$.
3. Полный: линейный + в любом непустом подмножестве есть наименьший элемент.

Пример

$\mathbb{Z}$ не вполне упорядочено: в $\mathbb{Z}$ нет наименьшего.

Пример

Отрезок $[0, 1]$ не вполне упорядочен: $(0, 1)$ не имеет наименьшего.

Пример

$\mathbb{N}$ вполне упорядочено.

Ординалы (порядковые числа)

Определение

Транзитивное множество X: $\forall x.\forall y.x \in y \,\&\, y \in X \to x \in X$.

Определение

Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ транзитивное множество.

Пример

Ординалы: $\varnothing$, $\varnothing'$, $\varnothing''$, $\ldots$

Определение

Предельный ординал: такой x, что $x \neq \varnothing$ и нет $y : y' = x$

Определение

Ординал x конечный, если он меньше любого предельного.

Теорема

Если x, y — ординалы, то $x = y$, или $x \in y$, или $y \in x$.

Предельные ординалы, ω

Определение

ω — *наименьший предельный ординал.*

Теорема

ω *существует.*

Доказательство.

Пусть $\omega = \{x \in N \mid x \text{ конечен}\}$. Пусть θ таков, что $\theta \in \omega$. Тогда θ конечен. Пусть θ таков, что $\theta' = \omega$. Тогда $\theta \in \omega$. $\square$

Пример

ω' — *тоже ординал.*

Операции над ординалами

Определение

$\sup x$ — *наименьший ординал, содержащий* x*:* $x \subseteq \sup x$.

Пример

$\sup\{\varnothing', \varnothing'', \varnothing''''\} = \{\varnothing, \varnothing', \varnothing'', \varnothing''', \varnothing''''\} = \varnothing'''''$

$$a + b \equiv \begin{cases} a, & b \equiv \varnothing \\ (a + c)', & b \equiv c' \\ \sup\{a + c \mid c \prec b\}, & b \text{ — предельный ординал} \end{cases}$$

Пример

$\omega + 1 = \omega \cup \{\omega\}$; $1 + \omega = \sup\{1 + \varnothing, 1 + 1, 1 + 2, \dots\} = \omega$

Ещё операции над ординалами

$$a \cdot b \equiv \begin{cases} 0, & b \equiv \varnothing \\ (a \cdot c) + a, & b \equiv c' \\ \sup\{a \cdot c \mid c \prec b\}, & b \text{ — предельный ординал} \end{cases}$$

$$a^b \equiv \begin{cases} 1, & b \equiv \varnothing \\ (a^c) \cdot a, & b \equiv c' \\ \sup\{a^c \mid c \prec b\}, & b \text{ — предельный ординал} \end{cases}$$

Пример

$\omega \cdot \omega = \sup\{\omega \cdot 0, \omega \cdot 1, \omega \cdot 2, \omega \cdot 3, \dots\} = \sup\{0, \omega, \omega \cdot 2, \omega \cdot 3, \dots\}$

Ординалы (порядковые числа) и порядок

Определение

Будем говорить, что $\langle S, (\prec) \rangle$ *имеет порядковое число (тип)* X*, если существует биекция* $f : S \to X$*, причём* $a \prec b$ *тогда и только тогда, когда* $f(a) \in f(b)$*.*

Пример

- *Добавить элемент перед бесконечностью:* $\mathbb{N}$ *и* $\mathbb{N}_0$*.* $1 + \omega = \omega$*.*
- *Добавить элемент после бесконечности* $(+\infty)$*.* $\omega + 1 \neq \omega$

Пары и списки

Пример

Упорядоченные пары натуральных чисел имеют порядковый тип ω^2.

$$\langle 3, 5\rangle < \langle 4, 3\rangle \qquad \omega \cdot 3 + 5 < \omega \cdot 4 + 3.$$

Пример

Списки натуральных чисел — порядковый тип ω^ω.

$$\langle 3, 1, 4, 1, 5, 9\rangle \qquad \omega^5 \cdot 3 + \omega^4 \cdot 1 + \omega^3 \cdot 4 + \omega^2 \cdot 1 + \omega^1 \cdot 5 + 9$$

Дизъюнктные множества

Определение

Дизъюнктное (разделённое) множество — множество, элементы которого не пересекаются.

$$Dj(x) \equiv \forall y.\forall z.(y \in x \,\&\, z \in x \,\&\, \neg y = z) \to \neg\exists t.t \in y \,\&\, t \in z$$

Пример

Дизъюнктное: $\{\{1,2\},\{\to\},\{\alpha,\beta,\gamma\}\}$
Не дизъюнктное: $\{\{1,2\},\{\to\},\{\alpha,\beta,\gamma,1\}\}$

Прямое произведение множеств

Определение

Прямое произведение дизъюнктного множества a — множество $\times a$ всех таких множеств b, что:

- *b пересекается с каждым из элементов множества a в точности в одном элементе*
- *b содержит элементы только из $\cup a$.*

$$\forall b.b \in \times a \leftrightarrow (b \subseteq \cup a \,\&\, \forall y.y \in a \rightarrow \exists! x.x \in y \,\&\, x \in b)$$

Пример

$\times\{\{\triangle, \square\}, \{1, 2, 3\}\} =$
$\{\{\triangle, 1\}, \{\triangle, 2\}, \{\triangle, 3\}, \{\square, 1\}, \{\square, 2\}, \{\square, 3\}\}$

Аксиома выбора

Определение

Прямое произведение непустого дизъюнктного множества, не содержащего пустых элементов, не пусто.

$$\forall t.Dj(t) \to (\forall x.x \in t \to \exists p.p \in x) \to (\exists p.p \in \times t)$$

Альтернативные варианты: любое множество можно вполне упорядочить, любая сюръективная функция имеет частичную обратную, и т.п.

Определение

Аксиоматика ZF + аксиома выбора = ZFC

Дискуссия вокруг аксиомы выбора

Пример

Парадокс Банаха-Тарского: трёхмерный шар равносоставен двум своим копиям.

Теорема

Теорема (Гёдель, 1938): аксиома выбора не добавляет противоречий в ZF.

Теорема

Теорема (Коэн, 1963): аксиома выбора не следует из других аксиом ZF.

Пример

Односторонние функции: Sha256 и т.п. У Sha256 есть обратная.

Теорема

Теорема Диаконеску: ZFC поверх интуиционистского исчисления предикатов содержит правило исключённого третьего.

Аксиома фундирования

Определение

Аксиома фундирования. В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x.x = \varnothing \vee \exists y.y \in x \,\&\, \forall z.z \in x \to z \notin y$$

Иными словами, в каждом множестве есть элемент, минимальный по отношению $(\in)$.
Идея Рассела: каждому множеству припишем *тип* (тип пустого 0, тип множеств 1, тип множеств множеств 2 и т.п.). Тогда конструкция невозможна: $\{x \mid x \in x\}$. Аксиома фундирования позволяет определить функцию ранга:

$$rk(x) = \sup\{rk(y) \mid y \in x\}$$

.

Схема аксиом подстановки

Определение

Схема аксиом подстановки. Пусть задана некоторая функция f, представимая в исчислении предикатов: то есть задана некоторая формула ϕ, такая, что $f(x) = y$ тогда и только тогда, когда $\phi(x, y)$ & $\exists!z.\phi(x, z)$. Тогда для любого множества S существует множество f(S) — образ множества S при отображении f.

$$\forall s.(\forall x.\forall y_1.\forall y_2.x \in s\&\phi(x, y_1)\&\phi(x, y_2) \to y_1 = y_2) \to (\exists t.\forall y.y \in t \leftrightarrow \exists$$

Алгебраические типы данных

Алгебра на типах данных

Множество	Мощность	Тип	Название
$\varnothing$	0	void	необитаемый
$\{\varnothing\}$	1	unit	одноэлементный
$\{T, F\}$	2	boolean	булевский, двухэлемен
$A \uplus B$	$\lvert\alpha\rvert + \lvert\beta\rvert$	Either Alpha Beta	тип-сумма
$A \times B$	$\lvert\alpha\rvert \cdot \lvert\beta\rvert$	(Alpha, Beta)	пара, декартово произв
B^A	$\lvert\beta\rvert^{\lvert\alpha\rvert}$	Alpha $\to$ Beta	функциональный

Пример

`(boolean, A -> boolean)` соответствует $2 \cdot (2^A)$

Алгебраический тип данных, тип-сумма

Определение

Отмеченным объединением множеств (дизъюнктным объединением) назовём:

$A \uplus B := \{\langle a, \text{“}L\text{”} \rangle \mid a \in A\} \cup \{\langle b, \text{“}R\text{”} \rangle \mid b \in B\} = \{a_L \mid a \in A\} \cup \{b_R \mid b \in$

Пример

$$\mathbb{N} \cup \mathbb{N} = \{1, 2, 3, \dots\} \qquad \mathbb{N} \uplus \mathbb{N} = \{1_L, 1_R, 2_L, 2_R, 3_L, 3_R, \dots\}$$

$$\mathbb{N} \uplus \mathbb{Z} = \{\cdots - 3_R, -2_R, -1_R, 0_R, 1_L, 1_R, 2_L, 2_R, 3_L, 3_R \dots\}$$

Алгебраический тип данных (тип-сумма) задаётся набором конструкторов, каждому конструктору сопоставляется тип параметра.

Пример

boolean := False | True $\quad B = \{\varnothing\} \uplus \{\varnothing\} \quad Л : \varnothing_L$

angle := Degrees of int | Radians of real $\quad A := \mathbb{Z} \uplus \mathbb{R} \quad 180^\circ : 180_$

Примеры из языков программирования

```
type angle = record
     case radians : boolean of
         true: (rads: real);
         false: (degs: integer);
     end;
```

```
struct angle {
    bool radians;
    union {
        float rads;
        int degs;
    }
};
```

Типичное применение:

```
union {
    short ax;
    struct {
        char al;
        char ah;
    }
};
```

Списки

- Список (целых чисел) — алгебраический тип:

```
type list = Nil | Cons of int * list
```

- Как строим значения:

```
Nil                                  =>  []
Cons (5, Nil)                        =>  [5]
Cons (3, Cons (4, Cons (5, Nil)))    =>  [3,4,5]
```

- Как используем значения:

```
let rec length l = match l with
    Nil -> 0
  | Cons (_,lt) -> 1 + length lt
```

Взглянем немного глубже

Надо научиться строить и разбирать тип
`list = Nil | Cons of int * list`:

$$L = \{\varnothing\} \uplus (\mathbb{Z} \times L)$$

- Строить. Конструкторы: Nil, Cons — или левая и правая инъекции (In_L, In_R).

$$Nil := In_L() \qquad Cons\ a\ b := In_R\ \langle a, b \rangle$$

- Разбирать.

```
let rec length l = match l with
    Nil -> 0
  | Cons (lh,lt) -> 1 + length lt
```

```
match l with
|InL p -> 0
|InR p -> 1 + lengt
```

В самом низу — элиминатор Case:
$length\ l := Case\ l\ (\lambda p.0)\ (\lambda p.1 + length\ (\pi_R p))$

Алгебраический тип как дизъюнкция

Общие соображения: BHK-интерпретация.
Интуиционистское исчисление высказываний

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta} \qquad \frac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta} \qquad \frac{\Gamma \vdash \alpha \vee \beta \quad \Gamma \vdash \alpha \to \gamma \quad \Gamma \vdash \beta \to \gamma}{\Gamma \vdash \gamma}$$

Просто-типизированное лямбда исчисление — придумаем названия

$$\frac{\Gamma \vdash A : \alpha}{\Gamma \vdash In_L A : \alpha \vee \beta} \qquad \frac{\Gamma \vdash B : \beta}{\Gamma \vdash In_R B : \alpha \vee \beta} \qquad \frac{\Gamma \vdash X : \alpha \vee \beta \quad \Gamma \vdash L : \alpha \to \gamma}{\Gamma \vdash \text{Case X L R} :}$$

Пример

Напомним, если $\tau = \varphi = unit$, *то* $\tau \vee \varphi \approx bool$.
Тогда $T^{\tau \vee \varphi} := In_L(), \quad F^{\tau \vee \varphi} := In_R()$. *И, например,*
$Not\ x := Case\ x\ (\lambda t.In_R())\ (\lambda t.In_L())$

Реализация алгебраического типа

Просто-типизированное лямбда исчисление:

$$\frac{\Gamma \vdash A : \alpha}{\Gamma \vdash In_L A : \alpha \vee \beta} \qquad \frac{\Gamma \vdash B : \beta}{\Gamma \vdash In_R B : \alpha \vee \beta} \qquad \frac{\Gamma \vdash X : \alpha \vee \beta \quad \Gamma \vdash L : \alpha \to \gamma}{\Gamma \vdash \text{Case X L R} :}$$

Предлагаем такую реализацию:

$In_L := \lambda x.\lambda t.\lambda f.t\ x, \qquad In_R := \lambda x.\lambda t.\lambda f.f\ x \qquad Case := \lambda x.\lambda l.\lambda r.x\ l\ r$

$Case\ (In_L\ X^{\tau})\ L^{\tau\to\gamma}\ R \twoheadrightarrow_\beta (In_L\ X)\ L\ R = (\lambda t.\lambda f.t\ X)\ L\ R \twoheadrightarrow_\beta (L\ X)^{\gamma}$

А где здесь дизъюнкция? Ожидаем, что $(In_L\ X^{\tau}) : \tau \vee \varphi$. А что на деле?

$$X : \tau \vdash \lambda t^{\tau\to\gamma}.\lambda f^{\varphi\to\gamma}.t\ X : (\tau \to \gamma) \to (\varphi \to \gamma) \to \gamma$$

«Если некоторое утверждение γ истинно всегда, когда оно следует из истинности τ и φ — то либо τ, либо φ истинно». Рассуждение не совсем формально, потому что не хватает кванторов по утверждениям, использующимся неявно:

$$\forall\gamma.(\tau \to \gamma) \to (\varphi \to \gamma) \to \gamma$$

Примеры алгебраических типов

Булевские значения:

$$T_1 := In_L() = \lambda t.\lambda f.t\ () \qquad F_1 := In_R() = \lambda t.\lambda f.f\ () \qquad If_1 := \lambda b.\lambda t.\lambda e$$

Ну или когда аргумент опущен за ненадобностью:

$$T := \lambda t.\lambda f.t \qquad F := \lambda t.\lambda f.f \qquad If := \lambda b.\lambda t.\lambda e.b\ t\ e$$

Списки:

$$Nil := In_L 0 \qquad Cons\ p\ q := In_R \langle p, q \rangle$$

Тогда $[1, 3, 5]$ превращается в $Cons\ 1\ (Cons\ 3\ (Cons\ 5\ Nil))$.
Для простоты раскроем полностью $[1] = Cons\ 1\ Nil$:

$$\lambda t.\lambda f.f(\lambda p.p\ (\lambda f.\lambda x.f\ x)\ (\lambda t.\lambda f.t\ (\lambda f.\lambda x.x)))$$

Мощность	Тип	Высказывание
0	$\bot$	необитаемый тип
1	() : unit	одноэлементный тип
$\lvert\alpha\rvert + \lvert\beta\rvert$	Either A^α B^β : $\alpha \vee \beta$	тип-сумма, дизъюнкция
$\lvert\alpha\rvert \cdot \lvert\beta\rvert$	$(A^\alpha, B^\beta) : \alpha \,\&\, \beta$	тип-произведение, конъюнкция
$\lvert\beta\rvert^{\lvert\alpha\rvert}$	$\lambda x^\alpha.B : \alpha \to \beta$	функциональный, импликация

Мощность множеств

Отношения

Определение

$A \times B := \{\langle a, b\rangle \mid a \in A, b \in B\}$

Бинарное отношение — $R \subseteq A \times B$

Функциональное бинарное отношение (функция) R — *такое, что* $\forall x.x \in A \to \exists! y.\langle x, y\rangle \in R$

R — *инъективная функция, если*
$\forall x.\forall y.\langle x, t\rangle \in R \,\&\, \langle y, t\rangle \in R \to x = y.$

R — *сюръективная функция, если* $\forall y.y \in B \to \exists x.\langle x, y\rangle \in R.$

Равномощные множества

Определение

Множество A равномощно B ($|A| = |B|$), если существует биекция $f : A \to B$.

Множество A имеет мощность, не превышающую мощности B ($|A| \leq |B|$), если существует инъекция $f : A \to B$.

Теорема Кантора-Бернштейна

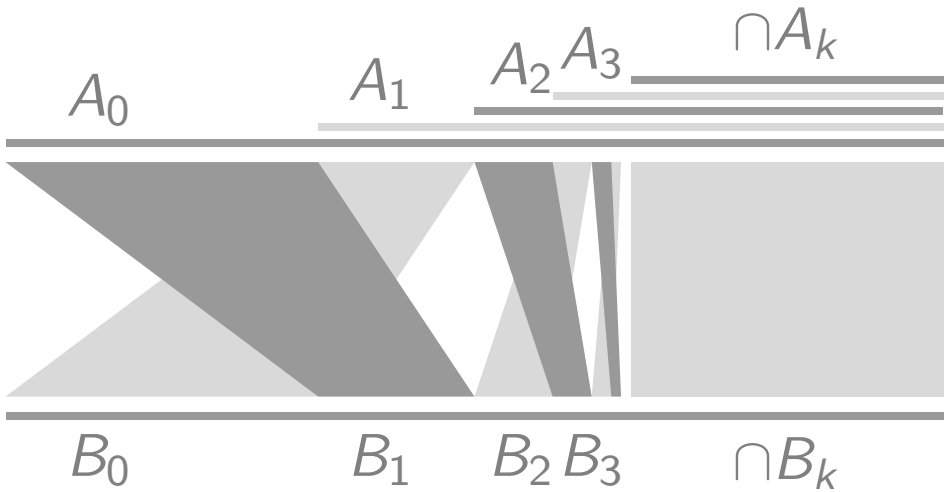
Теорема

Если $|A| \leq |B|$ *и* $|B| \leq |A|$, *то* $|A| = |B|$.

Заметим, $f : A \to B$, $g : B \to A$ — инъекции, но не обязательно $g(f(x)) = x$.

Доказательство.

Избавимся от множества B: пусть $A_0 = A$; $A_1 = g(B)$; $A_{k+2} = g(f(A_k))$.

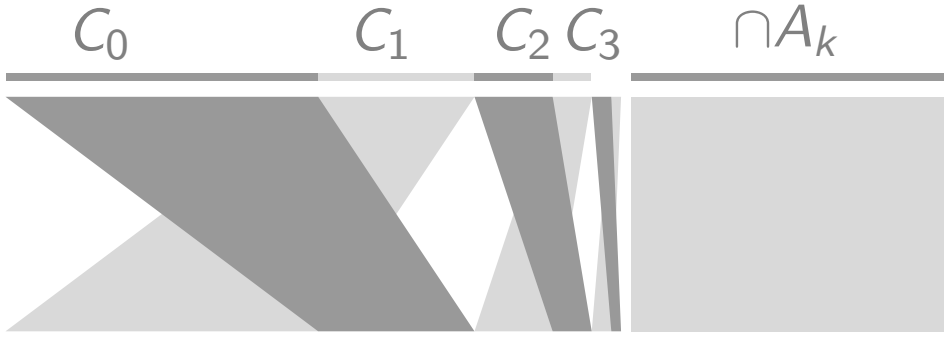


Тогда, если существует $h : A_0 \to A_1$ — биекция, то тогда $g^{-1} \circ h : A \to B$ — требуемая биекция.

□

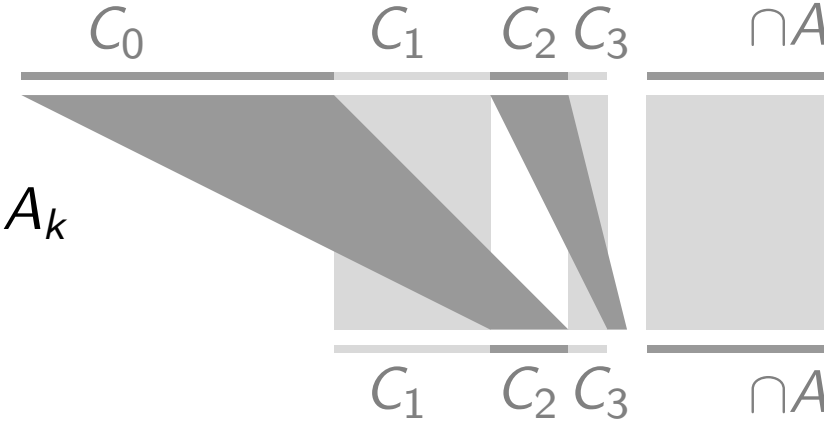
Построение биекции $h : A_0 \to A_1$

Пусть $C_k = A_k \setminus A_{k+1}$. Тогда
$g(f(C_k)) = g(f(A_k)) \setminus g(f(A_{k+1})) = A_{k+2} \setminus A_{k+3} = C_{k+2}$.



Тогда определим $h(x)$ следующим образом:

$$h(x) = \begin{cases} x, & x \in C_{2k+1} \vee x \in \cap A_k \\ g(f(x)), & x \in C_{2k} \end{cases}$$



Кардинальные числа

Определение

Кардинальное число — наименьший ординал, не равномощный никакому меньшему:

$$\forall x.x \in c \to |x| < |c|$$

Теорема

Конечные ординалы — кардинальные числа.

Определение

Мощность множества ($|S|$) *— равномощное ему кардинальное число.*

Диагональный метод

Лемма

$|\mathbb{R}| > |\mathbb{N}|$

Доказательство.

Рассмотрим $a \in (0,1)$ и десятичную запись: $0.a_0a_1a_2\ldots$. Пусть существует биективная $f : \mathbb{N} \to (0,1)$. По функции найдём значение σ, не являющееся образом никакого натурального числа.

n	$f(n)$	$f(n)_0$	$f(n)_1$	$f(n)_2$	$f(n)_3$	$f(n)_4$	$f(n)_5$	$\ldots$
n_0	0.3	3	0	0	0	0	0	$\ldots$
n_1	$\pi/10$	3	1	4	1	5	9	$\ldots$
n_2	$1/7$	1	4	2	8	5	7	$\ldots$
	σ	8	6	7	$\ldots\sigma_k = (f(n_k)_k + 5)\%10$			

□

Теорема Кантора

Теорема

$|\mathcal{P}(S)| > |S|$

Доказательство.

Пусть $S = \{a, b, c, \dots\}$

n	$a \in f(n)$	$b \in f(n)$	$c \in f(n)$	$\dots$
a	И	Л	И	
b	Л	Л	И	
c	И	И	И	
	Л	И	Л	$y \notin f(y)$

Пусть $f : S \to \mathcal{P}(S)$ — биекция. Тогда $\sigma = \{y \in S \mid y \notin f(y)\}$.
Пусть $f(x) = \sigma$. Но $x \in f(x)$ тогда и только тогда, когда $x \notin \sigma$, то есть $f(x) \neq \sigma$. $\square$

О буквах

https://en.wikipedia.org/wiki/Proto-Sinaitic_script

Иерархии $\aleph_n$ и $\beth_n$

Определение

$\aleph_0 := |\omega|$; $\aleph_{k+1} := \min\{a \mid a - \textit{ординал}, \aleph_k < |a|\}$

Определение

$\beth_0 := |\omega|$; $\beth_{k+1} := |\mathcal{P}(\beth_k)|$

Континуум-гипотеза (Г.Кантор, 1877): $\aleph_1 = \beth_1$ (не существует мощности, промежуточной между счётной и континуумом).
Обобщённая континуум-гипотеза: $\aleph_n = \beth_n$ при всех n.

Определение

Утверждение α противоречит аксиоматике: $\vdash \alpha$ ведёт к противоречию.
Утверждение α не зависит от аксиоматики: $\nvdash \alpha$ и $\nvdash \neg\alpha$.

Теорема (О независимости континуум-гипотезы, Дж.Коэн, 1963)

Утверждение $\aleph_1 = \beth_1$ не зависит от аксиоматики ZFC.

Примеры мощностей множеств

Пример	мощность
ω	$\aleph_0$
ω^2, ω^ω	$\aleph_0$
$\mathbb{R}$	$\beth_1$
все непрерывные функции $\mathbb{R} \to \mathbb{R}$	$\beth_1$
все функции $\mathbb{R} \to \mathbb{R}$	$\beth_2$

Как пересчитать вещественные числа (неформально)?

1. Номер вещественного числа — первое упоминание в литературе, т.е. $\langle j, y, n, p, r, c \rangle$:
   j — гёделев номер названия научного журнала (книги);
   y — год издания;
   n — номер;
   p — страница;
   r — строка;
   c — позиция
2. Попробуете предъявить число x, не имеющее номера? Это рассуждение сразу даст номер.

Мощность модели и аксиоматизации

Определение

Пусть задана модель $\langle D, F_n, P_n \rangle$ для некоторой теории первого порядка. Её мощностью будем считать мощность D.

Определение

Пусть задана формальная теория с аксиомами α_n. Её мощность — мощность множества $\{\alpha_n\}$.

Пример

Формальная арифметика, исчисление предикатов, исчисление высказываний — счётно-аксиоматизируемые.

Элементарная подмодель

Определение

$\mathcal{M}' = \langle D', F'_n, P'_n \rangle$ — *элементарная подмодель* $\mathcal{M} = \langle D, F_n, P_n \rangle$, *если:*

1. $D' \subseteq D$, F'_n, P'_n — *сужение* F_n, P_n *(замкнутое на* D'*).*
2. $\mathcal{M} \models \varphi(x_1, \ldots, x_n)$ *тогда и только тогда, когда* $\mathcal{M}' \models \varphi(x_1, \ldots, x_n)$ *при* $x_i \in D'$*.*

Пример

Когда сужение M не является элементарной подмоделью?
$\forall x.\exists y.x \neq y$. *Истинно в* $\mathbb{N}$. *Но пусть* $D' = \{0\}$.

Теорема Лёвенгейма-Сколема

Теорема

Пусть T — множество всех формул теории первого порядка. Пусть теория имеет некоторую модель $\mathcal{M}$. Тогда найдётся элементарная подмодель $\mathcal{M}'$, причём $|\mathcal{M}'| = \max(\aleph_0, |T|)$.

Доказательство.

(Схема доказательства)

1. Построим D_0 — множество всех значений, которые упомянуты в языке теории.
2. Будем последовательно пополнять D_i: $D_0 \subseteq D_1 \subseteq D_2 \ldots$, следя за мощностью. $D' = \cup D_i$.
3. Покажем, что $\langle D', F_n, P_n \rangle$ — требуемая подмодель.

□

Начальный D_0

Пусть $\{f_k^0\}$ — все 0-местные функциональные символы теории.

1. $D_0 = \{[\![f_k^0]\!]\}$, если есть хотя бы один f_k^0.
2. Если таких f_k^0 нет, возьмём какое-нибудь одно значение из D.

Очевидно, $|D_0| \leq |T|$.

Пополнение D

Фиксируем некоторый D_k. Напомним, T — множество всех формул теории. Рассмотрим $\varphi \in T$.

1. φ не имеет свободных переменных — пропустим.
2. φ имеет хотя бы одну свободную переменную y.
   - 2.1 $\varphi(y, x_1, \ldots, x_n)$ при $y, x_i \in D_k$ бывает истинным и ложным — ничего не меняем
   - 2.2 $\varphi(y, x_1, \ldots, x_n)$ при $y \in D$ и $x_i \in D_k$ либо всегда истинен, либо всегда ложен — ничего не меняем
   - 2.3 $\varphi(y, x_1, \ldots, x_n)$ при $y, x_i \in D_k$ тождественно истинен или ложен, но при $y' \in D \setminus D_k$ отличается — добавим y' к D_{k+1}. Вместе добавим всевозможные $[\![\theta(y')]\!]$.

Всего добавили не больше $|T| \cdot |D_k|$.
$|\cup D_i| \leq |T| \cdot |D_k| \cdot |\aleph_0| = \max(|T|, |\aleph_0|)$

$\mathcal{M}'$ — элементарная подмодель

Индукцией по структуре формул $\tau \in T$ покажем, что все формулы можно вычислить, и что $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.

1. База, 0 связок. $\tau \equiv P(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. Если $x_i \in D'$, то значит, добавлены на некоторых шагах (максимальный пусть t). Поэтому в D_{t+1} можно вычислить формулу, и её значение сохранилось.
2. Переход. Пусть формулы из k связок сохраняют значения. Рассмотрим τ с $k+1$ связкой.
   - 2.1 $\tau \equiv \rho \star \sigma$ — очевидно.
   - 2.2 $\tau \equiv \forall y.\varphi(y, x_1, \ldots, x_n)$. Каждый x_i добавлен на каком-то шаге — максимум t. Если $\varphi(y, x_1, \ldots, x_n)$ бывает истинен и ложен при $y_t, y_f \in D$, то $y_t, y_f \in D_{t+1}$ (по построению). Поэтому, если $\mathcal{M} \not\models \forall y.\varphi(y, x_1, \ldots, x_n)$, то и $\mathcal{M}' \not\models \forall y.\varphi(y, x_1, \ldots, x_n)$. Если же $\varphi(y, x_1, \ldots, x_n)$ не меняется от y, то тем более $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.
   - 2.3 $\tau \equiv \exists y.\varphi(y, x_1, \ldots, x_n)$ — аналогично.

«Парадокс» Сколема

1. Как известно, $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}| = \aleph_0$. Однако, ZFC — теория со счётным количеством формул. Значит, существует счётная модель ZFC, то есть $|\mathbb{R}| = \aleph_0$. В чём ошибка?
2. У равенств разный смысл, первое — в предметном языке, второе — в метаязыке.

Теорема Лёвенгейма-Сколема

Как пересчитать вещественные числа (неформально)?

1. Номер вещественного числа — первое упоминание в литературе, т.е. $\langle j, y, n, p, r, c \rangle$:
   j — гёделев номер названия научного журнала (книги);
   y — год издания;
   n — номер;
   p — страница;
   r — строка;
   c — позиция
2. Попробуете предъявить число x, не имеющее номера? Это рассуждение сразу даст номер.

Мощность модели и аксиоматизации

Определение

Пусть задана модель $\langle D, F_n, P_n \rangle$ для некоторой теории первого порядка. Её мощностью будем считать мощность D.

Определение

Пусть задана формальная теория с аксиомами α_n. Её мощность — мощность множества $\{\alpha_n\}$.

Пример

Формальная арифметика, исчисление предикатов, исчисление высказываний — счётно-аксиоматизируемые.

Элементарная подмодель

Определение

$\mathcal{M}' = \langle D', F'_n, P'_n \rangle$ — *элементарная подмодель* $\mathcal{M} = \langle D, F_n, P_n \rangle$, *если:*

1. $D' \subseteq D$, F'_n, P'_n — *сужение* F_n, P_n *(замкнутое на* D'*).*
2. $\mathcal{M} \models \varphi(x_1, \ldots, x_n)$ *тогда и только тогда, когда* $\mathcal{M}' \models \varphi(x_1, \ldots, x_n)$ *при* $x_i \in D'$*.*

Пример

Когда сужение M не является элементарной подмоделью?
$\forall x.\exists y.x \neq y$. *Истинно в* $\mathbb{N}$. *Но пусть* $D' = \{0\}$.

Теорема Лёвенгейма-Сколема

Теорема

Пусть T — множество всех формул теории первого порядка. Пусть теория имеет некоторую модель $\mathcal{M}$. Тогда найдётся элементарная подмодель $\mathcal{M}'$, причём $|\mathcal{M}'| = \max(\aleph_0, |T|)$.

Доказательство.

(Схема доказательства)

1. Построим D_0 — множество всех значений, которые упомянуты в языке теории.
2. Будем последовательно пополнять D_i: $D_0 \subseteq D_1 \subseteq D_2 \ldots$, следя за мощностью. $D' = \cup D_i$.
3. Покажем, что $\langle D', F_n, P_n \rangle$ — требуемая подмодель.

□

Начальный D_0

Пусть $\{f_k^0\}$ — все 0-местные функциональные символы теории.

1. $D_0 = \{[\![f_k^0]\!]\}$, если есть хотя бы один f_k^0.
2. Если таких f_k^0 нет, возьмём какое-нибудь одно значение из D.

Очевидно, $|D_0| \leq |T|$.

Пополнение D

Фиксируем некоторый D_k. Напомним, T — множество всех формул теории. Рассмотрим $\varphi \in T$.

1. φ не имеет свободных переменных — пропустим.
2. φ имеет хотя бы одну свободную переменную y.
   - 2.1 $\varphi(y, x_1, \ldots, x_n)$ при $y, x_i \in D_k$ бывает истинным и ложным — ничего не меняем
   - 2.2 $\varphi(y, x_1, \ldots, x_n)$ при $y \in D$ и $x_i \in D_k$ либо всегда истинен, либо всегда ложен — ничего не меняем
   - 2.3 $\varphi(y, x_1, \ldots, x_n)$ при $y, x_i \in D_k$ тождественно истинен или ложен, но при $y' \in D \setminus D_k$ отличается — добавим y' к D_{k+1}. Вместе добавим всевозможные $[\![\theta(y')]\!]$.

Всего добавили не больше $|T| \cdot |D_k|$.
$|\cup D_i| \leq |T| \cdot |D_k| \cdot |\aleph_0| = \max(|T|, |\aleph_0|)$

$\mathcal{M}'$ — элементарная подмодель

Индукцией по структуре формул $\tau \in T$ покажем, что все формулы можно вычислить, и что $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.

1. База, 0 связок. $\tau \equiv P(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. Если $x_i \in D'$, то значит, добавлены на некоторых шагах (максимальный пусть t). Поэтому в D_{t+1} можно вычислить формулу, и её значение сохранилось.
2. Переход. Пусть формулы из k связок сохраняют значения. Рассмотрим τ с $k+1$ связкой.
   - 2.1 $\tau \equiv \rho \star \sigma$ — очевидно.
   - 2.2 $\tau \equiv \forall y.\varphi(y, x_1, \ldots, x_n)$. Каждый x_i добавлен на каком-то шаге — максимум t. Если $\varphi(y, x_1, \ldots, x_n)$ бывает истинен и ложен при $y_t, y_f \in D$, то $y_t, y_f \in D_{t+1}$ (по построению). Поэтому, если $\mathcal{M} \not\models \forall y.\varphi(y, x_1, \ldots, x_n)$, то и $\mathcal{M}' \not\models \forall y.\varphi(y, x_1, \ldots, x_n)$. Если же $\varphi(y, x_1, \ldots, x_n)$ не меняется от y, то тем более $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.
   - 2.3 $\tau \equiv \exists y.\varphi(y, x_1, \ldots, x_n)$ — аналогично.

«Парадокс» Сколема

1. Как известно, $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}| = \aleph_0$. Однако, ZFC — теория со счётным количеством формул. Значит, существует счётная модель ZFC, то есть $|\mathbb{R}| = \aleph_0$. В чём ошибка?
2. У равенств разный смысл, первое — в предметном языке, второе — в метаязыке.

Аксиома выбора

Аксиома выбора

Аксиома (Аксиома выбора)

Из любого семейства дизъюнктных непустых множеств $\{A_i\}$ *можно выбрать непустую трансверсаль — множество* S*, что* $S \cap A_i = \{x_i\}$*. Иначе,* $S \in \times\{A_i\}$*.*

Теорема (Аксиома выбора)

Пусть $\{A_i\}$ *— семейство непустых множеств. Тогда существует* $f : \{A_i\} \to \cup A_i$*, причём* $\forall a.a \in \{A_i\} \to f(a) \in a$

Доказательство.

По семейству A_i рассмотрим семейство множеств $X(A_i)$: $X(A_i) = \{\langle A_i, a\rangle \mid a \in A_i\}$, если $A_i \neq A_j$, то $X(A_i) \cap X(A_j) = \varnothing$, тогда $\exists f.f \in \times\{X(A_i)\}$. □

Обратное утверждение также легко показать.

Аксиома выбора: альтернативные формулировки

Теорема (Лемма Цорна)

Если задано $\langle M, (\preceq) \rangle$ и для всякого линейно-упорядоченного $S \subseteq M$ выполнено $upb_M S \in M$, то в M существует максимальный элемент.

Теорема (Теорема Цермело)

На любом множестве можно задать полный порядок.

Теорема

У любой сюръективной функции существует частичная обратная.

Теорема

Аксиома выбора $\Rightarrow$ лемма Цорна: без доказательства

Начальный отрезок

Определение

Будем говорить, что $\langle S, (\prec_S)\rangle$ *— начальный отрезок* $\langle T, (\prec_T)\rangle$, *если:*

- $S \subseteq T$;
- *если* $a, b \in S$, *то* $a \prec_S b$ *тогда и только тогда, когда* $a \prec_T b$;
- *если* $a \in S$, $b \in T \setminus S$, *то* $a \prec_T b$.

Будем записывать это как $S \prec T$.

Теорема

Если множество начальных отрезков X *линейно упорядочено, то в нём есть наибольший элемент.*

Доказательство.

Пусть $M = \cup\{T | \langle T, (\prec)\rangle \in X\}$ и $(\prec)_M = \cup\{(\prec) | \langle T, (\prec)\rangle \in X\}$. Раз все элементы X сравнимы, значит, любые два отношения порядка не противоречат друг другу (одно – продолжение другого). Поэтому что все множества в X — начальные отрезки

Лемма Цорна $\Rightarrow$ теорема Цермело

Пусть выполнена лемма Цорна и дано некоторое X. Покажем, что на нём можно ввести линейный порядок.

- Пусть $S = \{\langle P, (\prec)\rangle \mid P \subseteq X, (\prec) \text{ — полный порядок}\}$. Например, для $X = \{0, 1\}$ множество $S = \{\langle \varnothing, \varnothing\rangle, \langle \{0\}, \varnothing\rangle, \langle \{1\}, \varnothing\rangle, \langle X, 0 \prec 1\rangle, \langle X, 1 \prec 0\rangle\}$
- Введём порядок на S: положим $\langle P, (\prec_p)\rangle < \langle Q, (\prec_q)\rangle$, если $P \subseteq Q$, $a \prec_p b$ тогда и только тогда, когда $a \prec_q b$, при $a, b \in P$, $a \prec_q b$ при $a \in P, b \in Q \setminus P$.
- Заметим, что $\langle \varnothing, \varnothing\rangle < \langle \{0\}, \varnothing\rangle$, но $\langle X, 0 \prec 1\rangle$ несравним с $\langle X, 1 \prec 0\rangle$.
- Любое линейно-упорядоченное подмножество $\langle T, (<)\rangle$ (где $T \subseteq S$) имеет верхнюю грань (она же максимальный элемент): $\langle \cup T, \cup(\prec)\rangle$ (например, для $\{\langle \varnothing, \varnothing\rangle, \langle \{0\}, \varnothing\rangle, \langle X, 0 \prec 1\rangle\}$ это $\langle X, 0 \prec 1\rangle$.
- По лемме Цорна тогда есть $\langle R, \sqsubset\rangle = \max S$. Заметим, что $R = X$, потому что иначе пусть $a \in X \setminus R$. Тогда положив $M = \langle R \cup \{a\}, (\prec_R) \cup \{x \prec a \mid x \in R\}\rangle$ получим, что M тоже вполне упорядоченное (и потому $M \in S$), значит, R

Теорема Цермело $\Rightarrow$ существование обратной $\Rightarrow$ аксиома выбора

Теорема

Теорема Цермело $\Rightarrow$ у сюръективных функций существует частичная обратная.

Доказательство.

Рассмотрим сюръективную $f : A \to B$. Рассмотрим семейство $R_b = \{a \in A \mid f(a) = b\}$. Построим полный порядок на каждом из R_b. Тогда $f^{-1}(b) = \min R_b$. $\square$

Теорема

Существует частичная обратная у сюръективных функций $\Rightarrow$ существует трансверсаль у дизъюнктных множеств.

Доказательство.

Пусть дано семейство дизъюнктных множеств $\{A_i\}$.
Рассмотрим $f : \cup A_i \to \{A_i\}$, что $f(a) = \cup\{A_i \in \{A_i\} \mid a \in A_i\}$.
Поскольку A_i дизъюнктны, $f(a) = A_i$ при всех a. Тогда существует $f^{-1}(A_i) \in A_i$. Тогда $\{f^{-1}(A_i)\} \in \times\{A_i\}$. $\square$

Зачем нужна аксиома выбора?

Определение

Пределом функции f в точке x_0 по Коши называется такой y, что

$$\forall \varepsilon \in \mathbb{R}^+ . \exists \delta . \forall x . |x - x_0| < \delta \to |f(x) - y| < \varepsilon$$

Определение

Пределом функции f в точке x_0 по Гейне называется такой y, что для любой $x_n \to x_0$ выполнено $f(x_n) \to y$.

Предел по Гейне влечёт предел по Коши

Теорема

Пусть $\lim_{x \to x_0} f(x) = y$ *по Гейне, тогда*
$\forall \varepsilon . \exists \delta . \forall x . |x_\delta - x_0| < \delta \to |f(x_\delta) - y| < \varepsilon$.

Доказательство.

Пусть не так. То есть, $\exists \varepsilon . \forall \delta . \exists x_\delta . |x_\delta - x_0| < \delta \;\&\; |f(x_\delta) - y| \geq \varepsilon$.
Фиксируем ε и возьмём $\delta_n = \frac{1}{n}$ и $p_n = x_{\delta_n}$. $p_n \to x_0$, так как $|x_{\frac{1}{n}} - x_0| < \frac{1}{n}$, по определению предела по Гейне $f(p_n) \to y$, но по предположению $|f(p_n) - y| \geq \varepsilon$. □

Пояснение

Для применения предела по Гейне нужна p_n *— как множество.*
$\langle p_1, p_2, p_3, \ldots \rangle$*?*
... *Фиксируем* ε *и рассмотрим*
$X_\delta = \{x_\delta \mid |x_\delta - x_0| < \delta \;\&\; |f(x_\delta) - y| \geq \varepsilon\}$. *Возьмём* $\delta_n = \frac{1}{n}$ *и* $x_{\frac{1}{n}} \in X_{\frac{1}{n}}$.
... *То есть, по семейству непустых множеств* $\{X_\delta\}$ *по аксиоме выбора построим* $p : \{X_\delta\} \to \cup X_\delta$, *что* $p(X_\delta) \in X_\delta$, *и построим*

Предел по Коши влечёт предел по Гейне

Теорема

Пусть $\lim_{x \to x_0} f(x) = y$ *и дана* $x_n \to x_0$. *Тогда* $f(x_n) \to y$.

Доказательство.

Фиксируем $\varepsilon > 0$.

- (определение предела по Коши) существует δ, что $\forall x. |x - x_0| < \delta \to |f(x) - y| < \varepsilon$.
- (сходимость x_n к x_0) найдётся N, что $\forall n. n > N \to |x_n - x_0| < \delta$.
- (предыдущие два пункта) $\forall n. n > N \to |f(x_n) - y| < \varepsilon$.

□

Почему здесь не требуется аксиома выбора? Потому что нам нужен δ из единственного множества $\{\delta \in \mathbb{R} \mid \forall x. |x - x_0| < \delta \to |f(x) - y| < \varepsilon\}$. То же про N. Аксиома выбора для конечного семейства множеств доказуема в ZF.

Равенство и функции

Пример

Пусть $A_0 = \{0, 1, 3, 5\}$ *и* $A_1 = \{3, 5, 1, 0, 0, 5, 3\}$. *Верно ли, что* $A_0 = A_1$?
Да, так как $\forall x.x \in \{0, 1, 3, 5\} \leftrightarrow x \in \{3, 5, 1, 0, 0, 5, 3\}$.

Теорема

Если $f : A \to B$, *также* $a, b \in A$ *и* $a = b$, *то* $f(a) = f(b)$.

Доказательство.

Пусть $F \subseteq A \times B$ — график функции f.
Легко показать, что если $a = b$ и $y_1 = y_2$, то $\langle a, y_1 \rangle = \langle b, y_2 \rangle$.
По определению функции,
$\forall x.\forall y_1.\forall y_2.\langle x, y_1 \rangle \in F \ \& \ \langle x, y_2 \rangle \in F \to y_1 = y_2$.
Также, если $f(a) = y_1$, $f(b) = y_2$, то $\langle a, y_1 \rangle \in F$ и $\langle b, y_2 \rangle \in F$.
Тогда: $\langle a, y_1 \rangle = \langle b, y_1 \rangle = \langle b, y_2 \rangle = \langle a, y_2 \rangle$, то есть
$f(a) = y_2 = f(b)$.

Теорема Диаконеску

Теорема

Если рассмотреть ИИП с ZFC, то для любого P выполнено $\vdash P \vee \neg P$.

Доказательство.

Рассмотрим $\mathcal{B} = \{0, 1\}$, $A_0 = \{x \in \mathcal{B} | x = 0 \vee P\}$ и $A_1 = \{x \in \mathcal{B} | x = 1 \vee P\}$. $\{A_0, A_1\}$ — непустое семейство непустых множеств, и по акс. выбора существует $f : \{A_0, A_1\} \to \cup A_i$, что $f(A_i) \in A_i$. (Если P, то $A_0 = A_1$ и $\{A_0, A_1\} = \{\mathcal{B}\}$).

$\vdash f(A_0) \in A_0 \,\&\, f(A_1) \in A_1$	$f(A_i)$
$\vdash (f(A_0) \in \mathcal{B} \,\&\, f(A_0) = 0 \vee P) \,\&\, (f(A_1) \in \mathcal{B} \,\&\, f(A_1) = 1 \vee P)$	Опр.
$\vdash (f(A_0) = 0 \,\&\, f(A_1) = 1) \vee P$	Удал
$\vdash P \vee f(A_0) \neq f(A_1)$	Пере
$\vdash P \to A_0 = A_1$	Опре
$\vdash A_0 = A_1 \to f(A_0) = f(A_1)$	Теор
$\vdash f(A_0) \neq f(A_1) \to \neg P$	Конт
$\vdash P \vee \neg P$	Подс

Слабые варианты аксиомы выбора

Теорема (конечного выбора)

Если $X_1 \neq \varnothing, \ldots, X_n \neq \varnothing$, $X_i \cap X_j = \varnothing$ *при* $i \neq j$, *то* $\times\{X_1, \ldots, X_n\} \neq \varnothing$.

Доказательство.

- База: $n = 1$. Тогда $\exists x_1 . x_1 \in X_1$, поэтому $\exists x_1 . \{x_1\} \in \times\{X_1\}$.
- Переход: $\exists v . v \in \times\{X_{1,n}\} \to \exists x_{n+1} . x_{n+1} \in X_{n+1} \to v \cup \{x_{n+1}\} \in \times(X_{1,n} \cup \{X_{n+1}\})$

□

Аксиома (счётного выбора)

Для счётного семейства непустых множеств существует функция, каждому из которых сопоставляющая один из своих элементов

Аксиома (зависимого выбора)

если $\forall x \in E . \exists y \in E . xRy$, *то существует последовательность* $x_n : \forall n . x_n R x_{n+1}$

Аксиома конструктивности: V=L

Определение

Универсум фон Неймана V — все наследственные фундированные множества.
Конструктивный универсум $L = \cup_a L_a$, где:

$$L_a = \begin{cases} \varnothing, & a = 0 \\ \{\{x \in L_b \mid \varphi(x, t_1, \ldots, t_k)\} \mid \varphi - \textit{формула}, t_i \in L_b\}, & a = b' \\ \bigcup_{b<a}(L_b), & a - \textit{пре} \end{cases}$$

При наличии аксиомы фундирования можно показать, что $V = \cup_a V_a$, где:

$$V_a = \begin{cases} \varnothing, & a = 0 \\ \mathcal{P}(V_b), & a = b' \\ \bigcup_{b<a}(V_b), & a - \text{предельный} \end{cases}$$

Аксиома конструктивности: $V = L$, то есть все фундированные множества задаются формулами.

Теорема о непротиворечивости формальной арифметики

Два вида индукции

Определение (принцип математической индукции)

Какое бы ни было $\varphi(x)$, *если* $\varphi(0)$ *и при всех* x *выполнено* $\varphi(x) \to \varphi(x')$, *то при всех* x *выполнено и само* $\varphi(x)$.

Определение (принцип полной математической индукции)

Какое бы ни было $\psi(x)$, *если* $\psi(0)$ *и при всех* x *выполнено* $(\forall t.t \leq x \to \psi(t)) \to \psi(x')$, *то при всех* x *выполнено и само* $\psi(x)$.

Теорема

Принципы математической индукции эквивалентны

Доказательство.

($\Rightarrow$) взяв $\varphi := \psi$, имеем выполненность $\varphi(x) \to \varphi(x')$, значит, $\forall x.\psi(x)$.
($\Leftarrow$) возьмём $\psi(x) := \forall t.t \leq x \to \varphi(t)$. $\square$

Наследственные множества

Определение

Назовём вполне упорядоченное отношением $(\in)$ *множество* S *наследственным подмножеством* A*, если*
$\forall x.x \in A \to (\forall t.t \in x \to t \in S) \to x \in S$.

Теорема

Единственным наследственным подмножеством вполне упорядоченного множества является оно само.

Доказательство.

Пусть $B \subseteq A$ — наследственное и $B \neq A$. Тогда существует $a = \min(A \setminus B)$. Тогда $(\forall t.t \in a \to t \in B) \to a \in B$ по наследственности B, и выполнено $\forall t.t \in a \to t \in B$ (по минимальности a). Значит, $a \in B$. $\square$

Трансфинитная индукция

Теорема (Принцип «полной» трансфинитной индукции)

Если для $\varphi(x)$ *(некоторого утверждения теории множеств) и некоторого ординала* ε *выполнено*
$\forall x.x \in \varepsilon \to (\forall t.t \in x \to \varphi(t)) \to \varphi(x)$, *то* $\forall x.x \in \varepsilon \to \varphi(x)$.

Доказательство.

Рассмотрим $S = \{x \in \varepsilon \mid \varphi(x)\}$. Тогда $x \in S$ равносильно $\varphi(x)$.
Тогда перепишем: $\forall e.e \in \varepsilon \to (\forall x.x \in e \to x \in S) \to e \in S$.
Отсюда по теореме о наследственных множествах $S = \varepsilon$. $\square$

Альтернативная формулировка

Теорема

Для ординала ε подмножество $S \in \varepsilon$ — наследственное, если одновременно:
Если $x \in \varepsilon$ и $x = \varnothing$, то $x \in S$;
Если $x \in \varepsilon$ и существует y: $y' = x$, то $y \in S \to x \in S$;
Если $x \in \varepsilon$ и x — предельный, то $(\forall t.t \in x \to t \in S) \to (x \in S)$.

Доказательство.

($\Rightarrow$) очевидно. Докажем ($\Leftarrow$): пусть S не наследственное: $E := \{e \in \varepsilon \mid (\forall t.t \in e \to t \in S)\ \&\ e \notin S\}$ и $E \neq \varnothing$. Тогда пусть $e = \min E$.

1. $e = \varnothing$ или предельный. Тогда $(\forall t.t \in e \to t \in S) \to (e \in S)$.
2. $e = y'$. Тогда $y \in \varepsilon$ (ε — ординал) и $(\forall t.t \in y \to t \in S) \to (y \in S)$ (так как e минимальный, для которого S не наследственное). По условию, $(y \in S) \to (e \in S)$, отсюда $(\forall t.t \in e \to t \in S) \to (e \in S)$.

Исчисление S_∞

1. Язык: связки $\neg$, $\vee$, $\forall$, $=$; нелогические символы: $(+)$,$(\cdot)$,$(')$,0; переменные: x.
2. Аксиомы: все истинные формулы вида $\theta_1 = \theta_2$; все истинные отрицания формул вида $\neg\theta_1 = \theta_2$ (θ_i — термы без переменных).
3. Структурные (слабые) правила:

$$\frac{\zeta \vee \alpha \vee \beta \vee \delta}{\zeta \vee \beta \vee \alpha \vee \delta} \qquad \frac{\alpha \vee \alpha \vee \delta}{\alpha \vee \delta}$$

сильные правила

$$\frac{\delta}{\alpha \vee \delta} \quad \frac{\neg\alpha \vee \delta \quad \neg\beta \vee \delta}{\neg(\alpha \vee \beta) \vee \delta} \quad \frac{\alpha \vee \delta}{\neg\neg\alpha \vee \delta} \quad \frac{\neg\alpha[x := \theta] \vee \delta}{(\neg\forall x.\alpha) \vee \delta}$$

и ещё два правила . . .

Ещё правила S_∞

бесконечная индукция

$$\frac{\alpha[x := \overline{0}] \vee \delta \quad \alpha[x := \overline{1}] \vee \delta \quad \alpha[x := \overline{2}] \vee \delta \quad \dots}{(\forall x.\alpha) \vee \delta}$$

сечение

$$\frac{\zeta \vee \alpha \qquad \neg\alpha \vee \delta}{\zeta \vee \delta}$$

Здесь:
α — секущая формула
Число связок в $\neg\alpha$ — степень сечения.

Дерево доказательства

1. Доказательства образуют деревья.
2. Каждой формуле в дереве сопоставим порядковое число (ординал).
3. Порядковое число заключения любого неструктурного правила строго больше порядкового числа его посылок (больше или равно в случае структурного правила).

$$\dfrac{\dfrac{(\neg 1 = 0)_1 \quad (\neg 2 = 0)_2 \quad (\neg 3 = 0)_4 \quad (\neg 4 = 0)_8 \ldots}{(\forall x.\neg x' = 0)_\omega}}{(\neg\neg\forall x.\neg x' = 0)_{\omega+1}}$$

4. Существует конечная максимальная степень сечения в дереве (назовём её степенью вывода).

Любая теорема Ф.А. — теорема S_∞

Теорема

Если $\vdash_{\text{фа}} \alpha$, *то* $\vdash_\infty |\alpha|_\infty$

Пример

Обратное неверно:

$$\frac{\neg\omega(\overline{0}, \overline{\ulcorner\sigma\urcorner}) \qquad \neg\omega(\overline{1}, \overline{\ulcorner\sigma\urcorner}) \qquad \neg\omega(\overline{2}, \overline{\ulcorner\sigma\urcorner}) \qquad \ldots}{\forall x.\neg\omega(x, \overline{\ulcorner\sigma\urcorner})}$$

Теорема

Если Ф.А. противоречива, то противоречива и S_∞

Обратимость правил де Моргана, отрицания, бесконечной индукции

Теорема

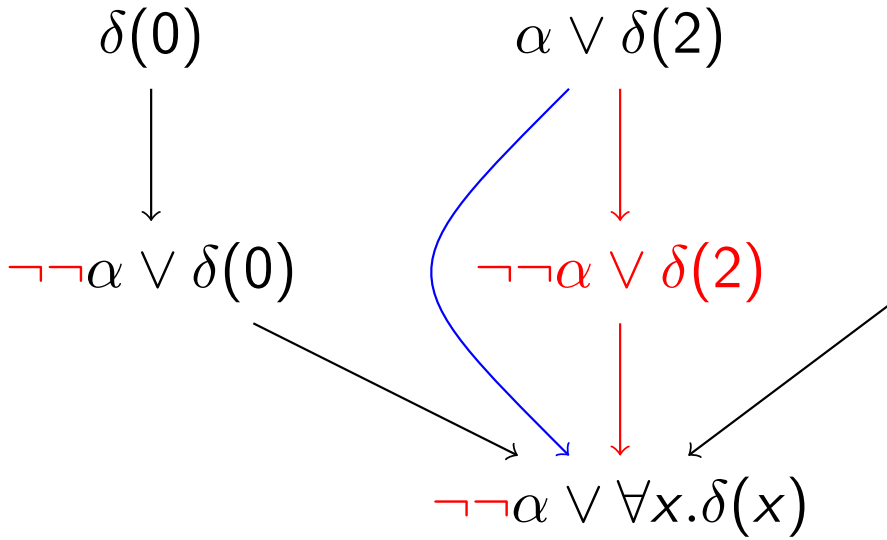
$$\frac{\neg(\alpha \vee \beta) \vee \delta}{\neg\alpha \vee \delta \quad \neg\beta \vee \delta} \qquad \frac{\neg\neg\alpha \vee \delta}{\alpha \vee \delta} \qquad \frac{(\forall x.\alpha) \vee \delta}{\alpha[x := \overline{0}] \vee \delta \quad \alpha[x := \overline{1}] \vee \delta \quad \alpha[x := \overline{2}] \vee \delta}$$

Доказательство.

Например, формула вида $\neg\neg\alpha \vee \delta$.

Проследим историю $\neg\neg\alpha$; она могла быть получена:

1. ослаблением — заменим $\neg\neg\alpha$ на α в этом узле и последующих.
2. отрицанием — выбросим правило, заменим $\neg\neg\alpha$ на



Устранение сечений

Теорема

Если α имеет вывод степени $m > 0$ порядка t, то можно найти вывод степени строго меньшей m с порядком 2^t.

Доказательство.

Трансфинитная индукция. Пусть для всех деревьев порядка $t_1 < t$ условие выполнено. Покажем, что оно выполнено для порядка t. Рассмотрим заключительное правило. Это может быть...

1. Не сечение.
2. Сечение, секущая формула — элементарная.
3. Сечение, секущая формула — $\neg\alpha$.
4. Сечение, секущая формула — $\alpha \vee \beta$.
5. Сечение, секущая формула — $\forall x.\alpha$.

Случай 1. Не сечение

$$\frac{(\pi_0)_{t_0} \quad (\pi_1)_{t_1} \quad (\pi_2)t_2 \quad \dots}{(\alpha)_t}$$

Заменим доказательства посылок $(\pi_i)_{t_i}$ на $(\pi'_i)_{2^{t_i}}$ по индукционному предположению.

1. Поскольку степени посылок $m'_i < m_i$, то $\max m'_i < \max m_i$.
2. Поскольку $t_i \leq t$, то $2^{t_i} \leq 2^t$.

Случай 5. Сечение с формулой вида $\forall x.\alpha$

$$\frac{\zeta \vee \forall x.\alpha \qquad (\neg\forall x.\alpha) \vee \delta}{\zeta \vee \delta}$$

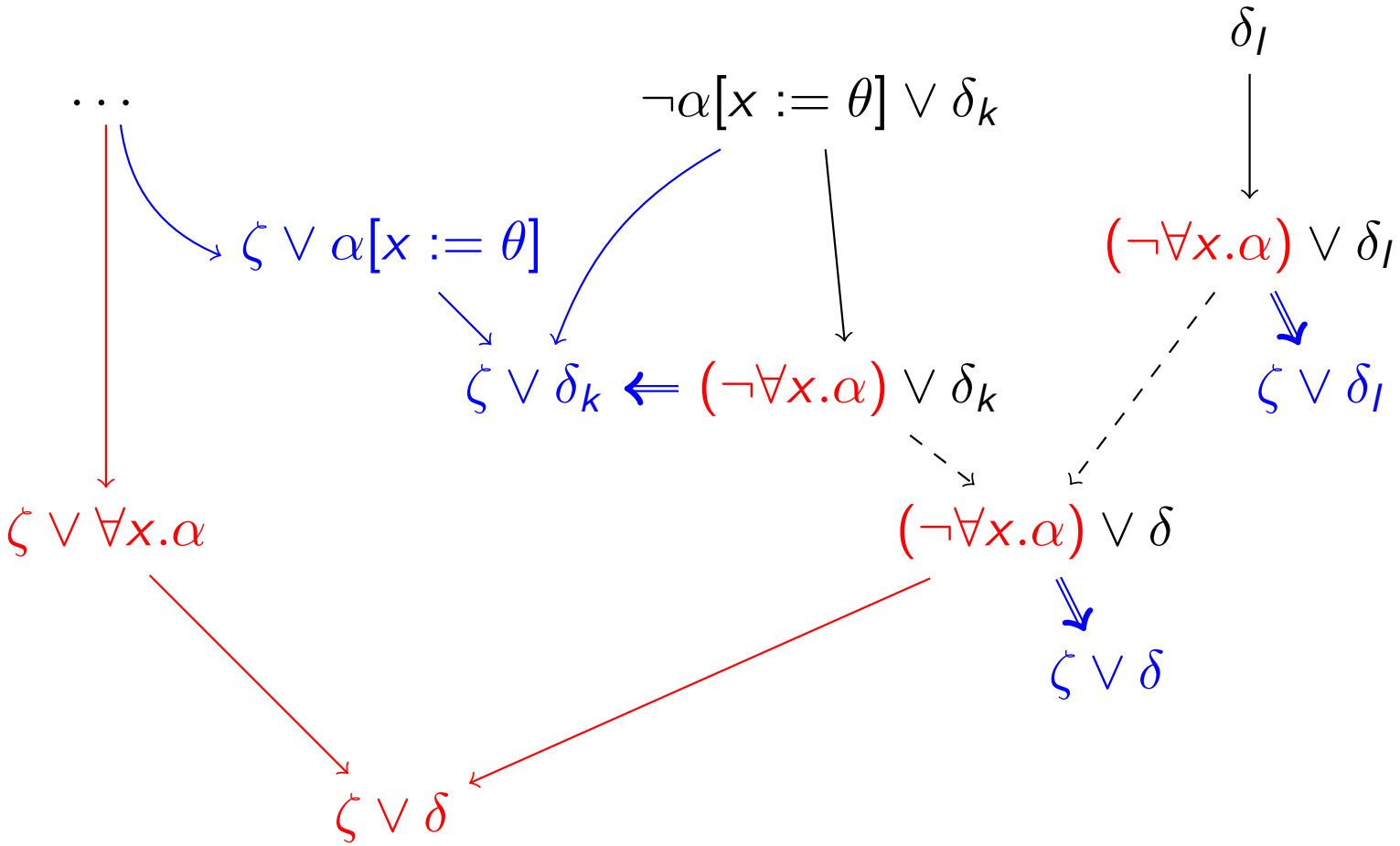
Причём степень и порядок выводов компонент, соответственно, (m_1, t_1) и (m_2, t_2).

1. По индукции, вывод $\zeta \vee \forall x.\alpha$ можно упростить до $(m_1', 2^{t_1})$.
2. По обратимости, можно построить вывод $\zeta \vee \alpha[x := \theta]$ за $(m_1', 2^{t_1})$.
3. В формуле $(\neg\forall x.\alpha) \vee \delta$ формула $\neg\forall x.\alpha$ получена либо ослаблением, либо квантификацией из $\neg\alpha[x := \theta_k] \vee \delta_k$.
   - 3.1 Каждое правило квантификации заменим на:

$$\frac{\zeta \vee \alpha[x := \theta_k] \qquad (\neg\alpha[x := \theta_k]) \vee \delta_k}{\zeta \vee \delta_k}$$

   - 3.2 Остальные вхождения $\neg\forall x.\alpha$ заменим на ζ (в правилах ослабления).
4. В получившемся дереве меньше степень — так как в $\neg\alpha[x := \theta]$ меньше связок, чем в $\neg\forall x.\alpha$.

Случай 5. Как перестроим доказательство



Теорема об устранении сечений

Определение

Итерационная экспонента

$$(a\uparrow)^m(t) = \begin{cases} t, & m = 0 \\ a^{(a\uparrow)^{m-1}(t)}, & m > 0 \end{cases}$$

Теорема

Если $\vdash_\infty \sigma$ степени m порядка t, то найдётся доказательство без сечений порядка $(2\uparrow)^m(t)$

Доказательство.

В силу конечности m воспользуемся индукцией по m и теоремой об уменьшении степени. $\square$

Порядок трансфинитной индукции

Определение

ε_0 — *неподвижная точка* $\varepsilon_0 = \omega^{\varepsilon_0}$

Иначе говоря, $\varepsilon_0 = \{\omega, \omega^\omega, \omega^{\omega^\omega}, (\omega \uparrow)^3(\omega), (\omega \uparrow)^4(\omega), \dots\}$.
Очевидно, что теорема об устранении сечений может быть доказана трансфинитной индукцией до ординала ε_0 (максимальный порядок дерева вывода, при правильной нумерации вершин).

Непротиворечивость формальной арифметики

Теорема

Система S_∞ непротиворечива

Доказательство.

Рассмотрим формулу $\neg 0 = 0$. Если эта формула выводима в S_∞, то она выводима и в S_∞ без сечений. Тогда какое заключительное правило?

1. Правило Де-Моргана? Нет отрицаний дизъюнкции $(\neg(\alpha \vee \beta) \vee \delta)$.
2. Отрицание? Нет двойного отрицания $(\neg\neg\alpha \vee \delta)$.
3. Бесконечная индукция или квантификация? Нет квантора.
4. Ослабление? Нет дизъюнкции $(\alpha \vee \delta)$.

То есть, неизбежно, $\neg 0 = 0$ — аксиома, что также неверно. $\square$

Метод резолюций

Разрешимость исчислений

«Извини, Теодор, но это ты очень странно рассуждаешь. Бессмыслица — искать решение, если оно и так есть. Речь идет о том, как поступить с задачей, которая решения не имеет. Это глубоко принципиальный вопрос, который, как я вижу, тебе, прикладнику, к сожалению, не доступен.»

А. и Б. Стругацкие, «Понедельник начинается в субботу»

- Разрешимы: КИВ, ИИВ.
- Неразрешимы: всё остальное (ИП, ФА, ZF(C), ...)

Однако, (1) разрешимости хочется и (2) человек как-то умеет.

Ищем доказательство в исчислении предикатов: упрощение задачи

- По теореме о полноте можем рассматривать ($\models$) вместо ($\vdash$). Напомним: $\models \alpha$, если для всех $M = \langle D, F, P, E \rangle$ выполнено $M \models \alpha$.

- Что мешает:
  1. слишком сложные формулы — кванторы по бесконечным множествам;
  2. слишком больше разнообразие D, включая несчётные;
  3. даже $D = \mathbb{N}$ в формальной арифметике представляет проблему.

- Будем последовательно бороться:
  1. упростим формулу (борьба с кванторами);
  2. заменим произвольное D на какое-то рекурсивно-перечислимое множество, устроенное некоторым фиксированным образом (борьба с разнообразием D);
  3. устроим правильный перебор, позволяющий быстро находить решения, если они есть (борьба с бесконечностью

Упрощаем формулу α. Сколемизация

1. Предварённая форма (поверхностные кванторы) — *для примера* возьмём чередующиеся:

$$\beta := \forall x_1.\exists x_2.\forall x_3.\exists x_4 \ldots \forall x_{n-1}.\exists x_n.\varphi$$

2. Убрать кванторы существования: заменим x_{2k} функциями Сколема $e_{2k}(x_1, x_2, \ldots, x_{2k-1})$. Получим:

$$\gamma := \forall x_1.\forall x_3 \ldots \forall x_{n-1}.\varphi[x_2 := e_2(x_1), x_4 := e_4(x_1, x_3), \ldots, x_n := e_n($$

3. ДНФ (c конъюнктов, в каждом $d(c)$ дизъюнктов):

$$\delta := \forall x_1.\forall x_3 \ldots \forall x_{n-1}. \bigwedge_c \left(\bigvee_{i=\overline{1,d(c)}} (\neg) P_i(\theta_i) \right)$$

4. $\vdash \alpha$ эквивалентно $\models \alpha$ и эквивалентно выполнимости δ при всех D (найдутся e_i, что $[\![\delta]\!] = \text{И}$).

Шаги рассуждения

1. Упростим формулу — поверхностные кванторы всеобщности, сколемизация.
2. Заменяем D.
3. Правильный перебор

Эрбранов универсум.

Определение

$H_0(\varphi)$ — все константы в формуле φ (либо особая константа a, если констант в φ нет)
$H_{k+1}(\varphi)$ — $H_k(\varphi)$ и все функции от значений $H_k(\varphi)$ (как строки)
$H = \cup H_n(\varphi)$ — основные термы.

Пример

$P(a) \vee Q(f(b))$:
$H_0 = \{a, b\}$
$H_1 = \{a, b, f(a), f(b)\}$
$H_2 = \{a, b, f(a), f(b), f(f(a)), f(f(b))\}$
...
$H = \{f^{(n)}(x) \mid n \in \mathbb{N}_0, x \in \{a, b\}\}$

Выполнимость не теряется. Заменяем D на H

Теорема

Формула выполнима тогда и только тогда, когда она выполнима на Эрбрановом универсуме.

Доказательство.

($\Rightarrow$) Пусть $M \models \forall \overline{x}.\varphi$. Тогда построим отображение $\mathrm{eval} : H \to M$ (смысл названия вдохновлён языками программирования: eval("$f(f(b))$") перейдёт в $f(f(b))$, где f и b — из M).

Предикатам дадим согласованную оценку: $P_H(t_1, \ldots, t_n) = P_M(h(t_1), \ldots, h(t_n))$. Очевидно, любая формула сохранит своё значение, кванторы всеобщности по меньшему множеству также останутся истинными.

($\Leftarrow$) Очевидно. $\square$

Противоречивость системы дизъюнктов

Определение

Система дизъюнктов $\{\delta_1, \ldots, \delta_n\}$ *противоречива, если для каждой интерпретации* M *найдётся* δ_k *и такой набор* $d_1 \ldots d_v$, *что* $[\![\delta_k]\!]^{x_1:=d_1,\ldots,x_v:=d_v} = Л$.

Теорема

Система дизъюнктов противоречива, если она невыполнима на Эрбрановом универсуме.

Доказательство.

Контрапозиция теоремы о выполнимости + разбор определения. □

Основные примеры.

Определение

Дизъюнкт с подставленными основными термами вместо переменных называется основным примером. Системой основных примеров $\mathcal{E}$ назовём множество основных примеров. А именно, рассмотрим $\delta_1 \,\&\, \delta_2 \,\&\, \cdots \,\&\, \delta_n$.

$\mathcal{E} = \{$ *все возможные основные примеры* $\delta_k \mid \mathcal{M} \not\models \delta_k, \mathcal{M}$ *из* $H \}$

Теорема

Система дизъюнктов S противоречива тогда и только тогда, когда система всевозможных основных примеров $\mathcal{E}$ противоречива

Доказательство.

Для некоторой эрбрановой интерпретации дизъюнкт δ_k опровергается тогда и только тогда, когда соответствующая ему подстановка в $\mathcal{E}$ опровергается. □

Теорема Гёделя о компактности

Теорема

Если Γ *— некоторое семейство бескванторных формул, то* Γ *имеет модель тогда и только тогда, когда любое его конечное подмножество имеет модель.*

Доказательство.

($\Leftarrow$): очевидно

($\Rightarrow$): пусть каждое конечное подмножество имеет модель.

Тогда Γ непротиворечиво:

Иначе, для любой σ выполнено $\Gamma \vdash \sigma$. В частности, для $\gamma \in \Gamma$ выполнено $\Gamma \vdash \neg\gamma$. Доказательство имеет конечную длину, и использует конечное количество формул $\gamma_1, \ldots, \gamma_n \in \Gamma$. Тогда рассмотрим $\Sigma = \{\gamma, \gamma_1, \ldots, \gamma_n\}$, и модель $\mathcal{S}$ для неё. Тогда:

1. $\models_S \gamma$ (определение модели)
2. $\models_S \neg\gamma$ (теорема о корректности: $\Sigma \vdash \neg\gamma$, значит $\Sigma \models \neg\gamma$ в любой модели)

Значит, Γ имеет модель (вспомогательная теорема к теореме Гёделя о полноте). $\square$

Теорема Эрбрана

Теорема (Эрбрана)

Система дизъюнктов S противоречива тогда и только тогда, когда существует конечное противоречивое множество основных примеров системы дизъюнктов S

Доказательство.

($\Leftarrow$) Пусть $\delta_1[\overline{x} := \overline{\theta}], \ldots, \delta_k[\overline{x} := \overline{\theta}]$ — противоречивое множество примеров дизъюнктов. Тогда интерпретация $\overline{\theta}$ опровергает хотя бы один из δ_k и система противоречива.
($\Rightarrow$) Если S противоречива, то значит, множество основных примеров S противоречиво (по теореме о выполнимости Эрбранова универсума). Тогда по теореме компактности в нём найдётся конечное противоречивое подмножество. $\square$

Шаги рассуждения

1. Упростим формулу — поверхностные кванторы всеобщности, сколемизация.
2. Упрощаем D — заменили на H, свели к перебору основных примеров.
3. Правильный перебор.

Пример: как проверяем выполнимость формулы?

Допустим, формула: $(\forall x.P(x)\ \&\ P(x'))\ \&\ \exists x.\neg P(x'''')$

1. Поверхностные кванторы, сколемизация, ДНФ:
   $(\forall x.P(x))\ \&\ (\forall x.P(x'))\ \&\ (\neg P(e))$
2. Строим Эрбранов универсум: $H = \{e, e', e'', e''', \dots\}$
3. Если есть противоречие, то среди основных примеров:

$$\mathcal{E} = \{P(e), P(e'), P(e''), P(e'''), P(e''''), \neg P(e''''), \dots\}$$

Напомним, $\mathcal{E}$ — подстановки элементов H вместо переменных под кванторами. Причём, либо $\models \&\, E$, либо противоречие достигается на конечном подмножестве (т. Эрбрана).
Добавляем по примеру и проверяем. $P(e)$ при $[\![P(e)]\!] = \text{И}$.
$P(e')$ при $[\![P(e')]\!] = \text{И}$.
...
$P(e'''')$ при $[\![P(e'''')]\!] = \text{И}$.
$\neg P(e'''')$ при $[\![P(e'''')]\!] = \text{Л}$. Противоречие.

Правило резолюции (исчисление высказываний)

Пусть даны два дизъюнкта, $\alpha_1 \vee \beta$ и $\alpha_2 \vee \neg\beta$. Тогда следующее правило вывода называется правилом резолюции:

$$\frac{\alpha_1 \vee \beta \qquad \alpha_2 \vee \neg\beta}{\alpha_1 \vee \alpha_2}$$

Теорема

Система дизъюнктов противоречива, если в процессе всевозможного применения правила резолюции будет построено явное противоречие, т.е. найдено два противоречивых дизъюнкта: β *и* $\neg\beta$.

Расширение правила резолюции на исчисление предикатов

Заметим, что правило резолюции для исчисления высказываний не подойдёт для исчисления предикатов.

$$S = \{P(x), \neg P(0)\}$$

Здесь $P(x)$ противоречит $\neg P(0)$, но правило резолюции для исчисления высказываний здесь неприменимо, потому что x можно заменять, это не константа:

$$\frac{P(x) \qquad \neg P(0)}{???}$$

Нужно заменять $P(x)$ на основные примеры, и искать среди них. Модифицируем правило резолюции для этого.

Алгебраические термы

Определение

Алгебраический терм

$$\theta := x | (f(\theta_1, \ldots, \theta_n))$$

где x — переменная, $f(\theta_1, \ldots, \theta_n)$ — применение функции. Напомним, что константы — нульместные функциональные символы, собственно переменные будем обозначать последними буквами латинского алфавита.

Определение

Система уравнений в алгебраических термах

$$\begin{cases} \theta_1 = \sigma_1 \\ \vdots \\ \theta_n = \sigma_n \end{cases}$$

где θ_i и σ_i — термы

Уравнение в алгебраических термах

Определение

$\{x_i\} = X$ — множество переменных, $\{\theta_i\} = T$ — множество термов.

Определение

Подстановка — отображение вида: $\pi_0 : X \to T$, тождественное почти везде.
$\pi_0(x)$ может быть либо $\pi_0(x) = \theta_i$, либо $\pi_0(x) = x$.

Доопределим $\pi : T \to T$, где

1. $\pi(x) = \pi_0(x)$
2. $\pi(f(\theta_1, \ldots, \theta_k)) = f(\pi(\theta_1), \ldots, \pi(\theta_k))$

Определение

Решить уравнение в алгебраических термах — найти такую наиболее общую подстановку π, что $\pi(\theta_1) = \pi(\theta_2)$. Наиболее общая подстановка — такая, для которой другие подстановки являются её частными случаями.

Задача унификации

Определение

Пусть даны формулы α и β. Тогда решением задачи унификации будет такая наиболее общая подстановка $\pi = \mathcal{U}\big[\alpha, \beta\big]$, что $\pi(\alpha) = \pi(\beta)$.
Также, η назовём наиболее общим унификатором.

Пример

- *Формулы $P(a, g(b))$ и $P(c, d)$ не имеют унификатора (мы считаем, что a, b, c, d — нульместные функции, а f — одноместная функция).*
- *Проверим формулу на соответствие 11 схеме аксиом:*

$$(\forall x.P(x)) \to P(f(t, g(t), y))$$

Пусть $\pi = \mathcal{U}\big[P(x), P(f(t, g(t), y))\big]$, тогда $\pi(x) = f(t, g(t), y)$.

Правило резолюции для исчисления предикатов

Определение

Пусть σ_1 и σ_2 — подстановки, заменяющие переменные в формуле на свежие. Тогда правило резолюции выглядит так:

$$\frac{\alpha_1 \vee \beta_1 \qquad \alpha_2 \vee \neg\beta_2}{\pi(\sigma_1(\alpha_1) \vee \sigma_2(\alpha_2))}\ \pi = \mathcal{U}\left[\sigma_1(\beta_1), \sigma_2(\beta_2)\right]$$

σ_1 и σ_2 разделяют переменные у дизъюнктов, чтобы π не осуществила лишние замены, ведь
$\vdash (\forall x.P(x)\ \&\ Q(x)) \leftrightarrow (\forall x.P(x))\ \&\ (\forall x.Q(x))$, но
$\not\vdash (\forall x.P(x) \vee Q(x)) \rightarrow (\forall x.P(x)) \vee (\forall x.Q(x))$.

Пример

$$\frac{Q(x) \vee P(x) \quad \neg P(a) \vee T(x)}{Q(a) \vee T(x'')}$$ *подстановки:* $\sigma_1(x) = x', \sigma_2(x) = x'', \pi(x$

Метод резолюции

Ищем $\vdash \alpha$.

1. будем искать опровержение $\neg\alpha$.
2. перестроим $\neg\alpha$ в ДНФ.
3. будем применять правило резолюции, пока получаем новые дизъюнкты и пока не найдём явное противоречие (дизъюнкты вида β и $\neg\beta$).

Если противоречие нашлось, значит, $\vdash \neg\neg\alpha$. Если нет — значит, $\vdash \neg\alpha$. Процесс может не закончиться.

SMT-решатели

Обычно требуется не логическое исчисление само по себе, а теория первого порядка. То есть, «Satisfability Modulo Theory», «выполнимость в теории» — вместо SAT, выполнимости.

- Иногда можно вложить теорию в логическое исчисление, даже в исчисление высказываний: $\overline{S_2 S_1 S_0} = \overline{A_1 A_0} + \overline{B_1 B_0}$

$$
\begin{array}{ll}
S_0 = A_0 \oplus B_0 & C_0 = A_0 \,\&\, B_0 \\
S_1 = A_1 \oplus B_1 \oplus C_0 & C_1 = (A_1 \,\&\, B_1) \vee (A_1 \,\&\, C_0) \vee (B_1 \,\&\, C_0) \\
S_2 = C_1 &
\end{array}
$$

- А можно что-то добавить прямо на уровень унификации / резолюции: Например, можем зафиксировать арифметические функции — и производить вычисления в правиле резолюции вместе с унификацией.
  Тогда противоречие в $\{x = 1 + 3 + 1, \neg x = 5\}$ можно найти за один шаг.

Уточнённые типы (Refinement types), LiquidHaskell

Определение

(Неформальное) Уточнённый тип — тип вида $\{\tau(x) \mid P(x)\}$*, где* P *— некоторый предикат.*

Пример на LiquidHaskell:

```
data [a] <p :: a -> a -> Prop> where
   | []  :: [a] <p>
   | (:) :: h:a -> [a<p h>]<p> -> [a]<p>
```

- `h:a` — голова (h) имеет тип a
- `[a<p h>]<p>` — хвост состоит из значений типа a, уточнённых p — $\{t : a \mid p\ h\ t\}$ (карринг: `a <p h>`).

```
{-@ type IncrList a = [a] <{\xi xj -> xi <= xj}> @-}
{-@ insertSort    :: (Ord a) => xs:[a] -> (IncrList a) @-}
insertSort []     = []
insertSort (x:xs) = insert x (insertSort xs)
```