Логика и алгоритмы

Лев Дмитриевич Беклемишев

Факультет математики НИУ ВШЭ, 2-й курс, весна 2021 г.

9.02.2020

Кризис оснований математики рубежа XIX – XX веков

- К концу XIX века математика прочно встала на теоретико-множественную основу.
- В самой теории множеств Кантора обнаружились противоречия: парадоксы Рассела, Кантора, Бурали-Форти.
- Кризис оснований математики заставил многих выдающихся ученых той эпохи (Пеано, Фреге, Рассел, Гильберт, Пуанкаре, Брауэр, Вейль и др.) задуматься о философских вопросах.

Философские вопросы

- Что означает доказать математическую теорему? Какие средства при этом законно использовать?
- Что значит дать определение тому или иному математическому понятию?
- Правомерно ли рассуждать об актуально бесконечных множествах?
- Когда мы говорим об истинности и о доказуемости какого-либо математического утверждения, имеется ли в виду одно и то же?
- Противоречива ли математика? И если нет, то каким образом это можно установить?

Направления философии математики

- Логицизм (Фреге, Рассел, Уайтхед)
- Интуиционизм (Брауэр, Вейль)
- Формализм (Гильберт)
- Платонизм (Гёдель)
- ...

Читай: С. Клини. Введение в метаматематику (начало).

Формальные аксиоматические теории

Аксиоматический метод Гильберта предполагает явную формулировку всех предположений теории и допускает лишь чисто логические выводы из этих посылок (в частности, запрещены опора на зрительную интуицию, рассуждения по аналогии и т.д.)

Логический вывод может быть записан в символьном виде,[1] что превращает его в вычислительный процесс: «игру» в переписывание логических выражений по определенным правилам. Это привело к созданию *формальных аксиоматических теорий* в начале 20-го века (Frege, Peano, Russell, Whitehead).

[1] используя логические связки $\to$ (влечет), $\&$ (и), $\neg$ (не) и кванторы $\exists$ (существует), $\forall$ (для всех).

Стандартные теории

Арифметика Пеано PA: формализует «математику конечного»; основана на аксиомах для натуральных чисел с операциями $+$ и $\cdot$.

Теория множеств Цермело – Френкеля ZFC: формализует *всю* обычную математику; основана на аксиомах для множеств и отношения принадлежности.

Арифметика второго порядка PA^2*:* формализует бóльшую часть анализа. Основана на аксиомах для натуральных чисел и подмножеств $\mathbb{N}$.

Компьютерная реализация

Формальные теории реализованы в различных системах *автоматического* и *интерактивного поиска вывода*, таких как Coq, HOL или Mizar.

- В системе Coq была получена формальная верификация гипотезы четырех красок (Gonthier).
- В системе HOL получено формальное доказательство гипотезы Кеплера об оптимальной упаковке шаров (Hales).

Бурно развивающаяся область CS.

Программа Гильберта

- Формализовать математику (теорию множеств) в рамках формальной аксиоматической теории T.
- Формальные доказательства в T представляют собой конечные объекты (строки символов), строящиеся по вполне определенным правилам.
- Их следует проанализировать элементарными комбинаторными средствами («финитными средствами», не опирающимися на актуально бесконечные множества) и установить, что противоречие в T не доказуемо.
- Тем самым мы сведем использование теоретико-множественных методов к заведомо надежным элементарным методам.

О чем математическая логика?

Математическая логика — построение и исследование формальных языков математическими методами.
(Формальные языки могут быть самыми разными, в том числе не имеющими отношения к формализации математики.)

- *Метаязык* — язык, на котором мы описываем изучаемый нами (формальный) язык.
- *Метатеория* — теория, в рамках которой мы рассуждаем об исследуемой нами теории.
- *Синтаксис* — правила построения выражений языка.
- *Семантика* — значение (смысл) выражений языка; то, что этот язык описывает.

План дальнейшего в этом модуле

1. Логика высказываний (связки $\wedge$, $\vee$, $\to$, $\neg$)
2. Логика предикатов (кванторы $\forall$, $\exists$)
3. Основы теории моделей

Предикаты и функции

Пусть M — непустое множество.

- *n-арный предикат на M*: функция $Q : M^n \to \{0,1\}$ (Интуитивно: $Q(x_1,\ldots,x_n)$ есть высказывание, зависящее от выбора параметров $x_1,\ldots,x_n \in M$. Предикаты можно также понимать как n-арные отношения на M, то есть подмножества M^n.)
- *n-арная функция на M*: функция $f : M^n \to M$
- *константа*: элемент M

Опр.

Сигнатурой называется некоторая совокупность имён функций, предикатов и констант. Сигнатура Σ задаётся:

- Pred_{Σ} предикатные символы;
- Func_{Σ} функциональные символы;
- Const_{Σ} символы констант;
- функция *валентности* (число аргументов):

$$\mathrm{Pred}_{\Sigma} \cup \mathrm{Func}_{\Sigma} \to \mathbb{N} \setminus \{0\}.$$

Модели

Опр.

Модель сигнатуры Σ есть непустое множество M вместе с отображением (*интерпретацией*), сопоставляющим

- каждому $P \in \mathrm{Pred}_\Sigma$ некоторый предикат P_M на M той же валентности;
- каждому $f \in \mathrm{Func}_\Sigma$ функцию f_M на M той же валентности;
- каждому $c \in \mathrm{Const}_\Sigma$ константу $c_M \in M$.

- Модели называют также *алгебраическими системами* или *интерпретациями*.
- Множество M называют *носителем* или *универсумом* данной интерпретации (модели).
- Модель сигнатуры Σ с носителем M обозначается $(M; \Sigma)$ (если интерпретация символов сигнатуры известна).

Примеры

Пример.

Стандартная модель арифметики:
$(\mathbb{N}; =, S, +, \times, 0)$

- $S(x) \rightleftharpoons x + 1$ есть одноместная функция следования;
- $+$ бинарная функция сложения;
- $\times$ бинарная функция умножения;
- 0 константа ноль.

Пример.

Кольцо целых чисел:
$(\mathbb{Z}; =, +, -, \times, 0, 1)$
Здесь «$-$» есть одноместная функция $x \mapsto -x$.

Пример.

Любое другое кольцо может рассматриваться как модель той же сигнатуры, например:

- $\mathbb{Q}[X]$ — кольцо многочленов над полем $\mathbb{Q}$;
- $\mathbb{Z}_n$ — кольцо вычетов по модулю n;
- $M_n(\mathbb{R})$ — кольцо матриц порядка n над $\mathbb{R}$.

Пример.

Элементарная геометрия плоскости:

$(\mathbb{R}^2; =, \cong, B)$, где

- $\mathbb{R}^2$ — множество точек евклидовой плоскости;
- $B(a, b, c)$ — трёхместный предикат «*точка b лежит на прямой ac между точками a и c*»;
- $\cong$ — четырёхместный предикат $ab \cong cd$ «*отрезки, задаваемые парами точек ab и cd, имеют равные длины*».

Пример.

Модель Пуанкаре геометрии Лобачевского:

$(\mathsf{H}^2; =, \cong, B)$, где

- $\mathsf{H}^2 \rightleftharpoons \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ — множество точек верхней евклидовой полуплоскости;
- $B(a, b, c)$ — трёхместный предикат «*точка b лежит между точками a и c на полуокружности (или полупрямой), проходящей через a, c и ортогональной вещественной оси*»;

- $\cong$ — четырёхместный предикат (записываемый $ab \cong cd$)

  «*пару точек ab можно перевести в cd последовательностью инверсий (отражений) относительно окружностей (прямых), ортогональных вещественной оси*»

Пример.

Частично упорядоченные множества

1. $(\mathcal{P}(U); \subseteq)$, где U — любое множество;
2. $(\mathbb{Z}; |)$, где $a \mid b$ — бинарное отношение «быть делителем».

Пример.

Графы можно рассматривать как модели $(V; E, =)$, где V — множество вершин, а E — симметричное бинарное отношение «смежности».

Пример.

Упорядоченное поле действительных чисел:
$(\mathbb{R}; =, <, +, -, \times, 0, 1)$

Пример.

Векторное пространство над полем F можно рассматривать как модель $(V; =, +, 0, (f_\lambda)_{\lambda \in F})$, где $f_\lambda(x) \rightleftharpoons \lambda x$ для всех $x \in F$.

Синтаксис логики первого порядка

Алфавит языка $\mathcal{L}_\Sigma$ содержит:

Символы сигнатуры: Σ;

Свободные переменные: $\mathsf{FrVar} = \{a_0, a_1, a_2, \dots\}$,

Связанные переменные: $\mathsf{BdVar} = \{v_0, v_1, v_2, \dots\}$,

Булевы связки: $\to$, $\neg$, $\wedge$, $\vee$;

Кванторы: $\forall$ (квантор всеобщности, «для всех»);
$\exists$ (квантор существования, «существует»);

Знаки пунктуации: «(», «)» и «,».

Термы

Опр.

Множество *термов* Tm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

1. Свободные переменные и константы суть термы.
2. Если $f \in \mathrm{Func}_\Sigma$ валентности n и $t_1, \ldots, t_n$ — термы, то выражение $f(t_1, \ldots, t_n)$ есть терм.

Пример.

Если $f \in \mathrm{Func}_\Sigma$ — бинарный функциональный символ, то $f(a_0, a_1)$ и $f(f(a_5, a_0), a_1)$ — термы, а $f(v_0, a_1)$ — не терм.

Формулы

Опр.

Множество формул Fm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

- Если $P \in \mathrm{Pred}_\Sigma$ валентности n и $t_1, \ldots, t_n$ — термы, то $P(t_1, \ldots, t_n)$ есть формула (называемая *атомарной формулой*).
- Если A, B — формулы, то формулами являются $(A \to B)$, $\neg A$, $(A \land B)$, $(A \lor B)$.

- Если A — формула, и a — свободная переменная, то для любой связанной переменной x, не входящей в A, выражения $(\forall x\ A[a/x])$ и $(\exists x\ A[a/x])$ — формулы.

(Здесь $A[a/x]$ означает результат замены всех вхождений a в A на x.)

Пример.

$P(f(a_0, a_1))$ и $(\forall v_0(\forall v_1 P(f(v_0, v_1))))$ — формулы,
$(\forall v_0(\forall v_0 P(f(v_0, v_0))))$ — не формула.

Опр.

- Формулы, в которые не входят кванторы, называются *бескванторными*.
- Формулы и термы, в которые не входят свободные переменные, называются *замкнутыми*.
- Замкнутые формулы также называются *предложениями*.

Сокращения

- соглашения об опускании скобок;
- сокращения для логических связок;
- пишут a, b, c вместо a_0, a_1, a_2 и т.д.; x, y, z вместо v_0, v_1, v_2 и т.д.;
- пишут $\forall x_1 \ldots x_n\, A$ вместо $(\forall x_1(\forall x_2(\ldots(\forall x_n A)\ldots)))$ и аналогично для последовательностей кванторов $\exists$.
- пишут $a = b$ вместо $=(a, b)$,
- $a + b$ вместо $+(a, b)$;
- и т.д.

Семантика логики первого порядка

Пусть M — модель сигнатуры Σ. Обозначим через $\Sigma(M)$ сигнатуру, получаемую из Σ добавлением новых символов констант для всех элементов M, то есть $\{\underline{c} : c \in M\}$.

Значение терма в модели

Опр.

Пусть t — замкнутый терм сигнатуры $\Sigma(M)$. *Значение t в модели M* есть элемент $t_M \in M$, определяемый индукцией по построению t.

1. Если $a \in M$, то $\underline{a}_M \rightleftharpoons a$.
2. Если $c \in \mathrm{Const}_\Sigma$, то $c_M \in M$ есть данная нам интерпретация c.
3. Если t есть $f(t_1, \ldots, t_n)$, где $f \in \mathrm{Func}_\Sigma$, то $t_M \rightleftharpoons f_M((t_1)_M, \ldots, (t_n)_M)$.

Истинность формулы в модели

Опр.

Пусть A — замкнутая формула сигнатуры $\Sigma(M)$. Отношение $M \vDash A$ «*формула A истинна в модели M*» определяется индукцией по построению A.

- $M \vDash P(t_1, \ldots, t_n) \overset{\text{def}}{\Longleftrightarrow} P_M((t_1)_M, \ldots, (t_n)_M)$, если $A = P(t_1, \ldots, t_n)$ — атомарная формула;

Стандартные определения для булевых связок:

- $M \models (B \to C) \overset{\text{def}}{\iff} (M \not\models B$ **или** $M \models C)$;
- $M \models \neg B \overset{\text{def}}{\iff} M \not\models B$;
- $M \models (A \wedge B) \overset{\text{def}}{\iff} (M \models A$ **и** $M \models B)$;
- $M \models (A \vee B) \overset{\text{def}}{\iff} (M \models A$ **или** $M \models B)$;

Кванторы:

- $M \vDash (\forall x A[a/x]) \overset{\text{def}}{\Longleftrightarrow}$ для всех $c \in M$ $M \vDash A[a/\underline{c}]$;
- $M \vDash (\exists x A[a/x]) \overset{\text{def}}{\Longleftrightarrow}$ существует $c \in M$ $M \vDash A[a/\underline{c}]$.

Логика предикатов
лекция 2

Лев Дмитриевич Беклемишев

lbekl@yandex.ru

16.02.2021

Синтаксис логики первого порядка

Алфавит языка $\mathcal{L}_\Sigma$ содержит:

Символы сигнатуры: Σ;

Свободные переменные: $\mathsf{FrVar} = \{a_0, a_1, a_2, \dots\}$,

Связанные переменные: $\mathsf{BdVar} = \{v_0, v_1, v_2, \dots\}$,

Булевы связки: $\to$, $\neg$, $\wedge$, $\vee$;

Кванторы: $\forall$ (квантор всеобщности, «для всех»);
$\exists$ (квантор существования, «существует»);

Знаки пунктуации: «(», «)» и «,».

Термы

Опр.

Множество *термов* Tm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

1. Свободные переменные и константы суть термы.
2. Если $f \in \mathrm{Func}_\Sigma$ валентности n и $t_1, \ldots, t_n$ — термы, то выражение $f(t_1, \ldots, t_n)$ есть терм.

Пример.

Если $f \in \mathrm{Func}_\Sigma$ — бинарный функциональный символ, то $f(a_0, a_1)$ и $f(f(a_5, a_0), a_1)$ — термы, а $f(v_0, a_1)$ — не терм.

Формулы

Опр.

Множество формул Fm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

- Если $P \in \mathrm{Pred}_\Sigma$ валентности n и $t_1, \ldots, t_n$ — термы, то $P(t_1, \ldots, t_n)$ есть формула (называемая *атомарной формулой*).
- Если A, B — формулы, то формулами являются $(A \to B)$, $\neg A$, $(A \wedge B)$, $(A \vee B)$.

- Если A — формула, и a — свободная переменная, то для любой связанной переменной x, не входящей в A, выражения $(\forall x\, A[a/x])$ и $(\exists x\, A[a/x])$ — формулы.

(Здесь $A[a/x]$ означает результат замены всех вхождений a в A на x.)

Опр.

- Формулы, в которые не входят кванторы, называются *бескванторными*.
- Формулы и термы, в которые не входят свободные переменные, называются *замкнутыми*.
- Замкнутые формулы также называются *предложениями*.

Семантика логики первого порядка

Пусть M — модель сигнатуры Σ. Обозначим через $\Sigma(M)$ сигнатуру, получаемую из Σ добавлением новых символов констант для всех элементов M, то есть $\{\underline{c} : c \in M\}$.

Значение терма в модели

Опр.

Пусть t — замкнутый терм сигнатуры $\Sigma(M)$. *Значение t в модели M* есть элемент $t_M \in M$, определяемый индукцией по построению t.

1. Если $a \in M$, то $\underline{a}_M \rightleftharpoons a$.
2. Если $c \in \mathrm{Const}_\Sigma$, то $c_M \in M$ есть данная нам интерпретация c.
3. Если t есть $f(t_1, \ldots, t_n)$, где $f \in \mathrm{Func}_\Sigma$, то $t_M \rightleftharpoons f_M((t_1)_M, \ldots, (t_n)_M)$.

Пример.

Значение терма $S(S(0)) + S(S(0))$ в стандартной модели арифметики есть 4.

Значение терма $\underline{\sqrt{2}} \cdot \underline{\sqrt{2}}$ в поле $\mathbb{R}$ есть 2.

Истинность формулы в модели

Опр.

Пусть A — замкнутая формула сигнатуры $\Sigma(M)$. Отношение $M \vDash A$ «*формула A истинна в модели M*» определяется индукцией по построению A.

- $M \vDash P(t_1, \ldots, t_n) \overset{\text{def}}{\Longleftrightarrow} P_M((t_1)_M, \ldots, (t_n)_M) = 1$, если $A = P(t_1, \ldots, t_n)$ — атомарная формула;

Стандартные определения для булевых связок:

- $M \models (B \to C) \overset{\text{def}}{\iff} (M \not\models B \text{ или } M \models C)$;
- $M \models \neg B \overset{\text{def}}{\iff} M \not\models B$;
- $M \models (A \wedge B) \overset{\text{def}}{\iff} (M \models A \text{ и } M \models B)$;
- $M \models (A \vee B) \overset{\text{def}}{\iff} (M \models A \text{ или } M \models B)$;

Кванторы:

- $M \vDash (\forall x A[a/x]) \overset{\text{def}}{\iff}$ для всех $c \in M$ $M \vDash A[a/\underline{c}]$;
- $M \vDash (\exists x A[a/x]) \overset{\text{def}}{\iff}$ существует $c \in M$ $M \vDash A[a/\underline{c}]$.

Замечание.
Нельзя говорить об истинности или ложности незамкнутых формул, поскольку их истинностные значения зависят от выбора значений параметров — входящих в формулу свободных переменных.

Пример: формула $a + 1 = b$ в стандартной модели арифметики может быть как истинна, так и ложна, в зависимости от значений a и b.

Сокращение: вместо

$$M \vDash A[a_1/\underline{c}_1, \ldots a_n/\underline{c}_n]$$

пишут

$$M \vDash A[a_1/c_1, \ldots a_n/c_n]$$

или даже

$$M \vDash A[c_1, \ldots c_n]$$

.

Примеры

Пример.

В модели $(\mathbb{N}; =, S, +, \cdot, 0)$ истинна формула

$\exists x, y, z\,(\neg x = 0 \wedge \neg y = 0 \wedge x \cdot x + y \cdot y = z \cdot z)$

и ложна формула

$\exists x, y, z\,(\neg x = 0 \wedge \neg y = 0 \wedge x \cdot x \cdot x + y \cdot y \cdot y = z \cdot z \cdot z)$

Пример.

В модели $(\mathbb{R}^2; =, \cong, B)$ истинна формула

$$\forall x, y, y', z\, (B(x, y, z) \wedge B(x, y', z) \to B(x, y, y') \vee B(x, y', y)).$$

Эта же формула верна и в модели $(\mathrm{H}^2; =, \cong, B)$.

Определимость в модели

Любая формула A от свободных переменных $b_1, \ldots, b_n$ определяет n-местный предикат A_M в модели M:

$$A_M(x_1, \ldots, x_n) = 1 \overset{\text{def}}{\iff} M \models A[b_1/x_1, \ldots, b_n/x_n].$$

Пример.

В модели $(\mathbb{N}; =, +)$ формула $\exists x\, (x + x = a)$ определяет предикат «a чётно», т.е. множество чётных чисел.

Опр.

Предикат $P(x_1, \ldots, x_n)$ называется *определимым в модели* $(M; \Sigma)$, если $P = A_M$ для некоторой формулы A языка $\mathcal{L}_\Sigma$.

Опр.

Функция f называется *определимой в модели* M, если определим её график, то есть предикат
$G_f(x_1, \ldots, x_n, y) \overset{\text{def}}{\Longleftrightarrow} f(x_1, \ldots, x_n) = y.$

Пример.

В модели $(\mathbb{Z}; \leq)$ предикат $b = a + 1$ определим формулой

$$\neg\, b \leq a \wedge \forall x\, (x \leq a \vee b \leq x).$$

Следовательно, функция $s(x) \rightleftharpoons x + 1$ определима в $(\mathbb{Z}; \leq)$.

Аксиома о параллельных

Определим следующие предикаты в $(\mathbb{R}^2; =, \cong, B)$

- $a \neq b \rightleftharpoons \neg\, a = b$
- $c \in ab$ «c лежит на прямой ab»
  $c \in ab \rightleftharpoons (B(c,a,b) \vee B(a,c,b) \vee B(a,b,c))$
- $ab \| cd$ «прямые ab и cd параллельны»
  $ab \| cd \rightleftharpoons a \neq b \wedge c \neq d \wedge \neg\exists x\, (x \in ab \wedge x \in cd)$

Аксиома о параллельных

«*Через точку* z *вне прямой* xy *можно провести не более одной прямой, параллельной данной.*»

$$\forall x, y, z\,(x \neq y \wedge \neg\, z \in xy \to \forall u, v\,(zu \| xy \wedge zv \| xy \to v \in zu))$$

Верно в $\mathbb{R}^2$, но не в H^2.

Выполнимость и общезначимость

Опр.

Формула $A(b_1, \ldots, b_n)$ сигнатуры Σ *выполнима в модели* (M, Σ), если для некоторых констант $c_1, \ldots, c_n \in M$ предложение $A[b_1/\underline{c}_1, \ldots, b_n/\underline{c}_n]$ (сигнатуры $\Sigma(M)$) истинно.

Формула A сигнатуры Σ *выполнима*, если она выполнима в некоторой модели (M, Σ).

Опр.

Формула A *общезначима* (*тождественно истинна*), если $\neg A$ не выполнима.

Опр.

Формула A *тождественно ложна*, если A не выполнима.

Пример.

Формулы $P(a) \vee \neg P(a)$, $\exists x \forall y A(x, y) \to \forall y \exists x\, A(x, y)$ общезначимы. Формула $P(a_0) \to P(a_1)$ выполнима, но не общезначима.

Важность понятия общезначимости

- Общезначимые формулы представляют собой *универсальные законы логики*, истинные вне зависимости от предметной области и интерпретации входящих в них предикатных символов.
- Логическое следование утверждения B из утверждений $A_1, \ldots, A_n$ сводится к проверке общезначимости формулы $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$.
- *Entscheidungsproblem*: найти алгоритм, определяющий по данной формуле A, общезначима ли она. Гильберт считал этот вопрос важнейшей математической проблемой.

Важность понятия общезначимости

- Общезначимые формулы представляют собой *универсальные законы логики*, истинные вне зависимости от предметной области и интерпретации входящих в них предикатных символов.
- Логическое следование утверждения B из утверждений $A_1, \ldots, A_n$ сводится к проверке общезначимости формулы $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$.
- *Entscheidungsproblem*: найти алгоритм, определяющий по данной формуле A, общезначима ли она. Гильберт считал этот вопрос важнейшей математической проблемой.

Важность понятия общезначимости

- Общезначимые формулы представляют собой *универсальные законы логики*, истинные вне зависимости от предметной области и интерпретации входящих в них предикатных символов.
- Логическое следование утверждения B из утверждений $A_1, \dots, A_n$ сводится к проверке общезначимости формулы $A_1 \wedge A_2 \wedge \dots \wedge A_n \to B$.
- *Entscheidungsproblem*: найти алгоритм, определяющий по данной формуле A, общезначима ли она. Гильберт считал этот вопрос важнейшей математической проблемой.

Теория алгоритмов и теория доказательств

- А. Чёрч (1935) и А. Тьюринг (1936) независимо показали, что такого алгоритма не существует. Для этого потребовалось сначала дать точное определение понятия *алгоритма*.
- Тем не менее, конструктивное описание множества общезначимых формул можно дать: *исчисление предикатов*. Это исчисление даёт формальную модель математического *доказательства*.

Логика высказываний

- Пропозициональные переменные: $\mathrm{Var} = \{P_0, P_1, \dots\}$.
- Связки: $\neg, \wedge, \vee, \to$; константы $\bot$ (ложь), $\top$ (истина).
- Формулы Fm строятся по правилам:
  1. Если $P \in \mathrm{Var}$ или $P \in \{\top, \bot\}$, то P — формула;
  2. Если A и B — формулы, то $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — формулы.
- Fm есть наименьшее множество, удовлетворяющее условиям 1 и 2.

Логика высказываний

- Пропозициональные переменные: $\mathrm{Var} = \{P_0, P_1, \dots\}$.
- Связки: $\neg, \wedge, \vee, \to$; константы $\bot$ (ложь), $\top$ (истина).
- Формулы Fm строятся по правилам:

  1. Если $P \in \mathrm{Var}$ или $P \in \{\top, \bot\}$, то P — формула;
  2. Если A и B — формулы, то $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — формулы.

- Fm есть наименьшее множество, удовлетворяющее условиям 1 и 2.

Логика высказываний

- Пропозициональные переменные: $\mathrm{Var} = \{P_0, P_1, \ldots\}$.
- Связки: $\neg$,$\wedge$,$\vee$,$\to$; константы $\bot$ (ложь), $\top$ (истина).
- Формулы Fm строятся по правилам:

  1. Если $P \in \mathrm{Var}$ или $P \in \{\top, \bot\}$, то P — формула;
  2. Если A и B — формулы, то $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — формулы.

- Fm есть наименьшее множество, удовлетворяющее условиям 1 и 2.

Логика высказываний

- Пропозициональные переменные: $\mathrm{Var} = \{P_0, P_1, \dots\}$.
- Связки: $\neg, \wedge, \vee, \to$; константы $\bot$ (ложь), $\top$ (истина).
- Формулы Fm строятся по правилам:

  1. Если $P \in \mathrm{Var}$ или $P \in \{\top, \bot\}$, то P — формула;
  2. Если A и B — формулы, то $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — формулы.

- Fm есть наименьшее множество, удовлетворяющее условиям 1 и 2.

Лемма об однозначном прочтении

Лемма.
Любая формула F, отличная от переменной или константы, однозначно представляется в виде $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ или $(\neg A)$ для некоторых формул A, B.

Доказательство.
Соображения баланса скобок в формуле.

Опр.

- A и B называются *непосредственными подформулами* F;
- G — *подформула* F, если $G \mathrel{\hat{=}} F$ или G — подформула одной из непосредственных подформул F.

Лемма об однозначном прочтении

Лемма.
Любая формула F, отличная от переменной или константы, однозначно представляется в виде $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ или $(\neg A)$ для некоторых формул A, B.

Доказательство.
Соображения баланса скобок в формуле.

Опр.

- A и B называются *непосредственными подформулами* F;
- G — *подформула* F, если $G \triangleq F$ или G — подформула одной из непосредственных подформул F.

Лемма об однозначном прочтении

Лемма.
Любая формула F, отличная от переменной или константы, однозначно представляется в виде $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ или $(\neg A)$ для некоторых формул A, B.

Доказательство.
Соображения баланса скобок в формуле.

Опр.

- A и B называются *непосредственными подформулами* F;
- G — *подформула* F, если $G \triangleq F$ или G — подформула одной из непосредственных подформул F.

Соглашения об опускании скобок

- Опускаем внешние скобки;
- Приоритет связок: $\neg$, $\wedge$, $\vee$, $\to$;
  $\neg P \wedge Q \to R$ читается как $(((\neg P) \wedge Q) \to R)$;
- Кратные $\wedge$ и $\vee$ ассоциируем влево:
  $A \wedge B \wedge C$ читается как $((A \wedge B) \wedge C)$.

Семантика логики высказываний

Опр.

Истинностные значения: $\mathbb{B} \rightleftharpoons \{\text{Л}, \text{И}\} \rightleftharpoons \{0, 1\}$.
Булевы функции: $f : \mathbb{B}^n \to \mathbb{B}$.

Таблицы истинности

Функции $f : \mathbb{B}^n \to \mathbb{B}$ принято задавать *таблицами истинности* вида

x_1	x_2	$\dots$	x_n	$f(x_1, x_2, \dots, x_n)$
0	0	$\dots$	0	$f(0, 0, \dots, 0)$
0	0	$\dots$	1	$f(0, 0, \dots, 1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
1	1	$\dots$	1	$f(1, 1, \dots, 1)$

В такой таблице 2^n строк.

Оценка и значение формулы

Опр.

Оценка переменных: функция $f : \mathrm{Var} \to \mathbb{B}$.

Любая оценка продолжается естественным образом до отображения $f : \mathsf{Fm} \to \mathbb{B}$.

Опр.

$f(A) =$ *значение* формулы A при оценке f.
Определяется индукцией по построению A:

Значение $f(A)$ определяется индукцией по построению A:

$$
\begin{aligned}
&f(\top) = 1;\ \ f(\bot) = 0;\\
&f(\neg A) = 1 - f(A);\\
&f(A \wedge B) = \min(f(A), f(B));\\
&f(A \vee B) = \max(f(A), f(B));\\
&f(A \to B) = \max(1 - f(A), f(B)).
\end{aligned}
$$

В частности, $f(A \to B) = 1 \iff f(A) \leq f(B)$.

Значение $f(A)$ определяется индукцией по построению A:

$$
\begin{aligned}
& f(\top) = 1;\ \ f(\bot) = 0; \\
& f(\neg A) = 1 - f(A); \\
& f(A \wedge B) = \min(f(A), f(B)); \\
& f(A \vee B) = \max(f(A), f(B)); \\
& f(A \to B) = \max(1 - f(A), f(B)).
\end{aligned}
$$

В частности, $f(A \to B) = 1 \iff f(A) \leq f(B)$.

То же самое другими словами:

$$
\begin{aligned}
f(\neg A) = \text{И} &\iff f(A) = \text{Л};\\
f(A \wedge B) = \text{И} &\iff f(A) = \text{И и } f(B) = \text{И};\\
f(A \vee B) = \text{И} &\iff f(A) = \text{И или } f(B) = \text{И};\\
f(A \to B) = \text{И} &\iff f(A) = \text{Л или } f(B) = \text{И}.
\end{aligned}
$$

Утверждение.

Пусть $\mathrm{Var} = \{P_1, \ldots, P_n\}$.
Тогда существует взаимно-однозначное соответствие между оценками $f : \mathrm{Var} \to \mathbb{B}$ и наборами $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$.

$f \longmapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{B}^n$

$\vec{x} = (x_1, \ldots, x_n) \longmapsto f_{\vec{x}}$, где оценка $f_{\vec{x}}$ определена таблицей

P_1	P_2	$\ldots$	P_n
x_1	x_2	$\ldots$	x_n

Утверждение.

Пусть $\mathrm{Var} = \{P_1, \ldots, P_n\}$.
Тогда существует взаимно-однозначное соответствие между оценками $f : \mathrm{Var} \to \mathbb{B}$ и наборами $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$.

$$f \longmapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{B}^n$$

$\vec{x} = (x_1, \ldots, x_n) \longmapsto f_{\vec{x}}$, где оценка $f_{\vec{x}}$ определена таблицей

P_1	P_2	$\ldots$	P_n
x_1	x_2	$\ldots$	x_n

Таблицы истинности формул

Опр.

Таблица истинности формулы A от n переменных есть булева функция $\varphi_A : \mathbb{B}^n \to \mathbb{B}$ такая, что

$$\varphi_A(\vec{x}) = f_{\vec{x}}(A),$$

для всех $\vec{x} \in \mathbb{B}^n$.

Функциональная полнота

Теорема.

Для любой функции $\varphi : \mathbb{B}^n \to \mathbb{B}$ *найдётся такая формула* A *от* n *переменных, что* $\varphi = \varphi_A$. *При этом можно считать, что* A *содержит лишь связки* $\neg$ *и* $\vee$.

Доказательство.

Для $x \in \mathbb{B}$ положим

$$P^x = \begin{cases} P, & \text{если } x = \text{И};\\ \neg P, & \text{если } x = \text{Л}. \end{cases}$$

Для $\vec{x} = (x_1, \dots, x_n) \in \mathbb{B}^n$ обозначим

$$A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i},$$

где $\bigwedge_{j=1}^{m} B_j \rightleftharpoons ((B_1 \wedge B_2) \wedge \dots \wedge B_m)$.

Доказательство.

Для $x \in \mathbb{B}$ положим

$$P^x = \begin{cases} P, & \text{если } x = \text{И}; \\ \neg P, & \text{если } x = \text{Л}. \end{cases}$$

Для $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ обозначим

$$A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i},$$

где $\bigwedge_{j=1}^{m} B_j \rightleftharpoons ((B_1 \wedge B_2) \wedge \cdots \wedge B_m)$.

Доказательство.

Для $x \in \mathbb{B}$ положим

$$P^x = \begin{cases} P, & \text{если } x = \text{И}; \\ \neg P, & \text{если } x = \text{Л}. \end{cases}$$

Для $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ обозначим

$$A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i},$$

где $\bigwedge_{j=1}^{m} B_j \rightleftharpoons ((B_1 \wedge B_2) \wedge \cdots \wedge B_m)$.

Имеем: для любой оценки f

$$f(A_{\vec{x}}) = \text{И} \iff f = f_{\vec{x}}. \tag{1}$$

Пусть список $\vec{x}_1, \ldots, \vec{x}_m$ исчерпывает все $\vec{x} \in \mathbb{B}^n$ для которых $\varphi(\vec{x}) = \text{И}$, то есть

$$\varphi(\vec{x}) = \text{И} \iff \exists j \ \vec{x} = \vec{x}_j. \tag{2}$$

Положим

$$A \rightleftharpoons \bigvee_{j=1}^{m} A_{\vec{x}_j}.$$

Имеем: для любой оценки f

$$f(A_{\vec{x}}) = \text{И} \iff f = f_{\vec{x}}. \tag{1}$$

Пусть список $\vec{x}_1, \ldots, \vec{x}_m$ исчерпывает все $\vec{x} \in \mathbb{B}^n$ для которых $\varphi(\vec{x}) = \text{И}$, то есть

$$\varphi(\vec{x}) = \text{И} \iff \exists j \ \vec{x} = \vec{x}_j. \tag{2}$$

Положим

$$A \rightleftharpoons \bigvee_{j=1}^{m} A_{\vec{x}_j}.$$

Тогда

$$\begin{aligned} f_{\vec{x}}(A) = И \quad &\iff \quad \exists j\ f_{\vec{x}}(A_{\vec{x}_j}) = И \\ &\iff \quad \exists j\ \vec{x} = \vec{x}_j \quad \text{по } (1) \\ &\iff \quad \varphi(\vec{x}) = И \quad \text{по } (2). \end{aligned}$$

Значит, $\varphi_A(\vec{x}) = f_{\vec{x}}(A) = \varphi(\vec{x})$. $\boxtimes$

Тогда

$$\begin{aligned} f_{\vec{x}}(A) = \text{И} \quad &\Longleftrightarrow \quad \exists j \ f_{\vec{x}}(A_{\vec{x}_j}) = \text{И} \\ &\Longleftrightarrow \quad \exists j \ \vec{x} = \vec{x}_j \quad \text{по (1)} \\ &\Longleftrightarrow \quad \varphi(\vec{x}) = \text{И} \quad \text{по (2)}. \end{aligned}$$

Значит, $\varphi_A(\vec{x}) = f_{\vec{x}}(A) = \varphi(\vec{x})$. $\boxtimes$

Тогда

$$\begin{aligned} f_{\vec{x}}(A) = \text{И} \quad &\Longleftrightarrow \quad \exists j \ f_{\vec{x}}(A_{\vec{x}_j}) = \text{И} \\ &\Longleftrightarrow \quad \exists j \ \vec{x} = \vec{x}_j \quad \text{по (1)} \\ &\Longleftrightarrow \quad \varphi(\vec{x}) = \text{И} \quad \text{по (2)}. \end{aligned}$$

Значит, $\varphi_A(\vec{x}) = f_{\vec{x}}(A) = \varphi(\vec{x})$. ⊠

Тогда

$$\begin{aligned} f_{\vec{x}}(A) = \text{И} \quad &\Longleftrightarrow \quad \exists j \ f_{\vec{x}}(A_{\vec{x}_j}) = \text{И} \\ &\Longleftrightarrow \quad \exists j \ \vec{x} = \vec{x}_j \quad \text{по } (1) \\ &\Longleftrightarrow \quad \varphi(\vec{x}) = \text{И} \quad \text{по } (2). \end{aligned}$$

Значит, $\varphi_A(\vec{x}) = f_{\vec{x}}(A) = \varphi(\vec{x})$. $\boxtimes$

Выполнимые формулы и тавтологии

Опр.

Формула A *выполнима*, если $\exists f: \ f(A) = \text{И}$.

Опр.

Формула A — *тавтология*, если $\forall f \ f(A) = \text{И}$.

Опр.

Формула A — *тождественно ложна*, если $\forall f \ f(A) = \text{Л}$.

Предложение.

Следующие условия равносильны.

1. *Формула A тождественно ложна.*
2. *Формула A не выполнима.*
3. *Формула $\neg A$ — тавтология.*

Пример.

$\neg(P \to P)$ тождественно ложна (и не выполнима); $P \to P$ тавтология; $P \to Q$ выполнима, но не тавтология.

Проверка формулы на выполнимость

Очевидный алгоритм — перебор всех 2^n возможных оценок.

Открытый вопрос: существует ли алгортм, проверяющий формулу на выполнимость за полиномиальное число шагов (от длины формулы).

Проверка формулы на выполнимость — стандартный пример NP-полной задачи, поэтому этот вопрос эквивалентен знаменитой проблеме P=NP?.

Логика предикатов
лекция 3

Лев Дмитриевич Беклемишев

lbekl@yandex.ru

22.02.2021

Эквивалентность формул

Опр.

Формула $A(b_1, \ldots, b_n)$ сигнатуры Σ *общезначима*, если для любой модели $(M; \Sigma)$ и любых констант $c_1, \ldots, c_n \in M$
$M \vDash A[b_1/\underline{c}_1, \ldots, b_n/\underline{c}_n]$.

Опр.

Формулы A и B сигнатуры Σ *равносильны* (обозначение $A \equiv B$), если в любой модели $(M; \Sigma)$ они определяют один и тот же предикат, то есть если $A_M = B_M$.

Утверждение.

$A \equiv B \iff$ *формула* $A \leftrightarrow B$ *общезначима.*

$A \leftrightarrow B$ есть сокращение для $(A \to B) \wedge (B \to A)$.

Эквивалентность формул

Опр.

Формула $A(b_1, \ldots, b_n)$ сигнатуры Σ *общезначима*, если для любой модели $(M; \Sigma)$ и любых констант $c_1, \ldots, c_n \in M$
$M \models A[b_1/\underline{c}_1, \ldots, b_n/\underline{c}_n]$.

Опр.

Формулы A и B сигнатуры Σ *равносильны* (обозначение $A \equiv B$), если в любой модели $(M; \Sigma)$ они определяют один и тот же предикат, то есть если $A_M = B_M$.

Утверждение.

$A \equiv B \iff$ *формула* $A \leftrightarrow B$ *общезначима.*

$A \leftrightarrow B$ есть сокращение для $(A \to B) \wedge (B \to A)$.

Эквивалентность формул

Опр.

Формула $A(b_1, \ldots, b_n)$ сигнатуры Σ *общезначима*, если для любой модели $(M; \Sigma)$ и любых констант $c_1, \ldots, c_n \in M$ $M \vDash A[b_1/\underline{c}_1, \ldots, b_n/\underline{c}_n]$.

Опр.

Формулы A и B сигнатуры Σ *равносильны* (обозначение $A \equiv B$), если в любой модели $(M; \Sigma)$ они определяют один и тот же предикат, то есть если $A_M = B_M$.

Утверждение.

$A \equiv B \iff$ *формула* $A \leftrightarrow B$ *общезначима.*

$A \leftrightarrow B$ есть сокращение для $(A \to B) \wedge (B \to A)$.

Основные равносильности логики высказываний (тождества булевой алгебры)

$A \wedge B$	$\equiv$	$B \wedge A$	$A \vee B$	$\equiv$	$B \vee A$
$A \wedge (B \wedge C)$	$\equiv$	$(A \wedge B) \wedge C$	$A \vee (B \vee C)$	$\equiv$	$(A \vee B) \vee C$
$A \wedge A$	$\equiv$	A	$A \vee A$	$\equiv$	A
$A \wedge (B \vee C)$	$\equiv$	$(A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C)$	$\equiv$	$(A \vee B) \wedge (A \vee C)$
$A \vee (A \wedge B)$	$\equiv$	A	$A \wedge (A \vee B)$	$\equiv$	A
$\neg(A \wedge B)$	$\equiv$	$\neg A \vee \neg B$	$\neg(A \vee B)$	$\equiv$	$\neg A \wedge \neg B$
$\perp$	$\equiv$	$A \wedge \neg A$	$\top$	$\equiv$	$A \vee \neg A$
$\neg\neg A$	$\equiv$	A	$A \to B$	$\equiv$	$\neg A \vee B$

Основные равносильности логики высказываний (тождества булевой алгебры)

$A \wedge B$	$\equiv$	$B \wedge A$	$A \vee B$	$\equiv$	$B \vee A$
$A \wedge (B \wedge C)$	$\equiv$	$(A \wedge B) \wedge C$	$A \vee (B \vee C)$	$\equiv$	$(A \vee B) \vee C$
$A \wedge A$	$\equiv$	A	$A \vee A$	$\equiv$	A
$A \wedge (B \vee C)$	$\equiv$	$(A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C)$	$\equiv$	$(A \vee B) \wedge (A \vee C)$
$A \vee (A \wedge B)$	$\equiv$	A	$A \wedge (A \vee B)$	$\equiv$	A
$\neg(A \wedge B)$	$\equiv$	$\neg A \vee \neg B$	$\neg(A \vee B)$	$\equiv$	$\neg A \wedge \neg B$
$\perp$	$\equiv$	$A \wedge \neg A$	$\top$	$\equiv$	$A \vee \neg A$
$\neg\neg A$	$\equiv$	A	$A \to B$	$\equiv$	$\neg A \vee B$

Основные равносильности с кванторами

$$
\begin{aligned}
\forall x\ A[a/x] &\equiv \forall y\ A[a/y] \\
\exists x\ A[a/x] &\equiv \exists y\ A[a/y] \\
(\forall x\ A[a/x] \vee B) &\equiv \forall x\ (A[a/x] \vee B) \\
(\exists x\ A[a/x] \vee B) &\equiv \exists x\ (A[a/x] \vee B) \\
(\forall x\ A[a/x] \wedge B) &\equiv \forall x\ (A[a/x] \wedge B) \\
(\exists x\ A[a/x] \wedge B) &\equiv \exists x\ (A[a/x] \wedge B) \\
\neg \forall x A[a/x] &\equiv \exists x \neg A[a/x] \\
\neg \exists x A[a/x] &\equiv \forall x \neg A[a/x]
\end{aligned}
$$

Подстановка в логике предикатов

Стандартные факты:

- Допустимость правил подстановки и замены подформулы на эквивалентную
- Переименование связанных переменных
- Теорема о предварённой нормальной форме

Скучные детали смотри в записках лекций, учебниках и проходи на семинарских занятиях.

Подстановка в логике предикатов

Стандартные факты:

- Допустимость правил подстановки и замены подформулы на эквивалентную
- Переименование связанных переменных
- Теорема о предварённой нормальной форме

Скучные детали смотри в записках лекций, учебниках и проходи на семинарских занятиях.

Расширение языка пропозициональными переменными

- Обогатим язык логики первого порядка пропозициональными переменными. Можно считать переменную P нульместным предикатным символом.
- Распространим на расширенный язык все синтаксические понятия, включая понятие формулы.
- Пропозициональные переменные считаются атомарными формулами.

Подстановка

Опр.

$C[P/A]$ означает результат замены всех вхождений P в формулу C на формулу A.

Замечание.

$C[P/A]$ не всегда является формулой. Если $C = \forall x\,(Q(x) \wedge P)$ и $A = \exists x R(x)$, то

$$C[P/A] = \forall x\,(Q(x) \wedge \exists x R(x))\ .$$

Подстановка

Опр.

$C[P/A]$ означает результат замены всех вхождений P в формулу C на формулу A.

Замечание.

$C[P/A]$ не всегда является формулой. Если $C = \forall x\,(Q(x) \wedge P)$ и $A = \exists x R(x)$, то

$$C[P/A] = \forall x\,(Q(x) \wedge \exists x R(x))\ .$$

Лемма.
$C[P/A]$ — формула, если и только если любое вхождение P в формулу C не находится в области действия квантора по переменной $x \in \mathrm{BdVar}$, входящей в A.

Опр.
Говорим, что *разрешена подстановка формулы A вместо P в C*, если выполнено условие предыдущей леммы.

Лемма.
$C[P/A]$ — формула, если и только если любое вхождение P в формулу C не находится в области действия квантора по переменной $x \in \mathrm{BdVar}$, входящей в A.

Опр.
Говорим, что *разрешена подстановка формулы A вместо P в C*, если выполнено условие предыдущей леммы.

Замена подформулы на эквивалентную

Теорема.

Если $A \equiv B$ и разрешена подстановка формул A, B вместо P в C, то $C[P/A] \equiv C[P/B]$.

Доказательство: индукция по построению формулы C. Шаг индукции на основе леммы:

Лемма.

Если $A \equiv A'$ и $B \equiv B'$, то

1. $A \wedge B \equiv A' \wedge B'$, $\quad A \vee B \equiv A' \vee B'$, $\quad \neg A \equiv \neg A'$,
2. $\forall x\, A[a/x] \equiv \forall x\, A'[a/x]$ (если x не входит в A и A'),
3. $\exists x\, A[a/x] \equiv \exists x\, A'[a/x]$ (если x не входит в A и A').

Семантика расширенного языка

- Пропозициональная переменная P в модели M интерпретируется как логическая константа, то есть $P_M \in \mathbb{B}$.
- Считается $M \models P_M$, если $P_M = И$ и $M \not\models P_M$, если $P_M = Л$.
- Понятие общезначимой формулы распространяется на формулы расширенного языка.

Теорема о подстановке

Теорема.

Пусть формула A общезначима и разрешена подстановка формулы C вместо P в A, тогда общезначима формула $A[P/C]$.

Доказательство.

- Допустим, $M \not\models f(A[P/C])$ при некоторой оценке f.
- Расширим M до модели (M, P) сигнатуры с переменной P: $P_M = \text{И} \iff M \models f(C)$.

Теорема о подстановке

Теорема.

Пусть формула A общезначима и разрешена подстановка формулы C вместо P в A, тогда общезначима формула $A[P/C]$.

Доказательство.

- Допустим, $M \not\models f(A[P/C])$ при некоторой оценке f.
- Расширим M до модели (M, P) сигнатуры с переменной P: $P_M = \text{И} \iff M \models f(C)$.

- Индукцией по построению формулы B проверим, что

$$(M, P) \models B \iff M \models B[P/C]$$

для любой замкнутой формулы B, в которую разрешена подстановка C вместо P.

- Отсюда получаем $(M, P) \not\models f(A)$.

Следствие.
Если $A \equiv B$ и разрешена подстановка C вместо P в A и B, то $A[P/C] \equiv B[P/C]$.

- Индукцией по построению формулы B проверим, что

$$(M, P) \models B \iff M \models B[P/C]$$

 для любой замкнутой формулы B, в которую разрешена подстановка C вместо P.
- Отсюда получаем $(M, P) \not\models f(A)$.

Следствие.
Если $A \equiv B$ и разрешена подстановка C вместо P в A и B, то $A[P/C] \equiv B[P/C]$.

Замена связанной переменной

Лемма.
Пусть $y \in \mathrm{BdVar}$ не входит в формулу B. Тогда $B[x/y]$ есть формула и $B[x/y] \equiv B$.

Доказательство.
Применяем индукцию по числу вхождений кванторов по переменной x в B. Каждая подформула $\forall x C[a/x]$ или $\exists x C[a/x]$ заменяется на эквивалентную $\forall y C[a/y]$ или $\exists y C[a/y]$.

Замена связанной переменной

Лемма.
Пусть $y \in \mathsf{BdVar}$ не входит в формулу B. Тогда $B[x/y]$ есть формула и $B[x/y] \equiv B$.

Доказательство.
Применяем индукцию по числу вхождений кванторов по переменной x в B. Каждая подформула $\forall x C[a/x]$ или $\exists x C[a/x]$ заменяется на эквивалентную $\forall y C[a/y]$ или $\exists y C[a/y]$.

Предварённая нормальная форма

Опр.

Формула A называется *предварённой*, если A имеет вид $\mathsf{Q}x_1\mathsf{Q}x_2\ldots\mathsf{Q}x_nA_0[b_1/x_1,\ldots,b_n/x_n]$, где Q означает квантор $\forall$ или $\exists$, а формула A_0 бескванторная.

Теорема.

Для каждой формулы A можно указать эквивалентную ей предварённую формулу A' от тех же свободных переменных.

Доказательство.

Последовательно выносим кванторы наружу, используя основные эквивалентности и леммы о замене связанных переменных и о подстановке. Разбор алгоритма на семинарских занятиях.

Предварённая нормальная форма

Опр.

Формула A называется *предварённой*, если A имеет вид $\mathsf{Q}x_1\mathsf{Q}x_2\ldots\mathsf{Q}x_nA_0[b_1/x_1,\ldots,b_n/x_n]$, где Q означает квантор $\forall$ или $\exists$, а формула A_0 бескванторная.

Теорема.

Для каждой формулы A можно указать эквивалентную ей предварённую формулу A' от тех же свободных переменных.

Доказательство.

Последовательно выносим кванторы наружу, используя основные эквивалентности и леммы о замене связанных переменных и о подстановке. Разбор алгоритма на семинарских занятиях.

Теории

Опр.

Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка $\mathcal{L}_\Sigma$. Элементы $A \in T$ называем *нелогическими аксиомами* T.

Пример.

Теория отношения эквивалентности:

- $\forall x\, R(x, x)$;
- $\forall x, y\, (R(x, y) \to R(y, x))$;
- $\forall x, y, z\, (R(x, y) \wedge R(y, z) \to R(x, z))$.

Теории

Опр.

Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка $\mathcal{L}_\Sigma$. Элементы $A \in T$ называем *нелогическими аксиомами* T.

Пример.

Теория отношения эквивалентности:

- $\forall x \, R(x, x)$;
- $\forall x, y \, (R(x, y) \to R(y, x))$;
- $\forall x, y, z \, (R(x, y) \wedge R(y, z) \to R(x, z))$.

Модель теории

Опр.

Модель $(M; \Sigma)$ есть *модель теории* T (обозначение $M \vDash T$), если для любой $A \in T$ $M \vDash A$.

Пример.

R есть отношение эквивалентности на множестве M, если и только если $(M; R) \vDash T$, где T — теория отношения эквивалентности.

Модель теории

Опр.

Модель $(M;\Sigma)$ есть *модель теории* T (обозначение $M \vDash T$), если для любой $A \in T$ $M \vDash A$.

Пример.

R есть отношение эквивалентности на множестве M, если и только если $(M;R) \vDash T$, где T — теория отношения эквивалентности.

Пример.

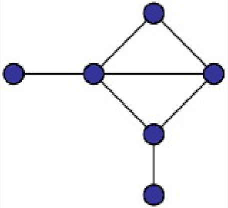
Модель $(M;<)$ есть *строгий частичный порядок*, если в $(M;<)$ истинны следующие предложения:

1. $\forall x, y, z\,(x < y \wedge y < z \to x < z)$
2. $\forall x \neg\, x < x$

Пример.

Простой граф — это модель вида $(V; E)$, где E — бинарный предикат смежности, причём отношение E симметрично и иррефлексивно:

- $\forall x \neg E(x, x)$
- $\forall x, y\, (E(x, y) \to E(y, x))$



Пример.

$(M;=,\cdot,1)$ есть *группа*, если M есть модель следующей теории (при условии, что «$=$» в M понимается как равенство):

1. $\forall x,y,z \;\; x\cdot(y\cdot z)=(x\cdot y)\cdot z$
2. $\forall x\,(1\cdot x=x\wedge x\cdot 1=x)$
3. $\forall x\exists y\,(x\cdot y=1\wedge y\cdot x=1)$

Равенство

Пусть Σ — сигнатура, содержащая выделенный предикатный символ $=$.

Опр.

Нормальной моделью называем модель $(M;\Sigma)$, в которой $=$ интерпретируется как равенство $\{\langle x,x\rangle \mid x\in M\}$.

Опр.

Аксиомы равенства для Σ — универсальные замыкания следующих формул:

1. аксиомы отношения эквивалентности для $=$
2. $$a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_n = b_n \to (P(a_1, \dots, a_n) \leftrightarrow P(b_1, \dots, b_n))$$
3. $$a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_n = b_n \to (f(a_1, \dots, a_n) = f(b_1, \dots, b_n))$$

для всех $f \in \mathrm{Func}_\Sigma$ and $P \in \mathrm{Pred}_\Sigma$.

Предложение.

Если $(M;\Sigma)$ — нормальная модель, то в M истинны все аксиомы равенства.

Опр.

Теорией с равенством называем теорию сигнатуры Σ с равенством, содержащую все аксиомы равенства.

Предложение.

Если $(M; \Sigma)$ — нормальная модель, то в M истинны все аксиомы равенства.

Опр.

Теорией с равенством называем теорию сигнатуры Σ с равенством, содержащую все аксиомы равенства.

Теорема.

Пусть T — теория с равенством. Если T выполнима, то T имеет нормальную модель.

Доказательство.

Пусть $M \vDash T$. Предикат $=_M$ есть отношение эквивалентности на M. Положим $M' \rightleftharpoons M/{=_M}$ — множество классов эквивалентности и $\varphi : M \to M'$ сопоставляет любому $x \in M$ его класс $\varphi(x) \in M'$.

Теорема.

Пусть T — теория с равенством. Если T выполнима, то T имеет нормальную модель.

Доказательство.

Пусть $M \vDash T$. Предикат $=_M$ есть отношение эквивалентности на M. Положим $M' \rightleftharpoons M/{=_M}$ — множество классов эквивалентности и $\varphi : M \to M'$ сопоставляет любому $x \in M$ его класс $\varphi(x) \in M'$.

Интерпретируем предикатные и функц. символы в M':
$P_{M'}(\varphi(x_1), \dots, \varphi(x_n)) \overset{\text{def}}{\Longleftrightarrow} P_M(x_1, \dots, x_n)$;
$f_{M'}(\varphi(x_1), \dots, \varphi(x_n)) := \varphi(f_M(x_1, \dots, x_n))$.

В силу аксиом равенства в M, определение корректно и M' — нормальная модель.

Индукцией по построению формулы A проверяем

$$M \models A[x_1, \dots, x_n] \iff M' \models A[\varphi(x_1), \dots, \varphi(x_n)].$$

Отсюда следует $M' \models T$.

Формальная арифметика Пеано

Сигнатура $\Sigma = \{0, S, +, \cdot, =\}$.

1. аксиомы равенства для Σ;
2. $\neg S(a) = 0, \quad S(a) = S(b) \to a = b,$
3. $a + 0 = a, \quad a + S(b) = S(a + b),$
4. $a \cdot 0 = 0, \quad a \cdot S(b) = a \cdot b + a,$
5. (Схема аксиом индукции)

   $A[a/0] \wedge \forall x\,(A[a/x] \to A[a/S(x)]) \to \forall x\,A[a/x],$

   для любой формулы A.

Теория множеств ZFC

Сигнатура $\Sigma = \{=, \in\}$.

1. (Аксиомы равенства)
2. (Экстенсинальность) $a = b \leftrightarrow \forall x\,(x \in a \leftrightarrow x \in b)$
3. (Пара) $\exists z\,\forall x\,(x \in z \leftrightarrow (x = a \vee x = b))$
4. (Объединение) $\exists z\,\forall x\,(x \in z \leftrightarrow \exists y\,(x \in y \wedge y \in a))$
5. (Степень) $\exists z\,\forall x\,(x \in z \leftrightarrow \forall y\,(y \in x \to y \in a))$
6. (Схема выделения) $\exists z\,\forall x\,(x \in z \leftrightarrow (x \in a \wedge \varphi[b/x]))$ для всех формул φ сигнатуры Σ
7. (Бесконечность) $\exists z\,(\varnothing \in z \wedge \forall x\,(x \in z \to x \cup \{x\} \in z))$
8. (Регулярность) $\exists z\,(z \in a \wedge \forall x\,(x \in a \to x \notin z))$
9. (Схема подстановки)
10. (Аксиома выбора)

Аксиоматика Тарского:

$G1.$ $ab \cong ba$

$G2.$ $ab \cong pq \wedge ab \cong rs \to pq \cong rs$

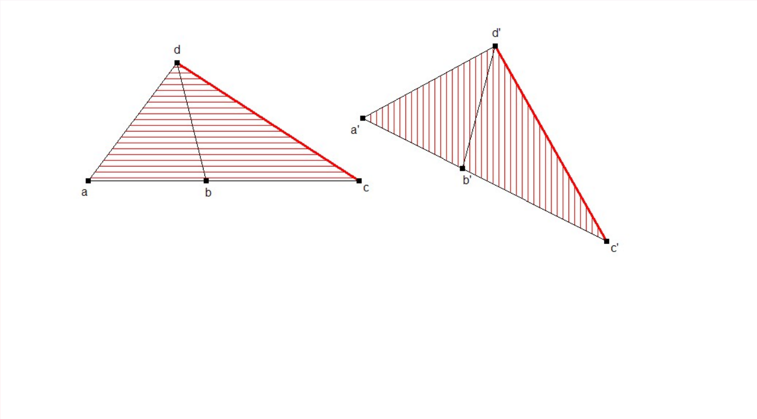
$G3.$ $ab \cong cc \to a = b$

$G4.$ $Babd \wedge Bbcd \to Babc$

$G5.$ $\exists x(Bqax \wedge ax \cong bc)$

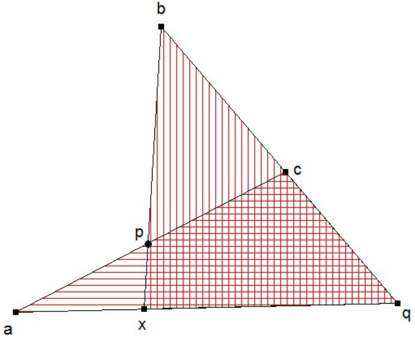
G6. (пять отрезков)

$$(a \neq b \wedge Babc \wedge Ba'b'c' \wedge ab \cong a'b' \wedge bc \cong b'c' \wedge ad \cong a'd' \wedge bd \cong b'd') \to cd \cong c'd'$$



G7. (аксиома Паша)

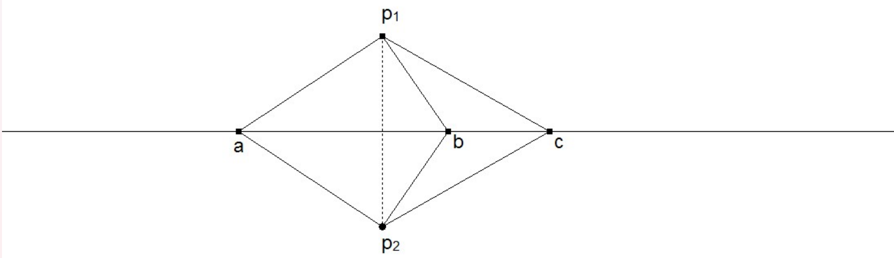
$Bapc \wedge Bqcb \rightarrow \exists x\,(Baxq \wedge Bbpx)$



Аксиомы размерности

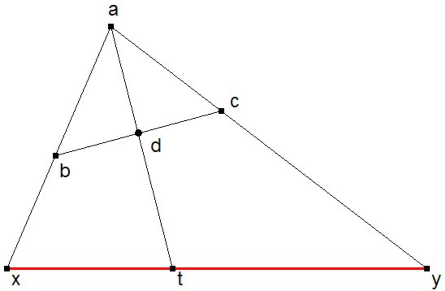
G8. $\exists x, y, z\,(\neg Bxyz \wedge \neg Byzx \wedge \neg Bzxy)$

G9. $(dim \leq 2)$
$(p_1 \neq p_2 \wedge ap_1 \cong ap_2 \wedge bp_1 \cong bp_2 \wedge cp_1 \cong cp_2) \rightarrow$
$a \in bc$



G10. (аксиома Евклида)

$Badt \wedge Bbdc \wedge a \neq d \to \exists x, y\, (Babx \wedge Bacy \wedge Bytx)$



G11. (схема аксиом непрерывности)

$$\exists u \forall x, y\, (C[a/x] \wedge D[a/y] \to Buxy) \to \\ \exists v \forall x, y\, (C[a/x] \wedge D[a/y] \to Bxvy)$$

Здесь x, y, u, v не входят в C, D.

G11′. (аксиома непрерывности 2-го порядка)

$$\forall X, Y\, (\exists u \forall x, y\, (x \in X \wedge y \in Y \to Buxy) \to \\ \exists v \forall x, y\, (x \in X \wedge y \in Y \to Bxvy))$$

Теорема Тарского о полноте

Теорема.

Для любого предложения A языка элементарной геометрии, если $(\mathbb{R}^2; =, B, \cong) \vDash A$, то A логически следует из аксиом $G1 - G11$.

Теорема.

Существует алгоритм проверки формулы A на выполнимость в $\mathbb{R}^2$.

Логика предикатов
лекция 4

Лев Дмитриевич Беклемишев
http://lpcs.math.msu.su/vml2020

lbekl@yandex.ru

02.03.2021

Исчисление предикатов

Исчисление предикатов сигнатуры Σ задаётся след. аксиомами и правилами вывода.

Аксиомы:

A1. Подстановочные примеры тавтологий,

A2. $\forall x A[a/x] \to A[a/t]$,

A3. $A[a/t] \to \exists x A[a/x]$.

Подстановочным примером тавтологии A мы называем результат замены всех пропозициональных переменных A на некоторые формулы сигнатуры Σ.

Пример: $B \vee \neg B$, где B — любая формула.

В A2 и A3 A — любая формула сигнатуры Σ и t — любой терм (x не входит в A).

Правила вывода:

$$R1.\ \frac{A \quad A \to B}{B} \ (\textit{modus ponens})$$

$$R2.\ \frac{A \to B}{A \to \forall x B[a/x]}$$

$$R3.\ \frac{B \to A}{\exists x B[a/x] \to A}$$

Здесь a не входит в A (и x не входит в B).

Правила R2 и R3 называются *правилами Бернайса*.

Выводимость

Опр.

Выводом в исчислении предикатов называется конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Пример.

$$\begin{array}{ll} \forall x A[a/x] \to A & \text{(A2)} \\ \forall x A[a/x] \to \forall y A[a/y] & \text{(R2)} \end{array}$$

Опр.

Формула A называется *выводимой* в исчислении предикатов или *теоремой* исчисления предикатов (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть A.

Пример.

$\vdash \forall x A[a/x] \to \forall y A[a/y]$ для любой формулы A.

Выводы в теории

Опр.

Выводом в теории T называется конечная последовательность формул, каждая из которых либо принадлежит множеству T, либо является логической аксиомой вида $A1 - A3$, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Доказуемость, опровержимость

Опр.

Формула A называется *выводимой (доказуемой) в теории* T или *теоремой* T (обозначение $T \vdash A$), если существует вывод в T, в котором последняя формула есть A.

Опр.

Формула A *опровержима* в T, если $T \vdash \neg A$.

Опр.

Формула A *независима* от T, если $T \nvdash A$ и $T \nvdash \neg A$.

Свойства выводимости

- Если $T \subseteq U$ и $T \vdash A$, то $U \vdash A$ (*монотонность*).
- Если $T \vdash A$, то существует такое конечное множество $T_0 \subseteq T$, что $T_0 \vdash A$ (*компактность*).
- Если $T \vdash A$ и для каждой аксиомы $B \in T$ имеет место $U \vdash B$, то $U \vdash A$ (*транзитивность*).

Теорема о дедукции

Опр.

Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка $\mathcal{L}_\Sigma$.
Теорию $T \cup \{A\}$ обозначаем также T, A или $T + A$.

Теорема.

Для любой теории T и замкнутой формулы A

$$T, A \vdash B \iff T \vdash A \to B.$$

Доказательство.

Индукция по длине вывода $T, A \vdash B$.
Если B является логической аксиомой или $B \in T$, то в T выводимо:

$$\begin{array}{ll} B & \\ B \to (A \to B) & \text{(тавтология)} \\ A \to B & \text{(MP)} \end{array}$$

Если $B = A$, то используем тавтологию $A \to A$.

Пусть B получена из C и $C \to B$ по modus ponens.

Имеем $T \vdash (A \to C)$ и $T \vdash (A \to (C \to B))$ по предположению индукции.

Соединяем эти два вывода и достраиваем так:

$$(A \to (C \to B)) \to ((A \to C) \to (A \to B)) \quad \text{(тавтология)}$$

$$(A \to C) \to (A \to B) \quad \text{(MP)}$$

$$A \to B \quad \text{(MP)}$$

Допустим $B = (C \to \forall x D[a/x])$ получена из $C \to D$ по $R2$. По пр. индукции

$$T \vdash A \to (C \to D).$$

Надо построить вывод

$$T \vdash A \to (C \to \forall x D[a/x]).$$

Достраиваем вывод $A \to (C \to D)$ в T:

$A \to (C \to D)$	
$(A \to (C \to D)) \to (A \wedge C \to D)$	(тавтология)
$(A \wedge C) \to D$	(MP)
$(A \wedge C) \to \forall x D[a/x]$	(R2, A замкнута)
$A \to (C \to \forall x D[a/x])$	(аналогично)

Правило $R3$ рассматривается аналогично.

Непротиворечивость теории

Опр.

Теория T *противоречива*, если существует A такая, что $T \vdash A$ и $T \vdash \neg A$. В противном случае теория T называется *непротиворечивой*.

Следствие.

$T \cup \{A\}$ противоречива $\iff$ $T \vdash \neg A$.

Теорема о корректности исчисления предикатов

Теорема.

Если $M \models T$ и $T \vdash A$, то $M \models A$.

Доказательство.

Индукция по длине вывода A в T.

Следствие.

Если $\vdash A$, то A общезначима.

Доказательства непротиворечивости

Следствие.
Если теория T имеет модель, то T непротиворечива.

Следствие.
Следующие теории непротиворечивы:

- исчисление предикатов (пустая теория);
- теория групп;
- элементарная геометрия;
- формальная арифметика.

Теория множеств?

Доказательства независимости

Следствие.
Если существует модель M теории T для которой $M \not\models A$, то $T \nvdash A$.

Пример.
Модель Пуанкаре $\mathbf{H}^2$ показывает, что аксиома Евклида независима от остальных аксиом элементарной геометрии.

Теорема Гёделя о полноте

Теорема.

1. *Всякая непротиворечивая теория T выполнима, то есть имеет модель $M \models T$.*
2. *Если $T \nvdash A$, то найдётся модель $M \models T$ для которой $M \not\models A$.*

Покажем равносильность этих утверждений.

$(1 \Rightarrow 2)$: Если $T \nvdash A$, то $T \cup \{\neg A\}$ непротиворечива. Действительно, если $T, \neg A$ противоречива, то $T \vdash \neg\neg A$, а значит $T \vdash A$ (используем тавтологию $\neg\neg A \to A$). Следовательно, $T \cup \{\neg A\}$ имеет модель M.

$(2 \Rightarrow 1)$: Пусть T непротиворечива. Возьмём $A = (B \wedge \neg B)$. Тогда $T \nvdash A$, следовательно у теории T должна быть модель (опровергающая A).

Теорема Гёделя–Мальцева о компактности

Теорема.

Теория T выполнима $\iff$ любое конечное подмножество $T_0 \subseteq T$ выполнимо.

Доказательство.

Если T невыполнима, то существует вывод противоречия в T, использующий лишь конечное число аксиом T.

Нестандартные модели арифметики

Пример.

Пусть $(\mathbb{N}; =, S, +, \cdot, 0)$ — стандартная модель арифметики и $Th(\mathbb{N})$ есть множество *всех* истинных в $\mathbb{N}$ предложений.

Добавим к сигнатуре новую константу c и рассмотрим теорию

$$T \rightleftharpoons Th(\mathbb{N}) \cup \{\neg c = 0, \neg c = S0, \neg c = SS0, \dots\}.$$

Терм $\bar{n} \rightleftharpoons SS\ldots S0$ (n раз) называем *нумералом*. Нумералы служат именами натуральных чисел.

Утверждение.

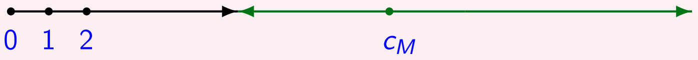
Каждая конечная подтеория $T_0 \subseteq T$ выполнима.

Доказательство.

T_0 содержит лишь конечное число аксиом вида $c \neq \bar{n}_1$, ..., $c \neq \bar{n}_k$. Интерпретируем константу c в стандартной модели как любое число $m > n_1, \ldots, n_k$.

По теореме о компактности существует (нормальная) модель $M \models T$. Модель M обладает следующими свойствами:

- $\mathbb{N}$ изоморфна начальному сегменту M; вложение $\mathbb{N} \to M$ задаётся функцией $\varphi : n \longmapsto \bar{n}_M$.
- $M \models Th(\mathbb{N})$;
- $M \not\cong \mathbb{N}$, в частности $c_M \in M$ есть «бесконечно большое число», поскольку c_M отлично от всякого $n \in \mathbb{N}$.

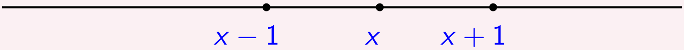


Порядок на модели M

Формула $a < b \rightleftharpoons \exists x\,(x \neq 0 \wedge a + x = b)$ определяет порядок в $\mathbb{N}$. Для данной формулы в $\mathbb{N}$ выполнены аксиомы строгого линейного порядка и следующие предложения:

- $\forall x\,(0 < x \vee 0 = x)$;
- $\forall x \exists y\,(x < y \wedge \forall z\,(z < y \to z = x \vee z < x))$;
- $\forall y\,(y \neq 0 \to \exists x\,(x < y \wedge \forall z\,(z < y \to$
  $\to z = x \vee z < x)))$.

Следовательно, те же аксиомы выполнены и в M. Поэтому предикат $<_M$ на M представляет собой строгий линейный порядок с наименьшим элементом 0. При этом каждый элемент имеет последователя, и каждый элемент, кроме 0, имеет непосредственного предшественника.



Опр.

Элементы $x, y \in M$ *близки*, если для некоторого $n \in \mathbb{N}$ выполнено $y = SS \dots S(x)$ или $x = SS \dots S(y)$ (n символов S).

Классы эквивалентности по отношению близости называем *галактиками*.

Утверждение.

Если G — галактика в M, $G \neq \mathbb{N}$, то порядок $(G, <_M)$ изоморфен $(\mathbb{Z}, <)$.

Пусть $\mathcal{G}$ есть множество всех галактик в M. Определим $G_1 <_M G_2$, если для любых $x \in G_1$, $y \in G_2$ $x <_M y$.

Теорема.

Порядок $(\mathcal{G}, <_M)$ *есть плотный порядок без наибольшего элемента и с наименьшим элементом* $\mathbb{N}$.

Доказательство.

Если $G_1 < G_2$, возьмём чётные $x_1 \in G_1$ и $x_2 \in G_2$ и рассмотрим $y = (x_1 + x_2)/2$ (функция $g(x) = x/2$ определима в $\mathbb{N}$, а значит и в M).

Если $y \in G_1$, то $(x_1 + x_2)/2 = x_1 + \bar{n}$ для некоторого $n \in \mathbb{N}$. Тогда $2x_1 + 2\bar{n} = x_1 + x_2$, откуда $x_1 + 2\bar{n} = x_2$, то есть $x_2 \in G_1$.

Аналогично показываем $y \notin G_2$.