Введение в математическую логику

Лекция 5

Логика предикатов

- Будем называть эквивалентными на данной модели $<S\ldots>$ формулы, задающие одно и то же отношение (на S^{ω}).
- Будем назвать эквивалентными формулы, эквивалентные на любой модели.
- Отношение – то же, что подмножество многомерного пространства.
- Логические связки соответствуют операциям над множествами (конъюнкция – пересечение, и т. д.).
- Навешивание квантора существования соответствует проекции (нарисуйте двумерное множество и его проекции на оси координат).

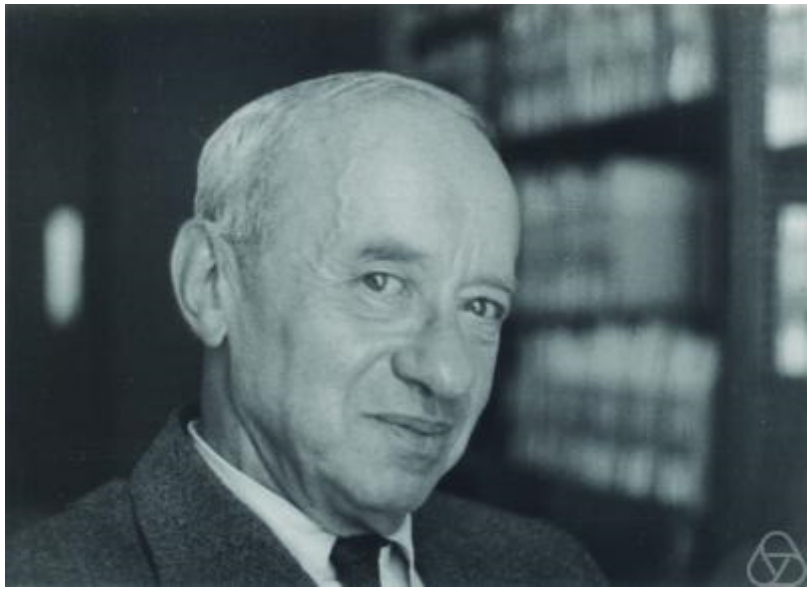
Поле действительных чисел

- Модель: $\langle \mathbb{R}, \langle \{0, 1\}, \{+, \cdot\}, \{ =, > \} \rangle, \mathit{Зн} \rangle$

  (упорядоченное множество действительных чисел со сложением и умножением и константами 0 и 1).
- Что выразимо в этой модели?
- Алгебраические множества – системы (конъюнкции) уравнений.
- Полуалгебраические множества – объединения, пересечения и дополнения множеств, задаваемых уравнениями и неравенствами.
- Можно применять к полуалгебраическим множествам проекцию, соответствующую квантору существования для формул (отношений). Получится ли больше отношений?
- Нет – теорема Тарского – Зайденберга.

Теорема Тарского (– Зайденберга)

- Существует алгоритм, который для всякой формулы сигнатуры $\langle\{0, 1\}, \{+, *\}, \{ =, >\}\rangle$ строит бескванторную формулу, задающую то же отношение на множестве действительных чисел.
- **Следствие.** Проекция полуалгебраического множества – полуалгебраическое множество.
- **Пример.** Равенство $x^2+px+q = 0$ задаёт полуалгебраическое множество троек $\langle x, p, q\rangle$. Его проекция вдоль оси x на плоскость p, q – это полуалгебраическое множество $p^2 - 4q \geq 0$.



Доказательство теоремы Тарского – Зайденберга

- Начнем с формул с единственным квантором существования $\exists u\, B(u, x_1, \ldots, x_n)$, где B – бесквантворная. Будем строить эквивалентную ей бесквантворную (задающую то же отношение на $\mathbb{R}^\omega$).
- Будем считать, что атомные формулы в B имеют вид $p(u, x_1, \ldots, x_n) = 0$ или $p(u, x_1, \ldots, x_n) > 0$.
- Многочлен p можно рассматривать как многочлен от переменной u, коэффициенты которого – многочлены от $x_1, \ldots, x_n$. Надо доказать, что те $\langle x_1, \ldots, x_n \rangle$, при которых формула истинна – полуалгебраическое множество.

Доказательство теоремы Тарского – Зайденберга.

Диаграмма семейства многочленов.

- *Знак многочлена* – это 0, +, -. *Диаграмма семейства многочленов* – таблица знаков, где строки пронумерованы многочленами, а столбцы – сегментами, на которые прямая разбивается корнями многочленов (включая одноточечные):
  $(-\infty, a_1)$, $[a_1]$, (a_1, a_2), $[a_2]$,…, $[a_n]$, $(a_n, +\infty)$. В клетке стоит знак многочлена на сегменте.
- **Пример.** Семейство двух многочленов u^2-1 и $u(u-1)(u-2)$. Корни: -1, 0, 1, 2. Столбцы таблицы соответствуют корням и промежуткам между корнями. В ячейках таблицы – знак многочлена. Сегменты в таблицу не входят.

u^2-1	+	0	–	–	–	0	+	+	+
$u(u-1)(u-2)$	–	–	–	0	+	0	–	0	+

Доказательство теоремы Тарского – Зайденберга.

- Диаграмма зависит от Зн $\langle x_1, \ldots, x_n \rangle$, ширина диаграммы может меняться, но ограничена.
- Пусть все многочлены, входящие в бескванторную формулу $\Phi(u, x_1, \ldots, x_n)$, входят в семейство F. Тогда истинность формулы $\exists u\, \Phi(u, x_1, \ldots, x_n)$ при каждом наборе $\langle x_1, \ldots, x_n \rangle$ определяется диаграммой семейства F на этом наборе.
- Число возможных диаграмм для данного F конечно, пространство $\mathbb{R}^n$ наборов $\langle x_1, \ldots, x_n \rangle$ разбивается на конечное число частей, отвечающих всем возможным диаграммам.
- Нужно доказать, что эти части – полуалгебраические множества.

Доказательство теоремы Тарского – Зайденберга

Определим 4 операции на семействах многочленов.

1. Операция для пары p, q многочленов от u (с коэффициентами из $\mathbb{Z}[x_1, \ldots, x_n]$).

Пусть k = (степень $p(u)$ – степень $q(u)$ + 1),

a = (старший коэффициент $q(u)$).

Дает: *модифицированный остаток* от деления $p(u)$ на $q(u)$ =

= остаток от деления $a^k p(u)$ на $q(u)$.

Считаем, что степень p не меньше степени q (тогда остаток отличен от p).

Доказательство теоремы Тарского – Зайденберга

Определяем 4 операции на семействах многочленов.

2. Отбрасывание старшего члена
3. Взятие старшего коэффициента
4. Дифференцирование по u

В результате применения каждой операции к многочленам положительной степени эти степени уменьшаются. Применение операции к многочлену нулевой степени дает его самого или 0.

Поэтому замыкание конечного семейства многочленов относительно этих операций конечно.

Доказательство теоремы Тарского – Зайденберга.

- **Лемма.** Пусть F – конечное множество многочленов из $(\mathbb{Z}[x_1, \ldots, x_n])[u]$, замкнутое относительно

  перечисленных операций.
- Пусть F_0 – его часть, состоящая только из многочленов степени 0 по u (они представляют собой многочлены из $\mathbb{Z}[x_1, \ldots, x_n]$).
- Тогда диаграмма множества F при данных $x_1, \ldots, x_n$ полностью определяется диаграммой множества F_0 при тех же $x_1, \ldots, x_n$.

Доказательство теоремы Тарского – Зайденберга.
Доказательство Леммы

- Добавляем в множество F_0 многочлены в порядке неубывания их степеней (то есть можем добавить многочлен, если все многочлены меньшей степени уже добавлены), пока не получим всё множество F.
- Покажем, что на каждом шаге диаграмма расширенного множества (с новым многочленом) может быть однозначно восстановлена по диаграмме предыдущего множества.

Доказательство теоремы Тарского – Зайденберга

Добавляем многочлен *p*.

- Старший коэффициент p уже есть в диаграмме. Если он:

  $= 0$ в диаграмме (нулевая строка), то для p дублируем строку, соответствующую многочлену «p без старшего члена»;

  $\neq 0$, тогда:

- Определяем знаки p в корнях других многочленов:

  – В корне $q(u)$ используем модифицированный остаток:
  $a^k p(u) = s(u)q(u) + r(u)$.
  Знак a и четность k, как и знак r, – известны. Отсюда ясен знак p.

Доказательство теоремы Тарского – Зайденберга

Добавляем многочлен *p*.

• Ищем знаки и корни p в промежутках между корнями других многочленов. В промежутках:

– Если в соседних корнях $p(u)$ имеет одинаковые знаки, то между этими корнями нет корней $p(u)$ (иначе между корнями был бы корень производной, но его нет, т. к. корни – соседние) и знак – тот же, что в корнях.

– Если в одном из соседних корней $p(u) = 0$, то на промежутке нет корней $p(u)$ (аналогично).

– Если в соседних корнях у $p(u)$ разные знаки, то на промежутке – ровно 1 корень $p(u)$ (аналогично).

• Ищем корни на крайних (полубесконечных) сегментах или на сегменте $(-\infty, +\infty)$. Знаки в бесконечностях легко определить, зная степень многочлена и знак старшего коэффициента. Корней не больше одного на сегмент, аналогично предыдущему.

Доказательство теоремы Тарского – Зайденберга

Добавляем многочлен *p*.

- Добавляем строку для *p.*
- Заменяем один столбец на три там, где есть корни $p(u)$.
- Заполняем строчку для *p* в соответствии с предыдущим.
- Дублируем, где надо, клетки в других строчках.

Лемма доказана.

Доказательство теоремы Тарского – Зайденберга

Мы можем заменить всякую формулу $\exists u\, B(u, x_1, \ldots, x_n)$, где B – бесквантворная, на эквивалентную бесквантворную.

Именно: применяем лемму – в качестве F берём замыкание множества всех многочленов, соответствующих атомным формулам из B; перебираем возможные диаграммы для F_0 (их количество $3^{|F_0|}$); по каждой диаграмме D' для F_0 строим диаграмму D для F; по D определяем, истинна ли формула $\exists u\, B(u, x_1, \ldots, x_n)$ при условиях, соответствующих диаграмме D'. Каждая диаграмма D' описывается конъюнкцией атомных формул. Берем дизъюнкцию этих конъюнкций по всем диаграммам D', для которых $\exists u\, B(u, x_1, \ldots, x_n)$ истинна.

Всякую формулу $\forall u\, B(u, x_1, \ldots, x_n)$ мы можем заменить на эквивалентную $\neg\exists u\, \neg B(u, x_1, \ldots, x_n)$. Если в формуле несколько кванторов, устраняем их, начиная с внутренних.

Пример. Формула $\exists x(x^2+px+q = 0)$

Множество F состоит из 11 многочленов:

(1) x^2+px+q – соответствует атомной формуле,

(2) $px+q$ – (1) без старшего члена,

(3) $2x+p$ – производная от (1),

(4) 1 – старший коэффициент (1),

(5) q – (2) без старшего члена,

(6) p – ст. коэфф. (2) = произв.(2) = (3) без ст.чл.,

(7) 2 – старший коэфф. (3) = произв. от (3),

(8) q^2 – остаток деления $p^2 \cdot$(1) на (2),

(9) $4q - p^2$ – остаток деления $4 \cdot$(1) на (3),

(10) $2q - p^2$ – остаток деления $2 \cdot$(2) на (3),

(11) $p^2 - 2q$ – остаток деления $p \cdot$(3) на (2).

Пример. Формула $\exists x(x^2+px+q = 0)$

- Множество F_0 составляют 8 многочленов (4) – (11).
- В непротиворечивой диаграмме знаки многочленов, тождественно равных 1 и 2, – известны. Для сокращения перебора можно не рассматривать противоречивые диаграммы. Также, зная знак q, знаем и знак q^2. Зная знак $2q - p^2$, знаем знак $p^2 - 2q$. Для построения диаграмм D' оставляем только многочлены q, p, $4q - p^2$, $2q - p^2$. Количество диаграмм D' равно 3^4=81.
- Для примера рассмотрим одну диаграмму D':

q	>
p	<
$4q - p^2$	<
$2q - p^2$	<

- Строим по ней диаграмму D, добавляя по очереди многочлены $2x+p$, $px+q$, x^2+px+q.
- Добавляем многочлен $2x+p$. Единственному столбцу диаграммы соответствует интервал $(-\infty, +\infty)$. При $-\infty$ многочлен отрицателен, при $+\infty$ – положителен. Значит, на интервале есть корень, и столбец разбивается на три столбца.

Пример. Формула $\exists x(x^2+px+q = 0)$

- Добавляем многочлен $px+q$.
- Каков его знак в нуле многочлена $2x+p$?
  Деление: $2(px+q) = s(2x+p) + 2q - p^2$.
  Знак $px+q$ равен знаку остатка $2q - p^2$ (<).
- Так как $p < 0$, то при $-\infty$ многочлен $px+q$ положителен, а при $+\infty$ – отрицателен.
  Корень имеется в первом столбце.

q	>	>	>
p	<	<	<
$4q - p^2$	<	<	<
$2q - p^2$	<	<	<
$2x+p$	<	0	>

- Добавляем многочлен x^2+px+q.
- Его знак в нуле многочлена $2x+p$?
  $4(x^2+px+q) = s(2x+p) + 4q - p^2$.
  Знак равен знаку остатка $4q - p^2$ (<).
- Его знак в нуле многочлена $px+q$?
  $p^2(x^2+px+q) = s(px+q) + q^2$.
  Так как $p^2 > 0$, знак равен знаку остатка q^2(>).

q	>	>	>	>	>
p	<	<	<	<	<
$4q - p^2$	<	<	<	<	<
$2q - p^2$	<	<	<	<	<
$2x+p$	<	<	<	0	>
$px+q$	>	0	<	<	<

Пример. Формула $\exists x(x^2+px+q = 0)$

- Во 2 и 4 столбцах знаки разные. Значит, в 3 столбце – корень. 3-й столбец делим на три столбца.
- При $-\infty$ и при $+\infty$ многочлен x^2+px+q положителен. Корень – в последнем столбце, последний столбец делим на три столбца.
- Расставляем знаки.
- Диаграмма D по диаграмме D' построена.
- Видим, что при условиях $q>0$, $p<0$, $4q-p^2<0$, $2q-p^2<0$ многочлен x^2+px+q имеет два корня.
- Для полной картины нужно рассмотреть оставшиеся 80 вариантов диаграммы D'.

q	>	>	>	>	>
p	<	<	<	<	<
$4q - p^2$	<	<	<	<	<
$2q - p^2$	<	<	<	<	<
$2x+p$	<	<	<	0	>
$px+q$	>	0	<	<	<
x^2+px+q		>		<	

q	>	>	>	>	>	>	>	>	>
p	<	<	<	<	<	<	<	<	<
$4q - p^2$	<	<	<	<	<	<	<	<	<
$2q - p^2$	<	<	<	<	<	<	<	<	<
$2x+p$	<	<	<	<	<	0	>	>	>
$px+q$	>	0	<	<	<	<	<	<	<
x^2+px+q	>	>	>	0	<	<	<	0	>

Поле действительных чисел

- Модель: $\langle \mathbb{R}, \langle \{0, 1\}, \{+, *\}, \{ =, > \} \rangle, \mathit{Зн} \rangle$ (упорядоченное множество действительных чисел со сложением и умножением и константами 0 и 1).
- Что дает алгоритм для формул без свободных переменных?
- Он отвечает на вопрос об истинности формул.
- Следствие теоремы Тарского – Зайденберга. Множество формул, истинных в модели $\langle \mathbb{R}, \langle \{0, 1\}, \{+, *\}, \{ =, > \} \rangle, \mathit{Зн} \rangle$ – разрешимо.

Геометрия

- С помощью метода координат большинство геометрических утверждений можно записать как утверждения о действительных числах.
- Исключение. Не нужно говорить об n-угольниках без указания конкретного n.
- Пример. Гипотеза 13 шаров: спор между Ньютоном и Грегори: "Сколько материальных шаров равных радиусов можно "прислонить" к фиксированному шару того же радиуса?"
- Существование решения у системы уравнений с 39 неизвестными.
- Невозможность (правота Ньютона) доказана Л. Ван дер Варденом и К. Шютте в 1953 году (без теоремы Тарского).
- http://www.etudes.ru/ru/mov/mov004/