

Введение в математическую логику и теорию алгоритмов

Лекция 6

Алексей Львович Семенов

Логика отношений

- Будем называть *эквивалентными* в данной структуре $\langle D, \dots \rangle$ формулы, задающие одно и то же отношение (на D^ω)
- [Повторение] Замыкание класса отношений (определялось с использованием имен и не зависит от использованных имен).
- [Изменение терминологии] Замкнутые классы отношений были названы *определимостью* – **отменяется**. Будем их называть *многообразиями отношений*.
- Сегодня будет изучаться одно важное многообразие.

Поле действительных чисел. Многообразиие всех отношений

Структура: $\mathcal{R} = \langle \mathbb{R}, p(\) =, > 0 \text{ – для всех}$
полиномов с целыми коэффициентами, $\mathbb{Z}n \rangle$

- Что определимо?
- Алгебраические множества – системы (конъюнкции) уравнений

Ю.И. Манин (16.02.1937 –):

- *Если уравнения выбраны и зафиксированы, мы представляем себе множество всех их решений... в виде геометрического образа, формы... В одних направлениях эта форма уходит в бесконечность, а в других прихотливо замыкается на себе. Разнообразие и сложность таких форм бесконечно богаче, чем все, что можно увидеть на современных выставках абстрактного искусства. Математики научились находить регулярности, взаимосвязи и закономерности в этом огромном мире.*

Поле действительных чисел. Многообразиие всех отношений

- 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 структуры \mathcal{R} строит эквивалентную ей в этой структуре бескванторную формулу.
- **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 $p^2 - 4q \geq 0$.
- Альфред Тарский
(14.01.1901 — 26.10.1983)



Доказательство теоремы Тарского – Зайденберга

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

Доказательство. Метод интервалов

Пол Коэн (02.04.1934 — 23.03.2007)

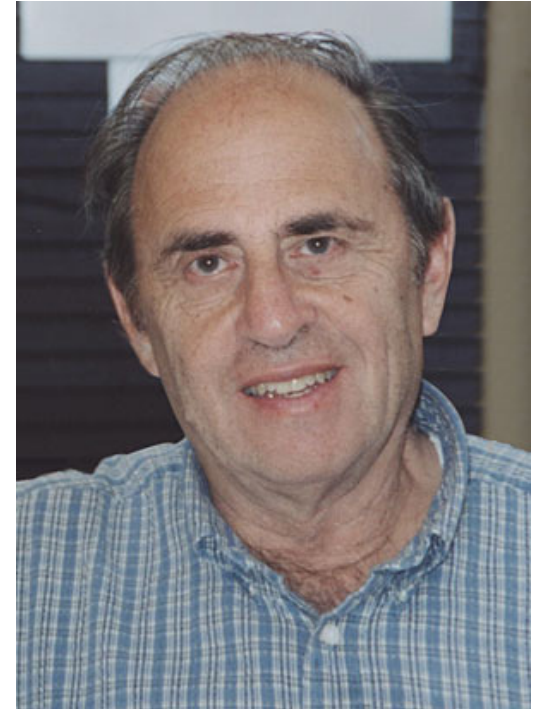
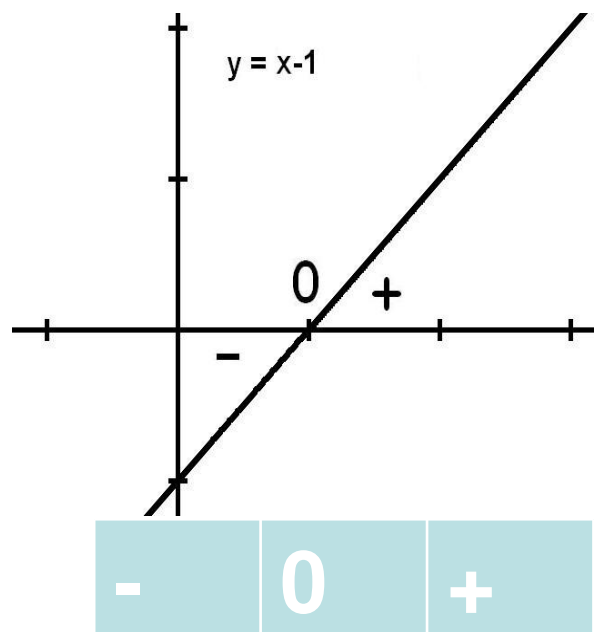
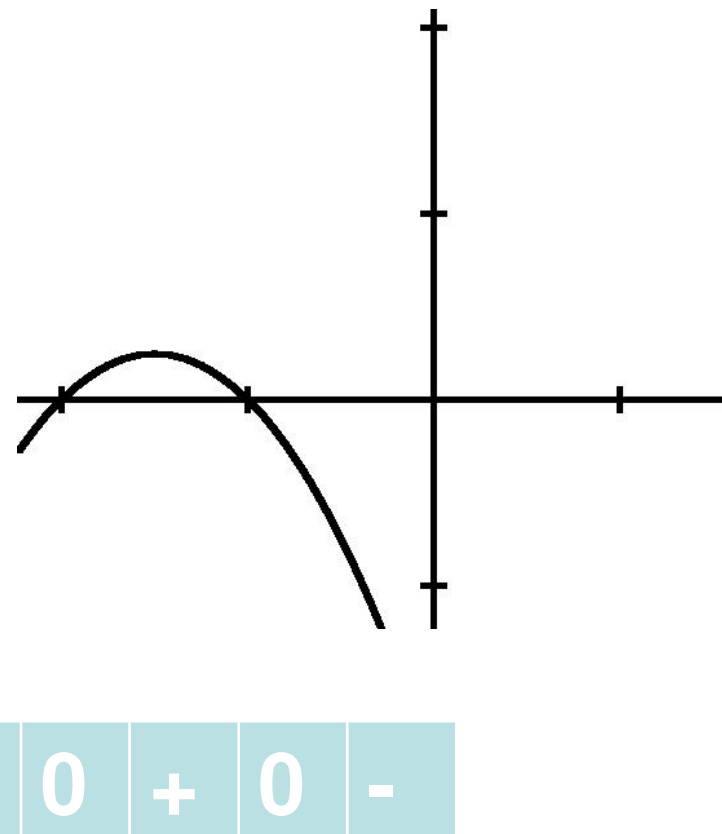


Диаграмма многочлена

Знак многочлена в точке –
это 0, +, -.



Это - диаграмма $ax + b \leftrightarrow$
 $a > 0$



Это - диаграмма $ax^2 + bx + c \leftrightarrow$
 $a < 0 \wedge b^2 - 4ac > 0$

Знак многочлена в корне другого многочлена

Пусть

- $p = sq + r$
- a – корень $q(x)$

Тогда

- Знак $p(a) =$ Знак $r(a)$
- Если r – остаток от деления p на q , то r проще (имеет меньшую степень), чем q

Диаграмма семейства многочленов.

- Пусть задано семейство многочленов. Прямая \mathbb{R} разбивается всеми корнями многочленов семейства на сегменты (включая одноточечные):
 $(-\infty, a_1), [a_1], (a_1, a_2), [a_2], \dots, [a_n], (a_n, +\infty)$
- Построим таблицу: имена строк – многочлены, имена столбцов – сегменты. В клетке – знак многочлена на сегменте (он постоянен).
- **Пример.** Семейство: u^2-1 и $u(u-1)(u-2)$. Корни: $-1, 0, 1, 2$.

	$(-\infty, -1)$	$[-1]$	$(-1, 0)$	$[0]$	$(0, 1)$	$[1]$	$(1, 2)$	$[2]$	$(2, +\infty)$
u^2-1	+	0	–	–	–	0	+	+	+
$u(u-1)(u-2)$	–	–	–	0	+	0	–	0	+

Диаграмма семейства многочленов – таблица без сегментов

Доказательство теоремы Тарского – Зайденберга.

- Диаграмма зависит от $\exists n \langle X_1, \dots, X_n \rangle$, ширина диаграммы может меняться, но ограничена.
- Пусть все многочлены, входящие в бескванторную формулу $\Phi(u, X_1, \dots, X_n)$, входят в семейство F . Тогда истинность формулы $\exists u \Phi(u, X_1, \dots, X_n)$ при каждом наборе $\langle X_1, \dots, X_n \rangle$ определяется диаграммой семейства F на этом наборе.
- Число возможных диаграмм для данного F конечно, пространство \mathbb{R}^n наборов $\langle X_1, \dots, X_n \rangle$ 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. Дана: пара p, q многочленов от u
(с коэффициентами из $\mathbb{Z}[x_1, \dots, x_n]$).

Пусть $k = (\text{степень } p(u) - \text{степень } q(u)) + 1$,
 a – старший коэффициент $q(u)$.

Дает: *модифицированный остаток*

от деления $p(u)$ на $q(u) =$

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

Он лежит в $\mathbb{Z}[x_1, \dots, x_n]$.

Степень модифицированного остатка меньше степени q .

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 операции 1 к паре многочленов положительной степени получаем многочлен степени меньшей, чем максимум степеней в паре.

В результате применения операций 2 - 4 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 $(\mathbb{Z}[X_1, \dots, X_n])[U]$, замкнутое относительно перечисленных операций.
- Пусть F_0 – его часть, состоящая только из многочленов степени 0 по U (они представляют собой многочлены из $\mathbb{Z}[X_1, \dots, X_n]$).
- Тогда диаграмма множества F при данных X_1, \dots, X_n полностью определяется диаграммой множества F_0 при тех же X_1, \dots, 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 p .

- Старший коэффициент p есть в диаграмме. (Ему соответствует строка постоянных знаков.)
- Он:
 - $=0$ (нулевая строка в диаграмме), тогда p уже есть в диаграмме
 - $\neq 0$, тогда:
- Ищем знак p в корне каждого многочлена q , представленного в диаграмме ($\text{Ст } q \leq \text{Ст } p$).
 - В корне $q(u)$ используем модифицированный остаток:
$$a^k p(u) = s(u) q(u) + r(u). \quad \text{Ст } r < \text{Ст } q \leq \text{Ст } p$$
Знак a и четность k , как и знак r – известны. Отсюда ясен знак p .

Доказательство теоремы Тарского – Зайденберга

Добавляем 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, входящей в диаграмму) и знак в промежутке тот же.
 - Если в одном из соседних корней $p(u)=0$, то на промежутке нет корней $p(u)$ (аналогично).
 - Если в соседних корнях u $p(u)$ разные знаки, то на промежутке – ровно 1 корень $p(u)$ (аналогично).
- Ищем корни на крайних (полубесконечных) сегментах. Знаки в бесконечностях известны. Корней не больше одного на сегмент, аналогично предыдущему.

Доказательство теоремы Тарского – Зайденберга

Добавляем 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, в появившихся столбцах, клетки из других строчек.

Лемма доказана.

Доказательство теоремы Тарского – Зайденберга

Мы можем заменить всякую формулу

$\exists u B(u, x_1, \dots, x_n)$, где B – бескванторная, на эквивалентную, построенную в предыдущем доказательстве.

Именно: для каждой диаграммы D (расширенной) системы многочленов, для которой $\exists u B(u, x_1, \dots, x_n)$ - истинна, берем ее часть D' – диаграмму без u , из которой она восстанавливается. Берем конъюнкцию атомных формул, описывающую диаграмму D' . Берем дизъюнкцию этих конъюнкций по всем диаграммам D , для которых $\exists u B(u, x_1, \dots, x_n)$ истинна.

Мы можем заменить всякую формулу

$\forall u B(u, x_1, \dots, x_n)$ на эквивалентную $\neg \exists u \neg B(u, x_1, \dots, x_n)$.

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' :
- 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.

q	+
p	–
$4q - p^2$	–
$2q - p^2$	–

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

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

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

Корень имеется в первом столбце.

- Добавляем многочлен x^2+px+q .
- Его знак в нуле многочлена $2x+p$?
 $4(x^2+px+q) = (2x+p)(2x+p) + 4q - p^2$.
Знак равен знаку остатка $4q - p^2$ (-).
- Его знак в нуле многочлена $px+q$?
 $p^2(x^2+px+q) = (px+p^2-q)(px+q) + q^2$.
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: $\langle \mathbb{R}, \langle \{0, 1\}, \{+, *\}, \{=, >\} \rangle, \exists N \rangle$
(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 $\langle \mathbb{R}, \langle \{0, 1\}, \{+, *\}, \{=, >\} \rangle, \exists N \rangle$ – 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 (права Ньютона) доказана Л. Ван дер Варденом и К. Шютте в 1953 году (без теоремы Тарского).
- <http://www.etudes.ru/ru/mov/mov004/>