Математическая логика и теория алгоритмов

Алексей Львович Семенов

Заведующий кафедрой математической логики и теории алгоритмов
Академик Российской академии наук
и Российской академии образования

Лекция 4. Элиминация кванторов для поля действительных чисел

План:

- Примеры. Уравнения с параметрами
- Алгебра многочленов
- Доказательство: диаграммы
- Полуалгебраические множества
- Проекция. Элиминация кванторов
- Теорема Тарского
- Применения: геометрия

Исходный пример

Условие существования решения уравнения

$$x^2+px+q = 0:$$

$$p^2 - 4q \geq 0$$

В терминах определимости:

Формула $\exists x\ (x^2+px+q = 0)$
эквивалентна формуле

$$p^2 - 4q \geq 0,$$

то есть задает то же отношение:
множество пар действительных чисел (p, q).

x - переменная p, q - параметры

$\exists x\ (ax^2 + bx - c > 0)$?

$a>0$

$a=0 \wedge\ldots$

$a<0\ldots$

Еще примеры

Есть ли (действительный) корень у алгебраического уравнения
(с параметрами) от одной переменной?

(Нечетная и четная степень. Случай нулевого коэффициента)

При каких значениях параметров есть корень?

Как записать ответ в виде **алгебраических** условий на параметры?

Как быть, когда многочленов несколько и спрашивается про комбинацию их знаков, есть ли «корень» - выполняющее все условия значение x ?

Обобщение

Рассмотрим любую систему уравнений и неравенств от *x*:

- $p(x)=0$, $p(x)>0$, $p(x)<0$, где $p(x)$ – многочлены от нескольких переменных с целыми коэффициентами; *x* - выделенная переменная, коэффициенты - многочлены от других переменных – параметров.
- Еще общее – любая бескванторная формула (например, ДНФ без отрицаний), где атомные формулы имеют вид $p(x)=0$ $p(x)>0$ $p(x)<0$, где $p(x)$ – многочлены от нескольких переменных с целыми коэффициентами.

Вопрос, существует ли *x*?

Можно ли записать существование *x* как ДНФ от многочленов от параметров.

Общая идея

«Обобщенный метод интервалов»

«Змея» метода интервалов дает ответ о существовании *x* для одного многочлена. «Точные» корни знать ненужно (и невозможно).

Можно нарисовать несколько «змей», но нужно рассмотреть все варианты взаимного расположение (порядка на прямой) корней и понять, каким значениям параметров эти варианты соответствуют.

Понятие ***диаграммы***.

Диаграмма семейства многочленов

Действительные числа. Метод интервалов

$p_1(x)$	+	0	–	0	+	0	+	+	+
$p_2(x)$	–	0	+	+	+	+	+	+	+
$p_3(x)$	–	–	–	0	+	+	+	0	–

О. Знак многочлена в точке: 0, +, –…

Сегмент – точка, или открытый интервал.

На каждом сегменте знак каждого многочлена постоянен.

В левом столбце перечислены все многочлены семейства.

Что значит, что строчка диаграммы состоит из одних плюсов?

Что значит, что строчка диаграммы содержит только из + и --, и есть и те и другие?

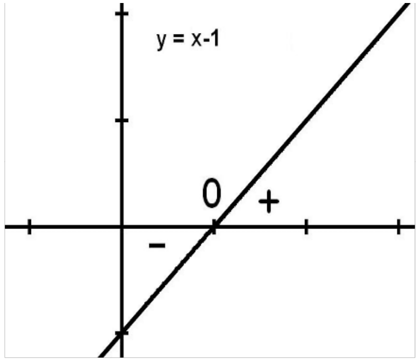
Если взять другие значения параметров, то диаграмма будет другой.

У. Сведение к диаграммам

Если известна диаграмма семейства многочленов, то известно, существует ли *x*, для которого данная бескванторная формула, включающая только многочлены семейства, истинна.

Диаграмма для одного многочлена

Пример



$x_2x + x_1$	-	0	+

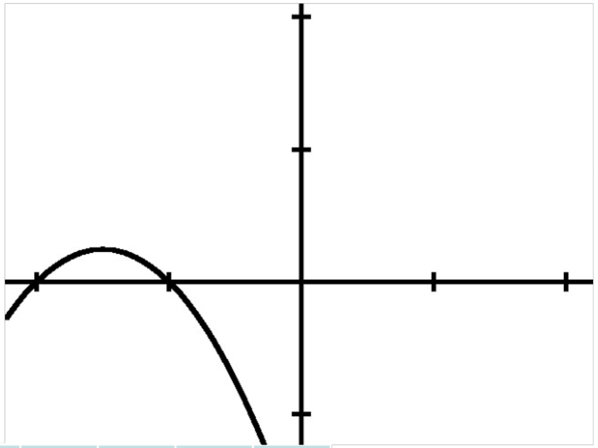
«это – диаграмма x_2x+x_1»
$\leftrightarrow$ $x_2>0$

Диаграмма для многочлена от параметров:

x_2	**+**

Диаграмма для одного многочлена

Пример



-	0	+	0	-

«это – диаграмма $x_3x^2+x_2x+x_1$»
$\leftrightarrow x_3<0 \land x_2^2 - 4x_3x_1>0$

Диаграмма для многочленов от параметров:

x_3	--
$x_2^2 - 4x_3x_1$	+

Цель: Доказать, что диаграмма семейства многочленов от *x* определяется диаграммой семейства многочленов от параметров, входящих в коэффициенты

Вопрос о существовании корня сводится к вопросу о диаграммах: относится ли диаграмма к одному из видов…

Вопрос о виде диаграммы можно свести к вопросам о диаграммах для более простых многочленов – меньшей степени.

В конце концов, понижая степень, мы придем к вопросу о многочленах нулевой степени (по x) – это и будет элиминация квантора существования.

Дойдя до нуля мы должны будем восстановить исходную диаграмму.

Что это за более простые многочлены?

Построение диаграммы для семейства нескольких многочленов

Взаимное расположение корней

Добавляем многочлен *p(x)* к семейству, для которого есть диаграмма

Чтобы построить диаграмму, включающую *p*, нужно для каждого уже имеющегося сегмента:

- определить знак на этом сегменте
- может быть, разбить сегмент на несколько

Есть ли корень многочлена *p* на сегменте?

- Знак многочлена *p* в корне другого многочлена *q*
- Наличие корня многочлена *p* между корнями других многочленов
- Может ли между корнями оказаться два корня *p?*

Если знаки *p* концах сегмента различные, то…? Если знаки *p* в концах сегмента одинаковые…?

Вариант: есть ли корни *p* меньше самого маленького корня многочлена *q* ?

Алгебра многочленов

Самый важный элемент редукции

Многочлены от одной переменной (как всегда – с параметрами)

По многочлену *p* и многочлену *q* той же, или меньшей степени, можно построить такой многочлен *r* **меньшей степени**, чем *q*, что:

- **знак многочлена *p* в корне многочлена *q* равен знаку многочлена *r* в том же корне.**

У. Как построить ***r*** ?

Алгебра многочленов

Ключевое соображение

Многочлены от многих переменных. По многочлену p и многочлену q той же или меньшей степени можно построить такой многочлен r меньшей степени, что:

- знак многочлена p в корне многочлена q можно найти по знаку многочлена r в той же точке.

У. Как построить r ?

$$p = uq + r,$$

для некоторого u – деление с остатком.

Знаки просто совпадают. Но всегда ли r – многочлен?

Числовой пример:

делим $4x^3 + 3x^2 + 2x + 1$ на $5x^2 + 6x + 7$.

$$4x^3 + 3x^2 + 2x + 1 = ((4/5)\,x - 9/25) \cdot (5x^2 + 6x + 7) - (36/25)\,x + 88/25$$

У. Как построить r так, чтобы он действительно был многочленом (от всех переменных), не содержал алгебраических дробей?

Алгебра многочленов

Где возникают дроби?

У. На что мы умножаем и делим в процессе деления?

Чтобы не возникало дробей, надо заранее *p* **домножить** на нужную степень старшего ненулевого коэффициента *q*.

Нужно использовать настоящий (не нулевой) старший коэффициент.

У. Найти степень для **домножения**.

$d = deg(p) - deg(q) + 1$

Получается *операция модифицированного деления*.

У. Как теперь определить знак *p* в корне *q* по знаку *r* ?

Алгебра многочленов

Соображения, которые мы будем использовать

У. Если в концах интервала у функции разные знаки, то на этом интервале у нее есть корень.

- В диаграмме добавится этот корень

У. Если в концах интервала функция имеет один знак, и есть корень, то на интервале есть корень производной.

- Надо предусмотреть производную при редукции,
- тогда если в концах СЕГМЕНТА знак одинаковый, то корня нет

У. Знак многочлена в плюс и минус бесконечности определяется номером и знаком старшего **не нулевого** коэффициента.

Алгебра многочленов

Соображения, которые мы использовали

У. Если на интервале функция меняет знак,
на этом интервале есть корень

- Не нулевой старший коэффициент
- Модифицированный остаток от деления на многочлен, где отброшены члены с нулевым коэффициентом

У. Если на интервале у **производной** функции нет корня, то на этом интервале у функции нет двух корней.

У. Знак многочлена в плюс и минус бесконечности определяется номером и знаком старшего **не нулевого** коэффициента.

Формальное доказательство. Редукция

Операции редукции

Мы выясняли что-то про знаки и корни многочлена, пользуясь информацией о многочленах меньшей степени, получавшихся операциями:

1. **Модифицированный остаток**
2. **Взятие старшего коэффициента**
3. **Отбрасывание старшего члена**
4. **Дифференцирование**

У. Что нам дает каждая из операций?

Формальное доказательство.

Расширение семейства многочленов

Последовательность семейств многочленов

Дано семейство многочленов F, степени, не превосходящей n. Индуктивно определим последовательность: $F_n, \ldots F_0$:

$F_n = F;$

F_{k-1} получается из F_k применением операций 1–4 к F_k, а также применением операции модифицированного остатка от деления многочленов из F_k на все уже полученные многочлены из F_{k-1}.

У. Степени многочленов F_k не превосходят k.

У. F_0 содержит все коэффициенты всех многочленов из F_n.

Построение (потенциальной) Большой диаграммы

Диаграмма исходного семейства – верхняя часть Большой диаграммы

Левый столбец большой диаграммы состоит из блоков.

F_n
F_{n-1}
….
F_0

В n-ом блоке выписаны в каком-то порядке элементы F_n.

Построение (потенциальной) Большой диаграммы

Нулевой шаг

Добавляем к таблице один столбец.

F_n	
F_{n-1}	
….	….
F_0	

В нижнем (0-ом) блоке столбца в каждой строке ставим какой-то знак против каждого многочлена. Все они – нулевой степени по *x*.

Построение (потенциальной) Большой диаграммы

Идем снизу вверх. Очередной шаг.

Заполняем строки, соответствующие многочлену *p* из *k*-ого блока и создаем новые столбцы.

F_n	
F_{n-1}	
p ….	….
F_0	

I) заполняем каждую клетку, отвечающую <u>корню</u> стоящего ниже многочлена (степени не выше *k*).
Делим *p* на этот многочлен, используем и знаки старших коэффициентов (где их взять?) и знак из остатка (он есть в блоке ниже)

II) заполняем клетки, отвечающие <u>конечным интервалам</u>:
в концах одинаковые знаки, или ноль и не ноль. Копируем не ноль.
в концах + и –. Разбиваем столбец
на три (по всей высоте), ставя соответствующие знаки (какие?).

III) заполняем клетки, отвечающие <u>бесконечным интервалам</u>, с учетом старшего члена с ненулевым коэффициентом; могут возникнуть три столбца

У. Доказать, что получается диаграмма

Завершение доказательства

Формула $\exists x(\Phi)$, где Φ – бескванторная, атомные – знак многочлена:

1. F - все многочлены, входящие в Φ
2. Строим последовательность редукций $F_n = F, \ldots, F_0$.
3. Все заполнения знаками F_0 , потенциальные большие диаграммы (ПБД).
4. Отбираем ПБД, где существует x, выполняющее Φ. Как?
5. Из каждой отобранной диаграммы выделяем F_0 . Конъюнкция атомных формул. Каких?
6. Строим дизъюнкцию выписанных конъюнкций. Она эквивалентна формуле $\exists x(\Phi)$.

Полуалгебраические множества

Что определимо (является значением формулы) в структуре действительных чисел, полиномиальных равенств и неравенств?

Мы представляем себе множество решений… в виде формы... в одних направлениях 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.

Юрий Иванович Манин
16.02.1937 -

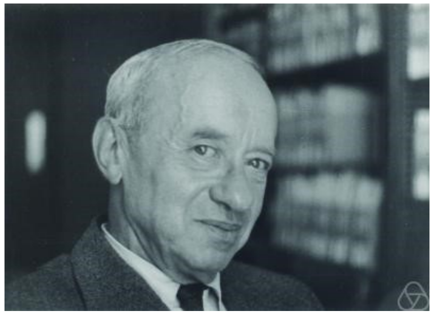
Теорема Тарского об определимости в поле действительны чисел

Универсум – действительные числа. Язык *LR: логические связки, переменные для действительных чисел, кванторы*

Атомная формула – равенство нулю, положительность или отрицательность многочлена (от нескольких переменных) с целыми коэффициентами.

Т. Тарского: По всякой формуле можно построить бескванторную, ей эквивалентную.

Иная формулировка: Все определимые отношения определяются бескванторными формулами.



Альфред Тарский
14.01.1901 –
26.10.1983

Разрешимость

Частный случай. Что происходит, если в исходной формуле нет свободных переменных?

У. Построить алгоритм, выясняющий истинность любого высказывания языка *LR.*

Следствие. Геометрия

Любое утверждение элементарной геометрии можно записать как алгебраическое.

В силу теоремы Тарского можно проверить истинность любой теоремы.

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/

Лекция 4. Элиминация кванторов

Что было:

- Примеры. Уравнения с параметрами
- Алгебра многочленов
- Доказательство: диаграммы, редукция
- Полуалгебраические множества
- Проекция, как элиминация кванторов
- Теорема Тарского
- Применения: геометрия