Введение в математическую логику и теорию алгоритмов

Лекция 4

Алексей Львович Семенов

Определимость отношений (повт.)

- Множество *D*
- Семейство *R* отношений на *D*. Структура
- Какие отношения (элементы D^N) можно объяснить, выразить, определить через *R*?
- Объяснять можно на языке – языке логики отношений.
- Например, можно определить, объяснить отношение «между» на действительной прямой через отношение «меньше».
- Через сложение и умножение можно определить отношения на **N**:
  - z является остатком от деления x на y
  - $y=2^x$
  - Произвольное вычислимое (каким-то алгоритмом) отношение

Порядок на рациональных числах

Структура <**Q**, =, <, Зн>. Какие отношения определимы?

- Фиксируем натуральное n. Все формулы от n переменных. Интерпретации – последовательности (цепочки) длины n рациональных чисел.
- Последовательная формула имеет вид:
- $\Lambda\, x_{\sigma(i)}\, \mu_i\, x_{\sigma(i+1)}$, $i = 1,\ldots, n$,
- где σ – некоторая перестановка (изоморфизм) множества {1,… n}, для каждого i: μ_i - один из символов =, <.
- **Вопрос**. В чем содержательный смысл понятия последовательной формулы?

Задача. Всякая бесквантворная формула эквивалентна дизъюнкции последовательных и для каждой из них существует интерпретация, в которой и она, и исходная формулы истинны.

Вопрос. Как быть с отрицанием?

Д. Истинность бесквантворной формулы в интерпретации однозначно определяется последовательной формулой для этой интерпретации.

- О. Две интерпретации эквивалентны, если их последовательные формулы совпадают.

Аналогия с СДНФ

Конструкция «Разбор случаев». Были: «Диагональ», «Челнок» (К – Б).

Задача. Как для каждой формулы вида $\exists u\ \Phi(x_1, x_2, \ldots, x_n)\ [\ u / x_i\ ]$, где Φ – последовательная, построить эквивалентную ей бесквантворную?

Задача. Как для любой формулы построить эквивалентную ей бесквантворную?

Все определимое устроено просто.

Что с утверждениями (формулами без свободных переменных)?

Элиминация кванторов

Поле действительных чисел. Определимые отношения

Структура:

$\mathcal{R} = \langle \mathbb{R}, p(\ ) =, > 0$ – для всех полиномов p с целыми коэфф., *Зн*$\rangle$

• Что определимо?

• Алгебраические отношения (множества в $\mathbb{R}^N$) – системы (конъюнкции) уравнений

Юрий Иванович 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. Многообразие всех отношений

- Полуалгебраические множества – объединения, пересечения и дополнения множеств, задаваемых уравнениями и неравенствами
- Применим к полуалгебраическим множествам (отношениям) проекцию.
- Она соответствует квантору существования для формул.
- Получится ли больше отношений?
- Нет – теорема Тарского – Зайденберга
- Логическая (кванторная) сложность – ограничена.

Теорема Тарского (– Зайденберга)

- **О**. *эквивалентные* в данной структуре <*D*,…> формулы - задают одно и то же отношение (на D^N)
- **Т**. Существует алгоритм, который для всякой формулы сигнатуры структуры $\mathfrak{R}$ строит эквивалентную ей в этой структуре бескванторную формулу.
- **Следствие.** Проекция полуалгебраического множества – полуалгебраическое множество.

Пример. $x^2+px+q = 0$ задаёт множество троек $\langle x, p, q\rangle$.

- Его проекция вдоль оси x

  на плоскость $p, q – p^2 - 4q \geq 0$.

  полуалгебраическое множество

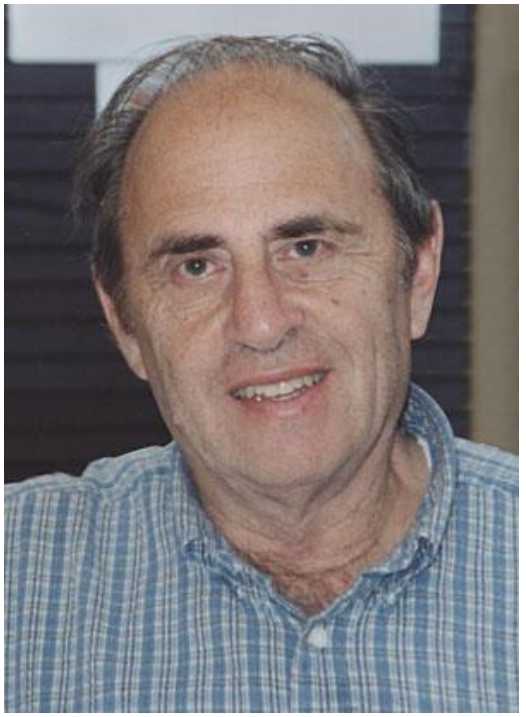
Альфред Тарский

(14.01.1901 — 26.10.1983)

Доказательство теоремы Тарского – Зайденберга

- Для формул с единственным квантором существования $\exists u\ \Phi(x_1, \ldots, x_n)\ [\ \boldsymbol{u}\ /\ x_i\ ]$, где Φ – бесквантворная, будем строить эквивалентную (задающую то же отношение на $\mathbb{R}^N$) бесквантворную .
- Атомные формулы в Φ имеют вид $p(u, x_1, \ldots, x_n) = 0$ или $p(u, x_1, \ldots, x_n) > 0$, где p – многочлен с целыми коэффициентами.
- Многочлен p можно рассматривать как многочлен от переменной u, коэффициенты которого – многочлены от $x_1, \ldots, x_n$.
  Надо доказать, что те векторы $\langle x_1, \ldots, x_n \rangle$, при которых u существует, образуют полуалгебраическое множество.

Доказательство



Пол Коэн (02.04.1934 — 23.03.2007)

Школьный «Метод интервалов»

Диаграмма – схема из метода интервалов.

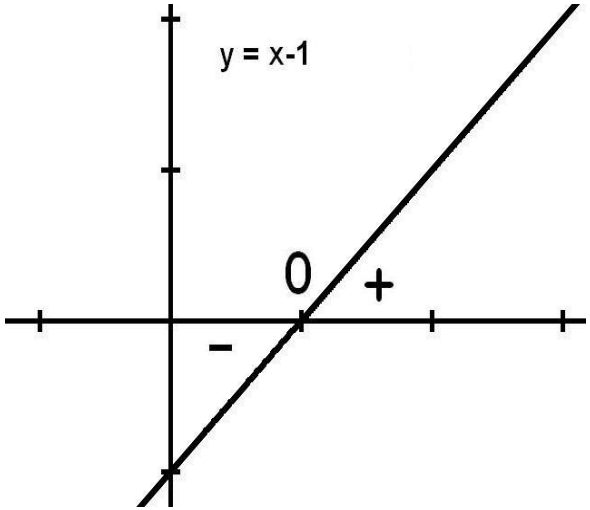
Вместо графика функции, или его наброска используется схема:

- прямая, где (обычно, без соблюдения масштаба) помечены корни и проведена пересекающая ее в корнях «змейка», там, где она выше прямой, функция положительна, где ниже – отрицательна.
- $\langle x_1, \ldots, x_n \rangle$ - параметры, из «уравнений с параметрами»

Диаграмма многочлена (неформ.)

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

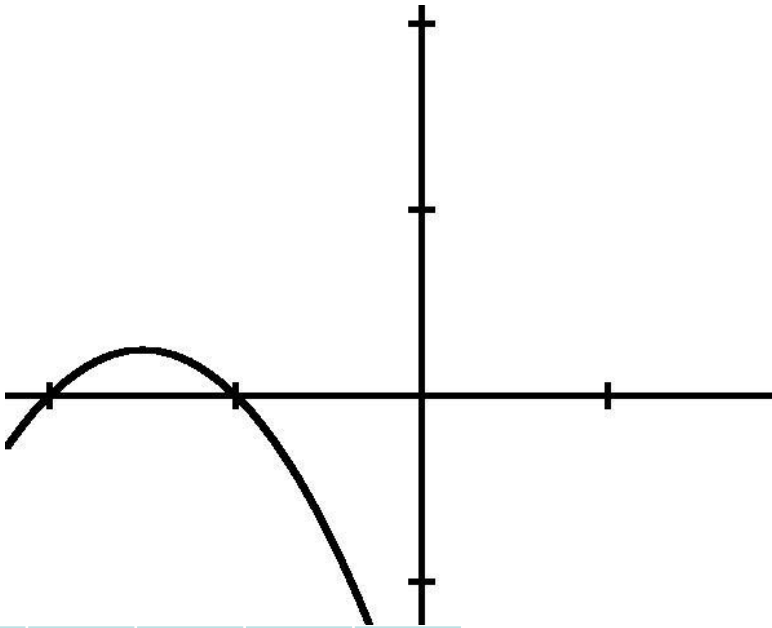
Диаграмма – цепочка знаков от минус до плюс бесконечности



-	0	+

«это – диаграмма x_2u+x_1»

$\leftrightarrow x_2>0$



-	0	+	0	-

«это – диаграмма $x_3u^2+x_2u+x_1$»

$\leftrightarrow x_3<0 \wedge x_2^2 - 4x_3x_1>0$

Существование корня, точки положительности…- видны из диаграммы

Пример используемых соображений.

Знак многочлена в корне другого многочлена

Пусть $p = sq + r$,

d – корень многочлена $q(u)$

Нужно найти Знак p в точке d

- Знак $p(d)$ = Знак $r(d)$
- Если r – остаток от деления p на q,

то r проще (имеет меньшую степень), чем q

Если q проще p, то r проще, чем p

Диаграмма семейства многочленов.

- Все семейства в этом доказательстве - конечные.
- Пусть задано семейство многочленов. Прямая $\mathbb{R}$ разбивается всеми корнями многочленов семейства на сегменты (включая одноточечные):
  $(-\infty, a_1), [a_1], (a_1, a_2), [a_2], \ldots, [a_n], (a_n, +\infty)$
- 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

Выбросим из таблицы имена сегментов

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

Диаграмма семейства многочленов в точке a – наборе значений $x_1, \ldots, x_n$.

Это – диаграмма семейства $u^2-\mathbf{x}_1\,\mathbf{x}_2$, $u(u-\mathbf{x}_2)(u-\mathbf{x}_1)$ в точке <1, 2>.

$u^2-\mathbf{x}_1$	+	0	–	–	–	0	+	+	+
$\mathbf{x}_1\,u(u-\mathbf{x}_2)(u-\mathbf{x}_1)$	–	–	–	0	+	0	–	0	+

Задача. Дать определение диаграммы семейства.

Таблица для семейство многочленов: имена строк – все элементы семейства, количество столбцов – не больше удвоенного возможного числа корней (степени по u) плюс 1, в клетках – знаки.

Таких таблиц – много. Среди них есть все диаграммы семейства в разных точках, но могут быть и не диаграммы.

Доказательство теоремы Тарского – Зайденберга.

- **Задача**. Различных таблиц для данного семейства многочленов – конечное число.
- Фиксируема формулу $\Phi(u, x_1, \ldots, x_n)$. Пусть F – семейство всех многочленов, входящих в $\Phi(u, x_1, \ldots, x_n)$, a – набор значений переменных $x_1, \ldots, x_n$
- Тогда по диаграмме F в точке a можно определить истинность формулы $\exists u\ \Phi(u, x_1, \ldots, x_n)$ в этой точке.
- пространство $\mathbb{R}^n$ точек – значений для $\langle x_1, \ldots, x_n \rangle$ разбивается на конечное число частей, отвечающих всем возможным диаграммам (по u).
- Нужно доказать, что эти части – полуалгебраические.

Доказательство теоремы Тарского – Зайденберга

Определим 4 операции на семействах многочленов.

1. Модифицированный остаток

Дано: пара 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 $q(u)$.

Получаем: *модифицированный остаток от деления* $p(u)$ на $q(u)$ = остаток от деления $a^k p(u)$ на $q(u)$.

Вопрос. Что дает домножение на a^k ?

Степень (по *u*) модифицированного остатка меньше степени *q*.

Доказательство теоремы Тарского – Зайденберга

Определяем еще 3 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 многочлену положительной степени эта степень уменьшается. Применение операции к многочлену нулевой степени дает его самого или 0.

Поэтому замыкание конечного семейства многочленов относительно этих операций конечно.

Задача. Оценить, сколько.

Доказательство теоремы Тарского – Зайденберга.

- Пусть F_0 – часть F, состоящая только из многочленов степени 0 по u (они представляют собой многочлены из $\mathbb{Z}[x_1, \ldots, x_n]$).
- Диаграмма для множества F_0 состоит из одного столбца.
- **Лемма.** Пусть F – семейство многочленов из $(\mathbb{Z}[x_1, \ldots, x_n])[u]$, замкнутое относительно перечисленных операций 1-4.
- Тогда диаграмма множества F в данной точке может быть построена по диаграмме множества F_0 в той же точке.
- То, что диаграмма множества F_0 данная, записывается бескванторной формулой (конъюнкцией знаков многочленов от $X_1, \ldots, X_n$).

Доказательство теоремы Тарского – Зайденберга. Доказательство Леммы

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

Доказательство теоремы Тарского – Зайденберга. Доказательство Леммы

Задача. Добавляем многочлен p. Что происходит с диаграммой?

- Какие появляются строки?
- Какие появляются столбцы?
- Как искать Знак p в корнях уже рассмотренных многочленов?
- Использование операций 1 – 4.

пример соображения:

Если в соседних корнях уже рассмотренных многочленов $p(u)$ 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

Доказательство теоремы Тарского – Зайденберга

Для всякой формулы

$\exists u\, B(u, x_1, \ldots, x_n)$, где B – бескванторная, мы строим эквивалентную бескванторную:

- Выписываем семейство всех многочленов из B.
- Строим замыкание F' семейства (относительно 4-ех операций).
- Берем в замыкании часть нулевой степени F_0.
- Строим (восстанавливаем) таблицу для F, из таблицы для F_0 (из одного столбца),
- Отбираем из таблиц для F те, которые обращают $\exists\, u\, B(u, x_1, \ldots, x_n)$ в истину. Берем те таблицы из F_0, из которых они получились.
- Для каждой взятой таблицы из F_0 записываем бескванторную формулу, (конъюнкция утверждений о каждой клетке).
- Искомая – дизъюнкция построенных формул.

. Доказательство теоремы Тарского – Зайденберга

Преобразование произвольной формулы в бесквантворную идет индукцией по построению («изнутри»)

Если при построении мы навешивали квантор $\exists$, то теперь мы его навешиваем и сразу избавляемся.

Мы заменяем всякую формулу

$\forall u\, B(u, x_1, \ldots, x_n)$ на эквивалентную

$\neg\exists u \neg B(u, x_1, \ldots, x_n)$.

Со связками – очевидно.

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

(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).

- Множество F_0 составляют 8 многочленов (4) – (11).

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

- Для сокращения перебора можно не рассматривать противоречивые диаграммы. Знаки многочленов, тождественно равных 1 и 2, – известны. 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 $3^4=81$.

q	+
p	–
$4q - p^2$	–
$2q - p^2$	–

- 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.

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.
  Корень имеется в первом столбце.

q	+	+	+
$\boldsymbol{p}$	–	–	–
$4q - p^2$	–	–	–
$2q - p^2$	–	–	–
$2x+p$	–	0	+

- Добавляем многочлен x^2+px+q.
- Его знак в нуле многочлена $2x+p$?
  $4(x^2+px+q) = (2x+p)(2x+p) + 4q - p^2$.
  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

- Что дает алгоритм для формул без свободных переменных?
- Он отвечает на вопрос об истинности формул.
- Следствие Теоремы Тарского – Зайденберга.
- Теория $\mathcal{R}$ разрешима: существует алгоритм, который по утверждению в нашей сигнатуре (многочлены…), выясняет, истинная ли она в нашей структуре (действительные числа…).

Геометрия

- С помощью метода координат большинство геометрических утверждений можно записать как утверждения о действительных числах.
- Исключение. Не получится 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/