Лекция 5

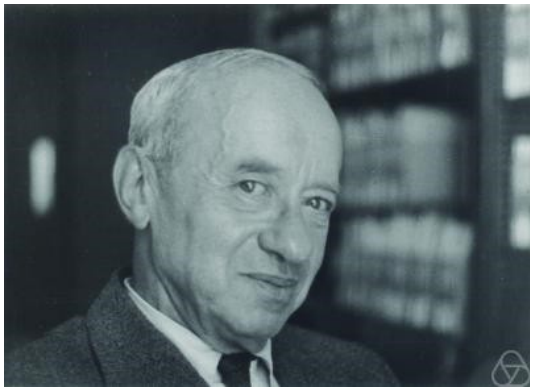
Сегодня мы будем заниматься выразимостью отношений в некотором специальном и важном случае – это случай поля действительных чисел, и я докажу теорему, одну из двух или трёх технически сложных теорем курса. Основное содержание доказательства – это простые соображения из математического анализа. Чтобы понять это доказательство, достаточно школьных знаний.

Начнём с некоторых вспомогательных определений. Будем называть эквивалентными на данной модели <*S*…> формулы, задающие одно и то же отношение (на S^{ω}). Будем назвать эквивалентными формулы, эквивалентные на любой модели.

Выше мы уже упоминал, что отношения – это подмножества многомерного (или счетно-мерного) пространства. Естественно, что логические связки соответствуют операциям над множествами (конъюнкция – пересечение, дополнение и т. д.). При выполнении операций удобно использовать именно бесконечномерное пространство. Логическим связкам при этом естественно соответствуют операции над множествами: например, конъюнкции – пересечение.

Навешивание квантора существования соответствует проекции (нарисуйте двумерное множество и его проекции на оси координат и выпишите соответствующие формулы, если множеству соответствует имя отношения $R(x_1,x_2)$). Итак, вернемся к нашей теме. Мы будем заниматься моделью,которая называется поле действительных чисел: ⟨ℝ, ⟨{0, 1}, {+, ⋆}, { =, >}⟩, *Зн*⟩ (упорядоченное множество действительных чисел со сложением и умножением и константами 0 и 1). Что выразимо в этой модели? Ясно, что в рассматриваемом языке можно записать равенство нулю любого многочлена с целыми коэффициентами. Для этого можно, например, записать равенство двух многочленов с натуральными коэффициентами и т. д. Далее, нетрудно записать и конъюнкцию таких равенств. Варажаемые такими формулами множества называются алгебраическими. Полуалгебраические множества – это объединения, пересечения и дополнения множеств, выражаемых уравнениями и неравенствами. Ответы к задачам школьного задачника по алгебре – это, обычно, полуалгебраические множества. Можно применять к полуалгебрическим множествам проекцию, соответствующую квантору существования для формул. Получится ли больше отношений? Оказывается – нет, и в этом состоит т. н. теорема Тарского, или Тарского – Зайденберга, доказательство которой мы сегодня занимаемся.

Альфред Тарский – один из тех знаменитых математических логиков 20 века, относящийся к той, примерно, десятке математиков, некоторых из которых я уже упоминал, это Гильберт и Гёдель. Альфред Тарский, польский еврей, большую часть своей жизни прожил в Соединённых Штатах. Открытая им в 1930-е гг. теорема (опубликованная в 1948 году) имеет множество приложений, вы с ними наверняка ещё встретитесь, если вы будете заниматься, скажем, современной алгеброй. Зайденберг внятно изложил этот результат и популяризировал его.



Теорема Тарского (– Зайденберга)

Существует алгоритм, который для всякой формулы сигнатуры $\langle\langle 0, 1\rangle, \langle +, *\rangle, \langle =, >\rangle\rangle$ строит бесквантерную 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 $p^2 - 4q \geq 0$. Это – материал школьного учебника алгебры. Но теорема Тарского утверждает, что аналогичные условия могут быть сформулированы для уравнений третьей, четвертой, пятой и т. д. степеней! Можно рассматривать уравнения с несколькими неизвестными и т.д.

Перейдем к доказательству.

Будем надеяться, что вы сумеете уследить за ходом доказательства. Значит, как мы помним, таким ключевым моментом является действительно устранение одного квантора существования, то есть проекция. С этим мы уже несколько свыклись. И мы сейчас займёмся только этим случаем.

Начнем с формул с единственным квантором существования $\exists u\ B(u, x_1,\ldots, x_n)$, где B - бесквантерная. Будем строить эквивалентную ей (задающую то же отношение на $\mathbb{R}^\omega$)бесквантерную.

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 $\exists u\ B(u, x_1,\ldots, x_n)$ истинна, – полуалгебраическое множество.

Следующее определение – центральное в доказательстве.
Диаграмма набора многочленов от одной переменной.
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) , $[a_2]\ldots$, $[a_n]$, $(a_n, +\infty)$. В клетке стоит знак многочлена на сегменте.
При этом сами сегменты (написанный над верхней строкой диаграммы) в диаграмму не входят, а многочлены (первый столбец диаграммы) входят.
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.

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

Наше понятие диаграммы непосредственно связано со школьным методом интервалов. Только мы не рисуем змею, пересекающую числовую ось, а выписываем таблицу.

Легко видеть следующее:

- Пусть все многочлены, входящие в бескванторную формулу $\Phi(u, x_0, \ldots, x_{n-1})$ входят в набор F. Тогда истинность формулы $\exists u\, \Phi(u, x_0, \ldots, x_{n-1})$ при каждом векторе $\langle x_0, \ldots, x_{n-1}\rangle$ определяется диаграммой набора F для этого вектора
- Ширина диаграммы может меняться, но ограничена для данного набора (поскольку число корней каждого из многочленов ограничено его степенью).
- Число возможных диаграмм для данного F конечно, пространство $\mathbb{R}^n$ наборов $\langle x_0, \ldots, x_{n-1}\rangle$ разбивается на конечное число частей, отвечающих всем возможным диаграммам.

Наша задача - доказать, что эти части – полуалгебраические множества.

Определим 4 операции на семействах многочленов.

1. Операция для пары p,q многочленов от u (с коэффициентами из $\mathbb{Z}[x_0, \ldots, x_{n-1}]$).
   Пусть k = степень $p(u)$ – степень $q(u)+1$, a – старший коэффициент $q(u)$.
   Дает: *модифицированный остаток* от деления $p(u)$ на $q(u)$ = это остаток от деления $a^k p(u)$ на $q(u)$.

Считаем, что степень p больше степени q (тогда остаток отличен от q). Модификация нам понадобилась, чтобы в результате операции получался многочлен с коэффициентами, являющимися многочленами от $x_0, \ldots, x_{n-1}$ (с целыми коэффициентами).

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.

Лемма. Пусть F – конечный набор многочленов из $(\mathbb{Z}[x_0, \ldots, x_{n-1}])[u]$, замкнутый относительно перечисленных операций.

- Пусть F_0 – его часть, состоящая только из многочленов степени 0 по u (они представляют собой многочлены из $\mathbb{Z}[x_0, \ldots, x_{n-1}]$, в диаграмме для F_0 – один столбец).
- Тогда диаграмма множества F при данных $x_0, \ldots, x_{n-1}$ полностью определяется диаграммой множества F_0 при тех же $x_0, \ldots, x_{n-1}$.

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.

Добавляем p.

- Старший коэффициент p имеет нулевую степень и есть в диаграмме. Он:

$=0$ (нулевая строка в диаграмме), тогда p уже есть в диаграмме

$\neq 0$, тогда:

- Ищем 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.
- 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 у $p(u)$ 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.

Теперь меняем нашу диаграмму.

- 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.

Переходим к доказательству теоремы.

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

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

Мы можем заменить всякую формулу $\forall\ u\ B(u, x_1, \ldots, x_n)$, на эквивалентную $\neg\exists u\ \neg\ B(u, x_1, \ldots, x_n)$

Таким образом, для всякой формулы строим эквивалентную ей без кванторов.

Итак, мы рассмотрели модель: $\langle \mathbb{R}, \langle \{0, 1\}, \{+, \cdot\}, \{=, >\}\rangle, Зн\rangle$ (упорядоченное множество действительных чисел со сложением и умножением и константами 0 и 1).

Что дает алгоритма для формул без свободных переменных? Он отвечает на вопрос об истинности формул.

Следствие Теоремы З-Т. Множество формул, истинных в модели $\langle \mathbb{R}, \langle \{0, 1\}, \{+, \cdot\}, \{=, >\}\rangle, Зн\rangle$ -разрешимо.

С помощью метода координат большинство геометрических утверждений можно записать как утверждения о действительных числах. (Это было открытие Декарта)

Исключение: n-угольники без указания конкретного n.

Возьмём какую-нибудь теорему из геометрии, например, что высоты треугольника пересекаются в одной точке. Можем ли мы это утверждение записать в виде факта про действительные числа? Подумайте.
Пример. Гипотеза 13 шаров: спор между Ньютоном и Грегори (1694 г.): "Сколько материальных шаров равных радиусов можно "прислонить" к фиксированному шару того же радиуса?" Ньютон – 12, Грегори – 13. (Подумайте, сколько монет можно прислонить к одной.) Двенадцать шаров помещаются довольно свободно (для начала поставив их в вершины икосаэдра). Можно ли поместить тринадцатый?

- Существование решения у системы уравнений с 39 неизвестными
- Невозможность 13 шаров (правота Ньютона), доказана Л. Ван дер Варденом и К. Шютте в 1953 году (без теоремы Тарского).
- http://www.etudes.ru/ru/mov/mov004/ (Коллекция Николая Андреева.)