Лекции по математической логике и теории алгоритмов
А. Л. Семенов, 2022
Лекция 4

1 Элиминация кванторов в поле действительных чисел

Неформальное замечание. Как было замечено на прошлой лекции, сложность отношения, определяемого формулой, бывает связана с кванторами, входящими в эту формулу, например, в ее предваренной нормальной форме, когда кванторы впереди. Стратегия в соответствующей игре может быть сложной и т.д. Во многих важных случаях, например, когда в качестве универсума выбрано множество натуральных чисел, а в качестве сигнатуры взяты трехместные отношения суммы $x+y=z$ и произведения $x \cdot y = z$, добавление кванторов дает все более и более сложные отношения, образующие т. н. *арифметическую иерархию.*

Есть, однако, замечательный случай, когда добавление кванторов не приводит к расширению множества отношений.
Это случай поля действительных чисел, где сигнатура также состоит из трехместных отношений сложения и умножения. Мы будем рассматривать другую, более широкую сигнатуру для того же универсума действительных чисел. В ней атомными формулами будут: равенство нулю, положительность и отрицательность полиномов от нескольких переменных с целыми коэффициентами. Логику отношений с такой сигнатурой и естественной семантикой мы будем обозначать LR.

Задача 1. Опишите формально только что определенную бесконечную сигнатуру.
Докажите, что отношения, определимые на $\mathbb{R}$ в логике отношений с сигнатурой $\langle \cdot, + \rangle$ определимы в данной бесконечной сигнатуре.

На самом деле, как легко видеть, множества отношений, определимых в двух рассмотренных сигнатурах, совпадают, но нам это не понадобится.

Мы начнем с простейшего, «школьного» примера, поясняющего базовую ситуацию «избавления» от квантора, его «элиминации».

Задача 2. Напишите бескванторную формулу, эквивалентную формуле:
$\exists x(ax^2 + bx - c > 0)$,
здесь x, a, b, c – переменные.

Подсказка. Вспомните про дискриминант квадратного уравнения и обратите внимание на то, что многочлен в данной формуле может иметь степень меньше двух.

Определение 1. *Полуалгебраическим отношением* будем называть всякое отношение, задаваемое формулой языка LR.
Полуалгебраическим множеством будем называть множество в конечномерном действительном пространстве R^n, задаваемое полуалгебраическим отношением, т. е. состоящее из всех точек, где это отношение истинно.

Задача 3. Пусть некоторое множество в R^n задается формулой Φ, как написать формулу, задающую проекцию этого множества вдоль оси y?

Основным результатом настоящей лекции будет **теорема Тарского**, состоящая в том, что всякая формула рассматриваемой логики отношений LR эквивалентна бескванторной. Основным шагом в доказательстве будет устранение (или как еще говорят — "элиминация") квантора существования. Мы это проделали выше в случае квадратного трехчлена. Можно сообразить, как, пользуясь этим шагом, доказать и всю теорему.

Определение 2. (Диаграмма)
Назовем *сегментом* всякую точку и всякий открытый интервал, концом интервала может быть и + или − бесконечность.
Знаком назовем каждый из трёх символов $+$, $-$ или 0.
Пусть $F_1(x), ..., F_k(x)$ — многочлены от x с действительными коэффициентами. *Диаграммой* набора $F_1, ..., F_k$ называется таблица, которая строится следующим образом:
Расположим все корни наших многочленов, не считая нулевых многочленов, в порядке возрастания:
$\alpha_1 < \alpha_2 < ... < \alpha_m$
Корни разобьют числовую ось на $2m + 1$ сегментов, на каждом из которых знаки всех F_i постоянны.
Составим таблицу, в которой будет k строк (по одной для каждого из многочленов) и нужное количество $2m + 1$ столбцов, соответствующих всем сегментам.
В каждой ячейке таблицы запишем знак соответствующего многочлена (строка) на соответствующем сегменте (столбец).
Наконец, в строках, соответствующих нулевым многочленам, поставим все нули. Если вся система многочленов состоит из такого многочлена, то в таблице будет одна клетка с нулем, соответствующая всей прямой.

Задача 4. Какими могут быть диаграммы для набора, состоящего из одного многочлена:
$ax^2 + bx - c$?
Перечислите все возможные диаграммы и для каждой укажите соответствующие ей условия на a, b, c.

Подсказка. Основные альтернативы связаны со знаком старшего ненулевого коэффициента многочлена.

Чтобы понять, с какими трудностями нам придется столкнуться, рассмотрим случай двух многочленов

Задача 5. Напишите бескванторную формулу, эквивалентную формуле:
$\exists x((x^2 + bx - c < 0) \wedge (dx + e = 0))$,
здесь x, b, c, d, e — переменные.
Нарисуйте все гипотетически возможные диаграммы для данной пары многочленов, входящих в формулу, для которых нужное x существует?

Подсказка. Попробуйте нарисовать всевозможные взаимные расположения графиков двух многочленов при разных значениях параметров b, c, d, e.
Воспользуйтесь явной формулой для решения линейного уравнения.

Заметим, что эту задачу мы решили, не обращаясь к явной формуле для корней многочлена второй степени. В случае многочленов пятой степени такая формула и невозможна.

Оказывается, и в самом общем случае удается решить вопрос о существовании значения переменной x, для которого выполнена бескванторная формула Φ, свести к истинности бескванторной формулы, не содержащей x, но, естественно, содержащей коэффициенты полиномов, входящих в формулу Φ. Конечно, сами эти коэффициенты могут быть полиномами от переменных, отличных от x. Так и было в уже рассмотренных примерах. Эти переменные мы, в наших рассмотрениях, будем называть параметрами.

В элиминации квантора ключевым звеном являются следующие **неформальные соображения**:
1. Истинность бескванторной формулы полностью определяется знаками всех входящих в эту формулу многочленов во всех сегментах прямой, если среди этих сегментов есть корни всех многочленов, то есть диаграммой набора многочленов.
2. Указанная информация о корнях и знаках для набора многочленов от переменной может быть получена из аналогичной информации для некоторого набора многочленов меньшей степени: диаграмма может быть построена исходя из диаграммы для многочленов меньшей степени.
Эти неформальные соображения будут прояснены в следующих определениях и задачах.

Говоря о многочленах, мы всегда выделяем одну переменную, скажем x, говоря о степени, имеем в виду степень по x и т.д. При этом мы понимаем, что коэффициенты многочленов сами являются многочленами от других переменных — параметров.

Задача 6. Пусть p и q — многочлены от одной переменной (в данном случае без параметров) над полем действительных чисел, причем степень q меньше или равна степени

p и больше нуля. Как построить такой многочлен r, степень которого меньше степени p, что знак многочлена p в корне многочлена q равен знаку многочлена r в той же точке?

Комментарий. Вы видите, что наша задача имеет отношение к нашим неформальным соображениям: в ней идет речь о знаке одного многочлена в корне другого, и она помогает свести вопрос о таком знаке к вопросу, относящемуся к многочленам меньшей степени.

Задача 7. Разделите с остатком многочлен $4x^3+3x^2+2x+1$ на многочлен $5x^2+6x+7$. Как найти знак первого многочлена в корнях второго?
На что можно домножить делимое, чтобы остаток имел целые коэффициенты?

Подсказка. Можно воспользоваться алгоритмом деления “в столбик”.

Перейдем теперь к многочленам от многих переменных, среди которых одна — выделенная. Говоря о степени, будем говорить о степени по x.

Задача 8. Пусть p и q — многочлены от нескольких переменных с целыми коэффициентами, степень q больше 0 и старший коэффициент q отличен от 0.
На что нужно домножить делимое, чтобы коэффициенты остатка при делении p на q стали многочленами с целыми коэффициентами?

Подсказка. Задача эта похожа на предыдущую. Попробуем делить один многочлен на другой в столбик. При этом у нас получится частное и остаток, однако коэффициенты у них могут стать дробными, в знаменателе может появиться многочлен. Однако дело можно поправить, если заранее, еще до начала деления, делимое домножить на подходящий коэффициент (многочлен нулевой степени по x).

Почему нас так беспокоит дробность коэффициентов? Ведь мы могли и с самого начала рассматривать многочлены с коэффициентами из поля рациональных чисел. Дело, однако, в том, что наши коэффициенты — не числа, а сами — многочлены. Деление в столбик здесь «работает» точно так же, как и для многочленов с числовыми коэффициентами. Но появление алгебраических дробей уже усложнило бы наше рассуждение существенно.

Определение 3. Результатом операции *модифицированного деления* многочлена p на многочлен q является остаток от деления многочлена $a^d p$ на q, где a — это старший коэффициент многочлена q, а $d = deg(p) - deg(q) + 1$.

Задача 9. Как, используя операцию модифицированного деления, определить знак p в корне многочлена q?

Подсказка. Надо рассматривать знаки коэффициентов многочлена q и модифицированно делить p на многочлены, получающиеся вычеркиванием из q нулевых старших членов. Знак p получать, учитывая знак того одночлена, на который p домножали.

Нам понадобится несколько простых утверждений из алгебры и математического анализа.

Задача 10. Если на интервале непрерывная функция меняет знак, на этом интервале у нее есть корень.

Задача 11. Если на интервале у производной многочлена нет корня, то на этом интервале у многочлена нет двух корней.

Задача 12. Знак многочлена в плюс и в минус бесконечности определяется номером и знаком его старшего ненулевого коэффициента.

Следующая задача сводит проблему существования значения переменной, для которой бескванторная формула истинна, к анализу диаграммы семейства многочленов, входящих в формулу.

Задача 13. Пусть задана бескванторная формула и все входящие в нее многочлены принадлежат набору F. Если известна диаграмма набора F при фиксированных значениях всех переменных, кроме переменной x, то можно сказать, существует ли x, для которого истинная эта формула.

Отметим, что в утверждении этой задачи диаграмма, конечно, может зависеть от параметров. Более того, какие-то диаграммы невозможны ни при каких значениях параметров.

Определение 4. Определим **операции редукции** по отношению к произвольному набору многочленов F:

1. Взятие старшего коэффициента многочлена из F
2. Отбрасывание старшего члена многочлена из F
3. Взятие производной многочлена из F
4. Взятие остатка от модифицированного деления одного многочлена из F на другой из F.

Результат применения всех возможных операций редукции по отношению к многочленам из F назовем **редукцией набора** F.

Задача 14. Максимальная степень многочленов из редукции набора меньше максимальной степени многочленов этого набора, если последняя степень не ноль.

Подсказка. Рассмотрите каждую из операций отдельно.

Пусть дан набор многочленов F, степени, не превосходящей n. Индуктивно определим последовательность наборов $F_n, ..., F_0$:
$F_n = F$;
F_{k-1} получается из F_k применением операций редукции 1–4 к F_k, а также взятием остатка от модифицированного деления всех уже полученных многочленов из $F_n ... F_k$ на многочлены из F_k. Порядок многочленов в наборе F_{k-1} несуществен.

Задача 15. Правда ли, что степени многочленов F_k не превосходят k? Правда ли, что набор F_0 содержит все коэффициенты всех многочленов из F_n?

Подсказка. Вытекает из предшествующих задач и определений.

Обозначим набор $F_n, ..., F_0$ через F^*.
Будем строить семейство *потенциальных диаграмм* для F^*.

Начнем с того, что выпишем сверху вниз столбец F^* имен строк: на самом верху идут многочлены из набора F_n, ниже из F_{n-1} и т.д. При этом строки таблицы, отвечающие очередному F_k, будем называть k-ым *блоком (потенциальной) диаграммы.*

Первый шаг в построении диаграммы — это построение одного столбца диаграммы, в нем мы произвольным образом заполняем знаками все клетки нулевого блока. Дальнейшее построение потенциальной диаграммы полностью определяется этим заполнением и, конечно, многочленами из набора F^*. Последнее утверждение является ключевым для доказываемой теоремы.

На очередном шаге мы будем заполнять клетки очередного блока двигаясь снизу вверх. При этом некоторые из имеющихся стобцов будут заменяться на три столбца.Одновременно будет идти заполнение клеток таблицы знаками.
Опишем действия, соответствующие k-ому блоку таблицы при движении снизу вверх, то есть при переходе от $k-1$-го блока к k-ому.
Пусть $k > 0$, многочлен p — это имя очередной строки в этом блоке и диаграмма для строк, идущих ниже, построена.
Последовательно для клеток строки с именем p выполняем приведенные далее шаги 1, 2, 3.

1. Клетка отвечает построенному ранее сегменту из одной точки, соответствующему какому-то корню какого-то многочлена q, стоящего ниже, его степень не выше k. Для заполнения клетки знаком используем: знак и степень старшего ненулевого коэффициента q, модифицированное деление p на многочлен, получаемый отбрасыванием нулевых слагаемых из q, знак из строки остатка.

2. Клетка отвечает какому-то конечному интервалу. Тогда в концах этого интервала уже стоят знаки p. Возможны случаи:

   (a) в концах интервала одинаковые ненулевые знаки p, или ноль и не ноль. Копируем не ноль в клетку. На этом интервале у p нет корней, т.к. если бы корень был, то были бы и два корня на отрезке, включащем концы интервала, но тогда интервал был бы уже разбит корнем производной (находящейся в блоке ниже). По той же причине невозможен интервал, где в обоих концах знак p — ноль.

   (b) в концах интервала $+$ и $-$. Значит, на этом интервале у p есть корень (в силу указанных соображений — только один), и в диаграмме нужно один сегмент заменить на три. Разбиваем столбец на три (по всей высоте), ставя в трех появившихся клетках строки p соответствующие знаки p из концов интервала, в средней — 0. В клетках трех появившихся столбцов ниже p ставим тот знак, которых стоял в клетке, которая "растроилась".

3. Клетки, отвечающие бесконечным интервалам, заполняем с учетом старшего члена многочлена p с ненулевым коэффициентом. Знаки коэффициентов берем из нулевого блока диаграммы. Здесь также могут возникнуть три столбца, если знак в крайнем корне отличается от знака на $+$ или $-$ бесконечности.

Задача 16. Докажите, что построенная диаграмма является диаграммой набора F^* при условии, что нулевой блок содержит диаграмму коэффициентов этого набора.

Подсказка. Проверьте правильность «подъема» — заполнения каждого блока диаграммы, когда заполнены все блоки ниже.

Задача 17. Завершаем доказательство теоремы.
Для произвольной формулы $\exists x(\Phi)$ языка LR, где Φ — бескванторная:

1. Выписываем семейство F всех многочленов, входящих в Φ.

2. Строим последовательность редукций $F_n, ..., F_0$.

3. Для каждого заполнения знаками нулевого блока F_0 строим диаграмму для F^*.

4. Отбираем те диаграммы для F^*, где для блока F_n существует x, выполняющее Φ: для этого перебираем все столбцы F_n и получаем возможные комбинации знаков многочленов из F, для каждой комбинации знаков проверяем Φ.

5. Из каждой отобранной диаграммы выделяем нулевой блок F_0. Выписываем конъюнкцию атомных формул, отвечающих диаграмме этого блока (в них нет x).

6. Строим дизъюнкцию выписанных конъюнкций.

Докажите, что эта дизъюнкция эквивалентна формуле $\exists x(\Phi)$.

Подсказка. Проверьте эквивалентность $\exists x(\Phi)$ и того, что соответствующая диаграмма отобрана в п. 4.

Задача 18. Докажите, что всякая формула логики LR эквивалентна бескванторной.

Подсказка. Вспомните индукцию по построению формулы.