ЛИКБЕЗ
Лекция 4:
Исчисление предикатов.

Дмитрий Ицыксон

ПОМИ РАН

14 октября 2007

План

1. Формулы исчисления предикатов
2. Интерпретации и модели
3. Предваренная форма
4. Скулемизация, СНФ
5. Эрбранов универсум, эрбранова интерпретация
6. Метод резолюций для исчисления предикатов
7. Алгоритмическая неразрешимость исчисления предикатов
8. Арифметика Пеано
9. Элементы теории моделей
10. *1-ая теорема Геделя о неполноте арифметики

Литература

1. Н.К. Верещагин, А. Шень. Языки и исчисления.
2. Н. К. Верещагин, А. Шень. Вычислимые функции.

Язык предикатных формул

Γ — бесконечное множество предметных переменных.
$\Gamma = \{x_1, x_2, x_3, \dots\}$.
$\mathfrak{F} = \{f_1^{(i_1)}, f_2^{(i_2)} \dots\}$ — множество функциональных символов с указанием их арности, $i_k \geq 0$ (в этом множестве есть бесконечное число функциональных символов любой арности).

Определение. Термы:

- Предметная переменная $x \in \Gamma$ — терм.
- Если $f^{(i)} \in \mathfrak{F}$, а $t_1, t_2, \dots, t_i$ — термы, то $f^{(i)}(t_1, t_2, \dots, t_i)$ — терм.

Пример.

- $f^{(0)}()$ — терм;
- $f^{(2)}(x, y)$ — терм;
- $f^{(2)}(g^{(1)}(x), h^{(3)}(x, y, g^{(1)}(x)))$ — терм.

Нульместные функциональные символы обычно называют константами .

Язык предикатных формул

$\mathfrak{P} = \{p_1^{(i_1)}, p_2^{(i_2)} ...\}$ — множество предикатных символов с указанием их арности, $i_k \geq 0$ (в этом множестве есть бесконечное число предикатных символов любой арности).

Определение. Атомарной формулой называется строчка вида $p^{(i)}(t_1, t_2, \ldots, t_i)$, где $p^{(i)} \in \mathfrak{P}$, а $t_1, t_2, \ldots, t_i$ — термы.

Определение. Предикатная формула 1-го порядка

- Если A — атомарная формула, то A — предикатная формула.
- Если A, B — предикатные формулы, то $(A), \neg A, A \vee B, A \wedge B, A \to B$ — предикатные формулы.
- Если A — предикатная формула, $x \in \Gamma$, то $\forall x A$ и $\exists x A$ являются предикатными формулами.

Примеры предикатных формул

- p(f(x)) — свободная переменная x;
- $p_1(f_1(x)) \vee p_2()$ — свободная переменная x;
- $\forall x \exists y (p_1(z) \vee p_1(x))$ — свободная переменная z;
- $\forall x (p_1(f(x))) \to \exists y p_1(y)$ — замкнутая формула;
- $\forall y (p_1(x, y) \vee \exists z p_2(f(x, y), g(x)))$ — свободная переменная x.

Определение. Переменная называется свободной, если она не входит в область действия квантора по этой переменной. Формула без свободных переменных называется замкнутой.

Интерпретация

Пусть φ — предикатная формула со свободными переменными $x_1, x_2, \ldots, x_k$, функциональными символами $f_1^{(i_1)}, f_2^{(i_2)}, \ldots, f_m^{(i_m)}$ и предикатными символами $p_1^{(j_1)}, p_2^{(j_2)}, \ldots p_n^{(j_n)}$.
Интерпретацией формулы φ называется множество M, заданные на нем отображения $f^{(i_s)} : M^{i_s} \longrightarrow M$ и предикаты $p^{(j_r)} : M^{j_r} \longrightarrow \{0, 1\}$, каждой переменной x_l сопоставлен элемент M.
Для каждой такой интерпретации можно посчитать значение формулы.
Моделью называется интерпретация, в которой значение формулы равняется 1.

Примеры

- $\forall x(p(x) \to q(x))$.
  В интерпретации $M = \mathbb{Z}$, $p(x) = x \vdots 4, q(x) = x \vdots 2$ значение формулы 1.
  В интерпретации $M = \mathbb{Z}$, $p(x) = x \vdots 3, q(x) = x \vdots 2$ значение формулы 0.
- $\forall x(p(f(x))) \to \forall x p(x)$ В интерпретации $M = \mathbb{Z}$, $p(x) = x \vdots 2, f(x) = 2x$ значение формулы 0.
- $(p() \vee q()) \wedge (p() \vee \neg q())$ — пропозициональные формулы — это частный случай предикатных. Если в предикатных формулах содержатся только нульместные предикаты и нет кванторов, предметных переменных и функциональных символов.

Выполнимость, общезначимость, противоречивость

Определение. Предикатная формула называется выполнимой, если существует такая интерпретация, при которой значение формулы равняется 1.

Определение. Предикатная формула называется невыполнимой (или противоречивой), если при всех интерпретациях значение формулы равняется 0.

Определение. Предикатная формула называется общезначимой (или тавтологией), если при всех интерпретациях значение формулы равняется 1.

Определение. Предикатная формула называется необщезначимой , если существует интерпретация, при которой значение формулы равняется 0.

Исчисление предикатов 1-го порядка

- Мы доказываем, что формула является тавтологией. (Иногда, что ее отрицание является противоречием).
- Доказательство — это строка.
- Доказательство можно легко проверить (за полиномиальное время). Найти доказательство, возможно, сложно (обычно алгоритмически неразрешимо).
- Корректность: если формула имеет доказательство, то она тавтология.
- Полнота: все тавтологии имеют доказательства.

Метод резолюций для исчисления предикатов

- Чтобы доказать, что формула φ является тавтологией, мы будем доказывать, что формула $\neg\varphi$ является противоречивой.
- Избавимся от всех вхождений импликаций в формулу: заменим $A \to B$ на $\neg A \vee B$
- Пронесем отрицания до атомарных формул, пользуясь правилами:
  - $\neg\forall x A$ эквивалентно $\exists x \neg A$,
  - $\neg\exists x A$ эквивалентно $\forall x \neg A$,
  - $\neg(A \vee B)$ эквивалентно $(\neg A \wedge \neg B)$,
  - $\neg(A \wedge B)$ эквивалентно $(\neg A \vee \neg B)$.

Предваренная форма

- Переименуем связанные переменные так, чтобы их имена не совпадали ни с одной свободной переменной. И у связанных переменных, соответствующих разным кванторам, были бы разные имена.
- Вынесем все кванторы вперед, руководствуясь правилами
  - $(\forall x A) \vee B$ эквивалентно $\forall x(A \vee B)$,
  - $(\forall x A) \wedge B$ эквивалентно $\forall x(A \wedge B)$,
  - $(\exists x A) \vee B$ эквивалентно $\exists x(A \vee B)$,
  - $(\exists x A) \wedge B$ эквивалентно $(\exists x A) \wedge B$.

Пример. $(p(f(x)) \vee \forall x q(g(x))) \wedge \exists y q(y)$

- Переименовываем переменные $(p(f(x)) \vee \forall z q(g(z))) \wedge \exists y q(y)$
- $(\forall z(p(f(x)) \vee q(g(z)))) \wedge \exists y q(y)$
- $\forall z(((p(f(x)) \vee q(g(z)))) \wedge \exists y q(y))$
- $\forall z \exists y(\forall z(p(f(x)) \vee q(g(z))) \wedge q(y))$

Скулемизация

Имеем формулу в предваренной форме $\varphi = q_1 x_1 q_2 x_2 \dots q_k x_k A$, где $q_i \in \{\forall, \exists\}$, а формула A не содержит кванторов.

- Пусть q_l — первый квантор существования. Т.е., $q_1 = q_2 = \dots = q_{l-1} = \forall$.
- Заменим φ на формулу $\varphi' = \forall x_1 \forall x_2 \dots \forall x_{l-1} q_{l+1} x_l \dots q_k x_k A[x \mapsto f_l(x_1, x_2, \dots, x_{l-1})]$, где формула $A[x_l \mapsto f_l(x_1, x_2, \dots, x_{l-1})]$ получается из формулы A заменой всех вхождений переменной x_l на терм $f_l(x_1, x_2, \dots, x_{l-1})$.
- Если у формулы φ есть модель, то и у формулы φ' есть модель: достаточно функцию f_l определить так: она сопоставляет значениям переменных $x_1, \dots, x_{l-1}$ значение x_l, чтобы была истинна формула $q_{l+1} x_l \dots q_k x_k A$.
- Если у формулы φ' есть модель, то и у формулы φ есть модель. В модели для φ' задана функция, указывающая, как по значениям переменных $x_1, \dots, x_{l-1}$ находить значение x_l, чтобы была истинна формула $q_{l+1} x_l \dots q_k x_k A$.

Скулемизация (продолжение)

- Аналогично избавляемся от второго квантора существования.
- Так получаем формулы $\varphi', \varphi'', \ldots, \varphi^{(m)}$
- Формула $\varphi^{(m)}$ не содержит кванторов существования.
- Формула φ выполнима тогда и только тогда, когда выполнима формула $\varphi^{(m)}$
- Формула φ противоречива тогда и только тогда, когда противоречива формула $\varphi^{(m)}$

Пример. $\forall x \exists y \forall z \exists t (p(g(x, y)) \wedge \neg q(h(z, g(x, t))))$
переписывается в виде
$\forall x \forall z (p(g(x, f_2(x))) \wedge \neg q(h(z, g(x, f_4(x, z)))))$

СНФ

Скулемовская нормальная форма (СНФ):

- Приводим в предваренную форму (кванторы вперед)
- Делаем скулемизацию (избавляемся от $\exists$)
- Бескванторную часть формулы приводим в КНФ (например, ее отрицание приводим в ДНФ): атомарные формулы можно рассматривать как пропозициональные переменные.

Пример приведения в СНФ

Пример. $\forall x(p(g(x)) \wedge \neg p(h())) \to \forall y(\neg p(g(h())) \wedge p(y))$

- Избавляемся от $\to$:
  $\neg(\forall x(p(g(x)) \wedge \neg p(h()))) \vee \forall y(\neg p(g(h())) \wedge p(y))$
- Проносим отрицание:
  $(\exists x(\neg p(g(x)) \vee p(h()))) \vee \forall y(\neg p(g(h())) \wedge p(y)))$
- Выносим кванторы вперед:
  $\exists x \forall y(\neg p(g(x)) \vee p(h()) \vee \neg p(g(h())) \wedge p(y)))$
- Избавляемся от кванторов существования:
  $\forall y(\neg p(g(f())) \vee p(h()) \vee \neg p(g(h())) \wedge p(y))$
- Приводим в КНФ: $\neg p(g(f())) \vee p(h()) \vee \neg p(g(h())) \wedge p(y)$
- Для этого приводим в ДНФ:
  $p(g(f())) \wedge \neg p(h()) \wedge (p(g(h())) \vee p(y))$
- Раскрываем скобки:
  $(p(g(f())) \wedge \neg p(h()) \wedge p(g(h()))) \vee (p(y) \wedge p(g(f())) \wedge \neg p(h()))$
- Ответ: $\forall y((\neg p(g(f())) \vee p(h()) \vee \neg p(g(h()))) \wedge (\neg p(y) \vee \neg p(g(f())) \vee p(h())))$

Эрбранов универсум

- Мы доказываем, что формула является противоречивой
- Интерпретаций слишком много, хочется уменьшить их количество
- Высотой терма называется максимальное число вложенных скобок в нем.
  Пример. Высота $f(x, y)$ и $h()$ равняется 1, высота $f(g(h(y), z), x)$ равняется 3.
- Пусть дана формула φ. $\mathfrak{F}_\varphi$ — множество ее функциональных символов (если там нет констант (нульместных символов), то добавим!!!) Обозначим
  $U_\varphi^{(1)}$ — множество замкнутых термов из $\mathfrak{F}_\varphi$ высоты 1.
  $U_\varphi^{(2)}$ — множество замкнутых термов из $\mathfrak{F}_\varphi$ высоты 2.
  $U_\varphi^{(k)}$ — множество замкнутых термов из $\mathfrak{F}_\varphi$ высоты k.
  $U_\varphi^H = \bigcup\limits_{i=1}^{\infty} U_\varphi^{(i)}$ — эрбранов универсум

Пример эрбранова универсума

$\varphi = \forall x \exists y (p(f(x, g(y))))$
$\mathfrak{F}_\varphi = \{f^{(2)}, g^{(1)}, c^{(0)}\}$
$U_\varphi^{(1)} = \{c\}$
$U_\varphi^{(2)} = \{f(c,c), g(c)\}$
$U_\varphi^{(3)} = \{f(g(c),c), f(g(c),g(c)), f(g(c),f(c,c)),$
$f(c,g(c)), f(c,f(c,c)),$
$f(f(c,c),c), f(f(c,c),g(c)), f(f(c,c),f(c,c),$
$g(f(c,c),g(g(c))\}$

Эрбрановская интерпретация

- φ — формула
- Множество: U_{φ}^{H}
- Функции задаются синтаксически : $f(t_1, t_2, \ldots, t_k) = f(t_1, t_2, \ldots, t_k)$
- Предикаты задаются произвольно

  Итого:
- Множество задано
- Функции заданы
- Предикаты можно варьировать

Модель на эрбрановской интерпретации

Теорема. Если формула ϕ в СКНФ выполнима, то ее можно выполнить с помощью Эрбрановской интерпретации.
Доказательство. $\varphi = \forall x_1 \forall x_2 \ldots \forall x_k (S_1 \wedge S_2 \wedge \cdots \wedge S_n)$, где S_i — дизъюнкция литералов (атомарных формул или их отрицаний). Пусть I — интерпретация. M — множество. Если для определения эрбрановского универсума мы добавляли константу, то придадим ей тоже какое-то значение. Интерпретация I задает отображение из $\mu_I : U_\varphi^H \to M$.
Значения предикатов в I_H:
$p_{I_H}(t_1, t_2, \ldots, t_r) = p_I(\mu(t_1), \mu(t_2), \ldots, \mu(t_r))$.
Для каждого i дизъюнкт S_i выполняется при всех значениях переменных при интерпретации I. Значит, выполняется и при всех значениях переменных в интерпретации I_H.

Поиск опровержения

Для каждого дизъюнкта S_j формулы φ напишем огромное число дизъюнктов, которые получаются из S_j подстановкой вместо переменных всевозможных термов из $\bigcup_{i=1}^{k} U_{\varphi}^{(i)}$.

Получившееся множество дизъюнктов обозначим через D_k.

D_k можно рассматривать как пропозициональную формулу от переменных $p(t_1, \ldots, t_r)$, где $t_j \in \bigcup_{i=1}^{k} U_{\varphi}^{(i)}$

Если D_k — противоречива как пропозициональная формула, то и формула φ противоречива.

Если все D_k — выполнимы, то и φ выполнима. В эрбрановской интерпретации зададим $p_{I_H}(t_1, t_2, \ldots, t_r)$ то значение, которое принималось в лексикографически первом выполняющем наборе D_k, $1 \leq k < \infty$ бесконечное число раз.

Метод резолюций

- Если формула φ противоречива, то существует такое k, что пропозициональная формула D_k противоречива.
- Противоречивость пропозициональной формулы D_k можно показать с помощью метода резолюций.

  Пример.

  $\varphi = \forall xy((p(f(x)) \vee q(y)) \wedge \neg q(g(b)) \wedge \neg p(y))$

  b — единственная константа.

  Опровержение.

$$\frac{(p(f(b)) \vee q(g(b)));\neg q(g(b))}{p(f(b))};$$

$$\frac{p(f(b));\neg p(f(b))}{\square}$$

Разрешимые и перечислимые языки

Σ — алфавит, $L \subset \Sigma^*$ — язык.

Язык L называется алгоритмически разрешимым, если существует такая машина Тьюринга M, что

$$\begin{cases} x \in L \iff M(x) \text{ останавливается в состоянии } q_{yes} \\ x \notin L \iff M(x) \text{ останавливается в состоянии } q_{no} \end{cases}$$

Язык L называется перечислимым, если существует такая машина Тьюринга M, что

$$\begin{cases} x \in L \iff M(x) \text{ останавливается в состоянии } q_{yes} \\ x \notin L \iff M(x) \text{ не останавливается} \end{cases}$$

Перечислимость тавтологий

Замечание. Язык тавтологий является перечислимым

- Отрицание формулы приводим в СНФ, перебираем все k и проверяем, является ли D_k противоречивой. Если является, то остановиться в состоянии q_{yes}.
- Метод Британского музея. Перебираем все строчки и проверяем, являются ли они доказательством формулы φ. Если является, то остановиться в состоянии q_{yes}.

Вопрос. А является ли язык тавтологий алгоритмически разрешимым?
Нет.

Предикат равенства

- Инфиксная запись: пишем $x = y$ вместо $=(x, y)$
- Чтобы во всех интерпретациях он воспринимался одинаково, нужны аксиомы равенства.
  Аксиомы равенства:
- $\forall x \forall y (x = y \to y = x)$ — симметричность
- $\forall x \forall y \forall z ((x = y \wedge y = z) \to x = z)$ — транзитивность
- Для каждого функционального символа $f^{(r)}$:
  $\forall x_1 \ldots \forall x_r \forall y_1 \ldots \forall y_r ((x_1 = y_1 \wedge \cdots \wedge x_r = y_r) \to$
  $f(x_1, \ldots, x_r) = f(y_1, \ldots, y_r))$ — согласованность с функциональными символами
- Для каждого предикатного символа $p^{(r)}$:
  $\forall x_1 \ldots \forall x_r \forall y_1 \ldots \forall y_r ((x_1 = y_1 \wedge \cdots \wedge x_r = y_r) \to$
  $(p(x_1, \ldots, x_r) \to p(y_1, \ldots, y_r)))$ — согласованность с предикатными символами

Формулу φ с предикатом равенства надо воспринимать как $(A_1 \wedge \cdots \wedge A_n) \to \varphi$

Алгоритмическая неразрешимость

Теорема. Язык тавтологий является алгоритмически неразрешимым.

Доказательство. Сведем задачу об остановке МТ к проверке, является ли формула тавтологией.

- Для каждого ленточного символа $s \in \Sigma$ заводим константу $s()$, для каждого состояния $q \in Q$ заводим константу $q()$.
- Ленту будем кодировать так: $q()|c_1() \circ c_2() \circ \cdots \circ c_{l-1}() \circ g(c_l()) \circ \cdots \circ c_m()$
- Правило $(q_1, c_1) \mapsto (q_2, c_2, \leftarrow)$ записываем формулой: $\forall x \forall y (q_1()|x \circ c_0() \circ g(c_1()) \circ y = q_2()|x \circ g(c_0()) \circ c_2() \circ y)$
- Предикат остановки $stop$: $\forall x (stop(q_f|x))$ для конечного состояния q_f

МТ остановится на входе $x \iff$ формула $(A_1 \wedge \ldots A_n) \to stop(q_0()|x_1() \circ \ldots x_m())$ является тавтологией.
A_i — это аксиомы равенства и правила, задающие МТ.

Арифметика Пеано

Константа 0, функциональные символы: $+$, $\cdot$, s, предикат $=$
Аксиомы Пеано:

- $\forall x \neg(s(x) = 0)$
- $\forall x \forall y(s(x) = s(y) \to x = y)$
- $\forall x(x + 0 = x)$
- $\forall x \forall y(x + s(y) = s(x + y))$
- $\forall x \forall y(x \cdot s(y) \to x \cdot y + x)$
- $\forall x(x \cdot 0 = 0)$
- $(\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(s(x)))) \to \forall x \varphi(x)$ для каждой формулы φ с одной свободной переменной. Это схема аксиом (схема индукции), нельзя обойтись конечным числом аксиом.

Элементы теории моделей

Определение. Высказыванием называется замкнутая формула.
Определение. Теорией называется множество высказываний (возможно, бесконечное).
Определение. Мы говорим, что из теории T выводится формула α ($T \vdash \alpha$), если она доказуема, при условии что можно использовать формулы из T, как аксиомы. Более формально: все формулы из T и $\neg\alpha$ приводим в СНФ, если выводится противоречие из множества полученных дизъюнктов по методу резолюции, то $T \vdash \alpha$.
Теорема. (компактности) Если $T \vdash \alpha$, то существует конечная подтеория $T' \subset T : T' \vdash \alpha$.
Доказательство. Вывод конечен, значит, в нем используется лишь конечное число формул из T.
Следствие. $T \vdash \alpha \iff$ существует конечное множество формул $A_1, \ldots, A_n \in T$: формула $(A_1 \wedge \cdots \wedge A_n) \to \alpha$ является тавтологией.

Модели для теорий

Определение. Интерпретация I называется моделью для теории T ($I \models T$), если она является моделью (выполняет) каждой формулы из T.

Лемма. $I \models T$, $T \vdash \alpha$. Тогда $I \models \alpha$.

Доказательство.

Существуют $A_1, A_2, \ldots, A_n \in T$: формула $(A_1 \wedge \cdots \wedge A_n) \to \alpha$ тавтология. В частности, I выполняет эту формулу. Значения формул $A_1, \ldots, A_n$ в интерпретации I равняются 1, значит и значение формулы α в интерпретации I равняется 1.

Определение. Теория называется непротиворечивой, если из нее не выводима противоречивая формула.

Замечание. Если теория имеет модель, то она непротиворечива.

Теорема. (о полноте, К. Гедель) Если теория T непротиворечива, то она имеет модель.

Противоречивые теории

- Теория противоречива, если после приведения всех ее формул в СНФ из дизъюнктов можно вывести противоречие
- Теория противоречива, если из нее можно вывести противоречивую формулу
- Теория противоречива, если из нее можно вывести любую формулу
- Если $T \cup \{\neg\varphi\}$ противоречива, то $T \vdash \varphi$

Геделева нумерация

Пусть T непротиворечивая теория, содержащая арифметику Пеано.

Числами в арифметике Пеано являются термы $0, s(0), s(s(0)), \ldots$

Факт. По любой МТ M можно построить предикатную формулу $\varphi_M(x, y)$, которая в стандартной модели теории T, обладает следующим свойством: для всех натуральных чисел m и n формула $\varphi_M(m, n)$ будет выполняться $\iff$ Машина Тьюринга M, получив на вход m закончит работу и на ее ленте будет написано n.

- Можно пронумеровать (алгоритмом) все строчки, которые являются замкнутыми формулами
- Можно пронумеровать (алгоритмом) все строчки, которые являются доказательствами
- Можно построить МТ, которая по числам m и n проверит, является ли доказательство с номером m доказательством формулы с номером n.

Геделева нумерация (продолжение)

- Можно построить формулу $Proof(x, y)$, которая в стандартной модели теории T, обладает следующим свойством: для всех натуральных чисел m и n формула $Proof(m, n)$ выполняется $\iff$ доказательство с номером m является доказательством формулы с номером n.
- Можно пронумеровать все формулы с одной свободной переменной.
- Можно построить формулу $Subst(x, y, z)$, которая в стандартной модели теории T, обладает следующим свойством: для всех натуральных чисел m и n формула $Subst(m, n, k)$ выполняется $\iff$ m — это номер формулы, которая получится, если в формулу с одной свободной переменной с номером n подставить число k вместо свободной переменной.

1-я теорема Геделя о неполноте

Теорема. (К. Гедель) Пусть T непротиворечивая теория, содержащая арифметику Пеано. Тогда существует формула φ, которая выполняется в стандартной модели модели теории T, которая не выводится из T.

Доказательство.

- $\neg\exists z\exists p[Subst(z, x, x) \wedge Proof(p, z)]$
- Эта формула с одной свободной переменной x. Пусть ее номер N.
- Подставим N в эту формулу. Получилась формула φ.
- По построению формула φ выполняется в стандартной модели теории T, когда недоказуема и невыполняется, когда доказуема.
- Либо формула φ выполняется в стандартной модели теории T и недоказуема, либо T противоречива.

Упражнения

- Докажите, что если языки L и $\overline{L}$ перечислимы, то они оба алгоритмически разрешимы.
- Докажите, что язык формул, которые не являются тавтологиями, неперечислим.
- Запишите в арифметике Пеано формулы, кодирующие следующие высказывания:
  - $a \vdots b$
  - p — простое число.
  - a — степень числа 2.
  - a — степень числа 4.