Введение в математическую логику и теорию алгоритмов

Лекция 5

Алексей Львович Семенов

Логика высказываний

- Построение **сложных** высказываний из **простых**
- Для **простых** – существенна только их **истинность**.
- О чем высказывания – не существенно и **не видно**.
- Добавляем объекты и отношения между ними.

Отношения

- Множество D - *область*
- n-местное отношение (n-местное свойство) на D – любое подмножество в D^n.
- ω-местное отношение – подмножество в D^ω.
- Отношение – отображение из D^λ в $\mathbf{B} = \{0,1\}$, высказывание об элементах D.

Примеры

- 2-местное отношение равенства – множество всех пар $\langle x,x \rangle$, $x \in D$.
- Отношения на натуральных числах:
  - следования $y=x+1$,
  - порядка $x<y$,
  - сложения $x+y=z$.

Логика отношений

Синтаксис 1. Начало

• Алфавит *имен объектов* $Ob=\{a_0, a_1, a_2,\ldots\}$

• Алфавит *имен отношений* $Pr=\{P_0, P_1, P_2,\ldots\}$, каждому имени сопоставлена его арность (число аргументов).

- Иногда логические имена считаются отношениями с нулем аргументов – 0-арными, у нас их не будет.

• Сигнатура $\Sigma = \langle Ob, Pr\rangle$

• Часто используются также имена функций, но мы этого делать не будем, сводя функции к отношениям, как мы только что делали.

Логика отношений

Семантика 1. Начало

- *Структура данной сигнатуры* –
  это набор <D, Σ, *Зн*>, где *Зн* ставит в соответствие:
- имени объекта – элемент из D,
- имени отношения – отношение на D (с нужным числом аргументов).

Примеры структур

Синтаксис и семантика

Упорядоченное поле рациональных чисел:

- **Q** , {0, 1}, { +, $*$, >}, **Зн**
  - Вместо 5<7 пишем <(5,7).
  - $*(a,b,c)$ – c есть произведение a и b.

Поле действительных чисел

Многочлены с целыми коэффициентами >,= 0.

Свободный моноид с данной системой образующих

- Все образующие
- Приписывание

Логика предикатов

Синтаксис 2. Продолжение

• Фиксируем упорядоченный алфавит *свободных переменных* $FVar = <x_0, x_1, x_2, \ldots>$.

Термы:

• Имя объекта – терм.

• Свободная переменная – терм.

Атомные формулы

• **Если** P – имя n-арного отношения и $t_0, t_1, \ldots, t_{n\text{-}1}$ – термы, то $P(t_0, t_1, \ldots, t_{n\text{-}1})$ – атомная формула.

• **Если** t_0, t_1 – термы, то $(t_0 = t_1)$ – атомная формула.

Пример: $P_2\,(a_1, x_2, x_2)$ – атомная формула.

Логика отношений

Семантика 2. Продолжение

- Пусть задана структура: <*D*, Σ, *Зн*> и *интерпретация* $\alpha = \alpha_0, \alpha_1, \alpha_2, \ldots$ из D^ω.
- *Зн* терма при интерпретации α – элемент *D*:
  - *Зн* имен объектов задано *Зн*
  - *Зн* x_i – это α_i.
- *Зн* атомной формулы при интерпретации α – элемент **B.**

Зн $P(t_0, t_1, \ldots, t_{n-1})$ – применяем *Зн* P к *Зн* t_0, *Зн* $t_1, \ldots,$ *Зн* t_{n-1}.

Зн $(t_0 = t_1)$ – совпадение *Зн* t_0 и *Зн* t_1.

Значение атомной формулы – это отображение $D^\omega \rightarrow$ **B**, то есть – ω-местное отношение,

если номера всех переменных формулы меньше n, то с атомной формулой сопоставляется – n-местное отношение.

Логика отношений

Синтаксис 3. Продолжение

Связанные переменные

Пример:

- $\sum_{i=1}^{100} \sin(i)$, что значит подставить вместо *i* число 8? *i* - связанная
- Фиксируем упорядоченный *алфавит связанных предметных переменных BVar= <u_0, u_1, u_2,… >*

Кванторы:

- $\forall$ - *квантор всеобщности*, «для всех»
- $\exists$ - *квантор существования*, «существует»

Замена:

A[x/u] означает результат замены всех вхождений символа *x* в слове *A* на символ *u (x не обязан входить в A)*

Логика отношений

Синтаксис 3 Окончание

Еще один *алфавит связанных переменных Bvar ,*

Формула (заданной сигнатуры), индуктивное определение:

- Атомные формулы – формулы.
- Если Φ, Ψ – формулы, $\tau \in \{\wedge, \vee, \rightarrow, \equiv\}$,

  то $(\neg\Phi)$, $(\Phi\tau\Psi)$ – формулы.
- Если Φ – формула,

  x – свободная переменная ($x \in FVar$),

  u – связанная переменная ($u \in BVar$), не входящая в Φ,

  то $(\forall u\ \Phi[x/u])$, $(\exists u\ \Phi[x/u])$, – формулы (в эти формулы x – не входит). $\forall$ **- для всех,** $\exists$ **- существует**

Сокращения.

- Опускание внешних скобок
- Вместо $\forall u\ \forall v$ пишем $\forall u, v$.

Однозначность анализа. Тонкость – восстановление свободной переменной – берем первую не использованную.

Логика отношений

Семантика 3 (окончание построения).

- Пусть задана структура: <*D*, Σ, *Зн*>

и интерпретация $\alpha = \alpha_0, \alpha_1, \alpha_2, \ldots$ из D^ω.

Зн формулы $\Phi \in$ ***B*** определяется индуктивно.

- *Зн* атомной формулы $P(t_0, t_1, \ldots, t_{n-1})$ – было.
- *Зн* $(\Phi\tau\Psi)$, где $\tau \in \{\rightarrow, \wedge, \vee, \equiv\}$ – результат применения τ к Зн Φ, Ψ; Зн $(\neg\Phi)$ = 1- Зн Φ.
- *Зн* $(\forall u\ \Phi[x_i/u])$ = $\wedge$ Зн(Φ) по всем β, совпадающим с α на всех местах, кроме i–го,
- *Зн* $(\exists u\ \Phi[x_i/u])$ = $\vee$ Зн(Φ) по всем β, совпадающим с α на всех местах, кроме i–го.

(Восстановление Φ, т.е. x_i по кванторной формуле – см. выше.)

Логика отношений

- Задана структура $M = <D, \Sigma, Зн>$.
- Значение формулы зависит только от значений ее (свободных) переменных (соответствующих членов последовательности α).
- Если все свободные переменные Φ имеют номера < n, то Φ *выражает* n-местное отношение на *D.* Это отношение *определимо* (или *выразимо*) *в M*.

Задача изучения отношений, определимых в данной структуре

Примеры определимых отношений

- Структура $< N, +, * >$ – натуральные числа, сложение, умножение.

- x – чётное число $\Leftrightarrow$ $\exists y\ (x=y+y)$
- $x = 1$ $\Leftrightarrow$ $\forall y\ (x*y=y)$

- x делит y $\Leftrightarrow$ $\exists z\ (y=x*z)$

- $x < y$ $\Leftrightarrow$ $\exists z\ (y=x+z) \wedge \neg(x=y)$
- $\text{Ост}(x, y) = v$ $\Leftrightarrow$ $(0 \leq v < y) \wedge \exists t\ (x = y*t + v)$

КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ

(**Сунь Цзы**, 3 век н.э., исследование календаря)

Т. Пусть $u_0, u_1, \ldots, u_{n-1}$ - попарно взаимно простые натуральные числа, $0 \leq v_i < u_i$ для всех i,

- Тогда найдется $p < u_0 u_1 \ldots u_{n-1}$,
  Ост (p, u_i) = v_i для всех i

Д. Пусть p и q дают одинаковые цепочки остатков, тогда их разность делится на все u_i, то есть на их произведение. То есть все цепочки остатков различны. Значит, получаются все возможные цепочки.

Кодирование цепочек чисел

- Мы умеем кодировать цепочки слов с помощью слов.
- Как можно кодировать цепочки чисел с помощью (пар) чисел?
- Для этого мы применим Китайскую теорему об остатках. В ней, чтобы получить цепочку из n чисел, используется цепочка из n попарно взаимно простых чисел. Как ее получить?

Кодирование цепочки чисел

- $u_i = yi+z$, где $i = 0,1,2…n-1$. Взаимная простота?
- Общий делитель u_i и u_j делит $u_i - u_j = y(i-j)$.
- Положим: $z=y+1$, т.е. $u_i = 1+y(1+i)$, y кратно $(n-1)!$ (и больше всех кодируемых), u_i и $u_i – u_j$ – вз. просты
- $\forall\ v_0, v_1, ..., v_{n-1}$ **найдутся такие**

  p (из Китайской теоремы), y (разность прогрессии),
- что v_i является остатком от деления p на $1+y(1+i)$.

Обозначим β $(x, y, i) =$ Остаток $(x, 1+y(1+i))$

Бета-функция Геделя.

Кодирование цепочки чисел

- Удобно кодировать вместе с элементами цепочки и ее длину. Ее можно ставить в начале цепочки.
- Итак, для любого набора натуральных v_0, ..., v_{n-1} можно подобрать числа x, y такие, что

  β (x, y, 0)=n, β (x, y, 1)=v_0,..., β (x,y,n)=v_{n-1}.

Чем это может нам помочь при определении «естественных» отношений?

Определимость отношений

Отношение $m = 2^n$?

- найдется цепочка длины n, первый элемент которой 1, каждый следующий вдвое больше предыдущего, а последний – это m.

То есть, существуют x и y, для которых: $\wedge$

- β (x, y, 0)=n,
- β (x, y, 1)=2
- $\forall j\ (0 < j < n) \rightarrow \quad \beta$ (x, y, j+1)= 2β (x, y, j)
- β (x,y,n)= m.

Утв. Все вычислимые функции определимы…

Алгебра определимостей

- Фиксируем множество D
- Множество отношений R
- Дадим всем отношениям из R имена из Σ, то есть зададим Зн.
- Структура $S = \langle D, \Sigma, \text{Зн} \rangle$
- Множество всех отношений, определимых в структуре S, назовем замыканием R.
- Замыкание $C(R)$ определяется R (а не выбором имен).
- $CC(R) = C(R)$
- Замкнутое множество – совпадающее с замыканием, *определимость*

Алгебра определимостей

- Замыкание монотонно по включению множеств
- Пересечение определимостей – замкнуто
- Операция объединения определимостей = замыкание теоретико-множественного определения

Логика отношений

- *Замкнутая* формула – формула без свободных переменных
- Фиксируем структуру
- Замкнутая формула истинна (Зн = 1) или ложна (Зн = 0) в данной структуре
- Множество истинных замкнутых формул – *теория* структуры
- Теория структуры может быть разрешимой
- Логику отношений часто называют *логикой предикатов*

Просеминар

- по математической логике и информатике
- проходит по пятницам с 16:45 до 18:20 в аудитории 16-22.