Введение в математическую логику и теорию алгоритмов

Лекция 3

Алексей Львович Семенов

План

- Логика высказываний
- Структуры
- Логика отношений
- Что значит определить отношение?

Логика высказываний

- Построение **сложных** высказываний из **простых**
- Для **простых** – существенна только их **истинность**.
- О чем высказывания – не существенно и **не видно**.
- Значение сложного высказывания (формулы) определяется значением его частей. В конце концов – «атомных» высказываний.

Решение задачи?

Построение формулы логики высказываний по булевой функции (решение задачи)

- В длинной конъюнкции и дизъюнкции будем опускать скобки.
- $\vee \Phi_i$, $\wedge \Phi_i$ аналогично выражениям $\Sigma\, a_i$, $\Pi\, a_i$.
- Если множество одноэлементно, то значение совпадает с ним,

  если пустое, то $\vee$ **= 0,** $\wedge$ **= 1**.
- Где функция, задаваемая формулой $A_0 \wedge \neg A_1 \wedge \neg A_2 \wedge A_3$, равна 1?
  - Только при значении $< \alpha_0, \alpha_1, \alpha_2, \alpha_3 > \; = \; < 1, 0, 0, 1 >$.
- Фиксируем натуральное число *n*.

  Обозначения $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$; $A = A_0, A_1, \ldots, A_{n-1}$,
- $(0, A_i) = \neg A_i$
- $(1, A_i) = A_i$
- $(\alpha, A) = ((\alpha_0, A_0) \wedge (\alpha_1, A_1) \wedge \ldots \wedge (\alpha_{n-1}, A_{n-1}))$

Теорема о совершенной дизъюнктивной нормальной форме.
Всякая функция $f : \boldsymbol{B}^n \longrightarrow \boldsymbol{B}$ ***з***адается формулой.

$\vee$**$(\alpha$, A)** по всем α, для которых ***f*** **(α) = 1 (если пусто, то 0)**

Это – СДНФ. (д.н.ф. …)

Синтаксис логики высказываний (повт.)

Индуктивное определение (построение) формулы

- Логические константы 0 и 1 – формулы.
- Имена высказываний A_0, A_1, A_2,… – формулы.
- Если Ф, Ψ – формулы, τ – связка: $\wedge$ (конъюнкция), $\vee$ (дизъюнкция), $\rightarrow$ (импликация), ≡ (эквивалентность), то $\neg$Ф, (Ф τ Ψ) – формулы.

(Знак $\neg$ означает отрицание.)

Семантика логики высказываний (повт.)

Индуктивное определение (вычисление) значения формулы в (при) заданной интерпретации $\alpha \in \mathbf{B}^{\mathbf{N}}$.

1. Значением логической константы является она сама.
2. Значением имени высказывания A_i является α_i .
3. Значением:
   - формулы $\neg\Phi$ является отрицание значения Φ, т.е.
     Зн $\neg\Phi$ = 1 - Зн Φ.
   - формулы **($\Phi\ \tau\ \Psi$), где $\tau \in \{\rightarrow, \wedge, \vee, \equiv\}$** является результат применения τ к значениям формул Φ, Ψ.

<u>Значение формулы</u> **–** функция $\boldsymbol{B}^{\mathbf{N}} \rightarrow \boldsymbol{B}$.

Если наибольший номер переменной в формуле равен $\boldsymbol{n} - \mathbf{1}$,

<u>то формула задает функцию</u> $\boldsymbol{B}^{\boldsymbol{n}} \rightarrow \boldsymbol{B}$.

Отношения (повт.)

- Множество D – *область*.
- Отношение – отображение (характеристическая функция) D^λ в $\boldsymbol{B} = \{0,1\}$.
- n-местное отношение (n-местное свойство) на D – любое подмножество в D^n, при $n = 0$ – логическая константа.
- **N**-местное (бесконечноместное) отношение – подмножество в $D^{\mathbf{N}}$.

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

• Последовательность (обыкновенно, но не обязательно, конечная) *имен отношений*

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

• Сигнатура $\Sigma = < Pr >$ (Дальше у нас будут более сложные сигнатуры.)

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

• В последней части лекции будет пояснено, как построить логику отношений и операций.

Логика отношений

Семантика 1. Начало

- *Структура данной сигнатуры* –

это набор <D, Σ, $Зн$>, где $Зн$ ставит в соответствие каждому имени отношения некоторое отношение на D (с нужным числом аргументов).

Примеры структур

Семантика и синтаксис

Упорядоченное поле рациональных чисел:

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

Поле действительных чисел

Многочлены с целыми коэффициентами >,=, 0

- бесконечная сигнатура.

Множество всех слов в данном алфавите (свободный моноид)

- Все символы алфавита
- Приписывание (трехместное отношение)

Логика отношений

Синтаксис 2. Продолжение

• Фиксируем последовательность *свободных переменных* $FVar = x_0, x_1, x_2, \ldots$

Атомные формулы

• **Если** P – имя n-арного отношения и $t_0, t_1, \ldots, t_{n-1}$ – свободные переменные, то $P(t_0, t_1, \ldots, t_{n-1})$ – атомная формула. (Если P – имя 0-арного отношения, то P – атомная формула.)

• **Если** t_0, t_1 – свободные переменные, то $t_0 = t_1$ – атомная формула.

Пример: $P_2(x_1, x_2, x_2)$, $x_3 = x_5$, P_3 – атомные формулы, если P_2 – имя трехместного отношения, а P_3 – имя 0-местного отношения.

Логика отношений

Семантика 2. Продолжение

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

  и *интерпретация* $\alpha = \alpha_0, \alpha_1, \alpha_2,\ldots$ *из* D^N.
- *Зн* терма при интерпретации α – это элемент *D*:
  - *Зн* x_i = это α_i
- *Зн* атомной формулы при интерпретации α – элемент **B**.

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

- *Зн* $t_0 = t_1$ – совпадение *Зн* t_0 и *Зн* t_1.

Значение атомной формулы в данной структуре – это отображение $D^N \to$ **B**, то есть N-местное отношение,

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

Логика отношений 3. Бескванторные синтаксис и семантика

Формула 3 (заданной сигнатуры), индуктивное определение:

- Атомные формулы – формулы.
- Если Φ, Ψ - формулы, $\tau \in \{\wedge, \vee, \rightarrow, \equiv\}$, то $(\neg\Phi)$, $(\Phi\ \tau\ \Psi)$ – формулы.

Семантика 3.

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

  и интерпретация $\alpha = \alpha_0, \alpha_1, \alpha_2, \ldots$ *из* D^N.
- *Зн* формулы Φ определяется индуктивно.
- *Зн* атомной формулы $P(t_0, t_1, \ldots, t_{n-1})$ – было.
- *Зн*$(\Phi\tau\Psi)$, где $\tau \in \{\rightarrow, \wedge, \vee, \equiv\}$, – это результат применения τ к

  Зн Φ, Зн Ψ. Зн $\neg\Phi$ = 1- Зн Φ…

  <u>Значение формулы</u> – отображение D^N в **B.**

Далее мы определим формулы с кванторами и семантику для них.

Примеры (задачи):

Упорядоченное множество рациональных чисел:

- $\langle$**Q**, { > }, ***Зн***$\rangle$
  - ***Зн*** – обычное.
  - $(x<y) \vee (x>y)$ – что означает?
  - $(x<y \wedge y<z) \vee (x>y \wedge y>z)$ – как это представить наглядно?
  - $(x<y \wedge y<z) \vee (z<x \wedge x<y) \vee (y<z \wedge z<x)$?
  - $(x<y \wedge t<z) \vee (x>y \wedge t>z)$?
  - Как записать, что два отрезка зацеплены (то есть – пересекаются, но не вложены один в другой)?

Как определить семантику формул с кванторами?

- Нужно «подставить все возможные значения вместо переменной x».
- Трудность:
- $\forall z\ (x<y \wedge \forall x\ (x < z))$
- Находя, при некоторых *x* и *y* значение этой формулы, мы должны будем в некоторые места подставлять что-то вместо *x*, а в другие – нет.
- Чтобы сохранить ясность, принимаются специальные меры.

Использовать другие имена

Логика отношений (комментарий)

- Синтаксис 3. Продолжение
- Связанные переменные
- Пример: $\sum_{\mathtt{i}=1}^{100} \mathbf{sin}(\mathtt{i})$ – что значит подставить вместо $\mathtt{i}$ число 8 ? Переменная $\mathtt{i}$ – 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* [*u* / *x*]** 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 – *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 $(\forall u\ \Phi[u/x])$, $(\exists u\ \Phi[u/x])$, – 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 $P(t_0, t_1, \ldots, t_{n\text{-}1})$ – было.
- *Зн*$(\Phi\ \tau\ \Psi)$, где $\tau \in \{\rightarrow, \wedge, \vee, \equiv\}$ – результат

применения τ к Зн Φ, Зн Ψ.   Зн $\neg\Phi$ = 1 - Зн Φ…

- *Зн* $\forall u\ \Phi[u/x_{\text{i}}]$ = $\wedge$ Зн Φ по всем β, совпадающим с α

на всех местах, кроме i–го.

- *Зн* $\exists u\ \Phi[u/x_{\text{i}}]$ = $\vee$ 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, меньшие n, то Φ *выражает* n-местное отношение на *D.* Это отношение <u>определимо</u> (или <u>выразимо</u>) в *M.*
- Задача изучения отношений, определимых в данной структуре

Примеры определимых отношений

- Структура $\langle \mathbb{N}, +, \times \rangle$ - натуральные числа, сложение, умножение.
- $\boldsymbol{x}$ – чётное число $\Leftrightarrow \exists y\ (x=y+y)$
- $\boldsymbol{x} = 1 \Leftrightarrow \forall y\ (x \times y = y)$
- $\boldsymbol{x}$ делит $y \Leftrightarrow \exists z\ (y = x \times z)$
- $\boldsymbol{x} < y \Leftrightarrow \exists z\ (y = x + z) \wedge \neg\ (y = x)$
- Ост $(x, y) = v \Leftrightarrow (0 \leq v < y) \wedge \exists \boldsymbol{t}\ (x = y \times \boldsymbol{t} + v)$

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, и пусть $v_0, v_1, \ldots, v_{n-1}$ – такие натуральные числа, что $0 \le v_k < u_k$ для всех k.
- Тогда найдётся p такое, что $0 \le p < u_0 u_1 \ldots u_{n-1}$ и Ост$(p, u_k) = v_k$ для всех k.
- Д. Количество возможных цепочек остатков $v_0, v_1, \ldots, v_{n-1}$ равно $u_0 u_1 \ldots u_{n-1}$, то есть количеству таких чисел p, что $0 \le p < u_0 u_1 \ldots u_{n-1}$. Разные числа из указанного диапазона дают разные цепочки остатков, значит, каждая цепочка остатков встречается ровно один раз. (Пусть p и q дают одинаковые цепочки остатков, тогда их разность делится на все u_k, а в силу взаимной простоты чисел u_k, и на их произведение $u_0 u_1 \ldots u_{n-1}$.)

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

- $u_{\boldsymbol{i}} = y\boldsymbol{i}+z$, где $\boldsymbol{i} = 0, 1, \ldots n$-1. Взаимная простота?
- Общий делитель $u_{\boldsymbol{i}}$ и $u_{\boldsymbol{j}}$ делит $u_{\boldsymbol{i}} - u_{\boldsymbol{j}} = y(\boldsymbol{i} - \boldsymbol{j})$.
- Положим $z = y+1$, т.е. $u_{\boldsymbol{i}} = 1+y(1+\boldsymbol{i})$, y кратно (n-1)! (и больше всех кодируемых) $u_{\boldsymbol{i}}$ и $u_{\boldsymbol{i}} - u_{\boldsymbol{j}}$ взаимно просты.
- $\forall v_{\mathbf{0}}, v_{\mathbf{1}}, \ldots, v_{\boldsymbol{n}\mathbf{-1}}$ найдутся такие p (из китайской теоремы), y (разность прогрессии), что $v_{\boldsymbol{i}}$ является остатком от деления p на $1+y(1+\boldsymbol{i})$.
- Обозначим $\beta(x, y, \boldsymbol{i})$ = Ост$(x, 1+y(1+\boldsymbol{i}))$.
- *Бета-функция Гёделя*

Кодирование цепочки чисел

- Удобно кодировать вместе с элементами цепочки и её длину. Её можно ставить в начале цепочки.
- Итак, для любого набора натуральных чисел

$v_0, v_1, \ldots, v_{n\text{-}1}$ можно подобрать числа x, y такие, что

- $\beta(x, y, 0) = n$,
- $\beta(x, y, 1) = v_0$,
- $\beta(x, y, 2) = v_1$,
- …
- $\beta(x, y, n) = v_{n\text{-}1}$.
- Чем это может нам помочь при определении «естественных» отношений?

Определимость отношений

- Отношение $m = 2^n$ определимо?
- Найдётся цепочка длины n, первый элемент которой 1, каждый следующий вдвое больше предыдущего, а последний – это m.
- То есть, существуют x и y, для которых: $\wedge$
- $\beta(x, y, 0) = n$,
- $\beta(x, y, 1) = 2$,
- $\forall j \ (0 < j < \mathrm{n}) \ \rightarrow \ \beta(x, y, \mathrm{j} + 1) = 2\beta(x, y, \mathrm{j})$,
- $\beta(x, y, n) = m$.
- 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 = <D, Σ, Зн>.
- 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.*

Операции

- Имена операций
- Алфавит *имен объектов* $Ob=\{a_0, a_1, a_2,\ldots\}$

- Термы
- Задача. Построить синтаксис и семантику для термов.
- Задача. Построить синтаксис и семантику для алгебры отношений и операций.

Просеминар

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