Введение в математическую логику и теорию алгоритмов

Лекция 3

Алексей Львович Семенов

План

- Логика высказываний
- Структуры
- Логика отношений
- Что значит определить отношение?
- Примеры определимости
- Пространства определимости

Логика высказываний (повт.)

- 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.

Синтаксис логики высказываний (повт.)

Индуктивное определение (построение) формулы

- <u>Логические константы</u> 0 и 1 – формулы.
- <u>Имена высказываний</u> A_1, A_2,… – формулы. (Номера начинаются с 1.)
- Если Φ, Ψ – формулы, τ – связка: $\wedge$ (конъюнкция), $\vee$ (дизъюнкция), $\rightarrow$ (импликация), ≡ (эквивалентность), то $\neg$Φ, (Φ τ Ψ) – формулы.

Семантика логики высказываний (повт.)

Индуктивное определение (вычисление) значения формулы в (при) заданной интерпретации $\alpha \in$ B^{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 **(Φ τ Ψ),** где $\tau \in \{\to, \wedge, \vee, \equiv\}$, является (заданный таблично) результат применения τ к значениям формул Φ, Ψ.

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

Если наибольший номер переменной в формуле равен ***n***,

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

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 формула – одна, то выражение совпадает с ней,

  если последовательность пустая: $\vee$ **= 0,** $\wedge$ **= 1**.
- Где функция, задаваемая формулой $\neg A_1 \wedge \neg A_2 \wedge A_3$, равна 1?
  - Только при значении $<\alpha_1, \alpha_2, \alpha_3> \;=\; < 0, 0, 1 >$.
- Фиксируем натуральное число *n*.
  Обозначения: $\alpha = \alpha_1, \ldots, \alpha_n$; $A = A_1, \ldots, A_n$,
- $(0, A_i) = \neg A_i$
- $(1, A_i) = A_i$
- $(\alpha, A) = \wedge\, (\alpha_i, A_i)$

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

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

Это – СДНФ. (Д.Н.Ф. …)

Отношения (повт.)

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

Примеры

- 2-местное отношение равенства – множество всех пар $<x,x>$, $x \in D$.
- 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*

$Pr = \{P_1, P_2, \ldots\}$, каждому имени сопоставлено его количество аргументов.

• Сигнатура $\Sigma = < Pr >$, или конечный отрезок *Pr*.

• Часто используются также имена операций (функций), можно сводить функции к отношениям, см. выше. В последней части лекции мы вернемся к операциям.

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 множество рациональных чисел:

$\langle$**Q**, {<}, **3н**$\rangle$

Вместо 5<7 пишем <(5,7).

Поле действительных чисел

{Многочлен с целыми коэффициентами > или = 0}

- бесконечная сигнатура.

Множество всех слов в данном алфавите (свободный моноид)

– Каждый символ алфавита (одноместное отношение)

– Приписывание (трехместное отношение)

Логика отношений

Синтаксис 2. Продолжение

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

Атомные формулы

- **Если** P – имя n-местного отношения и $t_1, \ldots, t_\mathrm{n}$ – свободные переменные, то $P(t_1,\ldots,t_n)$ – атомная формула. (Если P – имя 0-местного отношения, то P – атомная формула.)
- **Если** t_1, t_2 – свободные переменные, то $t_1 = t_2$ – атомная формула.

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

Логика отношений. 2. Атомные формулы

Семантика 2. Продолжение

- Пусть задана структура: $< D, \Sigma, Зн >$, здесь *Зн* определена на символах отношений из Σ,

  и *интерпретация* $\alpha = \alpha_1, \alpha_2, \ldots$ *из* D^N.

- *Зн* свободной переменной – это элемент *D*:
  - *Зн* x_i = это α_i
- *Зн* атомной формулы – элемент **B**.

- *Зн* $P(t_1, \ldots, t_n)$ – применяем *Зн P* к *Зн* $t_1, \ldots,$ *Зн* t_n.
  - *Зн* $t_1 = t_2$ – совпадение *Зн* t_1 и *Зн* t_2.

  Значение атомной формулы в данной структуре – это отображение $D^N \rightarrow$ **B**, то есть N-местное отношение, α принимает все возможные значения;

  если наибольший номер переменной в формуле равен n, то с атомной формулой сопоставляется n-местное отношение.

Логика отношений. 3. Бескванторные синтаксис и семантика

Формула (заданной сигнатуры), индуктивное определение:

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

Семантика.

- Пусть задана структура: $<D, \Sigma, Зн>$

  и интерпретация $\alpha = \alpha_1, \alpha_2, \ldots$ *из* D^N.
- *Зн* формулы Φ определяется индуктивно.
- *Зн* атомной формулы $P(t_1, \ldots, t_n)$ – было.
- *Зн*$(\Phi\tau\Psi)$, где $\tau \in \{\to, \wedge, \vee, \equiv\}$, – 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:

- $\langle \mathbf{Q}, \{ > \}, \boldsymbol{\mathit{Зн}} \rangle$ ***Зн*** – обычное.
- **Как наглядно представить:**
  - $(x<y) \lor (x>y)$
  - $(x<y \land y<z) \lor (x>y \land y>z)$
  - $(x<y \land y<z) \lor (z<x \land x<y) \lor (y<z \land z<x)$
  - $(x<y \land t<z) \lor (x>y \land t>z)$?
  - Как записать, что два отрезка зацеплены (то есть – пересекаются, но не вложены один в другой)?

Как определить семантику формул с кванторами?

Кванторы:

- $\forall$ – *квантор всеобщности*, «для всех»
- $\exists$ – *квантор существования*, «существует»
- 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.
- Пример: $\sum_{k=0}^{100} x^{n-k}$ – что значит подставить вместо k число 8 ? Переменная k – связанная.
- Чтобы сохранить ясность, принимаются специальные меры.
- «Другие» имена для связанных переменных

Логика отношений

Замена:

- $\boldsymbol{A}\,[\,\boldsymbol{u}\,/\,\boldsymbol{x}\,]$ означает результат замены в слове ***A*** всех вхождений символа ***x*** на слово ***u*** (если ***x*** не входит в ***A,*** то результат – ***A***).

Синтаксис 3. Окончание

Фиксируем упорядоченный алфавит связанных переменных
BVar = $<\boldsymbol{u_1}, \boldsymbol{u_2},\ldots>$.
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).

Анализ. Тонкость – восстановление свободной переменной – берем первую не использованную.

Сокращения.

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

Логика отношений

Семантика 3 (окончание построения).

- Пусть задана структура: $<D, \Sigma, Зн>$

и интерпретация $\alpha = \alpha_1, \alpha_2, \ldots$ *из* D^{ω}.

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

- *Зн* атомной формулы $P(t_1, \ldots, t_n)$ – было.
- *Зн*$(\Phi \ \tau \ \Psi)$, где $\tau \in \{\to, \wedge, \vee, \equiv\}$ – результат

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

- *Зн* $\forall u \ \Phi[u/x_i]$ = $\wedge$ Зн Φ по всем β, совпадающим с α

на всех местах, кроме *i*–го.

- *Зн* $\exists u \ \Phi[u/x_i]$ = $\vee$ 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, не более 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**, IV век до н.э., исследование календаря, «Искусство войны»)

- Т. Пусть $u_1, \ldots, u_n$ – попарно взаимно простые натуральные числа, и пусть $v_1, \ldots, v_n$ – такие натуральные числа (остатки), что $0 \le v_k < u_k$ для всех k.
- Тогда найдётся p такое, что $0 \le p < u_1 \ldots u_n$ и Ост$(p, u_k) = v_k$ для всех k.
- Д. Количество возможных цепочек остатков $v_1, \ldots, v_n$ равно $u_1 \ldots u_n$, то есть количеству таких чисел p, что $0 \le p < u_1 \ldots u_n$. Разные числа из указанного диапазона дают разные цепочки остатков, значит, каждая цепочка остатков встречается (и 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 $u_1 \ldots u_n$.)

Кодирование цепочек чисел

- Как можно кодировать цепочки чисел с помощью чисел? (Или, хотя бы, с помощью цепочек ограниченной длины.)
- Китайская теорема об остатках.
  Чтобы получить цепочку из n чисел,
  используется число *p*,
  которое и оказывается кодом.
- Нужна какая-нибудь цепочка
  из n попарно взаимно простых чисел.
- Как ее получить без того,
  чтобы не вернуться к кодированию
  произвольных цепочек?

Кодирование цепочки чисел

Попробуем взять в качестве u_i арифметическую прогрессию:

• $u_i = y\mathbf{i}+z$, где $\mathbf{i} = 1,\dots n$.

Задача. Подобрать y, z чтобы обеспечить взаимную простоту.

• $\forall v_1, \dots, v_n$ найдутся такие p (из китайской теоремы), y (разность прогрессии), что v_i является остатком от деления p на $1+y(1+\mathbf{i})$.

• Обозначим $\beta(x, y, \mathbf{i}) = \text{Ост}(x, 1+y(1+\mathbf{i}))$.

• *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

$v_1, \ldots, v_n$ можно подобрать числа x, y такие, что

- $\beta(x, y, 0) = n$,
- $\beta(x, y, 1) = v_1$,
- $\beta(x, y, 2) = v_2$,
- …
- $\beta(x, y, n) = v_n$.
- Чем это может нам помочь при определении «естественных» отношений?

Определимость отношений

- **Задача**. Отношение $m = 2^n$ определимо?
- Найдётся цепочка длины n, первый элемент которой 1, каждый следующий вдвое больше предыдущего, а последний – это m…
- **Задача**. Все функции, вычислимые алгоритмами, определимы…

Пространства определимости

- Фиксируем множество D.
- Множество отношений R.
- Дадим всем отношениям из R имена из Σ, то есть зададим *Зн*.
- Структура $S = \langle D, \Sigma, \mathit{Зн} \rangle$.
- 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, *пространство определимости.*

Алгебра пространств определимости

- Замыкание монотонно по включению множеств.
- **Задача**. Пересечение пространств – замкнуто.
- Объединение пространств = замыкание теоретико-множественного объединения.

Операции

- Имена операций
- Алфавит *имен объектов* $Ob=\{a_0, a_1, a_2,\ldots\}$
- **Задача.** Определить термы – выражения…
- **Задача**. Построить синтаксис и семантику для термов.
- **Задача**. Построить синтаксис и семантику для логики отношений и операций.

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.
- Для теории структуры может существовать алгоритм выяснения истинности.
- Логику отношений часто называют *логикой предикатов.*

Просеминар

- по математической логике и информатике http://proseminar.math.ru/
- пятница, 16:45–18:20, аудитория 16–22
- 3 октября