

Математическая логика и теория алгоритмов

Сергей Григорян

11 сентября 2024 г.

Содержание

1	Инфа	3
2	Синтаксис \leftrightarrow Семантика	3
3	Правильные скобочные п-ти (ПСП)	4
3.1	ОПР 1 \Rightarrow ОПР 3	5
3.2	ОПР 2 \Rightarrow ОПР 1	5
3.3	ОПР 3 \Rightarrow ОПР 2	5
4	Синтаксис \leftrightarrow Семантика	5
5	Формулы с 1-ой бинарной связкой * (Правильные алгебраические выр-я)	6
6	Булевы функции	7
7	Пропозициональные ф-лы \leftrightarrow Булевы ф-ции	8

1 Инфа

Лектор: Мусатов

Книги: Верещагин Н. К., Шень А. "Лекции по мат. логике":

№ 1 Начало теории мн-в

№ 2 Языки и исчисления

№ 3 Вычислимые ф-ции

2 Синтаксис \leftrightarrow Семантика

Определение 2.1. Синтаксис - правила составления форм. выр-ий.

Определение 2.2. Семантика - сопоставление форм выр-ия некоторого смысла.

Определение 2.3. Алфавит - мн-во символов. (Непустое, обычно конечно)

Определение 2.4. Слово - конечная последовательность символов алфавита. (Может быть пустым)

Пустое слово - ε

Определение 2.5. Язык - любое мн-во слов.

Пустой язык - \emptyset

Синглетон - $\{\varepsilon\}$

Операции над словами:

- Конкатенация: $u * v$
- Возведение в степень: $u^n = u * u * \dots * u$ - n раз ($u^0 = \varepsilon$)
- Обращение: $u^R = u_n u_{n-1} \dots u_1$, если $u = u_1 u_2 \dots u_n$

$$(ab)^R = b^R a^R.$$

Отношения над словами:

- Префикс $u \sqsubset v \iff \exists w: uw = v$

- Суффикс $u \sqsupset v \iff \exists w: wu = v$
- Подслово $u(\text{subset})v \iff \exists t, w: tuw = v$
- Подп-ть $u \subset v \iff$ вычеркнута часть символов v и получили u

Операции над языками:

0) Теоретико-мнoж.

1) Конкатенация:

$$L * M = \{u * v | u \in L, v \in M\}.$$

$$L * \emptyset = \emptyset.$$

Пример.

$$L = \{a, ab\}, M = \{a, ba\}, LM = \{aa, aba, abba\}.$$

2) $L^n = L * L * \dots * L$ - n раз

$$L^0 = \{\varepsilon\}.$$

3) Итерация/Звезда Клини:

$$L^* = L^0 \cup L^1 \cup L^2 \cup \dots = \bigcup_{k=0}^{\infty} L^k.$$

$$L^+ = \bigcup_{k=1}^{\infty} L^k = L^* * L.$$

$$L^* = L^+ * \{\varepsilon\}.$$

3 Правильные скобочные п-ти (ПСП)

Определение 3.1. ПСП - это п-ть скобок, разбитых на пары, и в каждой паре "(" раньше ")".

Определение 3.2. ПСП - это п-ть, получ. из правил:

1. ε - это ПСП;
2. s - ПСП $\Rightarrow (s)$ - ПСП;
3. s, t - ПСП, $\Rightarrow st$ - ПСП.

Определение 3.3. Баланс СП - (кол-во "(" - (кол-во ")")

Определение 3.4. ПСП - СП, для кот. баланс всей п-ти = 0, а любого др. префикса ≥ 0

3.1 ОПР 1 \Rightarrow ОПР 3

Все скобки разбиты на пары \Rightarrow баланс = 0.

"("левее ")" \Rightarrow в любом префиксе из каждой пары, ни одной, обе или только "(" . В любом случае итоговый баланс префикса ≥ 0 .

3.2 ОПР 2 \Rightarrow ОПР 1

Скобки, добавленные по правилу (s), будут в паре.

3.3 ОПР 3 \Rightarrow ОПР 2

Д-во: индукция по длине СП

База: $s = \varepsilon \Rightarrow$ подх. по опр. 2

Осн. случ.: $|s| > 0 \Rightarrow$ первый символ "(".

Рассм. кратчайший непустой префикс с балансом = 0:

Случай 1: Это вся п-ть: $s = (s') \Rightarrow$ для s' верно ОПР 3 (т. к. любой другой баланс по случаю ≥ 1) \Rightarrow и ОПР 2.

Случай 2: Это собств. префикс (\neq всей строке): $s = (s')t$. И для s' , и для t - выполнено ОПР 3 \Rightarrow ОПР 2.

4 Синтаксис \leftrightarrow Семантика

Синтаксис	Семантика
Пропозициональные формулы Пропозициональные переменные Знаки логических действий ($\wedge, \vee, \rightarrow, \neg$) Скобки	Булевы ф-ции

5 Формулы с 1-ой бинарной связкой * (Правильные алгебраические выр-я)

Рекурсивное правила:

- 1) p - переменная $\Rightarrow p$ - ПАВ (правильное алг. выр-е).
- 2) ϕ, ψ - ПАВ $\Rightarrow (\phi * \psi)$ - ПАВ.

Пример. $((a * b) * (c * (d * e)))$

Теорема 5.1. *Между ПАВ и деревьями синт. разбора \exists взаимно однозначное соотв. (биекция)*

Мы докажем: для любого ПАВ η , не являющегося перменной, $\exists!$ пара (ϕ, ψ) , т. ч. $\eta = (\phi * \psi)$

Лемма 5.2 (О балансе скобок). *Баланс любого префикса ПАВ ≥ 0 , при этом $= 0$ только для ε и всего ПАВ.*

Доказательство. Индукция по построению.

База: p - переменная \Rightarrow 2 префикса: ε и p , баланс = 0

Переход: Пусть для ϕ и ψ лемма верна. Докажем для $(\phi * \psi)$

Префиксы	Баланс
ε	0
$(\phi', \phi' \sqsubset \phi$	$1 + \text{bal}(\phi') > 0$
$(\phi * \psi', \psi' \sqsubset \psi$	$1 + 0 + \text{bal}(\psi') > 0$
$(\phi * \psi)$	0

□

Лемма 5.3. ϕ и ψ восстанавливаются однозначно.

Доказательство. От противного: пусть $(\phi * \psi) = (\zeta * \xi)$

Случай 1) ϕ - собств. префикс ζ , $\phi \neq \varepsilon$. Тогда в конце ϕ баланс = 0 (т. к. ϕ - ПАВ), и > 0 (т. к. ζ - ПАВ, которое на момент конца ϕ не кончилось) \Rightarrow !!! (противоречие)

Случай 2) $\phi = \zeta$. Однако тогда и $\psi = \xi$ (сократили одинаковые символы)

□

Для пропозициональных формул (ПФ):

Рекурс. опр.:

- 1) p - переменная $\Rightarrow p$ - ПФ
- 2) ϕ, ψ - ПФ $\Rightarrow (\phi \wedge \psi), (\phi \vee \psi), (\phi \rightarrow \psi)$ - ПФ.
- 3) ϕ - ПФ $\Rightarrow \neg\psi$ - ПФ

Лемма 5.4 (О балансе). Баланс префикса ПФ ≥ 0 , при этом $= 0$ только для ε , всей ПФ или $\neg\neg\dots\neg$.

Замечание. *Однозначность разбора:* для любой ПФ сущ. единств. правило из (1-3) и единств. сост., из кот. она получ.

6 Булевы функции

Булевы значения: $\{0, 1\}$

Булева ф-ция от k переменных $f : \{0, 1\}^k \rightarrow \{0, 1\}$

$\Rightarrow f$ принимает на вход 2^k различных кортежей. Каждому кортежу может быть сопоставлено 2 значения \Rightarrow .

Общее число ф-ций - 2^{2^k}

Пример. $k = 1 \Rightarrow 2^{2^k} = 4$

p	\perp	p	$\neg p$	T
0	0	0	1	1
1	0	1	0	1

Пример. $k = 0 \Rightarrow 2^{2^0} = 2$ 2 ф-ции:

$$\begin{cases} f(\varepsilon) = 0(\perp) \\ f(\varepsilon) = 1(T) \end{cases}$$

Пример. $k = 2 \Rightarrow 2^{2^2} = 16$

p	q	\perp	T	$p = pr_1$	$q = pr_2$	$\neg p$	$\neg q$	\wedge	\vee	\oplus	$p \rightarrow q$	$q \rightarrow p$	\leftrightarrow	\nrightarrow	\nleftarrow
0	0	0	1	0	0	1	1	0	0	0	1	1	1	0	0
0	1	0	1	0	1	1	0	0	1	1	1	0	0	0	1
1	0	0	1	1	0	0	1	0	1	1	0	1	0	1	0
1	1	0	1	1	1	0	0	1	0	0	1	1	1	0	0
								\min	\max	$\text{xor } (\neq)$	\leq	\geq	$=$		

\downarrow	\uparrow
1	1
0	1
0	1
0	0
<i>Стрелка Пирса (NOR)</i>	<i>Штрих Шеффера (NAND)</i>

Обозначение. $k > 2$, $\wedge_k, \vee_k, \oplus_k$, (\oplus_k - ϕ -ция чётности (PARITY))

Обозначение.

$$\text{maj}(p, q, r) = \begin{cases} 1, & p + q + r \geq 2 \\ 0, & p + q + r \leq 1 \end{cases}$$

Функция большинства

maj_{2k+1} - задаётся аналогичным образом

Пороговые функции:

$$\text{thr}_{k,n}(p_1, \dots, p_n) = \begin{cases} 1, & \sum_{i=1}^n p_i \geq k \\ 0, & \text{иначе} \end{cases}$$

Тернарный оператор:

$$p ? q : r = \begin{cases} q, & p = 1 \\ r, & p = 0 \end{cases}$$

7 Пропозициональные ф-лы \leftrightarrow Булевы ф-ции

- Переход \implies : Вычисление (По табл. истинности)
- Переход \longleftarrow : Представление

Пример. $((p \wedge q) \vee (r \rightarrow \neg s)) \iff$ *Дерево разбора*
Листья дерева = значения переменных

Правила вычисления знач. ф-лы:

Обозначение.

p_1, p_2, \dots, p_n - переменные.

a_1, a_2, \dots, a_n - значения переменных (0/1)

$[\phi](a_1, a_2, \dots, a_n)$ - знач. ф-лы ϕ на арг-тах (a_1, a_2, \dots, a_n)

Определение 7.1. 1) $[p_i](a_1, a_2, \dots, a_n) = a_i$

2) $[\neg\psi](a_1, a_2, \dots, a_n) = \text{neg}([\psi](a_1, \dots, a_n))$

- \neg - символ из ф-лы
- neg - булева ф-ция

3) $[(\eta \wedge \xi)](a_1, a_2, \dots, a_n) = \text{and}([\eta](a_1, a_2, \dots, a_n), [\xi](a_1, a_2, \dots, a_n))$

(\vee - or, \rightarrow - implies)

Булева ф-ция получается из пропоз. ф-лы, если провести вычисл. для всех (a_1, a_2, \dots, a_n)

Определение 7.2. Литерал - переменная или отрицание переменной.
 $(p, \neg q)$

Определение 7.3. Конъюнкт - конъюнкция литералов $(p \wedge \neg q \wedge r)$

Определение 7.4. Дизъюнкт - дизъюнкция литералов $(p \vee \neg q \vee r)$

Определение 7.5. Конъюнктивная нормальная форма (КНФ) - конъюнкция дизъюнктов $((\neg p \vee \neg q \vee r) \wedge (q \vee \neg s))$

Определение 7.6. Дизъюнктивная нормальная форма (ДНФ) - дизъюнкция конъюнктов $((p \wedge \neg q \wedge r) \vee (\neg p \wedge s))$

Теорема 7.1. Любая булева ф-ция выражима как КНФ и как ДНФ

p	q	r	Значения ф-ции	ДНФ	КНФ
0	0	0	0		$(p \vee q \vee r) \wedge$
0	0	1	1	$(\neg p \wedge \neg q \wedge \neg r) \vee$	
0	1	0	1	$(\neg p \wedge q \wedge \neg r) \vee$	
0	1	1	0		$(p \vee \neg q \vee \neg r) \wedge$
1	0	0	0		$(\neg p \vee q \vee r) \wedge$
1	0	1	0		$(\neg p \vee q \vee \neg r) \wedge$
1	1	0	1	$(p \wedge q \wedge \neg r) \vee$	
1	1	1	0		$(\neg p \vee \vee \neg q \vee \neg r) \wedge$

Пример.

$$f \equiv 0 \Rightarrow f = p \wedge \neg p$$