Математическая логика и теория алгоритмов

Сергей Григорян

18 сентября 2024 г.

Содержание

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** - соспоставление форм выр-ия некоторого смысла.

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

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: $u^n = u * u * \cdots * u$ - n раз ($u^0 = \varepsilon$)
- Обращение: $u^R = u_n u_{n-1} \cdots u_1,$ если $u = u_1 u_2 \cdots u_n$

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

Отношения над словами:

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

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

Операции над языками:

0) Теоретико-множ.

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

Синтакис	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 деревъями синт. разбора $\exists$ взаимно однозначное соотв. (биекция)*

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

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
$(\phi', \phi' \sqsubset \phi$	$1 + \mathrm{bal}(\phi') > 0$
$(\phi * \psi', \psi' \sqsubset \psi$	$1 + 0 + \mathrm{bal}(\psi') > 0$
$(\phi * \psi)$	0

$\square$

Лемма 5.3. *ϕ и ψ восстанавливаются однозначно.*

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

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)

$\square$

Для пропозициональных формул (ПФ):
Рекурс. опр.:

1) p - переменная $\Rightarrow p$ - ПФ
2) ϕ, ψ - ПФ $\Rightarrow (\phi \wedge \psi), (\phi \vee \psi), (\phi \to \psi)$ - 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 $f : \{0,1\}^k \to \{0,1\}$

$\Rightarrow f$ 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:*

$$\left[\begin{array}{l} f(\varepsilon) = 0(\perp) \\ f(\varepsilon) = 1(T) \end{array}\right.$$

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

p	q	$\perp$	T	$p = pr_1$	$q = pr_2$	$\neg p$	$\neg q$	$\wedge$	$\vee$	$\oplus$	$p \to q$	$q \to p$	$\leftrightarrow$	$\to$	$\leftarrow$
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*	*xor* ($\neq$)	$\leq$	$\geq$	$=$		

$\downarrow$	$\uparrow$
1	*1*
0	*1*
0	*1*
0	*0*
Стрелка Пирса (NOR)	*Штрих Шеффера (NAND)*

<u>Обозначение</u>. *$k > 2$, $\wedge_k, \vee_k, \oplus_k$, ($\oplus_k$ - ф-ция чётности (PARITY))*

<u>Обозначение</u>.

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

Функция большинства

maj_{2k+1} - задаётся аналогичным образом

Пороговые функции:

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

Тернарный оператор:

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

7 Пропозициональные ф-лы $\leftrightarrow$ Булевы ф-ции

- Переход $\Longrightarrow$: <u>Вычисление</u> (По табл. истинности)
- Переход $\Longleftarrow$: <u>Представление</u>

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

Правила вычисления знач. ф-лы:

Обозначение.

$p_1, p_2, \ldots, p_n$ - *переменные.*
$a_1, a_2, \ldots, a_n$ - *значения переменных (0/1)*
$[\phi](a_1, a_2, \ldots, a_n)$ - *знач. ф-лы* ϕ *на арг-тах* $(a_1, a_2, \ldots, a_n)$

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

2) $[\neg\psi](a_1, a_2, \ldots, a_n) = neg([\psi](a_1, \ldots, a_n))$

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

3) $[(\eta \wedge \xi)](a_1, a_2, \ldots, a_n) = and([\eta](a_1, a_2, \ldots, a_n), [\xi](a_1, a_2, \ldots, a_n))$
($\vee$ - or, $\to$ - implies)

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

Определение 7.2. Литерал - перменная 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 выразима 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.

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

Пропозициональные ф-лы	$\leftrightarrow$	Булевы ф-ции
	$\rightarrow$	Семантика табл. истины
КНФ/ДНФ	$\leftarrow$	

8 Мн-ны Жегалкина

Вместо $\neg, \wedge, \vee$ используем $*(\wedge), \oplus$

Особенности мн-нов над булевыми переменными:

1) $x^2 = x$

2) $x \oplus x = 0$

Эти особенности можно отразить в определении.

Определение 8.1. Пусть $x_1, \ldots, x_n$ - переменные.

Тогда **одночленом Жегалкина** наз-ся произведение каких-то переменных (В том числе 1 = произведению пустого мн-ва переменных).

Многочленом Жегалкина наз-ся сумма каких-то одночленов. (В том числе 0 = сумма пустого мн-ва одночленов)

(Порядок произведения и суммы не важен)

Пример. *1)*

$$\neg p = p \oplus 1$$

2)

$$p \wedge q = pq$$

3)

$$p \vee q = \neg(\neg p \wedge \neg q) = (p \oplus 1)(q \oplus 1) \oplus 1 = p \oplus q \oplus pq$$

4)

$$p \to q = \neg p \vee q = (p \oplus 1) \oplus q \oplus (p \oplus 1)q = pq \oplus p \oplus 1$$

5)

$$maj_3(p, q, r) = \begin{cases} 1, p + q + r \geq 2 \\ 0, p + q + r \leq 1 \end{cases} = pq \oplus qr \oplus pr$$

Теорема 8.1. *Любую булеву ф-цию можно однозначно представить как мн-н Жегалкина. (С точностью до порядка множителей и слагаемых)*

Кол-во булевых ф-ций $= 2^{2^n}$
Кол-во одночленов $= 2^n$
Кол-во многочленов $= 2^{2^n}$
Мн-н $\mapsto$ Ф-ция (вычисл.)
Почему 2 мн-на не могут дать одну ф-цию?

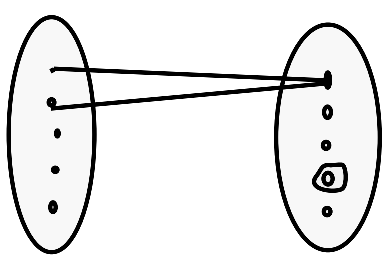

Рис. 1:

Доказательство. Пусть не так, и есть 2 мн-на $P \neq Q\colon \forall x\colon P(x) = Q(x)$

Рассм. $S(x) = P(x) \oplus Q(x) \not\equiv 0$ (как мн-н)

Тогда $\forall x\colon S(x) = 0$

Рассм. одночлен, в кот. меньше всего множителей. Если таких несколько, то любой из них.

Б. О. О. это $x_1 x_2 \dots x_k$. Рассм. $a = (1, 1, 1, \dots, 1, 0, 0, 0, \dots, 0)$ (k ед-ц, $(n-k)$ нулей).

$$S(a) = x_1 x_2 \dots x_k \oplus (\dots)$$

$S(a) = 1 * \dots * 1 \oplus (\dots) = 1$(т. к., в ост. слагаемых есть перменные, кроме $x_1 \dots x_k$)

Но, $\forall x\colon S(x) = 0 \Rightarrow$ противоречие. $\square$

Все ф-ции можно выразить через: $\neg, \wedge, \vee$ (КНФ/ДНФ). Даже можно через $\neg, \wedge$ или $\neg, \vee$(используем законы Де Моргана).

Мн-н Жегалкина позволяет выразить все ф-ции через $\wedge, \oplus$ и 1

А можно ли выразить всё через $\wedge, \vee, \rightarrow$? **ОТВЕТ: НЕТ.**

Причина: т. к.:

- $1 \wedge 1 = 1$
- $1 \vee 1 = 1$
- $1 \rightarrow 1 = 1$

$\Rightarrow$ Значение такой ф-лы, на $(1, 1, \dots, 1) = 1$. Те ф-ции, где $f(1, 1, \dots, 1) = 0$ выр-ть нельзя.

Обозначение. ***Класс ф-ций, сохр. единицу****, обозначается как* P_1

Определение 8.2. Суперпозиция ф-ций $f, g_1, \dots, g_k$ (где k - число арг-ов f) - это

$$h(x_1, x_2, \dots, x_n) = f(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n)) \qquad (1)$$

Более формально:

Суперпозиция **нулевого порядка** - это проекторы:

$$pr_i(x_1, \dots, x_n) = x_i$$

Суперпозиция порядка $(m+1)$ - это f (см. (1)), где f - одна из базовых ф-ций, $g_1, g_2, \dots, g_k$ - суперпозиции порядка $\leq m$.

Теорема 8.2. *Все базовые ф-ции сохр. 1 $\Rightarrow$ все суперпозиции тоже.*

Определение 8.3. Пусть C - мн-во ф-ций. Тогда мн-во всех суперпозиций ф-ций из C наз-ся **замыканием** C и обозначается $[C]$

Когда $[C]$ - это все функции? (Если это так, то C наз-ся полной системой)

8.1 Препятствие 1: $C \subset P_1$

Определение 8.4. P_0 - класс ф-ций, сохр. 0, т. е. таких, что $f(0, \dots, 0) = 0$

Аналогичная теорема верна для P_0 (Все баз. ф-ции, сохр. 0 $\Rightarrow$ все суперпоз-ции тоже)

8.2 Препятствие 2: $C \subset P_0$

Пример. $\wedge, \vee, \oplus$

Определение 8.5. M - монотонная ф-ции:

f - монотонна, если $\forall(a_1, \dots, a_n), \forall(b_1, \dots, b_n)\colon (a_i \leq b_i), \forall i = 1, \dots, n \Rightarrow (f(a_1, \dots, a_n) \leq f(b_1, \dots, b_n))$

Пример. $\vee, \wedge$ - *монот.*

$\neg, \rightarrow, \oplus$ - *немонот.*

Утверждение 8.1. *Суперпозиция монот. ф-ций монотонна.*

Доказательство. $f(g_1(x_1, x_2, \dots, x_n), \dots, g_k(x_1, \dots, x_n))$

$g_i - \uparrow, \forall i = 1, \dots, k \Rightarrow f \uparrow$ $\square$

8.3 Препятствие 3: $C \subset M$