

# Математическая логика и теория алгоритмов

Сергей Григорян

23 сентября 2024 г.

# Содержание

<b>1</b>	<b>Лекция 1</b>	<b>3</b>
1.1	Инфа . . . . .	3
1.2	Синтаксис $\leftrightarrow$ Семантика . . . . .	3
1.3	Правильные скобочные п-ти (ПСП) . . . . .	5
1.4	ОПР 1 $\Rightarrow$ ОПР 3 . . . . .	5
1.5	ОПР 2 $\Rightarrow$ ОПР 1 . . . . .	5
1.6	ОПР 3 $\Rightarrow$ ОПР 2 . . . . .	5
<b>2</b>	<b>Лекция 1++</b>	<b>6</b>
2.1	Синтаксис $\leftrightarrow$ Семантика . . . . .	6
2.2	Формулы с 1-ой бинарной связкой * (Правильные алгебраические выр-я) . . . . .	6
<b>3</b>	<b>Лекция 2</b>	<b>7</b>
3.1	Булевы функции . . . . .	7
3.2	Пропозициональные ф-лы $\leftrightarrow$ Булевы ф-ции . . . . .	9
<b>4</b>	<b>Лекция 3</b>	<b>10</b>
4.1	Мн-ны Жегалкина . . . . .	10
4.2	Препятствие 1: $C \subset P_1$ . . . . .	13
4.3	Препятствие 2: $C \subset P_0$ . . . . .	13
4.4	Препятствие 3: $C \subset M$ . . . . .	13

# 1 Лекция 1

## 1.1 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

## 1.2 Синтаксис $\leftrightarrow$ Семантика

**Определение 1.1. Синтаксис** - правила составления форм. выр-ий.

**Определение 1.2. Семантика** - сопоставление форм выр-ия некоторого смысла.

**Определение 1.3. Алфавит** - мн-во символов. (Непустое, обычно конечно)

**Определение 1.4. Слово** - конечная последовательность символов алфавита. (Может быть пустым)

**Пустое слово** -  $\varepsilon$

**Определение 1.5. 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-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:

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

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

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

### 1.3 Правильные скобочные п-ти (ПСП)

**Определение 1.6.** ПСП - это п-ть скобок, разбитых на пары, и в каждой паре "(" раньше ")".

**Определение 1.7.** ПСП - это п-ть, получ. из правил:

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

**Определение 1.8.** Баланс СП - (кол-во "(") - (кол-во ")")

**Определение 1.9.** ПСП - СП, для кот. баланс всей п-ти = 0, а любого др. префикса  $\geq 0$

### 1.4 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  $\geq 0$ .

### 1.5 ОПР 2 $\Rightarrow$ ОПР 1

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

### 1.6 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  $\geq 1$ )  $\Rightarrow$  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.

## 2 Лекция 1++

### 2.1 Синтаксис $\leftrightarrow$ Семантика

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

### 2.2 Формулы с 1-ой бинарной связкой \* (Правильные алгебраические выр-я)

Рекурсивное правила:

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

**Пример.**  $((a * b) * (c * (d * e)))$

**Теорема 2.1.** *Между ПАВ и деревьями синт. разбора  $\exists$  взаимно однозначное соотв. (биекция)*

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

**Лемма 2.2** (О балансе скобок). *Баланс любого префикса ПАВ  $\geq 0$ , при этом  $= 0$  только для  $\varepsilon$  и всего ПАВ.*

*Доказательство.* Индукция по построению.

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

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

Префиксы	Баланс
$\varepsilon$	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 2.3.**  $\phi$  и  $\psi$  восстанавливаются однозначно.

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

Случай 1)  $\phi$  - собств. префикс  $\zeta$ ,  $\phi \neq \varepsilon$ . Тогда в конце  $\phi$  баланс = 0 (т. к.  $\phi$  - ПАВ), и  $> 0$  (т. к.  $\zeta$  - ПАВ, которое на момент конца  $\phi$  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)  $\phi, \psi$  - ПФ  $\Rightarrow (\phi \wedge \psi), (\phi \vee \psi), (\phi \rightarrow \psi)$  - ПФ.
- 3)  $\phi$  - ПФ  $\Rightarrow \neg\phi$  - ПФ

**Лемма 2.4** (О балансе). Баланс префикса ПФ  $\geq 0$ , при этом = 0 только для  $\varepsilon$ , 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.

## 3 Лекция 2

### 3.1 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  $\phi$ -цм:

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

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

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

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

**Обозначение.**  $k > 2$ ,  $\wedge_k, \vee_k, \oplus_k$ , ( $\oplus_k$  -  $\phi$ -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

$\text{maj}_{2k+1}$  - 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:**

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



### 3.2 Пропозициональные ф-лы $\leftrightarrow$ Булевы ф-ции

- Переход  $\Rightarrow$ : Вычисление (По табл. истинности)
- Переход  $\Leftarrow$  : Представление

Пример.  $((p \wedge q) \vee (r \rightarrow \neg s)) \iff \text{Дерево разбора}$   
*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  $\phi$  на арг-тах  $(a_1, a_2, \dots, a_n)$

Определение 3.1. 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 3.2. **Литерал** - переменная или отрицание переменной.  
 $(p, \neg q)$

Определение 3.3. **Конъюнкт** - конъюнкция литералов  $(p \wedge \neg q \wedge r)$

Определение 3.4. **Дизъюнкт** - дизъюнкция литералов  $(p \vee \neg q \vee r)$

Определение 3.5. **Конъюнктивная нормальная форма (КНФ)** - конъюнкция дизъюнктов  $((\neg p \vee \neg q \vee r) \wedge (q \vee \neg s))$

Определение 3.6. **Дизъюнктивная нормальная форма (ДНФ)** - дизъюнкция конъюнктов  $((p \wedge \neg q \wedge r) \vee (\neg p \wedge s))$

**Теорема 3.1.** 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		$(\neg p \vee \neg q \vee \neg r) \wedge$

**Пример.**

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

## 4 Лекция 3

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

### 4.1 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 4.1.** Пусть  $x_1, \dots, x_n$  - 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)

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

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 4.1. 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?

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

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

Тогда  $\forall x: S(x) = 0$

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 переменные, кроме  $x_1 \dots x_k$ )

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

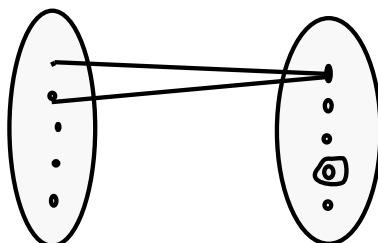


Рис. 1:

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

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

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

**Определение 4.3.** 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**)

## 4.2 Препятствие 1: $C \subset P_1$

**Определение 4.4.**  $P_0$  - 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 суперпозиции тоже)

## 4.3 Препятствие 2: $C \subset P_0$

**Пример.**  $\wedge, \vee, \oplus$

**Определение 4.5.**  $M$  - монотонная ф-ции:

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

**Пример.**  $\vee, \wedge$  - монот.

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

**Утверждение 4.1.** *Суперпозиция монот. ф-ций монотонна.*

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

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

□

## 4.4 Препятствие 3: $C \subset M$