Математическая логика и теория алгоритмов

Сергей Григорян

25 сентября 2024 г.

Содержание

1 Лекция 3

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

1.1 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 1.1. 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)

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

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 1.1. *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?

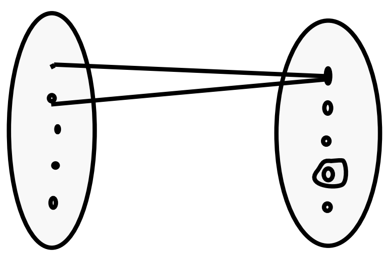

Рис. 1:

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

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

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

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 $\wedge, \vee, \to$? **ОТВЕТ: НЕТ.**

Причина: т. к.:

- $1 \wedge 1 = 1$
- $1 \vee 1 = 1$
- $1 \to 1 = 1$

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

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

Определение 1.2. **Суперпозиция** ф-ций $f, g_1, \ldots, g_k$ (где k - число арг-ов f) - это

$$h(x_1, x_2, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n)) \tag{1}$$

Более формально:

Суперпозиция **нулевого порядка** - это проекторы:

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

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

Теорема 1.2. *Все базовые ф-ции сохр.* 1 $\Rightarrow$ *все суперпозиции тоже.*

Определение 1.3. 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)

1.2 Препятствие 1: $C \subset P_1$

См. выше

1.3 Препятствие 2: $C \subset P_0$

Определение 1.4. P_0 - класс ф-ций, сохр. 0, т. е. таких, что

$$f(0, \ldots, 0) = 0$$

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

Пример. $\wedge, \vee, \oplus$

1.4 Препятствие 3: $C \subset M$

Определение 1.5. M - монотонная ф-ции:

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

Пример. $\vee, \wedge$ - *монот.*

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

Утверждение 1.1. *Суперпозиция монот. ф-ций монотонна.*

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

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

2 Лекция 4

2.1 Системы связок

Бывают двух типов:

- Полные (все ф-ции выразимы)

  Пример. – $\{\neg, \wedge, \vee, \rightarrow\}$
  – $\{\neg, \wedge\}$
  – $\{\neg, \vee\}$
  – $\{1, \oplus, \wedge\}$
  – $\{\rightarrow, 0\}$

Доказательство. $\neg p = p \to 0$
$p \vee q = \neg p \to q$ $\square$

- Неполные
  - $\{\to, \wedge, \vee\}$ - сохраняют 1
  - $\{\wedge, \oplus\}$ - сохраняют 0
  - $\{\wedge, \vee, 0, 1\}$ - монотонность
  - $\{\neg, maj_3\}$ - самодвойственные ($f(\neg\overline{p}) = \neg f(\overline{p}); \overline{p} = (p_1, p_2, \ldots, p_n)$)
    Иными словами, $f = f^*\colon f^*(p_1, p_2, \ldots, p_n) = \neg f(\neg p_1, \neg p_2, \ldots, \neg p_n)$

    Пример.

    $$\wedge^* = \vee, \vee^* = \wedge$$

    $$\neg(\neg p \wedge \neg q) = p \vee q$$

    $$\oplus^* = \leftrightarrow$$

    $$\neg(\neg p \oplus \neg q) = \neg(p \oplus q) = (p \leftrightarrow q)$$

    $$h(p_1, p_2, \ldots, p_n) = f(g_1(p_1, \ldots, p_n), g_2(p_1, \ldots, p_n), \ldots, g_n(p_1, \ldots, p_n))$$

    $$h(\neg p_1, \ldots, \neg p_n) = f(g_1(\neg p_1, \ldots, \neg p_2), \ldots, g_n(\neg p_1, \ldots, \neg p_n))$$

    $$h(\neg p_1, \ldots, \neg p_n) = f(\neg g_1(p_1, \ldots, p_n), \ldots, \neg g_n(p_1, \ldots, p_n))$$

    $$h(\neg p_1, \ldots, \neg p_n) = \neg f(g_1(p_1, \ldots, p_n), \ldots, g_n(p_1, \ldots, p_n)) = \neg h(p_1, \ldots, p_n)$$
  - $\{\oplus, 1\}$ - Линейные (Афинные) - ф-ции, задающиеся линейными мн-нами Жегалкина

Теорема 2.1 (Критерий Поста)**.** *Система связок полна $\iff$ она не является подмн-вом ни одного из 5-ти классов:*

- P_0 - *сохр. 0*
- P_1 - *сохр. 1*
- M - *монотонные*
- $D(S)$ - *самодвойственные*
- L - *линейные*

$\iff$ *система содержит некот. ф-цию (ф-ции):*

$$f_0 \notin P_0, f_1 \notin P_1, g \notin M, h \notin D, R \notin L$$

Доказательство.

<ins>Шаг 1</ins>

$$f_0(0,0,\ldots,0) = 1, (\text{т. к. } f_0 \text{ не сохр. } 0)$$

$$f_0(1,1,\ldots,1) = \begin{bmatrix} 0 \Rightarrow f_0(p,p,p,\ldots,p) = \neg p \\ 1 \Rightarrow f_0(p,p,p,\ldots,p) = 1 \end{matrix}$$

<ins>Шаг 2</ins>

$$f_1(1,\ldots,1) = 0$$

$$f_1(0,\ldots,0) = \begin{bmatrix} 0 \Rightarrow f_1(p,\ldots,p) = 0 \\ 1 \Rightarrow f_1(p,\ldots,p) = \neg p \end{matrix}$$

$f_1 \backslash f_0$	$\neg$	1
$\neg$	шаг 4	$0 = \neg 1$
0	$1 = \neg 0$	шаг 3

0, 1, $\neg \rightarrow$ шаг 5

<ins>Шаг 3</ins> $0, 1, g \notin M \mapsto \neg$

<ins>Пример</ins>.

$$\neg p = (p \to 0)$$

$$\neg p = (p \oplus 1)$$

$$\neg p = exact_{1,3}(0,1,p)$$

<ins>Определение</ins> 2.1. Монотонная ф-ция - ф-ция, т. ч.:

$$\forall p_1, q_1, \ldots, p_n, q_n \colon (\forall i \colon (p_i \le q_i) \to f(p_1,\ldots,p_n) \le f(q_1,\ldots,q_n))$$

$\Rightarrow$ ф-ция **немонот.** $\iff$:

$\exists p_1, q_1, \ldots, p_n, q_n (\forall i \colon (p_i \le q_i) \to g(p_1,\ldots,p_n) = 1 \land g(q_1,\ldots,q_n) = 0)$

Лемма 2.2. *g немонотонна* $\Rightarrow$

$$\exists i, \exists (a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)\colon$$

$$g(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) = 1 \wedge g(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n) = 0$$

Тогда $\neg p = g(a_1, \ldots, a_{i-1}, p, a_{i+1}, \ldots, a_n)$

Шаг 4 $\neg, h \notin D \mapsto 0, 1$

$$h \notin D \Rightarrow \exists (a_1, \ldots, a_n)$$

$$h(a_1, \ldots, a_n) = h(\neg a_1, \ldots, \neg a_n)$$

Пример.

$$\neg, \oplus \Rightarrow p \oplus \neg p = 1$$

$$\neg, \wedge \Rightarrow p \wedge \neg p = 0$$

Общий подход:

$$h(0, 1, 1, 0, 1, 0) = h(1, 0, 0, 1, 0, 1) = 1$$

$$\Rightarrow h(\neg p, p, p, \neg p, p, \neg p) = 1, p = \overline{0, 1}$$

Шаг 5

$$\neg, 0, 1, k \notin L$$

Б. О. О. в мн-не Жегалкина ф-ции k есть слагаемое с $x_1 x_2$

$$k(x_1, \ldots, x_n) = x_1 x_2 \cdot A(x_3, \ldots, x_n) \oplus x_1 \cdot B(x_3, \ldots, x_n) \oplus x_2 \cdot C(x_3, \ldots, x_n) + D(x_3, \ldots, x_n)$$

Мн-н A непустой $\Rightarrow \exists (a_3, \ldots, a_n)\colon A(a_3, \ldots, a_n) = 1$
Тогда $k(x_1, x_2, a_3, \ldots, a_n) = x_1 x_2 \oplus x_1 \cdot B \oplus x_2 \cdot C \oplus D$

Использование орицания позволяет менять 1

- $B = C = 0 \Rightarrow$ выразили x_1, x_2, т. е. $\wedge$. $\wedge, \neg \mapsto$ ВСЁ
- $B = C = 1 \Rightarrow x_1 \oplus x_2 \oplus x_1 x_2$, т. е. $\vee$. $\vee, \neg \mapsto$ ВСЁ
- $B = 0, C = 1 \Rightarrow 1 \oplus x_1 \oplus x_1 x_2$, т. е. $\rightarrow$. $\rightarrow, \neg \mapsto$ ВСЁ

$\square$