ДИСКРЕТНАЯ МАТЕМАТИКА

ИУ5 — 4 семестр, 2015 г.

Семинар 7. ТЕОРЕМА ПОСТА

Определение 7.1. Множество булевых функций F называют **полным**, если любая булева функция может быть представлена некоторой формулой над F .

Стандартный базис $\{\vee, \wedge, \bar{}\}$ является **полным множеством**, в силу теоремы о любой булевой функции **дизъюнктивной** или **конъюнктивной нормальной формой**.

Определение 7.2. Функцию f называют **функцией, сохраняющей константу 0** (соответственно **константу 1**), если $f(\tilde{0}) = 0$ (соответственно: $f(\tilde{1}) = 1$), где $\tilde{0}$ — нулевой, а $\tilde{1}$ — *единичный наборы значений переменных функции* f .

Наборы $\tilde{\alpha}$ и $\overline{\tilde{\alpha}}$ из булева куба $\mathbb{B}^n = \{0, 1\}^n$ будем называть **взаимно противоположными**, говоря при этом также, что набор $\overline{\tilde{\alpha}}$ есть **инверсия** (или **отрицание**) **набора** $\tilde{\alpha}$ (в силу единственности дополнения любого элемента булевой алгебры набор $\tilde{\alpha}$ будет, очевидно, инверсией набора $\overline{\tilde{\alpha}}$).

Определение 7.3. Функцию $g \in \mathcal{P}_{2,n}$ называют **двойственной к функции** $f \in \mathcal{P}_{2,n}$, если для всякого $\tilde{\alpha} \in \{0, 1\}^n$ ($n > 0$) имеет место $g(\tilde{\alpha}) = \overline{f}(\overline{\tilde{\alpha}})$.

Определение 7.4. Функцию $f \in \mathcal{P}_{2,n}$ называют **самодвойственной**, если она двойственна к себе самой, т.е. $(\forall \tilde{\alpha} \in \{0, 1\}^n)(f(\tilde{\alpha}) = \overline{f}(\overline{\tilde{\alpha}}))$

Функция самодвойственна тогда и только тогда, когда на взаимно противоположных наборах она принимает взаимно противоположные значения.

Определение 7.5. Функцию $f \in \mathcal{P}_{2,n}$ называют **монотонной**, если для любых наборов $\tilde{\alpha}$, $\tilde{\beta} \in \mathbb{B}^n$, таких, что $\tilde{\alpha} \leq \tilde{\beta}$, имеет место $f(\tilde{\alpha}) \leq f(\tilde{\beta})$.

базис Жегалкина $\{\oplus, \cdot, 1\}$ Любую формулу над базисом Жегалкина называют **полиномом Жегалкина**.

Полином Жегалкина от n переменных можно записать в виде

$$P(x_1, \ldots, x_n) = \sum_{\{i_1,\, i_2,\, \ldots,\, i_m\} \subseteq \{1,\, 2,\, \ldots,\, n\}} (\mathrm{mod}\ 2)\, a_{i_1 i_2 \ldots i_m} x_{i_1} x_{i_2} \ldots x_{i_m},$$

где коэффициенты полинома $a_{i_1 i_2 \ldots i_m} \in \{0, 1\}$ индексированы всеми возможными подмножествами множества $\{1,\ 2,\ \ldots,\ n\}$ (коэффициент a_0 соответствует пустому множеству).

Формула вида

$$\sum_{i=1}^{n} (\mathrm{mod}\ 2)\, a_i x_i \oplus a_0 \tag{7.1}$$

называется **полиномом Жегалкина первой степени** от переменных. В таком полиноме отсутствуют „нелинейные“ слагаемые.

Определение 7.6. Функцию $f \in \mathcal{P}_{2,n}$ называют **линейной**, если она может быть представлена полиномом Жегалкина первой степени от n переменных.

Определение Множества функций T_0, T_1, S, M, L называются **классами Поста**.

Теорема Поста (критерий Поста) Множество F булевых функций полно тогда и только тогда, когда оно не содержится целиком ни в одном из классов Поста.

Расчет булевой функции, заданной формулой

Таблица значений наиболее часто употребляемых булевых функций от двух переменных.

x_1	x_2	$x_1 \vee x_2$	$x_1 \cdot x_2$	$x_1 \oplus x_2$	$x_1 \to x_2$	$x_1 \sim x_2$	$x_1 \mid x_2$	$x_1 \downarrow x_2$
0	0	0	0	0	1	1	1	1
0	1	1	0	1	1	0	1	0
1	0	1	0	1	0	0	1	0
1	1	1	1	0	1	1	0	0

Рассмотрим булеву функцию от трех переменных, заданную формулой $f(x_1, x_2, x_3) = (((x_1 \downarrow x_2) \oplus ((x_1 \vee x_2) \sim x_3)) \vee (x_1 \mid x_3)) \mid (\overline{x_1} \wedge x_2)$.

Для расчета разобьем формулу на подформулы A, B, C, D, E, I и J и сведем результаты расчетов в таблицу.

№	x_1	x_2	x_3	A	B	C	D	E	I	J	f
				$x_1 \downarrow x_2$	$x_1 \vee x_2$	$B \sim x_3$	$A \oplus C$	$x_1 \mid x_3$	$\overline{x_1} \wedge x_2$	$D \vee E$	$J \mid I$
0	0	0	0	1	0	1	0	1	0	1	1
1	0	0	1	1	0	0	1	1	0	1	1
2	0	1	0	0	1	0	0	1	1	1	0
3	0	1	1	0	1	1	1	1	1	1	0
4	1	0	0	0	1	0	0	1	0	1	1
5	1	0	1	0	1	1	1	0	0	1	1
6	1	1	0	0	1	0	0	1	0	1	1
7	1	1	1	0	1	1	1	0	0	1	1

Разбиение исходной формулы на подформулы однозначно задается расстановкой скобок.

Пусть дано множество функций $F = \{g,\ w\}$, где $g = (11111101)$; $w = (11100110)$.

Исследовать элементы этого множества на принадлежность к классам Поста.

	x_1	x_2	x_3	g	w
0	0	0	0	1	1
1	0	0	1	1	1
2	0	1	0	1	1
3	0	1	1	1	0
4	1	0	0	1	0
5	1	0	1	1	1
6	1	1	0	0	1
7	1	1	1	1	0

1. Сохранение 0.

Функцию f называют функцией, **сохраняющей константу 0**, если $f(\tilde{0}) = 0$, где $\tilde{0}$ — нулевой набор значений переменных функции f.

	x_1	x_2	x_3	g	w
0	0	0	0	1	1
1	0	0	1	1	1
2	0	1	0	1	1
3	0	1	1	1	0
4	1	0	0	1	0
5	1	0	1	1	1
6	1	1	0	0	1
7	1	1	1	1	0

$g(0,0,0) = 1$. Функция g не сохраняет константу 0, $g \notin T_0$.

$w(0,0,0) = 1$. Функция w не сохраняет константу 0, $w \notin T_0$.

2. Сохранение 1 .

Функцию f называют функцией, **сохраняющей константу 1**, если $f(\tilde{1}) = 1$, где $\tilde{1}$ — единичный наборы значений переменных функции f .

	x_1	x_2	x_3	g	w
0	0	0	0	1	1
1	0	0	1	1	1
2	0	1	0	1	1
3	0	1	1	1	0
4	1	0	0	1	0
5	1	0	1	1	1
6	1	1	0	0	1
7	1	1	1	1	0

$g(1,1,1) = 1$.Функция g сохраняет константу 1 . $g \in T_1$

$w(1,1,1) = 0$. Функция w не сохраняет константу 1 . $w \notin T_1$.

3. Самодвойственность.

Функцию $f \in \mathcal{P}_{2,n}$ называют **самодвойственной**, если она двойственна к себе самой, т.е.

$(\forall \tilde{\alpha} \in \{0,\, 1\}^n)(f(\tilde{\alpha}) = \overline{f}(\overline{\tilde{\alpha}}))$

Функция самодвойственна тогда и только тогда, когда на взаимно противоположных наборах она принимает взаимно противоположные значения.

	x_1	x_2	x_3	g	w
0	0	0	0	1	1
1	0	0	1	1	1
2	0	1	0	1	1
3	0	1	1	1	0
4	1	0	0	1	0
5	1	0	1	1	1
6	1	1	0	0	1
7	1	1	1	1	0

Функции g и w не самодвойственны.

$g(0,0,0) = f(1,1,1) = 1\,.\ \ g \notin S$

$w(0,1,1) = w(1,0,0) = 0\,.\ \ w \notin S$

4. Монотонность.

Функцию $f \in \mathcal{P}_{2,n}$ называют **монотонной**, если для любых наборов $\tilde{\alpha}$, $\tilde{\beta} \in \mathbb{B}^n$, таких, что $\tilde{\alpha} \leq \tilde{\beta}$, имеет место $f(\tilde{\alpha}) \leq f(\tilde{\beta})$.

	x_1	x_2	x_3	g	w
0	0	0	0	1	1
1	0	0	1	1	1
2	0	1	0	1	1
3	0	1	1	1	0
4	1	0	0	1	0
5	1	0	1	1	1
6	1	1	0	0	1
7	1	1	1	1	0

Функции g и w не монотонны.

$g \notin M$, т.к. $(0,0,0) \leq (1,1,0)$, но $g(0,0,0) \geq g(1,1,0)$
$(g(0,0,0) = 1;\ g(1,1,0) = 0)$.

$w \notin M$, т.к. $(0,1,0) \leq (0,1,1)$, но $w(0,1,0) \geq w(0,1,1)$
$(w(0,1,0) = 1;\ w(0,1,1) = 0)$.

5. Линейность.
Формула вида

$$\sum_{i=1}^{n} (\mathrm{mod}\ 2)\, a_i x_i \oplus a_0 \tag{7.2}$$

называется **полиномом Жегалкина первой степени** от переменных. В таком полиноме отсутствуют „нелинейные“ слагаемые.
Функцию $f \in \mathcal{P}_{2,n}$ называют **линейной**, если она может быть представлена полиномом Жегалкина первой степени от n переменных.
Найдем полином Жегалкина, представляющий f.
f задана как функция от трех переменных, т.к. размерность вектора значений f равна $2^3 = 8$.
Функция f представляется некоторым полиномом Жегалкина третьей степени, общий вид которого дает формула

$$a_{123}x_1x_2x_3 \oplus a_{12}x_1x_2 \oplus a_{13}x_1x_3 \oplus a_{23}x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0$$

Значение функции g на наборе 000 равно коэффициенту a_0:
$g(0,0,0) = a_0 = 1$.

Найдем коэффициенты a_3, a_2 и a_1, рассмотрим значения функции на наборах 001, 010 и 100 соответственно ($a_0 = 1$).

$g(0,0,1) = a_3 \oplus a_0 = a_3 \oplus 1 = 1, \Rightarrow a_3 = 0;$

$g(0,1,0) = a_2 \oplus 1 = 1 \Rightarrow a_2 = 0;$

$g(1,0,0) = a_1 \oplus 1 = 1 \Rightarrow a_1 = 0;$

Чтобы найти коэффициенты a_{12}, a_{13} и a_{23}, рассмотрим значения функции на наборах 110, 101 и 011 соответственно.

Находим a_{12}.

$$g(1,1,0) = 0; g(1,1,0) = a_{12} \cdot 1 \cdot 1 \oplus a_1 \cdot 1 \oplus a_2 \cdot 1 \oplus a_0 = \{\text{т.к. } a_1 = a_2 = 0\} = a_{12} \oplus a_0 = a_{12} \oplus 1 = 0 \Rightarrow a_{12} = 1$$

Находим a_{13}. $g(1,0,1) = 1 \quad (a_1 = a_3 = 0)$

$g(1,0,1) = a_{13} \oplus a_0 = a_{13} \oplus 1 = 1 \Rightarrow a_{13} = 0;$

Находим a_{23}. $g(0,1,1) = 1 \quad (a_2 = a_3 = 0)$

$g(0,1,1) = a_{23} \oplus a_0 = a_{23} \oplus 1 = 1 \Rightarrow a_{23} = 0$

Находим a_{123}. $g(1,1,1) = 1 \quad (a_1 = a_2 = a_3 = a_{13} = a_{23} = 0)$

$g(1,1,1) = a_{123} \oplus a_{12} \oplus a_0 = a_{123} \oplus 1 \oplus 1 = 1 \Rightarrow a_{123} = 1.$

Полином Жегалкина, представляющий g есть:

$g = x_1x_2x_3 \oplus x_1x_2 \oplus 1.$

Функция g не линейна, w проверять не будем.

Заполненная критериальная таблица

Таблица 7.1

	T_0	T_1	S	M	L
g	$-$	$+$	$-$	$-$	$-$
w	$-$	$-$	$-$	$-$	$?$

Множество функций $F = \{g,\ w\}$ не содержится целиком ни в одном из классов Поста, следовательно система полна.

Можно реализовать константы 0, 1 и стандартный базис $\{\vee, \wedge, \bar{}\}$.

Реализация основных элементов.

Таблица 7.2

	T_0	T_1	S	M	L
g	$-$	$+$	$-$	$-$	$-$
w	$-$	$-$	$-$	$-$	?

Константа 1

$g \notin T_0$ и $g \in T_1$

Функция g сохраняет константу 1 и функция g не сохраняет константу 0, $g(0,0,0) = 1$ и $g(1,1,1) = 1$. Следовательно, $g(x,x,x) = 1$.

Отрицание.

$w \notin T_0$ и $w \notin T_1$.

Функция w не сохраняет константу 0 и не сохраняет константу 1. $w(0,0,0) = 1$ и $w(1,1,1) = 0$. Следовательно, $w(x,x,x) = \overline{x}$.

Константа 0

$0 = \overline{1}$. $w(1,1,1) = 0$ т.е. $w(g(x,x,x), g(x,x,x), g(x,x,x)) = 0$.

Реализация конъюнкции из нелинейной функции g**.**

$g = x_1x_2x_3 \oplus x_1x_2 \oplus 1$. Положим $x_3 = 0$, получим $\varphi(x_1,x_2) = x_1x_2 \oplus 1 = \overline{x_1x_2}$, т.к. $x \oplus 1 = \overline{x}$. Пусть $x_1 = x$, $x_2 = y$, тогда $\psi(x,y) = \overline{\varphi(x,y)} = xy$. Следовательно, $x \cdot y = \overline{g(x,y,0)}$.

В итоге имеем представление конъюнкции следующей формулой:

$$x \cdot y = w(\ g(x,y,w(g(x,x,x),g(x,x,x),g(x,x,x))),\ g(x,y,w(g(x,x,x),g(x,x,x),g(x,x,x))),\ g(x,y,w(g(x,x,x),g(x,x,x),g(x,x,x)))\ )$$

Практическая реализация конъюнкции из нелинейной функции f от 2-х переменных.

Функцию от 2-х переменных всегда можно получить из функции от большего числа переменных положив какие-то переменные равными 0 или 1. Например, пусть $f_1 = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus 1$. Положим $x_1 = 0$, получим $\varphi(x_2, x_3) = x_2x_3 \oplus 1$.

Или пусть $f_2 = x_1x_2x_3 \oplus 1$. Положим $x_1 = 1$, получим $\varphi(x_2, x_3) = x_2x_3 \oplus 1$, положить $x_1 = 0$ мы не можем, т.к. "потеряем" единственную конъюнкцию $x_1x_2x_3$

Возможны следующие варианты вида функции от 2-х переменных :

1. $f(x,y) = xy \oplus 1 = \overline{xy}$. Следовательно, $x \cdot y = \overline{f(x,y)}$.

2. $f(x,y) = xy \oplus x \oplus 1 = x(y \oplus 1) \oplus 1 = x\overline{y} \oplus 1 = \overline{x\overline{y}};\ x \cdot y = \overline{f(x,\overline{y})}$.

2.a. $f(x,y) = xy \oplus x = x(y \oplus 1) = x\overline{y};\ x \cdot y = f(x,\overline{y})$.

3. $f(x,y) = xy \oplus x \oplus y \oplus 1 = x(y \oplus 1) \oplus (y \oplus 1) = (x \oplus 1)(y \oplus 1) = \overline{x} \cdot \overline{y};\ x \cdot y = f(\overline{x},\overline{y})$.

3.a. $f(x,y) = xy \oplus x \oplus y = xy \oplus x \oplus y \oplus 1 \oplus 1 = [\text{т.к.} 1 \oplus 1 = 0] = x(y \oplus 1) \oplus (y \oplus 1) \oplus 1 = (x \oplus 1)(y \oplus 1) \oplus 1 = \overline{x} \cdot \overline{y} \oplus 1 = \overline{\overline{x} \cdot \overline{y}};\ x \cdot y = \overline{f(\overline{x},\overline{y})}$.