Лекция 7. ЛКНФ и мультиаффинные функции. Критерий мультиаффинности функции. Полиномиальность проверки выполнимости ЛКНФ. Полиномиальность проверки представимости функции в виде ЛКНФ. Функции, сохраняющие константу.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Линейная форма

Линейной формой (ЛФ) называется выражение вида

$$c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n,$$

где $c_0, c_1, \ldots, c_n \in E_2$.

Например, $x_1 \oplus 1$, $x_1 \oplus x_3$, 1 — линейные формы.

Линейная КНФ

Линейной КНФ (ЛКНФ) называется конъюнкция линейных форм.

Например, $(x_1 \oplus x_2 \oplus 1)(x_1 \oplus x_3)$ — ЛКНФ.

Мультиаффинная функция

Функция алгебры логики называется **мультиаффинной**, если ее можно представить ЛКНФ.

Множество всех мультиаффинных функций алгебры логики обозначим MA.

Например, $(x_1 \oplus x_2 \oplus 1)(x_1 \oplus x_3) \in MA$.

Отметим, что каждая линейная функция является мультиаффинной.

Приведенное представление функции из MA

Любую ЛКНФ функции $g \in MA$ назовем **приведенным представлением** этой мультиаффинной функции g.

Например, $(x_1 \oplus x_2 \oplus 1)(x_1 \oplus x_3)$ — приведенное представление функции из MA.

Приведенное представление функции из *MA*

Приведенное представление мультиаффинной функции g **не обязательно** однозначно.

Например,

$$K_1 = (x_1 \oplus x_2)(x_3 \oplus 1)(x_1 \oplus x_2 \oplus x_3)$$

и

$$K_2 = (x_1 \oplus x_2)(x_3 \oplus 1)$$

два различных приведенных представления функции $g \in MA$, где $\alpha_g = (0010\ 1000)$.

Критерий мультиаффинности функции

Теорема 1. *Функция $g \in P_2$ является мультаффинной тогда и только тогда, когда $N_1(g)$ является множеством решений некоторой системы линейных уравнений над полем вычетов по модулю два.*

Критерий мультиаффинности функции

Доказательство.

Необходимость. Пусть $g(x_1, \ldots, x_n) \in MA$, и $\prod_{j=1}^{m} L_j$ — ее приведенное представление, где $L_1, \ldots, L_m$ — ЛФ. Тогда $N_1(g)$ совпадает с множеством решений системы линейных уравнений:

$$\begin{cases} L_1(x_1, \ldots, x_n) = 1, \\ \ldots, \\ L_m(x_1, \ldots, x_n) = 1. \end{cases}$$

Критерий мультиаффинности функции

Доказательство.
Достаточность. Пусть для функции $g(x_1, \ldots, x_n) \in P_2$ выполнено, что $N_1(g)$ является множеством решений системы линейных уравнений:

$$\begin{cases} a_{1,1}x_1 \oplus \ldots \oplus a_{1,n}x_n = b_1, \\ \ldots, \\ a_{m,1}x_1 \oplus \ldots \oplus a_{m,n}x_n = b_m, \end{cases}$$

где $a_{1,1}, \ldots, a_{m,n}, b_1, \ldots, b_m \in E_2$, $m \geqslant 1$. Тогда функцию g можно представить в виде $\prod_{j=1}^{m} L_j$, где L_j — ЛФ,

$$L_j = a_{j,1}x_1 \oplus \ldots \oplus a_{j,n}x_n \oplus b_m \oplus 1,$$

$j = 1, \ldots, m$. Значит, $g \in MA$.

□

Критерий мультиаффинности функции

Теорема 2. *Функция $g \in P_2$ является мультиаффинной тогда и только тогда, когда для любых $\alpha, \beta, \gamma \in N_1(g)$ выполняется $\alpha \oplus \beta \oplus \gamma \in N_1(g)$.*

Критерий мультиаффинности функции

Доказательство. *Необходимость*.
Пусть $g(x_1, \ldots, x_n) \in MA$. Тогда по теореме 1 $N_1(g)$ является множеством решений некоторой системы линейных уравнений над полем вычетов по модулю два.

Множество решений любой системы линейных уравнений является линейным аффинным многообразием.

Значит,

$$N_1(g) = \{\delta_0 \oplus \delta \mid \delta \in H\},$$

где $\delta_0 \in N_1(g)$, H — подпространство линейного пространства E_2^n над полем вычетов по модулю два.

Критерий мультиаффинности функции

Теперь если $\alpha, \beta, \gamma \in N_1(g)$, то

$$\begin{aligned} \alpha &= \delta_0 \oplus \delta_1, \\ \beta &= \delta_0 \oplus \delta_2, \\ \gamma &= \delta_0 \oplus \delta_3 \end{aligned}$$

для некоторых $\delta_1, \delta_2, \delta_3 \in H$. Поэтому

$$\alpha \oplus \beta \oplus \gamma = (\delta_0 \oplus \delta_1) \oplus (\delta_0 \oplus \delta_2) \oplus (\delta_0 \oplus \delta_3) = \delta_0 \oplus \delta,$$

где $\delta = \delta_1 \oplus \delta_2 \oplus \delta_3 \in H$.

Поэтому $\alpha \oplus \beta \oplus \gamma \in N_1(g)$.

Критерий мультиаффинности функции

Достаточность. Пусть для функции $g(x_1, \ldots, x_n) \in P_2$ выполнено, что для любых $\alpha, \beta, \gamma \in N_1(g)$ верно $\alpha \oplus \beta \oplus \gamma \in N_1(g)$.

Пусть $\delta_0 \in N_1(g)$ и

$$H = \{\delta_0 \oplus \delta \mid \delta \in N_1(g)\}.$$

Критерий мультиаффинности функции

Покажем, что H является подпространством линейного пространства E_2^n над полем вычетов по модулю два.

Если $\delta_1, \delta_2 \in H$, то

$$\begin{aligned} \delta_1 &= \delta_0 \oplus \alpha, \\ \delta_2 &= \delta_0 \oplus \beta \end{aligned}$$

для некоторых $\alpha, \beta \in N_1(g)$. Поэтому

$$\delta_1 \oplus \delta_2 = (\delta_0 \oplus \alpha) \oplus (\delta_0 \oplus \beta) = \delta_0 \oplus \delta,$$

где $\delta = \delta_0 \oplus \alpha \oplus \beta \in N_1(g)$.

Критерий мультиаффинности функции

Итак, H — линейное подпространство E_2^n. Если $\delta_1, \ldots, \delta_t$ — какой-то базис линейного пространства H, $t \geqslant 1$, то множество решений однородной системы линейных уравнений

$$\begin{cases} \delta_{1,1}x_1 \oplus \ldots \oplus \delta_{1,n}x_n = 0, \\ \ldots, \\ \delta_{t,1}x_1 \oplus \ldots \oplus \delta_{t,n}x_n = 0, \end{cases}$$

является ортогональным к H подпространством $H^{\perp}$.

Критерий мультиаффинности функции

Если $\gamma_1, \ldots, \gamma_m$ — какой-то базис линейного пространства $H^{\perp}$, $m \geqslant 1$, то множество решений однородной системы линейных уравнений

$$\begin{cases} \gamma_{1,1}x_1 \oplus \ldots \oplus \gamma_{1,n}x_n = 0, \\ \ldots, \\ \gamma_{m,1}x_1 \oplus \ldots \oplus \gamma_{m,n}x_n = 0, \end{cases}$$

является пространством H.

Критерий мультиаффинности функции

А значит, множество решений неоднородной системы линейных уравнений

$$\begin{cases} \gamma_{1,1}x_1 \oplus \ldots \oplus \gamma_{1,n} = \gamma_{1,1}\delta_{0,1} \oplus \ldots \oplus \gamma_{1,n}\delta_{0,n}, \\ \ldots, \\ \gamma_{m,1}x_1 \oplus \ldots \oplus \gamma_{m,n} = \gamma_{m,1}\delta_{0,1} \oplus \ldots \oplus \gamma_{m,n}\delta_{0,n}, \end{cases}$$

является линейным аффинным многообразием $N_1(g) = \delta_0 \oplus H$.

По теореме 1 это означает, что $g \in MA$.

□

Проверка мультиаффинности функции

Пример. Применим критерий из теоремы 2 к функции $g \in P_2$, где $\alpha_g = (0010\ 1000)$.

Получаем:

$$N_1(g) = \{\alpha_1 = (0,1,0), \alpha_2 = (1,0,0)\}.$$

Проверяем:

$$\alpha_1 \oplus \alpha_2 \oplus \alpha_1 = (1,0,0),$$
$$\alpha_1 \oplus \alpha_2 \oplus \alpha_2 = (0,1,0).$$

Значит, $g \in MA$.

Поиск приведенного представления

Пример (продолжение). По доказательству теоремы 2 и по теореме 1 найдем приведенное представление мультиаффинной функции $g \in P_2$, где $\alpha_g = (0010\ 1000)$.

Получаем:

$$N_1(g) = \{\alpha_1 = (0,1,0), \alpha_2 = (1,0,0)\}.$$

Значит,

$$N_1(g) = \delta_0 \oplus H,$$

где $\delta_0 = (0,1,0)$,

$$H = \{(0,0,0), (1,1,0)\},$$

H — подпространство E_2^n и $\delta_1 = (1,1,0)$ — его базис.

Поиск приведенного представления

Итак, $\delta_1 = (1, 1, 0)$ — базис H.

Находим подпространство $H^\perp$:

$$x_1 \oplus x_2 = 0.$$

Значит,

$$H^\perp = \{(0, 0, 0), (0, 0, 1), (1, 1, 0), (1, 1, 1)\},$$

и $\gamma_1 = (0, 0, 1)$, $\gamma_2 = (1, 1, 0)$ — его базис.

Поиск приведенного представления

Итак, $\gamma_1 = (0,0,1)$, $\gamma_2 = (1,1,0)$ — базис $H^{\perp}$ и $\delta_0 = (0,1,0)$.

Определяем $N_1(g)$:

$$\begin{cases} x_3 = 0, \\ x_1 \oplus x_2 = 1. \end{cases}$$

Значит,

$$g(x_1, x_2, x_3) = (x_3 \oplus 1)(x_1 \oplus x_2).$$

Проверка мультиаффинности функции

Пример. Применим критерий из теоремы 2 к функции $g \in P_2$, где $\alpha_g = (0000\ 0000\ 0110\ 1001)$.

Получаем:

$$\begin{aligned} N_1(g) &= \{\alpha_1 = (1,0,0,1), \alpha_2 = (1,0,1,0), \\ &\quad \alpha_3 = (1,1,0,0), \alpha_4 = (1,1,1,1)\}. \end{aligned}$$

Проверяем:

$$\begin{aligned} \alpha_1 \oplus \alpha_2 \oplus \alpha_3 &= (1,1,1,1), \\ \alpha_1 \oplus \alpha_2 \oplus \alpha_4 &= (1,1,0,0), \\ \alpha_1 \oplus \alpha_3 \oplus \alpha_4 &= (1,0,1,0), \\ \alpha_2 \oplus \alpha_3 \oplus \alpha_4 &= (1,0,0,1). \end{aligned}$$

Значит, $g \in MA$.

Проверка мультиаффинности функции

Пример. Применим критерий из теоремы 2 к функции $g \in P_2$, где $\alpha_g = (0111\ 1000)$.

Получаем:

$$N_1(g) = \{\alpha_1 = (0,0,1), \alpha_2 = (0,1,0), \alpha_3 = (0,1,1), \alpha_4 = (1,0,0)\}.$$

Проверяем:

$$\alpha_1 \oplus \alpha_2 \oplus \alpha_3 = (0,0,0) \notin N_1(g).$$

Значит, $g \notin MA$.

Проверка выполнимости ЛКНФ

Опишем алгоритм проверки выполнимости ЛКНФ.

Проверка выполнимости ЛКНФ

Алгоритм 9. *Проверка выполнимости ЛКНФ*.

Вход: ЛКНФ $K = L_1 \cdot \ldots \cdot L_m$, где L_j — ЛФ, $j = 1, \ldots, m$, функции $g \in MA \cap P_2^{(n)}$.

Выход: «да» и такой набор $\alpha \in E_2^n$, что $g(\alpha) = 1$, если $g \neq 0$, и «нет», если $g = 0$.

Проверка выполнимости ЛКНФ

Алгоритм 9.

1. Составляем систему линейных уравнений над полем вычетов по модулю два:

$$\begin{cases} L_1(x_1, \ldots, x_n) = 1, \\ \ldots, \\ L_m(x_1, \ldots, x_n) = 1, \end{cases}$$

и решаем ее.

2. Если система совместна, то ответ «да» и α — одно из ее решений, если эта система не совместна, то ответ «нет».

Правильность и сложность алгоритма

Правильность алгоритма 9 следует из теоремы 1.

Если систему линейных уравнений решать полиномиальным алгоритмом, например, методом исключения неизвестных, то алгоритм 9 является полиномиальным.

Проверка выполнимости ЛКНФ

Пример. Проверим по алгоритму 9, является ли ЛКНФ

$$K = (x_1 \oplus x_2)(x_1 \oplus x_3)(x_2 \oplus x_3)$$

выполнимой.

Получаем:

$$\begin{cases} x_1 \oplus x_2 = 1, \\ x_1 \oplus x_3 = 1, \\ x_2 \oplus x_3 = 1. \end{cases}$$

Проверка выполнимости ЛКНФ

Итак,

$$\begin{cases} x_1 \oplus x_2 = 1, \\ x_1 \oplus x_3 = 1, \\ x_2 \oplus x_3 = 1. \end{cases}$$

Сложим второе и третье уравнения:

$$\begin{cases} x_1 \oplus x_2 = 1, \\ x_1 \oplus x_3 = 1, \\ x_1 \oplus x_2 = 0. \end{cases}$$

Система несовместна, значит ответ **«нет»**.

Проверка выполнимости ЛКНФ

Пример. Проверим по алгоритму 9, является ли ЛКНФ

$$K = (x_1 \oplus x_2)(x_1 \oplus x_4)(x_2 \oplus x_3)(x_3 \oplus x_4)$$

выполнимой.

Получаем:

$$\begin{cases} x_1 \oplus x_2 = 1, \\ x_1 \oplus x_4 = 1, \\ x_2 \oplus x_3 = 1, \\ x_3 \oplus x_4 = 1. \end{cases}$$

Проверка выполнимости ЛКНФ

Итак,

$$\begin{cases} x_1 \oplus x_2 = 1, \\ x_1 \oplus x_4 = 1, \\ x_2 \oplus x_3 = 1, \\ x_3 \oplus x_4 = 1. \end{cases}$$

Находим:

$$\begin{cases} x_2 = x_1 \oplus 1, \\ x_3 = x_1, \\ x_4 = x_1 \oplus 1. \end{cases}$$

Система совместна, значит ответ **«да»**, и $\alpha = (0, 1, 0, 1)$ — одно из ее решений.

Проверка представимости в виде ЛКНФ

А можно ли по полиному Жегалкина функции $f \in P_2$ быстро проверить, задается ли функция f в виде ЛКНФ?

Линейные соимплиценты

ЛФ L называется **линейной соимплицентой** функции $f \in P_2$, если верно равенство:

$$L \cdot f = 0.$$

Множество всех линейных соимплицент функции $f \in P_2$ является линейным пространством $L(f)$ над полем вычетов по модулю два.

По полиному Жегалкина функции f базис пространства $L(f)$ можно найти полиномиальным алгоритмом.

Кратчайшая ЛКНФ

Если функцию f можно задать ЛКНФ и $L_1, \ldots, L_m$ — базис пространства $L(f)$, то ЛКНФ

$$L_f = (L_1 \oplus 1) \cdot \ldots \cdot (L_m \oplus 1)$$

является **кратчайшей** ЛКНФ функции f.

Но можно ли быстро проверить равенство:

$$f = (L_1 \oplus 1) \cdot \ldots \cdot (L_m \oplus 1)?$$

Производная функции

Производной функции $f(x_1, \ldots, x_n) \in P_2$ **по переменной** x_1 называется функция

$$f'_{x_1}(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n) \oplus f(1, x_2, \ldots, x_n).$$

Аналогично вводится производная функции f по любой переменной x_i.

Производная функции

Утверждение 1. *Если* $f(x_1, \ldots, x_n) \in P_2$ *и*

$$f(x_1, \ldots, x_n) = x_1 \cdot g(x_2, \ldots, x_n) \oplus h(x_2, \ldots, x_n),$$

то

$$\begin{aligned} g(x_2, \ldots, x_n) &= f'_{x_1}(x_2, \ldots, x_n), \\ h(x_2, \ldots, x_n) &= f_0(x_2, \ldots, x_n). \end{aligned}$$

Доказательство. Действительно,

$$\begin{aligned} f'_{x_1} &= h \oplus (g \oplus h) = g, \\ f_0 &= h. \end{aligned}$$

□

Производная функции

Следствие. *Если* $f(x_1, \ldots, x_n) \in P_2$, *то*

$$f(x_1, \ldots, x_n) = x_1 \cdot f'_{x_1}(x_2, \ldots, x_n) \oplus f_0(x_2, \ldots, x_n).$$

Производная функции

Пример. Пусть функция $f \in P_2$ задана полиномом Жегалкина:

$$P_f = x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus 1.$$

Тогда

$$f = x_1 \cdot (x_2x_3 \oplus x_3) \oplus x_2x_3 \oplus x_2 \oplus 1.$$

Значит,

$$f'_{x_1} = x_2x_3 \oplus x_3.$$

Свойства линейных соимплицент

Теорема 3. *Пусть* $f(x_1, \ldots, x_n) \in P_2$ *и* L *— линейная соимплицента функции* f*, причем* $L = x_1 \oplus L_0(x_2, \ldots, x_n)$ *для некоторой ЛФ* L_0*. Тогда верно равенство:*

$$f(L_0(x_2, \ldots, x_n), x_2, \ldots, x_n) = f'_{x_1}(x_2, \ldots, x_n).$$

Свойства линейных соимплицент

Доказательство. Для функции f верно представление:

$$f = x_1 f'_{x_1} \oplus f_0.$$

Т. к. L — линейная соимплицента функции f, верно равенство:

$$L \cdot f = (x_1 \oplus L_0) \cdot f = 0.$$

Поэтому

$$(x_1 \oplus L_0) \cdot (x_1 f'_{x_1} \oplus f_0) = 0,$$

откуда

$$x_1(L_0 \cdot f'_{x_1} \oplus f'_{x_1} \oplus f_0) \oplus L_0 \cdot f_0 = 0$$

и

$$L_0 \cdot f'_{x_1} \oplus f'_{x_1} \oplus f_0 = 0.$$

Свойства линейных соимплицент

Доказательство. Итак,

$$f = x_1 f'_{x_1} \oplus f_0$$

и

$$L_0 \cdot f'_{x_1} \oplus f'_{x_1} \oplus f_0 = 0.$$

Значит,

$$f(L_0, x_2, \ldots, x_n) = L_0 \cdot f'_{x_1} \oplus f_0 = (f'_{x_1} \oplus f_0) \oplus f_0 = f'_{x_1}.$$

□

Линейные имплиценты

ЛФ L называется **линейной имплицентой** функции $f \in P_2^{(n)}$, если для любого набора $\alpha \in E_2^n$ из $L(\alpha) = 0$ следует $f(\alpha) = 0$.

Проверка представимости в виде ЛКНФ

Алгоритм 10. *Проверка представимости в виде ЛКНФ функции $f \in P_2$ по ее полиному Жегалкина P_f.*

Вход: полином Жегалкина P_f и какие-то линейные имплиценты $L_1, \ldots, L_m$ функции $f \in P_2$, $f \neq 0$.

Выход: «да», если $f = L_1 \cdot \ldots \cdot L_m$, и «нет» иначе.

Проверка представимости в виде ЛКНФ

Алгоритм 10.

1. $P_0 := P_f$, $K_0 := L_1 \cdot \ldots \cdot L_m$.

2.j, $j = 1, \ldots, m$.

1) Если в ЛКНФ K_0 найдется ЛФ L, не равная константе 1, переменная x_i содержится в ЛФ L и $L = x_i \oplus L_0$ (где L_0 не содержит x_i), то выполнить:

1а) получить полином Жегалкина P_0, заменив P_0 на $(P_0)'_{x_i}$;

1б) получить ЛКНФ K_0, заменив в K_0 все вхождения x_i на $L_0 \oplus 1$ и выполнив упрощения.

2) Если $j < m$, то перейти на 2.(j+1), иначе перейти на 3.

3. Если $P_0 = 1$, то ответ «да», иначе — ответ «нет».

Проверка представимости в виде ЛКНФ

Пример. Применим алгоритм 10 к функции $f(x_1, x_2, x_3)$ и ее линейным имплицентам L_1, L_2, где

$$\begin{aligned} P_f &= x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1, \\ L_1 &= x_1 \oplus x_2, \\ L_2 &= x_1 \oplus x_3. \end{aligned}$$

Проверка представимости в виде ЛКНФ

1.

$$\begin{aligned} P_0 &= x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1, \\ K_0 &= (x_1 \oplus x_2)(x_1 \oplus x_3). \end{aligned}$$

2.1. $L = x_1 \oplus x_2$, $x_i = x_1$, $L_0 = x_2$. Получаем:

$$\begin{aligned} P_0 &= x_2 \oplus x_3 \oplus 1, \\ K_0 &= ((x_2 \oplus 1) \oplus x_2)((x_2 \oplus 1) \oplus x_3)(x_2 \oplus x_3 \oplus 1) = x_2 \oplus x_3 \oplus 1. \end{aligned}$$

2.2. $L = x_2 \oplus x_3 \oplus 1$, $x_i = x_3$, $L_0 = x_2 \oplus 1$. Получаем:

$$\begin{aligned} P_0 &= 1, \\ K_0 &= x_2 \oplus x_2 \oplus 1 = 1. \end{aligned}$$

3. $P_0 = 1$, поэтому ответ «да».

Правильность алгоритма

Теорема 4. *Алгоритм 10 работает правильно, т. е. он выдает «да», если* $f = L_1 \cdot \ldots \cdot L_m$, *и «нет» иначе.*

Доказательство. Докажем утверждение теоремы индукцией по числу n существенных переменных функции f.

Базис индукции $n = 0$ верен.

Индуктивный переход. Пусть для всех функций, существенно зависящих не более, чем от $(n-1)$ переменной, алгоритм работает правильно.

Пусть на вход алгоритма подается полином Жегалкина P_f функции $f \in P_2$, существенно зависящей от n переменных, $n \geqslant 1$, и какие-то ее линейные имплиценты $L_1, \ldots, L_m$.

Правильность алгоритма

Итак, $P_0 := P_f$, $K_0 := L_1 \cdot \ldots \cdot L_m$.

1. Если в ЛКНФ K_0 **не найдется ЛФ**, не равная константе 1, то алгоритм выдает «нет», что верно.

Правильность алгоритма

Итак, $P_0 := P_f$, $K_0 := L_1 \cdot \ldots \cdot L_m$.

2. Пусть в ЛКНФ K_0 **найдется** ЛФ $L = x_i \oplus L_0$, где ЛФ L_0 не содержит переменную x_i.

Тогда равенство $f = L_1 \cdot \ldots \cdot L_m$ верно тогда и только тогда, когда оно верно при $L = x_i \oplus L_0 = 0$ и $L = x_i \oplus L_0 = 1$.

Если $L = 0$, то равенство верно, т. к. L — линейная имплицента функции f.

Правильность алгоритма

Если же $L = 1$, то в силу того, что $L \oplus 1 = x_i \oplus L_0 \oplus 1$ — линейная соимплицента функции f, применяем теорему 3.

Далее по индуктивному предположению для функции f'_{x_i}, существенно зависящей не более, чем от $(n-1)$ переменной, алгоритм работает правильно.

□

Полиномиальность алгоритма

Отметим, что алгоритм 10 является полиномиальным относительно $N = n \cdot (l + m)$, где n — число переменных функции, а l — длина ее полинома Жегалкина.

Проверка мультиаффинности функции по полиному

Теорема 5. *По полиному Жегалкина P_f функции $f \in P_2$ с полиномиальной сложностью можно проверить, верно ли $f \in MA$, и при положительном ответа найти кратчайшую ЛКНФ L_f функции f.*

Доказательство. Действительно, можно применить алгоритмы 4 и 10.

Полиномиальность S-ВЫП при $S \subseteq MA$

Теорема 6. *Пусть $S \subseteq P_2$ и S — конечно.*

Если $S \subseteq MA$, то S-ВЫП $\in P$.

Сохранение единицы

Функция алгебры логики f **сохраняет константу** 1, если $f(1,\ldots,1) = 1$.

Множество всех функций алгебры логики, сохраняющих 1, обозначим T_1.

Например, $x_1x_2 \oplus x_1 \oplus x_3 \in T_1$.

Критерий сохранения константы 1

Теорема 7. *Функция* $g \in P_2$ *сохраняет* 1 *тогда и только тогда, когда* $(1, \ldots, 1) \in N_1(g)$.

Несохранение нуля

Функция алгебры логики f **не сохраняет константу** 0, если $f(0,\ldots,0) = 1$.

Множество всех функций алгебры логики, не сохраняющих 0, обозначим T_0'.

Например, $x_1x_2x_3 \oplus x_1 \oplus 1 \in T_0'$.

Критерий несохранения константы 0

Теорема 8. *Функция* $g \in P_2$ *не сохраняет* 0 *тогда и только тогда, когда* $(0, \ldots, 0) \in N_1(g)$.

Полиномиальность S-ВЫП при $S \subseteq T_1$ или $S \subseteq T_0'$

Теорема 9. *Пусть $S \subseteq P_2$ и S — конечно.*

1. *Если $S \setminus \{0\} \subseteq T_1$, то S-ВЫП $\in P$.*
2. *Если $S \setminus \{0\} \subseteq T_0'$, то S-ВЫП $\in P$.*

Конец лекции