Теоретическая информатика - 1

Булевы функции

Определение

Булевой функцией называется функция вида

$$f : \{0,1\}^n \to \{0,1\}.$$

(Иначе говоря, булева функция сопоставляет каждому кортежу длины n из 0 и 1 одно из двух значений, 0 или 1.)

Интерпретация в логике: 0 — ложь, 1 — истина.

Основные функции:

- Конъюнкция (логическое "и") $x \wedge y$ (также обозн. $x\&y$, xy):

  $x \wedge y = 1 \Leftrightarrow$ оба $x = 1$ и $y = 1$
- Дизъюнкция (логическое "или") $x \vee y$:

  $x \vee y = 1 \Leftrightarrow$ хотя бы один из аргументов $= 1$ ($x = 1$ или $y = 1$)
- Импликация (логическое "следует") $x \to y$:

  $x \to y = 1 \Leftrightarrow$ верно хотя бы одно из $x = 0$ или $y = 1$
- Симметрическая разность (сумма по модулю 2) $x \oplus y$:

  $x \oplus y = 1 \Leftrightarrow x \neq y$
- Отрицание $\neg x$ (также обозн. $\overline{x}$): $\neg x = 1 \Leftrightarrow x = 0$

Представление булевых функций

Сколько всего булевых функций от n переменных?

Представление булевых функций

Сколько всего булевых функций от n переменных? 2^{2^n}

Представление булевых функций

Сколько всего булевых функций от n переменных? 2^{2^n}

Булеву функцию можно задать *таблицей истинности*:

x	$\neg x$
0	1
1	0

x	y	$x \wedge y$	$x \vee y$	$x \to y$	$x \oplus y$
0	0	0	0	1	0
0	1	0	1	1	1
1	0	0	1	0	1
1	1	1	1	1	0

Представление булевых функций

Сколько всего булевых функций от n переменных? 2^{2^n}

Булеву функцию можно задать *таблицей истинности*:

x	$\neg x$
0	1
1	0

x	y	$x \wedge y$	$x \vee y$	$x \to y$	$x \oplus y$
0	0	0	0	1	0
0	1	0	1	1	1
1	0	0	1	0	1
1	1	1	1	1	0

Или же *вектором истинности*:

- упорядочим все 2^n кортежей в лексикографическом порядке
- i-я компонента вектора истинности равна значению функции на i-м кортеже
- какой номер у кортежа $(\sigma_1, \ldots, \sigma_n)$?

Представление булевых функций

Сколько всего булевых функций от n переменных? 2^{2^n}

Булеву функцию можно задать *таблицей истинности*:

x	$\neg x$
0	1
1	0

x	y	$x \wedge y$	$x \vee y$	$x \to y$	$x \oplus y$
0	0	0	0	1	0
0	1	0	1	1	1
1	0	0	1	0	1
1	1	1	1	1	0

Или же *вектором истинности*:

- упорядочим все 2^n кортежей в лексикографическом порядке
- i-я компонента вектора истинности равна значению функции на i-м кортеже
- какой номер у кортежа $(\sigma_1, \ldots, \sigma_n)$?

$$\Sigma_{i=1}^{n} \sigma_i 2^{n-i}$$

Например, $x \wedge y = (0001)$.

Основные эквивалентности

Следующие функции тождественно равны (т.е. совпадают на любом значении):

1. $\neg\neg x \equiv x$
2. $x \to y \equiv \neg x \vee y$
3. $x \to y \equiv \neg y \to \neg x$
4. $x \vee y \equiv y \vee x$ коммутативность
5. $x \wedge y \equiv y \wedge x$
6. $(x \vee y) \vee z \equiv x \vee (y \vee z)$ ассоциативность
7. $(x \wedge y) \wedge z \equiv x \wedge (y \wedge z)$
8. $x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z)$ дистрибутивность
9. $x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z)$
10. $\neg(x \vee y) \equiv \neg x \wedge \neg y$ закон Моргана
11. $\neg(x \wedge y) \equiv \neg x \vee \neg y$

Формулы

Базис $\mathcal{F}$ — некоторое подмножество булевых функций

Определение

Формула над базисом $\mathcal{F}$ определяется по индукции.

- База: всякая функция $f \in \mathcal{F}$ является формулой над $\mathcal{F}$;
- Индуктивный переход: Если $f(x_1, \ldots, x_n)$ — формула над базисом $\mathcal{F}$, а $\Phi_1, \ldots, \Phi_n$ — либо формулы над $\mathcal{F}$, либо переменные, то тогда $f(\Phi_1, \ldots, \Phi_n)$ — формула над базисом $\mathcal{F}$.

Пример

$(x \vee y) \wedge (z \vee x)$ — формула над базисом $\{\vee, \wedge\}$

ДНФ

Обозначение для переменной x или ее отрицания $\neg x$:

$$x^\sigma = \begin{cases} x, & \text{если } \sigma = 1, \\ \neg x, & \text{если } \sigma = 0. \end{cases}$$

Простой конъюнкцией называется конъюнкция одной или нескольких переменных или их отрицаний, причем каждая переменная встречается не более одного раза.

Дизъюнктивная нормальная форма (ДНФ) — представление БФ в виде дизъюнкции простых конъюнкций.

Пример: $(x \wedge \neg y) \vee z$

Если в каждой конъюнкции участвуют все переменные, это совершенная ДНФ (СДНФ).

Построение СДНФ по таблице истинности

- В таблице истинности отмечаем все наборы переменных, на которых функция равна 1.

Построение СДНФ по таблице истинности

- В таблице истинности отмечаем все наборы переменных, на которых функция равна 1.
- Для каждого такого набора $(\sigma_1, \ldots, \sigma_n)$ берем конъюнкцию $(x_1^{\sigma_1} \wedge \cdots \wedge x_n^{\sigma_n})$

Построение СДНФ по таблице истинности

- В таблице истинности отмечаем все наборы переменных, на которых функция равна 1.
- Для каждого такого набора $(\sigma_1, \ldots, \sigma_n)$ берем конъюнкцию $(x_1^{\sigma_1} \wedge \cdots \wedge x_n^{\sigma_n})$
- Включаем в СДНФ все полученные конъюнкции:

$$f(x_1, \ldots, x_n) = \bigvee_{f(\sigma_1, \ldots, \sigma_n) = 1} (x_1^{\sigma_1} \wedge \cdots \wedge x_n^{\sigma_n})$$

Построение СДНФ по таблице истинности

- В таблице истинности отмечаем все наборы переменных, на которых функция равна 1.
- Для каждого такого набора $(\sigma_1, \ldots, \sigma_n)$ берем конъюнкцию $(x_1^{\sigma_1} \wedge \cdots \wedge x_n^{\sigma_n})$
- Включаем в СДНФ все полученные конъюнкции:

$$f(x_1, \ldots, x_n) = \bigvee_{f(\sigma_1, \ldots, \sigma_n)=1} (x_1^{\sigma_1} \wedge \cdots \wedge x_n^{\sigma_n})$$

По построению: выражение справа принимает значение 1 $\Leftrightarrow f = 1$.

Построение СДНФ по таблице истинности

- В таблице истинности отмечаем все наборы переменных, на которых функция равна 1.
- Для каждого такого набора $(\sigma_1, \ldots, \sigma_n)$ берем конъюнкцию $(x_1^{\sigma_1} \wedge \cdots \wedge x_n^{\sigma_n})$
- Включаем в СДНФ все полученные конъюнкции:

$$f(x_1, \ldots, x_n) = \bigvee_{f(\sigma_1, \ldots, \sigma_n)=1} (x_1^{\sigma_1} \wedge \cdots \wedge x_n^{\sigma_n})$$

По построению: выражение справа принимает значение 1 $\Leftrightarrow f = 1$. Мы доказали:

Теорема

Для любой булевой функции, не равной тождественно нулю, существует СДНФ, ее задающая.

КНФ и СКНФ

Аналогично определяется и строится СКНФ:
Простой дизъюнкцией называется дизъюнкция одной или нескольких переменных или их отрицаний, причем каждая переменная встречается не более одного раза.

Конъюнктивная нормальная форма (КНФ) — представление БФ в виде конъюнкции простых дизъюнкций.

Пример: $(x \vee \neg y) \wedge z$

Если в каждой дизъюнкции участвуют все переменные, это совершенная КНФ (СКНФ).

Строится аналогично по таблице истинности:

$$f(x_1, \ldots, x_n) = \bigwedge_{f(\sigma_1,\ldots,\sigma_n)=0} (x_1^{\neg\sigma_1} \vee \cdots \vee x_n^{\neg\sigma_n})$$

Многочлен Жегалкина

Многочлен Жегалкина: сумма по модулю 2 конъюнкций переменных (также допускается слагаемое-единица) без повторений слагаемых, а также константа 0.

Например, $f(x, y, z) = 1 \oplus x \oplus x \wedge y \wedge z$.

Многочлен Жегалкина

Многочлен Жегалкина: сумма по модулю 2 конъюнкций переменных (также допускается слагаемое-единица) без повторений слагаемых, а также константа 0.

Например, $f(x, y, z) = 1 \oplus x \oplus x \wedge y \wedge z$.

Общий вид:

$$f(x_1, \ldots, x_n) = a \oplus \bigoplus_{\substack{1 \le i_1 < \cdots < i_k \le n \\ k \in \{1, \ldots, n\}}} a_{i_1 \ldots i_k} \wedge x_{i_1} \wedge \cdots \wedge x_{i_k},$$

где $\quad a, a_{i_1 \ldots i_k} \in \{0, 1\}$.

Многочлен Жегалкина

Многочлен Жегалкина: сумма по модулю 2 конъюнкций переменных (также допускается слагаемое-единица) без повторений слагаемых, а также константа 0.

Например, $f(x, y, z) = 1 \oplus x \oplus x \wedge y \wedge z$.

Общий вид:

$$f(x_1, \dots, x_n) = a \oplus \bigoplus_{\substack{1 \le i_1 < \dots < i_k \le n \\ k \in \{1, \dots, n\}}} a_{i_1 \dots i_k} \wedge x_{i_1} \wedge \dots \wedge x_{i_k},$$

где $\quad a, a_{i_1 \dots i_k} \in \{0, 1\}$.

Или, что то же самое: $f(x_1, \dots, x_n) =$

$$a \oplus a_1 x_1 \oplus \dots a_n \wedge x_n \oplus a_{12} \wedge x_1 \wedge x_2 \oplus \dots a_{1 \dots n} \wedge x_1 \wedge \dots \wedge x_n$$

Многочлен Жегалкина

Многочлен Жегалкина: сумма по модулю 2 конъюнкций переменных (также допускается слагаемое-единица) без повторений слагаемых, а также константа 0.

Например, $f(x,y,z) = 1 \oplus x \oplus x \wedge y \wedge z$.

Общий вид:

$$f(x_1,\ldots,x_n) = a \oplus \bigoplus_{\substack{1 \le i_1 < \cdots < i_k \le n \\ k \in \{1,\ldots,n\}}} a_{i_1\ldots i_k} \wedge x_{i_1} \wedge \cdots \wedge x_{i_k},$$

где $\quad a, a_{i_1\ldots i_k} \in \{0,1\}$.

Или, что то же самое: $f(x_1,\ldots,x_n) =$

$$a \oplus a_1 x_1 \oplus \ldots a_n \wedge x_n \oplus a_{12} \wedge x_1 \wedge x_2 \oplus \ldots a_{1\ldots n} \wedge x_1 \wedge \cdots \wedge x_n$$

Примечание: Зачастую константу 0 не считают полиномом Жегалкина, то есть в выражении допускаются только конъюнкции, сложения и константа 1.

Многочлен Жегалкина

Теорема

Для каждой функции существует единственное представление многочленом Жегалкина.

Многочлен Жегалкина

Теорема

Для каждой функции существует единственное представление многочленом Жегалкина.

Доказательство. **Существование**. Преобразуем ДНФ:

- замена дизъюнкции: $x \vee y = x \oplus y \oplus x \wedge y$ (Д/З)

Многочлен Жегалкина

Теорема

Для каждой функции существует единственное представление многочленом Жегалкина.

Доказательство. **Существование**. Преобразуем ДНФ:

- замена дизъюнкции: $x \vee y = x \oplus y \oplus x \wedge y$ (Д/З)
- замена отрицаний: $\neg x = x \oplus 1$

Многочлен Жегалкина

Теорема

Для каждой функции существует единственное представление многочленом Жегалкина.

Доказательство. **Существование**. Преобразуем ДНФ:

- замена дизъюнкции: $x \vee y = x \oplus y \oplus x \wedge y$ (Д/З)
- замена отрицаний: $\neg x = x \oplus 1$
- раскрываем скобки по тождеству:
  $(x \oplus y) \wedge z = (x \wedge z) \oplus (y \wedge z)$ (Д/З)

Многочлен Жегалкина

Теорема

Для каждой функции существует единственное представление многочленом Жегалкина.

Доказательство. **Существование**. Преобразуем ДНФ:

- замена дизъюнкции: $x \vee y = x \oplus y \oplus x \wedge y$ (Д/З)
- замена отрицаний: $\neg x = x \oplus 1$
- раскрываем скобки по тождеству: $(x \oplus y) \wedge z = (x \wedge z) \oplus (y \wedge z)$ (Д/З)
- сокращаются одинаковые слагаемые: $x \oplus x = 0$.

Многочлен Жегалкина

Теорема

Для каждой функции существует единственное представление многочленом Жегалкина.

Доказательство. **Существование**. Преобразуем ДНФ:

- замена дизъюнкции: $x \vee y = x \oplus y \oplus x \wedge y$ (Д/З)
- замена отрицаний: $\neg x = x \oplus 1$
- раскрываем скобки по тождеству:
  $(x \oplus y) \wedge z = (x \wedge z) \oplus (y \wedge z)$ (Д/З)
- сокращаются одинаковые слагаемые: $x \oplus x = 0$.

Единственность: всего многочленов Жегалкина 2^{2^n}; функций столько же — следовательно, представление единственно.

Замкнутые классы

$\mathcal{F}$ — множество булевых функций
замыкание $[\mathcal{F}]$ (относительно суперпозиции) — это множество всех булевых функций, представимых формулой над $\mathcal{F}$.

Замкнутые классы

$\mathcal{F}$ — множество булевых функций

замыкание $[\mathcal{F}]$ (относительно суперпозиции) — это множество всех булевых функций, представимых формулой над $\mathcal{F}$.

Примеры:

$[\emptyset] = \{\emptyset\}$,

$[\neg x] = \{x, \neg x\}$,

$[x \vee y] = \{x_1 \vee \cdots \vee x_n | n > 1\}$.

Замкнутые классы

$\mathcal{F}$ — множество булевых функций
замыкание $[\mathcal{F}]$ (относительно суперпозиции) — это множество всех булевых функций, представимых формулой над $\mathcal{F}$.

Примеры:
$[\emptyset] = \{\emptyset\}$,
$[\neg x] = \{x, \neg x\}$,
$[x \vee y] = \{x_1 \vee \cdots \vee x_n | n > 1\}$.

Замкнутый класс — равный своему замыканию.

Замкнутые классы

T_0: класс функций, сохраняющих ноль:
$T_0 = \{f | f(0, \ldots, 0) = 0\}$

T_1: класс функций, сохраняющих единицу:
$T_1 = \{f | f(1, \ldots, 1) = 1\}$

Замкнутые классы

T_0: класс функций, сохраняющих ноль:
$T_0 = \{f | f(0, \ldots, 0) = 0\}$

T_1: класс функций, сохраняющих единицу:
$T_1 = \{f | f(1, \ldots, 1) = 1\}$

Примеры:

- $\vee$ и $\wedge$ сохраняют как ноль, так и единицу
- $\oplus$ сохраняет ноль, но не сохраняет единицу
- $\rightarrow$ сохраняет единицу, но не сохраняет ноль
- $\neg$ не сохраняет ни единицу, ни ноль

Замкнутые классы

T_0: класс функций, сохраняющих ноль:
$T_0 = \{f | f(0, \ldots, 0) = 0\}$

T_1: класс функций, сохраняющих единицу:
$T_1 = \{f | f(1, \ldots, 1) = 1\}$

Примеры:

- $\vee$ и $\wedge$ сохраняют как ноль, так и единицу
- $\oplus$ сохраняет ноль, но не сохраняет единицу
- $\to$ сохраняет единицу, но не сохраняет ноль
- $\neg$ не сохраняет ни единицу, ни ноль

Предложение

Классы функций T_0 и T_1 замкнуты.

Двойственные функции

Двойственная функция к f:

$$f^*(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n).$$

Самодвойственная функция: $f^* = f$.

Двойственные функции

Двойственная функция к f:

$$f^*(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n).$$

Самодвойственная функция: $f^* = f$.

Примеры:

- $\vee$ и $\wedge$ двойственны друг другу
- $\neg$ двойственно самому себе (самодвойственно)

Двойственные функции

Двойственная функция к f:

$$f^*(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n).$$

Самодвойственная функция: $f^* = f$.

Примеры:

- $\vee$ и $\wedge$ двойственны друг другу
- $\neg$ двойственно самому себе (самодвойственно)

Предложение

$(f^*)^* = f$.

S: класс самодвойственных функций.

Предложение

Класс функций S замкнут.

Монотонные функции

Частичный порядок на множестве двоичных наборов:
$(b_1, \ldots, b_n) \le (c_1, \ldots, c_n)$, если $b_i \le c_i$ для всех i.

Монотонные функции

Частичный порядок на множестве двоичных наборов:
$(b_1, \ldots, b_n) \leq (c_1, \ldots, c_n)$, если $b_i \leq c_i$ для всех i.

f — монотонная функция, если $f(\alpha) \leq f(\beta)$, если $\alpha \leq \beta$.

M: класс монотонных функций.

Монотонные функции

Частичный порядок на множестве двоичных наборов:
$(b_1, \ldots, b_n) \le (c_1, \ldots, c_n)$, если $b_i \le c_i$ для всех i.

f — монотонная функция, если $f(\alpha) \le f(\beta)$, если $\alpha \le \beta$.

M: класс монотонных функций.

Примеры:

- $\vee$ и $\wedge$ монотонны
- $\neg$, $\oplus$, $\to$ немонотонны

Монотонные функции

Частичный порядок на множестве двоичных наборов:
$(b_1, \ldots, b_n) \leq (c_1, \ldots, c_n)$, если $b_i \leq c_i$ для всех i.

f — монотонная функция, если $f(\alpha) \leq f(\beta)$, если $\alpha \leq \beta$.

M: класс монотонных функций.

Примеры:

- $\vee$ и $\wedge$ монотонны
- $\neg$, $\oplus$, $\to$ немонотонны

Предложение

Класс M замкнут.

Линейные функции

Линейные функции — такие, многочлен Жегалкина которых не использует конъюнкции; а также константа 0.

Линейные функции

Линейные функции — такие, многочлен Жегалкина которых не использует конъюнкции; а также константа 0.

L: класс линейных функций:

$$L = \{x_{i_1} \oplus \cdots \oplus x_{i_m} \oplus c \mid m > 0, 1 \leq i_1 < \cdots < i_m \leq n, c \in \{0, 1\}\}$$

Линейные функции

Линейные функции — такие, многочлен Жегалкина которых не использует конъюнкции; а также константа 0.

L: класс линейных функций:

$$L = \{x_{i_1} \oplus \cdots \oplus x_{i_m} \oplus c \,|\, m > 0, 1 \leq i_1 < \cdots < i_m \leq n, c \in \{0,1\}\}$$

Предложение

Класс L замкнут.

Примеры:

- $\oplus$, $\neg$ линейны
- $\vee$, $\wedge$ нелинейны

Критерий полноты системы функций

Множество булевых функций $\mathcal{F}$ называется полной системой, если все булевы функции выразимы формулами над этим базисом.

Критерий полноты системы функций

Множество булевых функций $\mathcal{F}$ называется полной системой, если все булевы функции выразимы формулами над этим базисом.

Теорема (Пост, 1921)

Множество булевых функций $\mathcal{F}$ является полным тогда и только тогда, когда $\mathcal{F}$ не содержится ни в одном из пяти классов T_0, T_1, S, M, L.

Доказательство

$\Rightarrow$: Если содержится, то его замыкание $[\mathcal{F}]$ также содержится в этом классе.

Доказательство

$\Rightarrow$: Если содержится, то его замыкание $[\mathcal{F}]$ также содержится в этом классе.

$\Leftarrow$: Пусть не содержится, т.е., есть функции $f_0, f_1, f_S, f_M, f_L \in \mathcal{F}$, где $f_0 \notin T_0$, $f_1 \notin T_1$, $f_S \notin S$, $f_M \notin M$, $f_L \notin L$ (эти функции не обязательно различны).

Доказательство

$\Rightarrow$: Если содержится, то его замыкание $[\mathcal{F}]$ также содержится в этом классе.

$\Leftarrow$: Пусть не содержится, т.е., есть функции $f_0, f_1, f_S, f_M, f_L \in \mathcal{F}$, где $f_0 \notin T_0$, $f_1 \notin T_1$, $f_S \notin S$, $f_M \notin M$, $f_L \notin L$ (эти функции не обязательно различны).

План доказательства:

1. Сперва из f_0 и f_1 выражается или отрицание, или обе константы, или и то и другое (как получится).

Доказательство

$\Rightarrow$: Если содержится, то его замыкание $[\mathcal{F}]$ также содержится в этом классе.

$\Leftarrow$: Пусть не содержится, т.е., есть функции $f_0, f_1, f_S, f_M, f_L \in \mathcal{F}$, где $f_0 \notin T_0$, $f_1 \notin T_1$, $f_S \notin S$, $f_M \notin M$, $f_L \notin L$ (эти функции не обязательно различны).

План доказательства:

1. Сперва из f_0 и f_1 выражается или отрицание, или обе константы, или и то и другое (как получится).
2. Выразим отрицание и константы следующим образом:

Доказательство

$\Rightarrow$: Если содержится, то его замыкание $[\mathcal{F}]$ также содержится в этом классе.

$\Leftarrow$: Пусть не содержится, т.е., есть функции $f_0, f_1, f_S, f_M, f_L \in \mathcal{F}$, где $f_0 \notin T_0$, $f_1 \notin T_1$, $f_S \notin S$, $f_M \notin M$, $f_L \notin L$ (эти функции не обязательно различны).

План доказательства:

1. Сперва из f_0 и f_1 выражается или отрицание, или обе константы, или и то и другое (как получится).
2. Выразим отрицание и константы следующим образом:
   - 2.1 Если получилось отрицание, то из f_S выражаются константы;
   - 2.2 Если же вышли обе константы, то отрицание выражается из f_M.

Доказательство

$\Rightarrow$: Если содержится, то его замыкание $[\mathcal{F}]$ также содержится в этом классе.

$\Leftarrow$: Пусть не содержится, т.е., есть функции $f_0, f_1, f_S, f_M, f_L \in \mathcal{F}$, где $f_0 \notin T_0$, $f_1 \notin T_1$, $f_S \notin S$, $f_M \notin M$, $f_L \notin L$ (эти функции не обязательно различны).

План доказательства:

1. Сперва из f_0 и f_1 выражается или отрицание, или обе константы, или и то и другое (как получится).
2. Выразим отрицание и константы следующим образом:
   - 2.1 Если получилось отрицание, то из f_S выражаются константы;
   - 2.2 Если же вышли обе константы, то отрицание выражается из f_M.
3. из f_L выражается конъюнкция.

Доказательство

(1) Так как $f_0 \notin T_0$, то по определению T_0 имеем $f_0(0, \ldots, 0) = 1$.

Доказательство

(1) Так как $f_0 \notin T_0$, то по определению T_0 имеем $f_0(0, \dots, 0) = 1$.

1. Если при этом $f_0(1, \dots, 1) = 1$, то получена константа 1 в виде $\varphi_1(x) = f_0(x, \dots, x) = 1$.

Доказательство

(1) Так как $f_0 \notin T_0$, то по определению T_0 имеем $f_0(0, \ldots, 0) = 1$.

1. Если при этом $f_0(1, \ldots, 1) = 1$, то получена константа 1 в виде $\varphi_1(x) = f_0(x, \ldots, x) = 1$.
2. Если же $f_0(1, \ldots, 1) = 0$, то в таком же виде получено отрицание, $\overline{\varphi}(x) = \neg x = f_0(x, \ldots, x)$

Доказательство

(1) Так как $f_0 \notin T_0$, то по определению T_0 имеем $f_0(0, \ldots, 0) = 1$.

1. Если при этом $f_0(1, \ldots, 1) = 1$, то получена константа 1 в виде $\varphi_1(x) = f_0(x, \ldots, x) = 1$.
2. Если же $f_0(1, \ldots, 1) = 0$, то в таком же виде получено отрицание, $\overline{\varphi}(x) = \neg x = f_0(x, \ldots, x)$

Аналогично, для $f_1 \notin T_1$: известно, что $f_1(1, \ldots, 1) = 0$, и рассматривая значение $f_1(0, \ldots, 0)$, получаем или константу 0, или отрицание.

Доказательство

(2.1) Пусть получено отрицание.

Для функции $f_S \notin S$ известно, что существует набор $(\sigma_1, \ldots, \sigma_n)$, на котором

$$f_S(\sigma_1, \ldots, \sigma_n) \neq \neg f_S(\neg\sigma_1, \ldots, \neg\sigma_n),$$

т.е.

$$f_S(\sigma_1, \ldots, \sigma_n) = f_S(\neg\sigma_1, \ldots, \neg\sigma_n).$$

Доказательство

(2.1) Пусть получено отрицание.

Для функции $f_S \notin S$ известно, что существует набор $(\sigma_1, \ldots, \sigma_n)$, на котором

$$f_S(\sigma_1, \ldots, \sigma_n) \neq \neg f_S(\neg\sigma_1, \ldots, \neg\sigma_n),$$

т.е.

$$f_S(\sigma_1, \ldots, \sigma_n) = f_S(\neg\sigma_1, \ldots, \neg\sigma_n).$$

Тогда формула $f_S(x^{\sigma_1}, \ldots, x^{\sigma_n})$, построенная из f_S и из отрицания, выражает одну из констант.

Доказательство

(2.1) Пусть получено отрицание.

Для функции $f_S \notin S$ известно, что существует набор $(\sigma_1, \ldots, \sigma_n)$, на котором

$$f_S(\sigma_1, \ldots, \sigma_n) \neq \neg f_S(\neg\sigma_1, \ldots, \neg\sigma_n),$$

т.е.

$$f_S(\sigma_1, \ldots, \sigma_n) = f_S(\neg\sigma_1, \ldots, \neg\sigma_n).$$

Тогда формула $f_S(x^{\sigma_1}, \ldots, x^{\sigma_n})$, построенная из f_S и из отрицания, выражает одну из констант.

С помощью отрицания выражается вторая константа.

Доказательство

(2.2) Пусть на шаге (1) получены обе константы.

Для функции $f_M \notin M$ существуют два набора α и β, для которых $\alpha < \beta$, но $f_M(\alpha) = 1$ и $f_M(\beta) = 0$.

Доказательство

(2.2) Пусть на шаге (1) получены обе константы.

Для функции $f_M \notin M$ существуют два набора α и β, для которых $\alpha < \beta$, но $f_M(\alpha) = 1$ и $f_M(\beta) = 0$.

Пусть $i_1, \ldots, i_k$ — номера всех координат, в которых α и β отличаются друг от друга. Соответственно, в α там 0, в β — 1, а остальные координаты общие, σ_i, где $i \notin \{i_1, \ldots, i_k\}$:

$$f_M(\sigma_1, \ldots, \sigma_{i_1-1}, 0, \sigma_{i_1+1}, \ldots, \sigma_{i_k-1}, 0, \sigma_{i_k+1} \ldots \sigma_n) = 1$$

$$f_M(\sigma_1, \ldots, \sigma_{i_1-1}, 1, \sigma_{i_1+1}, \ldots, \sigma_{i_k-1}, 1, \sigma_{i_k+1} \ldots \sigma_n) = 0$$

Доказательство

(2.2) Пусть на шаге (1) получены обе константы.

Для функции $f_M \notin M$ существуют два набора α и β, для которых $\alpha < \beta$, но $f_M(\alpha) = 1$ и $f_M(\beta) = 0$.

Пусть $i_1, \ldots, i_k$ — номера всех координат, в которых α и β отличаются друг от друга. Соответственно, в α там 0, в β — 1, а остальные координаты общие, σ_i, где $i \notin \{i_1, \ldots, i_k\}$:

$$f_M(\sigma_1, \ldots, \sigma_{i_1-1}, 0, \sigma_{i_1+1}, \ldots, \sigma_{i_k-1}, 0, \sigma_{i_k+1} \ldots \sigma_n) = 1$$

$$f_M(\sigma_1, \ldots, \sigma_{i_1-1}, 1, \sigma_{i_1+1}, \ldots, \sigma_{i_k-1}, 1, \sigma_{i_k+1} \ldots \sigma_n) = 0$$

Чтобы получить отрицание, подставим:

- константы вместо всех общих координат
- одной и той же переменной x во всех изменяющиеся координатах:

$$\neg x = f_M(\sigma_1, \ldots, \sigma_{i_1-1}, x, \sigma_{i_1+1}, \ldots, \sigma_{i_k-1}, x, \sigma_{i_k+1} \ldots \sigma_n)$$

Доказательство

Мы построили $0, 1, \neg$; нужно $\wedge$:

Доказательство

Мы построили 0,1,$\neg$; нужно $\wedge$:

(3) Так как функция f_L нелинейна, ее многочлен Жегалкина содержит хотя бы одну конъюнкцию.

Доказательство

Мы построили 0,1,$\neg$; нужно $\wedge$:

(3) Так как функция f_L нелинейна, ее многочлен Жегалкина содержит хотя бы одну конъюнкцию.

Пусть переменные x и y входят в состав этой конъюнкции.

Доказательство

Мы построили 0,1,$\neg$; нужно $\wedge$:

(3) Так как функция f_L нелинейна, ее многочлен Жегалкина содержит хотя бы одну конъюнкцию.

Пусть переменные x и y входят в состав этой конъюнкции.

Тогда функцию можно представить в виде $f_L(x, y, z, \dots) = xyP(z, \dots) \oplus xQ(z, \dots) \oplus yR(z, \dots) \oplus S(z, \dots)$, где P, Q, R, S — многочлены Жегалкина (Q,R,S могут отсутствовать).

Доказательство

Мы построили 0,1,$\neg$; нужно $\wedge$:

(3) Так как функция f_L нелинейна, ее многочлен Жегалкина содержит хотя бы одну конъюнкцию.

Пусть переменные x и y входят в состав этой конъюнкции.

Тогда функцию можно представить в виде $f_L(x, y, z, \dots) = xyP(z, \dots) \oplus xQ(z, \dots) \oplus yR(z, \dots) \oplus S(z, \dots)$, где P, Q, R, S — многочлены Жегалкина (Q,R,S могут отсутствовать).

Так как P — не константа 0, она равна единице на некотором наборе α.

Доказательство

Тогда $g(x, y) = f_L(x, y, \alpha) =$
$= xyP(\alpha) \oplus xQ(\alpha) \oplus yR(\alpha) \oplus S(\alpha) =$
$= xy \oplus xb \oplus yc \oplus d$, где $b, c, d \in \{0, 1\}$.

Доказательство

Тогда $g(x, y) = f_L(x, y, \alpha) =$
$= xyP(\alpha) \oplus xQ(\alpha) \oplus yR(\alpha) \oplus S(\alpha) =$
$= xy \oplus xb \oplus yc \oplus d$, где $b, c, d \in \{0, 1\}$.

Подстановкой $g(x \oplus c, y \oplus b)$ получается следующая функция:

$h(x, y) = g(x \oplus c, y \oplus b) =$
$(x \oplus c)(y \oplus b) \oplus (x \oplus c)b \oplus (y \oplus b)c \oplus d = xy \oplus bc \oplus d$

Доказательство

Тогда $g(x, y) = f_L(x, y, \alpha) =$
$= xyP(\alpha) \oplus xQ(\alpha) \oplus yR(\alpha) \oplus S(\alpha) =$
$= xy \oplus xb \oplus yc \oplus d$, где $b, c, d \in \{0, 1\}$.

Подстановкой $g(x \oplus c, y \oplus b)$ получается следующая функция:

$h(x, y) = g(x \oplus c, y \oplus b) =$
$(x \oplus c)(y \oplus b) \oplus (x \oplus c)b \oplus (y \oplus b)c \oplus d = xy \oplus bc \oplus d$

В зависимости от значения константного слагаемого $bc \oplus d$, получилась или конъюнкция, или ее отрицание. В последнем случае можно применить к ней ранее выраженную операцию отрицания. ЧТД