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:
$T_1 = \{f | f(1, \ldots, 1) = 1\}$

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

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: $f^* = f$.

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:
$(b_1, \ldots, b_n) \leq (c_1, \ldots, c_n)$, 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.

L: класс линейных функций:

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

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.

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.

$\Leftarrow$: 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 $f_0(0, \ldots, 0) = 1$.

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

(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 $f_M(\beta) = 0$.

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 $\wedge$:

(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 $b, c, d \in \{0, 1\}$.

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