Лекция 5. Замыкание множества функций. Замкнутые классы. Замкнутость классов T_0, T_1, L, S, M. Леммы о несамодвойственной, немонотонной и нелинейной функциях.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Полная система

Пусть $A \subseteq P_2$. Множество A называется **полной системой**, если формулами над A можно выразить любую функцию алгебры логики.

А как проверить полноту заданной системы A?

Оказывается, что можно рассматривать **замкнутые классы**.

Замыкание множества

Пусть $A \subseteq P_2$. **Замыканием** $[A]$ множества A называется множество всех функций, которые могут быть выражены формулами над A.

Замыкание множества

Замыкание множества A можно определить по-другому.

Замыканием $[A]$ называется множество всех функций из P_2, которые можно получить из функций множества A применением следующих операций:

1) добавлением или удалением несущественных переменных;

2) подстановкой в функции из A вместо переменных других переменных (не обязательно различных);

3) подстановкой в функции из A вместо переменных функций из A или функций, которые уже получены.

Суперпозиция

Операции 1–3 называем операциями **суперпозиции**.

Поэтому замыкание $[A]$ — множество всех функций из P_2, которые можно получить из функций из A **суперпозициями**.

Предложение 5.1. *Два приведенных определения замыкания множества A, $A \subseteq P_2$, равносильны, т. е. они определяют одно и то же понятие.*

Свойства замыкания множества

Для произвольных множеств $A, B \subseteq P_2$ верны следующие свойства:

1. $[P_2] = P_2$,
2. $A \subseteq [A]$,
3. если $A \subseteq B$, то $[A] \subseteq [B]$,
4. $[[A]] = [A]$.

Замкнутый класс

Пусть $A \subseteq P_2$. Множество A называется **замкнутым классом**, если $[A] = A$.

Из свойств замыкания множества следует, что если $A = [B]$ для некоторого множества B, $B \subseteq P_2$, то A — замкнутый класс.

В частности, P_2 — замкнутый класс.

Замкнутые классы и полнота

Предложение 5.2. *Пусть $A \subseteq P_2$, A — замкнутый класс и $A \neq P_2$. Тогда для любого множества B, $B \subseteq P_2$, верно: если $B \subseteq A$, то B — не полная система.*

Доказательство. Итак,

$$B \subseteq A.$$

По свойствам замыкания и из условия получаем:

$$[B] \subseteq [A] = A \neq P_2.$$

Значит, $[B] \neq P_2$, т. е. B — не полная система.

□

Конгруэнтные функции

Напомним, что функции $f \in P_2$ и $g \in P_2$ называются **конгруэнтными**, если переменные одной из них можно так переименовать, что получится функция, равная другой.

Т. к. в при построении формулы можно подставлять любые переменные (из X) в функции, любой замкнутый класс вместе с каждой функцией содержит все функции, конгруэнтные ей.

Конгруэнтные функции

1. Функции $f_1 = x_1$ и $f_2 = x_2$ — конгруэнтны (считаем, что разные переменные обозначаются по-разному).

Их можно рассматривать как функции переменных x_1, x_2:

$$f_1(x_1, x_2) = x_1, \;\; f_2(x_1, x_2) = x_2.$$

2. Функции $f_1 = x_1$, $f_2 = x_2$, ..., $f_n = x_n$, ... — также конгруэнтны.

Это функции, конгруэнтные тождественной функции $f(x) = x$, их счетное число.

Функции, конгруэнтные тождественной функции

Пусть $e_i^n \in P_2^{(n)}$ и $e_i^n(x_1, \ldots, x_n) = x_i$, $1 \leqslant i \leqslant n$, $n \geqslant 1$.

Положим:

$$I = \{e_i^n \mid i = 1, \ldots, n, n \geqslant 1\}.$$

Т. е. I — множество всех функций (переменных из X), конгруэнтных тождественной функции.

Лемма о замкнутом классе

Для дальнейшего нам понадобится следующая лемма.

Лемма 5.1. *Пусть $A \subseteq P_2$ и $I \subseteq A$. Если для любых функций $f_0(y_1, \ldots, y_m) \in A$, $f_i(x_1, \ldots, x_n) \in A$, $i = 1, \ldots, m$, причем функции f_i могут зависеть несущественно от некоторых своих переменных, верно*

$$f_0(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) \in A,$$

то множество A является замкнутым классом.

Лемма о замкнутом классе

Доказательство. Рассмотрим произвольную функцию $f \in [A]$ Она выражается некоторой формулой F над множеством A.

Докажем индукцией по числу d вхождений в формулу F обозначений функций из $A \setminus I$, что $f \in A$.

1. *Базис индукции*: $d = 0$. Если $F = x_i$, то $f \in A$ по условию утверждения.

Лемма о замкнутом классе

2. *Индуктивный переход*. Пусть любая функция, которая может быть выражена формулой не более чем с d_0 вхождениями обозначений функций из $A \setminus I$, содержится в A.

Рассмотрим функцию $f(x_1, \ldots, x_n) \in [A]$, которая выражается формулой F с $d_0 + 1$ вхождениями обозначений функций из $A \setminus I$.

Тогда $F = f_0(F_1, \ldots, F_m)$, где $f_0 \in A \setminus I$, а F_i — формулы не более чем с d_0 вхождениями обозначений функций из $A \setminus I$, $i = 1, \ldots, m$.

По предположению индукции $f_{F_i} \in A$, $i = 1, \ldots, m$. Значит,

$$f(x_1, \ldots, x_n) = f_0(f_{F_1}(x_1, \ldots, x_n), \ldots, f_{F_m}(x_1, \ldots, x_n)).$$

Далее по условию утверждения $f \in A$.

□

Функции, сохраняющие константу 0

Функция $f(x_1, \dots, x_n) \in P_2$ **сохраняет** 0, если

$$f(0, \dots, 0) = 0.$$

Множество всех функций, сохраняющих 0, обозначим T_0.

Отметим, что $I \subseteq T_0$.

Заметим, что $T_0 \neq \emptyset$, т. к., например, $0, x \oplus y, x \cdot y \in T_0$, и $T_0 \neq P_2$, т. к., например, $1, \bar{x}, x \sim y \notin T_0$.

Замкнутость T_0

Теорема 5.1. *Множество T_0 является замкнутым классом.*

Доказательство. Применим лемму о замкнутом классе. Пусть $f_0(y_1, \ldots, y_m) \in T_0$ и $f_i(x_1, \ldots, x_n) \in T_0$, $i = 1, \ldots, m$, причем функции f_i, $i = 1, \ldots, m$, могут зависеть несущественно от некоторых своих переменных.

Рассмотрим функцию

$$f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)).$$

Получаем:

$$\begin{aligned} f(0, \ldots, 0) &= f_0(f_1(0, \ldots, 0), \ldots, f_m(0, \ldots, 0)) = \\ &= f_0(0, \ldots, 0) = 0, \end{aligned}$$

т. к. $f_i \in T_0$ для всех $i = 1, \ldots, m$ и $f_0 \in T_0$.

Значит, $f \in T_0$.

Функции, сохраняющие константу 1

Функция $f(x_1, \ldots, x_n) \in P_2$ **сохраняет** 1, если

$$f(1, \ldots, 1) = 1.$$

Множество всех функций, сохраняющих 1, обозначим T_1.

Отметим, что $I \subseteq T_1$.

Заметим, что $T_1 \neq \emptyset$, т. к., например, $1, x \sim y, x \cdot y \in T_1$, и $T_1 \neq P_2$, т. к., например, $0, \bar{x}, x \oplus y \notin T_1$.

Замкнутость T_1

Теорема 5.2. *Множество T_1 является замкнутым классом.*

Доказательство полностью аналогично доказательству предыдущего утверждения.

Линейные функции

Функция $f(x_1, \ldots, x_n) \in P_2$ называется **линейной**, если она может быть представлена в виде:

$$f(x_1, \ldots, x_n) = c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n,$$

где коэффициенты $c_0, c_1, \ldots, c_n \in E_2$.

Другими словами, функция f — линейна, если в ее полиноме Жегалкина нет слагаемых с хотя бы двумя переменными (т. е. ранга, большего единицы).

Множество всех линейных функций обозначим L.

Отметим, что $I \subseteq L$.

Заметим, что $L \neq \emptyset$, т. к., например, $0, \bar{x}, x \oplus y \in L$, и $L \neq P_2$, т. к., например, $x \cdot y, x \vee y = xy \oplus x \oplus y \notin L$.

Замкнутость L

Теорема 5.3. *Множество L является замкнутым классом.*

Доказательство. Достаточно заметить, что при при подстановке вместо переменных линейной функции каких-то других линейных функций не могут появиться конъюнкции переменных в слагаемых. Поэтому при такой подстановке получается линейная функция.

□

Самодвойственные функции

Функция $f(x_1, \ldots, x_n) \in P_2$ называется **самодвойственной**, если

$$f^*(x_1, \ldots, x_n) = \overline{f(\bar{x}_1, \ldots, \bar{x}_n)} = f(x_1, \ldots, x_n).$$

Другими словами, функция f — самодвойственна, если двойственная к ней функция с ней совпадает.

Перепишем равенство прямой и двойственной функций в виде:

$$f(\bar{x}_1, \ldots, \bar{x}_n) = \overline{f(x_1, \ldots, x_n)}.$$

Теперь для любого набора $\alpha \in E_2^n$ получаем:

$$f(\bar{\alpha}) = \overline{f(\alpha)}.$$

Значит, функция f — самодвойственна тогда и только тогда, когда на всех парах противоположных наборов она принимает противоположные значения.

Самодвойственные функции

Множество всех самодвойственных функций обозначим S.

Отметим, что $I \subseteq S$.

Заметим, что $S \neq \emptyset$, т. к., например, $x, \bar{x} \in S$, и $S \neq P_2$, т. к., например, $0, 1, x \cdot y \notin S$.

Замкнутость S

Теорема 5.4. *Множество S является замкнутым классом.*

Доказательство. Применим лемму о замкнутом классе. Пусть $f_0(y_1,\ldots,y_m) \in S$ и $f_i(x_1,\ldots,x_n) \in S$, $i = 1,\ldots,m$, причем функции f_i, $i = 1,\ldots,m$, могут зависеть несущественно от некоторых своих переменных.

Рассмотрим функцию

$$f(x_1,\ldots,x_n) = f_0(f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n)).$$

Получаем:

$$\begin{aligned}
\overline{f(\bar{x}_1,\ldots,\bar{x}_n)} &= \overline{f_0(f_1(\bar{x}_1,\ldots,\bar{x}_n),\ldots,f_m(\bar{x}_1,\ldots,\bar{x}_n))} = \\
&= \overline{f_0(\overline{\overline{f_1(\bar{x}_1,\ldots,\bar{x}_n)}},\ldots,\overline{\overline{f_m(\bar{x}_1,\ldots,\bar{x}_n)}})} = \\
&= \overline{f_0(\overline{f_1(x_1,\ldots,x_n)},\ldots,\overline{f_m(x_1,\ldots,x_n)})} = \\
&= f_0(f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n)) = f(x_1,\ldots,x_n),
\end{aligned}$$

т. к. $f_i \in S$ для всех $i = 1,\ldots,m$ и $f_0 \in S$.

Монотонные функции

Напомним, что если $\alpha, \beta \in E_2^n$, то $\alpha \leqslant \beta$ при $\alpha_i \leqslant \beta_i$ для всех $i = 1, \ldots, n$.

Функция $f(x_1, \ldots, x_n) \in P_2$ называется **монотонной**, если для любых наборов $\alpha, \beta \in E_2^n$ из $\alpha \leqslant \beta$ следует $f(\alpha) \leqslant f(\beta)$.

Множество всех монотонных функций обозначим M.

Отметим, что $I \subseteq M$.

Заметим, что $M \neq \emptyset$, т. к., например, $0, 1, x \in M$, и $M \neq P_2$, т. к., например, $\bar{x} \notin M$.

Замкнутость M

Теорема 5.5. *Множество M является замкнутым классом.*

Доказательство. Применим лемму о замкнутом классе. Пусть $f_0(y_1, \ldots, y_m) \in M$ и $f_i(x_1, \ldots, x_n) \in M$, $i = 1, \ldots, m$, причем функции f_i, $i = 1, \ldots, m$, могут зависеть несущественно от некоторых своих переменных.

Замкнутость M

Доказательство. Рассмотрим функцию

$$f(x_1, \dots, x_n) = f_0(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)).$$

Пусть $\alpha, \beta \in E_2^n$ и $\alpha \leqslant \beta$. Тогда:

$$\begin{array}{rcl} f(\alpha) & = & f_0(f_1(\alpha), \dots, f_m(\alpha)) = f_0(\gamma), \\ f(\beta) & = & f_0(f_1(\beta), \dots, f_m(\beta)) = f_0(\delta), \end{array}$$

где $\gamma, \delta \in E_2^m$, $f_i(\alpha) = \gamma_i$, $f_i(\beta) = \delta_i$ для всех $i = 1, \dots, m$.

Но $f_1, \dots, f_m \in M$, поэтому $\gamma_i \leqslant \delta_i$ для всех $i = 1, \dots, m$, а значит, $\gamma \leqslant \delta$.

Но $f_0 \in M$, поэтому $f_0(\gamma) \leqslant f_0(\delta)$, а значит, $f(\alpha) \leqslant f(\beta)$.

Следовательно, $f \in M$. $\square$

Лемма о несамодвойственной функции

Лемма 5.2 (о несамодвойственной функции). *Если $f \notin S$, то, подставляя вместо ее переменных функции x, $\bar{x}$, можно получить функцию, равную константе.*

Лемма о несамодвойственной функции

Доказательство. Если $f(x_1, \ldots, x_n) \notin S$, то найдется такая пара противоположных наборов $\alpha, \bar{\alpha} \in E_2^n$, что

$$f(\alpha) = f(\bar{\alpha}) = c \in E_2.$$

Положим:

$$\varphi(x) = f(x \oplus \alpha_1, \ldots, x \oplus \alpha_n).$$

Отметим, что вместо переменной x_i подставили x при $\alpha_i = 0$ и подставили $\bar{x}$ при $\alpha_i = 1$.

Получаем:

$$\begin{aligned} \varphi(0) &= f(0 \oplus \alpha_1, \ldots, 0 \oplus \alpha_n) = f(\alpha) = c, \\ \varphi(1) &= f(1 \oplus \alpha_1, \ldots, 1 \oplus \alpha_n) = f(\bar{\alpha}) = c. \end{aligned}$$

Значит, $\varphi(x) = c$. $\square$

Лемма о несамодвойственной функции

Пример. Рассмотрим несамодвойственную функцию $f(x_1, x_2, x_3)$:

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Т. к. $f(0,1,0) = f(1,0,1) = 1$, получаем $\varphi(x) = f(x, \bar{x}, x)$.

Теперь $\varphi(0) = f(0,1,0) = 1$, $\varphi(1) = f(1,0,1) = 1$, т. е. $\varphi(x) = 1$.

Лемма о немонотонной функции

Лемма 5.3 (о немонотонной функции). *Если $f \notin M$, то, подставляя вместо ее переменных функции* 0, 1, x *можно получить функцию* $\bar{x}$.

Лемма о немонотонной функции

Доказательство. Если $f(x_1, \ldots, x_n) \notin M$, то найдется такая пара наборов $\alpha, \beta \in E_2^n$, что $\alpha \leqslant \beta$, но $f(\alpha) > f(\beta)$.

Значит, $f(\alpha) = 1$ и $f(\beta) = 0$.

Не ограничивая общности рассуждений, пусть $\alpha_i = 0$, $\beta_i = 1$ для всех $i = 1, \ldots, k$ и $\alpha_i = \beta_i$ для всех $i = k + 1, \ldots, n$, где $1 \leqslant k \leqslant n$.

Лемма о немонотонной функции

Доказательство. Положим:

$$\varphi(x) = f(\underbrace{x, \ldots, x}_{k}, \alpha_{k+1}, \ldots, \alpha_n).$$

Отметим, что вместо переменной x_i подставили x при $i = 1, \ldots, k$ и подставили 0 или 1 при $i = k+1, \ldots, n$.

Получаем:

$$\begin{aligned} \varphi(0) &= f(\underbrace{0, \ldots, 0}_{k}, \alpha_{k+1}, \ldots, \alpha_n) = f(\alpha) = 1, \\ \varphi(1) &= f(\underbrace{1, \ldots, 1}_{k}, \alpha_{k+1}, \ldots, \alpha_n) = f(\beta) = 0. \end{aligned}$$

Значит, $\varphi(x) = \bar{x}$.

$\square$

Лемма о немонотонной функции

Пример. Рассмотрим немонотонную функцию $f(x_1, x_2, x_3)$:

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

Т. к. $f(0,0,1) = 1$, $f(1,1,1) = 0$, получаем $\varphi(x) = f(x,x,1)$.

Теперь $\varphi(0) = f(0,0,1) = 1$, $\varphi(1) = f(1,1,1) = 0$, т. е. $\varphi(x) = \bar{x}$.

Свойство немонотонной функции

Напомним, что наборы $\alpha, \beta \in E_2^n$ называются **соседними**, если они отличаются только в одном разряде.

Предложение 5.3. *Если* $f(x_1, \ldots, x_n) \notin M$, *то найдутся два таких* **соседних** *набора* $\alpha, \beta \in E_2^n$, *что* $\alpha \leqslant \beta$, *но* $f(\alpha) > f(\beta)$.

Доказательство проведите самостоятельно.

Значит, функция f — монотонна тогда и только тогда, когда на всех парах соседних наборов она принимает значения, не нарушающие монотонность.

Лемма о нелинейной функции

Лемма 5.5 (о нелинейной функции). *Если $f \notin L$, то, подставляя вместо ее переменных функции* 0, 1, x, $\bar{x}$, y, $\bar{y}$ *можно получить функцию* $x \cdot y$ *или функцию* $\overline{x \cdot y}$.

Лемма о нелинейной функции

Доказательство. Если $f(x_1, \ldots, x_n) \notin L$, то в ее полиноме Жегалкина найдется слагаемое ранга, не меньшего двух.

Не ограничивая общности рассуждений, пусть в полиноме Жегалкина функции f содержится слагаемое $x_1 \cdot \ldots \cdot x_k$, где $k \geqslant 2$.

Представим полином Жегалкина функции f в виде:

$$\begin{aligned} f(x_1, \ldots, x_n) \quad = \quad & x_1 x_2 \cdot g_1(x_3, \ldots, x_n) \oplus x_1 \cdot g_2(x_3, \ldots, x_n) \oplus \\ & \oplus x_2 \cdot g_3(x_3, \ldots, x_n) \oplus g_4(x_3, \ldots, x_n), \end{aligned}$$

где $g_1, g_2, g_3, g_4 \in P_2$, причем $g_1 \neq 0$.

Значит, найдется такой набор $\alpha \in E_2^{n-2}$, что $g_1(\alpha) = 1$.

Лемма о нелинейной функции

Доказательство. Пусть $g_2(\alpha) = a$, $g_3(\alpha) = b$, $g_4(\alpha) = c$, где $a, b, c \in E_2$.
Тогда

$$f(x_1, x_2, \alpha_1, \ldots, \alpha_{n-2}) = x_1 x_2 \oplus a x_1 \oplus b x_2 \oplus c.$$

Положим:

$$\psi(x, y) = f(x \oplus b, y \oplus a, \alpha_1, \ldots, \alpha_{n-2}).$$

Отметим, что вместо переменной x_1 подставили x или $\bar{x}$, вместо переменной x_2 подставили y или $\bar{y}$ и вместо переменных x_i при $i = 3, \ldots, n$ подставили 0 или 1.

Лемма о нелинейной функции

Доказательство. Получаем:

$$\begin{aligned}
\psi(x,y) &= (x \oplus b)(y \oplus a) \oplus a(x \oplus b) \oplus b(y \oplus a) \oplus c = \\
&= (xy \oplus ax \oplus by \oplus ab) \oplus (ax \oplus ab) \oplus (by \oplus ab) \oplus c = \\
&= xy \oplus (ab \oplus c) = xy \oplus d,
\end{aligned}$$

где $d = ab \oplus c$.

Значит,

$$\psi(x,y) = \begin{cases} x \cdot y, & d = 0, \\ \overline{x \cdot y}, & d = 1. \end{cases}$$

$\square$

Лемма о нелинейной функции

Пример. Рассмотрим нелинейную функцию $f(x_1, x_2, x_3)$:

$$f = x_1x_2x_3 \oplus x_1x_2 \oplus x_2 \oplus x_3.$$

Перепишем f в виде:

$$f = x_1x_2 \cdot (x_3 \oplus 1) \oplus x_1 \cdot (0) \oplus x_2 \cdot (1) \oplus x_3.$$

Значит, $g_1(x_3) = x_3 \oplus 1$, $g_2(x_3) = 0$, $g_3(x_3) = 1$, $g_4(x_3) = x_3$.

Заметим, что $g_1(0) = 1$. Тогда:

$$a = g_2(0) = 0, \;\; b = g_3(0) = 1, \;\; c = g_4(0) = 0.$$

Получаем:

$$\psi(x, y) = f(\bar{x}, y, 0) = (x \oplus 1)y \oplus y = x \cdot y.$$

Проверка принадлежности функции к T_0, T_1, L, S, M

Отметим, что для функции $f(x_1, \ldots, x_n) \in P_2$ алгоритмы проверки ее принадлежности к каждому из классов

$$T_0,\ T_1,\ L,\ S,\ M$$

можно построить на основе условий, определяющих наличие у функции каждого из этих свойств.

1. Сохранения константы: нужно проверить, что $f(0, \ldots, 0) = 0$ или, соответственно, $f(1, \ldots, 1) = 1$.

2. Линейность: можно найти коэффициенты полинома Жегалкина функции f и проверить, что $c_f(\alpha) = 0$ для всех таких $\alpha \in E_2^n$, что $|\alpha| \geqslant 2$.

Проверка принадлежности функции к T_0, T_1, L, S, M

3. Самодвойственность: можно проверить, что на всех парах противоположных наборов f принимает противоположные значения.

4. Монотонность: можно проверить, что на всех парах соседних наборов f принимает значения, не нарушающие монотонность.

Задачи для самостоятельного решения

1. Докажите теорему 5.2 и предложение 5.3.

2. Покажите, что если таблицу наборов из E_2^n, $n \geqslant 1$, разделить линией пополам, то все пары противоположных наборов будут находиться симметрично относительно этой линии. На основе этого наблюдения опишите алгоритм проверки принадлежности функции $f \in P_2^{(n)}$, $n \geqslant 1$, к классу S по ее вектору значений $\alpha_f \in E_2^{2^n}$.

Литература к лекции

1. Алексеев В. Б. Лекции по дискретной математике. М.: Инфра-М, 2012. С. 13–20.

2. Марченков С. С. Основы теории булевых функций. М.: Физматлит, 2014. С. 33–38.

3. Яблонский С. В. Введение в дискретную математику. М.: Высшая школа, 2001. С. 30–39.

4. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004.