Лекция Л9. Функционально замкнутые классы

Класс булевых функций называется *функционально замкнутым*, если вместе с функциями из этого класса он содержит и все их суперпозиции.

Очевидно, что для доказательства функциональной замкнутости класса достаточно показать, что элементарные суперпозиции не выводят из этого класса (суперпозиции ранга $r \in \mathrm{N}$ - результат применения r раз элементарных суперпозиций и если всегда все остается на месте, то и любое число применений элементарных суперпозиций оставит все на месте).

Рассмотрим некоторые функционально замкнутые классы. Через T_0 обозначим класс булевых функций сохраняющих 0, т.е. функций, удовлетворяющих условию $f(0,...,0)=0$. Через T_1 обозначим класс булевых функций сохраняющих 1, т.е. функций, удовлетворяющих условию $f(1,...,1)=1$.

Заметим, что $\&,\vee,+,0 \in T_0$; $\&,\vee,\sim,\supset,1 \in T_1$; $\neg,\supset,\circ,|,1 \notin T_0$; $\neg,+,\circ,|,0 \notin T_1$.

Поскольку элементарные суперпозиции не выводят из T_0, T_1, то эти классы функций функционально замкнуты. Например, если $f_1(X_1,...,X_{k_1})$, $f_2(X_1,...,X_{k_2}) \in T_0$, то функция $f_1(X_1,...,X_{i-1}, f_2(X_1,...,X_{k_2}), X_{i+1},...,X_{k_1}) \in T_0$, т.к.

$$f_1(0,...,0, f_2(0,...,0),0,...,0) = f_1(0,...,0) = 0.$$

Переименование переменной также, очевидно, не выводит из T_0. Аналогичные рассуждения применимы и к классу T_1.

Пусть $f(X_1,...,X_n)$ - булева функция. Функция $f^*(X_1,...,X_n)$ называется двойственной к $f(X_1,...,X_n)$, если $f^*(X_1,...,X_n) = \neg f(\bar{X}_1,...,\bar{X}_n)$. Очевидно, что

$$(X_1 \vee X_2)^* = X_1 \,\&\, X_2,\ (X_1 \,\&\, X_2)^* = X_1 \vee X_2,\ 0^* = 1,\ 1^* = 0.$$

Утверждение 7.1 (*принцип двойственности*). Пусть

$$F = f_1(X_1,...,X_{i-1}, f_2(X_1,...,X_{k_2}), X_{i+1},...,X_{k_1}).$$

Тогда

$$F^* = f_1^*(X_1,...,X_{i-1}, f_2^*(X_1,...,X_{k_2}), X_{i+1},...,X_{k_1}).$$

Доказательство. Возможны случаи: (а) $k_1 \ge k_2$; (б) $k_1 < k_2$. Рассмотрим первый случай; второй рассматривается аналогично. В случае (а)

$$F^* = F^*(X_1,...,X_{k_1}) = \neg F(\bar{X}_1,...,\bar{X}_{k_1}) =$$

$$= \neg f_1(\bar{X}_1,...,\bar{X}_{i-1}, \neg\neg f_2(\bar{X}_1,...,\bar{X}_{k_2}), \bar{X}_{i+1},...,\bar{X}_{k_1}) =$$

$$= \neg f_1(\bar{X}_1,...,\bar{X}_{i-1}, \neg f_2^*(X_1,...,X_{k_2}), \bar{X}_{i+1},...,\bar{X}_{k_1}) =$$

$$= f_1^*(X_1,...,X_{i-1}, f_2^*(X_1,...,X_{k_2}), X_{i+1},...,X_{k_1})$$

(в случае (б) $F^* = F^*(X_1,...,X_{k_2})$).

Функция $f(X_1,...,X_n)$ называется *самодвойственной*, если $f(X_1,...,X_n) = f^*(X_1,...,X_n)$. Класс самодвойственных функций обозначается через S.

Класс S самодвойственных функций функционально замкнут. Это следует из утверждения 1, поскольку, если $f_1, f_2 \in S$, т.е. $f_1 = f_1^*$, $f_2 = f_2^*$, то $F^* = F$. Переименование переменной также, очевидно, не выводит из S.

Пример 7.1. Функции X, $\neg X$, $X+Y+Z$, $XY+XZ+YZ$ - самодвойственные (на двойственных оценках принимают двойственные значения):

$$(X+Y+Z)^* = (X+1)+(Y+1)+(Z+1)+1 = X+Y+Z;$$

$$(XY+XZ+YZ)^* = (X+1)(Y+1)+(X+1)(Z+1)+(Y+1)(Z+1)+1 =$$

$$= XY+X+Y+1+XZ+X+Z+1+YZ+Y+Z+1+1 = XY+XZ+YZ.$$

Из определения самодвойственной функции следует, что она задается верхней (или наоборот, нижней) половинной частью таблицы своих значений (в случае перечисления оценок аналогично таблице 7.1 так что в верхней или нижней половине таблицы ни одна оценка не находится вместе с двойственной). Перечислим, например, самодвойственные функции $f(X,Y)$ от двух переменных: X, Y. Пусть $f(1,1) = \alpha$, $f(1,0) = \beta$, где $\alpha, \beta \in \{0,\ 1\}$. Тогда, если $f(X,Y) \in S$, т.е.

$$f(X,Y) = f^*(X,Y) = \neg f(\bar{X}, \bar{Y}),$$

то $f(0,0) = \neg f(1,1) = \bar{\alpha}$, $f(0,1) = \neg f(1,0) = \bar{\beta}$. Всего возможны 4 различные комбинации для значений $\alpha, \beta \in \{0,\ 1\}$:

1) $\alpha = 1, \beta = 1$. В этом случае $f(1,1) = \alpha = 1$, $f(1,0) = \beta = 1$, $f(0,1) = \bar{\beta} = 0$, $f(0,0) = \bar{\alpha} = 0$, т.е. $f(X,Y) = X$.

2) $\alpha = 1, \beta = 0$. В этом случае $f(1,1) = \alpha = 1$, $f(1,0) = \beta = 0$, $f(0,1) = \bar{\beta} = 1$, $f(0,0) = \bar{\alpha} = 0$, т.е. $f(X,Y) = Y$.

3) $\alpha = 0, \beta = 1$. В этом случае $f(1,1) = \alpha = 0$, $f(1,0) = \beta = 1$, $f(0,1) = \bar{\beta} = 0$, $f(0,0) = \bar{\alpha} = 1$, т.е. $f(X,Y) = \bar{Y}$.

4) $\alpha = 0, \beta = 0$. В этом случае $f(1,1) = \alpha = 0$, $f(1,0) = \beta = 0$, $f(0,1) = \bar{\beta} = 1$, $f(0,0) = \bar{\alpha} = 1$, т.е. $f(X,Y) = \bar{X}$.

Таким образом, самодвойственные функции от двух переменных фактически являются функциями от одной переменной, при этом $\&, \vee, +, \sim, \supset, \circ, | \notin S$. Поэтому менее тривиальные самодвойственные функции, фактически зависящие более чем от одной переменной, следует искать среди функций от трех и большего числа переменных.

Простой способ проверки некоторой булевой функции f на принадлежность S дает табличное представление этой функции. Тогда для доказательства непринадлежности

f классу S достаточно указать две двойственные оценки, на которых f принимает одинаковые значения. Воспользуемся в связи с этим табл. 7.1.

X	Y	X	$\bar{X}$	$X \& Y$	$X \vee Y$	$X \supset Y$	$X \sim Y$	$X + Y$	$X \circ Y$	$X \mid Y$
1	1	1	0	1	1	1	1	0	0	0
1	0	1	0	0	1	0	0	1	1	0
0	1	0	1	0	1	1	0	1	1	0
0	0	0	1	0	0	1	1	0	1	1

Табл. 7.1

Из этой таблицы видим, что только функции от одной переменной: X, $\bar{X}$ принадлежат классу S, а остальные не являются самодвойственными. Например, $f(X,Y) =$ $= X \& Y \notin S$, т.к. $f(1,0) = f(0,1)$, т.е. нашлись двойственные оценки, на которых булева функция $X \& Y$ принимает одинаковые значения.

Функция $f(X_1,..., X_n)$ называется *линейной*, если $f(X_1,..., X_n) = a_0 + a_1X_1 + ... + a_nX_n$, где $a_i \in \{0,\ 1\}$, $i = 0,..., n$. Класс линейных функций обозначается через L.

Пример 7.2. Функции $0, 1, X, \neg X, X + Y, X \sim Y, X + Y + Z$ - линейные, $\&, \vee, \supset, \circ, | \notin L$.

Класс L линейных функций функционально замкнут. Если

$$f_1 = a_0 + a_1X_1 + ... + a_{k_1}X_{k_1} \in L,\ f_2 = b_0 + b_1X_1 + ... + b_{k_2}X_{k_2} \in L,$$

то

$$a_0 + a_1X_1 + ... + a_{i-1}X_{i-1} + a_i(b_0 + b_1X_1 + ... + b_{k_2}X_{k_2}) + a_{i+1}X_{i+1} + ... + a_{k_1}X_{k_1} \in L$$

(см. свойства 1 - 6 булевых функций $\cdot, +$ из темы Многочлены Жегалкина). Переименование переменной также, очевидно, не выводит из L.

Введем отношение частичного порядка на множестве оценок списка переменных $< X_1,..., X_n >$. Это ранее введенное отношение Парето:

$$\alpha = < \alpha_1,...,\alpha_n > \leq \beta = < \beta_1,...,\beta_n > \Leftrightarrow \alpha_i \leq \beta_i, i = 1,..., n.$$

Функция $f(X_1,..., X_n)$ называется *монотонной*, если

$$\forall \alpha, \beta \in \{0,\ 1\}^n \quad \alpha \leq \beta \Rightarrow f(\alpha) \leq f(\beta).$$

Класс монотонных функций обозначим через M.

Пример 7.3. Функции $0, 1, X, \&, \vee \in M$; $\neg, +, \sim, \supset, \circ, | \notin M$.

Класс M монотонных функций функционально замкнут. Действительно, элементарные суперпозиции не выводят из M. В частности, если $f_1(X_1,..., X_{k_1})$, $f_2(X_1,..., X_{k_2}) \in$ $\in M$, то $f_1(X_1,..., X_{i-1}, f_2(X_1,..., X_{k_2}), X_{i+1},..., X_{k_1}) \in M$. Покажем это. Пусть, например, $k_1 \geq k_2$ (рассмотрение случая $k_1 < k_2$ аналогично). Если $\alpha = < \alpha_1,...,\alpha_{k_1} >$, $\beta = < \beta_1,...,\beta_{k_1} >$ и $\alpha \leq \beta$, то $f_2(\alpha_1,...,\alpha_{k_2}) \leq f_2(\beta_1,...,\beta_{k_2})$, а следовательно,

$$<\alpha_1,...,\alpha_{i-1}, f_2(\alpha_1,...,\alpha_{k_2}),\alpha_{i+1},...,\alpha_{k_1}>\le<\beta_1,...,\beta_{i-1}, f_2(\beta_1,...,\beta_{k_2}),\beta_{i+1},...,\beta_{k_1}>\Rightarrow$$

$$\Rightarrow f_1(\alpha_1,...,\alpha_{i-1}, f_2(\alpha_1,...,\alpha_{k_2}),\alpha_{i+1},...,\alpha_{k_1})\le f_1(\beta_1,...,\beta_{i-1}, f_2(\beta_1,...,\beta_{k_2}),\beta_{i+1},...,\beta_{k_1}).$$

Переименование переменной также, очевидно, не выводит из M. Простой способ проверки некоторой булевой функции f на принадлежность M дает табличное представление этой функции. Тогда для доказательства непринадлежности f классу M достаточно указать две оценки α,β, для которых выполняется: $\alpha\le\beta$, $f(\alpha)>f(\beta)$. Воспользуемся в связи с этим табл. 7.1. Например, $f(X,Y)=X\supset Y\notin M$, т.к. $<0,0>\le<1,0>$, но $f(0,0)=1>0=f(1,0)$.

Классы T_0,T_1,S,L,M неполные (например, булевы функции $\circ,|$ не принадлежат всем этим классам) и попарно различные. Для любых двух из перечисленных пяти классов можно привести пример булевой функции, принадлежащей первому из них, но не принадлежащий второму. Например, $0\in T_0, 0\notin T_1$; $1\in T_1, 1\notin T_0$; $\neg\in S,\neg\notin T_0$; $\vee\in T_0$, $\vee\notin S$; $\neg\in S,\neg\notin T_1$; $\neg\in L,\neg\notin T_0$; $\neg\in L,\neg\notin T_1$; $\neg\in L,\neg\notin S$ и т.д.

Рассмотрение этих классов дает критерий для проверки полноты системы булевых функций.

Теорема Поста. Для того, чтобы система булевых функций $\{f_1,..., f_m\}$ была полной, необходимо и достаточно, чтобы для каждого из классов T_0,T_1,S,L,M нашлась функция из этой системы, не принадлежащая этому классу.

Необходимость. Если бы все функции системы $\{f_1,..., f_m\}$ принадлежали какому-либо из этих классов, то в силу функциональной замкнутости этих классов ему бы принадлежали и все суперпозиции функций этой системы. Но любой из этих классов отличен от множества всех булевых функций (в каждом из них отсутствуют, например, функции $\circ,|$). Следовательно, эта система не является полной.

Пример 7.4. Используя теорему Поста, покажем полноту системы $\{+,\vee,1\}$. Составим следующую таблицу (*таблица Поста*). В случае принадлежности функции из этой системы некоторому классу из T_0,T_1,S,L,M ставим напротив него символ +, а в противном случае ставим символ $-$. В случае непринадлежности некоторой функции классам S, M указываем номера оценок списка переменных из табл. 7.1 (порядок нумерации - сверху вниз) со значениями функции, подтверждающими эту непринадлежность. В случае непринадлежности некоторой функции классу L приводим многочлен Жегалкина, выражающий эту булеву функцию. Поскольку в каждом столбце табл. 7.2 присутствует хотя бы один символ $-$, то в силу теоремы Поста рассматриваемая система булевых функций полна.

f	T_0	T_1	S	L	M
+	+	–	– строки 1, 4	+	– строки 1, 2
$\vee$	+	+	– строки 2, 3	– $X\vee Y=XY+X+Y$	+
1	–	+	– строки 1, 4	+	+

Табл. 7.2

Система булевых функций G называется *независимой*, если никакая функция $f \in G$ не является суперпозицией функций системы $G \setminus \{f\}$.

Независимая система булевых функций G называется *базисом* функционально замкнутого класса K, если

1) $G \subseteq K$;

2) всякая функция из K является суперпозицией функций из G.

Пример 7.5. Система булевых функций $\{+, \vee, 1\}$ является независимой. Функцию 1 нельзя выразить через $+, \vee$. Это следует из столбца табл. 7.2, соответствующего классу T_0. Действительно, если предположить, что функция 1 является суперпозицией функций $+, \vee$, то поскольку $+, \vee \in T_0$ (см. символы $+$ в столбце для T_0), функция 1 также должна принадлежать классу T_0, что противоречит символу $-$ в столбце для T_0 напротив функции 1. Функцию $+$ нельзя выразить через функции $1, \vee$ (см. столбец табл. 7.2, соответствующий классу T_1). Функцию $\vee$ нельзя выразить через функции 1,+ (см. столбец табл. 7.2, соответствующий классу L).

Упражнения для самоподготовки:

1) Доказать, что $\{\sim, 0\}$ - базис для L.

2) Доказать, что $\{\cdot, +\}$ - базис для T_0.

3) Доказать, что $\{\supset, \&\}$ - базис для T_1. Указание: 1) выразите через $\supset, \&$ булевы функции из T_1 от двух переменных X, Y, принимающих ровно на одной оценке (отличной от $<1,1>$) значение 0, а на остальных – 1. Конъюнкцией таких функций является любая булева функция из T_1, зависящая от X, Y. Например,

$$X \supset (X \supset Y) = 0 \Leftrightarrow X = 1, Y = 0, Y \supset (Y \supset X) = 0 \Leftrightarrow X = 0, Y = 1.$$

Постройте самостоятельно булеву функцию, принимающую значение 0 только на оценке $<0,0>$. Выразите с помощью этих булевых функций и операции $\&$ булеву функцию $X \sim Y$. 2) Действуйте по аналогии для булевых функций от трех переменных: X, Y, Z (постройте, булеву функцию, принимающую значение 0 только на оценке $<0,0,1>$, или только на оценке $<1,1,0>$, или только на оценке $<0,0,0>$, а затем – на произвольном наборе оценок, отличных от $<1,1,1>$). 3) Действуйте по аналогии для булевых функций с произвольным списком переменных $<X_1, ..., X_n>$. Постройте, например, булеву функцию, принимающую значение 0 только на оценке $<0,0,1,1,1>$. 4) Опишите теперь общий алгоритм для произвольной функции $f(X_1, ..., X_n) \in T_1$.