Лекция 1. Вступление. Алгебра логики. Функции алгебры логики. Формулы. Полнота. Замкнутые классы. Классы T_0, T_1, L, S, M. Теорема Поста.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Цель курса

О чем это курс?

Достаточно часто возникает необходимость проверить, совместимы ли некоторые условия, содержащие общие переменные.

Рассмотрим примеры некоторых задач.

Выполнимость выражений

Задача 1. Проверить выполнимость формулы $F(x_1, \ldots, x_n)$ алгебры логики, т. е. существует ли такой набор α из нулей и единиц, что $F(\alpha) = 1$.

Например, проверить выполнимость формулы:

$$F(x_1, x_2, x_3, x_4) = (x_1 \to x_2)(x_2 \sim x_4)(x_3 \to x_4)(x_4 \to x_1)(x_3 \sim x_4).$$

Ограничения значений переменных

Задача 2. Проверить выполнимость условий вида $x_i = x_j$ или $x_i \neq x_j$ для переменных $x_1, \ldots, x_n$, т. е. найдутся ли такие значения переменных $x_1, \ldots, x_n$ из некоторого конечного множества D, что все условия выполняются.

Например, проверить выполнимость условий для переменных x_1, x_2, x_3, x_4, x_5 на конечном множестве $D = \{0, 1, 2\}$:

$$x_1 \neq x_2, \quad x_1 \neq x_4, \quad x_2 = x_4, \quad x_2 \neq x_5, \quad x_3 \neq x_4, \quad x_3 = x_5.$$

Решение систем алгебраических уравнений

Задача 3. Проверить совместность системы алгебраических уравнений над конечным полем F.

Например, проверить совместность системы уравнений над полем F_2 вычетов по модулю два:

$$\left\{\begin{array}{rcl} x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 & = & 1, \\ x_1x_4 \oplus x_1x_5 \oplus x_4x_5 \oplus x_4 & = & 1, \\ x_2x_4 \oplus x_2 \oplus x_4 & = & 0. \end{array}\right.$$

Решение задач

Можно ли для подобных задач найти **общий алгоритм**, который по каждой системе условий выясняет, найдутся ли значения их переменных, для которых все условия системы верны?

Такой алгоритм существует: надо перебрать все возможные значения переменных из системы (т. к. каждая переменная определена на конечном множестве) и проверить, выполняются ли все условия на каком-то из этих наборов.

Однако трудоемкость такого алгоритма велика.

А можно ли построить **быстрый (полиномиальный)** алгоритм?

Постановка задач

Введем ограничения рассматриваемых задач:

1) входное выражение имеет вид конъюнкции некоторых условий, т. е.

$$F(x_1, \ldots, x_n) = g_1 \cdot \ldots \cdot g_m;$$

2) эти условия принадлежат заранее известному конечному множеству S, т. е. $g_j \in S$ (с точностью до переименования переменных) для всех $j = 1, \ldots, m$.

Задача 1

Задача 1. В этом случае:

$$F(x_1, x_2, x_3, x_4) = (x_1 \to x_2)(x_2 \sim x_4)(x_3 \to x_4)(x_4 \to x_1)(x_3 \sim x_4),$$

поэтому:

$$S = \{x \to y, x \sim y\}.$$

Задача 2

Задача 2. В этом случае:

$$x_1 \neq x_2, \quad x_1 \neq x_4, \quad x_2 = x_4, \quad x_2 \neq x_5, \quad x_3 \neq x_4, \quad x_3 = x_5,$$

поэтому

$$S = \{x = y, x \neq y\}.$$

Задача 3

Задача 3. Заметим, что совместность системы над полем F_2:

$$\begin{cases} x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 & = & 1, \\ x_1x_4 \oplus x_1x_5 \oplus x_4x_5 \oplus x_4 & = & 1, \\ x_2x_4 \oplus x_2 \oplus x_4 & = & 0. \end{cases}$$

равносильна выполнимости формулы:

$$F = (x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1)(x_1x_4 \oplus x_1x_5 \oplus x_4x_5 \oplus x_4)(x_2x_4 \oplus x_2 \oplus x_4 \oplus 1).$$

Поэтому:

$$S = \{x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\}.$$

Постановка задачи

Пусть задано **конечное** множество S условий на каком-то **конечном** множестве D, т. е.

$$S = \{g_1, \dots, g_t\},$$

где $g_i : D^{n_i} \to \{0, 1\}$, $i = 1, \dots, t$.

С какой сложностью по произвольному выражению вида:

$$F(x_1, \dots, x_n) = g_{i_1} \cdot \ldots \cdot g_{i_m},$$

где $g_{i_j} \in S$ и зависят от каких-то переменных переменных, $j = 1, \dots, m$, можно проверить, найдется ли такой набор $\alpha \in D^n$, что $F(\alpha) = 1$, т. е.

$$g_{i_1}(\alpha) = 1, \dots, g_{i_m}(\alpha) = 1?$$

Обобщенная выполнимость

Сначала рассмотрим случай булевых условий, т. е. когда $|D| = 2$.

В этом случае задача называется **задачей обобщенной выполнимости**.

Для ее решения повторим **алгебру логику**.

Декартова (прямая) степень множества

Если A — множество и $n \geqslant 1$, то множество A^n состоит из всех упорядоченных n-ок элементов из A.

Любой элемент из A^n будем называть **набором** (**длины** n). При этом составляющие набор элементы множества A будем называть его **разрядами**, или **компонентами**.

Если a — обозначение некоторого набора из A^n (возможно, с индексами), то i-й разряд набора a будем обозначать a_i, $1 \leqslant i \leqslant n$, т. е. $a = (a_1, \ldots, a_n)$.

В частности, если $a_j \in A^n$, то $a_j = (a_{j,1}, \ldots, a_{j,n})$.

Множество E_2^n

Введем обозначение: $E_2 = \{0, 1\}$.

В дальнейшем будем рассматривать множество E_2^n, $n \geqslant 1$.

Множество E_2^n будем также называть *n*-**мерным (двоичным) кубом**.

Любой элемент из E_2^n будем называть (**двоичным**) **набором**.

Наборы из множества E_2^n, как правило, будем обозначать греческими буквами начала алфавита: α, β и т. д., возможно, с индексами.

При этом если $\alpha \in E_2^n$, то $\alpha = (\alpha_1, \ldots, \alpha_n)$; если $\alpha_j \in E_2^n$, то $\alpha_j = (\alpha_{j,1}, \ldots, \alpha_{j,n})$.

Соединение наборов

Если $a \in E_2$ и $\alpha \in E_2^n$, то положим

$$(a, \alpha) = (a, \alpha_1, \ldots, \alpha_n) \in E_2^{n+1}.$$

Например, если $a = 1 \in E_2$ и $\alpha = (0, 1, 1) \in E_2^3$, то

$$(a, \alpha) = (1, 0, 1, 1) \in E_2^4.$$

Если $\alpha \in E_2^m$, $\beta \in E_2^n$, то положим

$$(\alpha, \beta) = (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) \in E_2^{m+n}.$$

Например, если $\alpha = (0, 1) \in E_2^2$ и $\beta = (0, 1) \in E_2^2$, то

$$(\alpha, \beta) = (0, 1, 0, 1) \in E_2^4.$$

Весом $|\alpha|$ набора $\alpha \in E_2^n$ назовем число единиц в нем.

Частичный порядок на E_2^n

На множестве E_2^n определим **частичный порядок** $\leqslant$: если $\alpha, \beta \in E_2^n$, то полагаем $\alpha \leqslant \beta$ при $\alpha_i \leqslant \beta_i$ для всех $i = 1, \ldots, n$ (считаем, что $0 < 1$). При этом если $\alpha \leqslant \beta$ и $\alpha \neq \beta$, то пишем $\alpha < \beta$.

Если $\alpha, \beta \in E_2^n$ и $\alpha \leqslant \beta$ или $\beta \leqslant \alpha$, то наборы α и β называются **сравнимыми**. В обратном случае наборы α и β называются **несравнимыми**.

Например, если $n = 2$, то $(0,0) \leqslant (0,1)$ и $(0,1) \leqslant (1,1)$; а наборы $(0,1)$ и $(1,0)$ являются несравнимыми.

Соседние и противоположные наборы из E_2^n

Наборы $\alpha, \beta \in E_2^n$ называются **соседними**, если они отличаются только в одном разряде. При этом если они отличаются в i-м разряде, то их также называют **соседними по i-му разряду**, $1 \leqslant i \leqslant n$.

Например, если $n = 3$, то наборы $(0, 0, 1)$ и $(1, 0, 1)$ являются соседними (по первому разряду).

Наборы $\alpha, \beta \in E_2^n$ называются **противоположными**, если они отличаются во всех n разрядах. Отметим, что для любого $\alpha \in E_2^n$ противоположный ему набор определен однозначно; обозначим его $\bar{\alpha}$.

Например, если $n = 3$ и $\alpha = (0, 0, 1)$, то $\bar{\alpha} = (1, 1, 0)$.

Функция алгебры логики

Функцией алгебры логики (или **булевой функцией**) называется произвольное отображение из E_2^n в E_2, $n \geqslant 1$.

Т. е. если $f : E_2^n \to E_2$, то f является *n-местной функцией алгебры логики*.

Константы 0 и 1 считаем 0-*местными функциями алгебры логики*.

Множество всех n-местных функций алгебры логики обозначим $P_2^{(n)}$, и $P_2 = \bigcup\limits_{n \geqslant 0} P_2^{(n)}$.

Множество единиц (нулей) функции

Если $f \in P_2^{(n)}$ и $a \in E_2$, то $N_a(f)$ обозначает множество всех наборов из E_2^n, на которых функция f принимает значение a, т.е.

$$N_a(f) = \{\alpha \in E_2^n \mid f(\alpha) = a\}.$$

Таблица истинности

Как можно задавать функции алгебры логики?

1. Таблицы истинности. Упорядочим все наборы из множества E_2^n в **лексико-графическом** порядке и сопоставим каждому набору значение функции $f \in P_2^{(n)}$ на нем:

x_1	$\dots$	x_{n-1}	x_n	$f(x_1,\dots,x_{n-1},x_n)$
0	$\dots$	0	0	$f(0,\dots,0,0)$
0	$\dots$	0	1	$f(0,\dots,0,1)$
	$\dots$			
1	$\dots$	1	0	$f(1,\dots,1,0)$
1	$\dots$	1	1	$f(1,\dots,1,1)$

Вектор значений

2. Если считать, что все наборы из E_2^n упорядочены лексико-графически, то функция $f \in P_2^{(n)}$ однозначно задается правым столбцом ее таблицы истинности. Назовем его **вектором значений** функции f и обозначим α_f. Другими словами,

$$\alpha_f = (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1})) \in E_2^{2^n},$$

где наборы $\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}$ из E_2^n перечислены в лексико-графическом порядке.

Функции алгебры логики

Некоторые важные функции алгебры логики.

$n = 0$: **константы** 0, 1.

$n = 1$:

x	x	$\bar{x}$
0	0	1
1	1	0

x — **тождественно равная** x;
$\bar{x}$ — **отрицание** x.

Функции алгебры логики

$n = 2$:

x_1	x_2	$x_1 \& x_2$	$x_1 \vee x_2$	$x_1 \oplus x_2$	$x_1 \to x_2$	$x_1 \sim x_2$
0	0	0	0	0	1	1
0	1	0	1	1	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

Слева направо по порядку: **конъюнкция**, **дизъюнкция**, **сложение по модулю** 2, **импликация**, **эквивалентность**.

Конъюнкцию & будем также обозначать точкой $\cdot$ или знак операции пропускать.

Знаки $\bar{\ }$, &, $\cdot$, $\vee$, $\oplus$, $\to$, $\sim$ будем называть **связками**.

Функции алгебры логики

$n = 3$:

x_1	x_2	x_3	$m(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Функция $m(x_1, x_2, x_3)$ называется **медианой**, или **функцией голосования**.

Отметим, что функция $m(x_1, x_2, x_3)$ на наборе $\alpha \in E_2^3$ равна 0, если в наборе α больше нулей, чем единиц, и равна 1, если в наборе α больше единиц, чем нулей.

Существенность переменных

Напомним понятие существенной переменной функции.

Переменная x_i называется **существенной** для функции $f(x_1, \ldots, x_n) \in P_2$, если найдутся такие элементы $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in E_2$, что

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Т. е. переменная x_i — существенна для функции $f \in P_2$, если все другие переменные можно так определить, что полученная функция одной переменной x_i не является константой.

Переменная, не являющаяся существенной, называется **несущественной**, или **фиктивной**.

Равенство функций алгебры логики

Считаем, что несущественные переменные можно добавлять и убирать; при этом функция переходит в функцию, равную исходной, но зависящую от другого множества переменных.

Функции $f \in P_2$ и $g \in P_2$ называем **равными**, если добавляя или убирая несущественные переменные из них можно получить совпадающие функции, т. е. *функции, зависящие от одних и тех же переменных и при любом наборе значений этих переменных принимающие одинаковые значения*.

Пример. Функции $f(x) = x$ и $g(x, y) = x$ равны.

Формула

Пусть $A \subseteq P_2$, причем каждая функция из A имеет свое, отличное от других функций, обозначение.

Формула над множеством A определяется по индукции.

1. *Базис индукции*. Если x — переменная, то выражение x — формула.

2. *Индуктивный переход*. Если f — обозначение m-местной функции из A и $F_1, \ldots, F_m$ — уже построенные формулы или переменные (не обязательно различные), то выражение $f(F_1, \ldots, F_m)$ — формула.

3. Других формул нет, т. е. каждая формула построена либо по базису индукции, либо по индуктивному переходу.

Формулы со связками

Укажем особенности при построении формул, если в A входят функции со связками.

При построении формулы над A в таком случае индуктивный переход проводим следующим образом:

1) если $f = \bar{x}$, то $F = \overline{F_1}$;

2) если $f = x \circ y$, где $\circ \in \{\&, \cdot, \vee, \oplus, \rightarrow, \sim\}$, то

$$F = (F_1) \circ (F_2),$$

причем если F_i — переменная, то ее в скобки не заключаем, $i = 1, 2$.

Кроме того, в построенной формуле убираем некоторые скобки, считая, что конъюнкция имеет самый высокий приоритет среди двуместных связок.

Формулы

Пример. Пусть

$$A = \{0, 1, \bar{x}, x \cdot y, x \vee y, x \oplus y, x \to y, x \sim y\} \subseteq P_2.$$

Тогда

$F_1 = x$ и $F_2 = y$	формулы, построенные по базису индукции из переменных x и y;
$F_3 = x \oplus y$	формула, построенная по индуктивному переходу из функции $x_1 \oplus x_2 \in A$ и формул F_1 и F_2;
$F_4 = (x \oplus y) \cdot x$	формула, построенная по индуктивному переходу из функции $x_1 \cdot x_2 \in A$ и формул F_3 и F_1;
$F_5 = \overline{(x \oplus y) \cdot x}$	формула, построенная по индуктивному переходу из функции $\bar{x} \in A$ и формулы F_4;
	и т. д.

Функция, определяемая формулой

Формула $F = F(x_1, \dots, x_n)$ над множеством A, $A \subseteq P_2$, однозначно задает **функцию** $f_F = f_F(x_1, \dots, x_n) \in P_2$, определяемую по индукции.

Базис индукции. Если $F = x$, где x — переменная, то $f_F(x) = x$, т. е. f_F — функция, тождественно равная x.

Индуктивный переход. Если $F = f(F_1, \dots, F_m)$, где f — обозначение m-местной функции из A и $F_1, \dots, F_m$ — формулы, причем формула $F_i = F_i(x_1, \dots, x_n)$ определяет функцию $f_{F_i}(x_1, \dots, x_n)$ (возможно, зависящую не от всех переменных существенно), $i = 1, \dots, m$, то

$$f_F(x_1, \dots, x_n) = f(f_{F_1}(x_1, \dots, x_n), \dots, f_{F_m}(x_1, \dots, x_n)).$$

Функции, определяемые формулами

Пример. Рассмотрим формулу $F_5 = \overline{(x \oplus y) \cdot x}$ из предыдущего примера. Тогда:

x	y	$f_{F_3} = x \oplus y$	$f_{F_4} = (x \oplus y) \cdot x$	$f_{F_5} = \overline{(x \oplus y) \cdot x}$
0	0	0	0	1
0	1	1	0	1
1	0	1	1	0
1	1	0	0	1

Функция f_{F_5}, определяемая формулой F_5, записана в самом правом столбце.

Эквивалентные формулы

Формулы F_1 и F_2 называются **эквивалентными**, если они определяют равные функции, т. е. функции f_{F_1} и f_{F_2} равны.

Обозначение эквивалентных формул: $F_1 = F_2$.

Верны следующие тождества:

1) коммутативность связок $\cdot, \vee, \oplus, \sim$;

2) ассоциативность связок $\cdot, \vee, \oplus, \sim$;

3) дистрибутивность видов

$$\begin{gathered}(x \vee y) \cdot z = x \cdot z \vee y \cdot z;\\ (x \cdot y) \vee z = (x \vee z) \cdot (y \vee z);\\ (x \oplus y) \cdot z = x \cdot z \oplus y \cdot z.\end{gathered}$$

Тождества алгебры логики

Тождества с одной переменной и с константами:

$$
\begin{array}{lllll}
x \cdot x = x, & x \vee x = x, & x \oplus x = 0, & x \to x = 1; & \\
x \cdot \bar{x} = 0, & x \vee \bar{x} = 1, & x \oplus \bar{x} = 1, & \bar{x} \to x = x; & \\
x \cdot 0 = 0, & x \vee 0 = x, & x \oplus 0 = x, & 0 \to x = 1, & x \to 0 = \bar{x}; \\
x \cdot 1 = x, & x \vee 1 = 1, & x \oplus 1 = \bar{x}, & x \to 1 = 1, & 1 \to x = x.
\end{array}
$$

Выражение одних связок через другие:

$$
\begin{array}{ll}
x \sim y = \overline{x \oplus y}, & x \sim y = (x \to y)(y \to x); \\
x \sim y = \bar{x}\bar{y} \vee xy, & x \sim y = (\bar{x} \vee y)(x \vee \bar{y}); \\
x \oplus y = \bar{x}y \vee x\bar{y}, & x \oplus y = (\bar{x} \vee \bar{y})(x \vee y); \\
x \to y = \bar{x} \vee y, & x \to y = \overline{x\bar{y}}.
\end{array}
$$

Тождества алгебры логики

Логические правила:

$x \cdot \bar{x} = 0$	правило противоречия;
$x \vee \bar{x} = 1$	правило исключенного третьего;
$\bar{\bar{x}} = x$	правило снятия двойного отрицания;
$\overline{x \cdot y} = \bar{x} \vee \bar{y}$ и $\overline{x \vee y} = \bar{x} \cdot \bar{y}$	правила де Моргана.

Доказать эти тождества можно, например, постров таблицы истинности функций, определяемых формулами в левой и правой частях равенства.

Функции и формулы

Как правило, мы не будем различать функции и их представления (т.е. формулы), если это не приводит к недоразумениям.

В частности, если F — формула, в которой встречаются только переменные $x_1, \ldots, x_n$ (но не обязательно все), то значение функции f_F на наборе $\alpha \in E_2^n$ будем обозначать $F(\alpha)$ вместо $f_F(\alpha)$.

Литерал

Если $\sigma \in E_2$, то введем обозначение: $x^\sigma = \begin{cases} x, & \sigma = 1; \\ \bar{x}, & \sigma = 0. \end{cases}$

Выражение x^σ называется **литералом** (переменной x).

Совершенная ДНФ

Теорема 1 (о совершенной ДНФ). *Каждая функция $f(x_1, \ldots, x_n) \in P_2$, $f \neq 0$, может быть представлена в виде совершенной дизъюнктивной нормальной формы (ДНФ) D_f, а именно:*

$$f(x_1, \ldots, x_n) = \bigvee_{\sigma \in E_2^n : f(\sigma) = 1} x_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot \ldots \cdot x_n^{\sigma_n}.$$

Совершенная ДНФ

Пример. Найдем совершенную ДНФ функции $f(x_1, x_2, x_3)$:

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

Получаем:

$$f(x_1, x_2, x_3) = \bar{x}_1 x_2 x_3 \vee x_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3 \vee x_1 x_2 x_3.$$

Совершенная КНФ

Теорема 2 (о совершенной КНФ). *Каждая функция* $f(x_1, \ldots, x_n) \in P_2$, $f \neq 1$, *может быть представлена в виде совершенной конъюнктивной нормальной формы (КНФ)* K_f, *а именно:*

$$f(x_1, \ldots, x_n) = \bigwedge_{\sigma \in E_2^n : f(\sigma) = 0} (x_1^{\bar{\sigma}_1} \vee x_2^{\bar{\sigma}_2} \vee \ldots \vee x_n^{\bar{\sigma}_n}).$$

Совершенная КНФ

Пример. Найдем совершенную КНФ функции $f(x_1, x_2, x_3)$:

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

Получаем:

$$f(x_1, x_2, x_3) = (x_1 \vee x_2 \vee x_3)(x_1 \vee x_2 \vee \bar{x}_3)(x_1 \vee \bar{x}_2 \vee x_3)(\bar{x}_1 \vee x_2 \vee x_3).$$

Полная система

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

Утверждение 1. *Следующие множества являются полными системами:*

$$
\begin{aligned}
&1) \quad A = \{x \cdot y, x \vee y, \bar{x}\},\\
&2) \quad A = \{x \cdot y, \bar{x}\},\\
&3) \quad A = \{x \vee y, \bar{x}\},\\
&4) \quad A = \{x \cdot y, x \oplus y, 1\}.
\end{aligned}
$$

Замкнутый класс

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

Множество A называется **замкнутым классом**, если $[A] = A$.

Множество A называется **полной системой**, если $[A] = P_2$.

Функции, сохраняющие константу

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

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

Множество всех функций, сохраняющих 0, обозначим T_0.

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

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.

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

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

Множество всех линейных функций обозначим L.

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

Самодвойственные функции

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

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

Т. е. f — самодвойственная функция, если на всех парах противоположных наборов она принимает противоположные значения.

Множество всех самодвойственных функций обозначим S.

Заметим, что, например, $x, \bar{x} \in S$, и, например, $0, 1, x \cdot y \notin S$.

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 $f(\alpha) \leqslant f(\beta)$.

Можно показать, что f — монотонная функция, если на всех парах соседних наборов она принимает значения, не нарушающие монотонность.

Множество всех монотонных функций обозначим M.

Заметим, что, например, $0, 1, x \in M$, и, например, $\bar{x} \notin M$.

Замкнутость классов T_0, T_1, L, S, M

Утверждение 2. *Каждое из множеств* T_0, T_1, L, S, M *является замкнутым классом*.

Три леммы

Лемма 1 (о несамодвойственной функции). *Если* $f \notin S$, *то, подставляя вместо ее переменных функции* x, $\bar{x}$, *можно получить функцию, равную константе.*

Лемма 2 (о немонотонной функции). *Если* $f \notin M$, *то, подставляя вместо ее переменных функции* 0, 1, x *можно получить функцию* $\bar{x}$.

Лемма 3 (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* $\overline{x \cdot y}$.

Теорема Поста

Теорема 3 (Поста). *Пусть* $A \subseteq P_2$*. Множество* A *является полной системой тогда и только тогда, когда* A *не содержится ни в одном из классов* T_0, T_1, L, S, M, *т. е.*

$$A \not\subseteq T_0, \quad A \not\subseteq T_1, \quad A \not\subseteq L, \quad A \not\subseteq S, \quad A \not\subseteq M.$$

Теорема Поста

По теореме Поста можно проверять полноту систем функций из P_2.

Если задано конечное множество $A = \{f_1, \ldots, f_t\} \subseteq P_2$, то можно построить таблицу со строками, помеченными функциями $f_1, \ldots, f_t$, и со столбцами, помеченными классами T_0, T_1, L, S, M.

На пересечении строки и столбца можно записывать «$+$» или «$-$» в зависимости от того, принадлежит или не принадлежит функция, которой помечена эта строка, к классу, которым помечен этот столбец.

По теореме Поста система A — полна, если в этой таблице в каждом столбце найдется хотя бы один «минус», и не полна, если в этой таблице найдется столбец, состоящий только из «плюсов».

Теорема Поста

Пример. Проверить, является ли полной система

$$A = \{\bar{x}, x \to y\}.$$

Применим теорему Поста:

	T_0	T_1	L	S	M
$\bar{x}$	$-$	$-$	$+$	$+$	$-$
$x \to y$	$-$	$+$	$-$	$-$	$-$

Значит, A — полная система.

Теорема Поста

Пример. Проверить, является ли полной система

$$A = \{\bar{x}, x \sim y\}.$$

Применим теорему Поста:

	T_0	T_1	L	S	M
$\bar{x}$	$-$	$-$	$+$	$+$	$-$
$x \sim y$	$-$	$+$	$+$	$-$	$-$

Значит, A — неполная система, т. к. $A \subseteq L$.

Конец лекции