Лекция 1. Двоичный куб. Функции алгебры логики. Таблицы истинности. Существенность переменных. Формулы. Тождества.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте https://mk.cs.msu.ru

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 $\alpha_j = (\alpha_{j,1}, \ldots, \alpha_{j,n})$.

Множество E_2^n

Пример.

1. Пусть $n = 2$. Перечислим все наборы из множества E_2^2:

$$(0,0), \quad (0,1), \quad (1,0), \quad (1,1).$$

Всего найдется 4 набора в множестве E_2^2.

2. Пусть $n = 3$. Перечислим все наборы из множества E_2^3:

$$\begin{array}{cccc} (0,0,0), & (0,0,1), & (0,1,0), & (1,0,0), \\ (0,1,1), & (1,0,1), & (1,1,0), & (1,1,1). \end{array}$$

Всего найдется 8 наборов в множестве E_2^3.

Мощность множества E_2^n

Предложение 1.1. *Если $n \geqslant 1$, то $|E_2^n| = 2^n$.*

Доказательство.
Рассмотрим произвольный набор $\alpha = (\alpha_1, \ldots, \alpha_n) \in E_2^n$.
Подсчитаем, сколькими способами можно построить такой набор α.
Каждый его разряд α_i, где $i = 1, \ldots, n$, равен одному из двух значений (0 или 1), причем вне зависимости от значений других разрядов.
Поэтому число способов построить набор из E_2^n (а значит, и число наборов в E_2^n) равно 2^n.
Следовательно, $|E_2^n| = 2^n$.

$\square$

Лексико-графический порядок на E_2^n

Номером $(\alpha_1, \ldots, \alpha_n)_2$ набора $\alpha \in E_2^n$ назовем целое неотрицательное число, для которого запись в двоичной системе счисления имеет вид $\alpha_1 \ldots \alpha_n$.

Другими словами,

$$(\alpha_1, \ldots, \alpha_n)_2 = \sum_{i=1}^{n} \alpha_i \cdot 2^{n-i}.$$

Отметим, что $0 \leqslant (\alpha_1, \ldots, \alpha_n)_2 \leqslant 2^n - 1$.

(Линейное) упорядочивание наборов из E_2^n в порядке возрастания их номеров назовем **лексико-графическим** (или **алфавитным**) порядком на E_2^n.

Лексико-графический порядок на E_2^n

Пример. Перечислим все наборы из E_2^3 в лексико-графическом порядке. В следующей таблице в левом столбце указаны числа от 0 до $7 = 2^3 - 1$, а в правом столбце — соответствующие наборы из E_2^3:

$(\alpha_1, \alpha_2, \alpha_3)_2$	$\alpha \in E_2^3$
0	$(0,0,0)$
1	$(0,0,1)$
2	$(0,1,0)$
3	$(0,1,1)$
4	$(1,0,0)$
5	$(1,0,1)$
6	$(1,1,0)$
7	$(1,1,1)$

Функция алгебры логики

Пусть $E_2 = \{0, 1\}$. **Функцией алгебры логики** называем произвольное отображение из E_2^n в E_2, $n \geqslant 1$.

Т. е. если $f : E_2^n \to E_2$, то f — *n-местная функция алгебры логики*.

При этом если $f = f(x_1, \dots, x_n)$, то говорим, что f — функция n переменных $x_1, \dots, x_n$.

Иногда константы $0, 1$ будем считать *0-местными функциями алгебры логики* (т. е. функциями без переменных).

Функции алгебры логики

Множество всех функций алгебры логики, зависящих от n переменных, обозначим $P_2^{(n)}$.

Множество всех функций алгебры логики обозначаем P_2, т. е. $P_2 = \bigcup\limits_{n \geqslant 1} P_2^{(n)}$.

Таблица истинности

Как можно задавать функции алгебры логики?

1. Таблицы истинности (таблицы значений). 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	$\ldots$	x_{n-1}	x_n	$f(x_1, \ldots, x_{n-1}, x_n)$
0	$\ldots$	0	0	$f(0, \ldots, 0, 0)$
0	$\ldots$	0	1	$f(0, \ldots, 0, 1)$
	$\ldots$			
1	$\ldots$	1	0	$f(1, \ldots, 1, 0)$
1	$\ldots$	1	1	$f(1, \ldots, 1, 1)$

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 имеют собственные названия.

$n = 0$: **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	$x_1 \& x_2$	$x_1 \vee x_2$	$x_1 \oplus x_2$	$x_1 \to x_2$	$x_1 \sim x_2$	x_1 / x_2	$x_1 \downarrow x_2$
0	0	0	0	0	1	1	1	1
0	1	0	1	1	1	0	1	0
1	0	0	1	1	0	0	1	0
1	1	1	1	0	1	1	0	0

Слева направо по порядку: **конъюнкция**, **дизъюнкция**, **сложение по модулю** 2, **импликация**, **эквивалентность**, **штрих Шеффера**, **стрелка Пирса**.

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

Знаки $\bar{\ }$, $\&$, $\cdot$, $\vee$, $\oplus$, $\to$, $\sim$, $/$, $\downarrow$ 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 **функцией голосования**, или **медианой**.

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.

Существенная переменная

Введем 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

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

Другими словами, переменная x_i — существенна для функции $f \in P_2$, если найдутся два соседних по i-му разряду набора, на которых функция f принимает различные значения.

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 принимает два значения: и 0, и 1 (т. е. не является константой).

Несущественная переменная

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

Как правило, мы будем рассматривать функции с точностью до несущественных переменных.

Т. е. будем считать, что несущественные переменные можно добавлять и убирать.

Существенные переменные

Пример. Добавим к функции $f(x)$ несущественную переменную y:

x	$f(x)$
0	0
1	1

,

x	y	$g(x,y)$
0	0	0
0	1	0
1	0	1
1	1	1

Получаем функцию $g(x,y)$.

Существенные переменные

Пример (продолжение). Проверим, что для функции $g(x, y)$ переменная y является несущественной:

x	y	$g(x, y)$
0	0	0
0	1	0
1	0	1
1	1	1

Действительно,

1) если $x = 0$, то $g(0, 0) = g(0, 1) = 0$;
2) если $x = 1$, то $g(1, 0) = g(1, 1) = 1$.

Переменная y — несущественна для функции g, а значит, ее можно убрать.

Существенные переменные

Пример (продолжение). Уберем из функции $g(x,y)$ несущественную переменную y:

x	y	$g(x,y)$
0	0	0
0	1	0
1	0	1
1	1	1

,

x	$f(x)$
0	0
1	1

Получаем функцию $f(x)$.

Равенство функций алгебры логики

Равенство функций рассматриваем с точностью до несущественных переменных.

Функции $f \in P_2$ и $g \in P_2$ назовем **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 одно и то же значение.

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

Переименование переменных

Пример. Рассмотрим функции $f(x,y)=x$ и $g(x,y)=y$.

Функции f и g не равны:

x	y	$f(x,y)$	$g(x,y)$
0	0	0	0
0	1	0	1
1	0	1	0
1	1	1	1

Например, $f(0,1)\neq g(0,1)$.

Но можно заметить, что функция g получается из функции f переименованием переменных.

Конгруэнтность функций алгебры логики

Функции $f \in P_2$ и $g \in P_2$ называются **конгруэнтными**, если переменные одной из них можно так переобозначить (при этом разные переменные переобозначаются по-разному), что получится функция, равная другой.

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

Число функций алгебры логики n переменных

Предложение 1.2. *При $n \geqslant 1$ верно равенство:* $|P_2^{(n)}| = 2^{2^n}$.

Доказательство.
Любую функцию $f \in P_2^{(n)}$ можно представить таблицей истинности, в которой 2^n строк.
В каждой строке (вне зависимости от других строк) находится 0 или 1 (значение f на соответствующем наборе).
Функций в $P_2^{(n)}$ столько же, сколько таких таблиц истинности.
Следовательно, $|P_2^{(n)}| = 2^{2^n}$.

$\square$

Формула

3. Функции алгебры логики можно задавать **формулами**.

Считаем, что задано некоторое счетно бесконечное множество переменных $X = \{x_1, x_2, \ldots\}$.

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

Определим **формулы** над множеством A.

Формула

Формула над множеством A определяется по индукции.

Базис индукции. Если f — обозначение m-местной функции из A и $x_1, \ldots, x_m$ — переменные (из X), причем не обязательно различные, то выражение $f(x_1, \ldots, x_m)$ — формула.

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.

Формула

Отметим, что если множество A содержит тождественную функцию, то базис индукции можно записать проще.

Базис индукции. Если x_i — переменная (из X), то выражение x_i — формула.

Формулы со связками

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

При построении формулы над A в таком случае записываем выражения следующим образом:

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

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

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

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 $x \oplus y \in A$ и формул F_1 и F_2;
$F_4 = (x \oplus y) \cdot x$	формула, построенная по индуктивному переходу из функции $x \cdot y \in A$ 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.

Формулы

Пусть F — формула над множеством A, $A \subseteq P_2$.

Если в формуле F встречаются только переменные $x_1, \ldots, x_n$ (но не обязательно все), то будем записывать $F(x_1, \ldots, x_n)$.

Если при построении формулы F применялись только функции $g_1, \ldots, g_t \in A$ (но не обязательно все), то будем записывать $F[g_1, \ldots, g_t]$.

Функция, определяемая формулой

Пусть $F(x_1, \ldots, x_n)$ — формула над множеством A, $A \subseteq P_2$.

Тогда формула F задает некоторую **функцию** $f_F \in P_2$ переменных $x_1, \ldots, x_n$ (возможно, зависящую не от всех переменных существенно).

Функция, определяемая формулой

Значение функции $f_F(x_1, \ldots, x_n)$ на наборе $\alpha \in E_2^n$ определяется по индукции.

Базис индукции. Если $F = x_i$, где x_i — переменная, то

$$f_F(\alpha) = \alpha_i.$$

Индуктивный переход. Если $F = f(F_1, \ldots, F_m)$, где f — обозначение m-местной функции из A и $F_1, \ldots, F_m$ — формулы или переменные, то

$$f_F(\alpha) = f(f_{F_1}(\alpha), \ldots, f_{F_m}(\alpha)).$$

При этом пользуемся тем, что f обозначает какую-то функцию из A.

Функция, определяемая формулой

Другими словами:

1) если $F = x_i$, где x_i — переменная, то $f_F(x_i) = x_i$, т. е. f_F — функция, тождественно равная переменной x_i;

2) если $F = f(F_1, \dots, F_m)$, где f — обозначение m-местной функции из A и $F_1, \dots, F_m$ — формулы или переменные, то

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

т. е. f_F является соответствующей композицией функций $f \in A$ и $f_{F_1}, \dots, f_{F_m}$.

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.

Т. е. формулы F_1 и F_2 — **эквивалентны**, если на любом наборе значений переменных, входящих в формулы F_1 и F_2, функции f_{F_1} и f_{F_2} принимают одинаковые значения.

Обозначение эквивалентных формул: $F_1 = F_2$; при этом равенство $F_1 = F_2$ называется **тождеством**.

Тождества алгебры логики

Верны следующие тождества:

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

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

3) дистрибутивность видов

$$(x \vee y) \cdot z = x \cdot z \vee y \cdot z;$$
$$(x \cdot y) \vee z = (x \vee z) \cdot (y \vee z);$$
$$(x \oplus y) \cdot z = x \cdot z \oplus y \cdot z.$$

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:

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

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.

Доказываются эти тождества построением функций, определяемых формулами в левой и правой частях равенства.

Правила тождественной замены

Пусть F и G — формулы, причем

$$F = f(F_1, \dots, F_m), \quad G = f(G_1, \dots, G_m),$$

где f — обозначение m-местной функции, а $F_1, \dots, F_m$ и $G_1, \dots, G_m$ — формулы.

Тогда если $F_1 = G_1, \dots, F_m = G_m$, то $F = G$.

Правила тождественной замены

Пусть F формула, причем

$$F = f(F_1, \ldots, F_m),$$

где f — обозначение m-местной функции, а $F_1, \ldots, F_m$ — формулы.

Пусть $H(y_1, \ldots, y_m)$ — формула, определяющая функцию f, и

$$G = H(F_1, \ldots, F_m),$$

т. е. в формулу H вместо переменной y_i подставляем формулу F_i для всех $i = 1, \ldots, m$.

Тогда $F = G$.

Эквивалентные преобразования формул

Пользуясь правилами тождественной замены, можно от одних представлений функций алгебры логики переходить к другим их представлениям.

При этом говорят, что выполняют эквивалентные преобразования формул.

Эквивалентные преобразования формул

Пример. Рассмотрим формулу $F_1 = (\bar{x}_1 \vee \bar{x}_2) \cdot (x_1 \vee x_2)$.

Применим тождество $\bar{x} \vee \bar{y} = \overline{x \cdot y}$:

$$F_1 = (\bar{x}_1 \vee \bar{x}_2) \cdot (x_1 \vee x_2) \quad = \quad (\overline{x_1 \cdot x_2}) \cdot (x_1 \vee x_2) = F_2.$$

Далее применим тождество $x \cdot y = \overline{\bar{x} \vee \bar{y}}$:

$$F_2 = \overline{(x_1 \cdot x_2)} \cdot (x_1 \vee x_2) \quad = \quad \overline{\overline{\overline{(x_1 \cdot x_2)}} \vee \overline{(x_1 \vee x_2)}} = F_3.$$

Затем применим тождество $\bar{\bar{x}} = x$:

$$F_3 = \overline{\overline{\overline{(x_1 \cdot x_2)}} \vee \overline{(x_1 \vee x_2)}} \quad = \quad \overline{(x_1 \cdot x_2) \vee \overline{(x_1 \vee x_2)}} = F_4.$$

Теперь применим тождество $\overline{x \vee y} = \bar{x} \cdot \bar{y}$:

$$F_4 = \overline{(x_1 \cdot x_2) \vee \overline{(x_1 \vee x_2)}} \quad = \quad \overline{(x_1 \cdot x_2) \vee (\bar{x}_1 \cdot \bar{x}_2)} = F_5.$$

При этом $F_1 = F_2$, $F_2 = F_3$, $F_3 = F_4$, $F_4 = F_5$, т. е. все эти формулы задают одну и ту же функцию $f(x_1, x_2) \in P_2$.

Задачи для самостоятельного решения

1. Покажите, что таблицу всех наборов из E_2^n, $n \geqslant 1$, в лексикографическом порядке можно построить следующим способом: для каждого $i = 1, \ldots, n$, начиная с первой строки таблицы, повторить 2^{i-1} раз: в i-м разряде в 2^{n-i} строках написать 0, затем в следующих 2^{n-i} строках написать 1.

Литература к лекции

1. Алексеев В. Б. Лекции по дискретной математике. М.: Инфра-М, 2012. С. 4–8.

2. Марченков С. С. Основы теории булевых функций. М.: Физматлит, 2014. С. 11–20.

3. Яблонский С. В. Введение в дискретную математику. М.: Высшая школа, 2001. С. 9–23.

4. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004. С. 9–10. Гл. I 1.1–1.5, 1.17, 1.19, 1.20, 1.28, 1.30, 1.31, 1.33, 1.34, 1.35.