Лекция 2. Булевы функции

1 Булевы функции

Булевы функции определяются на множестве, состоящем из двух элементов. В качестве такого множества удобно рассмотреть множество $0, 1$, которое обозначается E_2.

Определение 1: Булева функция

Булевой функцией от n переменных называют произвольное отображение вида

$$f : \{0, 1\}^n \to \{0, 1\}.$$

Множество всех булевых функций обозначается как P_2, а множество всех булевых функций от n переменных как $P_2^{(n)}$.

Булева функция $f(x_1, x_2, \ldots, x_n)$ является отображением n-ой декартовой степени множества E_2 в множество E_2, поэтому её можно задать с помощью таблицы.

x_1	x_2	$\ldots$	x_n	$f(x_1, x_2, \ldots, x_n)$
0	0	$\ldots$	0	$f(0, 0, \ldots, 0)$
0	0	$\ldots$	1	$f(0, 0, \ldots, 1)$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	1	$\ldots$	0	$f(1, 1, \ldots, 0)$
1	1	$\ldots$	1	$f(1, 1, \ldots, 1)$

Таблица 1: Табличное задание булевой функции

Заметим, что все 2^n наборов в левом столбце записывают в лексикографическом порядке, а значит для всех булевых функций от n переменных этот столбец будет одинаков.

Отсюда следуют два утверждения:

- Всякую булеву функцию от n переменных можно задать двоичным столбцом высоты 2^n.
- Всякий двоичный столбец высоты 2^n задаёт булеву функцию от n переменных.

Стало быть мы можем говорить о взаимно однозначном соответствии между множеством $P_2^{(n)}$ и множеством всех двоичных наборов длины 2^N, откуда следует, что число булевых функций от n переменных равно 2^{2^n}.

Рассмотрим булевы функции от одной переменной.

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	0	1	1
1	0	1	0	1

Таблица 2: Булевы функции одной переменной

При этом заметим:

- Функции $f_1(x)$ и $f_2(x)$ называются константами 0 и 1, а при обозначении так и пишут 0 и 1 не указывая явно переменную x.
- Значения функции $f_2(x)$ совпадает со значениями переменной x, поэтому её называют тождественной и при обозначении часто пишут лишь символ переменной x.
- Функция $f_3(x)$ осуществляет инвертирование значения переменной x, поэтому её называют отрицанием и обозначают $\overline{x}$.

Название		Дизъюнкция	Конъюнкция	Сложение по модулю 2	Импликация	Эквивалентность	Штрих Шеффера	Стрелка Пирса
Обозначение		$x_1 \vee x_2$	$x_1 \wedge x_2$	$x_1 \oplus x_2$	$x_1 \to x_2$	$x_1 \sim x_2$	$x_1 \mid x_2$	$x_1 \downarrow x_2$
x_1	x_2	$f_1(x_1, x_2)$	$f_2(x_1, x_2)$	$f_3(x_1, x_2)$	$f_4(x_1, x_2)$	$f_5(x_1, x_2)$	$f_6(x_1, x_2)$	$f_7(x_1, x_2)$
0	0	0	0	0	1	1	1	1
0	1	1	0	1	1	0	1	0
1	0	1	0	1	0	0	1	0
1	1	1	1	0	1	1	0	0

Таблица 3: Некоторые булевы функции двух переменных

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
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

Таблица 4: Булева функция трёх переменных

Булевых функций от двух переменных будет уже $2^{2^2} = 16$, но ограничимся рассмотрением лишь 7 наиболее важных. Приведём эти функции в таблице 3.

В качестве булевой функции трёх переменных в таблице 4 приведём лишь один пример – мажорирующую функцию или функцию голосования.

Определение 2: Существенная зависимость

Функция $f(x_1, \ldots, x_i \ldots, x_n)$ существенно зависит от переменной x_i, если найдутся такие значения $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, что

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

Если функция $f(x_1, \ldots, x_i \ldots, x_n)$ существенно зависит от переменной x_i, то переменная x_i называется существенной переменной функции $f(x_1, \ldots, x_i \ldots, x_n)$. В противном случае переменная называется несущественной или фиктивной.

В качестве примера рассмотрим функции $f(x, y) = x \vee y$ и $g(x, y, z) = xz \vee x\overline{z} \vee yz \vee y\overline{z}$.

Заметим, что используя тождества булевой алгебры можно записать, что

$$g(x, y, z) = (x \vee y)(z \vee \overline{z}),$$

но так как $z \vee \overline{z} = 1$, то

$$g(x, y, z) = x \vee y = f(x, y),$$

поэтому функции f и g естественно рассматривать как равные, несмотря на то, что они зависят от разного числа переменных.

2 Формулы

Хотя табличный способ задания булевых функция является универсальным, не практике он не является удобным, поэтому ставится вопрос о формульном задании булевых функций.

В теории булевых функций ставится задача представления булевой функции такой формулой, которая бы содержала строго определённое конечное множество элементарных булевых функций – главным образом тех, что мы определили ранее – функций одной и двух переменных. Иными словами, мы хотим определить нечто вроде функционального базиса, через элементы которого можно было бы выразить любую булеву функцию.

Стоит отметить, что одна и та же булева функция может быть представлена, вообще говоря, различными формулами как над одним и тем же базисом, так и над разными базисами. Для того, чтобы аккуратно определить механизм эквивалентного преобразования формул, необходимо уточнить понятие формулы.

Пусть задано непустое множество F булевых функций. Введём понятие формулы, составленной из символов функций множества F.

Определение 3: Формулы над множеством F

Пусть f – обозначение функции от n переменных из множества F, а $x_1, \dots, x_n$ – символы переменных. Тогда выражение

$$f(x_1, \dots, x_n)$$

считаем формулой над F.
Пусть также g – обозначение функции от m переменных из множества F, а $A_1, \dots, A_m$ – либо формулы над F, либо символы переменных (необязательно различные).
Тогда выражение

$$g(A_1, \dots, A_m)$$

считаем формулой над F.

В качестве примера определим множество F как

$$F = \{\bar{\ }, \vee, \wedge, \ , \oplus, \to, |\},$$

тогда следующие выражения будут являться формулами над F:

$$\overline{x}_1, \quad (x_1 \vee x_2) \wedge x_3, \quad \overline{(x_1 \oplus x_2)}|x_3, \quad x_1 \to (x_1 \vee x_3).$$

Определение 4: Эквивалентность формул

Формулы Φ и Ψ называются эквивалентными, если они реализуют одну и ту же булеву функцию.
Этот факт записывается как $\Phi = \Psi$.

Запишем наиболее употребительные эквивалентности для функций, определённых ранее.

1. $\overline{1} = x \wedge 0 = x \wedge \overline{x} = x \oplus x = 0$.
2. $\overline{0} = x \vee 1 = x \vee \overline{x} = x \to x = 1$.
3. $\overline{\overline{x}} = x \wedge x = x \vee x = x \wedge 1 = x \vee 0 = x \oplus 0 = x$.
4. $x \oplus 1 = x \to 0 = x|x = \overline{x}$.
5. $x \circ y = y \circ x$, где $\circ$ – любая из функций $\vee, \wedge, \oplus, |$ (коммутативность функции $\circ$).
6. $(x \circ y) \circ z = x \circ (y \circ z)$, где $\circ$ – любая из функций $\vee, \wedge, \oplus$ (ассоциативность функции $\circ$).
7. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ (дистрибутивность конъюнкции относительно дизъюнкции).
8. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ (дистрибутивность дизъюнкции относительно конъюнкции).
9. $x \wedge (y \oplus z) = (x \wedge y) \oplus (x \wedge z)$ (дистрибутивность конъюнкции относительно сложения по модулю 2).
10. $\overline{x \wedge y} = \overline{x} \vee \overline{y}$, $\overline{x \vee y} = \overline{x} \wedge \overline{y}$ (правила де Моргана).

11. $x \vee (x \wedge y) = x \wedge (x \vee y) = x$, $x \vee (\overline{x} \wedge y) = x \vee y$, $x \wedge (\overline{x} \vee y) = x \wedge y$ (правила поглощения).

12. $x \oplus y = (\overline{x} \wedge y) \vee (x \wedge \overline{y}) = (x \vee y) \wedge (\overline{x} \vee \overline{y})$,
    $x \vee y = ((x \wedge y) \oplus x) \oplus y = \overline{x} \to y$,
    $x \to y = \overline{x} \vee y = ((x \wedge y) \oplus x) \oplus 1$,
    $x | y = \overline{x \wedge y}$.

Справедливость этих эквивалентностей можно проверить непосредственно с помощью таблиц истинности.

Если формула содержит множество символов различных функций, то при отсутствии дополнительных скобок вначале выполняют конъюнкцию, затем сложение по модулю 2, после дизъюнкцию затем импликация или штрих Шеффера.

Например, формулу

$$\overline{x} \wedge y \oplus z \to \overline{y} \wedge z \vee \overline{x}$$

следует понимать как

$$((\overline{x} \wedge y) \oplus z) \to ((\overline{y} \wedge z) \vee \overline{x}).$$

Определение 5

Множество булевых функций F называют:

- замкнутым, если любая формула над F представляет некоторую функцию из F;
- полным, если любая булева функция может быть представлена некоторой формулой над F.

3 Разложение булевой функции по переменным

Теорема 1: О разложении по первой переменной

Для любой булевой функции $f(x_1, \dots, x_n)$ справедливо представление

$$f(x_1, \dots, x_n) = x_1 \cdot f(1, x_2, \dots, x_n) \vee \overline{x}_1 \cdot f(0, x_2, \dots, x_n).$$

Доказательство

Рассмотрим произвольный двоичный набор $a = (a_1, \dots, a_n)$ и сравним значения левой и правой частей доказываемого представления.

- В левой части имеем $f(a)$.
- Если $a_1 = 0$, то выражение $a_1 \cdot f(1, a_2, \dots, a_n)$ обращается в 0, откуда получим
$$\overline{a}_1 \cdot f(0, a_2, \dots, a_n) = \overline{0} \cdot f(a_1, a_2, \dots, a_n) = 1 \cdot f(a_1, a_2, \dots, a_n) = f(a).$$
- Если же $a_1 = 1$, то выражение $\overline{a}_1 \cdot f(0, x_2, \dots, x_n)$ обращается в 0, тогда
$$a_1 \cdot f(1, a_2, \dots, a_n) = 1 \cdot f(a_1, a_2, \dots, a_n) = f(a).$$

Отметим, что аналогичным образом можно рассмотреть разложение по любой переменной.

Пусть $n \geq 2$, применим указанную теорему к функциям $f(1, x_2, \dots, x_n)$ и $f(0, x_2, \dots, x_n)$ и переменной x_2. Получим представление

$$f(x_1, \dots, x_n) = x_1 \cdot x_2 \cdot f(1, 1, \dots, x_n) \vee x_1 \cdot \overline{x}_2 \cdot f(1, 0, \dots, x_n) \vee \overline{x}_1 \cdot x_2 \cdot f(0, 1, \dots, x_n) \vee \overline{x}_1 \cdot \overline{x}_2 \cdot f(0, 0, \dots, x_n).$$

Если ввести обозначения $x^1 = x$, $x^0 = \overline{x}$ и продолжить рассуждения, можно получить следующее утверждение.

Следствие 1: О разложении по первым m переменным

Для любой функции $f(x_1, \dots, x_n)$ и любого m $(1 \leq m \leq n)$ справедливо представление

$$f(x_1, \dots, x_n) = \bigvee_{(\sigma_1, \dots, \sigma_m)} x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} \cdot f(\sigma_1, \dots, \sigma_m, x_{m+1}, \dots, \sigma_n).$$

Особый интересный вид следствие 1 принимает в случае, когда $m = n$. Тогда каждое дизъюнктивное слагаемое имеет вид

$$x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} \cdot f(\sigma_1, \dots, \sigma_n).$$

При этом:

- если $f(\sigma_1, \dots, \sigma_n) = 0$, то всё слагаемое равно нулю и его можно опустить (за исключением случая, когда функция f тождественно равна нулю, тогда вся формула в следствии 1 вырождается в константу);
- если $f(\sigma_1, \dots, \sigma_n) = 1$, то вместо $x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} \cdot f(\sigma_1, \dots, \sigma_n)$ можно записать эквивалентную формулу $x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$.

Таким образом мы приходим к утверждению.

Следствие 2: О разложении по всем переменным

Если булева функция $f(x_1, \dots, x_n)$ не равна тождественно нулю, то справедливо представление

$$f(x_1, \dots, x_n) = \bigvee_{f(\sigma_1, \dots, \sigma_n)=1} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}.$$

Правая часть выражения в следствии 2 носит название совершенной дизъюнктивной нормальной формы (СДНФ).

Следствие 2 показывает, что любую не равную тождественно 0 булеву функцию можно представить в виде дизъюнкции конъюнкций одинаковой длины, составленных из переменных $x_1, \dots, x_n$ и их отрицаний.

СДНФ относится к более общему классу формул над множеством $\{\bar{\ }, \vee, \wedge\}$, которые носят название дизъюнктивных нормальных форм (ДНФ). В отличие от СДНФ в ДНФ конъюнкции могут состоять из различных переменных и иметь различную длину.