БУЛЕВЫ ФУНКЦИИ. СВЯЗЬ БУЛЕВЫХ ФУНКЦИЙ С ФОРМУЛАМИ АЛГЕБРЫ ВЫСКАЗЫВАНИЙ.

Булевы функции

Определение: Функциями алгебры логики (или булевыми функциями называются функции $f{:}E^n \to E$, *где* $E=\{0,1\}$.
Если

X_1

$$\beta(X_1)=\begin{cases}1, & \text{если } X_1 - \text{истинно}\\ 0, & \text{если } X_1 - \text{ложно}\end{cases} \Rightarrow x_1=\beta(X_1)$$ - булева переменная:

$\beta(A)$	$\beta(B)$	$\beta(\overline{A})$	$\beta(A \vee B)$	$\beta(A \oplus B)$	$\beta(A \to B)$	$\beta(A \wedge B)$
0	0	1	0	0	1	0
0	1	1	1	1	1	0
1	0	0	1	1	0	0
1	1	0	1	0	1	1

Причем, $\beta(A \vee B) = \beta(A) \vee \beta(B)$, где $(A \vee B)$ - дизъюнкция высказывания, а $\beta(A) \vee \beta(B)$ - дизъюнкции булевых функций.

<u>Лемма 1.</u> Для любых высказываний A и B:

$$\beta(\neg A) = \neg\beta(A)$$
$$\beta(A \vee B) = \beta(A) \vee \beta(B)$$
$$\beta(A \wedge B) = \beta(A) \wedge \beta(B)$$
$$\beta(A \to B) = \beta(A) \to \beta(B)$$
$$\beta(A \equiv B) = \beta(A) \equiv \beta(B)$$

Каждая формула логики высказываний канонически(естественным образом) порождает булеву функцию.

$$\beta((X_1 \vee X_2) \to X_1) = (\beta(X_1) \vee \beta(X_2)) \to \beta(X_1) = (x_1 \vee x_2) \to x_1$$

1. Связь булевых функций с формулами алгебры высказываний

Теорема 1. Всякая формула алгебры высказываний естественным образом (канонически) порождает некоторую булеву функцию, т.е. если A - некоторая формула, в которую входят высказывательные переменные $X_1, \ldots, X_n$ и только они, тогда канонически порожденная булева функция $a(x_1, x_2, \ldots, x_n) = \beta(A)$, где $x_i = \beta(X_i)$

Доказательство: проведем методом математической индукции по $n(A)$- количеству символов в слове A. Минимальное количество символов в формуле равно 1, т.к. пустое множество не является формулой.

Пусть $n(A) = 1, \Rightarrow A = X_i$ - высказывательная переменная, $\beta(X_i) = x_i$.

Пусть нам известно, что для всех формул у которых $n(A) \leq k$, где $k \in N$ утверждение теоремы 6 истинно. Докажем, что для формул, у которых $n(A) = k + 1$, оно тоже будет истинно.

Возьмем произвольную формулу F, у которой $(k+1)$ символов. Тогда $F = \neg A$, или $F = A \vee B$, или $F = A \wedge B$, или $F = A \rightarrow B$. Формулы A и B содержат меньше символов, чем формула F, т.е. $n(A) \leq k$ и $n(B) \leq k$, но для этих формул утверждение теоремы 1 истинно. Согласно индуктивному предположению формулы A и B канонически порождают булевы функции соответственно $a(x_1, x_2, \ldots, x_n)$ и $b(x_1, x_2, \ldots, x_n)$.

Так для $F = \neg A$, то согласно утверждению леммы 1 имеем:

$$\beta(F) = \beta(\neg A) = \neg\beta(A) = \neg a(x_1, x_2, \ldots, x_n)$$

Аналогично показывается это утверждение для остальных случаев. □

1. Связь булевых функций с формулами алгебры высказываний

Пример.

$$F = \neg X_1 \vee X_2$$

$$f(x_1, x_2) = \neg x_1 \vee x_2$$

Верна и обратная теорема.

Теорема 2. Для любой булевой функции $f(x_1, x_2, ..., x_n)$ существует высказывательная формула F, в которую входят высказывательные переменные $X_1, X_2, ..., X_n$, канонически порождающая функцию f.

3. Способы представления булевых функций.

1) Задание булевых функций формулами.
2) Табличное задание.
3) Геометрическое задание.

Множество наборов I_f значений переменных, на которых функция принимает значение 1, называется множеством истинности булевой функции. Порядок множества I_f называется весом б.ф. и обозначается $\|f\|$.

Для любых f и g выполнено:

$I_{\bar{f}} = V_n \setminus I_f$; $I_{f\cdot g} = I_f \cap I_g$; $I_{f\vee g} = I_f \cup I_g$

$\|\bar{f}\| = 2^n - \|f\|$; $\|f \vee g\| = \|f\| + \|g\| - \|f\cdot g\|$; $\|f \oplus g\| = \|f\| + \|g\| - 2\cdot\|f\cdot g\|$

Геометрическое задание б.ф. от n переменных – это изображение n-мерного куба со множеством вершин V_n, в котором выделены вершины множества I_f.

Графическое задание б.ф. реализуется неориентированным графом со множеством вершин I_f, в котором ребрами соединены соседние пары наборов.

4) В виде канонических форм. К каноническим формам относят СДНФ, СКНФ, АНФ.
5) В виде многочлена над полем действительных чисел.

Данное представление можно получить, используя равенства:

$x_1 \vee x_2 = x_1 + x_2 - x_1 \cdot x_2$; $x_1 \wedge x_2 = x_1 \cdot x_2$; $x_1 \oplus x_2 = x_1 + x_2 - 2\cdot x_1 \cdot x_2$; $\bar{x} = 1 - x$.

<u>Теорема 3.</u> Любая б.ф. однозначно представляется в виде действительного полинома, все коэффициенты которого являются целыми числами, а каждая переменная входит в полином в степени не выше первой.

1) Спектральное представление.

Поставим в соответствие двоичному вектору a = $(a_1,a_2,\ldots,a_n)\in V_n$ линейную б.ф. (a,x) = $a_1 \cdot x_1 \oplus \ldots \oplus a_n \cdot x_n$ и определим на V_n функцию $(-1)^{(a,x)}$ с действительными значениями:

$$(-1)^{(a,x)} = \begin{cases} 1, & (a,x)=0 \\ -1, & (a,x)=1 \end{cases}$$

<u>Теорема 4</u> (о разложении в ряд Фурье). Для любой б.ф. имеется единственное разложение вида

$$f(x) = 2^{-n} \cdot \sum_{a\in V_n} c_a^f \cdot (-1)^{(a,x)}$$

, где x = $(x_1,x_2,\ldots,x_n)\in V_n$ и коэффициенты c_a^f являются целыми числами, определяемыми равенствами:

$$c_a^f = \sum_{x\in V_n} f(x)\cdot(-1)^{(a,x)}$$

.

Вектор коэффициентов $C(f) = (c_a^f)$, a$\in V_n$ называется спектром Фурье, а его координаты-коэффициентами Фурье б.ф. f(x). Преобразование вектора табличного задания б.ф. f(x) в спектр Фурье называют преобразованием Фурье б.ф. f(x). Это преобразование задается матрицей H2n, называемой матрицей Адамара.

Наряду с б.ф. f(x) рассматривают ее действительно-значный аналог fd(x) где: fd(x)=(-1)f(x).

Преобразование вектора табличного задания функции f(x) с помощью матрицы H2n называется преобразованием Адамара -Уолша б.ф. f(x). Получаемый вектор коэффициентов $Z(f) = (z_a^f)$, a$\in V_n$,наз. спектром Уолша, а его координаты-коэффициентами Уолша б.ф. f(x):

Спектры Фурье и Уолша всякой б.ф. взаимосвязаны.

<u>Теорема 5.</u> Для всякой б.ф. f(x) и любого a$\in$Vn,

$$z_a^f = \begin{cases} -2\cdot c_a^f, & a \neq 0 \\ 2^n - 2\cdot c_a^f, & a = 0 \end{cases}$$

4. Разложение булевых функций по переменным

Определение: Булева функция существенно зависит от переменной x_i, если существует такой набор значений $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$, что

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

В этом случае переменная x_i называется существенной, в противном случае – несущественной (фиктивной).

Используем далее обозначение $x^{\sigma} = \begin{cases} \overline{x}, & \sigma = 0 \\ x, & \sigma = 1 \end{cases}$, $1^{\sigma} = \begin{cases} 0, & \sigma = 0 \\ 1, & \sigma = 1 \end{cases}$, $0^{\sigma} = \begin{cases} 1, & \sigma = 0 \\ 0, & \sigma = 1 \end{cases}$

Теорема 6. (о разложении функции по переменным). Для каждой $f{:}E^n \to E$, где $E=\{0,1\}$, при любом m = 1, 2, …, n справедливо представление:

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

Доказательство. Покажем, что левая и правая части равенства из условия теоремы принимают равные значения при произвольном наборе значений переменных $(a_1, \ldots, a_n)$.

Левая часть равна $f(a_1, \ldots, a_n)$. Правая часть равна

$$\bigvee_{(\sigma_1,\ldots,\sigma_m)\in V_m} a_1^{\sigma_1} \cdot \ldots \cdot a_m^{\sigma_m} \cdot f(\sigma_1,\ldots,\sigma_m, a_{m+1},\ldots,a_n)$$

Так как $a_i^{\sigma_i} = 1$ тогда и только тогда, когда $a_i = \sigma_i$, $i = 1,2,\ldots,m$, то слагаемые, соответствующие наборам $(\sigma_1,\ldots,\sigma_m) \neq (a_1,\ldots,a_m)$, равны 0, а слагаемое, соответствующее набору $(\sigma_1,\ldots,\sigma_m) = (a_1,\ldots,a_m)$, равно $f(a_1,\ldots,a_n)$. □

Следствие 1 (разложение б.ф. по одной переменной):

$$f(x_1, \ldots, x_{n-1}, x_n) = x_n \cdot f(x_1,\ldots,x_{n-1},1) \vee \overline{x_n} \cdot f(x_1,\ldots,x_{n-1},0)$$

Если f не равна константе 0, то спараведливо:

Следствие 2: (разложение б.ф. по всем переменным)

$$f(x_1, \ldots, x_n) = \bigvee_{\substack{(\sigma_1,\ldots,\sigma_n)\in V_n \\ f(\sigma_1,\ldots,\sigma_n)=1}} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$$

Данное представление называют совершенной дизъюнктивной нормальной формой (СДНФ) функции $f(x_1, \ldots, x_n)$, а двойственную формулу, получаемую взаимной заменой констант $0\leftrightarrow1$ и операций $\wedge \leftrightarrow \vee$,- совершенной конъюнктивной нормальной формой (СКНФ).

$$f(x_1, \ldots, x_n) = \bigwedge_{\substack{(\sigma_1,\ldots,\sigma_n)\in V_n \\ f(\sigma_1,\ldots,\sigma_n)=0}} (x_1^{\overline{\sigma_1}} \vee \ldots \vee x_n^{\overline{\sigma_n}})$$

Следствие 3. Каждая б.ф. представима в виде формулы через отрицание, конъюнкцию и дизъюнкцию.

Доказательство. Для функции $f(x_1, \ldots, x_n)$, отличной от константы 0, утверждение вытекает из теоремы 6. Для $f=0$ справедливо: $f = x \cdot \overline{x}$. □

Теорема 7 (И. И. Жегалкин). Каждая б.ф. однозначно представима многочленом по mod2:

$$f(x_1, \ldots, x_n) = \sum_{\{i_1\ldots i_s\}\subseteq\{1\ldots s\}} \oplus \alpha_{i_1\ldots i_s} \cdot x_{i_1} \cdot \ldots \cdot x_{i_s}$$

Так как число таких многочленов от n переменных совпадает с числом различных б.ф., то представление функции полиномом единственно. □

Это представление называется многочленом Жегалкина или Алгебраической нормальной формой (АНФ).

5. Полнота и замкнутость системы функций

Система функций Р = $\{f_1, \dots, f_s, \dots\}$ из P_2 называется (функционально) полной, если любая б.ф. представима формулой над Р. Следующая теорема связывает полноту одних систем с полнотой других систем.

Теорема 8. Пусть система Р = $\{f_1, f_2, \dots\}$ из P_2 полна и каждая ее функция выражается формулой над системой Q = $\{q_1, q_2, \dots\}$ Тогда система Q полна.

Доказательство. Произвольная б.ф. h в силу полноты системы Р выражается суперпозицией функций над Р.

$h = C[f_1, \dots, f_s, \dots]$

По условию теоремы каждая из функций системы Р является в свою очередь суперпозицией функций из Q.

$f_1 = C_1[q_1, q_2, \dots]$, $f_2 = C_2[q_1, q_2, \dots]$, …

В формуле для h исключаем вхождения функций из системы Р, заменяя их формулами над Q. В результате получаем:

$h = C[C_1[q_1, q_2, \dots], C_2[q_1, q_2, \dots], \dots] = C[q_1, q_2, \dots]$. □

Примеры полных систем функций:

1. Система P_2.
2. Система Р=$\{\bar{x}, x_1 \cdot x_2, x_1 \vee x_2\}$, полнота этой системы следует из следствия 2.
3. Система $\{\bar{x}, x_1 \cdot x_2\}$- ее полнота вытекает из примера 2 и теоремы 8, так как $x_1 \vee x_2 = \overline{\bar{x}_1 \cdot \bar{x}_2}$
4. Система $\{\bar{x}, x_1 \vee x_2\}$- ее полнота следует из примера 3 и теоремы 8, так как $x_1 \cdot x_2 = \overline{\bar{x}_1 \vee \bar{x}_2}$
5. Система $\{x_1 / x_2\}$- ее полнота следует из примера 3 и теоремы 8, так как

   $x / x = \bar{x} \vee \bar{x} = \bar{x}$; $(x_1 / x_2)/(x_1 / x_2) = \overline{\bar{x}_1 \vee \bar{x}_2} = x_1 \cdot x_2$
6. Система $\{x, x_1 \cdot x_2, x_1 \oplus x_2\}$- ее полнота следует из примера 3 и теоремы 8, так как $\overline{x_1} = x_1 \oplus 1$