Дискретная математика

Модуль 1.

Математическая логика

Лекция 2.

Авдошин С.М. (email: savdoshin@hse.ru)

Логика высказываний

- Пропозициональные переменные
- Формулы логики высказываний
- Равносильность формул
- Тавтология
- Противоречие
- Выполнимость
- Опровержимость

Пропозициональные переменные

В логике переменным параметрам, входящим в утверждения, естественно приписывать значение $\top$ или $\bot$, получая при этом высказывания. Назовем такие переменные параметры, следуя традиции, *пропозициональными переменными*. Как правило, для краткости пропозициональные переменные именуют просто *переменными*. Будем обозначать их как $X_1, X_2, \ldots, X_n, \ldots$

Индуктивное определение формулы

1) *пропозициональная переменная есть (атомарная) формула;*

2) *если* $\mathcal{A}$ *и* $\mathcal{B}$ *формулы, то* $(\mathcal{A}\&\mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \Rightarrow \mathcal{B})$ *формулы;*

3) *если* $\mathcal{A}$ *формула, то* $\neg\mathcal{A}$ *формула.*

Как видим, при построении формул используются скобки (и). Однако, как часто делается, лишние скобки опускают. К примеру, формулу $((\mathcal{A} \vee \mathcal{B})\&\mathcal{C})$ пишут как $(\mathcal{A} \vee \mathcal{B})\&\mathcal{C}$, а $(\mathcal{A}\&\mathcal{B})$ как $\mathcal{A}\&\mathcal{B}$.

Формулу $\mathcal{A}$, содержащую пропозициональные переменные $X_1, X_2, ..., X_n$, будем обозначать как $\mathcal{A}(X_1, X_2, ..., X_n)$.

Алгебра высказываний

Теория, которая изучает формулы, определенные выше, называется *алгеброй высказываний*. В алгебре высказываний каждая пропозициональная переменная, каждая формула принимает одно из двух *значений* – $\top$ (истина) или $\perp$ (ложь).

Функция $f(X_1, ..., X_n)$ такая, что ее переменные и она сама могут принимать только два значения – $\top$ или $\perp$ – называется *булевой* функцией. Иначе говоря, *булева функция* – это отображение

$$f : \underbrace{\{\perp, \top\} \times ... \times \{\perp, \top\}}_{n-\text{раз}} \to \{\perp, \top\}.$$

Равносильные формулы

$A(X_1, X_2, \dots, X_n)$ и $B(X_1, X_2, \dots, X_n)$ называются равносильными, если они совпадают при любых значениях, входящих в них переменных

Примеры равносильных формул

$$A\&(B\&C) = (A\&B)\&C$$
$$A\&B = B\&A$$
$$A\&A = A$$

Равносильность проверяется с помощью таблиц истинности

$$\overline{A\&\bar{B}} = \bar{A} + B \qquad \bar{A} + B = A \Rightarrow B$$

$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{A\&\bar{B}}$	$\overline{\boldsymbol{A} \,\&\, \bar{\boldsymbol{B}}}$
0	0	0	1
0	1	0	1
1	0	1	0
1	1	0	1

Отношение

Пусть $A_1, A_2, \ldots, A_n$ есть произвольные множества, вообще говоря, разнородные.

Определение. *n-арное отношение* p^n на множествах $A_1, A_2, \ldots, A_n$ есть подмножество p^n декартова произведения $A_1 \times A_2 \times \ldots \times A_n$.

Замечание. n-арное отношение p^n на множестве A есть подмножество p^n натуральной степени множества A^n, $n > 0$. Индекс n арности (местности) отношения p иногда опускается.

Возможна множественная (суффиксная) $(x_1, \ldots, x_n) \in \rho$ и предикатная (префиксная) $\rho(x_1, \ldots, x_n)$ формы записи отношений. В последнем случае отношение ρ называют также предикатом. Для бинарного отношения используется инфиксная запись $x \rho y$. Унарное отношение $\rho \subseteq E$ есть подмножество множества E. Предикат $\rho(x)$, соответствующий унарному отношению, называется свойством.

Набор $a = (a_1, a_2, \ldots, a_n) \in \rho$ (допустима запись $\rho(a_1, a_2, \ldots, a_n)$) называется элементом отношения.

Определение. Отношение *конечно*, если оно состоит из конечного числа элементов.

Отношение эквивалентности

Пусть A есть произвольное множество.

Определение. Бинарное отношение $\sigma \subseteq A \times A$ есть *отношение эквивалентности* (обозначение $a \sim b$), если оно удовлетворяет следующим аксиомам:

1) $a \sim a$, рефлексивность;
2) $a \sim b \rightarrow b \sim a$, симметричность;
3) $a \sim b \ \& \ b \sim c \rightarrow a \sim c$, транзитивность.

Обозначение. $a \sim b$, $\sigma(a, b)$, $(a, b) \in \sigma$, $a \, \sigma \, b$.

Определение. *Разбиение I множества A* есть семейство попарно непересекающихся непустых подмножеств множества A, таких, что: $A = \bigcup_{i \in I} A_i$, $\forall i \neq j$ $(A_i \bigcap A_j = \varnothing)$. Подмножества A_i называются *смежными классами* разбиения I.

Теорема. 1. Каждому отношению эквивалентности, определенному на множестве A, соответствует некоторое разбиение множества A.

2. Каждому разбиению множества A соответствует некоторое отношение эквивалентности, определенное на множестве A.

Коротко: между классом всех определенных на множестве A эквивалентностей и классом всех разбиений множества A существует взаимно-однозначное соответствие.

Классы эквивалентных функций

- $\Delta\{[A]\}$ класс всех формул А по отношению равносильности
- $\neg, \&, \vee, [A]$ – класс равносильных формул
  - $[A] \& [B] = [A \& B]$
  - $[A] \vee [B] = [A \vee B]$
  - $\neg[A] = [\neg A]$

Интерпретация

Интерпретацией I высказывания $A(x_1, x_2, \ldots, x_n)$ называют приписывание значений истинности $(c_1, c_2, \ldots, c_n) \in \{0,1\}^n$ пропозициональным переменным $(x_1, x_2, \ldots, x_n)$.

Для формулы $A(x_1, x_2, \ldots, x_n)$ существует 2^n интерпретаций $I=(c_1, c_2, \ldots, c_n)$.

Кванторы

Введены в логику Чарльзом Сандресом Пирсом.

Пусть $A(x)$ формула, содержащая переменную x.

В формуле $\forall x A(x)$ знак $\forall$ называют ***квантором всеобщности***. Символ $\forall x$ интерпретируется как фраза “для всех x”.

В формуле $\exists x A(x)$ знак $\exists$ называют ***квантором существования***. Символ $\exists x$ интерпретируется как фраза “существует x”.

Свободные и связанные переменные

Переменная x, входящая в формулу A, называется *связанной,* если она находится под действием квантора $\forall x$ или $\exists x$. В противном случае переменная x в формуле A называется *свободной*.

Пример. В формулах $\exists x\,(x = y)$ и $\forall x\, B(x,y)$ переменная x связанная, а переменная y свободная.

Формула без свободных переменных является – высказвыванием.

Выполнимость

Формула $A(x_1, x_2, \ldots, x_n)$ называется выполнимой, если $\exists\, I = (\text{c}_1, \text{c}_2, \ldots, \text{c}_n) \in \{0,1\}^n$, для которой $A(\text{c}_1, \text{c}_2, \ldots, \text{c}_n) = 1$.

Запись $I \vDash A$ означает, что формула A выполнима (истина) в интерпретации I.

Общезначимость

Формула $A(x_1, x_2, \ldots, x_n)$ называется общезначимой (тавтологией, тождественно истиной), если

$\forall\, I = (\text{c}_1, \text{c}_2, \ldots, \text{c}_n) \in \{0,1\}^n\ A(\text{c}_1, \text{c}_2, \ldots, \text{c}_n) = 1$.

Запись $\vDash A$ означает, что формула A общезначима.

Опровержимость

Формула $A(x_1, x_2, \ldots, x_n)$ называется опровержимой, если $\exists\ I = (\text{c}_1, \text{c}_2, \ldots, \text{c}_n) \in \{0,1\}^n$, для которой $A(\text{c}_1, \text{c}_2, \ldots, \text{c}_n) = 0$.

Запись $I \nvDash A$ означает, что формула A опровержима (ложна) в интерпретации I.

Противоречивость

Формула $A(x_1, x_2, \ldots, x_n)$ называется противоречивой (тождественно ложной), если

$\forall\ I = (\text{c}_1, \text{c}_2, \ldots, \text{c}_n) \in \{0,1\}^n\ A(\text{c}_1, \text{c}_2, \ldots, \text{c}_n) = 0$.

Запись $\nvDash A$ означает, что формула A противоречива.

$\overline{\text{общезначимость}}$ = опровержимость ($\overline{\vDash A} = I \nvDash A$)

$\overline{(\forall I \in \{0,1\}^n) A(I) = 1}$ = $(\exists I \in \{0,1\}^n)\, A(I) = 0$

$\overline{\text{опровержимость}}$ = общезначимость ($\overline{I \nvDash A} = \vDash A$)

$\overline{(\exists I \in \{0,1\}^n) A(I) = 0}$ = $(\forall I \in \{0,1\}^n)\, A(I) = 1$

$\overline{\text{противоречие}}$ = выполнимость ($\overline{\nvDash A} = I \vDash A$)

$\overline{(\forall I \in \{0,1\}^n) A(I) = 0}$ = $(\exists I \in \{0,1\}^n) A(I) = 1$

$\overline{\text{выполнимость}}$ = противоречие ($\overline{I \vDash A} = \nvDash A$)

$\overline{(\exists I \in \{0,1\}^n) A(I) = 1}$ = $(\forall I \in \{0,1\}^n)\, A(I) = 0$

Проблема разрешимости

Пусть дана произвольная формула $\mathcal{A}(X_1, ..., X_n)$. Можно ли как-то проверить, что она является *общезначимой*? Если существует такой способ (алгоритм), позволяющий в конечное число шагов убедиться в этом, то говорят, что проблема проверки общезначимости формул алгебры высказываний *разрешима*.

Рассматривая набор переменных $(X_1, ..., X_n)$ на множестве $\{\bot, \top\}$, имеем 2^n возможных комбинаций. Для каждой комбинации легко вычислить истинностное значение формулы $\mathcal{A}$. Это можно сделать, написав программу для компьютера. Найдя все значения формулы, мы узнаем всегда ли она истинна. Если «да», то формула $\mathcal{A}$ общезначима.

Логическое следствие

Пусть даны формулы $\mathcal{A}_1, ..., \mathcal{A}_m, \mathcal{B}$. Формула $\mathcal{B}$ является *логическим следствием* формул $\mathcal{A}_1, ..., \mathcal{A}_m$, если, придавая значения переменным $X_1, ..., X_n$, от которых зависят все рассматриваемые формулы, всякий раз, когда истинны одновременно все формулы $\mathcal{A}_1, ..., \mathcal{A}_m$, истинна и формула $\mathcal{B}$.

Для логического следствия используется запись

$$\mathcal{A}_1, ..., \mathcal{A}_m \models \mathcal{B}.$$

Для проверки наличия логического следования достаточно построить истинностную таблицу.

Пример. Проверить, что $X, Y, (Z\&X \Rightarrow \neg Y) \models \neg Z.$

Имеем истинную таблицу

X	Y	Z	$Z\&X \Rightarrow \neg Y$	$\neg Z$
$\top$	$\top$	$\top$	$\perp$	$\perp$
$\top$	$\top$	$\perp$	$\top$	$\top$

Из второй строки видно, что $X, Y, (Z\&X \Rightarrow \neg Y) \models \neg Z$

есть логическое следствие.

Теорема о дедукции (Жак Эрбран (1930))

Если $\mathcal{A} \models \mathcal{B}$, *то* $\models (\mathcal{A} \Rightarrow \mathcal{B})$

Доказательство.

Используем таблицу истинности для связки $\Rightarrow$. Из условия $\mathcal{A} \models \mathcal{B}$ вытекает, что если $\mathcal{A} = \top$, то $\mathcal{B} = \top$. Но тогда $\models (\mathcal{A} \Rightarrow \mathcal{B})$, ибо случай, когда $\mathcal{A} = \top$, $\mathcal{B} = \bot$, исключен.

Следствие.

$\mathcal{A}_1, \ldots, \mathcal{A}_m \models \mathcal{B}$ *тогда и только тогда, когда* $\models (\mathcal{A}_1 \& \ldots \& \mathcal{A}_m \Rightarrow \mathcal{B})$

Классический принцип двойственности

В булевых алгебрах существуют двойственные утверждения, они одновременно являются либо общезначимыми, либо выполнимыми, либо опровержимыми, либо противоречивыми.

Именно, если в формуле булевой алгебры, поменять все операции на двойственные, то

1. если исходная формула была общезначимой, то и двойственная будет общезначимой
2. если исходная формула была выполнимой, то и двойственная будет выполнимой
3. если исходная формула была опровержимой, то и двойственная будет опровержимой
4. если исходная формула была противоречием, то и двойственная будет противоречием

Булевы алгебры

Алгебра высказываний

Носитель алгебры $M = \{0,1\}$.

Бинарные операции $\cdot, +$. Унарная операция $\overline{}$. Константы (нульарные операции) $0, 1$.

Алгебра Кантора

Носитель алгебры – булеан универсального множества $2^U = \{X \mid X \subseteq U\}$.

Бинарные операции $\bigcap, \bigcup$. Унарная операция $\overline{}$. Константы (нульарные операции) $\varnothing, U$.

Алгебра Линденбаума-Тарского
(алгебра классов равносильных формул)

Носитель алгебры $\{[F] = \{G \mid \mathit{func}(G) = \mathit{func}(F) = P_n\} \mid P_n : M^n \to M\}$ –

множество классов эквивалентности по отношению равносильности.

Бинарные операции $[A] \cdot [B] = [A \cdot B]$, $[A] + [B] = [A + B]$. Унарная операция $\overline{[A]} = [\overline{A}]$.

Константы (нульарные операции) $[0], [1]$.

Законы булевых алгебр

Ассоциативности

$$A\cdot(B\cdot C)=(A\cdot B)\cdot C \qquad A+(B+C)=(A+B)+C$$

$$A\cap(B\cap C)=(A\cap B)\cap C \qquad A\cup(B\cup C)=(A\cup B)\cup C$$

$$[A]\cdot([B]\cdot[C])=([A]\cdot[B])\cdot[C] \qquad [A]+([B]+[C])=([A]+[B])+[C]$$

Коммутативности

$$A\cdot B=B\cdot A \qquad A+B=B+A$$

$$A\cap B=B\cap A \qquad A\cup B=B\cup A$$

$$[A]\cdot[B]=[B]\cdot[A] \qquad [A]+[B]=[B]+[A]$$

Идемпотентности

$$A\cdot A=A \qquad A+A=A$$

$$A\cap A=A \qquad A\cup A=A$$

$$[A]\cdot[A]=[A] \qquad [A]+[A]=[A]$$

Законы булевых алгебр

Дистрибутивности

слева

$$A\cdot(B+C)=(A\cdot B)+(A\cdot C) \qquad A+(B\cdot C)=(A+B)\cdot(A+C)$$

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C) \qquad A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$$

$$[A]\cdot([B]+[C])=([A]\cdot[B])+([A]\cdot[C]) \qquad [A]+([B]\cdot[C])=([A]+[B])\cdot([A]+[C])$$

справа

$$(A+B)\cdot C=(A\cdot C)+(B\cdot C) \qquad (A\cdot B)+C=(A+C)\cdot(B+C)$$

$$(A\cup B)\cap C=(A\cap C)\cup(B\cap C) \qquad (A\cap B)\cup C=(A\cup C)\cap(B\cup C)$$

$$([A]+[B])\cdot[C]=([A]\cdot[C])+([B]\cdot[C]) \qquad ([A]\cdot[B])+[C]=([A]+[C])\cdot([B]+[C])$$

Двойного отрицания

$$\overline{\overline{A}}=A$$

$$\overline{\overline{A}}=A$$

$$\overline{\overline{[A]}}=[A]$$

Законы булевых алгебр

Поглощения

$$A\cdot(A+B)=A \qquad A+(A\cdot B)=A$$

$$A\cap(A\cup B)=A \qquad A\cup(A\cap B)=A$$

$$[A]\cdot([A]+[B])=[A] \qquad [A]+([A]\cdot[B])=[A]$$

Порецкого

$$A\cdot(\overline{A}+B)=A\cdot B \qquad A+(\overline{A}\cdot B)=A+B$$

$$A\cap(\overline{A}\cup B)=A\cap B \qquad A\cup(\overline{A}\cap B)=A\cup B$$

$$[A]\cdot\left(\overline{[A]}+[B]\right)=[A]\cdot[B] \qquad [A]+\left(\overline{[A]}\cdot[B]\right)=[A]+[B]$$

де Моргана

$$\overline{A\cdot B}=\overline{A}+\overline{B} \qquad \overline{A+B}=\overline{A}\cdot\overline{B}$$

$$\overline{A\cap B}=\overline{A}\cup\overline{B} \qquad \overline{A\cup B}=\overline{A}\cap\overline{B}$$

$$\overline{[A]\cdot[B]}=\overline{[A]}+\overline{[B]} \qquad \overline{[A]+[B]}=\overline{[A]}\cdot\overline{[B]}$$

Законы булевых алгебр

Склеивания

$$(A+B)\cdot(A+\overline{B})=A \qquad (A\cdot B)+(A\cdot\overline{B})=A$$

$$(A\cup B)\cap(A\cup\overline{B})=A \qquad (A\cap B)\cup(A\cap\overline{B})=A$$

$$([A]+[B])\cdot([A]+\overline{[B]})=A \qquad ([A]\cdot[B])+([A]\cdot\overline{[B]})=[A]$$

Аристотеля

противоречия | *исключения третьего*

$$A\cdot\overline{A}=0 \qquad A+\overline{A}=1$$

$$A\cap\overline{A}=\varnothing \qquad A\cup\overline{A}=U$$

$$[A]\cdot\overline{[A]}=[0] \qquad [A]+\overline{[A]}=[1]$$

Законы булевых алгебр

Действия с константами

нейтральный элемент

$A \cdot 1 = A$ $\quad$ $A + 0 = A$

$A \bigcap U = A$ $\quad$ $A \bigcup \varnothing = A$

$[A] \cdot [1] = [A]$ $\quad$ $[A] + [0] = [A]$

поглощающий элемент

$A \cdot 0 = 0$ $\quad$ $A + 1 = 1$

$A \bigcap \varnothing = \varnothing$ $\quad$ $A \bigcup U = U$

$[A] \cdot [0] = [0]$ $\quad$ $[A] + [1] = [1]$