Введение в математическую логику (осень 2018)

В.Б. Шехтман

Лекция 3

Нормальные формы

Определение 1. Литерал — *это переменная или ее отрицание.* Элементарная конъюнкция от переменных $P_1, \dots, P_n$ — *это конъюнкция литералов, построенных из этих переменных, в которой каждая переменная встречается ровно 1 раз.*

Из определения ясно, что любая элементарная конъюнкция от $P_1, \dots, P_n$ равносильна сигнальной формуле вида $A_{\overrightarrow{x}}$, где $\overrightarrow{x}$ — двоичный вектор длины n (см. лекцию 2). Строго говоря, формула $A_{\overrightarrow{x}}$ определена неоднозначно: в конъюнкции можно по-разному расставить скобки. Для единообразия будем записывать скобки слева направо:

$$A_{\overrightarrow{x}} = (\dots(P_1^{x_1} \wedge P_2^{x_2}) \dots \wedge P_{n-1}^{x_{n-1}}) \wedge P_n^{x_n}.$$

В дальнейшем будем считать, что все элементарные конъюнкции имеют такой вид.

Определение 2. Совершенная дизъюнктивная нормальная форма *(СДНФ) от переменных $P_1, \dots, P_n$ — это дизъюнкция различных элементарных конъюнкций от этих переменных.*

Сюда включаются частные случаи: когда дизъюнкция берется по множеству, состоящему из одной формулы, а также случай пустой дизъюнкции — ее считаем равной $\perp$.

Теорема 3.1.

(1) Каждая формула, построенная из переменных $P_1, \dots, P_n$, равносильна некоторой СДНФ от этих переменных.

(2) *Каждая формула равносильна единственной СДНФ (с точностью до перестановок и расстановки скобок в дизъюнкциях):*
если $\bigvee\limits_{\overrightarrow{x} \in I} A_{\overrightarrow{x}} \sim \bigvee\limits_{\overrightarrow{x} \in J} A_{\overrightarrow{x}}$, *то* $I = J$.

Доказательство (1) уже доказано в процессе доказательства теоремы 2.6.

(2) Докажем единственность (это почти уже сделано). Заметим, что запись $\bigvee\limits_{\overrightarrow{x} \in I} A_{\overrightarrow{x}}$ не задает формулу однозначно, пока не определена расстановка скобок и порядок членов дизъюнкции. Для однозначности можно, например, считать, что скобки расставлены слева направо, а порядок членов определяется, исходя из порядка на множестве $\mathbb{B}^n$ всех двоичных векторов $\overrightarrow{x}$. Порядок на $\mathbb{B}^n$ можно задать, как в двоичной системе счисления: (0,...,0,0) — наименьший, (0,...,0,1) — следующий, и т.д.

Обозначим эту дизъюнкцию через A_I. Ее булева функция равна 1 в точности на множестве I:

$$\varphi_{A_I}(\overrightarrow{y}) = \begin{cases} 1, & \text{если } y \in I, \\ 0, & \text{если } y \notin I. \end{cases}$$

Действительно,

$$\varphi_{A_I}(\overrightarrow{y}) = 1 \Leftrightarrow f_{\overrightarrow{y}}(A_I) = 1 \Leftrightarrow \exists \overrightarrow{x} \in I \; f_{\overrightarrow{y}}(A_{\overrightarrow{x}}) = 1 \text{ (т.к. } A_I \text{ — дизъюнкция)}$$

$$\Leftrightarrow \exists \overrightarrow{x} \in I \; \overrightarrow{y} = \overrightarrow{x} \text{ (по лемме 2.5)} \Leftrightarrow y \in I.$$

Поэтому, если $I \neq J$, то $A_I \not\sim A_J$: у них разные булевы функции. ■

По аналогии с элементарными конъюнкциями, можно определить *элементарные дизъюнкции*: они имеют вид $P_1^{x_1} \vee \ldots \vee P_n^{x_n}$. И соответственно определяем *совершенную конъюнктивную нормальную форму* (СКНФ) (от $P_1, \ldots P_n$) как конъюнкцию элементарных дизъюнкций (причем пустая конъюнкция считается равной $\top$).

Справедлива следующая

Теорема (об СКНФ)**.**

(1) *Каждая формула, построенная из переменных $P_1, \ldots, P_n$, равносильна некоторой СКНФ от этих переменных.*

(2) *Каждая формула равносильна единственной СКНФ, с точностью до перестановок и расстановки скобок в конъюнкциях и дизъюнкциях.*

Дополнительная задача Докажите эту теорему.

Двойственность

Определение 3. *Для формулы A, построенной из $\wedge, \vee, \neg$,* двойственная формула A^* *получается заменой всех $\wedge$ на $\vee$ и наоборот. Более формальное определение A^* — по индукции:*

$$
\begin{array}{lcll}
A^* & = & A & \text{для } A \in Var, \\
(A \wedge B)^* & = & (A^* \vee B^*), & \\
(A \vee B)^* & = & (A^* \wedge B^*), & \\
(\neg A)^* & = & \neg A^*. &
\end{array}
$$

Теорема (о двойственности)**.** *Если $A \sim B$, то $A^* \sim B^*$. В частности, если $\models A$ (т.е. $A \sim \top$), то $\models \neg A^*$ (т.е. $A^* \sim \top^* \sim \bot$).*

Дополнительная задача Докажите эту теорему.

Булевы алгебры

По аналогии с двузначными оценками и таблицами истинности, для логических связок $\neg, \vee, \wedge$ можно построить таблицы с несколькими значениями истинности. Если желательно, чтобы сохранились основные свойства этих связок, мы приходим к понятию булевой алгебры.

Определение 4. Булевой алгеброй *называется непустое множество с заданными на нем операциями и выделенными элементами* $(\mathcal{B}, \sqcup, \sqcap, -, \mathbf{0}, \mathbf{1})$[1], *где*

- $\sqcup, \sqcap$ — *двуместные операции на $\mathcal{B}$,*
- $-$ — *одноместная операция на $\mathcal{B}$,*
- $\mathbf{0}, \mathbf{1} \in \mathcal{B}$,

причем выполняются следующие свойства (см. лемму 2.4):

(1) $x \sqcup y = y \sqcup x,\ x \sqcap y = y \sqcap x$ *(коммутативность),*

(2) $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z),\ (x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$ *(ассоциативность),*

(3) $x \sqcup x = x,\ x \sqcap x = x$ *(идемпотентность),*

[1] В каждой алгебре имеются свои операции, поэтому точнее были бы обозначения $\sqcup_{\mathcal{B}}, \sqcap_{\mathcal{B}}$ и т.д. Но для удобства мы опускаем индекс $\mathcal{B}$.

(4) $(x \sqcup y) \sqcap z = (x \sqcap y) \sqcup (x \sqcap z),\ (x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z)$ *(дистрибутивность),*

(5) $(x \sqcup y) \sqcap x = x,\ (x \sqcap y) \sqcup x = x$ *(поглощение),*

(6) $x \sqcap -x = \mathbf{0},\ x \sqcup \mathbf{0} = x,$
$x \sqcup -x = \mathbf{1},\ x \sqcap \mathbf{1} = x$ *(свойства* $\mathbf{0}$ *и* $\mathbf{1}$*),*

(7) $-(x \sqcup y) = -x \sqcap -y,\ -(x \sqcap y) = -x \sqcup -y$ *(законы Де Моргана),*

(8) $- - x = x$ *(закон двойного дополнения).*

Операции $\sqcup, \sqcap, -$ называются соответственно *булевой суммой* (или *объединением*), *булевым произведением* (или *пересечением*) и *дополнением.* $\mathbf{0}, \mathbf{1}$ называются *нулем* и *единицей.*

Список основных тождеств, задающих булевы алгебры, в действительности можно сократить. Например, можно ограничиться только (1), (2),(5), (6) и одним из (4); остальные тождества следуют из этих.

В частности, идемпотентность получается так:

$$x = x \sqcap (x \sqcup \mathbf{0}) \text{ (по (5)) } = x \sqcap x \text{ (по (6)).}$$

А закон двойного дополнения — так:

$$- - x = - - x \sqcap \mathbf{1} = - - x \sqcap (x \sqcup -x) = (- - x \sqcap x) \sqcup (- - x \sqcap -x)$$
$$= (- - x \sqcap x) \sqcup \mathbf{0} = - - x \sqcap x \text{ (по (6),(4), (1));}$$
с другой стороны,
$$x = x \sqcap \mathbf{1} = - - x \sqcap (-x \sqcup - - x) = (x \sqcap -x) \sqcup (x \sqcap - - x)$$
$$= \mathbf{0} \sqcup (x \sqcap - - x) = x \sqcap - - x \text{ (тоже по (6),(4), (1));}$$
отсюда $- -x = x$.

Пример 1 Тривиальный пример булевой алгебры — одноэлементная алгебра (она обозначается *1*). В ней $\mathbf{0} = \mathbf{1}$ и все операции дают $\mathbf{1}$; тогда тождества из определения 4 очевидны.

Пример 2 Двухэлементная булева алгебра *2* на множестве $\mathbb{B} = \{0, 1\}$:

$$2 = (\{0,1\},\ ⓥ,\ ⓐ,\ ⊖,\ 0,\ 1),$$

где $x ⓥ y = \max(x, y),\ x ⓐ y = \min(x, y),\ ⊖ x = 1 - x$ (см. лекцию 1). То, что *2* — булева алгебра, фактически доказано в лемме 2.4.

Пример 3 Стандартный пример булевой алгебры — множество $\mathcal{P}(E)$ всех подмножеств данного множества E с обычными операциями объединения, пересечения, дополнения (до E) и $\varnothing, E$ в качестве $\mathbf{0}, \mathbf{1}$.

Предложение 3.2. *Пусть* E *— произвольное множество. Тогда* $(\mathcal{P}(E), \cup, \cap, -, \varnothing, E)$ *(где* $-A = E \backslash A$*)— булева алгебра.*

Доказательство Надо проверить булевы тождества для $\mathcal{P}(E)$. При этом можно использовать равносильности из леммы 2.4.

Например, дистрибутивность

$$(x \cup y) \cap z = (x \cap z) \cup (y \cap z)$$

означает, что для любого $a \in E$

$$(\bullet) \qquad a \in (x \cup y) \cap z \Leftrightarrow a \in (x \cap z) \cup (y \cap z).$$

Чтобы это проверить, возьмем произвольное a и рассмотрим пропозициональные переменные P, Q, R, которые оценим соответственно как $a \in x$, $a \in y$, $a \in z$. Т.е. выберем оценку f такую, что

$$f(P) = 1 \Leftrightarrow a \in x;\ f(Q) = 1 \Leftrightarrow a \in y;\ f(R) = 1 \Leftrightarrow a \in z.$$

Тогда

$$a \in (x \cup y) \cap z \Leftrightarrow ((a \in x \text{ или } a \in y) \text{ и } a \in z) \Leftrightarrow f((P \vee Q) \wedge R) = 1,$$

и аналогично,

$$a \in (x \cap z) \cup (y \cap z) \Leftrightarrow f((P \wedge R) \vee (Q \wedge R)) = 1.$$

Но из леммы 2.4 мы знаем, что формулы $(P \vee Q) \wedge R$ и $(P \wedge R) \vee (Q \wedge R)$ равносильны (т.е. одновременно истинны или одновременно ложны). Отсюда следует $(\bullet)$.

Так же поступаем и с другими булевыми тождествами для $\mathcal{P}(E)$; они превращаются в равносильности из леммы 2.4, если знаки $\cup, \cap, -$ заменить соответственно на $\vee, \wedge, \neg$. ■

Определение 5. *Изоморфизм булевых алгебр — это биекция, сохраняющая все операции.*

Точнее, пусть $\mathcal{A}$, $\mathcal{B}$ — булевы алгебры. Биекция $\varphi : \mathcal{A} \longrightarrow \mathcal{B}$ называется изоморфизмом $\mathcal{A}$ на $\mathcal{B}$, *если $\varphi(\mathbf{0}_\mathcal{A}) = \mathbf{0}_\mathcal{B}$, $\varphi(\mathbf{1}_\mathcal{A}) = \mathbf{1}_\mathcal{B}$ и для всех $x, y \in \mathcal{A}$*

$$\varphi(x \sqcup_\mathcal{A} y) = \varphi(x) \sqcup_\mathcal{B} \varphi(y),\ \varphi(x \sqcap_\mathcal{A} y) = \varphi(x) \sqcap_\mathcal{B} \varphi(y),\ \varphi(-_\mathcal{A} x) = -_\mathcal{B} \varphi(x).$$

Если существует изоморфизм $\mathcal{A}$ на $\mathcal{B}$, то алгебры $\mathcal{A}$, $\mathcal{B}$ называются изоморфными.

Как легко видеть, изоморфность — отношение эквивалентности между алгебрами[2].

В частности, алгебра *2* изоморфна алгебре $\mathcal{P}(\{a\})$ подмножеств 1-элементного множества, а тривиальная алгебра *1* изоморфна алгебре $\mathcal{P}(\varnothing)$.

[2]В более общем контексте понятие изоморфизма будет обсуждаться позже.

Лемма 3.3. *В булевой алгебре можно определить частичный порядок, положив*

$$a \le b \Leftrightarrow a = (a \sqcap b).$$

Относительно этого порядка $\mathbf{0}$ *является наименьшим элементом,* $\mathbf{1}$ *— наибольшим элементом.*

Доказательство

- Рефлексивность $a = a \sqcap a$ — это идемпотентность $\sqcap$.
- Транзитивность получается из ассоциативности:
  если $a = a \sqcap b$ и $b = b \sqcap c$, то
  $$a = a \sqcap b = a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c = a \sqcap c.$$
- Антисимметричность следует из коммутативности:
  если $a = a \sqcap b$ и $b = b \sqcap a$, то $a = b$.
- $\mathbf{1}$ — наибольший: $a = a \sqcap \mathbf{1}$ — по определению 4.
- $\mathbf{0}$ — наименьший, т.е. $\mathbf{0} = \mathbf{0} \sqcap a$. Это получается так:
  $$\mathbf{0} \sqcap a = (-a \sqcap a) \sqcap a = -a \sqcap (a \sqcap a) = -a \sqcap a = \mathbf{0}.$$

■

Если алгебра содержит более 2 элементов, то этот порядок — не линейный.

Лемма 3.4. $a \le b \Leftrightarrow -a \sqcup b = \mathbf{1}$.

Доказательство ($\Leftarrow$). Пусть $-a \sqcup b = \mathbf{1}$. Тогда

$$a = a \sqcap \mathbf{1} = a \sqcap (-a \sqcup b) = (a \sqcap (-a)) \sqcup (a \sqcap b) = \mathbf{0} \sqcup (a \sqcap b) = a \sqcap b.$$

по свойствам $\mathbf{1}, \mathbf{0}$ и дистрибутивности. Значит, $a \le b$.

($\Rightarrow$). Пусть $a \le b$, т.е. $a = a \sqcap b$. Тогда

$$-a \sqcup b = -(a \sqcap b) \sqcup b = -a \sqcup -b \sqcup b = -a \sqcup \mathbf{1}$$

по закону Де Моргана и свойству $\mathbf{1}$. И заметим еще, что

$$-a \sqcup \mathbf{1} = -a \sqcup (-a \sqcup a) = (-a \sqcup -a) \sqcup a = -a \sqcup a = \mathbf{1}.$$

Следовательно, $-a \sqcup b = \mathbf{1}$. ■

Определение 6. Оценка в булевой алгебре $\mathcal{B}$ — *это отображение* $f : Var \longrightarrow \mathcal{B}$.

По аналогии с леммой 2.1, получаем:

Лемма 3.5. *Для любой оценки $f : Var \longrightarrow \mathcal{B}$ существует единственное отображение $\overline{f} : Fm \longrightarrow \mathcal{B}$, такое что для всех $A, B \in Fm$*

(1) $\overline{f}(A) = f(A)$, *если* $A \in Var$,

(2) $\overline{f}(A \wedge B) = \overline{f}(A) \sqcap \overline{f}(B)$,

(3) $\overline{f}(A \vee B) = \overline{f}(A) \sqcup \overline{f}(B)$,

(4) $\overline{f}(\neg A) = -\overline{f}(A)$,

(5) $\overline{f}(A \to B) = \overline{f}(\neg A \vee B) = -\overline{f}(A) \sqcup \overline{f}(B)$.

Доказательство полностью аналогично лемме 2.1 (по индукции, используя однозначность анализа формул).

Как и в случае оценок в *2*, пишем $f(A)$ вместо $\overline{f}(A)$; $f(A)$ называется *значением A в алгебре $\mathcal{B}$ при оценке f.*

Определение 7. *Формулы A, B называются* равносильными (эквивалентными) в булевой алгебре $\mathcal{B}$, *если их значения в $\mathcal{B}$ совпадают при всех оценках; обозначение: $A \sim_{\mathcal{B}} B$.*

Формула A называется общезначимой в булевой алгебре $\mathcal{B}$, *если ее значение в $\mathcal{B}$ равно $\mathbf{1}$ при любой оценке; обозначение: $\mathcal{B} \vDash A$.*

Ясно, что равносильность и общезначимость в алгебре *2* — это обычные равносильность ($\sim$) и тавтологичность ($\vDash$); они определялись в лекции 2.

Аналогично лемме 2.3, получаем:

Лемма 3.6.

(1) $A \sim_{\mathcal{B}} B \;\Leftrightarrow\; \mathcal{B} \vDash ((A \to B) \wedge (B \to A))$.

(2) $\mathcal{B} \vDash A \;\Leftrightarrow\; A \sim_{\mathcal{B}} \top$.

Доказательство Как и в лемме 2.3, проверяем, что для любой оценки f,

$$f(A) = f(B) \Leftrightarrow f((A \to B) \wedge (B \to A)) = \mathbf{1}.$$

Обозначим $a := f(A),\ b := f(B)$. Нам надо показать, что

$$a = b \Leftrightarrow (a \ominus\!\!\!\to b) \sqcap (b \ominus\!\!\!\to a) = \mathbf{1},$$

где $a \ominus\!\!\!\to b := -a \sqcup b$.

Утверждение ($\Rightarrow$) очевидно: $a \ominus\!\!\!\to a = -a \sqcup a = \mathbf{1}$, $\mathbf{1} \sqcap \mathbf{1} = \mathbf{1}$ по определению 4.

Чтобы доказать ($\Leftarrow$), заметим сначала, что

$$x \sqcap y = \mathbf{1} \Rightarrow x = y = \mathbf{1}.$$

Действительно, $x \sqcap y \leq x$, $x \sqcap y \leq y$, а $\mathbf{1}$ — наибольший элемент (относительно $\leq$).

Поэтому

$$(a \ominus b) \sqcap (b \ominus a) = \mathbf{1} \Rightarrow -a \sqcup b = -b \sqcup a = \mathbf{1}.$$

По лемме 3.4 из $-a \sqcup b = -b \sqcup a = \mathbf{1}$ следует $a \leq b$ и $b \leq a$, т.е. $a = b$. ■

Минимальные ненулевые элементы относительно порядка $\leq$ в булевой алгебреназываются *атомами*; их может быть несколько, а может не быть вообще.

Справедлива следующая теорема Стоуна (в курсе не доказывается):

Теорема 3.7. *

(1) Всякая булева алгебра изоморфна алгебре множеств, т.е. подалгебре некоторой алгебры $\mathcal{P}(E)$.

(2) Всякая конечная булева алгебра изоморфна алгебре вида $\mathcal{P}(E)$, и следовательно, состоит из 2^n элементов для некоторого n.

В конечном случае в качестве E можно взять множество всех атомов данной алгебры.

Дополнительная задача Докажите часть (2) в теореме Стоуна.

Заметим, что не все булевы алгебры имеют вид $\mathcal{P}(E)$.

Пример 4 Рассмотрим, например, такое множество подмножеств натурального ряда:

$$\{V \subseteq \mathbb{N} \mid V \text{ конечно или } \mathbb{N} \backslash V \text{ конечно}\}.$$

В него входят $\varnothing$ и $\mathbb{N}$. Очевидно, что оно замкнуто относительно дополнений, и нетрудно проверить, что оно замкнуто относительно объединений и пересечений, поэтому получается счетная подалгебра алгебры $\mathcal{P}(\mathbb{N})$.

Однако никакая алгебра $\mathcal{P}(E)$ не может быть счетной: такие алгебры конечны при конечном E и несчетны при бесконечном E — в силу теоремы Кантора (которая будет обсуждаться в этом курсе позже).

Пример 5 Алгебра Линденбаума — Тарского.

Рассмотрим множество классов всех пропозициональных формул по отношению равносильности $\mathcal{L} = Fm/\!\sim$. Пусть $\tilde{A}$ обозначает класс формулы A. Тогда определим

$$\mathbf{0} := \tilde{\bot},\ \mathbf{1} := \tilde{\top},\ \tilde{A} \sqcup \tilde{B} := \widetilde{A \vee B},\ \tilde{A} \sqcap \tilde{B} := \widetilde{A \wedge B},\ -\tilde{A} := \widetilde{\neg A}.$$

Корректность этого определения следует из того, что равносильность согласована с логическими связками: если $A \sim A'$ и $B \sim B'$, то $A \vee B \sim A' \vee B'$ и т.д.

Лемма 2.4 показывает, что $\mathcal{L}$ — булева алгебра. Эта алгебра счетна, и в ней, как можно доказать, атомов нет (в отличие от примера 4).

Дополнительная задача Докажите последнее утверждение.

Список литературы

[1] Н.К. Верещагин, А.Х. Шень. Лекции по математической логике и теории алгоритмов (часть 2), 2012, Изд. МЦНМО, http://www.mccme.ru.

[2] В.А. Успенский, Н.К. Верещагин, В.Е. Плиско. Вводный курс математической логики. Издательство МГУ. М., 1991 и 1997. Физматлит, 2002.

[3] Э. Мендельсон. Введение в математическую логику. М.,1984.

[4] А.Н.Колмогоров, А.Г.Драгалин. Математическая логика. Серия "Классический университетский учебник 2005.

[5] В.Н. Крупский, В. Е. Плиско. Математическая логика и теория алгоритмов, Академия, 2013.

[6] С.К. Клини. Математическая логика. М., Мир, 1973.

[7] W. Rautenberg. A concise introduction to mathematical logic. Springer, 2006.