Введение в математическую логику (осень 2016)

В.Б. Шехтман

Лекция 3

Нормальные формы

Определение 10 *Литерал — это переменная или ее отрицание. Дизъюнктивная нормальная форма (ДНФ) — это дизъюнкция нескольких конъюнкций литералов.*

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

Итак, на лекции 2 было доказано, что любая формула равносильна некоторой ДНФ. В действительности, доказано более сильное утверждение: эта ДНФ имеет специальный вид.

Определение 11 Элементарная конъюнкция от переменных $P_1, \ldots, P_n$ *— это конъюнкция литералов, построенных из этих переменных, в которой каждая переменная встречается ровно 1 раз.* Совершенная дизъюнктивная нормальная форма *(СДНФ) от переменных $P_1, \ldots, P_n$ — это дизъюнкция (различных) элементарных конъюнкций от этих переменных.*

Из определения ясно, что любая элементарная конъюнкция от $P_1, \ldots, P_n$ равносильна формуле вида $A_{\overrightarrow{x}}$, где $\overrightarrow{x}$ — двоичный вектор (см. лекцию 2).

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 конъюнкциях и 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 2.7.

(2) Докажем единственность (это почти уже сделано). Сначала отметим, что, строго говоря, даже формула $A_{\overrightarrow{x}}$ определена неоднозначно: в конъюнкции можно по-разному расставить скобки. Для единообразия можно считать, что скобки расставлены слева направо:

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

Запись $\bigvee\limits_{\overrightarrow{x} \in I} A_{\overrightarrow{x}}$ тоже не задает формулу однозначно, т.к. 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,

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

$$\Leftrightarrow \exists \overrightarrow{x} \in I \ \overrightarrow{y} = \overrightarrow{x} \text{ (по лемме 2.6)} \Leftrightarrow y \in I.$$

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 $P_1^{x_1} \vee \dots \vee P_n^{x_n}$. И далее определяем *совершенную конъюнктивную нормальную форму* (СКНФ) (от $P_1, \dots P_n$) как конъюнкцию (различных) элементарных дизъюнкций (причем пустая конъюнкция считается равной $\top$).

Справедлива следующая теорема

Теорема 3.2

(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.

Доказательство мы опускаем; оно аналогично теореме 3.1 или использует двойственность — см. далее.

Приведем еще другое доказательство части (1) теоремы 3.1 (с некоторыми сокращениями); оно пригодится в дальнейшем.

Именно, индукцией по длине доказываем, что всякая формула $A(P_1, \ldots, P_n)$ приводится к СДНФ от $P_1, \ldots, P_n$.

Базис индукции включает 2 случая: $A = P_i$ и $A = \neg P_i$, которые будут разобраны ниже.

Шаг индукции состоит из 3 случаев.

1. $A = B \vee C$. По предположению индукции, B и C можно записать виде СДНФ:

$$B \sim \bigvee_{\overrightarrow{x} \in I} A_{\overrightarrow{x}},\ C \sim \bigvee_{\overrightarrow{x} \in J} A_{\overrightarrow{x}},$$

где A_i — элементарные конъюнкции.

$$A \sim \bigvee_{\overrightarrow{x} \in I \cup J} A_{\overrightarrow{x}}$$

— по ассоциативности, коммутативности и идемпотентности (сокращаем повторяющиеся $A_{\overrightarrow{x}}$).

2. $A = B \wedge C$. Снова запишем B и C в виде СДНФ:

$$B \sim \bigvee_{\overrightarrow{x} \in I} A_{\overrightarrow{x}},\ C \sim \bigvee_{\overrightarrow{y} \in J} A_{\overrightarrow{y}}.$$

Тогда

$$A \sim (\bigvee_{\overrightarrow{x} \in I} A_{\overrightarrow{x}}) \wedge (\bigvee_{\overrightarrow{y} \in J} A_{\overrightarrow{y}}).$$

Теперь по дистрибутивности раскроем скобки:

$$A \sim \bigvee_{\overrightarrow{x} \in I, \overrightarrow{y} \in J} (A_{\overrightarrow{x}} \wedge A_{\overrightarrow{y}}).$$

Заметим, что если $\overrightarrow{x} \neq \overrightarrow{y}$, то $A_{\overrightarrow{x}} \wedge A_{\overrightarrow{y}} \sim \bot$ — эти конъюнкции противоречат друг другу в каком-то месте, а именно, $A_{\overrightarrow{x}} \wedge A_{\overrightarrow{y}}$ содержит P_k и $\neg P_k$, если $x_k \neq y_k$. С другой стороны, $(A_{\overrightarrow{x}} \wedge A_{\overrightarrow{x}}) \sim A_{\overrightarrow{x}}$. Удалив из большой дизъюнкции $\bigvee_{\overrightarrow{x} \in I, \overrightarrow{y} \in J} (A_i \wedge A_j)$ все ложные члены и сократив повторения, получаем в итоге:

$$A \sim \bigvee_{\vec{x} \in I \cap J} A_{\vec{x}}.$$

3. $A = \neg B$. По предположению индукции, $B \sim \bigvee_{\vec{x} \in I} A_{\vec{x}}$. По закону Де Моргана,

$$\neg(\bigvee_{\vec{x} \in I} A_{\vec{x}}) \sim \bigwedge_{\vec{x} \in I} \neg A_{\vec{x}}.$$

Но $A_{\vec{x}} = P_1^{x_1} \wedge \ldots \wedge P_n^{x_n}$, и, по (другому) закону Де Моргана,

$$\neg A_{\vec{x}} \sim \neg P_1^{x_1} \vee \ldots \vee \neg P_n^{x_n}.$$

Как мы сейчас увидим, все литералы представимы в виде СДНФ, и мы уже доказали, что конъюнкция и дизъюнкция сохраняют СДНФ-представимость. Отсюда следует СДНФ-представимость для A.

Рассмотрим теперь базис индукции.

4. $A = P_i$. Можем записать:

$$P_i \sim P_i \wedge \bigwedge_{j \neq i} (P_j \vee \neg P_j);$$

по дистрибутивности, ассоциативности и коммутативности, раскроем скобки:

$$P_i \wedge \bigwedge_{j \neq i} (P_j \vee \neg P_j) \sim \bigvee_{\vec{x} \in I} A_{\vec{x}}.$$

Здесь I — некоторое множество двоичных векторов — а именно, всех тех, у которых $x_i = 1$. Это происходит потому, что в возникших элементарных конъюнкциях $A_{\vec{x}}$ на i-м месте может появиться только P_i, а на других местах могут стоять как переменные, так и их отрицания.

5. $A = \neg P_i$. Рассуждаем аналогично.

$$\neg P_i \sim \neg P_i \wedge \bigwedge_{j \neq i} (P_j \vee \neg P_j).$$

Раскрыв скобки, получаем:

$$\neg P_i \wedge \bigwedge_{j \neq i} (P_j \vee \neg P_j) \sim \bigvee_{\vec{x} \in I'} A_{\vec{x}},$$

где I' состоит из векторов $\vec{x}$, у которых $x_i = 0$.

Двойственность

Определение 12 *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:*

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

Теорема 3.3 *Если $A \sim B$, то $A^* \sim B^*$. В частности, если $\vDash A$, то $\vDash A$,*

Доказательство на лекции не приводилось и в программу не входит. План его — такой. Сначала по индукции доказывается, что

$$A^*(P_1, \ldots, P_n) \sim \neg A(\neg P_1, \ldots, \neg P_n).$$

Затем можно проверить, что из $A(P_1, \ldots, P_n) \sim B(P_1, \ldots, P_n)$ следует $A(\neg P_1, \ldots, \neg P_n) \sim B(\neg P_1, \ldots, \neg P_n)$; это получается потому, что для любой оценки f, $f(A(\neg P_1, \ldots, \neg P_n)) = f'(A(P_1, \ldots, P_n))$, где $f'(P) = f(\neg P)$ для всех $P \in Var$.

И наконец, из $A(\neg P_1, \ldots, \neg P_n) \sim B(\neg P_1, \ldots, \neg P_n)$, очевидно, следует $\neg A(\neg P_1, \ldots, \neg P_n) \sim \neg B(\neg P_1, \ldots, \neg P_n)$.

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 13 Булевой алгеброй *называется множество с заданными на нем операциями и выделенными элементами $(\mathcal{B}, \sqcup, \sqcap, -, \mathbf{0}, \mathbf{1})$, 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 2.6):

(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),*

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

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

Заметим еще, что в булевой алгебре можно определить частичный порядок:

$$x \leq y \Leftrightarrow x \sqcap (x \sqcup y) = x \Leftrightarrow x \sqcup (x \sqcap y) = x.$$

Относительно этого порядка $\mathbf{0}$ является наименьшим элементом, $\mathbf{1}$ — наибольшим элементом, $x \sqcup y = \sup(x, y),\ x \sqcap y = \inf(x, y)$.

Стандартным примером булевой алгебры является множество $\mathbb{B}$ с операциями $\ovee$, $\owedge$, $\ominus$ (см. лекцию 2). Эта двухэлементная булева алгебра обозначается также *2*.

Еще один 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 $\mathbf{0}, \mathbf{1}$.

Лемма 3.4 $(\mathcal{P}(E), \cup, \cap, -, \varnothing, E)$ *— булева алгебра.*

Доказательство Первый способ доказательства — непосредственная проверка булевых тождеств.

Другой способ: докажем, что все равносильности логики высказываний превращаются в тождества, верные в $\mathcal{P}(E)$. Для этого каждой формуле[1] $A(P_1, \dots, P_n)$ поставим в соответствие "булевское выражение" $A^\sharp(x_1, \dots, x_n)$, заменив переменные P_i на x_i, а знаки $\vee, \wedge, \neg$ — соответственно, на $\cup, \cap, -$. Более формально это определяется по индукции:

- $P_i^\sharp = x_i$,
- $(A \vee B)^\sharp = A^\sharp \cup B^\sharp$,
- $(A \wedge B)^\sharp = A^\sharp \cap B^\sharp$,
- $(\neg A)^\sharp = -A^\sharp$.

Тогда справедливо следующее

Утверждение Для $a \in E$ рассмотрим оценку $g_a : Var \longrightarrow \mathbb{B}$, такую что для всех i

$$g_a(P_i) = 1 \Leftrightarrow a \in x_i.$$

Тогда для любой формулы $A(P_1, \dots, P_n)$

$$g_a(A) = 1 \Leftrightarrow a \in A^\sharp.$$

Это утверждение доказывается индукцией по длине A. Базис индукции следует из определения g_a, а шаг индукции легко проверяется. Например, если $A = \neg B$, то

$$g_a(A) = 1 \Leftrightarrow g_a(B) = 0 \Leftrightarrow a \notin B^\sharp \text{ (предположение индукции)}$$

$$\Leftrightarrow a \in -B^\sharp = (\neg B)^\sharp = A^\sharp.$$

Остальные случаи разбираются аналогично.

Теперь предположим, что $A(P_1, \dots, P_n) \sim B(P_1, \dots, P_n)$. Тогда значения этих формул при всех оценках совпадают, а потому $g_a(A) = g_a(B)$ для любого $a \in E$. Из доказанного утверждения получаем, что

$$a \in A^\sharp \Leftrightarrow a \in B^\sharp$$

для всех $a \in E$, т.е. $A^\sharp = B^\sharp$.

Таким образом, если формулы A и B равносильны, то выражения $A^\sharp$ и $B^\sharp$ тождественно равны (при всех $x_1, \dots, x_n$). ■

Можно заметить, что алгебра *2* оказывается изоморфной алгебре $\mathcal{P}(\{a\})$ подмножеств 1-элементного множества.

Алгебра $\mathcal{P}(\varnothing)$ состоит из одного элемента; такая алгебра называется *тривиальной* (в ней $\mathbf{0} = \mathbf{1}$, и любые тождества верны).

Справедлива следующая теорема (в курсе не доказывается):

Теорема 3.5 *Всякая конечная булева алгебра изоморфна алгебре вида $\mathcal{P}()$, и следовательно, состоит из 2^n элементов для некоторого n.*

[1] Предполагается, что A не содержит знака '$\to$', поскольку импликация выразима через другие связки.

Впрочем, не все булевы алгебры имеют такой вид. Рассмотрим, например, такое множество подмножеств натурального ряда:

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

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

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

Определение 14 Оценка в булевой алгебре $\mathcal{B}$ *— это отображение* $f : Var \longrightarrow \mathcal{B}$.

По аналогии с леммой 2.1, получаем:

Лемма 3.6 *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 15 *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 общезначимость ($\vDash$), как они определялись в лекции 2.

Аналогично лемме 2.6, получаем:

Лемма 3.7 $A \sim_{\mathcal{B}} B \Leftrightarrow \mathcal{B} \vDash ((A \to B) \wedge (B \to A))$.

Доказательство Как и в лемме 2.6, проверяем, что для любой оценки f,

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

■

Как и в алгебре $\mathcal{P}(E)$, в произвольной булевой алгебре $\mathcal{B}$ по формуле $A(P_1, \dots, P_n)$ (не содержащей $\to$) построим булевское выражение $A^\sharp(x_1, \dots, x_n)$ (см. доказательство леммы 3.4):

- $P_i^\sharp = x_i$,
- $(A \vee B)^\sharp = A^\sharp \sqcup B^\sharp$,
- $(A \wedge B)^\sharp = A^\sharp \sqcap B^\sharp$,
- $(\neg A)^\sharp = -A^\sharp$.

Лемма 3.8 $A \sim_{\mathcal{B}} B \Leftrightarrow A^\sharp = B^\sharp$ *в алгебре* $\mathcal{B}$.

Доказательство Для доказательства достаточно заметить, что

$$A^\sharp(x_1, \dots, x_n) = f(A),$$

где $f : Var \longrightarrow \mathcal{B}$ — оценка, такая что $f(P_i) = x_i$ Это легко получается по индукции. Базис очевиден, а шаг индукции, например, для $= B \wedge C$ выглядит так:

$$A^\sharp = B^\sharp \sqcap C^\sharp = f(B) \sqcup f(C) \text{ (по предположению индукции) } = f(A).$$

Поэтому $f(A) = f(B)$ при всех f тогда и только тогда, когда $A^\sharp(x_1, \dots, x_n) = B^\sharp(x_1, \dots, x_n)$ при всех $x_1, \dots, x_n$. ■

Отметим, что в алгебре *2* выражение $A^\sharp$ задает булеву функцию φ_A, т.е. $A^\sharp(x_1, \dots, x_n) = \varphi_A(x_1, \dots, x_n)$ (см. лекцию 2).

Теорема 3.9 *Для любой нетривиальной булевой алгебры* $\mathcal{B}$ *и формулы* A

$$\mathcal{B} \models A \Leftrightarrow 2 \models A \text{ (т.е. } A \text{ — тавтология).}$$

Эта теорема будет доказана на следующей лекции.