Математическая логика и теория вычислимости
Лекция 1. Логика высказываний

Денис Николаевич Москвин

ИТМО, корпоративная магистратура JetBrains
Разработка ПО / Software Engineering

10.02.2021

План лекции

1. Язык логики высказываний
2. Истинностное значение формул
3. Логические законы
4. Логическое следствие
5. Булева алгебра

Математическая логика

Подразделы:

- Теория доказательств
- Теория моделей
- Теория множеств
- Теория вычислимости
- Теория сложности вычислений

Формальные логические системы:

- Логика высказываний
- Логика предикатов первого порядка
- Логики высших порядков
- Неклассические логики

План лекции

1. Язык логики высказываний
2. Истинностное значение формул
3. Логические законы
4. Логическое следствие
5. Булева алгебра

Высказывания

- Высказывания (propositions):
  - $5 > 3$.
  - Река Волга впадает в Каспийское море.
  - В прямоугольном треугольнике все углы равны 60 градусам.
  - Все вороны черные.
  - Сегодняшняя дата меньше 13.05.2021.
  - Бог есть любовь.
  - Любое чётное число, начиная с 4, можно представить в виде суммы двух простых чисел.
  - Высказывание во второй части этого предложения истинно, и высказывание в первой части этого предложения ложно.
- Цель: запись однозначных высказываний на некотором полностью формализованном языке. Этот язык называют *предметным* или *объектным*.
- Рассуждения об этих высказываниях ведутся на другом языке, называемом *метаязыком*. Утверждения (на метаязыке) о высказываниях называют *метатеоремами*.

Формулы

- Имеется бесконечный набор *пропозициональных переменных*:

$$a, b, c, d, \ldots, x, y, z, a_1, a_2, a_3, \ldots$$

- Множество *пропозициональных формул* — это минимальное множество со следующими свойствами:
  - Всякая пропозициональная переменная есть формула;
  - Если A — формула, то $\neg A$ — формула;
  - Если A и B — формулы, то $(A \wedge B)$ — формула;
  - Если A и B — формулы, то $(A \vee B)$ — формула;
  - Если A и B — формулы, то $(A \to B)$ — формула.
- Символы $\neg$ (*отрицание*), $\wedge$ (*конъюнкция*), $\vee$ (*дизъюнкция*) и $\to$ (*импликация*) называют *пропозициональными связками*.
- Латинские буквы в верхнем регистре относятся к метатеории.

Примеры формул

Примеры формул:

$$
\begin{aligned}
&p\\
&(p \wedge q)\\
&((p \wedge q) \to p)\\
&(((p \wedge q) \to p) \vee \neg q)\\
&((s \to t) \to ((r \to s) \to (r \to t)))
\end{aligned}
$$

Свойства формул

- Свойства формул часто доказывают индукцией по построению формулы:
  - **база индукции**: доказывают, что любая пропозициональная переменная обладает данным свойством;
  - **индукционный переход**: доказывают, что если формулы A и B обладают данным свойством, то формулы $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ тоже обладают данным свойством.
- **Утверждение.** В любой пропозициональной формуле число открывающих скобок равно числу закрываюших.

Приоритет и ассоциативность связок

- Приоритет (в порядке убывания): $\neg$, $\wedge$, $\vee$, $\to$.
- Конъюнкцию и дизъюнкцию полагают левоассоциативными, а импликацию — правоассоциативной.
- Примеры :

$$\begin{array}{rl}
(p \wedge q) & \quad p \wedge q \\
((p \wedge q) \to p) & \quad p \wedge q \to p \\
(((p \wedge q) \to p) \vee \neg q) & \quad (p \wedge q \to p) \vee \neg q \\
((s \to t) \to ((r \to s) \to (r \to t))) & \quad (s \to t) \to (r \to s) \to r \to t
\end{array}$$

План лекции

1. Язык логики высказываний
2. Истинностное значение формул
3. Логические законы
4. Логическое следствие
5. Булева алгебра

Оценки переменных формулы

- Высказывания бывают истинными и ложными.
- Можно задать истинностную интерпретацию пропозициональных формул,
  1. приписав каждой переменной одно из двух значений 0 (ложь, false) или 1 (истина, true);
  2. и задав истиностные значения пропозициональных связок.
- Первую из этих операций иногда называют *оценкой* (valuation).

Истинностное значение формул

- Каждой составной формуле истинностное значение приписывают индуктивно, на основе *таблиц истинности* для пропозициональных связок:

A	$\neg A$
0	1
1	0

A	B	$A \wedge B$	$A \vee B$	$A \to B$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

- Импликация понимается в логике не в причинно-следственном смысле:

$$(2 \times 2 = 5) \to (\text{луна сделана из зеленого сыра});$$
$$(2 \times 2 = 5) \to (\text{снег белый}).$$

Пример

Для формул $p \vee q$, $p \vee q \to q$, $p \wedge q$, $p \wedge q \to q$ всевозможные оценки (valuation) пропозициональных переменных p и q порождают следующую таблицу истинности

p	q	$p \vee q$	$p \vee q \to q$	$p \wedge q$	$p \wedge q \to q$
0	0	0	1	0	1
0	1	1	1	0	1
1	0	1	0	0	1
1	1	1	1	1	1

- Если формула содержит n пропозициональных переменных, то имеется 2^n различных возможных наборов, значения на которых полностью определяют её истинностное значение.
- То есть формула определяет булеву функцию $\mathbb{B}^n \to \mathbb{B}$.
- Если две формулы задают одну и ту же булеву функцию, их называют *эквивалентными*.

- Если формула содержит n пропозициональных переменных, то имеется 2^n различных возможных наборов, значения на которых полностью определяют её истинностное значение.
- То есть формула определяет булеву функцию $\mathbb{B}^n \to \mathbb{B}$.
- Если две формулы задают одну и ту же булеву функцию, их называют *эквивалентными*.
- Являются ли эквивалентными формулы p и $p \wedge (q \to q)$?

Формулы и булевы функции

- Если формула содержит n пропозициональных переменных, то имеется 2^n различных возможных наборов, значения на которых полностью определяют её истинностное значение.
- То есть формула определяет булеву функцию $\mathbb{B}^n \to \mathbb{B}$.
- Если две формулы задают одну и ту же булеву функцию, их называют *эквивалентными*.
- Являются ли эквивалентными формулы p и $p \wedge (q \to q)$?
  Да, если ввести понятие фиктивной переменной и либерально подходить к арности булевой функции.

Уточнение понятия эквивалентности формул

- Формула, содержащая n пропозициональных переменных, определяет n-арную булеву функцию $\mathbb{B}^n \to \mathbb{B}$.
- Арность определяемой функции может быть и больше, скажем, формула $\neg p$ может определять как функцию одной переменной $f(p)$, так и функцию двух переменных $f(p, q)$:

p	$f(p)$
0	1
1	0

p	q	$f(p, q)$
0	0	1
0	1	1
1	0	0
1	1	0

- Переменная, подобная q, носит название *фиктивной*; подобная p — *существенной*.
- Эквивалентность формул мы определяем с точностью до фиктивных переменных.

Другие способы оценки формул

- Можно оценивать формулы, трактуя значения 0 и 1 как целые числа. Тогда значения связок задаются так

$$
\begin{array}{lclcl}
[\![\neg p]\!] & = & 1 - p & & \\
[\![p \wedge q]\!] & = & pq & = & \min(p, q) \\
[\![p \vee q]\!] & = & p + q - pq & = & \max(p, q) \\
[\![p \to q]\!] & = & 1 - p + pq & = & p \leqslant q
\end{array}
$$

- Удобной визуализацией являются диаграммы Венна.

План лекции

1. Язык логики высказываний
2. Истинностное значение формул
3. Логические законы
4. Логическое следствие
5. Булева алгебра

Логические законы

- Формулы истинные всегда, при всех оценках, называют *общезначимыми*, или *тавтологиями*, или *логическими законами*.
- Такова, например, $p \wedge q \to q$:

p	q	$p \wedge q \to q$
0	0	1
0	1	1
1	0	1
1	1	1

- Если есть оценка, на которой формула истинна, то такая формула называется *выполнимой*.
- Если формула является ложной на всех оценках, то она называется *невыполнимой* или *противоречием*.

Условие эквивалентности

- **Утверждение.** Две формулы A и B эквивалентны тогда и только тогда, когда формула $(A \to B) \wedge (B \to A)$ являлтся тавтологией.
- **Доказательство.** Напомним, что две формулы называют эквивалентными, если они задают одну и ту же булеву функцию. Тогда на произвольной оценке

A	B	$A \to B$	$B \to A$	$(A \to B) \wedge (B \to A)$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

Эквивалентность как пропозициональная связка

- Введём новую связку $A \leftrightarrow B$ как сокращение для $(A \to B) \wedge (B \to A)$.
- Эта связка выражает эквивалентность на языке пропозициональных формул.
- Для нее обычно полагают приоритет ниже $\to$.

Эквивалентность как пропозициональная связка

- Введём новую связку $A \leftrightarrow B$ как сокращение для $(A \to B) \wedge (B \to A)$.
- Эта связка выражает эквивалентность на языке пропозициональных формул.
- Для нее обычно полагают приоритет ниже $\to$.
- Являются ли эквивалентными две произвольные тавтологии?

Эквивалентность как пропозициональная связка

- Введём новую связку $A \leftrightarrow B$ как сокращение для $(A \to B) \wedge (B \to A)$.
- Эта связка выражает эквивалентность на языке пропозициональных формул.
- Для нее обычно полагают приоритет ниже $\to$.
- Являются ли эквивалентными две произвольные тавтологии?
  два произвольных противоречия?

Эквивалентность как пропозициональная связка

- Введём новую связку $A \leftrightarrow B$ как сокращение для $(A \to B) \wedge (B \to A)$.
- Эта связка выражает эквивалентность на языке пропозициональных формул.
- Для нее обычно полагают приоритет ниже $\to$.
- Являются ли эквивалентными две произвольные тавтологии?
  два произвольных противоречия?
  две произвольные выполнимые формулы?

Эквивалентность как пропозициональная связка

- Введём новую связку $A \leftrightarrow B$ как сокращение для $(A \to B) \wedge (B \to A)$.
- Эта связка выражает эквивалентность на языке пропозициональных формул.
- Для нее обычно полагают приоритет ниже $\to$.
- Являются ли эквивалентными две произвольные тавтологии?
  два произвольных противоречия?
  две произвольные выполнимые формулы?
- Является ли тавтологией формула $A \leftrightarrow A \leftrightarrow A$?

Эквивалентность как пропозициональная связка

- Введём новую связку $A \leftrightarrow B$ как сокращение для $(A \to B) \wedge (B \to A)$.
- Эта связка выражает эквивалентность на языке пропозициональных формул.
- Для нее обычно полагают приоритет ниже $\to$.
- Являются ли эквивалентными две произвольные тавтологии?
  два произвольных противоречия?
  две произвольные выполнимые формулы?
- Является ли тавтологией формула $A \leftrightarrow A \leftrightarrow A$? newline
  Зависит ли ответ от конкретного правила ассоциативности?

Логические законы (0)

- *нейтральные элементы*

$$\begin{aligned} p \vee 0 &\leftrightarrow p \\ p \wedge 1 &\leftrightarrow p \end{aligned}$$

- *аннигиляторы*

$$\begin{aligned} p \vee 1 &\leftrightarrow 1 \\ p \wedge 0 &\leftrightarrow 0 \end{aligned}$$

- *идемпотентность*

$$\begin{aligned} p \wedge p &\leftrightarrow p \\ p \vee p &\leftrightarrow p \end{aligned}$$

Логические законы (1)

- *коммутативность и ассоциативность конъюнкции*

$$\begin{aligned} p \wedge q &\leftrightarrow q \wedge p \\ (p \wedge q) \wedge r &\leftrightarrow p \wedge (q \wedge r) \end{aligned}$$

- *коммутативность и ассоциативность дизъюнкции*

$$\begin{aligned} p \vee q &\leftrightarrow q \vee p \\ (p \vee q) \vee r &\leftrightarrow p \vee (q \vee r) \end{aligned}$$

- *дистрибутивность конъюнкции относительно дизъюнкции и наоборот*

$$\begin{aligned} p \wedge (q \vee r) &\leftrightarrow p \wedge q \vee p \wedge r \\ p \vee q \wedge r &\leftrightarrow (p \vee q) \wedge (p \vee r) \end{aligned}$$

Логические законы (2)

- *законы поглощения*

$$
\begin{aligned}
p \wedge (p \vee q) \quad &\leftrightarrow \quad p \\
p \vee p \wedge q \quad &\leftrightarrow \quad p
\end{aligned}
$$

- *законы Де Моргана*

$$
\begin{aligned}
\neg(p \wedge q) \quad &\leftrightarrow \quad \neg p \vee \neg q \\
\neg(p \vee q) \quad &\leftrightarrow \quad \neg p \wedge \neg q
\end{aligned}
$$

- *закон контрапозиции*

$$p \to q \quad \leftrightarrow \quad \neg q \to \neg p$$

- *закон снятия двойного отрицания*

$$\neg\neg p \quad \leftrightarrow \quad p$$

Логические законы (3)

- *закон исключеннного третьего*

$$\neg p \quad \vee \quad p$$

- *закон отрицания посылки*

$$\neg p \to p \to q$$

- *выражение импликации через отрицание и дизъюнкцию*

$$p \to q \quad \leftrightarrow \quad \neg p \vee q$$

- *закон Пирса*

$$((p \to q) \to p) \to p$$

Подстановка

- Пусть A — некоторая формула, содержащая пропозициональную переменную p.
- Одновременная замена всех вхождений переменной p в формуле A на некоторую формулу B называется *подстановкой* B вместо p, нотация $A[p := B]$.
- **Теорема о подстановке.** Если A — тавтология, то $A[p := B]$ тоже тавтология для любой формулы B.

Подстановка

- Пусть A — некоторая формула, содержащая пропозициональную переменную p.
- Одновременная замена всех вхождений переменной p в формуле A на некоторую формулу B называется *подстановкой* B вместо p, нотация $A[p := B]$.
- **Теорема о подстановке.** Если A — тавтология, то $A[p := B]$ тоже тавтология для любой формулы B.
- Верна ли эта теорема для выполнимой A?

Подстановка

- Пусть A — некоторая формула, содержащая пропозициональную переменную p.
- Одновременная замена всех вхождений переменной p в формуле A на некоторую формулу B называется *подстановкой* B вместо p, нотация $A[p := B]$.
- **Теорема о подстановке.** Если A — тавтология, то $A[p := B]$ тоже тавтология для любой формулы B.
- Верна ли эта теорема для выполнимой A? если A — противоречие?

План лекции

Логическое (семантическое) следствие

- Пусть имеется набор формул $A_1, A_2, \ldots, A_n$.
- Формулу B называют *логическим следствием* этого набора, если при любой оценке, для которой истинны формулы $A_1, A_2, \ldots, A_n$, истинна также и формула B, нотация
$$A_1, A_2, \ldots, A_n \models B$$
- Символ $\models$ задает отношение следования в метатеории и читается как "влечет" ("влекут").
- Для обозначения того факта, что A — тавтология, часто используют нотацию $\models A$.
- **Примеры.**

$$p, p \to q \models q$$
$$p \models p \vee q$$
$$p \not\models p \wedge q$$

- **Теорема о логическом следствии.** $A_1, A_2, \ldots, A_n \models B$ тогда и только тогда, когда $\models A_1 \land A_2 \land \ldots \land A_n \to B$.

Скелет доказательства.

- $A \models B$ тттк $\models A \to B$.
- $A_1, A_2, \ldots, A_n \models B$ тттк $\models A_1 \to A_2 \to \ldots \to A_n \to B$.
- Вызываем `uncurry`.

■

План лекции

Булева алгебра это непустое множество A вместе с тремя операциями $\wedge$, $\vee$ и $\neg$ и двумя выделенными элементами 0 и 1, для которых выполнены аксиомы:

(асс)	$(p \wedge q) \wedge r = p \wedge (q \wedge r)$	$(p \vee q) \vee r = p \vee (q \vee r)$
(комм)	$p \wedge q = q \wedge p$	$p \vee q = q \vee p$
(погл)	$p \wedge (p \vee q) = p$	$p \vee p \wedge q = p$
(дист)	$p \wedge (q \vee r) = p \wedge q \vee p \wedge r$	$p \vee q \wedge r = (p \vee q) \wedge (p \vee r)$
(нейт)	$p \wedge 1 = p$	$p \vee 0 = p$
(доп)	$p \wedge \neg p = 0$	$p \vee \neg p = 1$

- Какая самая простая булева алгебра?

Булева алгебра это непустое множество A вместе с тремя операциями $\wedge$, $\vee$ и $\neg$ и двумя выделенными элементами 0 и 1, для которых выполнены аксиомы:

(асс)	$(p \wedge q) \wedge r = p \wedge (q \wedge r)$	$(p \vee q) \vee r = p \vee (q \vee r)$
(комм)	$p \wedge q = q \wedge p$	$p \vee q = q \vee p$
(погл)	$p \wedge (p \vee q) = p$	$p \vee p \wedge q = p$
(дист)	$p \wedge (q \vee r) = p \wedge q \vee p \wedge r$	$p \vee q \wedge r = (p \vee q) \wedge (p \vee r)$
(нейт)	$p \wedge 1 = p$	$p \vee 0 = p$
(доп)	$p \wedge \neg p = 0$	$p \vee \neg p = 1$

- Какая самая простая булева алгебра? Вырожденная: $A = \{e\}$, где $e = 0 = 1$.

Булева алгебра это непустое множество A вместе с тремя операциями $\wedge$, $\vee$ и $\neg$ и двумя выделенными элементами 0 и 1, для которых выполнены аксиомы:

(асс)	$(p \wedge q) \wedge r = p \wedge (q \wedge r)$	$(p \vee q) \vee r = p \vee (q \vee r)$
(комм)	$p \wedge q = q \wedge p$	$p \vee q = q \vee p$
(погл)	$p \wedge (p \vee q) = p$	$p \vee p \wedge q = p$
(дист)	$p \wedge (q \vee r) = p \wedge q \vee p \wedge r$	$p \vee q \wedge r = (p \vee q) \wedge (p \vee r)$
(нейт)	$p \wedge 1 = p$	$p \vee 0 = p$
(доп)	$p \wedge \neg p = 0$	$p \vee \neg p = 1$

- Какая самая простая булева алгебра? Вырожденная: $A = \{e\}$, где $e = 0 = 1$.
- Двухэлементная булева алгебра с $A = \{0, 1\}$ и «естественными» определениями операций используется в логике.

Булева алгебра: примеры

- Множество всех подмножеств непустого множества S (булеан, нотация 2^S) образует булеву алгебру с $\wedge := \cap$, $\vee := \cup$, $\neg X := S \setminus X$, $0 := \varnothing$ и $1 := S$.
- Напишите «таблицы истинности» операций $\wedge, \vee, \neg$ для булеана двухэлементного множества $S = \{a, b\}$.
- Непустое множество подмножеств множества S, замкнутое относительно операций пересечения, объединения и дополнения до S, образует булеву алгебру.
- Именно благодаря этому факту «работают» диаграммы Венна.

- $p = q \wedge p$ тогда и только тогда, когда $p \vee q = q$.
- Доказательство. $(\Rightarrow)$.

$$\begin{array}{ccccccc} q & = & q \vee (q \wedge p) & = & q \vee p & = & p \vee q \\ & \text{(погл2)} & & \text{(усл)} & & \text{(комм)} & \end{array}$$

- $(\Leftarrow)$.

$$\begin{array}{cccccccc} p & = & p \wedge (p \vee q) & = & p \wedge q & = & q \wedge p & \\ & \text{(погл1)} & & \text{(усл)} & & \text{(комм)} & & \blacksquare \end{array}$$

- Обратим внимание на двойственность, следующую из двойственности аксиом: верное утверждение остается верным при одновременной взаимной замене $\vee$ на $\wedge$ и 0 на 1.