Математическая логика

mk.cs.msu.ru → Лекционные курсы → Математическая логика (318, 319/2, 241, 242)

Блок 27

Как устроены математические доказательства
Логические исчисления

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2022/2023, весенний семестр

Как устроены математические доказательства

Теорема. Если все мурыки бюкают, а я не бюкаю, то я не мурыка.

Доказательство. ???

После слова «Доказательство» можно записать любой текст, но не всякий такой текст можно признать «правильным».

Доказательство. Это очевидно. ▼

Доказательство. Очевидно, что я не мурыка. ▼

Доказательство. «Я не мурыка» очевидным образом следует из «все мурыки бюкают» и «я не бюкаю». ▼

Где проходит граница между очевидным и неочевидным?

Как устроены математические доказательства

Теорема. Если все мурыки бюкают, а я не бюкаю, то я не мурыка.

Доказательство.
Никто никогда не видел небюкающую мурыку.
Значит, если я не бюкаю, то я не мурыка. ▼

Доказательство.
Известно, что все мурыки бюкают.
Но я не бюкаю.
Значит, я не мурыка. ▼

Доказательство.
Пусть известно, что все мурыки бюкают и я не бюкаю.
Все мурыки бюкают,
а значит, кто не бюкает, тот не мурыка.
Я не бюкаю.
Следовательно, я не мурыка. ▼

Какие отличить правильно построенные и связанные высказывания от тех, которые представляют собой демагогию?

Как устроены математические доказательства

Теорема. Если все мурыки бюкают, а я не бюкаю, то я не мурыка.

Доказательство.
Пусть известно, что все мурыки бюкают и я не бюкаю.
Предположим, что я мурыка.
Раз все мурыки бюкают, то и я бюкаю.
Но известно, что я не бюкаю.
Получено противоречие, из которого следует, что я не мурыка. ▼

Не обманул ли я вас, как это было в парадоксе пьяницы?

Как отличить правильное доказательство от неправильного?

Что такое «доказательство»?

Как устроены математические доказательства

Доказательство — это особым образом устроенный текст:

- Начало текста — это слово «Доказательство»
- Конец текста – это фраза «что и требовалось доказать»
  - или аналогичная: «ч.т.д.», «утверждение доказано», «утверждение верно», «□», «■», «☒», «▼», ...
- Основная часть доказательства — это последовательность **высказываний**, допускающих ровно одну из двух трактовок: высказывание либо **верно**, либо **неверно** — например:
  - $2 \times 2 = 4$: *всем известно, что* это верно
  - рассматриваемая последовательность чисел s монотонна: читатель может и не понимать, монотонна ли s, но каждая последовательность чисел либо монотонна, либо нет
  - $P \neq NP$: никто не знает, совпадают ли классы сложности P и NP, но в любом случае они либо совпадают, либо нет

Как устроены математические доказательства

Доказательство — это особым образом устроенный текст:

- Некоторые высказывания считаются **верными без доказательства**,
  и их можно записать в любом месте доказательства — например:
  - аксиомы и определения:
    «отношение эквивалентности транзитивно, а значит ...»
  - некоторые логические законы:
    «число либо чётно, либо нет, и третьего не дано»
  - высказывания, доказанные ранее:
    «по теореме компактности Мальцева, ...»
  - текущие предположения:
    «предположим, что формула φ необщезначима»

Как устроены математические доказательства

Доказательство — это особым образом устроенный текст:

- Все высказывания следуют друг за другом согласно особым **правилам** (логическим законам) — например:
  - если A верно и из A следует B, то B верно

    (это правило отделения, оно же modus ponens)
  - если A верно для **всех** предметов, то A верно и для предмета x

    (это правило перехода к частному)
  - если из верности A следует, что B и верно, и неверно, то A неверно

    (это правило приведения к абсурду/рассуждения от противного)
- Высказывание «*утверждение верно*» в конце доказательства представляет собой формулировку доказываемого утверждения и должно быть признано верным согласно этим правилам

Как устроены математические доказательства

Вернёмся к примеру:

Теорема. Если все мурыки бюкают, а я не бюкаю, то я не мурыка.

Доказательство.
Пусть известно, что все мурыки бюкают и я не бюкаю.
Предположим, что я мурыка.
Раз все мурыки бюкают, то и я бюкаю.
Но известно, что я не бюкаю.
Получено противоречие, из которого следует, что я не мурыка. ▼

Выделенный текст и знак «▼» — это основная часть доказательства:
последовательность высказываний,
оканчивающаяся формулировкой утверждения

Остальной текст доказательства — это обозначение правил,
на которых основывается корректность (правильность)
устройства основной части доказательства

Как устроены математические доказательства

Чтобы научиться отличать правильные доказательства от неправильных,
следует понять,

- что такое **высказывание**
- какие высказывания **верны без доказательства**
- по каким **правилам** из одних верных выскаызваний получаются другие верные высказывания

Если определить эти понятия и свойства **математически строго**, то в результате получится система, пригодная для строгого определения и анализа математических доказательств:

логическое исчисление

Логические исчисления

Логическое исчисление включает в себя

- алфавит: множество символов,
  используемых для записи высказываний
- синтаксис формул: правила, по которым
  из символов строятся высказывания (формулы исчисления)
- множество аксиом: формул, верных без доказательства
- множество правил вывода,
  согласно которым можно получать одни формулы из других

В исчислениях встречаются формулы
самых разнообразных и причудливых видов

В исчислениях высказываний формулами являются
формулы логики высказываний или наборы таких формул

В исчислениях предикатов формулами являются
формулы логики предикатов или наборы таких формул

Логические исчисления

Для наглядной записи аксиом и правил вывода принято использовать схемы формул: записи, отличающиеся от формул тем, что на месте *обычных* элементов формулы в них могут быть записаны параметры

$\Phi[\![p_1/v_1, \ldots, p_k/v_k]\!]$ — так будем обозначать формулу исчисления, получающуюся из схемы Φ заменой каждого вхождения каждого параметра p_i, $1 \le i \le k$, на его значение v_i

Будем говорить, что схемой Φ порождаются все формулы вида $\Phi[\![p_1/v_1, \ldots, p_k/v_k]\!]$

Например, схемой формулы $A \to (B \to A)$ с параметрами A, B, значения которых — произвольные формулы, в исчислении высказываний

- порождаются формулы $\mathtt{x} \to (\mathtt{x} \to \mathtt{x})$ и $\mathtt{x} \vee \mathtt{y} \to (\mathtt{z} \,\&\, \mathtt{u} \to \mathtt{x} \vee \mathtt{y})$
- **не** порождаются формулы $\mathtt{x} \,\&\, \mathtt{y}$ и $\mathtt{x} \to (\mathtt{x} \to \mathtt{y})$

Схема аксиом исчисления — это схема формулы, которой порождаются только аксиомы исчисления

Логические исчисления

Правило вывода местности n — это
$(n+1)$-местное отношение на множестве формул исчисления

Формула φ выводится из формул $\varphi_1, \ldots, \varphi_n$
по n-местному правилу R, если $(\varphi_1, \ldots, \varphi_n, \varphi) \in R$

Правило вывода местности n обычно записывается так:

$$\frac{\Phi_1, \ldots, \Phi_n}{\Phi}, \qquad (*)$$

где $\Phi_1, \ldots, \Phi_n, \Phi$ — схемы формул
с общим набором параметров $(p_1, \ldots, p_k)$

Правило, записанное в виде (*), — это множество наборов

$$(\Phi_1[\![p_1/v_1, \ldots, p_k/v_k]\!], \ldots, \Phi_n[\![p_1/v_1, \ldots, p_k/v_k]\!], \Phi[\![p_1/v_1, \ldots, p_k/v_k]\!])$$

для всевозможных значений $v_1, \ldots, v_k$ параметров $p_1, \ldots, p_k$

Логические исчисления

Вывод формулы φ_k из множества формул Γ в исчислении $\mathfrak{C}$ — это конечная последовательность формул

$$\varphi_1, \quad \varphi_2, \quad \ldots, \quad \varphi_k,$$

в которой для каждой формулы φ_i, $1 \leq i \leq k$,
выполнено хотя бы одно из трёх условий:

1. $\varphi_i \in \Gamma$
2. φ_i — аксиома исчисления $\mathfrak{C}$
3. Существуют формулы $\varphi_{j_1}, \ldots, \varphi_{j_n}$
   и n-местное правило вывода R исчисления $\mathfrak{C}$, такие что
   - $j_1 < i, \quad \ldots, \quad j_n < i$ и
   - φ_i выводится из $\varphi_{j_1}, \ldots, \varphi_{j_n}$ по правилу R

Формула φ выводима из множества Γ, если существует вывод φ из Γ

Вывод формулы φ из $\emptyset$ также называется доказательством формулы φ

Если для формулы существует доказательство,
то эту формулу принято называть доказуемой в исчислении

Логические исчисления

Пример: резолютивное исчисление дизъюнктов

- Формулы исчисления — это дизъюнкты логики предикатов (*с точностью до перестановки слагаемых и переименования переменных*)
- В исчислении не содержится ни одной аксиомы
- В исчислении содержатся два правила (правило резолюции и правило склейки):

$$\frac{D_1, D_2}{D_r} \qquad \frac{D_1}{D_s}$$

  D_1, D_2, D_r, D_s суть параметры, значения которых — соответственно два дизъюнкта, резольвента дизъюнктов D_1 и D_2 и склейка дизъюнкта D_1

В таком исчислении **вывод** и **выводимость формулы** — это в точности резолютивный вывод и резолютивная выводимость дизъюнктов

Для самостоятельного размышления:

А как устроено исчисление для табличного вывода?