Математическая логика

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

Блок 26

Как устроены математические доказательства
Логические исчисления

Лектор:
Подымов Владислав Васильевич

E-mail:
valdus@yandex.ru

ВМК МГУ, 2020/2021, весенний семестр

Вступление

Утверждение. Если верно A и B, то верно A или B

То же на языке логики высказываний:
Утверждение. $A \,\&\, B \to A \vee B$

Попробуем обосновать это утверждение так,
как это принято в "обычных" математических доказательствах,
не используя особые методы (семантических таблиц, резолюций, ...)

Доказательство. Предположим, что утверждение неверно

Тогда верно $A \,\&\, B$ и неверно $A \vee B$

Так как верно $A \,\&\, B$, верно и A

Так как верно A, верно и $A \vee B$,
что противоречит полученному выше

Значит, предположение неверно ▼

Действительно ли утверждение обосновывается этим "доказательством"?

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

Вступление

Утверждение. $A \mathbin{\&} B \to A \vee B$

Доказательство. Предположим, что верно $A \mathbin{\&} B$

Тогда, в частности, верно A

Значит, верно и $A \vee B$

Так как в предположении о верности $A \mathbin{\&} B$
обоснована верность $A \vee B$, то верно и $A \mathbin{\&} B \to A \vee B$ ▼

Доказательство. Это очевидно ▼

Доказательство. Достаточно заметить, что
из $A \mathbin{\&} B$ всегда следует $A \vee B$ ▼

Доказательство. В лекциях под словом “утверждение”
записываются только верные утверждения,
а значит, это утверждение верно ▼

Как отличить правильные доказательства от неправильных?

Что такое “доказательство”?

Как устроены математические доказательства

Прежде всего, **доказательство** — это текст,
(*явно или неявно*) начинающийся словом "Доказательство"
и оканчивающийся фразой "*Что и требовалось доказать*"
("*Ч.т.д.*", "*Утверждение доказано*", "*Утверждение верно*", "▼", "■", ...)

Основная часть доказательства — это
последовательность **высказываний**,
каждое из которых допускает ровно одну из двух оценок:
высказывание верно, или **высказывание 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

Высказывания доказательства особым образом связаны между собой

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:
  “A либо верно, либо неверно, и третьего не дано”
- теоремы, доказанные ранее:
  “по теореме компактности Мальцева, ...”
- текущие предположения:
  “предположим, что формула φ необщезначима”

Как устроены математические доказательства

Высказывания доказательства особым образом связаны между собой

Остальные высказывания должны следовать 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)

Фраза "*Утверждение верно*" располагается в конце доказательства,
следует тем же логическим законам построения доказательства
и представляет собой повтор формулировки утверждения

Как устроены математические доказательства

Вернёмся к примеру:

Утверждение. $A \mathbin{\&} B \to A \lor B$

Доказательство. Предположим, что верно $A \mathbin{\&} B$

Тогда, в частности, верно A

Значит, верно и $A \lor B$

Так как в предположении о верности $A \mathbin{\&} B$
обоснована верность $A \lor B$, верно и $A \mathbin{\&} B \to A \lor B$ ▼

Зелёный текст и знак "▼" — основная часть доказательства:
последовательность (*верных*) высказываний,
оканчивающаяся формулировкой утверждения

Остальной текст доказательства обозначает то,
как одни высказывания получаются из других
согласно правилам построения 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, $1 \leq i \leq k$, 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, если A и B — параметры и формулами исчисления являются формулы логики высказываний, то $A \to (B \to A)$ — схема формулы, которой

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

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

$$(\Phi_1 \llbracket p_1/v_1, \ldots, p_k/v_k \rrbracket, \ldots, \Phi_n \llbracket p_1/v_1, \ldots, p_k/v_k \rrbracket, \Phi \llbracket p_1/v_1, \ldots, p_k/v_k \rrbracket)$$

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

$$\varphi_1, \quad \varphi_2, \quad \dots, \quad \varphi_k,$$

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

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

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

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