Лекция 3

Математические определения, утверждения и доказательства

План:

1. Определение, утверждение, теорема, критерий. Запись с помощью формулы первого порядка (неформально).
2. Логический вывод, Modus Ponens
3. Методы доказательств: контрапозиция, индукция, от противного, конструктивные (примеры и контрпримеры), неконструктивные.

Литература: [MCS], [Sipser], [Мендельсон]

Изучив основы логики и теории множеств мы можем содержательно поговорить о доказательствах. Наш разговор не будет строгим; строгому изложению этого материала отведено место на втором курсе, но изучать доказательства и что-то доказывать при решении задач, нужно уже сейчас.

3.1 Определения

Определения описывают объекты и понятия. Если определение записано логической формулой, то оно имеет вид предиката $D(x)$, который истиннен тогда и только тогда, когда x, удовлетворяет определению.

Пример 4. Множеству $D = \{x \mid x^2 + 2x + 1 = 0\}$ соответствует предикат $D(x)$, который определяет корни многочлена $x^2 + 2x + 1$, т.е. 1 и -1.

Пример 5. Формула

$$\forall \varepsilon > 0 \; \exists N \in \mathbb{N} : \forall n \geqslant N \; |x_n - a| < \varepsilon$$

Как хорошо известно читателю, определяет предел числовой последовательности. Формально это предикат $D(a, \{x_n\})$, который зависит как от числа a, так и от последовательности $\{x_n\}$. Параметры, от которых зависит истинность формулы, не стоят под кванторами.

Определения, данные словами ничуть не хуже определений, данных формулами. На первом курсе последние встречаются чаще, чтобы научить студентов изложению в кванторах. Так, определение предела можно переформулировать словами: «число a — предел последовательности $\{x_n\}$, если любая окрестность числа a содержит все элементы последовательности, начиная с некоторого номера».

3.2 Математические утверждения

Математические утверждения — это утверждения, которые либо, истинны либо ложны. В отличие от определений, они не зависят от параметров. Если вы встретили утверждение вида «если последовательность x_n сходится, то она ограничена», то в силу вступает математическое соглашение о том, что в случае отсутствия в утверждении квантора по параметру, нужно поставить квантор всеобщности.

Среди математических утверждений выделяют ***теоремы*** — истинные утверждения. Как правило, теоремами называют значимые математические утверждения. Вспомогательные истинные математических утверждения называют ***леммами***, ***предложениями*** и просто ***утверждениями***.

Истинное утверждение называют ***критерием***, если оно имеет вид

$$\forall x \ (A(x) \leftrightarrow B(x)).$$

Критерии устанавливают необходимое и достаточное условие $B(x)$ для выполнения условия $A(x)$ или, что то же самое, устанавливает эквивалентность определений A и B. Например, в математическом анализе критерий Коши устанавливает эквивалентность сходящихся и фундаментальных последовательностей.

Условие $A(x)$ является ***необходимым*** для выполнения $B(x)$, если $\forall x(B(x) \to A(x))$.Симметрично, условие $A(x)$ является ***достаточным***, если $\forall x(A(x) \to B(x))$.Из сказанного вытекает, что $A(x)$ — ***необходимое и достаточное*** условие, если $\forall x(A(x) \leftrightarrow B(x))$.

3.3 Доказательства

Доказательство — это логическое рассуждение, которое убеждает в верности математического утверждения любого непредвзятого слушателя (или читателя). У доказательств есть формальное определение в математической логике, но оно требует введение формальных систем и фактически такие доказательства непроверяемы человеком. Математики любят пользоваться приведённым описанием доказательства, но в утилитарном смысле оно слабо годится. Откуда первокурснику знать, убедят ли его аргументы академика? Поэтому помимо философского описания, мы дадим ещё и утилитарное, но для этого нам потребуется сначала описать логический вывод.

Логический вывод

Представьте, что известна истинность утверждений A и $A \to B$. Из этого можно сразу заключить истинность утверждения B, ведь если B ложно, а A истинно, то импликация $A \to B$ ложна. Это правило вывода записывается так:

$$\frac{A, \quad A \to B}{B} \tag{M.P.}$$

Это правило вывода называется Modus Ponens (сокращённно M.P.). Запись вывода интерпретируется так: если доказано то, что выше черты, то доказано и то, что ниже черты. По аналогии с импликацией, то что выше черты называют посылкой, а то что ниже — заключением.

Правил вывода можно изобрести много. Например, очевидно

$$\frac{\neg A, \quad A \vee B}{B} \ ,$$

но многие такие правила сводятся к Modus Ponens: $A \vee B = \neg A \to B$.

Формально запись

$$\frac{A_1, \quad A_2, \quad \dots \quad A_n}{B}$$

означает, что

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n \to B. \tag{1}$$

Если известно, что все утверждения A_i истинны, и истинно утверждение (1), то эти факты в совокупности влекут (доказывают) истинность утверждения B.

Приведём пример рассуждений с помощью логических выводов.

Пример 6. Алису, Вениамина и Сергея вызвали к директору, потому что кто-то из них на перемене разбил окно. Алиса сказала, что ни она, ни Вениамин окно не разбивали. Вениамин сказал, что Алиса не разбивала окно, а это сделал Сергей, а Сергей сказал, что он не разбивал окно и окно разбила Алиса.

Директору известно, что ровно один школьник сказал правду, другой солгал в каждом из утверждений, а третий дал одно истинное, а другое ложное утверждение. Кто же разбил окно?

Решение. Обозначим через A, B, C высказывания «Алиса разбила окно», «Вениамин разбил окно», «Сергей разбил окно». Точно известно, что истинно высказывание

$$A \vee B \vee C.$$

Среди следующих высказываний истинно ровно одно, ещё в одном истинен ровно один конъюнкт, а в оставшемся ложны оба конъюнкта:

$$\neg A \wedge \neg B, \qquad \neg A \wedge C, \qquad \neg C \wedge A.$$

Предположим, что Алиса сказала правду. Тогда истины высказывания $\neg A$ и $\neg B$. Получаем отсюда, что окно разбил Сергей:

$$\frac{\neg A, \quad \neg B, \quad A \vee B \vee C}{C} \ .$$

Но это невозможно, потому что тогда Вениамин тоже сказал правду:

$$\frac{\neg A, \quad C}{\neg A \land C} \ .$$

Предположив, что правду сказал Вениамин, также получим, что окно разбил Сергей, и Алиса тоже сказала правду, что невозможно.

Получается, что правду сказал Сергей и окно разбила Алиса. На этом решение можно было бы закончить, при условии доверия к составителю задачи. Если быть формальными до конца, то нужно проверить оставшиеся условия. Ясно, что Алиса соврала наполовину (ровно одно из её высказываний истинно), а Вениамин соврал в каждом из утверждений. □

В этом примере, мы показали как использовать запись логического вывода и способ рассуждения с помощью этого метода. Если записать условие примера с помощью формулы, то она получится очень длинной, и придётся мучиться с её упрощением. Приведённые рассуждения похожи на реальные доказательства гораздо больше, чем запись условия утверждения в виде булевой формулы и её последующего преобразования.

Формализуем с помощью вывода наши требования к доказательству. Мы считаем логическое рассуждение доказательством, если оно представимо в виде последовательного применения правил вывода, посылки которых либо известные верные утверждения (из нашего курса, параллельных курсов или общеизвестные факты, например из школьной программы), либо уже доказанные утверждения.

Наши требования относятся к сути, а не к форме. Текст на естественном языке, удовлетворяющий им, ничуть не хуже (а часто лучше), чем набор формул с шагами вывода. Но при написании текста нужно понимать, какие утверждения в нём делаются, как они связаны шагами вывода; полезно помогать себе и читателю доказательства, явно выделяя вспомогательные утверждения.

Мы переходим к перечислению различных методов доказательств. Мы формализуем их с помощью правил вывода и приведём примеры.

Контрапозиция

Закон контрапозиции представим в виде

$$\frac{A \to B}{\neg B \to \neg A} \ .$$

Его смысл становится ясным при переходе на язык множеств (как и его справедливость): $A \subseteq B$ тогда и только тогда, когда $\overline{B} \subseteq \overline{A}$.

Приведём пример его использования.

Утверждение 1. *Если число r иррационально, то и число $\sqrt{r}$ иррационально.*

Доказательство. Воспользовавшись контрапозицией получим равносильное утверждение:

«Если число $\sqrt{r}$ рационально, то число r рационально.»

Это утверждение доказать нетрудно: если число $\sqrt{r}$ рационально, то $\sqrt{r} = \frac{m}{n}$, отсюда $r = \frac{m^2}{n^2}$ и получаем, что число r рационально по определению. □

Индукция

Отдельную сложность у студентов (увы, не только первокурсников) вызывают доказательства по индукции.

Доказательство по индукции возможно только тогда, когда доказываемое утверждение зависит от натурального параметра. То есть доказывается утверждение

$$\forall n \in \mathbb{N} : A(n).$$

С помощью правил вывода схему доказательства по индукции можно описать так:

$$\frac{A(0), \quad \forall n : A(n) \to A(n+1)}{\forall n : A(n)}\ .$$

Первая посылка называется ***базой***, а вторая — ***шагом*** индукции или ***переходом***.

Пример 7. Для каждого целого $n > 0$ справедливо

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

От противного

Мы полагаем, что если утверждение B истинно, то оно не может быть одновременно ложным. Если предположить, что утверждение A ложно и с помощью него доказать, что ложно утверждение B, то есть доказать истинность $\neg A \to \neg B$, то в случае, если утверждение B истинно, утверждение A не может быть ложным — иначе бы мы получили истинность B и $\neg B$. Отсюда вытекает способ доказательства от противного, который можно описать как

$$\frac{\neg A \to \neg B, \quad B}{A}\ .$$

Классический пример такого доказательства — иррациональность числа $\sqrt{2}$.
Доказательство. Доказательство от противного. Положим, что $\sqrt{2} = \frac{m}{n}$, где $\frac{m}{n}$ — несократимая дробь, $m \in \mathbb{Z}$, $n \in \mathbb{N}_1$. Тогда $m^2 = 2n^2$, отсюда m^2 делится на 2, и m делится на 2, значит m^2 делится на 4, и отсюда n^2 делится на 2 и n делится на 2. Но тогда и m делится на 2 и n делится на 2, а значит дробь $\frac{m}{n}$ сократима, пришли к противоречию. □

Примеры и контрпримеры

В случае если утверждение имеет вид $\exists x : A(x)$, его можно доказать, приведя ***пример*** (и доказав справедливость этого примера). Рассмотрим утверждение:

$$\exists n \in \mathbb{N}_1 : \sqrt{n} \in \mathbb{R} \setminus \mathbb{Q},$$

то есть существует натуральное число n, корень из которого — иррациональное число. Это утверждение очевидно верно, и для его доказательства достаточно предъявить число $n = 2$ и доказать иррациональность числа $\sqrt{2}$.

Рассмотрим теперь утверждение

$$\forall n \in \mathbb{N}_1 : \sqrt{n} \in \mathbb{R} \setminus \mathbb{Q}.$$

Это утверждение, очевидно, неверно: достаточно взять $n = 4$ и показать, что $\sqrt{4} = 2 \in \mathbb{Q}$. Для опровержения утверждения с квантором всеобщности $\forall x : A(x)$ достаточно привести ***контрпример***, т.е. пример x, для которого $A(x) = 0$.

Заметим, что для доказательства утверждений вида $\forall x : A(x)$ одного примера не достаточно. Даже если утверждение $A(x)$ верно при каком-то x или очень многих x, даже если их бесконечно много, отсюда ещё не вытекает, что утверждение $A(x)$ верно при всех x. Если все x не проверены, то возможно среди не рассмотренных есть контрпример. Но как проверить бесконечно много x? Вот несколько рецептов. Провести доказательство утверждения $A(x)$, которое не зависит от выбора x. Если x пробегает счётное множество значений (т. е. $\mathbb{N}_0$ или другое множество, элементы которого можно занумеровать натуральными числами), то можно воспользоваться индукцией. Воспользоваться методом доказательства от противного: предположить $\exists x : \neg A(x)$ и прийти к противоречию.

Неконструктивные доказательства

Утверждение вида $\exists x : A(x)$ не обязательно доказывать приводя пример, хотя это очень желательно, если таковой имеется — наличие примера или контрпримера лучше всего убеждает в справедливости утверждения. Бывает так, что само утверждение доказать проще, чем найти пример и мы приведём здесь такое доказательство.

Утверждение 2. *Существуют иррациональные числа a и b, такие что число a^b рационально.*

Доказательство. Положим, что $a = b = \sqrt{2}$. Если число $(\sqrt{2})^{\sqrt{2}}$ рационально, то утверждение доказано. Если нет, то возьмём $a = (\sqrt{2})^{\sqrt{2}}$, а $b = \sqrt{2}$:

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\left(\sqrt{2}\times\sqrt{2}\right)} = \left(\sqrt{2}\right)^{2} = 4.$$

То есть, либо подходит одна пара чисел, либо другая, а какая из — мы не знаем.

Обычно неконструктивные доказательства приводят в некоторое замешательство, особенно при первом знакомстве. Разберёмся со структурой доказательства, формализовав рассуждения.

Само утверждение имеет вид $\exists a, b : A(a, b)$. Мы предположили сначала, что справедливо утверждение $A(\sqrt{2}, \sqrt{2})$, если же оно неверно, то мы доказали, что отсюда вытекает утверждение $A((\sqrt{2})^{\sqrt{2}}, \sqrt{2})$. То есть мы доказали утверждение:

$$\neg A(\sqrt{2}, \sqrt{2}) \to A((\sqrt{2})^{\sqrt{2}}, \sqrt{2}).$$

Перейдя от импликации к дизъюнкции, получаем

$$A(\sqrt{2}, \sqrt{2}) \vee A((\sqrt{2})^{\sqrt{2}}, \sqrt{2}).$$

Доказанная дизъюнкция очевидно влечёт доказываемое утверждение $\exists a, b : A(a, b)$. $\square$