Матлог, лекции

1 Введение

Логика – довольно старая наука, но наш предмет довольно молодой В какой-то момент логики как дисциплины, которая учит просто правильно рассуждать, стало нехватать. Появилась теория множеств. Общего здравого смысла не хватает, нужен строгий математичесий язык. Это рубеж 19-20 веков.

У нас теория множеств не будет фокусом, как это могло бы быть на мат. факультете.

Теория множеств, когда она была впервые сформулирована, была противоречива (как матан, сформулированный Ньютоном). Чтобы уверенно и эффективно заниматься матаном, нужно суметь его формализовать.

<Парадокс Рассела / парадокс брадобрея> Мы приписываем элементу-человеку свойство, которое невыполнимо. Обьекта, выходит, не существует. Мы смогли очень быстро определить противоречие в этом определении. Но, может быть, мы не смогли его определить в других наших определениях? (конструкциях вещественной прямой, и т.д и т.д)

Программа Гильберта.

1. Формализуем математику! Сформулируем теорию на языке (не на русском или английском), который не будет допускать парадоксов,

2. ... и на котором можно будует доказать непротиворечивость.

В 1930 году становится понятно, что сколько-нибудь сильная (= в ней можно построить формальную арифметику) теория не может быть доказана непротиворечивой.

Возможно, сама наша логика неправильная? Эта идея будет нам полезна, и к ней мы ещё вернемся.

Возможно, что это просто свойство мира, и мы хотим невозможного.

Из этих рассуждений выросло большое множество хороших идей, которые оказались полезны в других местах. Матлогика служит широкому кругу нужд.

Мы можем доказывать, что программа работае корректно. Именно доказывать, а не проверять тестами!

Мы можем изучать свойства самих языков. Изоморфизм Карри-Говарда— доказательство это программа, утверждения это тип. Можно изучать языки программирования и можно развернуть изоморфизм: изучать математкиу как язык программирования.

Функциональные языки: окамль + хаскель. Ознакомление с этими языками преставляет собой способ ознакомиться с предметом немного с другой стороны.

2 Исчисление высказываний

Мы говоирм на двух языках: на предметном языке и метаязыке. Предметный язык – это то, что изучается, а метаязык – это язык, НА котором это изучается.

На уроках английского предметным является сам английский, а метаязыком может быть русский. Метаязык – это язык исследователя, а предметный язык – это язык исследоваемого. Что такое язык вообще? Хороший вопрос.

Высказывание — это одно из двух:

1. Большая латниская буква начала алфавита, возможно с индексами и штрихами — это пропозициональные переменные.

2. Выражение вида $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \to \beta)$, $(\neg\alpha)$.

В определении выше альфа и бета это метапеременные— места, куда можно подставить высказывание.

1. α, β, γ — метапеременные для всех высказываний.

2. X, Y, Z — метапеременные для пропозициональных переменных.

Метапеременные являются частью языка исследователя.

В формализации мы останавливаемся до места, в котором мы можем быть уверены, что сможем написать программу, которая всё проверяет.

Сокращение записи, приоритет операций: сначала $\neg$, потом $\&$, потом $\vee$, потом $\rightarrow$. Если скобки опущены, мы восстанавливаем их по приоритетам. Выражение без скобок является частью метаязыка, и становится частью предметного, когда мы восстанавливаем их. Скобки последовательных импликаций расставляются по правилу правой ассоциативности — справа налево.

2.1 Теория моделей

У нас есть истинные значения $\{T, F\}$ в классической логике. И есть оценка высказываний $[\![\alpha]\!]$. Например $[\![A \vee \neg A]\!]$ истинно. Всё, что касается истинности высказываний, касается теории моделей.

Определение 1. Оценка — это функция, сопоставляющая высказыванию его истинное (истинностное) значение.

2.2 Теория доказательств

Определение 2. Аксиомы — это список высказываний. Схема аксиомы — высказывание вместе с метопеременными; при любой подстановке высказываний вместо метапеременной получим аксиому.

Определение 3. Доказательство (вывод) — последовательность высказываний $\gamma_1, \gamma_2 \dots$ где γ_i— любая аксиома, либо существуют $j, k < i$ такие что $\gamma_j \equiv (\gamma_k \rightarrow \gamma_i)$. (знак $\equiv$ здесь сокращение для "имеет вид"). Это правило "перехода по следствию" или Modus ponens.

Определим следующие 10 схем аксиом для того исчисления высказываний, которое мы рассматриваем.

1. $\alpha \rightarrow \beta \rightarrow \alpha$ — добавляет импликацию
2. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)$ — удаляет импликацию
3. $\alpha \wedge \beta \rightarrow \alpha$
4. $\alpha \wedge \beta \rightarrow \beta$
5. $\alpha \rightarrow \beta \rightarrow \alpha \wedge \beta$
6. $\alpha \rightarrow \alpha \vee \beta$
7. $\beta \rightarrow \alpha \vee \beta$
8. $(\alpha \rightarrow \gamma) \rightarrow (\beta \rightarrow \gamma) \rightarrow (\alpha \vee \beta \rightarrow \gamma)$
9. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \neg\beta) \rightarrow (\neg\alpha)$
10. $\neg\neg\alpha \rightarrow \alpha$ — очень спорная штука.

$<$вывод $A \rightarrow A$$>$

3 Теорема о дедукции

Определение 4. (Метаметаопределение). Будем большими греческими буквами $\Gamma, \Delta, \Sigma \dots$ — списки формул, неупорядоченные.

Определение 5. Вывод из гипотез: $\Gamma \vdash \alpha$ (см. лекцию 1)

Теорема 1. $\Gamma, \alpha \vdash \beta$ тогда и только тогда, когда $\Gamma \vdash \alpha \rightarrow \gamma$.

Доказательство. $\Leftarrow$ Пусть $\delta_1, \delta_2 \dots \delta_n \equiv \alpha \to \beta$ выводит $\alpha \to \beta$. Дополним этот вывод двумя новыми высказываниями: $\delta_{n+1} \equiv \alpha$ (дано нам в гипотезе), $\gamma_{n+2} \equiv \beta$ (MP шагов n, $n+1$) — это и требовалось.

- Напишем программу, которая трансформирует один вывод в другой. Инвариант, который мы будем поддерживать: всё до $\alpha \to \delta_i$ — док-во. Доказательство индукцией по n.

  1. База: $n = 1$ — без комментариев.
  2. Если $\delta_1, \dots, \gamma_n$ можно перестроить в доказательство $\alpha \to \gamma_n$, то $\gamma_1 \dots \gamma_{n+1}$ тоже можно перестроить. Разберём случаи:

     (a) δ_i — аксиома или гипотиза из Γ.
     $(i - 0.6)$ δ_i
     $(i - 0.3)$ $\delta_i \to \alpha \to \delta_i$
     (i) $\alpha \to \delta_i$

     (b) $\alpha_i \to \delta$
     $(i - 0.8, i - 0.6, i - 0.4, i - 0.2)$ (доказательство $\alpha \to \alpha$)
     (i) $\alpha \to \alpha$

     (c) δ_i получено из δ_j и δ_k
     (j) $\alpha \to \dots$

     ДОПОЛНИТЬ

□

4 Теория моделей

Мы можем докаывать модели или оценивать их. "Мы можем доказать, что мост не развалится или можем выйти и попрыгать на нём."

Определение 6. $\mathbb{V}$ — истинностное множество.
F — множество высказываний нашего исчисления высказываний.
P — множество пропозициональных переменных.

$$[\![\cdot]\!] : F \to \mathbb{V} \text{ — оценка}$$

Определение 7. Для задания оценки необходимо задать оценку пропозициональных переменных.

$$[\![\cdot]\!] : P \to \mathbb{V} \quad f_P$$

Тогда:

$$[\![x]\!] = f_p(x)$$

Замечание 1. Обозначение: значения пропозициональных переменных будем определять в верхнем индексе: $[\![\alpha]\!]^{A=T,B=F\dots}$

Определение 8. α — общезначна (истинна), если $[\![\alpha]\!] = T$ при любой оценке P.
α — невыполнима (ложна), если $[\![\alpha]\!] = F$ при любой оценке P.
α — выполнима, если $[\![\alpha]\!] = T$ при некоторой f_P.
α — опровержима, если $[\![\alpha]\!] = F$ при некоторой f_P.

Определение 9. Теория корректна, если доказуемость влечёт общезначимость.
Теория полна, если общезначимость влечёт доказуемость.

Определение 10. $\Gamma \models \alpha$ означает, что α следует из $\Gamma = \{\gamma_1, \dots, \gamma_n\}$, если $[\![\alpha]\!] = T$ всегда при $[\![\gamma_i]\!] = T$ при любых i.

Теорема 2. Исчисление высказываний корректно

$$\vdash \alpha \text{ влечёт } \models \alpha.$$

Доказательство. Индукция по длине доказательства.

Разбор случаев:

1. γ_n аксиома $\implies$ построить таблицу истинности
2. γ_n — м.п. γ_j, γ_k

$\square$

Мы даём доказательство на метаязыке, не пускаясь в отчаянный формализм. Такая строгость нас устраевает.

В матлогике бесмысленно формализовывать русский язык. Она нужна, чтобы дать ответы на сложные вопросы в математике, где здравого смысла недостаточно и нужна формализация.

5 Полнота исчисления высказываний

Теорема 3. Исчисление высказываний полно.

Определение 11. ${}_{[\beta]}\alpha = \begin{cases} \alpha, & [\![\beta]\!] = T \\ \neg\alpha, & [\![\beta]\!] = F \end{cases}$

Лемма 3.1. ${}_{[\alpha]}\alpha,\ {}_{[\beta]}\beta \vdash_{[\alpha\star\beta]} \alpha\star\beta$
${}_{[\alpha]}\alpha \vdash_{[\neg\alpha]} \neg\alpha$

Лемма 3.2. Если $\Gamma \vdash \alpha$, то $\Gamma, \Delta \vdash \alpha$.

Лемма 3.3. Пусть дана α, $X_1, \dots, X_n$ — её переменные.

$${}_{[X_1]}X_1, \dots {}_{[X_n]}X_n \ \vdash_{[\alpha]} \alpha$$

Доказательство. Индукция по структуре. ДОПОЛНИТЬ $\square$

Сократим запись и вместо этой кучи X будем писать X'.

Лемма 3.4. Если $\models \alpha$, то $X' \vdash \alpha$.

Лемма 3.5.

$$\Gamma, Y \vdash \alpha, \quad \Gamma, \neg Y \vdash, \text{ то } \Gamma \vdash \alpha$$

Теорема 4. Если $\models \alpha$, то $\vdash \alpha$.

6 Интуиционистская логика

Мы не хотим дурацких коснтрукций вроде парадокса брадобрея. Мы не хотим странных, но логически верных утверждений вроде $A \to B \vee B \to A$. Интуиционисткая логика предлагает свою математику, в которой своя интерпретация логических связок. ВНК-интерпретация (Брауер-Гейтинг-Колмогоров).

- $\alpha, \beta, \gamma \dots$ — это конструкции.
- $\alpha \wedge \beta$ если мы умеем строить и α, и β.
- $\alpha \vee \beta$, если мы умеем строить α, β и знаем, что именно.
- $\alpha \to \beta$, если мы умеем перестроить α в β.
- $\perp$ — не имеет построения
- $\neg\alpha \equiv \alpha \to \perp$

"Теория доказательств". Рассмотрим классическое исчисление высказываний и заменим схему аксиом 10 на следующую

$$\alpha \to \neg\alpha \to \beta$$

В этой формализации мы следуем не сути интуиционисткой логики, а традиции. В интуиционисткой логике формализм это не источник логики.

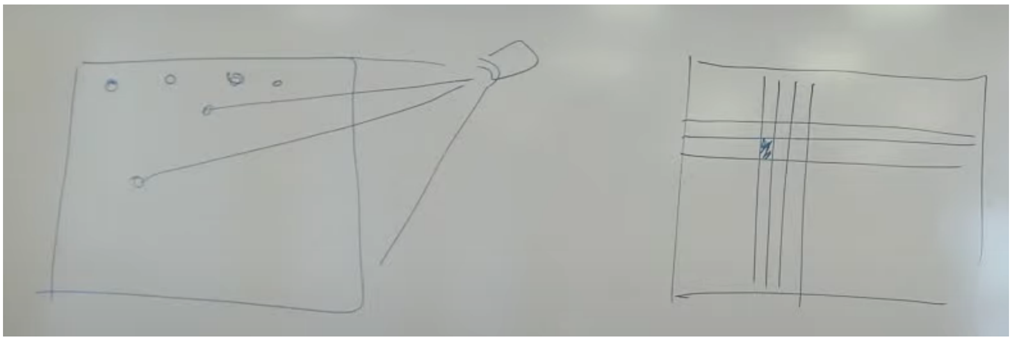
Примеры моделей.

1. Модели КИВ подходят: корректны, но не полны.

2. Пусть X топологическое пространство.

7 Общая топология

Раньше были телевизоры с *бесконченым* количеством пикселей (это зависит от химических свойств вещества кинескоп).



Возьмем множество X. Определим на нем топологию как подмножество множества всех подмножеств $\Omega \subseteq \mathcal{P}(X)$. Ω — топология, если это множество открытых множеств и выполнены следующие условия:

1. $\varnothing, X \in \Omega$;

2. $\bigcup\limits_i \in \Omega$, если все $A_i \in \Omega$;

3. $\bigcap\limits_{i=1}^{n} A_i \in \Omega$, если $A_1, \ldots, A_n \in \Omega$.

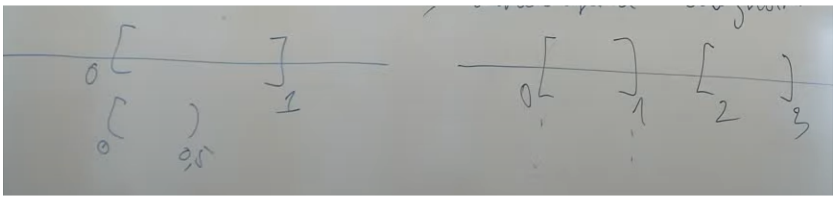
То есть топологическое пространство — пара $\langle X, \Omega \rangle$ и про Ω верны приведенные выше три утверждения.

Определение 12 (Замкнутое мноежство)**.** Множество B такое, что $X \setminus B \in \Omega$ называется замкнутым.

Определение 13 (Связное топологическое пространство)**.** $\langle X, \Omega \rangle$ связно, если нет $A, B \in \Omega \ : \ A \cup B = X$ и $A \cap B = \varnothing$

Определение 14 (Подпространство)**.** $\langle X_1, \Omega_1 \rangle$ — подпространство $\langle X, \Omega \rangle$, если $X_1 \subseteq X$ и $\Omega_1 = \{a \cap X_1 \mid a \in \Omega\ \}$

Определение 15 (Связное множество)**.** Множество, являющееся связным подпространством.



7.1 Примеры топологических пространств

Возьмем дерево (граф). Множество X — множество вержин. Ω — множество всех вершин, что $B \in \Omega$, если $a \in B$, $x \leqslant a$ влечет $x \in B$. То есть Ω — семейство множеств вершин, которые входят вместе с поддеревом.

Теорема 5. Граф без цикла свяен тогда и только тогда, когда оно своязно как топологическое пространство.

Доказательство будет в дз. □

Определение 16 (Решетки)**.** X — частично упорядоченное множество отношением $\leqslant$.
Множество верхних граней a, b — множество $\{x \in X \mid a \leqslant x, b \leqslant x\}$.
Множество нижних граней a, b — $a \sqcup b$ — множество $\{x \in X \mid a \geqslant x, b \geqslant x\}$.
A, наименьший элемент A — такой $a \in A$, что нет $b \in A$, $b \leqslant a$.
$a + b =$ наименьший элемент множества верхних граней.
$a * b =$ наибольший элемент множества нижних граней.

Решетка — частично упорядоченное множество, где для каждых двух элементов существуют $a + b$ и $a * b$.

Пример 1. Дерево — не решетка (в общем случае), так как $a + b$ есть, а $a * b$ может не быть.

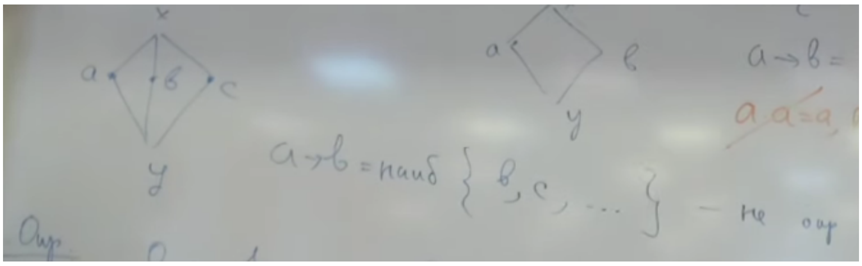
Теорема 6. Пусть $\langle X, \Omega \rangle$ топологическое пространство, $A, B \in \Omega$. $A \leqslant B$, если $A \subseteq B$.
Тогда $\langle \Omega, \leqslant \rangle$ — решетка. $A \cdot B = A \cap B$, $A + B = A \cup B$.

Определение 17. Дистрибутивная решетка — это такая решетка, что $a, b, c \in \Omega$, $a + (b \cdot c) = (a + b) \cdot (a + c)$.

Лемма 6.1. Для дистрибутивной решетки так же верно, что $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Определение 18. Псевдодополнение $a \to b =$ наименьшее$\{c \mid a \cdot c \leqslant b\} = b$.

Определение 19. Диамант — такая решетка, что там нет для кого-то псевдодопллнения.



Определение 20. Решетка с псевдодополнением для всех элементов называется импликативной.

Определение 21 (0 и 1)**.** .

- 0 — элемент, что $0 \leqslant x$ при всех x.
- 1 — элемент, что $x \leqslant 1$ при всех x.

Теорема 7 (В импликативной решетке 1 есть всегда)**.** $X, \leqslant$ — импликативная решетка.
Рассмотрим $a \to a =$ наиб$\{c \mid q \cdot c \leqslant a\} =$ наиб$X = 1$.

Теорема 8. Рассмотрим $\langle X, \Omega \rangle$ — импликативная решетка с 0. Рассмотрим И.И.В.
Определим оценки $\mathbb{V} = X$:

- $[\![\alpha \& \beta]\!] = [\![\alpha]\!] \cdot [\![\beta]\!]$.
- $[\![\alpha \vee \beta]\!] = [\![\alpha]\!] + [\![\beta]\!]$.

- $[\![\alpha \to \beta]\!] = [\![\alpha]\!] \to [\![\beta]\!]$.
- $[\![\neg\alpha]\!] = [\![\alpha]\!] \to 0$.

α истинно, если $[\![\alpha]\!] = 1$.
Полученная модель — корректная модель И.И.В.

У нас будет натуральный вывод, интуиция и все такое.
$\overline{\Gamma, \varphi \vdash \varphi}$ (аксиома).
Вывод утверждения в доказательстве $\Gamma \vdash \varphi$.

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}, \quad \frac{\Gamma, \varphi \vdash \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}, \quad \frac{\Gamma, \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \& \psi}, \quad \frac{\Gamma, \vdash \varphi \& \psi}{\Gamma \vdash \varphi}, \quad \frac{\Gamma, \vdash \varphi \& \psi}{\Gamma \vdash \psi},$$
$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma, \varphi \vdash \rho \quad \Gamma, \psi \vdash \rho \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}, \quad \frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}.$$

В теореме выше нужно добавить, что $[\![\bot]\!] = 0$.
$\neg\alpha \equiv \alpha \to \bot$.