

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 и общего здравого смысла оказалось не достаточно, нужен строгий математический язык. Это рубеж 19-20 веков.

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 или парадокс брадобрея — один пример парадокса в наивной теории множеств. Определим множество

$$A = \{X | X \notin X\}$$

Вопрос, принадлежит ли само A множеству A , неразрешим — оба варианта ответа (принадлежит / не принадлежит) приводят к противоречию с определением A .

У этого парадокса есть другая формулировка. На острове брадобрей бреет всех, кто не бреется сам. Вопрос — бреет ли брадобрей сам себя?

Мы приписываем элементу-человеку свойство, которое невыполнимо. Объект, 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.)?

В связи с этим была сформулирована программа Гильберта:

1. Формализуем математику! Сформулируем теорию на языке (не на русском или английском), который не будет допускать парадоксов,
2. ... и на котором можно будет доказать непротиворечивость.

В 1930 году становится понятно, что про сколько-нибудь сильную теорию (т.е. ту, в которой можно построить формальную арифметику) нельзя доказать, что она непротиворечивая.

Возможно, сама наша логика неправильная? Эта идея будет нам полезна, и к ней мы ещё вернемся. Возможно, что недоказуемость непротиворечивости — просто свойство нашего мира, и мы хотим невозможного. Из этих рассуждений выросло большое множество хороших идей, которые оказались полезны и в других местах.

Матлогика служит широкому кругу нужд. Мы можем доказывать, что программа работает 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 математику как язык программирования.

Функциональные языки: `Osaml + Haskell`. Ознакомление с этими языками представляет собой способ ознакомиться с предметом немного с другой стороны.

2 Исчисление высказываний

Мы говорим 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 исследуемого. Что такое язык вообще? Хороший вопрос.

Высказывание — это одно из двух:

1. Большая латинская буква начала алфавита, возможно с индексами и штрихами — это пропозициональные переменные;
2. Выражение вида $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$, $(\neg \alpha)$.

В определении выше α и β это метAPERЕМЕННЫЕ — места, куда можно подставить высказывание.

1. α, β, γ — метAPERЕМЕННЫЕ для всех высказываний;
2. X, Y, Z — метAPERЕМЕННЫЕ для пропозициональных переменных.

МетAPERЕМЕННЫЕ 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 $\llbracket \alpha \rrbracket$. Например $\llbracket A \vee \neg A \rrbracket$ 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 метAPERЕМЕННЫМИ; при любой подстановке высказываний вместо метAPERЕМЕННОЙ 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. $\alpha \wedge \beta \rightarrow \alpha$ — удаляет конъюнкцию;
4. $\alpha \wedge \beta \rightarrow \beta$;
5. $\alpha \rightarrow \beta \rightarrow \alpha \wedge \beta$ — добавляет конъюнкцию
6. $\alpha \rightarrow \alpha \vee \beta$ — добавляет дизъюнкцию
7. $\beta \rightarrow \alpha \vee \beta$
8. $(\alpha \rightarrow \gamma) \rightarrow (\beta \rightarrow \gamma) \rightarrow (\alpha \vee \beta \rightarrow \gamma)$;
9. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \neg \beta) \rightarrow (\neg \alpha)$ — добавляет отрицание
10. $\neg \neg \alpha \rightarrow \alpha$ — снимает двойное отрицание (очень спорная штука).

Вывод простого утверждения $A \rightarrow A$ выглядит вот так:

1. $A \rightarrow (A \rightarrow A) \rightarrow A$ (сх. 1)
2. $A \rightarrow A \rightarrow A$ (сх. 1)
3. $(A \rightarrow A \rightarrow A) \rightarrow (A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow (A \rightarrow A)$ (сх. 2)
4. $(A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow (A \rightarrow A)$ (М.Р. 2, 3)
5. $A \rightarrow A$ (М.Р. 1, 3)

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 $\Gamma \vdash \alpha \rightarrow \beta$.

Доказательство. \Leftarrow Пусть $\delta_1, \delta_2 \dots \delta_n \equiv \alpha \rightarrow \beta$ выводит $\alpha \rightarrow \beta$. 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 $\alpha \rightarrow \delta_i$ — док-во. Доказательство индукцией по n .

1. База: $n = 1$ — без комментариев.

2. Если $\delta_1, \dots, \gamma_n$ можно перестроить в доказательство $\alpha \rightarrow \gamma_n$, то $\gamma_1 \dots \gamma_{n+1}$ тоже можно перестроить. Разберём случаи:

— δ_i — гипотеза из Γ . Тогда

(i — 0.1) δ_i (аксиома или гипотеза)

(i — 0.2) $\delta_i \rightarrow \alpha \rightarrow \delta_i$ (схема 1)

(i) $\alpha \rightarrow \delta_i$ (MP)

ДОПОЛНИТЬ

□

4 Теория моделей

Мы можем доказывать 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.

$$\llbracket \cdot \rrbracket : F \rightarrow \mathbb{V} \text{ — оценка}$$

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

$$\llbracket \cdot \rrbracket : P \rightarrow \mathbb{V} \quad f_P$$

Тогда:

$$\llbracket x \rrbracket = f_P(x)$$

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

Определение 8. α — общезначна (истинна), если $\llbracket \alpha \rrbracket = T$ при любой оценке P .

α — невыполнима (ложна), если $\llbracket \alpha \rrbracket = F$ при любой оценке P .

α — выполнима, если $\llbracket \alpha \rrbracket = T$ при некоторой f_P .

α — опровержима, если $\llbracket \alpha \rrbracket = F$ при некоторой f_P .

Определение 9. Теория корректна, если доказуемость влечёт общезначимость.

Теория полна, если общезначимость влечёт доказуемость.

Определение 10. $\Gamma \models \alpha$, α следует из $\Gamma = \{\gamma_1, \dots, \gamma_n\}$, если $\llbracket \alpha \rrbracket = T$ всегда при $\llbracket \gamma_i \rrbracket = T$ для любых i .

Теорема 2. Исчисление высказываний корректно, т.е

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

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

Доказательство. Индукция по длине доказательства. Не очень сложно. ДОПОЛНИТЬ. \square

В матлогике бессмысленно 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. $[\beta]\alpha = \begin{cases} \alpha, & \llbracket \beta \rrbracket = T \\ \neg\alpha, & \llbracket \beta \rrbracket = F \end{cases}$

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

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 конструкций вроде парадокса брадобрея. Мы не хотим странных, но логически верных утверждений вроде $A \rightarrow B \vee B \rightarrow A$. Интуиционистская 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.
- $\alpha \rightarrow \beta$, если мы умеем перестроить α в β .
- \perp — не имеет построения
- $\neg\alpha \equiv \alpha \rightarrow \perp$

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

$$\alpha \rightarrow \neg\alpha \rightarrow \beta$$

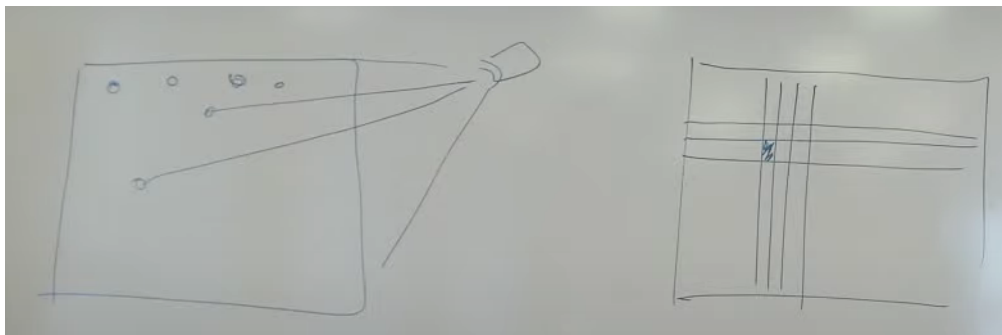
В этой формализации мы следуем не сути интуиционистской логики, а традиции. В интуиционистской логике формализм это не источник логики.

Примеры моделей.

1. Модели КИВ подходят: корректны, но не полны.
2. Пусть X топологическое пространство.

7 Общая топология

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



Определение 12. Топологическим пространством называется упорядоченная пара (X, Ω) , $\Omega \subset 2^X$, причем выполнено

1. $\emptyset, X \in \Omega$
2. $\bigcup A_i \in \Omega$ если $\forall i A_i \in \Omega$
3. $\bigcap_n A_i \in \Omega$, если $\forall i A_i \in \Omega$

Определение 13. Замкнутым называется множество B такое, что его дополнение $X \setminus B \in \Omega$ открыто.

Определение 14. Связным топологическим пространством называется такое топ. пространство (X, Ω) , в котором нет $A, B \in \Omega$ таких, что $A \cup B = X$ и $A \cap B = \emptyset$.

Определение 15. Подпространством пространства (X, Ω) называется топологическое пространство (X_1, Ω_1) , где $X_1 \subset X$ и $\Omega_1 = \{A \cap X_1 \mid A \in \Omega\}$. Это подпр-во так же называется индуцированным подпространством.

Например, промежуток $[0, \frac{1}{2})$ не является открытым в \mathbb{R} , но является открытым в подпространстве, индуцированным $[0, 1]$.

Определение 16. Подмножество пр-ва называется связным, если связно индуцированное им подпространство.

Пример: множество $[0, 1] \cup [2, 3]$ является несвязным подмножеством \mathbb{R} .

Пример 1. Определим топологию на ациклическом графе следующим образом: подвесим все его деревья (компоненты связности) и назовём множество открытым, если вместе с каждой своей вершиной оно содержит его поддереву.

Теорема 5. Лес (ациклический граф) связан титт., когда он связан как топ. пространство.

8 Решетки

Определение 17. Рассмотрим частично-упорядоченное множество X , (X, \leq) .

Множество верхних граней $\{a, b\} = \{x \in X \mid a \leq x, b \leq x\}$.

Множество нижних граней $\{a, b\} = \{x \in X \mid a \geq x, b \geq x\}$.

Наименьший элемент A — такой $a \in A$, что нет $b \in A$, такого что $b \leq a$. Аналогичное определение даётся наибольшему элементу.

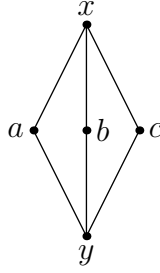


Рис. 1: Решетка, в которой для a, b не определено псевдодополнение

$a + b$ — наименьший элемент множества верхних граней $\{a, b\}$.

$a \cdot b$ — наибольший элемент множества нижних граней $\{a, b\}$.

(X, \leq) называется решеткой, если для любых $a, b \in X$ определены $a + b$ и $a \cdot b$.

Замечание 2. Наибольший и максимум это не одно и то же!

Пример 2. Топологическое пространство с порядком по включению является решеткой.

Антипример: произвольное дерево не является решеткой.

Определение 18. Дистрибутивной решеткой называется такая решетка, в которой

$$(a + b)c = ac + bc \quad a + bc = (ab) + (ac)$$

Лемма 5.1. Для дистрибутивной решетки так же верно, что $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Определение 19. Псевдодополнение $a \rightarrow b$ это наибольший c из всех таких c , что $ac \leq b$.

Решетка, в которой псевдодополнение определено для всех пар элементов, называется импликативной.

Определение 20. Ноль 0 и единица 1 — это нейтральные элементы операций $+$ и \cdot одновременно. Другими словами

- 0 — такой элемент, что $0 \leq x$ для всех x ;
- 1 — такой элемент, что $x \leq 1$ для всех x .

Теорема 6. Рассмотрим $\langle X, \Omega \rangle$ — импликативную решетку с 0 . Определим оценки $\mathbb{V} = X$:

- $\llbracket \alpha \& \beta \rrbracket = \llbracket \alpha \rrbracket \cdot \llbracket \beta \rrbracket$.
- $\llbracket \alpha \vee \beta \rrbracket = \llbracket \alpha \rrbracket + \llbracket \beta \rrbracket$.
- $\llbracket \alpha \rightarrow \beta \rrbracket = \llbracket \alpha \rrbracket \rightarrow \llbracket \beta \rrbracket$.
- $\llbracket \neg \alpha \rrbracket = \llbracket \alpha \rrbracket \rightarrow 0$.

α истинно, если $\llbracket \alpha \rrbracket = 1$, и $\llbracket \perp \rrbracket = 0$.

Полученная модель — корректная модель И.И.В.

Теорема 7. В импликативной решетке 1 есть всегда.

Доказательство. Пусть $\langle X, \leq \rangle$ — импликативная решетка. Рассмотрим $a \rightarrow a = \text{наиб}\{c \mid a \cdot c \leq a\} = \text{наиб}\{X\} = 1$. □

Исчисление высказываний с которым мы работали называется исчислением гильбертовского типа — очень много аксиом и практически одно правило вывода, и оно несколько неудобно, как мы увидели. Не мы одни такие умные. Люди придумали что-то ещё.

(Полноты ради секвенциальное исчисление будет обсуждаться в конце, если останется время.)

Теперь мы обсудим кое-что ещё. Доказательства в этой системе рисуются в виде дерева, в отличии от длинного списка, как получается в гильбертовском исчислении. Вид док-ва: $\Gamma \vdash \varphi$.

Схемы:

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}, \quad \frac{\Gamma, \varphi \vdash \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}, \quad \frac{\Gamma, \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \& \psi}, \quad \frac{\Gamma, \vdash \varphi \& \psi}{\Gamma \vdash \varphi}, \quad \frac{\Gamma, \vdash \varphi \& \psi}{\Gamma \vdash \psi},$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma, \varphi \vdash \rho \quad \Gamma, \psi \vdash \rho \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}, \quad \frac{\Gamma \vdash \perp}{\Gamma \vdash \varphi}.$$

9 Алгебра Гейтинга

Определение 21. Алгебра Гейтинга — это импликативная решетка с 0.

Определение 22. $\neg a \equiv a \rightarrow 0$.

Определение 23. Булева алгебра — алгебра Гейтинга, где $a + \neg a = 1$.

Пример.

Определение 24. $\alpha \preceq \beta$, если $\alpha \vdash \beta$.

Определение 25. $\alpha \approx \beta$, если $\alpha \preceq \beta$ и $\beta \preceq \alpha$.

Определение 26. Пусть E — множество всех высказываний ИИВ. Тогда $[E]_{\approx}$ — фактор-множество высказываний по отношению \approx , называется алгеброй Линденбаума, L .

Теорема 8. Алгебра Линденбаума — это алгебра Гейтинга.

Теорема 9. L — полная и корректная модель ИИВ.

Теорема 10. Алгебра Гейтинга — полная и корректная модель ИИВ.

Определение 27. Исчисление дизъюнктно, если для любых α, β доказуемость $\alpha \vee \beta$ влечет доказуемость или α или β .

Теорема 11. ИИВ дизъюнктно.

Определение 28. Пусть A, B — алгебры Гейтинга. f называется гомоморфизмом, если $f(0_A) = 0_B$, $f(1_A) = 1_B$, $f(\alpha \star_A \beta) = f(\alpha) \star_B f(\beta)$.

Определение 29. Гёделева алгебра — та, в которой $a + b = 1$ влечёт $a = 1$ или $b = 1$.

Определение 30. Пусть A — алгебра Гейтинга. Определим $\Gamma(A)$. $\gamma(x) = \begin{cases} \omega, & x = 1_A \\ x, & x < 1_A \end{cases}$.

Добавим 1_B , которое больше каждого $\gamma(t)$.

Теорема 12. $\Gamma(A)$ — гёделева алгебра. В этой алгебре $\Gamma(A)$ выполнено $a + b = 1$ влечёт $a = 1$ или $b = 1$.

Теорема 13. $\Gamma(L)$ гёделева.

Определим $\gamma : \Gamma(L) \rightarrow L$: $g(x) = \begin{cases} 1, & x = 1 \text{ или } x = \omega \\ x, & \text{иначе} \end{cases}$. Утверждается, что это гомоморфизм.

Рассмотрим ИИВ и алгебры $L, \Gamma(L)$. Рассмотрим $\vdash \alpha \vee \beta$. $\Gamma(L)$ — гёделева алгебра, т.е алгебра Гейтинга.

...

Определение 31. Модель ИИВ называется табличной, если множество истинностных значений $V = S$, $\llbracket \alpha \star \beta \rrbracket = f_{\star}(\llbracket \alpha \rrbracket, \llbracket \beta \rrbracket)$. и есть два значения, выделенная истинна И, и $\llbracket \alpha \rrbracket = \text{И}$ в том и только том случае, когда $\models \alpha$.