Практическая теория типов

Лекция 6: Соответствие Карри-Ховарда

Agenda

1. Формальные логики
2. Модели логики
3. ВНК нотация
4. Соответствие Карри-Ховарда-Ламбека
5. Примеры

Логики

Что такое формальная логика?

- формальная система, состоящая из языка, набора аксиом и правил вывода
- основная задача - изучение справедливости утверждений и способа их выводимости
- используется часто для построения систем типов языков программирования

Свойства формальных логик

- **консистентность** - существует хотя бы одна формула, которая не доказуема в данной логике (иначе такая система бессмысленна)
- **разрешимость** - существует алгоритм, проверяющий правильность доказательства
- **soundness** - если выражение $\Gamma \vdash A$ выводимо, то $\Gamma \models A$
- **completeness** - если выражение $\Gamma \models A$ выводимо, то $\Gamma \vdash A$

Формальные логики

- Интуиционистская
- Классическая
- Линейная
- Аффинная
- Упорядоченная
- Релевантная
- Логика первого порядка (исчисление предикатов)
- Логики высоких порядков

Формализация доказательств

$$\forall\varepsilon.(\varepsilon > 0 \Rightarrow \exists\eta.(\eta > 0 \land \forall x.|x| < \eta \Rightarrow |2x| < \varepsilon))$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varepsilon > 0 \vdash \varepsilon > 0}}{\varepsilon > 0 \vdash (\varepsilon/2) \times 2 > 0 \times 2}}{\varepsilon > 0 \vdash \varepsilon/2 > 0} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |x| < \varepsilon/2}}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |2x|/2 < \varepsilon/2}}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |2x| < \varepsilon}}{\varepsilon > 0 \vdash |x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \forall x.|x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \varepsilon/2 > 0 \land \forall x.|x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \exists\eta.(\eta > 0 \land \forall x.|x| < \eta \Rightarrow |2x| < \varepsilon)}}{\vdash \varepsilon > 0 \Rightarrow \exists\eta.(\eta > 0 \land \forall x.|x| < \eta \Rightarrow |2x| < \varepsilon)}}{\vdash \forall\varepsilon.(\varepsilon > 0 \Rightarrow \exists\eta.(\eta > 0 \land \forall x.|x| < \eta \Rightarrow |2x| < \varepsilon))}$$

Натуральный вывод

- формализм для доказательств, разработанный Генценым и Яськовским в 1934
- основан на безаксиоматическом подходе
    - Гильбертовские исчисления, основная альтернатива для натурального вывода, основаны на развитой системе аксиом и небольшом количестве правил вывода
- наиболее известные системы натурального вывода:
    - **NK** - для классической логики
    - **NJ** - для интуиционисткой логики

NJ: формализм

NJ состоит из формул, задаваемых по следующему правилу

$$A, B ::= X \mid A \Rightarrow B \mid A \wedge B \mid \top \mid A \vee B \mid \bot \mid \neg A$$

контекста $\Gamma = A_1, \ldots, A_n$

суждений или секвентов $\Gamma \vdash A$

правил вывода $$\frac{\Gamma_1 \vdash A_1 \qquad \ldots \qquad \Gamma_n \vdash A_n}{\Gamma \vdash A}$$

NJ: правила вывода

$$\frac{}{\Gamma, A, \Gamma' \vdash A}(\text{ax})$$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}(\Rightarrow_{\mathrm{E}}) \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}(\Rightarrow_{\mathrm{I}})$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}(\wedge^{\mathrm{l}}_{\mathrm{E}}) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}(\wedge^{\mathrm{r}}_{\mathrm{E}}) \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}(\wedge_{\mathrm{I}})$$

$$\frac{}{\Gamma \vdash \top}(\top_{\mathrm{I}})$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}(\vee_{\mathrm{E}}) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}(\vee^{\mathrm{l}}_{\mathrm{I}}) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}(\vee^{\mathrm{r}}_{\mathrm{I}})$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}(\bot_{\mathrm{E}})$$

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}(\neg_{\mathrm{E}}) \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}(\neg_{\mathrm{I}})$$

NJ: примеры вывода

Коммутативность дизъюнкции

$$(A \vee B) \Rightarrow (B \vee A)$$

$$\dfrac{\dfrac{}{A \vee B \vdash A \vee B}\,(\mathrm{ax}) \qquad \dfrac{\dfrac{}{A \vee B, A \vdash A}\,(\mathrm{ax})}{A \vee B, A \vdash B \vee A}\,(\vee_{\mathrm{I}}^{\mathrm{r}}) \qquad \dfrac{\dfrac{}{A \vee B, B \vdash B}\,(\mathrm{ax})}{A \vee B, B \vdash B \vee A}\,(\vee_{\mathrm{I}}^{\mathrm{l}})}{\dfrac{A \vee B \vdash B \vee A}{\vdash A \vee B \Rightarrow B \vee A}\,(\Rightarrow_{\mathrm{I}})}\,(\vee_{\mathrm{E}})$$

NJ: примеры вывода

Прямой закон контрапозиции:

$$(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, \neg B, A \vdash \neg B}\,(\mathrm{ax}) \qquad \dfrac{\dfrac{}{A \Rightarrow B, \neg B, A \vdash A \Rightarrow B}\,(\mathrm{ax}) \qquad \dfrac{}{A \Rightarrow B, \neg B, A \vdash A}\,(\mathrm{ax})}{A \Rightarrow B, \neg B, A \vdash B}\,(\Rightarrow_{\mathrm{E}})}{A \Rightarrow B, \neg B, A \vdash \bot}\,(\neg_{\mathrm{E}})}{A \Rightarrow B, \neg B \vdash \neg A}\,(\neg_{\mathrm{I}})}{A \Rightarrow B \vdash \neg B \Rightarrow \neg A}\,(\Rightarrow_{\mathrm{I}})}{\vdash (A \Rightarrow B) \Rightarrow \neg B \Rightarrow \neg A}\,(\Rightarrow_{\mathrm{I}})
$$

NJ: структурные правила

Структурные правила - это правила, которые основаны на структуре логического доказательства, а не на преобразовании конкретных логических связок. Обычно выделяют 4 основных правила:

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C}\ (\mathrm{xch}) \qquad \frac{\Gamma, A, A, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\mathrm{contr})$$

$$\frac{\Gamma, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\mathrm{wk}) \qquad \frac{\Gamma, \top, \Gamma' \vdash A}{\Gamma, \Gamma' \vdash A}\ (\mathrm{tstr})$$

NJ: правило сечений (cut rule)

Правило вывода, позволяющее удалить промежуточное значение A:

$$\frac{\Gamma \vdash A \qquad \Gamma, A, \Gamma' \vdash B}{\Gamma, \Gamma' \vdash B}\ (\mathrm{cut})$$

Является обобщением modus ponens:

Все люди смертны, Сократ является человеком => Сократ смертен

NJ: сечения (cut)

О сечении можно думать, как о лемме, которая используется при доказательстве теоремы.

Формально, это правило удаления, основная посылка которого доказывается правилом ввода той же посылки

$$
\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge_{\mathrm{I}})}{\Gamma \vdash A}\,(\wedge^{1}_{\mathrm{E}})
\qquad\qquad
\dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\mathrm{I}}) \qquad \dfrac{\pi'}{\Gamma \vdash A}}{\Gamma \vdash B}\,(\Rightarrow_{\mathrm{E}})
$$

NJ: устранимость сечений

Свойство формальных логик, согласно которому всякую секвенцию, выводимую в данном исчислении, можно вывести без применения правила сечений (всегда можно отбросить ненужные части доказательства)

Жирард: *Логика без устранимости сечений подобна машине без двигателя*

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\mathrm{I}}) \qquad \dfrac{\pi'}{\Gamma \vdash A}}{\Gamma \vdash B}\,(\Rightarrow_{\mathrm{E}}) \quad \rightsquigarrow \quad \dfrac{\pi[\pi'/A]}{\Gamma \vdash B}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge_{\mathrm{I}})}{\Gamma \vdash A}\,(\wedge^{\mathrm{l}}_{\mathrm{E}}) \quad \rightsquigarrow \quad \dfrac{\pi}{\Gamma \vdash A}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge_{\mathrm{I}})}{\Gamma \vdash B}\,(\wedge^{\mathrm{r}}_{\mathrm{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'}{\Gamma \vdash B}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash A \vee B}\,(\vee^{\mathrm{l}}_{\mathrm{I}}) \qquad \dfrac{\pi'}{\Gamma, A \vdash C} \qquad \dfrac{\pi''}{\Gamma, B \vdash C}}{\Gamma \vdash C}\,(\vee_{\mathrm{E}}) \quad \rightsquigarrow \quad \dfrac{\pi'[\pi/A]}{\Gamma \vdash C}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash B}}{\Gamma \vdash A \vee B}\,(\vee^{\mathrm{r}}_{\mathrm{I}}) \qquad \dfrac{\pi'}{\Gamma, A \vdash C} \qquad \dfrac{\pi''}{\Gamma, B \vdash C}}{\Gamma \vdash C}\,(\vee_{\mathrm{E}}) \quad \rightsquigarrow \quad \dfrac{\pi''[\pi/B]}{\Gamma \vdash C}$$

NJ: консистентность

Следующие три свойства эквивалентны:

- логическая система консистентна
- формула $\perp$ невыводима
- для любой формулы не выводимы одновременно она сама и её отрицание

Теорема. NJ консистентна.

NJ: устранимость сечений

Лемма: Доказательство без сечений всегда

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\mathrm{I}}) \qquad \dfrac{\pi'}{\Gamma \vdash A}}{\Gamma \vdash B}\,(\Rightarrow_{\mathrm{E}}) \quad \rightsquigarrow \quad \dfrac{\pi[\pi'/A]}{\Gamma \vdash B}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge_{\mathrm{I}})}{\Gamma \vdash A}\,(\wedge_{\mathrm{E}}^{\mathrm{l}}) \quad \rightsquigarrow \quad \dfrac{\pi}{\Gamma \vdash A}$$

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A} \qquad \dfrac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge_{\mathrm{I}})}{\Gamma \vdash B}\,(\wedge_{\mathrm{E}}^{\mathrm{r}}) \quad \rightsquigarrow \quad \dfrac{\pi'}{\Gamma \vdash B}$$

Интерпретация доказательств (Girard)

Boolean model: утверждения интерпретируется как булевские переменные, доказательство теорем как выполнимость формулы

Extensional model: утверждения интерпретируется как множества, доказательства - как возможность задать функцию

Intentional level: на данном уровне рассматриваются непосредственно сами доказательства и их преобразования с помощью усечения

Субструктурные правила

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C}\ (\mathrm{xch}) \qquad \frac{\Gamma, A, A, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\mathrm{contr})$$

$$\frac{\Gamma, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\mathrm{wk}) \qquad \frac{\Gamma, \top, \Gamma' \vdash A}{\Gamma, \Gamma' \vdash A}\ (\mathrm{tstr})$$

Субструктурные системы типов

	Exchange	Weakening	Contraction	Use
Ordered	—	—	—	Exactly once in order
Linear	Allowed	—	—	Exactly once
Affine	Allowed	Allowed	—	At most once
Relevant	Allowed	—	Allowed	At least once
Normal	Allowed	Allowed	Allowed	Arbitrarily

NK: закон исключённого третьего

NK отличается от NJ только наличием аксиомы исключённого третьего $\neg A \vee A$

Наличие такой аксиомы приводит к тому, что логика перестаёт быть конструктивной, иными словами мы для данной аксиомы не всегда известно, A или отрицание A было выполнено.

Классический пример рассуждений в классической логике:

- неконструктивное доказательство, что существуют иррациональные a и b такие, что a**b рационально
- неконструктивное доказательство, что множество простых чисел бесконечно

Тогда как NJ конструктивна и всегда можно извлечь конкретное доказательство

NK: альтернативы закону исключённого третьего

(i) *excluded middle*, also called *tertium non datur*:

$$\neg A \vee A$$

(ii) *double-negation elimination* or *reductio ad absurdum*:

$$\neg\neg A \Rightarrow A$$

(iii) *contraposition*:

$$(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$$

(iv) *counter-example principle*:

$$\neg(A \Rightarrow B) \Rightarrow A \wedge \neg B$$

(v) *Peirce's law*:

$$((A \Rightarrow B) \Rightarrow A) \Rightarrow A$$

(vi) *Clavius' law* or *consequentia mirabilis*:

$$(\neg A \Rightarrow A) \Rightarrow A$$

(vii) *Tarski's formula*:

$$A \vee (A \Rightarrow B)$$

(viii) one of the following *de Morgan laws*:

$$\neg(\neg A \wedge \neg B) \Rightarrow A \vee B$$
$$\neg(\neg A \vee \neg B) \Rightarrow A \wedge B$$

(ix) *material implication*:

$$(A \Rightarrow B) \Rightarrow (\neg A \vee B)$$

(x) $\Rightarrow/\vee$ *distributivity*:

$$(A \Rightarrow (B \vee C)) \Rightarrow ((A \Rightarrow B) \vee C)$$

NK: proof irrelevance

Рассмотрим интерпретацию формулы A как множества [[A]], которое бы соответствовало всем возможным доказательствам A.

А импликацию как функцию: A -> B = [[A]] -> [[B]].

В этой интерпретации ложь соответствует пустому множеству, а отрицание множеству функций из [[A]] в пустое множество.

Тогда

- если [[A]] не пусто, то [[A]] -> 0 пусто
- если [[A]] пусто, то [[A]] -> 0 не пусто

NK: proof irrelevance

С другой стороны

- если [[A]] не пусто, то [[A]] -> 0 ->0 пусто
- если [[A]] пусто, то ([[A]] -> 0) -> 0 не пусто

Другими словами двойное отрицание может быть рассмотрено, как формула, для которой важны не все доказательства, а только наличие или отсутствие их

Поэтому иногда говорят, что формулы с двойным отрицанием являются proof irrelevant (не важен конкретный пруф, важно его наличие)

Например, $\neg\neg(\neg A \vee A)$ доказуемо в NJ, потому что его можно рассматривать как наличие доказательства для A или не A

Исчисление предикатов

Логика первого порядка - исчисление позволяющее высказывание относительно переменных, фиксированных функций и предикатов (иными словами, допускает наличие кванторов)

Логика второго порядка - позволяет конструировать высказывания над произвольными предикатами и функциональными символами

Интерпретация Брауэра-Гейтинга-Колмогорова

- данная интерпретация рассматривает логические формулы как утверждения о разрешимости математических задач
- каждая формула обозначает некоторую задачу, истинность формулы означает, что задача имеет решение и это решение можно предъявить. Ложность - решения нет.
- логические связки позволяют конструировать из простых задач составные задачи

Интерпретация Брауэра-Гейтинга-Колмогорова

- P & Q - пара (a, b), где a - доказательство P, b - доказательство Q
- P || Q - или (0, a) или (1б и)
- P -> Q - функция, преобразующая пруф P в пруф Q
- $(\exists x{\in}S)(Px)$ - пара (x, a), где x элемент S, a - пруф Px
- $(\forall x{\in}S)(Px)$ - функция f, которая любой элемент S конвертирует в доказательство Px
- $\neg P$ - $P \to \bot$, функция переводящая P в доказательство $\bot$

Расширение STLC

$$\frac{}{\Gamma \vdash x : \Gamma(x)}\ (\mathrm{ax})$$

$$\frac{\Gamma \vdash t : A \to B \qquad \Gamma \vdash u : A}{\Gamma \vdash t\,u : B}\ (\to_{\mathrm{E}}) \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \to B}\ (\to_{\mathrm{I}})$$

$$\frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_{\mathrm{l}}(t) : A}\ (\times_{\mathrm{E}}^{\mathrm{l}}) \qquad \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_{\mathrm{r}}(t) : B}\ (\times_{\mathrm{E}}^{\mathrm{r}}) \qquad \frac{\Gamma \vdash t : A \qquad \Gamma \vdash u : B}{\Gamma \vdash \langle t, u \rangle : A \times B}\ (\times_{\mathrm{I}})$$

$$\frac{}{\Gamma \vdash \langle\rangle : 1}\ (1_{\mathrm{I}})$$

$$\frac{\Gamma \vdash t : A + B \qquad \Gamma, x : A \vdash u : C \qquad \Gamma, y : B \vdash v : C}{\Gamma \vdash \mathrm{case}(t, x \mapsto u, y \mapsto v) : C}\ (+_{\mathrm{E}})$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \iota_{\mathrm{l}}^{B}(t) : A + B}\ (+_{\mathrm{I}}^{\mathrm{l}}) \qquad \frac{\Gamma \vdash t : B}{\Gamma \vdash \iota_{\mathrm{r}}^{A}(t) : A + B}\ (+_{\mathrm{I}}^{\mathrm{r}})$$

$$\frac{\Gamma \vdash t : 0}{\Gamma \vdash \mathrm{case}^A(t) : A}\ (0_{\mathrm{E}})$$

Расширение STLC

β-reduction rules:

$$
\begin{aligned}
(\lambda x.t)\,u &\longrightarrow_\beta t[u/x] \\
\pi_\mathrm{l}(\langle t, u\rangle) &\longrightarrow_\beta t \\
\pi_\mathrm{r}(\langle t, u\rangle) &\longrightarrow_\beta u \\
\mathrm{case}(\iota_\mathrm{l}^B(t), x \mapsto u, y \mapsto v) &\longrightarrow_\beta u[t/x] \\
\mathrm{case}(\iota_\mathrm{r}^A(t), x \mapsto u, y \mapsto v) &\longrightarrow_\beta v[t/y]
\end{aligned}
$$

Соответствие Curry-Howard

- соответствие Curry-Howard расширяет BHK нотацию и является соответствием между доказательствами и программами, и теоремами и типами

Typing			Logic
function	$\to$	$\Rightarrow$	implication
product	$\times$	$\wedge$	conjunction
unit	1	$\top$	truth
coproduct	$+$	$\vee$	disjunction
empty	0	$\bot$	falsity