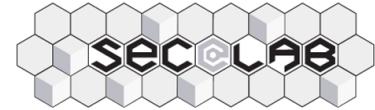


Практическая теория типов

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 $\Gamma \vDash A$.
- **completeness** - если выражение $\Gamma \vDash A$ выводимо, то $\Gamma \vdash A$



Формальные логики

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



Формализация доказательств

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

$\frac{\varepsilon > 0 \vdash \varepsilon > 0}{\varepsilon > 0 \vdash (\varepsilon/2) \times 2 > 0 \times 2}$	$\frac{\varepsilon > 0, x < \varepsilon/2 \vdash x < \varepsilon/2}{\varepsilon > 0, x < \varepsilon/2 \vdash 2x /2 < \varepsilon/2}$
$\frac{\varepsilon > 0 \vdash \varepsilon/2 > 0}{\varepsilon > 0 \vdash \varepsilon/2 > 0 \wedge \forall x. x < \varepsilon/2 \Rightarrow 2x < \varepsilon}$	$\frac{\varepsilon > 0, x < \varepsilon/2 \vdash x < \varepsilon/2}{\varepsilon > 0 \vdash x < \varepsilon/2 \Rightarrow 2x < \varepsilon}$
$\frac{\varepsilon > 0 \vdash \varepsilon/2 > 0 \wedge \forall x. x < \varepsilon/2 \Rightarrow 2x < \varepsilon}{\varepsilon > 0 \vdash \exists \eta. (\eta > 0 \wedge \forall x. x < \eta \Rightarrow 2x < \varepsilon)}$	$\frac{\varepsilon > 0 \vdash x < \varepsilon/2 \Rightarrow 2x < \varepsilon}{\varepsilon > 0 \vdash \forall x. x < \varepsilon/2 \Rightarrow 2x < \varepsilon}$
$\frac{\varepsilon > 0 \vdash \exists \eta. (\eta > 0 \wedge \forall x. x < \eta \Rightarrow 2x < \varepsilon)}{\vdash \varepsilon > 0 \Rightarrow \exists \eta. (\eta > 0 \wedge \forall x. x < \eta \Rightarrow 2x < \varepsilon)}$	
$\vdash \forall \varepsilon. (\varepsilon > 0 \Rightarrow \exists \eta. (\eta > 0 \wedge \forall x. x < \eta \Rightarrow 2x < \varepsilon))$	



Натуральный вывод

- формализм для доказательств, разработанный Генценом 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 интуиционистской логики

$A \vee \neg A$

$\exists a, b \text{ ирац, что } a^b \text{ рэз}$

$a = \sqrt{2}, b = \sqrt{2}$

если $a^b = \underline{\text{рэз}}$, \square

если a^b -ирак, что
 $a' = a^b, b' = b, a'^b = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} =$
 $= (\sqrt{2})^2 = 2$



NJ: формализм

NJ состоит из формул, задаваемых по следующему правилу

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

контекста $\Gamma = A_1, \dots, A_n$

суждений или секвентов $\Gamma \vdash A$

правил вывода
$$\frac{\Gamma_1 \vdash A_1 \quad \dots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}$$



NJ: правила вывода

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

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} (\Rightarrow_E)$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} (\Rightarrow_I)$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} (\wedge_E^l) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} (\wedge_E^r)$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} (\wedge_I)$$

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

$$\frac{}{\Gamma \vdash \top} (\top_I)$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} (\vee_E) \quad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} (\vee_I^l) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} (\vee_I^r)$$

т.ч. доказано

$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} (\perp_E)$ ↪ из этого следует то, что $A \vdash \perp$

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \perp} (\neg_E)$$

$$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A} (\neg_I) \quad \neg A = A \Rightarrow \perp$$

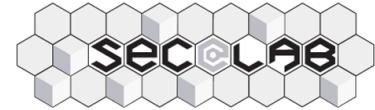


NJ: примеры вывода

Коммутативность дизъюнкции

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

$$\frac{\frac{\frac{A \vee B \vdash A \vee B \text{ (ax)} \quad \frac{\overline{A \vee B, A \vdash A} \text{ (ax)}}{A \vee B, A \vdash B \vee A \text{ (}\vee_I^r\text{)}} \quad \frac{\overline{A \vee B, B \vdash B} \text{ (ax)}}{A \vee B, B \vdash B \vee A \text{ (}\vee_I^l\text{)}}}{A \vee B \vdash B \vee A} \text{ (}\vee_E\text{)}}{\vdash A \vee B \Rightarrow B \vee A \text{ (}\Rightarrow_I\text{)}}$$

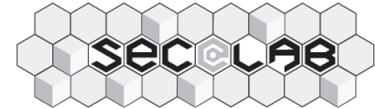


NJ: примеры вывода

Прямой закон контрапозиции:

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

$$\frac{\frac{\frac{\frac{A \Rightarrow B, \neg B, A \vdash A \Rightarrow B}{A \Rightarrow B, \neg B, A \vdash B} \text{ (ax)}}{A \Rightarrow B, \neg B, A \vdash \perp} \text{ (\neg E)}}{A \Rightarrow B, \neg B \vdash \neg A} \text{ (\neg I)}}{A \Rightarrow B \vdash \neg B \Rightarrow \neg A} \text{ (\Rightarrow I)}$$



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:

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C} \text{ (xch)}$$

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

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

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



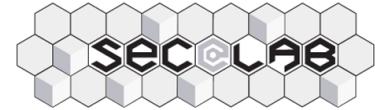
NJ: правило сечений (cut rule)

Правило вывода, позволяющее удалить промежуточное значение A:

$$\frac{\Gamma \vdash A \quad \Gamma, A, \Gamma' \vdash B}{\Gamma, \Gamma' \vdash B} \text{ (cut)}$$

Является обобщением modus ponens:

Все люди смертны, Сократ является человеком => Сократ смертен

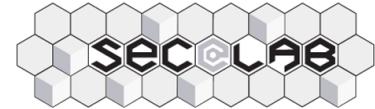


NJ: сечения (cut)

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

$$\frac{\pi \quad \pi'}{\Gamma \vdash A} \quad \frac{\pi}{\Gamma \vdash A \wedge B} \quad (\wedge_I) \quad \frac{\pi}{\Gamma \vdash A \wedge B} \quad (\wedge_E^1)$$
$$\frac{\pi}{\Gamma \vdash A} \quad \frac{\pi}{\Gamma \vdash A \Rightarrow B} \quad (\Rightarrow_I) \quad \frac{\pi'}{\Gamma \vdash A} \quad (\Rightarrow_E)$$
$$\frac{\pi \quad \pi'}{\Gamma \vdash A} \quad (\text{cut})$$



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)

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

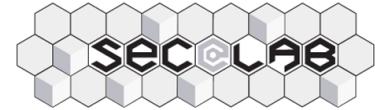
$$\frac{\frac{\pi}{\Gamma, A \vdash B} (\Rightarrow_I) \quad \frac{\pi'}{\Gamma \vdash A} (\Rightarrow_E)}{\Gamma \vdash B} \rightsquigarrow \frac{\pi[\pi'/A]}{\Gamma \vdash B}$$

$$\frac{\frac{\pi}{\Gamma \vdash A} \quad \frac{\pi'}{\Gamma \vdash B} (\wedge_I)}{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}} (\wedge_E^l) \rightsquigarrow \frac{\pi}{\Gamma \vdash A}$$

$$\frac{\frac{\pi}{\Gamma \vdash A} \quad \frac{\pi'}{\Gamma \vdash B} (\wedge_I)}{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}} (\wedge_E^r) \rightsquigarrow \frac{\pi'}{\Gamma \vdash B}$$

$$\frac{\frac{\pi}{\Gamma \vdash A} (\vee_I^l) \quad \frac{\pi'}{\Gamma, A \vdash C} \quad \frac{\pi''}{\Gamma, B \vdash C} (\vee_E)}{\Gamma \vdash C} \rightsquigarrow \frac{\pi'[\pi/A]}{\Gamma \vdash C}$$

$$\frac{\frac{\pi}{\Gamma \vdash B} (\vee_I^r) \quad \frac{\pi'}{\Gamma, A \vdash C} \quad \frac{\pi''}{\Gamma, B \vdash C} (\vee_E)}{\Gamma \vdash C} \rightsquigarrow \frac{\pi''[\pi/B]}{\Gamma \vdash C}$$



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

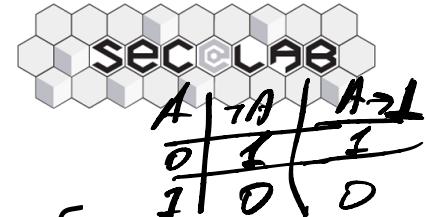
Лемма: Доказательство без сечений всегда

$$\frac{\frac{\pi}{\Gamma, A \vdash B} (\Rightarrow_I) \quad \frac{\pi'}{\Gamma \vdash A} (\Rightarrow_E)}{\Gamma \vdash B} \rightsquigarrow \frac{\pi[\pi'/A]}{\Gamma \vdash B}$$

$$\frac{\frac{\pi}{\Gamma \vdash A} \quad \frac{\pi'}{\Gamma \vdash B} (\wedge_I)}{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} (\wedge_E^1)} \rightsquigarrow \frac{\pi}{\Gamma \vdash A}$$

$$\frac{\frac{\pi}{\Gamma \vdash A} \quad \frac{\pi'}{\Gamma \vdash B} (\wedge_I)}{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} (\wedge_E^r)} \rightsquigarrow \frac{\pi'}{\Gamma \vdash B}$$

Интерпретация доказательств (Girard)



$$\neg A \equiv A \rightarrow \perp$$

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

A - ии-бо, тип

$$a \rightarrow \text{void}$$

a - тип с $N \neq 0$ областями видимости

$$a \rightarrow \text{void}$$

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

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

$$\neg A \equiv A \rightarrow \perp$$

Extensional model

a - Typ $\in N$ oder leer (wirkt auf N zuordnungen)

Typ leer

$$N=0 \quad \text{void} \rightarrow \text{void} \quad 0^0 = 1$$

$$N \neq 0 \quad |\alpha| = N \neq 0 \quad \alpha \rightarrow \text{void} \quad 0^{|\alpha|} = 0$$

(g)



alle - f

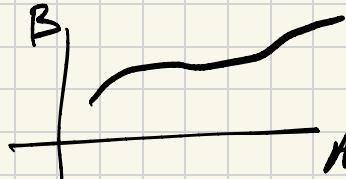
$$\emptyset \rightarrow \emptyset$$

$$|\alpha| = N \neq 0$$

$$\alpha \rightarrow \text{void}$$

$$(f, \emptyset) \in (\emptyset \times \emptyset), \quad A \\ (\underline{A \times \emptyset})$$

$$f: A \rightarrow B$$



$$C = (x, g) \in (A \times B)$$

$$f = C \subset (A, B)$$

$$A \rightarrow B \quad |A| \\ |B|$$



Субструктурные правила

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C} \text{ (xch)}$$

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

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

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



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, А или отрицание А 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

$$P_1 \cdots * P_n - 1$$

Тогда как NJ конструктивна и всегда можно извлечь конкретное доказательство

NK: альтернативы закону исключённого третьего



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

$$\neg A \vee A$$

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

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

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

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

(vii) *Tarski's formula*:

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

(iii) *contraposition*:

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

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

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

(iv) *counter-example principle*:

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

(ix) *material implication*:

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

(v) *Peirce's law*:

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

(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.

A импликацию как функцию: $A \rightarrow B = [[A]] \rightarrow [[B]]$.

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

Тогда

$$\neg A \equiv A \rightarrow \perp$$

- если $[[A]]$ не пусто, то $[[A]] \rightarrow 0$ пусто
- если $[[A]]$ пусто, то $[[A]] \rightarrow 0$ не пусто



NK: proof irrelevance

С другой стороны

- если $[[A]]$ не пусто, то $([[A]] \rightarrow 0) \rightarrow 0$ пусто
- если $[[A]]$ пусто, то $([[A]] \rightarrow 0) \rightarrow 0$ пусто

$$\emptyset \rightarrow \emptyset$$

не

$$\text{Unit} \rightarrow \emptyset$$

не

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

$$\neg\neg(\underbrace{\neg A \vee A}_0)$$

$$|B| \neq 0 \quad ((B \vee \emptyset) \rightarrow \emptyset) \rightarrow \emptyset$$

$$(B \rightarrow \emptyset) \rightarrow \emptyset$$



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
- $P \parallel Q$ - или $(0, a)$ или $(\cancel{1}, \cancel{b})$
- $P \rightarrow Q$ - 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 $f: S_x \Rightarrow P_{(f)}$
- $\neg P$ - $P \rightarrow \perp$: функция переводящая P в доказательство \perp

Расширение STLC



(a, b)

$$\frac{\Gamma \vdash t : A \rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash t u : B} (\rightarrow_E)$$

$$\frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_l(t) : A} (\times^l_E) \quad \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_r(t) : B} (\times^r_E)$$

$$\frac{\Gamma \vdash t : A + B \quad \Gamma, x : A \vdash u : C \quad \Gamma, y : B \vdash v : C}{\Gamma \vdash \text{case}(t, x \mapsto u, y \mapsto v) : C} (+_E)$$

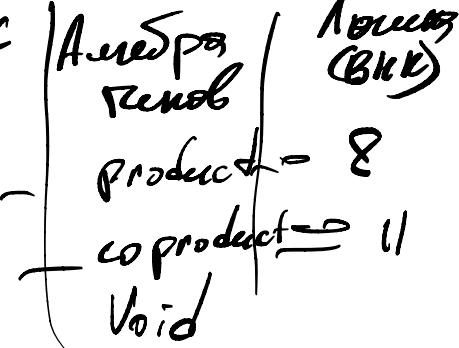
$$\frac{\Gamma \vdash t : 0}{\Gamma \vdash \text{case}^A(t) : A} (0_E)$$

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

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \rightarrow B} (\rightarrow_I)$$

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash \langle t, u \rangle : A \times B} (\times_I)$$

$$\frac{}{\Gamma \vdash \langle \rangle : 1} (1_I)$$



с: Either < A, B >
(a + b)

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \iota_l^B(t) : A + B} (+_I^l) \quad \frac{\Gamma \vdash t : B}{\Gamma \vdash \iota_r^A(t) : A + B} (+_I^r)$$

match C
Left => H
Right => V



Расширение STLC

β -reduction rules:

$$(\lambda x.t) u \longrightarrow_{\beta} t[u/x]$$

$$\pi_l(\langle t, u \rangle) \longrightarrow_{\beta} t$$

$$\pi_r(\langle t, u \rangle) \longrightarrow_{\beta} u$$

$$\text{case}(\iota_l^B(t), x \mapsto u, y \mapsto v) \longrightarrow_{\beta} u[t/x]$$

$$\text{case}(\iota_r^A(t), x \mapsto u, y \mapsto v) \longrightarrow_{\beta} v[t/y]$$



Соответствие Curry-Howard

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

		Typing		Logic
$\text{id} : \forall d. d \rightarrow d$	<i>Типы термов (программы)</i>	function	\rightarrow	\Rightarrow implication
$\lambda x. x : \forall d. d \rightarrow d$	<i>Теоремы Curry-Howard</i>	product	\times	\wedge conjunction
$\text{C} =$		unit	1	T truth
$\text{U}_\text{id} =$		coproduct	+	\vee disjunction
		empty	0	\perp falsity

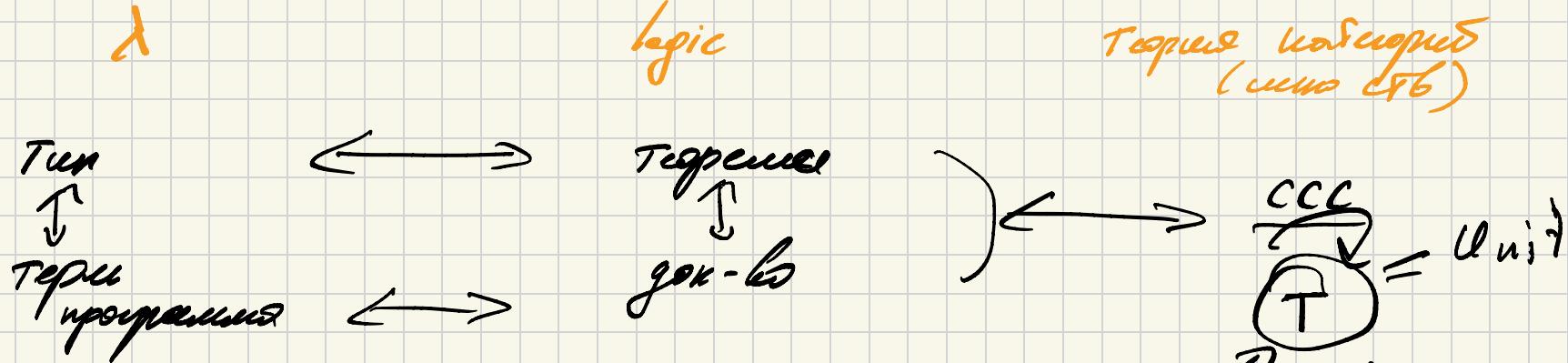


Соответствие Curry-Howard

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

Typing		Logic	
function	\rightarrow	\Rightarrow	implication
product	\times	\wedge	conjunction
unit	1	T	truth
coproduct	+	\vee	disjunction
empty	0	\perp	falsity

Числоподобие Каппа - Колесова - Лашенка



$\text{Int} \rightarrow \text{Int}$

$f(\text{int } a) \rightarrow \text{int} \{$

`return a;`

3

$$\text{func } n \rightarrow n \% 2 = 0 \Rightarrow$$

$$n \% 4 = 0$$

? ?

1
2
3
Void
 $\emptyset \rightarrow \emptyset$

