Типы в языках программирования
Лекция 11. λ-куб и чистые системы типов (PTS)

Денис Николаевич Москвин

ИТМО, корпоративная магистратура JetBrains
Разработка ПО / Software Engineering

19.05.2021

План лекции

1. Системы λ-куба: формализм
2. Чистые системы типов
3. Логический куб

План лекции

Типы и термы

- Мы не различаем заранее типы и термы.
- Множество *псевдовыражений* определяется индуктивно:

$$\mathcal{T} = V \mid C \mid \mathcal{T}\mathcal{T} \mid \lambda V^{\mathcal{T}} . \mathcal{T} \mid \Pi V^{\mathcal{T}} . \mathcal{T},$$

  где V — бесконечный набор переменных, а $C = \{*, \Box\}$.
- Константы $*$ и $\Box$ называют *сортами*.
- В дальнейшем переменные s, s_1, s_2 пробегают множество $\{*, \Box\}$.

Контексты

- *Высказывание* имеет вид $M : A$ (или M^A), где $M, A \in \mathcal{T}$.
- *Псевдо-контекст* — это конечное, линейно упорядоченное множество высказываний, с различными переменными в качестве субъекта.
- $\langle\rangle$ обозначает пустой контекст.
- Если $\Gamma = \langle x_1^{A_1}, \ldots, x_n^{A_n} \rangle$, то $\Gamma, y^B = \langle x_1^{A_1}, \ldots, x_n^{A_n}, y^B \rangle$.
- *Правила типизации* аксиоматизируют нотацию

$$\Gamma \vdash A : B,$$

  обозначающую, что высказывание $A : B$ может быть выведено из псевдо-контекста Γ.
- В таком случае A и B называются *(допустимыми) выражениями*, а Γ — *(допустимым) контекстом*.

Общие правила типизации

(аксиома) $$\langle\rangle \vdash * : \Box$$

(начальное правило) $$\frac{\Gamma \vdash A : s}{\Gamma, x^A \vdash x : A}, \quad x \notin \Gamma$$

(правило ослабления) $$\frac{\Gamma \vdash A : B \qquad \Gamma \vdash C : s}{\Gamma, x^C \vdash A : B}, \quad x \notin \Gamma$$

(правило применения) $$\frac{\Gamma \vdash M : \Pi x^A . B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\,N : [x \mapsto N]B}$$

(правило абстракции) $$\frac{\Gamma, x^A \vdash M : B \qquad \Gamma \vdash \Pi x^A . B : s}{\Gamma \vdash \lambda x^A . M : \Pi x^A . B}$$

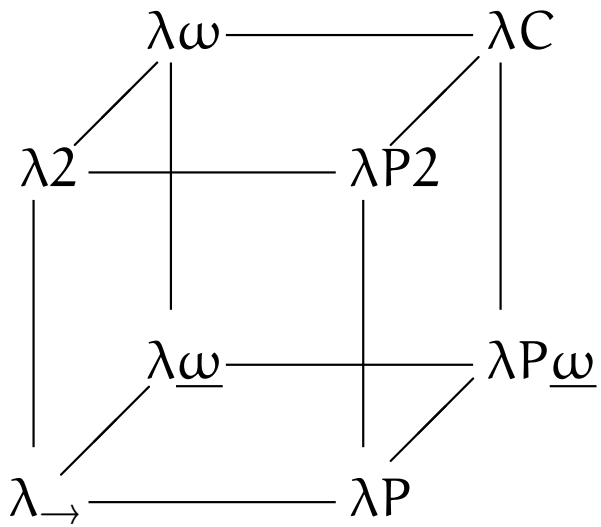
(правило преобразования) $$\frac{\Gamma \vdash A : B \qquad \Gamma \vdash B' : s \qquad B =_\beta B'}{\Gamma \vdash A : B'}$$

Специальные правила типизации

$$\text{правило } (s_1, s_2) \qquad \frac{\Gamma \vdash A : s_1 \qquad \Gamma, x^A \vdash B : s_2}{\Gamma \vdash \Pi x^A . B : s_2}$$

Восемь систем λ-куба определяются конкретным подмножеством правил.

	подмножество правил			
$\lambda\!\rightarrow$	$(*,*)$			
$\lambda 2$	$(*,*)$	$(\Box,*)$		
λP	$(*,*)$		$(*,\Box)$	
$\lambda P2$	$(*,*)$	$(\Box,*)$	$(*,\Box)$	
$\lambda\underline{\omega}$	$(*,*)$			$(\Box,\Box)$
$\lambda\omega$	$(*,*)$	$(\Box,*)$		$(\Box,\Box)$
$\lambda P\underline{\omega}$	$(*,*)$		$(*,\Box)$	$(\Box,\Box)$
$\lambda P\omega$	$(*,*)$	$(\Box,*)$	$(*,\Box)$	$(\Box,\Box)$



План лекции

Чистые системы типов (PTS)

Чистые системы типов (Pure Type Systems) задают абстрактную инфраструктуру, позволяющую унифицировано описывать конкретные системы типов:

- интерпретация «высказывания-как-типы» приобретает простую форму;
- легко сравнивать свойства разных систем;
- многие свойства доказываются для целых групп систем.

Чистые системы типов (PTS)

Обобщения систем λ-куба, формирующие системы PTS:

- количество сортов становится произвольным (на кубе их два $*$ и $\Box$);
- набор аксиом тоже может быть расширен (на кубе аксиома одна $*:\Box$);
- сорт всего Π-типа может отличаться от сорта «тела типа».

Определение PTS (1)

- Множество ***(пред)выражений***

$$\Lambda \ := \ \mathcal{V} \mid \mathcal{C} \mid \Lambda\,\Lambda \mid \lambda \mathcal{V}^{\Lambda}.\,\Lambda \mid \Pi \mathcal{V}^{\Lambda}.\,\Lambda$$

  где $\mathcal{V}$ — множество переменных, а $\mathcal{C}$ — констант.
- Высказывания $M{:}A$, объявления $x{:}A$, (пред)контексты Γ — как на λ-кубе.

Определение PTS (2)

Спецификация конкретной PTS задаётся тройкой $S = (\mathcal{S}, \mathcal{A}, \mathcal{R})$

- $\mathcal{S}$ — подмножество C, его элементы называют ***сортами***
- $\mathcal{A}$ — множество ***аксиом*** вида $c : s$, причём $c \in C$ и $s \in \mathcal{S}$
- $\mathcal{R}$ — множество ***правил*** вида (s_1, s_2, s_3), причём $s_1, s_2, s_3 \in \mathcal{S}$

V — объединение *непересекающихся* подмножеств

$$V = \cup_{s \in \mathcal{S}} V_s, \qquad V_{s_1} \cap V_{s_2} = \varnothing, \qquad V_s = \{{}^s x, {}^s y, {}^s z, \ldots\}$$

На λ-кубе, например, для выполнения последнего требования мы использовали «греко-латинскую» систему: ${}^* x, {}^* y, {}^* z$, ${}^\square \alpha, {}^\square \beta, {}^\square \gamma$.

Аксиомы и правила для $\Gamma \vdash M : A$ (1)

Нотация присваивания типов $\Gamma \vdash M : A$ задаётся так

Аксиомы	$\dfrac{}{\vdash c : s}$, если $(c : s) \in \mathcal{A}$
Начальное правило	$\dfrac{\Gamma \vdash A : s}{\Gamma, x^A \vdash x : A}$, если $x \equiv {}^s x \notin \Gamma$
Правило ослабления	$\dfrac{\Gamma \vdash M : A \qquad \Gamma \vdash B : s}{\Gamma,\, x^B \vdash M : A}$, если $x \equiv {}^s x \notin \Gamma$

Здесь $s \in \mathcal{S}$, $c \in \mathcal{C}$, $x \in V$ и $A, B, M \in \Lambda$.

(продолжение далее...)

Аксиомы и правила для $\Gamma \vdash M : A$ (2)

Правило произведения

$$\frac{\Gamma \vdash A : s_1 \qquad \Gamma, x^A \vdash B : s_2}{\Gamma \vdash \Pi x^A . B : s_3}, \quad \text{где } (s_1, s_2, s_3) \in \mathcal{R}$$

Правило применения

$$\frac{\Gamma \vdash M : \Pi x^A . B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\,N : [x \mapsto N]B}$$

Правило абстракции

$$\frac{\Gamma, x^A \vdash M : B \qquad \Gamma \vdash \Pi x^A . B : s}{\Gamma \vdash \lambda x^A . M : \Pi x^A . B}$$

Здесь $s, s_1, s_2, s_3 \in \mathcal{S}$, $x \in V$ и $A, B, M, N \in \Lambda$.

(продолжение далее...)

Аксиомы и правила для $\Gamma \vdash M : A$ (3)

Правило преобразования

$$\frac{\Gamma \vdash A : B \qquad \Gamma \vdash B' : s \qquad B =_\beta B'}{\Gamma \vdash A : B'}$$

Здесь $s \in \mathcal{S}$ и $A, B, B' \in \Lambda$.

Посылка $B =_\beta B'$ может быть неразрешима; её можно заменить на

$$B \to_\beta B' \ \vee \ B' \to_\beta B$$

Примеры PTS (1)

Принято обозначение $(s_1, s_2) \equiv (s_1, s_2, s_2)$.

$\lambda\!\!\rightarrow$

$\mathcal{S}$	$*, \Box$
$\mathcal{A}$	$*:\Box$
$\mathcal{R}$	$(*,*)$

$\lambda\tau$

$\mathcal{S}$	$*$
$\mathcal{A}$	$0:*$
$\mathcal{R}$	$(*,*)$

$\lambda 2$

$\mathcal{S}$	$*, \Box$
$\mathcal{A}$	$*:\Box$
$\mathcal{R}$	$(*,*), (\Box,*)$

$\lambda\omega$

$\mathcal{S}$	$*, \Box$
$\mathcal{A}$	$*:\Box$
$\mathcal{R}$	$(*,*), (\Box,*), (\Box,\Box)$

λP

$\mathcal{S}$	$*, \Box$
$\mathcal{A}$	$*:\Box$
$\mathcal{R}$	$(*,*), (*,\Box)$

Примеры PTS (2)

$\lambda P\omega$

$\mathcal{S}$	$*, \Box$
$\mathcal{A}$	$*:\Box$
$\mathcal{R}$	$(*,*), (*,\Box), (\Box,*), (\Box,\Box)$

$\lambda C'$

$\mathcal{S}$	$*^t, *^p, \Box$
$\mathcal{A}$	$*^t:\Box, *^p:\Box$
$\mathcal{R}$	$\mathcal{S}^2$

λECC

$\mathcal{S}$	$*,\ \{\Box_i\}_{i\in\mathbb{N}^+}$
$\mathcal{A}$	$*:\Box_i,\ \Box_i:\Box_{i+1}$
$\mathcal{R}$	$(*,*),\ (*,\Box_i),\ (\Box_i,*),\ (\Box_i,\Box_j,\Box_{\max(i,j)})$

Примеры «плохих» PTS

$\lambda*$

$\mathcal{S}$	$*$
$\mathcal{A}$	$*:*$
$\mathcal{R}$	$(*,*)$

$\lambda\mathcal{U}$

$\mathcal{S}$	$*, \Box, \Delta$
$\mathcal{A}$	$*:\Box, \Box:\Delta$
$\mathcal{R}$	$(*,*), (\Box,*), (\Box,\Box), (\Delta,\Box), (\Delta,*)$

- Эти системы «неконсистентны» в логическом смысле: для них все типы являются обитаемыми (парадокс Жирара).

Примеры «плохих» PTS

$\lambda*$

$\mathcal{S}$	$*$
$\mathcal{A}$	$*:*$
$\mathcal{R}$	$(*,*)$

$\lambda\mathcal{U}$

$\mathcal{S}$	$*, \Box, \Delta$
$\mathcal{A}$	$*:\Box, \Box:\Delta$
$\mathcal{R}$	$(*,*), (\Box,*), (\Box,\Box), (\Delta,\Box), (\Delta,*)$

- Эти системы «неконсистентны» в логическом смысле: для них все типы являются обитаемыми (парадокс Жирара).
- Если отбросить $(\Delta,*)$, получим $\lambda\mathcal{U}^-$, которая тоже неконсистентна.

Примеры «плохих» PTS

$\lambda*$

$\mathcal{S}$	$*$
$\mathcal{A}$	$*:*$
$\mathcal{R}$	$(*,*)$

$\lambda\mathcal{U}$

$\mathcal{S}$	$*, \Box, \Delta$
$\mathcal{A}$	$*:\Box, \Box:\Delta$
$\mathcal{R}$	$(*,*), (\Box,*), (\Box,\Box), (\Delta,\Box), (\Delta,*)$

- Эти системы «неконсистентны» в логическом смысле: для них все типы являются обитаемыми (парадокс Жирара).
- Если отбросить $(\Delta,*)$, получим $\lambda\mathcal{U}^-$, которая тоже неконсистентна.
- А если еще отбросить $(\Delta,\Box)$, получим замечательную λHOL.

Свойства PTS (1)

- Γ называется ***(допустимым) контекстом***, если

$$\exists A, B \in \Lambda.\ \Gamma \vdash A : B$$

- $A \in \Lambda$ называется ***(допустимым) выражением***, если

$$\exists \Gamma, B \in \Lambda.\ \Gamma \vdash A : B \ \vee \ \Gamma \vdash B : A$$

- $\Gamma \vdash A : B : C$ обозначает, что одновременно выполняются утверждения $\Gamma \vdash A : B$ и $\Gamma \vdash B : C$.

Свойства PTS (2)

- Пусть Γ — предконтекст, а A — предвыражение.
- A называется Γ-***термом***, если

$$\exists B \in \Lambda.\ \Gamma \vdash A : B \ \vee \ \Gamma \vdash B : A$$

- A называется Γ-***типом*** (сорта s), если

$$\exists s \in \mathcal{S}.\ \Gamma \vdash A : s$$

- A называется Γ-***элементом*** (типа B сорта s), если

$$\exists B \in \Lambda\ \exists s \in \mathcal{S}.\ \Gamma \vdash A : B : s$$

Свойства PTS (3)

Лемма подстановки для PTS

Пусть

$$\Gamma, x^A, \Delta \vdash M : B$$

и

$$\Gamma \vdash N : A$$

тогда

$$\Gamma, [x \mapsto N]\Delta \vdash [x \mapsto N]M : [x \mapsto N]B$$

Лемма thinning для PTS

Пусть Γ и Δ — допустимые контексты, причём $\Gamma \subseteq \Delta$, тогда

$$\Gamma \vdash M : A \Rightarrow \Delta \vdash M : A$$

Лемма генерации (1)

Для $\Gamma \vdash P : Q$ по известной структуре выражения P

$$\Lambda \;:=\; C \mid V \mid \Lambda\,\Lambda \mid \lambda V^{\Lambda}.\,\Lambda \mid \Pi V^{\Lambda}.\,\Lambda$$

лемма генерации представляет свойства Γ и Q.

Лемма генерации для PTS

$$\begin{aligned}
\Gamma \vdash c : Q \quad &\Rightarrow \quad \exists s \in \mathcal{S}. \\
&\quad Q =_\beta s \;\wedge\; (c{:}s) \in \mathcal{A}
\end{aligned}$$

$$\begin{aligned}
\Gamma \vdash x : Q \quad &\Rightarrow \quad \exists s \in \mathcal{S}.\; \exists B =_\beta Q. \\
&\quad \Gamma \vdash B : s \;\wedge\; (x{:}B) \in \Gamma \;\wedge\; x \equiv {}^{s}x
\end{aligned}$$

$$\ldots$$

(продолжение далее...)

Лемма генерации (2)

Лемма генерации для PTS (продолжение)

$\ldots$

$$\Gamma \vdash \Pi x^A.\, B : Q \;\Rightarrow\; \exists (s_1, s_2, s_3) \in \mathcal{R}.\; \Gamma \vdash A : s_1 \;\wedge\; \Gamma, x^A \vdash B : s_2 \;\wedge\; Q =_\beta s_3$$

$$\Gamma \vdash \lambda x^A.\, M : Q \;\Rightarrow\; \exists s \in \mathcal{S}.\; \exists B.\; \Gamma \vdash \Pi x^A.\, B : s \;\wedge\; \Gamma, x^A \vdash M : B \;\wedge\; Q =_\beta \Pi x^A.\, B$$

$$\Gamma \vdash M\,N : Q \;\Rightarrow\; \exists A, B.\; \Gamma \vdash M : \Pi x^A.\, B \;\wedge\; \Gamma \vdash N : A \;\wedge\; Q =_\beta [x \mapsto N]B$$

Следствия леммы генерации (1)

- $$\Gamma \vdash M : A \quad \Rightarrow \quad \exists s \in \mathcal{S}. \; A \equiv s \;\vee\; \Gamma \vdash A : s$$
- $$\Gamma \vdash M : \Pi x^{B_1}. B_2 \quad \Rightarrow \quad \exists s_1, s_2 \in \mathcal{S}. \; \Gamma \vdash B_1 : s_1 \;\wedge\; \Gamma, x^{B_1} \vdash B_2 : s_2$$
- Если A является Γ-термом, то A — это сорт, или Γ-тип или Γ-элемент.
- Если A допустим и B — его подтерм, то B допустим.

Следствия леммы генерации (2)

- Классы сортов, Γ-типов и Γ-элементов могут пересекаться.
- Например,

$$\alpha^* \quad \vdash \quad \lambda x^{\alpha}.\, x : \alpha \to \alpha : *$$
$$\alpha^* \quad \vdash \quad \alpha \to \alpha : * : \Box$$

  Γ-терм $\alpha \to \alpha$ выступает в роли и Γ-типа и Γ-элемента.
- Есть здесь ещё смешение ролей?

Свойства PTS: редукция субъекта

Теорема о редукции субъекта для PTS

$$\Gamma \vdash M : A \ \wedge \ M \twoheadrightarrow_\beta M' \ \Rightarrow \ \Gamma \vdash M' : A$$

Следствия

- $\Gamma \vdash M : B \ \wedge \ B \twoheadrightarrow_\beta B' \ \Rightarrow \ \Gamma \vdash M : B'$
- Если A является Γ-термом и $A \twoheadrightarrow_\beta A'$, то A' тоже является Γ-термом.

Свойства PTS: Лемма конденсации

Лемма конденсации для PTS (Condensing, Strengthening)

$$\Gamma,\ x^A,\ \Delta\ \vdash\ M : B\ \wedge\ x \notin FV(\Delta) \cup FV(M) \cup FV(B)$$
$$\Rightarrow\ \Gamma, \Delta\ \vdash\ M : B$$

Свойства PTS: Теорема о единственности типа

Определение

PTS называется ***функциональной*** или ***односортной*** (singly sorted), если

1. $(c{:}s_1), (c{:}s_2) \in \mathcal{A} \Rightarrow \ s_1 \equiv s_2$;
2. $(s_1, s_2, s_3), (s_1, s_2, s_4) \in \mathcal{R} \Rightarrow \ s_3 \equiv s_4$.

Все рассматриваемые нами ранее системы функциональны.

Теорема о единственности типа

Для функциональной PTS

$$\Gamma \vdash M : A \ \wedge \ \Gamma \vdash M : A' \ \Rightarrow \ A =_\beta A'$$

Степень терма на λ-кубе

Имеется классификация предтермов, полезная для анализа допустимых термов в системах λ-куба. Задаётся отображение $\sharp : \Lambda \to \{0, 1, 2, 3\}$:

$$\begin{aligned} \sharp(\Box) &= 3 \\ \sharp(*) &= 2 \\ \sharp({}^{\Box}x) &= 1 \\ \sharp({}^{*}x) &= 0 \\ \sharp(\lambda x{:}A.\,B) = \sharp(\Pi x{:}A.\,B) &= \sharp B \\ \sharp(M\,N) &= \sharp M \end{aligned}$$

Для $M \in \Lambda$ значение $\sharp(M)$ называют ***степенью*** M.

Утверждение

Для всех систем λ-куба $\Gamma \vdash M : A \;\Rightarrow\; \sharp(M) + 1 = \sharp(A)$.

Нормализуемость и разрешимость

Определение

PTS называется ***сильно нормализуемой***, если все её допустимые термы сильно нормализуемы, то есть

$$\Gamma \vdash M : A \;\Rightarrow\; SN(M) \;\wedge\; SN(A)$$

Теорема (о нормализуемости систем λ-куба)

Все системы λ-куба сильно нормализуемы.

Теорема (о разрешимости TCP и TSP для нормализуемой PTS)

Если PTS с конечным числом сортов сильно или слабо нормализуема, то TCP и TSP разрешимы.

Населённость $\bot$

Утверждение

Пусть λS — это PTS, расширяющая $\lambda 2$. Тогда

$$\vdash_{\lambda S} M : \bot \ \Rightarrow \ M \text{ не имеет NF}$$

Доказательство: по лемме генерации для $\vdash M : \Pi\alpha^*.\,\alpha$ единственный *нормальный* случай — это $\vdash \lambda\alpha^*.\,B : \Pi\alpha^*.\,\alpha$. Тогда $\alpha^* \vdash B : \alpha$. Анализируя B по лемме генерации имеем, что такое допустимо, только если $B \equiv x\,C_1\,\ldots\,C_k$, что приводит к $B \equiv \alpha$. Отсюда $* \equiv \alpha$, противоречие (C не пересекается с V). ■

- То есть $\bot = \Pi\alpha^*.\,\alpha$ может быть населён только термами, не имеющими нормальной формы. Отсюда следует, что если система нормализуема, то $\bot$ не населён.

Barendregt-Geuvers-Klop conjecture

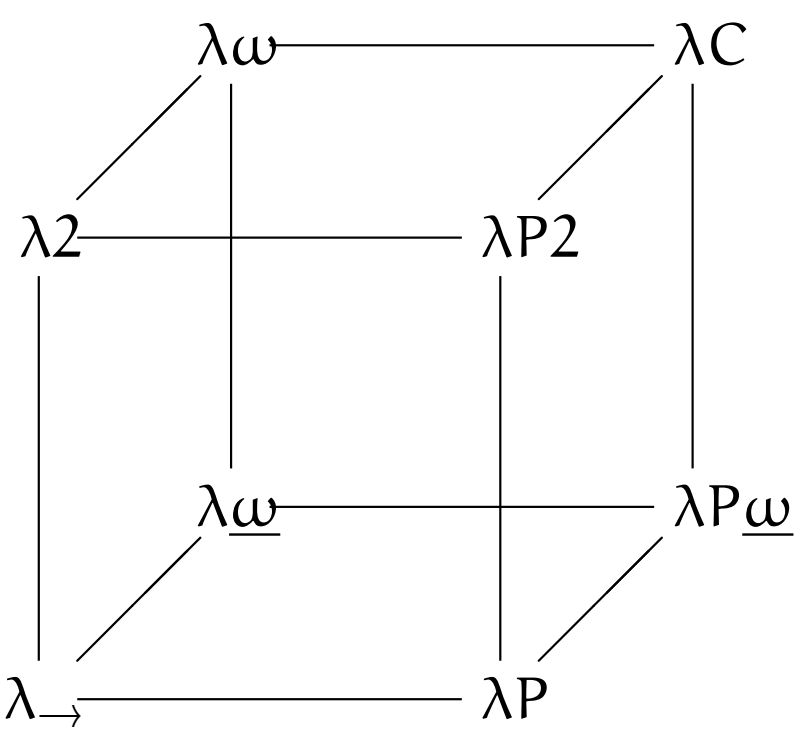
Гипотеза (1993)

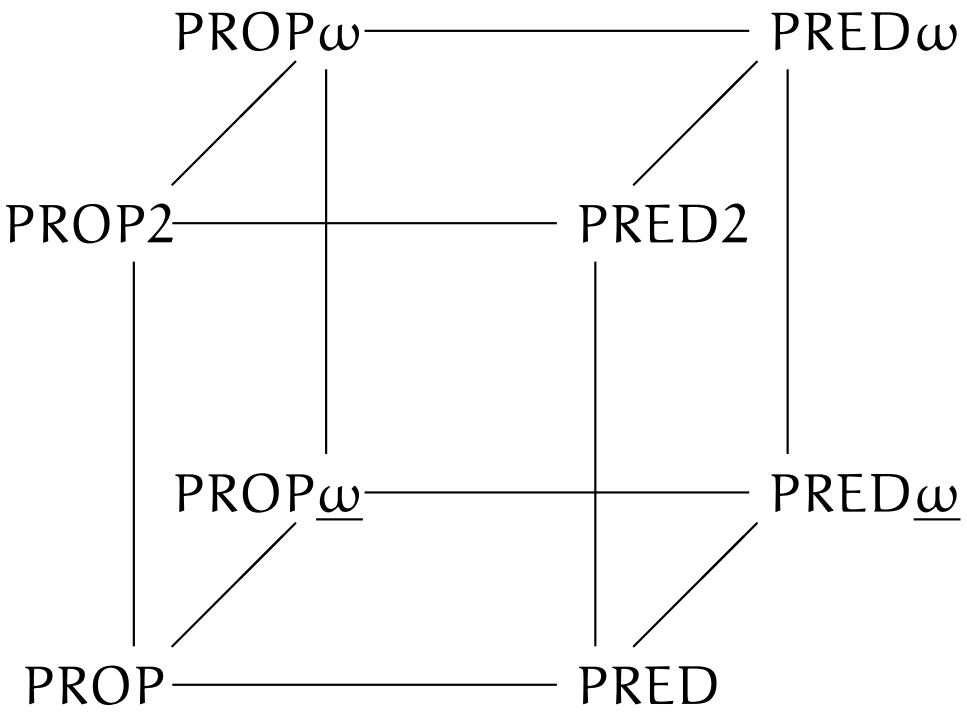
Каждая слабо нормализуемая PTS сильно нормализуема.

Это — открытая проблема.

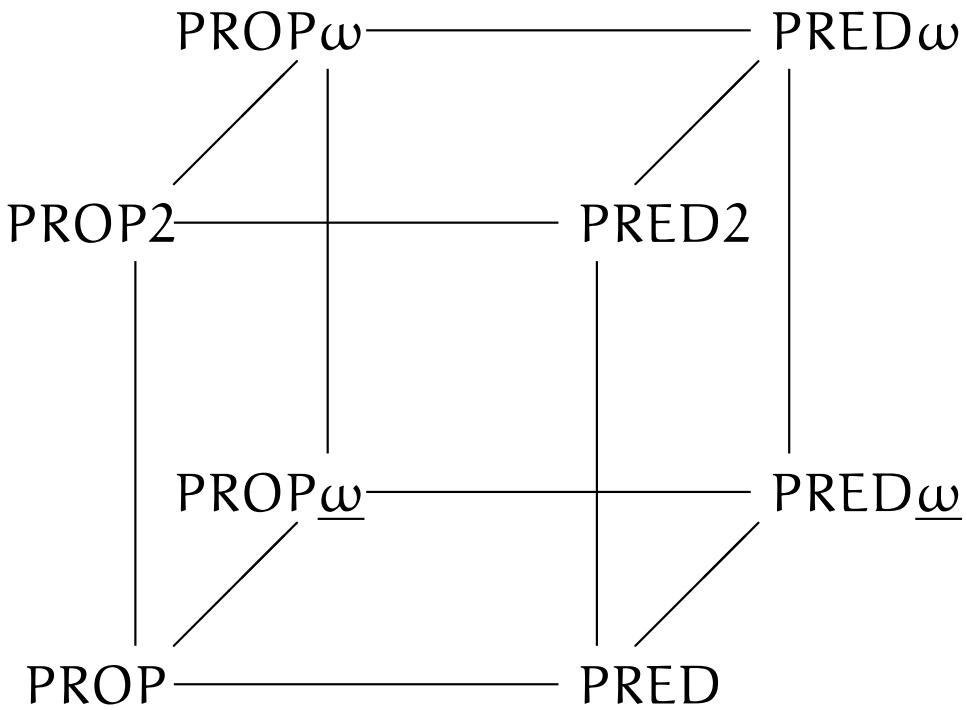
План лекции

Логический куб





Логический куб



PROP proposition logic; PROP2 second-order proposition logic; PROP$\underline{\omega}$ weakly higher-order proposition logic; PROPω higher-order proposition logic; PRED predicate logic; PRED2 second-order predicate logic; PRED$\underline{\omega}$ weakly higher-order predicate logic; PREDω higher-order predicate logic.

Логический куб: связки и кванторы

- Системы на логическом кубе задают минимальные многосортовые логики.
- Многосортовые — в предикатных логиках формулы строят из атомарных разных сортов, то есть в сигнатуру входят несколько «базовых типов».
- Минимальные — только одна связка (импликация) и один квантор (общности).
- Однако, начиная со PROP2, мы можем выразить $\bot$, $\wedge$, $\vee$ и $\neg$.
- Начиная с PRED2, можем выразить квантор $\exists$ и равенство Лейбница $=_L$:

$$\begin{aligned} \exists x^S.\, A &\equiv \Pi\gamma^{*^p}.\, (\Pi x^S.\, A \to \gamma) \to \gamma \\ x =_L y &\equiv \Pi P^{S \to *^p}.\, P\, x \to P\, y \end{aligned}$$

Метатеория

- Пусть A — высказывание некоторой логики L.
- Пусть $[[A]]$ — интерпретация A (тип) в некоторой системе типов.
- Основные метатеоретические проблемы:
  - ***корректность*** (soundness):
    Если A — доказуемо в L, то $[[A]]$ — обитаем.
  - ***полнота*** (completness):
    Если $[[A]]$ — обитаем, то A — доказуемо в L.
- ***Корректность.***

  Имеет место для всех вершин λ-куба.
- ***Полнота.***
  - Имеет место для левой грани куба.
  - При некоторых оговорках (недопустимость пустого домена) выполняется для $\lambda\mathrm{P}$.
  - Не имеет места для $\lambda\mathrm{P}\omega$: неразличимость $*^{\mathrm{s}}$ и $*^{\mathrm{p}}$ приводит к странным конструкциям (см. диссертацию Herman Geuvers, Logics and Type Systems).

Промежуточные конструкции

- Идея доказательств такая: построить PTS максимально точно описывающую логическую систему, и доказывать полноту и корректность в два этапа.
- Например, для PRED строим эквивалентную PTS λPRED

λP

$\mathcal{S}$	$*, \Box$
$\mathcal{A}$	$*:\Box$
$\mathcal{R}$	$(*,*),(*,\Box)$

λPRED

$\mathcal{S}$	$*^{\mathrm{p}}, *^{\mathrm{s}}, *^{\mathrm{f}}, \Box^{\mathrm{p}}, \Box^{\mathrm{s}}$
$\mathcal{A}$	$*^{\mathrm{p}}:\Box^{\mathrm{p}}, *^{\mathrm{s}}:\Box^{\mathrm{s}}$
$\mathcal{R}$	$(*^{\mathrm{p}},*^{\mathrm{p}}),(*^{\mathrm{s}},*^{\mathrm{p}}),(*^{\mathrm{s}},\Box^{\mathrm{p}}),$ $(*^{\mathrm{s}},*^{\mathrm{s}},*^{\mathrm{f}}),(*^{\mathrm{s}},*^{\mathrm{f}},*^{\mathrm{f}})$

а потом доказываем «равномощность» λPRED и λP, используя подходящее стирающее отображение.