Введение в вычислительную теорию доказательств
Часть I: λ-исчисление

С. Л. Кузнецов

Кафедра математической логики и теории алгоритмов, мехмат МГУ

23 сентября 2013 г.

Типы и термы

Типы:

1. Базовые типы.
2. Если A и B — типы, то $(A \to B)$ — тип.

Типы и термы

Типы:

1. Базовые типы.
2. Если A и B — типы, то $(A \to B)$ — тип.

Термы: каждый терм имеет тип. Тот факт, что терм t имеет тип A, обозначим $t : A$.

1. Константы: для каждого типа A имеется счётное множество констант данного типа c_1^A, c_2^A, ...
2. Переменные: для каждого типа A имеется счётное множество переменных данного типа x_1^A, x_2^A, ...
3. *Произведение* (применение функции): если $t : A \to B$ и $s : A$, то $(t \cdot s)$ — терм типа B (если же типы термов t и s не согласованы, то выражение $(t \cdot s)$ не является термом).
4. λ-*абстракция:* если $t : B$, то $\lambda x^A.t$ — терм типа $A \to B$.

Соответствие Карри – Говарда

Теорема

Если A — тип и существует такой *замкнутый* λ-терм u, что $u : A$. Тогда A, если рассмотреть его как формулу логики высказываний, будет тавтологией.

Соответствие Карри – Говарда

Теорема

Если A — тип и существует такой *замкнутый* λ-терм u, что $u : A$. Тогда A, если рассмотреть его как формулу логики высказываний, будет тавтологией.

Обратное неверно: не существует замкнутого λ-терма типа $((p \to q) \to p) \to p$.

Соответствие Карри – Говарда

Доказывать удобнее более общую теорему, индукцией по построению терма u:

Теорема

Пусть A, B_1, ..., B_k — типы и существует такой λ-терм u со свободными переменными $x_1^{B_1}$, ..., $x_k^{B_k}$, что $u : A$. Тогда $B_1, \ldots, B_k \vdash A$.

Исчисление естественного вывода (для $\mathrm{Int}_{\to}$)

$$\Gamma, A \vdash A$$

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

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

Исчисление естественного вывода (для $\mathrm{Int}_{\to}$)

$$\Gamma, A \vdash A$$

$$\frac{\Gamma, B \vdash A}{\Gamma \vdash (A \to B)} \qquad x : B, u : A \rightsquigarrow \lambda x.u : (A \to B)$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash (A \to B)}{\Gamma \vdash B} \qquad u : (A \to B), v : A \rightsquigarrow (uv) : B$$

Упрощение λ-термов

β-редукция

$$(\lambda x.u)v \to_\beta u[x := v]$$

(подстановка осуществляется на место всех свободных вхождений x)

Упрощение λ-термов

β-редукция

$$(\lambda x.u)v \to_\beta u[x := v]$$

(подстановка осуществляется на место всех свободных вхождений x)

η-редукция

$$\lambda x.fx \to_\eta f$$

Упрощение λ-термов

β-редукция

$$(\lambda x.u)v \to_\beta u[x := v]$$

(подстановка осуществляется на место всех свободных вхождений x)

η-редукция

$$\lambda x.fx \to_\eta f$$

Редукции могут применяться не только к терму в целом, но и к *подтермам* внутри него. Такой подтерм называется *редексом*. Если терм u_2 получается из терма u_1 применением β- или η-редукции к какому-либо подтерму, будем писать $u_1 \to_{\beta\eta} u_2$.

Нормализуемость

Теорема

Не существует бесконечной последовательности термов $u_1 \to_{\beta\eta} u_2 \to_{\beta\eta} u_3 \to_{\beta\eta} \dots$

Нормализуемость

Теорема

Не существует бесконечной последовательности термов $u_1 \to_{\beta\eta} u_2 \to_{\beta\eta} u_3 \to_{\beta\eta} \dots$

Из теоремы о нормализуемости следует, что всякий λ-терм можно конечным числом редукций привести к терму, к которому редукции уже не применимы. Этот терм называется *нормальной формой.*

Свойство Чёрча – Россера

Теорема

Если термы v_1 и v_2 получаются различными последовательностями редукций из терма u, то существует такой терм w, что его можно получить последовательностями редукций как из v_1, так и из v_2.

Свойство Чёрча – Россера

Теорема

Если термы v_1 и v_2 получаются различными последовательностями редукций из терма u, то существует такой терм w, что его можно получить последовательностями редукций как из v_1, так и из v_2.

Из свойства Чёрча – Россера следует, что нормальная форма терма единственна.

Эквивалентность

Термы u и v называются $\beta\eta$-*эквивалентными*, если их нормальные формы совпадают.

Теоретико-множественная интерпретация

Каждому базовому типу p сопоставляется произвольное (непустое) множество D_p.

Теоретико-множественная интерпретация

Каждому базовому типу p сопоставляется произвольное (непустое) множество D_p.
Типу вида $A \to B$ сопоставляется множество $D_{A\to B} = D_B^{D_A} = \{f \mid f\colon D_A \to D_B\}$ всех функций из D_A в D_B.
Множество D_A назовём *областью* (domain) типа A.

Теоретико-множественная интерпретация

Каждому базовому типу p сопоставляется произвольное (непустое) множество D_p.
Типу вида $A \to B$ сопоставляется множество $D_{A\to B} = D_B^{D_A} = \{f \mid f\colon D_A \to D_B\}$ всех функций из D_A в D_B.
Множество D_A назовём *областью* (domain) типа A.
Константы интерпретируются произвольными элементами областей соответствующих типов.

Теоретико-множественная интерпретация

Каждому базовому типу p сопоставляется произвольное (непустое) множество D_p.

Типу вида $A \to B$ сопоставляется множество $D_{A\to B} = D_B^{D_A} = \{f \mid f\colon D_A \to D_B\}$ всех функций из D_A в D_B.

Множество D_A назовём *областью* (domain) типа A.

Константы интерпретируются произвольными элементами областей соответствующих типов.

Интерпретация переменных: $\theta\colon \mathrm{Var}_A \to D_A$.

Теоретико-множественная интерпретация

Каждому базовому типу p сопоставляется произвольное (непустое) множество D_p.
Типу вида $A \to B$ сопоставляется множество $D_{A\to B} = D_B^{D_A} = \{f \mid f\colon D_A \to D_B\}$ всех функций из D_A в D_B.
Множество D_A назовём *областью* (domain) типа A.
Константы интерпретируются произвольными элементами областей соответствующих типов.

Интерпретация переменных: $\theta\colon \mathrm{Var}_A \to D_A$.

Интерпретация произвольного терма $[\![w]\!]^\theta$:

1. для переменных: $[\![x]\!]^\theta = \theta(x)$;
2. для констант — задана произвольно;
3. $[\![uv]\!]^\theta = [\![u]\!]^\theta([\![v]\!]^\theta)$;
4. $[\![\lambda x^A.u]\!]$, где $u : B$, — это функция $f\colon a \mapsto [\![u]\!]^{\theta[x:=a]}$.

Теоремы о корректности и полноте

Теорема

Для любого терма u типа A при любой интерпретации имеем $[\![u]\!]^\theta \in D_A$.

Теоремы о корректности и полноте

Теорема

Для любого терма u типа A при любой интерпретации имеем $[\![u]\!]^\theta \in D_A$.

Теорема

Два терма u и v эквивалентны тогда и только тогда, когда при любой интерпретации $[\![u]\!]^\theta = [\![v]\!]^\theta$.

Функции многих переменных (currying)

В предложенном исчислении нет прямого способа задать функцию $f\colon A \times B \to C$. Заменим её на $\tilde{f}\colon A \to (B \to C)$. Аргументы в новую функцию подставляются не одновременно, а *последовательно:* $f(x, y) = \tilde{f}(x)(y)$ (при этом $\tilde{f}(x)\colon B \to C$).

Эта конструкция, называемая *каррированием* (currying, в честь Х. Карри), применима и для большего числа аргументов.

Применение в языкознании: семантика Монтегю

λ-исчисление используется лингвистами для исследования семантики предложений.

Словам в предложении сопоставляются λ-термы определённых типов. Каждый терм соответствует «смыслу» данного слова, а «смысл» всего предложения получается последовательным применением (в порядке, обусловленном синтаксисом языка) этих термов друг к другу.

Семантика Монтегю: тривиальный пример

В качестве базовых типов выберем два:
e (entity) — объекты из предметной области;
t (truth value) — значения «истина/ложь».

Семантика Монтегю: тривиальный пример

В качестве базовых типов выберем два:
e (entity) — объекты из предметной области;
t (truth value) — значения «истина/ложь».
Собственные имена будут иметь тип e, повествовательное предложение в целом должно получить тип t.

Семантика Монтегю: тривиальный пример

В качестве базовых типов выберем два:
e (entity) — объекты из предметной области;
t (truth value) — значения «истина/ложь».
Собственные имена будут иметь тип e, повествовательное предложение в целом должно получить тип t.
В частности, переходный глагол имеет тип $e \to (e \to t)$ (принимает два аргумента-объекта, возвращает истинностное значение).

Семантика Монтегю: тривиальный пример

В качестве базовых типов выберем два:
e (entity) — объекты из предметной области;
t (truth value) — значения «истина/ложь».
Собственные имена будут иметь тип e, повествовательное предложение в целом должно получить тип t.
В частности, переходный глагол имеет тип $e \to (e \to t)$ (принимает два аргумента-объекта, возвращает истинностное значение).

предложение:	Иван	любит	Марью	
типы:	e	$e \to (e \to t)$	e	
термы:	J	L	M	(все константы)

Семантика Монтегю: тривиальный пример

В качестве базовых типов выберем два:
e (entity) — объекты из предметной области;
t (truth value) — значения «истина/ложь».
Собственные имена будут иметь тип e, повествовательное предложение в целом должно получить тип t.
В частности, переходный глагол имеет тип $e \to (e \to t)$ (принимает два аргумента-объекта, возвращает истинностное значение).

предложение:	Иван	любит	Марью	
типы:	e	$e \to (e \to t)$	e	
термы:	J	L	M	(все константы)

Правильный порядок применения: $L(M)(J)$.

Семантика Монтегю: более сложный пример

предложение:	Нарцисс	любит	себя
типы:	e	$e \to (e \to t)$	$(e \to (e \to t)) \to (e \to t)$
термы:	N	L	$\lambda y.\lambda x.y(x)(x)$

Семантика Монтегю: более сложный пример

предложение:	Нарцисс	любит	себя
типы:	e	$e \to (e \to t)$	$(e \to (e \to t)) \to (e \to t)$
термы:	N	L	$\lambda y.\lambda x.y(x)(x)$

Применяем:

$$(\lambda y.\lambda x.y(x)(x))(L)(N) \to_\beta (\lambda x.L(x)(x))(N) \to_\beta L(N)(N)$$

Семантика Монтегю: более сложный пример

предложение:	Нарцисс	любит	себя
типы:	e	$e \to (e \to t)$	$(e \to (e \to t)) \to (e \to t)$
термы:	N	L	$\lambda y.\lambda x.y(x)(x)$

Применяем:

$$(\lambda y.\lambda x.y(x)(x))(L)(N) \to_\beta (\lambda x.L(x)(x))(N) \to_\beta L(N)(N)$$

Иначе говоря, мы получили тот же смысл, что и для предложения «Нарцисс любит Нарцисса».

Исчисление Ламбека

$p_i \to p_i$

$$\frac{A\,\Pi \to B}{\Pi \to A \backslash B}\ (\to \backslash),\ \text{где}\ \Pi \neq \Lambda; \qquad \frac{\Pi \to A \quad \Gamma\, B\, \Delta \to C}{\Gamma\, \Pi\, (A \backslash B)\, \Delta \to C}\ (\backslash \to);$$

$$\frac{\Pi\, A \to B}{\Pi \to B \,/\, A}\ (\to /),\ \text{где}\ \Pi \neq \Lambda; \qquad \frac{\Pi \to A \quad \Gamma\, B\, \Delta \to C}{\Gamma\, (B \,/\, A)\, \Pi\, \Delta \to C}\ (/ \to);$$

$$\frac{\Gamma \to A \quad \Delta \to B}{\Gamma\, \Delta \to A \cdot B}\ (\to \cdot); \qquad \frac{\Gamma\, A\, B\, \Delta \to C}{\Gamma\, (A \cdot B)\, \Delta \to C}\ (\cdot \to);$$

$$\frac{\Pi \to A \quad \Gamma\, A\, \Delta \to C}{\Gamma\, \Pi\, \Delta \to C}\ (\mathrm{cut}).$$

Соответствие Карри – Говарда для L

Если $\mathrm{L} \vdash \Gamma \to A$, то $\Gamma \vdash_{\mathrm{Int}_{\to}} A$.

Соответствие Карри – Говарда для L

Если $\mathrm{L} \vdash \Gamma \to A$, то $\Gamma \vdash_{\mathrm{Int}_\to} A$.

Если $\mathrm{L} \vdash B_1 \ldots B_n \to A$, $x_i : B_i$, то существует λ-терм u, т. ч. $u : A$.

Соответствие Карри – Говарда для L

Если $\mathrm{L} \vdash \Gamma \to A$, то $\Gamma \vdash_{\mathrm{Int}_{\to}} A$.

Если $\mathrm{L} \vdash B_1 \ldots B_n \to A$, $x_i : B_i$, то существует λ-терм u, т. ч. $u : A$. Обратное неверно.

Категориальная грамматика Ламбека

$\mathcal{G} = \langle \Sigma, \triangleright, H \rangle$.
$\triangleright \subset \mathrm{Tp} \times \Sigma$.
H — выделенный тип, обычно базовый.

Категориальная грамматика Ламбека

$\mathcal{G} = \langle \Sigma, \triangleright, H \rangle$.
$\triangleright \subset \mathrm{Tp} \times \Sigma$.
H — выделенный тип, обычно базовый.

Семантическая разметка: $a \in \Sigma$, $A \in \mathrm{Tp}$, $u : A$.

Продолжение следует...