Нормални доказателства

Трифон Трифонов

λ-смятане и теория на доказателствата, 2018/19 г.

4 юни 2019 г.

Нормализация в $Nm(\to\forall)$

(β-)редукция наричаме прилагане на $\circ^-$ правило непосредствено след съответното $\circ^+$ правило.

$$
\begin{array}{c}
\to^+ \\ \to^-
\end{array}
\dfrac{\dfrac{\begin{array}{c}\cancel{[A^u]}\\ \mid M\\ B\end{array}}{A\to B}\,u \qquad \begin{array}{c}\mid N\\ A\end{array}}{B}
\quad \xrightarrow{\beta} \quad
\begin{array}{c}\mid N\\ [A]\\ \mid M\\ B\end{array}
$$

$$
\left((\lambda_{u^A} M^B)^{A\to B} N^A\right)^B \quad \xrightarrow{\beta} \quad M^B[u^A \mapsto N^A]
$$

$$
\begin{array}{c}
\forall^+ \\ \forall^-
\end{array}
\dfrac{\dfrac{\begin{array}{c}\mid M\\ A\end{array}}{\forall_x A}\,(*) \qquad t}{A[x\mapsto t]}
\quad \xrightarrow{\beta} \quad
\begin{array}{c}\mid M[x\mapsto t]\\ A[x\mapsto t]\end{array}
$$

$$
\left((\lambda_x M^A)^{\forall_x A} t\right)^{A[x\mapsto t]} \quad \xrightarrow{\beta} \quad M[x\mapsto t]^{A[x\mapsto t]}
$$

Силна нормализация и конфлуентност

Теорема

Всяко доказателство е силно нормализируемо, т.е. всяка поредица от редукционни стъпки неизбежно завършва.

Теорема

$\xrightarrow{\beta}$ *е конфлуентна, т.е. всяка поредица от редукционни стъпки води до една и съща нормална форма.*

Структура на доказателствата

Дефиниция (Пътека в доказателство)

Пътека от ред k в доказателство наричаме път в дървото $A_0, A_1, \ldots, A_n$, където

1. A_0 е листо
2. A_i е главна (лява) предпоставка на правило
3. A_n е
   - корен, тогава пътеката е от ред $k = 0$; или
   - вторична (дясна) предпоставка на $\to^-$, чиято главна предпоставка е на пътека от ред $k - 1$

Задача

Всяка формула в дадено доказателство принадлежи на някоя пътека.

Структура на нормалните доказателства в $Nm(\to\forall)$

Да разгледаме пътека в нормално доказателство:

- не можем $\circ^-$ да следва веднага $\circ^-$
- имаме (евентуално празна) последователност от $\circ^-$ и след това (евентуално празна) последователност от $\circ^+$
- съществува *минимална формула* A_j, която разделя $\circ^-$ от $\circ^+$ правилата
- всяка формула е подформула на заключението или на някое незадраскано допускане
- ако минималната формула е $A \to B$ или $\forall_x A$, можем да я заместим с

$$\to^- \frac{A \to B \qquad \cancel{A^u}}{\to^+ \dfrac{B}{A \to B}\, u} \quad \text{или} \quad \forall^- \frac{\forall_x A \qquad x}{\forall^+ \dfrac{A}{\forall_x A}}$$

- така можем да сведем минималната формула до атомарна
- получената нормална форма се нарича *дълга*

Експлозия при нормализация

Ще покажем, че при нормализация можем да получим експоненциална експлозия на големината на доказателството.

- Разглеждаме функцията $f(y,x) = y + 2^x$
- Графиката ѝ R може да се зададе със следните две (Хорнови) клаузи:
  - $C_1 := \forall_y Ry0(\mathsf{S}y)$
  - $C_2 := \forall_{x,y,z,v}\big(Ryxz \to Rzxv \to Ry(\mathsf{S}x)v\big)$
- Ще изразим функцията $2 \uparrow\uparrow n := \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n}$
- $D_n := \tilde{\exists}_{\vec{z}}(R00z_0 \tilde{\wedge} R0z_0z_1 \tilde{\wedge} \ldots \tilde{\wedge} R0z_{n-1}z_n)$
  - интиуция: $z_i := 2 \uparrow\uparrow i$
- $G_n := C_1 \to C_2 \to D_n$

Извод на G_n

Разглеждаме помощните формули:

- $A_0(x) := \forall_y \tilde{\exists}_z Ryxz$
- $A_{i+1}(x) := \forall_y (A_i(y) \to \tilde{\exists}_z (A_i(z) \to Ryxz))$
- интуиция: $A_i(x)$ означава "$i+1$-кратната итерация на f при фиксиран десен аргумент x дава резултат"

Лема 1

$A_n(0)$ и $\forall_x(A_n(x) \to A_n(\mathsf{S}x))$ са изводими от C_1 и C_2 с доказателства с констатнтна (независима от n) дължина.

Теорема

G_n е изводимо с доказателство с дължина $O(n)$.

Теорема

Всяко нормално доказателство на G_n е с дължина поне $2 \uparrow\uparrow n$.

β-редукция за $\vee$

Можем да въведем аналог на β-редукцията за $\vee$:

$$\vee^-\ \dfrac{\vee_0^+\ \dfrac{\begin{array}{c}\mid M\\ A\end{array}}{A\vee B} \qquad \begin{array}{c}\cancel{A^u}\\ \mid N\\ C\end{array} \qquad \begin{array}{c}\cancel{B^v}\\ \mid K\\ C\end{array}}{C}\ u, v \qquad \xrightarrow{\beta} \qquad \begin{array}{c}\mid M\\ [A]\\ \mid N\\ C\end{array}$$

$$\begin{array}{rcl}
\vee^-\ (\vee_0^+ M^A)^{A\vee B}(\lambda_{u^A} N^C)(\lambda_{v^B} K^C) & \xrightarrow{\beta} & N^C[u^A \mapsto M^A] \\
\vee^-\ (\vee_0^+ M^A)^{A\vee B} P^{A\to C} Q^{B\to C} & \xrightarrow{\beta} & (P^{A\to C} M^A)^C
\end{array}$$

и аналогично

$$\begin{array}{rcl}
\vee^-\ (\vee_1^+ M^B)^{A\vee B}(\lambda_{u^A} N^C)(\lambda_{v^B} K^C) & \xrightarrow{\beta} & K^C[v^B \mapsto M^B] \\
\vee^-\ (\vee_0^+ M^B)^{A\vee B} P^{A\to C} Q^{B\to C} & \xrightarrow{\beta} & (Q^{B\to C} M^B)^C
\end{array}$$

β-редукция за $\wedge$

Аналогично за $\wedge$:

$$
\dfrac{\wedge^+ \dfrac{\begin{array}{c}\mid M\\ A\end{array} \qquad \begin{array}{c}\mid N\\ B\end{array}}{A \wedge B} \qquad \begin{array}{c}\cancel{A^u} \quad \cancel{B^v}\\ \mid K\\ C\end{array}}{C} \wedge^- u, v
\quad \overset{\beta}{\to} \quad
\begin{array}{c}
\begin{array}{cc}\mid M & \mid N\\ A & B\end{array}\\
\mid K\\
C
\end{array}
$$

$$
\begin{array}{lcl}
\wedge^- \left\langle M^A, N^B \right\rangle^{A \wedge B} (\lambda_{u^A, v^B} K^C) & \overset{\beta}{\to} & K^C[u^A \mapsto M^A][v^B \mapsto N^B] \\
\wedge^- \left\langle M^A, N^B \right\rangle^{A \wedge B} P^{A \to B \to C} & \overset{\beta}{\to} & (P^{A \to B \to C} M^A N^B)^C
\end{array}
$$

β-редукция за $\exists$

И за $\exists$:

$$\exists^- \dfrac{\exists^+ \dfrac{t \qquad \begin{array}{c} \mid M \\ A[x \mapsto t] \end{array}}{\exists_x A} \qquad \begin{array}{c} \cancel{A^u} \\ \mid N \\ C \end{array}}{C} u \quad \stackrel{\beta}{\to} \quad \begin{array}{c} \mid M \\ [A[x \mapsto t]] \\ \mid N[x \mapsto t] \\ C \end{array}$$

$$\exists^- \left\langle t, M^{A[x \mapsto t]} \right\rangle^{\exists_x A} (\lambda_{x, u^A} N^C) \quad \stackrel{\beta}{\to} \quad N^C[x \mapsto t][u^{A[x \mapsto t]} \mapsto M^{A[x \mapsto t]}]$$

$$\exists^- \left\langle t, M^{A[x \mapsto t]} \right\rangle^{\exists_x A} P^{\forall_x (A \to C)} \quad \stackrel{\beta}{\to} \quad (P^{\forall_x (A \to C)}\ t\ M^{A[x \mapsto t]})^C$$

Блокиране на β-редукция

Правилата $\vee^-, \wedge^-, \exists^-$, които използват допълнителна формула C, могат да "блокират" потенциална β-редукция.

Пример:

$$\rightarrow^- \dfrac{\vee^- \dfrac{\begin{matrix}\mid M\\ A \vee B\end{matrix} \qquad \rightarrow^+ \dfrac{\begin{matrix}\cancel{A^u} \quad \cancel{C^w}\\ \mid N\\ D\end{matrix}}{C \to D}\,w \qquad \rightarrow^+ \dfrac{\begin{matrix}\cancel{B^v} \quad \cancel{C^w}\\ \mid K\\ D\end{matrix}}{C \to D}\,w}{C \to D}\,u, v \qquad \begin{matrix}\mid L\\ C\end{matrix}}{D}$$

Бихме искали да можем да разменим $\vee^-$ и $\to^-$:

$$\vee^- \dfrac{\begin{matrix}\mid M\\ A \vee B\end{matrix} \qquad \rightarrow^- \dfrac{\rightarrow^+ \dfrac{\begin{matrix}\cancel{A^u} \quad \cancel{C^w}\\ \mid N\\ D\end{matrix}}{C \to D}\,w \qquad \begin{matrix}\mid L\\ C\end{matrix}}{D} \qquad \rightarrow^- \dfrac{\rightarrow^+ \dfrac{\begin{matrix}\cancel{B^v} \quad \cancel{C^w}\\ \mid K\\ D\end{matrix}}{C \to D}\,w \qquad \begin{matrix}\mid L\\ C\end{matrix}}{D}}{D}\,u, v$$

Пермутиране на $\vee^-$ и $\to^-$

$$
\dfrac{\dfrac{\begin{array}{c} \mid M \\ A \vee B \end{array} \quad \begin{array}{c} \cancel{A^u} \\ \mid N \\ C \to D \end{array} \quad \begin{array}{c} \cancel{B^v} \\ \mid K \\ C \to D \end{array}}{C \to D}\,\vee^-\,u,v \qquad \begin{array}{c} \mid L \\ C \end{array}}{D}\,\to^-
$$

$$\downarrow \pi$$

$$
\dfrac{\begin{array}{c} \mid M \\ A \vee B \end{array} \quad \dfrac{\begin{array}{c} \cancel{A^u} \\ \mid N \\ C \to D \end{array} \quad \begin{array}{c} \mid L \\ C \end{array}}{D}\,\to^- \quad \dfrac{\begin{array}{c} \cancel{B^v} \\ \mid K \\ C \to D \end{array} \quad \begin{array}{c} \mid L \\ C \end{array}}{D}\,\to^-}{D}\,\vee^-\,u,v
$$

$$
\left(\vee^-_{A,B,C\to D}\,(\lambda_{u^A} N^{C\to D})(\lambda_{v^B} K^{C\to D}) L^C\right)^D \quad \stackrel{\pi}{\to} \quad \left(\vee^-_{A,B,D}\,(\lambda_{u^A} N^{C\to D} L^C)(\lambda_{v^B} K^{C\to D} L^C)\right)^D
$$

Възможни пермутативни конверсии

$\xrightarrow{\pi}$	$\to^-$	$\vee^-$	$\wedge^-$	$\forall^-$	$\exists^-$
$\vee^-$	$\checkmark$				
$\wedge^-$					
$\exists^-$					

Задача

Да се опишат останалите 14 пермутативни конверсии.

Опростяващи конверсии

Правилата $\vee^-, \wedge^-, \exists^-$, които използват допълнителна формула C, могат да бъдат приложени изкуствено ненужно.

$$\vee^- \cfrac{\begin{array}{c} \\ \mid M \\ A \vee B \end{array} \quad \begin{array}{c} \cancel{A^u} \\ \mid N \\ C \end{array} \quad \begin{array}{c} \cancel{B^v} \\ \mid K \\ C \end{array}}{C}\, u, v \quad \xrightarrow{\sigma} \quad \begin{array}{c} \mid N \\ C \end{array}, \text{ ако } u \notin \mathrm{FA}(N)$$

$$\left(\vee^- M^{A \vee B}(\lambda_{u^A} N^C)(\lambda_{v^B} K^C)\right)^C \quad \xrightarrow{\sigma} \quad N^C, \text{ ако } u \notin \mathrm{FA}(N)$$

$$\vee^- \cfrac{\begin{array}{c} \\ \mid M \\ A \vee B \end{array} \quad \begin{array}{c} \cancel{A^u} \\ \mid N \\ C \end{array} \quad \begin{array}{c} \cancel{B^v} \\ \mid K \\ C \end{array}}{C}\, u, v \quad \xrightarrow{\sigma} \quad \begin{array}{c} \mid K \\ C \end{array}, \text{ ако } v \notin \mathrm{FA}(K)$$

$$\left(\vee^- M^{A \vee B}(\lambda_{u^A} N^C)(\lambda_{v^B} K^C)\right)^C \quad \xrightarrow{\sigma} \quad K^C, \text{ ако } v \notin \mathrm{FA}(K)$$

Опростяващи конверсии за $\wedge^-$ и $\exists^-$

$$\wedge^- \dfrac{\dfrac{\mid M}{A \wedge B} \qquad \begin{array}{c}\cancel{A^u} \quad \cancel{B^v} \\ \mid N \\ C\end{array}}{C}\, u, v \quad \stackrel{\sigma}{\to} \quad \begin{array}{c}\mid N \\ C\end{array}, \text{ ако } u, v \notin \mathrm{FA}(N)$$

$$\left(\wedge^- M^{A \wedge B}(\lambda_{u^A, v^B} N^C)\right)^C \quad \stackrel{\sigma}{\to} \quad N^C, \text{ ако } u, v \notin \mathrm{FA}(N)$$

$$\exists^- \dfrac{\begin{array}{c}\mid M \\ \exists_x A\end{array} \qquad \begin{array}{c}\cancel{A^u} \\ \mid N \\ C\end{array}}{C}\, u \quad \stackrel{\sigma}{\to} \quad \begin{array}{c}\mid N \\ C\end{array}, \text{ ако } u \notin \mathrm{FA}(N)$$

$$\left(\exists^- M^{\exists_x A}(\lambda_{x, u^A} N^C)\right)^C \quad \stackrel{\sigma}{\to} \quad N^C, \text{ ако } u \notin \mathrm{FA}(N)$$

Силна нормализация и конфлуентност на $Nm(\to\wedge\vee\forall\exists)$

Теорема

$\xrightarrow{\beta,\pi,\sigma}$ *е силно нормализираща.*

Теорема

$\xrightarrow{\beta,\pi,\sigma}$ *е конфлуентна.*

Структура на нормалните доказателства в $Nm(\to\wedge\vee\forall\exists)$

Дефиниция (Сегмент)

Сегмент с дължина n в дадено доказателство наричаме път в дървото от еднакви формули такъв, че:

1. всички възли без последния са вторични (десни) предпоставки на $\vee^-, \wedge^-$ или $\exists^-$
2. всички възли без първия са заключения на $\vee^-, \wedge^-$ или $\exists^-$

Ако последният възел в сегмента е главна предпоставка на $\circ^-$ правило, сегмента наричаме *максимален* или *cut сегмент*.

Факт: всеки възел, който не е нито вторична предпоставка, нито заключение на $\vee^-, \wedge^-$ или $\exists^-$ е сегмент с дължина 1.

Структура на нормалните доказателства в $Nm(\to\wedge\vee\forall\exists)$

Дефиниция (Пътека в доказателство)

Пътека от ред k в доказателство наричаме последователност от сегменти $\sigma_0, \sigma_1, \ldots, \sigma_n$, такава, че

1. σ_0 започва с листо, което не е задраскано или е задраскано от $\to^+$
2. σ_i завършва като
   - главна предпоставка на $\to^-$; или
   - главна предпоставка на $\vee^-, \wedge^-$ или $\exists^-$, а σ_{i+1} започва със задраскано листо от същото правило
3. σ_n завършва като
   - корен, тогава пътеката е от ред $k = 0$; или
   - главна предпоставка на $\vee^-, \wedge^-$ или $\exists^-$, което не задрасква листа, тогава пътеката е от ред $k = 0$; или
   - вторична предпоставка на $\to^-$, чиято първична предпоставка е в пътека от ред $k - 1$.

Свойства на нормалните доказателства

Задача

Всяка формула в произволно доказателство принадлежи на някоя пътека.

Твърдение 1

В нормално доказателство съществува минимален сегмент, който служи за разделителна линия между последователни прилагания на $\circ^-$ *и* $\circ^+$ *правила.*

Твърдение 2 (Свойство на подформулите)

В нормално доказателство всяка формула е подформула на заключението или на някое незадраскано допускане.

Извличане на свидетели от нормални доказателства

Теорема (Свойство на $\vee$)

Ако $\Gamma \vdash_m A \vee B$ *и* Γ *не съдържа* $\vee$, *то* $\Gamma \vdash_m A$ *или* $\Gamma \vdash_m B$.

Доказателство.

Проследяване на главната пътека до достигане на $\vee^+$. $\square$

Теорема (Свойство на $\exists$)

Ако $\Gamma \vdash_m \exists_x A$ *и* Γ *не съдържа* $\exists$, *то съществуват термове* $\vec{t}$, *така че* $\Gamma \vdash_m A[x \mapsto t_1] \vee \ldots \vee A[x \mapsto t_n]$. *Ако в допълнение* Γ *не съдържа и* $\vee$, *то съществува терм* t, *така че* $\Gamma \vdash_m A[x \mapsto t]$.

Доказателство.

Проследяване на главната пътека до достигане на $\vee^-$ или $\exists^+$. $\square$