β-redukce

(osnova redukce = pojem redukce)

Připomeňme, že β-redukce je dána osnovou

$$\underline{\beta} = \{((\lambda x.M)N,\ M\{x:=N\}) \mid M,N \in \Lambda\}.$$

Má dvě důležité vlastnosti:

1. Charakterizuje dokazatelnost v teorii λ
2. Je CR, takže pro ni platí výsledky z minula.

Dokazatelnost v λ a β-redukce:

Platí $M =_\beta N$ právě když $\lambda \vdash M = N$.

Důkaz. „⇐" Indukcí přes délku důkazu $M = N$.

„⇒" Indukcí přes strukturu relací $\to_\beta$, $\twoheadrightarrow_\beta$, $=_\beta$.

PODROBNĚJI:

„⇐": 1. Délka důkazu je 1, neboli $M = N$ je axiom. Máme dva axiomy: $M = M$ a (β).

Je $M =_\beta M$ z reflexivity a

$\overbrace{(\lambda x.K)L}^{M \equiv} =_\beta \overbrace{K\{x:=L\}}^{\equiv N}$, jelikož $((\lambda x.K)L, K\{x:=L\}) \in \underline{\beta}$.

Tím je dokázán základní krok.

2. Mějme důkaz délky $k > 1$:

$$M_1 = N_1,\ M_2 = N_2,\ \dots,\ M_{k-1} = N_{k-1},\ M = N.$$

Podle indukčního předpokladu je $M_i =_\beta N_i$ pro každé $i < k$. Chceme dokázat $M =_\beta N$. $M = N$ je buď axiom (což už jsme řešili), nebo plyne odvozovacím pravidlem z předchozí rovnosti. Například:

$$M = N \quad \text{je} \quad M_i Z = N_i Z$$

pro nějaké $i < k$. (Tedy $M \equiv M_i Z$, $N \equiv N_i Z$.) Víme, že $M_i =_\beta N_i$. Odtud ale $M_i Z =_\beta N_i Z$ z kompatibility.

„$\Rightarrow$": Máme $M =_\beta N$ a chceme dokázat, že $M = N$ je teorém. Je třeba projít všechny možnosti pro $M =_\beta N$. Například:

1. $M \equiv N$. Pak $M = N$ je teorém, protože je to axiom.
2. $(M, N) \in \underline{\beta}$. Pak $M \equiv (\lambda x.K)L$, $N = K[x:=L]$. Ale $M = N$ je pak teorém, protože je to axiom.
3. $M \to_\beta N$ a $(M, N) \notin \underline{\beta}$. Indukční předpoklad například: $M \equiv KZ$, $N \equiv LZ$ a $\lambda \vdash K = L$.

Pak tato je důkaz:

$$\ldots\ldots, K = L, M = N.$$

4. $M \twoheadrightarrow_\beta N$, $M \not\equiv N$, $M \not\to_\beta N$. Pak podle ind. předpokladu ex. K tak, že $M \twoheadrightarrow_\beta K$, $K \twoheadrightarrow_\beta N$, $\lambda \vdash M = K, K = N$. Pak tato je důkaz:

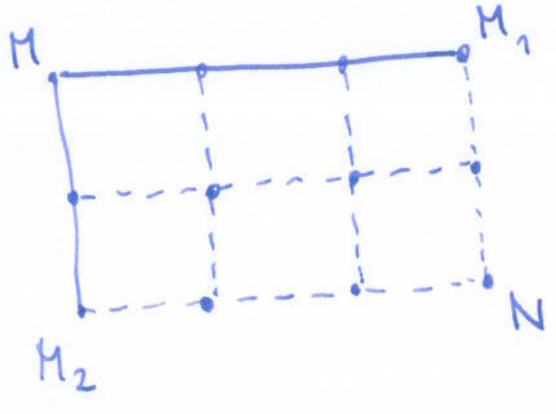
$$\ldots\ldots, M = K, K = N, M = N.$$

ATD.

Teď ukážeme, že β je CR.

<u>Pomocné tvrzení</u>: Je-li R^* tranzitivní uzávěr binární relace R, pak $R \models \Diamond$ implikuje $R^* \models \Diamond$.

Důkaz pomocí diagramu



Budeme postupovat takto: definujeme relaci $\underset{1}{\twoheadrightarrow}$ a ukážeme, že

(1) $\underset{1}{\twoheadrightarrow}$ má diamantovou vlastnost

(2) $\twoheadrightarrow_\beta$ je tranzitivní uzávěr $\underset{1}{\twoheadrightarrow}$.

Položíme

- $M \underset{1}{\twoheadrightarrow} M$
- jestliže $M \underset{1}{\twoheadrightarrow} M'$, pak $\lambda x.M \underset{1}{\twoheadrightarrow} \lambda x.M'$
- jestliže $M \underset{1}{\twoheadrightarrow} M'$, $N \underset{1}{\twoheadrightarrow} N'$, pak $MN \underset{1}{\twoheadrightarrow} M'N'$
- jestliže $M \underset{1}{\twoheadrightarrow} M'$, $N \underset{1}{\twoheadrightarrow} N'$, pak $(\lambda x.M)N \underset{1}{\twoheadrightarrow} M'[x:=N']$

<u>Kostra (technického) důkazu</u>.

1. Jestliže $M \underset{1}{\twoheadrightarrow} M'$ a $N \underset{1}{\twoheadrightarrow} N'$, pak $M[x:=N] \underset{1}{\twoheadrightarrow} M'[x:=N']$
(indukcí podle definice $M \underset{1}{\twoheadrightarrow} M'$)

2. $\lambda x.M \underset{1}{\twoheadrightarrow} N$ znamená $N \equiv \lambda x.M'$, kde $M \underset{1}{\twoheadrightarrow} M'$
a $MN \underset{1}{\twoheadrightarrow} L$ znamená buď

$$L \equiv M'N', \text{ kde } M \underset{1}{\twoheadrightarrow} M', N \underset{1}{\twoheadrightarrow} N',$$

nebo

$$M \equiv \lambda x.P, \ L \equiv P'[x:=N'], \ P \underset{1}{\twoheadrightarrow} P', N \underset{1}{\twoheadrightarrow} N'.$$

(indukcí podle definice $\underset{1}{\twoheadrightarrow}$)

3. $\underset{1}{\twoheadrightarrow}$ má diamantovou vlastnost
(indukcí podle definice $M \underset{1}{\twoheadrightarrow} M_1$ dokážeš, že jestliže $M \underset{1}{\twoheadrightarrow} M_2$, pak existuje N takové, že $M_1 \underset{1}{\twoheadrightarrow} N$, $M_2 \underset{1}{\twoheadrightarrow} N$)

4. $\twoheadrightarrow_\beta$ je tranzitivní uzávěr $\underset{1}{\twoheadrightarrow}$.

(pro $\underset{=}{\rightarrow}_\beta = \rightarrow_\beta \cup$ „$=$" platí $\underset{=}{\rightarrow}_\beta \subseteq \underset{1}{\twoheadrightarrow} \subseteq \twoheadrightarrow_\beta$, přičemž $\twoheadrightarrow_\beta$ je tranzitivní uzávěr $\underset{=}{\rightarrow}_\beta$)

a máme výsledek:

<u>Churchův - Rosserův teorém pro β-redukci</u>

1. β je CR
2. Jestliže $M =_\beta N$, pak existuje Z tak, že $M \twoheadrightarrow_\beta Z$ a $N \twoheadrightarrow_\beta Z$.

a známý <u>důsledek</u>:

1. Je-li N β-nf M, pak $M \twoheadrightarrow_\beta N$.
2. M má maximálně jednu β-nf.

a odtud:

Teorie λ je konzistentní.

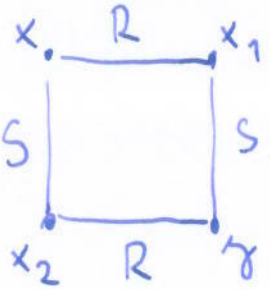
Další témata ohledně redukce už zkratkovitě.

η-redukce

Je dána rovnou $\eta = \{(\lambda x.Mx, M) \mid M \in \Lambda, x \notin FV(M)\}$
Klademe $\beta\eta = \beta \cup \eta$.

Platí $M =_{\beta\eta} N$ p.k. $\lambda\eta \vdash M = N \iff \lambda + ext \vdash M = N$
(stačí dokázat první ekvivalenci; indukcí jako obvykle)

Dvě binární relace R, S na množině X komutují, jestliže z $(x, x_1) \in R$ a $(x, x_2) \in S$ plyne, že existuje prvek y tak, že $(x_1, y) \in S$ a $(x_2, y) \in R$.



Je to jiný pojem komutativity než pro skládání relací.

Platí η je CR, $\twoheadrightarrow_\beta$ a $\twoheadrightarrow_\eta$ komutují.

Platí jestliže R_1, R_2 jsou CR a $\twoheadrightarrow_{R_1}, \twoheadrightarrow_{R_2}$ komutují, pak $R_1 R_2$ je CR.

Odtud (podobně jako dříve) plyne

Churchův-Rosserův teorém pro $\beta\eta$-redukci:

1. $\beta\eta$ je CR

2. Jestliže $M =_{\beta\eta} N$, pak ex. Z: $M \twoheadrightarrow_{\beta\eta} Z$ a $N \twoheadrightarrow_{\beta\eta} Z$.

Důsledky.

- Jestliže N je $\beta\eta$-nf M, pak $M \twoheadrightarrow_{\beta\eta} N$.
- Každý M má max. jednu $\beta\eta$-nf
- Pro různé $\beta\eta$-nf M, N platí $M \neq_{\beta\eta} N$
- Teorie λ+ext je konzistentní.

NEDOKÁZALI JSME

- M má β-nf právě když má $\beta\eta$-nf
- Pro různé $\beta\eta$-nf M, N platí $M \# N$ (silnost)

POZNÁMKA K HLAVOVÉ-NF (head-nf)