REDUKCE

Doposud jsme mluvili o konverzi. Pro $\lambda \vdash M = N$ říkáme, že M a N jsou (vzájemně) konvertibilní.

(název β-redukce byl nesprávný, patří β-konverze.)

Výpočty (úpravy) jdou ale často jen jedním směrem:

$$(\lambda x. x^2+1)3 = 10$$

můžeme chápat jako „výsledkem výpočtu $(\lambda x. x^2+1)3$ je 10, ale nikoliv naopak.

To nás vede k redukci.

Pojmy redukce (redukční pojmy)

Můžeme mít různé redukce (podle různých pravidel) proto se jimi budeme zabývat obecně.

Binární relace R na Λ je kompatibilní, když z $(M, M') \in R$ plyne:

- $(ZM, ZM') \in R$ - $(MZ, M'Z) \in R$
- $(\lambda x.M, \lambda x M') \in R$.

R je kompatibilní právě když pro libovolné $M, M' \in \Lambda$ a kontext $C[\;]$ s jednou dírou z $(M, M') \in R$ plyne $(C[M], C[M']) \in R$.

Každá binární relace na Λ má kompatibilní uzávěr. (Důkaz?)

Rovnost (kongruence, konvertibilita) na Λ je kompatibilní ekvivalence.

Například relace mezi $M, N \in \Lambda$ dané $\lambda \vdash M = N$, resp. $\lambda\eta \vdash M = N$ jsou rovnosti na Λ.

(Relace) redukce na Λ je kompatibilní, reflexivní a tranzitivní.

Pojem redukce (redukční pojem) na Λ (notion of reduction) je libovolná binární relace R na Λ.

Například $\beta = \{((\lambda x.M)N, M[x := N]) \mid M, N \in \Lambda\}$ je pojem redukce.

$\rightarrow_R$: jeden krok R-redukce: kompatibilní uz. R

$\twoheadrightarrow_R$: R-redukce: reflex. a tranzit. uzávěr $\rightarrow_R$

$=_R$: R-rovnost (R-konvertibilita): ekviv. generovaná $\twoheadrightarrow_R$.

Poznámky ke kompatibilitě

- Pojem kompatibilního uzávěru má smysl, pokud průnikem kompatibilních relací je opět kompatibilní relace. To je třeba dokázat.
  Uzávěr R je pak průnik všech kompatibilních $S \supseteq R$.

- $\twoheadrightarrow_R$ a $=_R$ jsou kompatibilní. Dokazuje se indukcí.
  Například pro $\twoheadrightarrow_R$:

1. Předpokl., že $M \twoheadrightarrow_R N$ protože $M \equiv N$.
   Pak $C[M] \equiv C[N]$, takže $C[M] \twoheadrightarrow_R C[N]$.
2. Předp., že $M \twoheadrightarrow_R N$ protože $M \to_R N$.
   Jelikož $\to_R$ je kompatibilní, máme $C[M] \to_R C[N]$ a tedy (protože $\to_R \subseteq \twoheadrightarrow_R$) $C[M] \twoheadrightarrow_R C[N]$.
3. To byl základní krok indukce. Teď předp., že $M \twoheadrightarrow_R N$ a ex. L tak, že $M \twoheadrightarrow_R L$, $L \twoheadrightarrow_R N$ a (indukční předpoklad:) $C[M] \twoheadrightarrow_R C[L]$, $C[L] \twoheadrightarrow_R C[N]$.
   Z tranzitivity: $C[M] \twoheadrightarrow_R C[N]$.

C.B.D.

Příklad.

$$(\lambda x.xx)(\lambda y.y)z \to_\beta (\lambda y.y)(\lambda y.y)z$$

$$\to_\beta (\lambda y.y)z \to_\beta z.$$

Tedy $(\lambda x.xx)(\lambda y.y)z \twoheadrightarrow_\beta z.$

a tedy $(\lambda x.xx)(\lambda y.y)z =_\beta z.$

R-normální forma

- M je R-redex (reducible expression), když existuje N tak, že $(M,N) \in R$.
  N je ~~[illegible]~~ R-kontraktum M.
- M je R-normální forma (v R-nf), pokud neobsahuje R-redex (jako podvýraz)
- N je R-normální forma výrazu M, pokud je R-nf a $M =_R N$.

„Proces kontrakce"

Příklad. $(\lambda x.xx)(\lambda y.y)$ je β-redex. Proto $(\lambda x.xx)(\lambda y.y)z$ není β-nf, ale má β-nf.

Tvrzení.

Jestliže $M \to_R N$, pak ex. $C[\,]$ s jednou dírou, $P, Q \in \Lambda$ tak, že $(P, Q) \in R$.

Důkaz. Z definice.

Důsledek.

Je-li M R-nf, pak

(1) Pro žádné N neplatí $M \to_R N$

(2) $M \twoheadrightarrow_R N$ implikuje $M \equiv N$.

Pozor, obecně neplatí, že pokud M splňuje (2), je v R-nf. Protipříklad:

$$M = \Omega = (\lambda x.xx)(\lambda x.xx).$$

Diamantová vlastnost

Je to vlastnost, která zaručí, že každý výraz má nejvýše jednu R-nf.

Pro binární relaci $\succ$ na Λ: Jestliže $M \succ M_1$ a $M \succ M_2$, pak ex. N tak, že $M_1 \succ N$ a $M_2 \succ N$. Zápis: $\succ \models \Diamond$.

(konfluence)

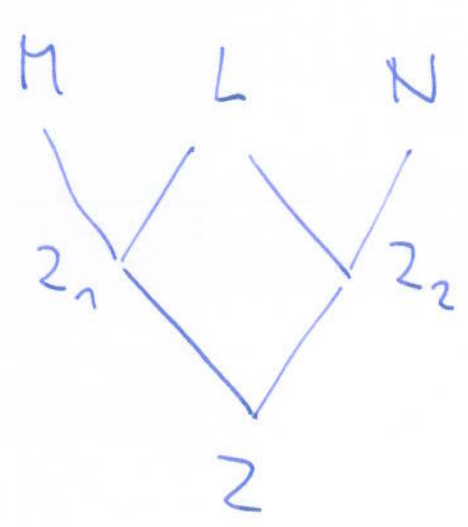
Redukční pojem R má <u>Church-Rosserovu vlastnost</u> (je <u>CR</u>), jestliže $\twoheadrightarrow_R$ má diamantovou vlastnost (splňuje diamantovou podmínku).

<u>Teorém o CR</u>

Jestliže R je CR, pak z $M =_R N$ plyne, že existuje Z tak, že $M \twoheadrightarrow_R Z$ a $N \twoheadrightarrow_R Z$.

<u>Důkaz</u>. Indukcí přes strukturu $=_R$.

1. $M =_R N$ protože $M \twoheadrightarrow_R N$. Pak stačí vzít $Z \equiv N$
2. $M =_R N$ protože $N \twoheadrightarrow_R M$. Pak $Z \equiv M$.
3. $M =_R N$ jelikož $M =_R L$, $L =_R N$ a tyto rovnosti splňují indukční předpoklad:



Důsledky. (R je CR)

(1) Jestliže N je R-nf M, pak $M \twoheadrightarrow_R N$.

(2) $M \in \Lambda$ má nejvýše jednu R-nf.

~~K důkazu výsledků z 3. přednášky o jedinečnosti β-nf stačí dokázat, že β je CR.~~

2. Máme důkaz délky $k > 1$:

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

~~Podle~~ 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 ~~pro~~ 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 $M \equiv (\lambda x.K)L$, ~~$N \equiv K[x$~~ $N = K[x := L]$. 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:

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

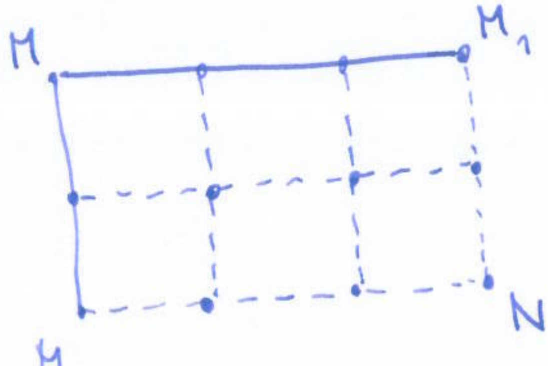
4. $M \twoheadrightarrow_\beta N$, $M \not\equiv N$, $M \not\to_\beta N$. Pak podle ind. předpokladu ex. K tak, že $M \twoheadrightarrow_\beta K$, $K \twoheadrightarrow_\beta N$, $\lambda \vdash M = K, K = N$. Pak tato je důkaz:

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

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 $(\lambda x.M)N \underset{1}{\twoheadrightarrow} M'[x:=N']$

Kostra (technického) důkazu.

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 $M \underset{1}{\twoheadrightarrow} M_1$ dokázat, že jestliže $M \underset{1}{\twoheadrightarrow} M_2$, pak existuje N takový, 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.

<u>η-redukce</u>

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

<u>Platí</u> $M =_{\beta\eta} N$ 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 <u>komutují</u>, 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 $(x_2, y) \in R$.

$$\begin{tikzcd} x \arrow[r, dash, "R"] \arrow[d, dash, "S"'] & x_1 \arrow[d, dash, "S"] \\ x_2 \arrow[r, dash, "R"'] & y \end{tikzcd}$$

<u>Je to jiný pojem komutativity než pro skládání relací.</u>

<u>Platí</u> η je CR, $\twoheadrightarrow_\beta$ a $\twoheadrightarrow_\eta$ komutují.

<u>Platí</u> Jestliže R_1, R_2 jsou CR a $\twoheadrightarrow_{R_1}, \twoheadrightarrow_{R_2}$ komutují, pak R_1R_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 ~~β~~ 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 $M \# N$ (úplnost)

~~POZNÁMKA K HLAVOVÉ-NF (head-nf)~~