LMSE 1

Logische Methoden des Software Engineerings

Vertiefungsmodul 1

Prof. Dr. Jakob Rehof

M.Sc. Andrej Dudenhefner

Lehrstuhl XIV, Software Engineering

Diese Vorlesung

- Induktionsprinzipien
- Newman‘s Lemma
- Konfluenz des Lambda-Kalküls:

  Church-Rosser Satz

Lesen und Übungen

- Lesen: LCHI Abschn. 1.4 (S. 8-11)

- Übungen:
  - Folie 17
  - LCHI 1.7.8
  - LCHI 1.7.9
  - LCHI 1.7.10

Principle of mathematical induction

For every property of natural numbers $\mathscr{P} \subseteq \mathbb{N}$:

$$[\mathscr{P}(0) \land (\forall n \in \mathbb{N}.\ \mathscr{P}(n) \Rightarrow \mathscr{P}(n+1))] \Rightarrow [\forall n \in \mathbb{N}.\ \mathscr{P}(n)]$$

Stated as rule of inference:

$$\frac{\mathscr{P}(0) \quad (\forall n \in \mathbb{N}.\ \mathscr{P}(n) \Rightarrow \mathscr{P}(n+1))}{\forall n \in \mathbb{N}.\ \mathscr{P}(n)}$$

Principle of mathematical induction

EXAMPLE. *For all $n \in \mathbb{N}$:*

$$\sum_{i=0}^{n} i = n(n+1)/2$$

Proof. By induction on n.

For the base case $\mathscr{P}(0)$ ($n = 0$) we have

$$\sum_{i=0}^{0} i = 0 = 0(0+1)/2$$

and the claim is true in this case.

For the inductive step, assume $\mathscr{P}(n)$ as induction hypothesis (I.H.)

$$\sum_{i=0}^{n} i = n(n+1)/2$$

We must prove $\mathscr{P}(n+1)$:

$$\sum_{i=0}^{n+1} i = (n+1)((n+1)+1)/2$$

We have

$$\begin{aligned}
\textstyle\sum_{i=0}^{n+1} i & = \\
(\textstyle\sum_{i=0}^{n} i) + n + 1 & = \quad (I.H.) \\
(n(n+1)/2) + n + 1 & = \\
(n(n+1) + 2(n+1))/2 & = \\
(n+1)(n+2)/2 & = \\
(n+1)((n+1)+1)/2 &
\end{aligned}$$

□

Strong (complete) induction

For every property of natural numbers $\mathscr{P} \subseteq \mathbb{N}$:

$$[\mathscr{P}(0) \land (\forall m > 0.\, \forall n < m.\, \mathscr{P}(n) \Rightarrow \mathscr{P}(m))] \Rightarrow [\forall n \in \mathbb{N}.\, \mathscr{P}(n)]$$

Stated as rule of inference:

$$\frac{\mathscr{P}(0) \quad (\forall m > 0. \forall n < m.\, \mathscr{P}(n) \Rightarrow \mathscr{P}(m))}{\forall n \in \mathbb{N}.\, \mathscr{P}(n)}$$

Induction on terms

For every property of λ-terms $\mathscr{P} \subseteq \Lambda$:

$$\left.\begin{array}{ll} \mathscr{P}(x) & \wedge \\ \forall M \in \Lambda.\ \mathscr{P}(M) \Rightarrow \mathscr{P}(\lambda x.M) & \wedge \\ \forall M \in \Lambda. \forall N \in \Lambda.\ \mathscr{P}(M) \wedge \mathscr{P}(N) \Rightarrow \mathscr{P}(M\ N) & \end{array}\right\} \Rightarrow \forall M \in \Lambda.\ \mathscr{P}(M)$$

This principle can easily be proven by induction on the measure $d(\_)$ defined by:

$$\begin{array}{lcl} d(x) & = & 0 \\ d(\lambda x.N) & = & d(N) + 1 \\ d(MN) & = & \max\{d(M), d(N)\} + 1 \end{array}$$

Well founded induction

Let X be an arbitrary set, and let $R \subseteq X \times X$ be a binary relation on X. We say that R is *well founded* on X, if the following condition is true:

$$\forall S \subseteq X.\, (S \neq \emptyset \Rightarrow \exists m \in S. \forall s \in S.\, (s, m) \notin R)$$

This is sometimes expressed informally as the principle: "Every non-empty subset has a minimal element". A relation is sometimes called *Noetherian* (after Emily Noether), if R^{-1} is well founded.

Let $\mathscr{P} \subseteq X$ be a property on X. The principle of well founded induction states:

$$\forall x \in X.[(\forall y \in X.\, (yRx \Rightarrow \mathscr{P}(y))) \Rightarrow \mathscr{P}(x)] \Rightarrow \forall x \in X.\, \mathscr{P}(x)$$

Informally: If we can show $\mathscr{P}(x)$, whenever $\mathscr{P}$ is true of smaller elements than x, then we can conclude that $\mathscr{P}$ holds everywhere.

Terminating relations (strong normalization)

Let X be an arbitrary set, and let $R \subseteq X \times X$ be a binary relation on X. For $x, y \in X$, let us write $x \longrightarrow_R y$, if and only if, $(x, y) \in R$. Let $\longrightarrow_R^*$ be the transitive closure of $\longrightarrow_R$. We say that R is *terminating*, if and only if there are no infinite chains

$$x_0 \longrightarrow_R x_1 \longrightarrow_R \cdots \longrightarrow_R x_n \longrightarrow_R \cdots$$

Then R^{-1} is well founded on X: For let $S \subseteq X, S \neq \emptyset$. Pick any $x \in S$. Then by termination of R there exists an s_x (a "normal form" of x) such that either $x = s_x$ or $x \longrightarrow_R^* s_x$, and there is no $y \in S$ such that $s_x \longrightarrow_R^* y$. Then s_x is a minimal element in S.

Confluence and local confluence

Let X be an arbitrary set, and let $\longrightarrow_R \subseteq X \times X$ be a binary relation on X. We write $\longrightarrow_R^*$ for the transitive closure of R, and we write $\twoheadrightarrow_R$ for the reflexive transitive closure of R.

Definition (Local clonfluence). *A relation $\longrightarrow_R$ on X is called* locally confluent*, if and only if the following is true:*

$$\forall x, x_1, x_2 \in X.\ [(x \longrightarrow_R x_1 \wedge x \longrightarrow_R x_2) \Rightarrow (\exists x_3 \in X.\ x_1 \twoheadrightarrow_R x_3 \wedge x_2 \twoheadrightarrow_R x_3)]$$

Definition (Confluence). *A relation $\longrightarrow_R$ on X is called* confluent*, if and only if the following is true:*

$$\forall x, x_1, x_2 \in X.\ [(x \twoheadrightarrow_R x_1 \wedge x \twoheadrightarrow_R x_2) \Rightarrow (\exists x_3 \in X.\ x_1 \twoheadrightarrow_R x_3 \wedge x_2 \twoheadrightarrow_R x_3)]$$

Definition (Diamond property). *A relation $\longrightarrow_R$ on X is said to have the* diamond property*, if and only if the following is true:*

$$\forall x, x_1, x_2 \in X.\ [(x \longrightarrow_R x_1 \wedge x \longrightarrow_R x_2) \Rightarrow (\exists x_3 \in X.\ x_1 \longrightarrow_R x_3 \wedge x_2 \longrightarrow_R x_3)]$$

Note that a relation $\longrightarrow_R$ is confluent, if and only if $\twoheadrightarrow_R$ has the diamond property.

Newman's Lemma

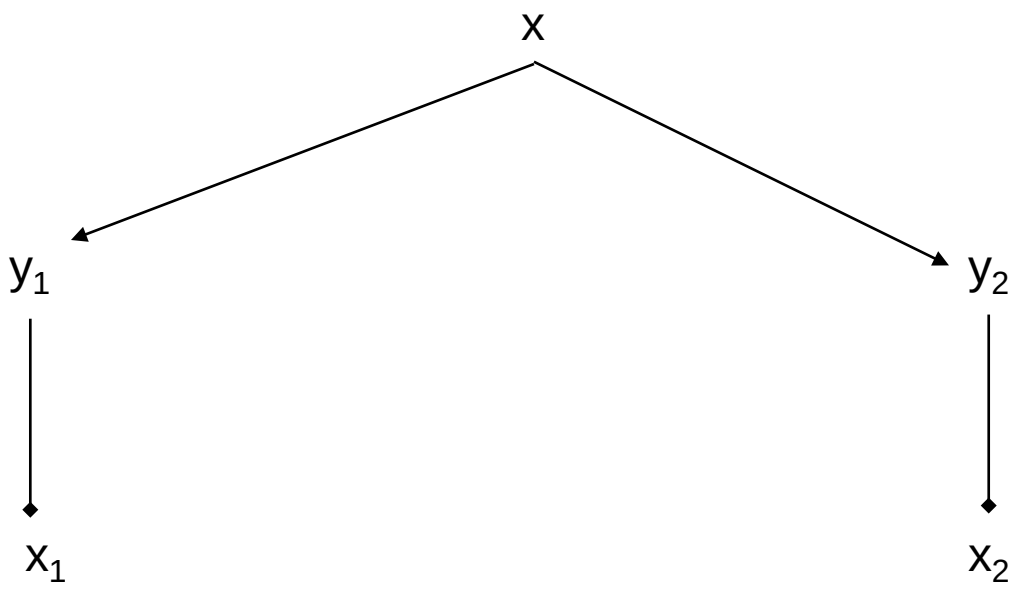
Lemma (Newman's Lemma). *Let R be a terminating relation on X. If R is locally confluent, then R is confluent.*

Proof. By well founded (Noetherian) induction.

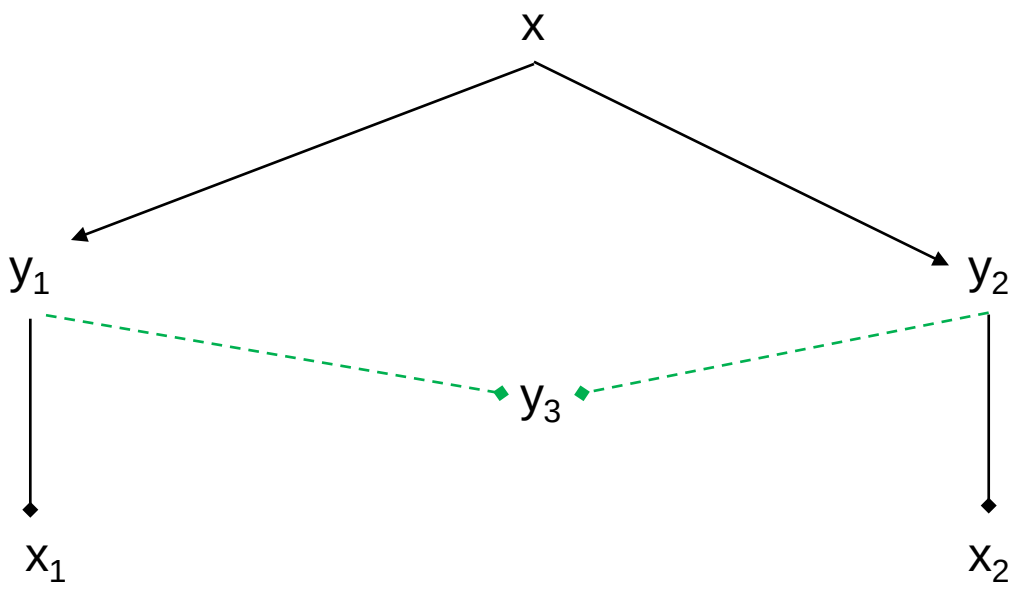
Assume $x \twoheadrightarrow_R x_1$ and $x \twoheadrightarrow_R x_2$. If x is minimal (i.e. there is no $y \in X$ such that $x \twoheadrightarrow_R y$), the claim is true, since we can take $x_1 = x_2 = x$. So assume x is not minimal. If eiter $x = x_1$ or $x = x_2$, the claim is evidently true (take $x_3 = x_2$ or $x_3 = x_1$, respectively), so it suffices to consider the situation $x \longrightarrow_R x_1$ and $x \longrightarrow_R x_2$. The claim now follows by a diagram chase using local confluence of R followed by three applications of induction hypothesis. □

The Lemma was originally proven by M. H. A. Newman in *Annals of Mathematics*, vol. 43, No. 2, April 1941. The proof is by a very complicated "direct" combinatorial argument. The reduction in proof complexity resulting from the application of Noetherian induction is astounding.

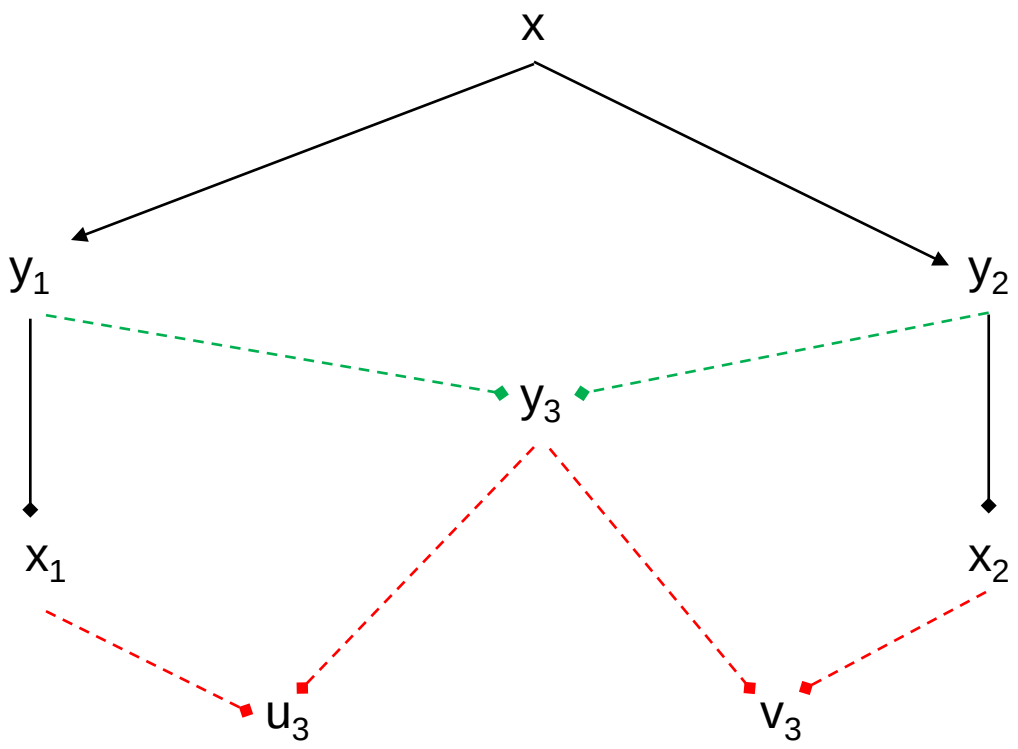
Initial situation



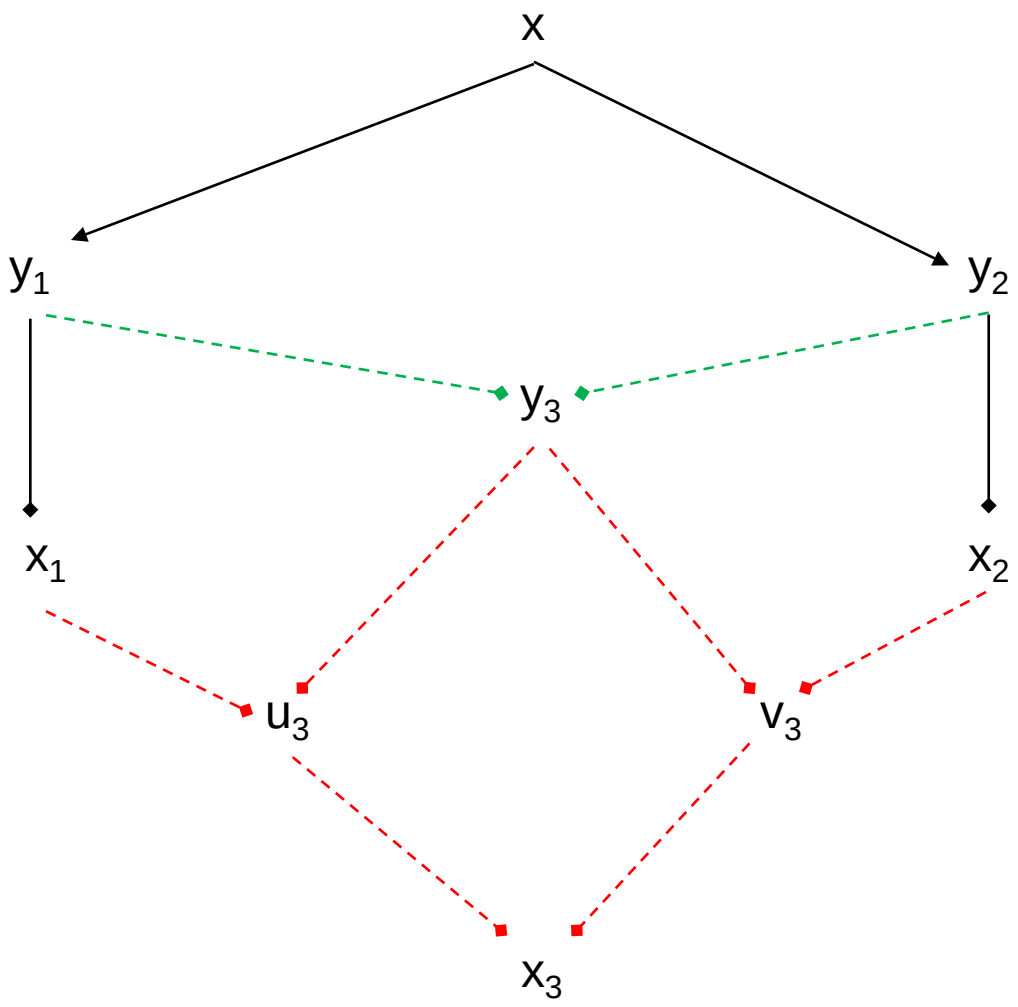
Local confluence



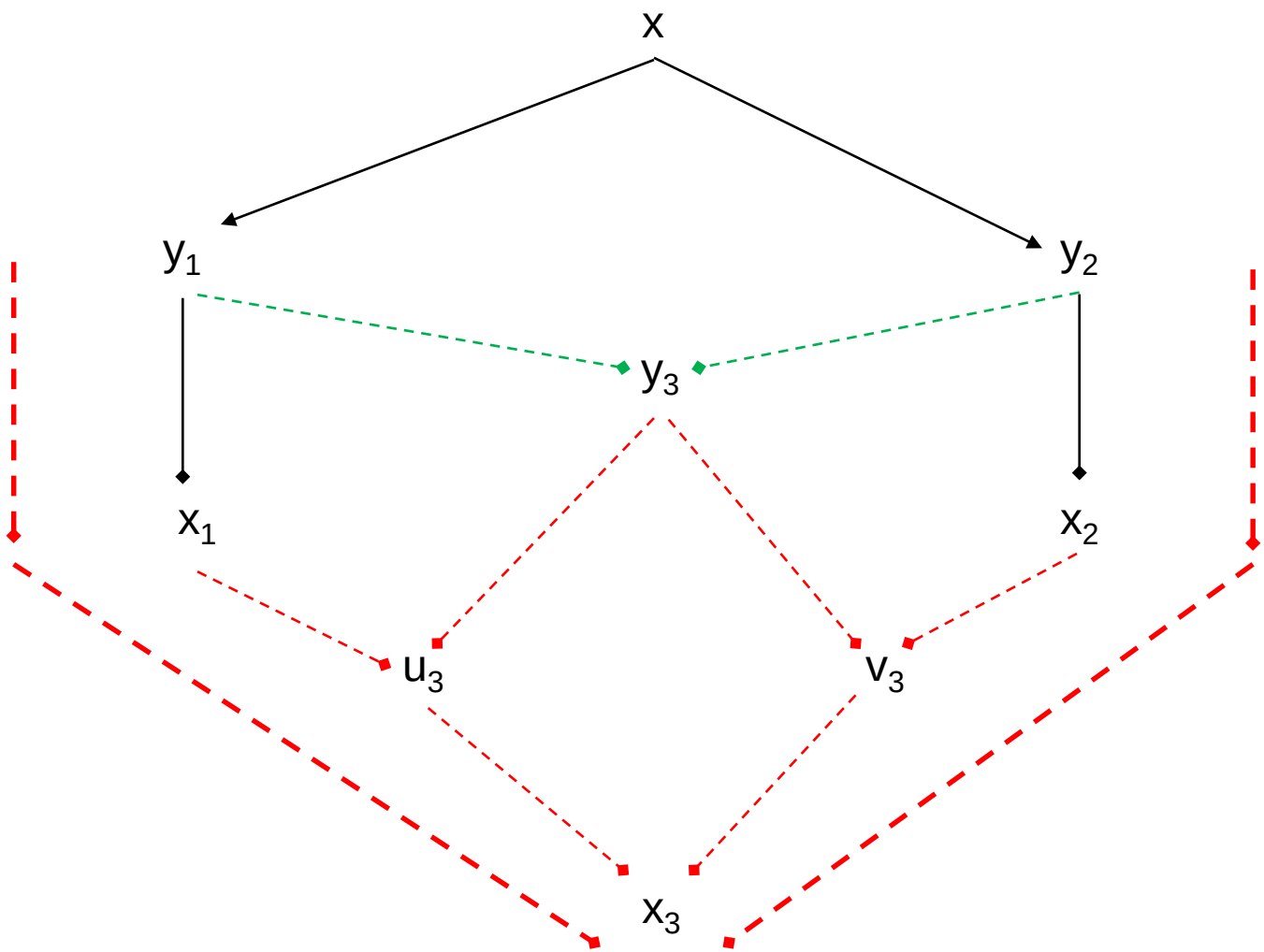
Induction hypothesis (twice)!



Induction hypothesis again!



QED!



Übung

Warum ist die Annahme der Terminierung von R notwendig in Newman‘s Lemma?

Geben Sie ein Beispiel für eine nicht-terminierende Relation R, die lokal konfluent aber nicht konfluent ist!

Reflexive und transitive Hülle

---

[1] Let R be a relation on Λ. The *transitive closure* of R is the least relation R^* satisfying:

$$\begin{array}{lcl} PRP' & \Rightarrow & PR^*P' \\ PR^*P' \ \& \ P'R^*P'' & \Rightarrow & PR^*P'' \end{array}$$

The *reflexive closure* of R is the least relation $R^=$ satisfying:

$$\begin{array}{lcl} PRP' & \Rightarrow & PR^=P' \\ PR^=P & & \end{array}$$

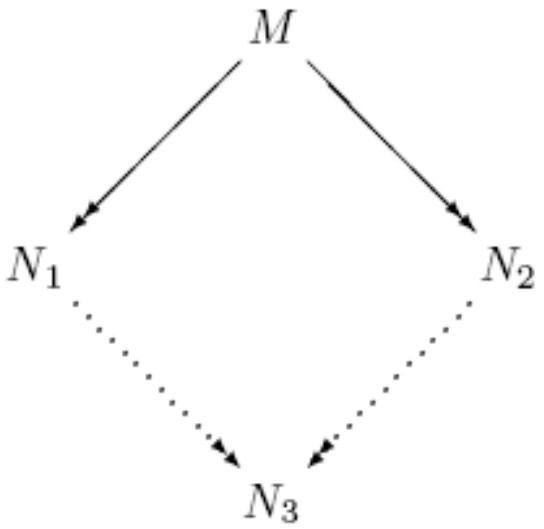
The Church-Rosser theorem (confluence)

$$\mathbf{K}\ (\mathbf{I}\ \mathbf{I}) \rightarrow_\beta \lambda x.(\mathbf{I}\ \mathbf{I})$$

$$\mathbf{K}\ (\mathbf{I}\ \mathbf{I}) \rightarrow_\beta \mathbf{K}\ \mathbf{I}$$

Church-Rosser (confluence) property

If $M \twoheadrightarrow_\beta N_1$, $M \twoheadrightarrow_\beta N_2$, *then for some* N_3 *one has* $N_1 \twoheadrightarrow_\beta N_3$ *and* $N_2 \twoheadrightarrow_\beta N_3$; *in diagram*



Frage: Warum nicht direkt durch Induktion beweisen?
Frage: Warum nicht von lokaler Konfluenz generalisieren?

Diamond property

1.4.1. DEFINITION. A relation $>$ on Λ satisfies the *diamond property* if, for all $M_1, M_2, M_3 \in \Lambda$, if $M_1 > M_2$ and $M_1 > M_3$, then there exists an $M_4 \in \Lambda$ such that $M_2 > M_4$ and $M_3 > M_4$.

Frage: Hat beta-Reduktion die Diamanteigenschaft?

Diamond property

1.4.2. LEMMA. *Let $>$ be a relation on Λ and suppose that its transitive closure*[1] *is $\twoheadrightarrow_\beta$. If $>$ satisfies the diamond property, then so does $\twoheadrightarrow_\beta$.*

PROOF. First show by induction on n that $M_1 > N_1$ and $M_1 > \ldots > M_n$ implies that there are $N_2, \ldots, N_n$ such that $N_1 > N_2 > \ldots > N_n$ and $M_n > N_n$.

Using this property, show by induction on m that if $N_1 > \ldots > N_m$ and $N_1 >^* M_1$ then there are $M_2, \ldots, M_m$ such that $M_1 > M_2 > \ldots > M_m$ and $N_m >^* M_m$.

Now assume $M_1 \twoheadrightarrow_\beta M_2$ and $M_1 \twoheadrightarrow_\beta M_3$. Since $\twoheadrightarrow_\beta$ is the transitive closure of $>$ we have $M_1 > \ldots > M_2$ and $M_1 > \ldots > M_3$. By what was shown above, we can find M_4 such that $M_2 > \ldots > M_4$ and $M_3 > \ldots > M_4$. Since $\twoheadrightarrow_\beta$ is the transitive closure of $>$, also $M_2 \twoheadrightarrow_\beta M_4$ and $M_3 \twoheadrightarrow_\beta M_4$. $\square$

Parallel reduction (Tait & Martin-Löf)

1.4.3. DEFINITION. Let $\twoheadrightarrow_l$ be the relation on Λ defined by:

$$
\begin{array}{lcl}
P \twoheadrightarrow_l P & & \\
P \twoheadrightarrow_l P' & \Rightarrow & \lambda x.P \twoheadrightarrow_l \lambda x.P' \\
P \twoheadrightarrow_l P' \ \& \ Q \twoheadrightarrow_l Q' & \Rightarrow & P\,Q \twoheadrightarrow_l P'\,Q' \\
P \twoheadrightarrow_l P' \ \& \ Q \twoheadrightarrow_l Q' & \Rightarrow & (\lambda x.P)\,Q \twoheadrightarrow_l P'[x := Q']
\end{array}
$$

Parallel reduction

1.4.4. LEMMA. $M \twoheadrightarrow_l M' \ \& \ N \twoheadrightarrow_l N' \Rightarrow M[x := N] \twoheadrightarrow_l M'[x := N']$.

PROOF. By induction on the definition of $M \twoheadrightarrow_l M'$. In case M' is M, proceed by induction on M. $\square$

Parallel reduction has diamond property

1.4.5. LEMMA. *$\twoheadrightarrow_l$ satisfies the diamond property, i.e., for all $M_1, M_2, M_3 \in \Lambda$, if $M_1 \twoheadrightarrow_l M_2$ and $M_1 \twoheadrightarrow_l M_3$, then there exists an $M_4 \in \Lambda$ such that $M_2 \twoheadrightarrow_l M_4$ and $M_3 \twoheadrightarrow_l M_4$.*

PROOF. By induction on the definition of $M_1 \twoheadrightarrow_l M_2$, using the above lemma. □

Parellel reduction and beta reduction

1.4.6. LEMMA. *$\twoheadrightarrow_\beta$ is the transitive closure of $\twoheadrightarrow_l$.*

PROOF. Clearly[2]

$$(\rightarrow_\beta)^= \subseteq \twoheadrightarrow_l \subseteq \twoheadrightarrow_\beta$$

Then

$$\twoheadrightarrow_\beta = ((\rightarrow_\beta)^=)^* \subseteq \twoheadrightarrow_l^* \subseteq (\twoheadrightarrow_\beta)^* = \twoheadrightarrow_\beta$$

In particular, $\twoheadrightarrow_l^* = \twoheadrightarrow_\beta$. □

Church-Rosser theorem

1.4.7. THEOREM (Church and Rosser, 1936). *For every* $M_1, M_2, M_3 \in \Lambda$, *if* $M_1 \twoheadrightarrow_\beta M_2$ *and* $M_1 \twoheadrightarrow_\beta M_3$, *then there exists an* $M_4 \in \Lambda$ *such that* $M_2 \twoheadrightarrow_\beta M_4$ *and* $M_3 \twoheadrightarrow_\beta M_4$.

PROOF (Tait & Martin-Löf). By the above three lemmas. □

Corollaries of the Church-Rosser theorem

1.4.8. COROLLARY. *For all $M, N \in \Lambda$, if $M =_\beta N$, then there exists an $L \in \Lambda$ such that $M \twoheadrightarrow_\beta L$ and $N \twoheadrightarrow_\beta L$.*

1.4.9. COROLLARY. *For all $M, N_1, N_2 \in \Lambda$, if $M \twoheadrightarrow_\beta N_1$ and $M \twoheadrightarrow_\beta N_2$ and both N_1 and N_2 are in β-normal form, then $N_1 = N_2$.*

1.4.10. COROLLARY. *For all $M, N \in \Lambda$, if there are β-normal forms L_1 and L_2 such that $M \twoheadrightarrow_\beta L_1$, $N \twoheadrightarrow_\beta L_2$, and $L_1 \neq L_2$, then $M \neq_\beta N$.*

Notions of consistency and completeness for beta-conversion

- Equational consistency (non-triviality)
  - There exists an unprovable equation
- Hilbert-Post completeness
  - Maximal consistency
  - No new equation can be consistently added