

# LMSE

Logische Methoden des Software  
Engineerings

Prof. Dr. Jakob Rehof

Lehrstuhl XIV, Software Engineering

# Diese Vorlesung

- ❖ Induktionsprinzipien
- ❖ Newman's Lemma
- ❖ Konfluenz des Lambda-Kalküls:  
Church-Rosser Satz

# Lesen und Übungen für nächste Woche

- Lesen: LCHI Abschn. 1.4 (S. 8-11)
- Übungen:
  - Folie 17
  - LCHI 1.7.8
  - LCHI 1.7.9
  - LCHI 1.7.10

Note (JR)

---

## Principle of mathematical induction

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

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

Stated as rule of inference:

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

## 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  $\mathcal{P}(0)$  ( $n = 0$ ) 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  $\mathcal{P}(n)$  as induction hypothesis (I.H.)

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

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

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

We have

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

□

Note (JR)

---

## Strong (complete) induction

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

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

Stated as rule of inference:

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

Note (JR)

---

## Induction on terms

For every property of  $\lambda$ -terms  $\mathcal{P} \subseteq \Lambda$ :

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

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

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

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

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

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



Note (JR)

---

## 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,  $(y, x) \in R$  (that is,  $\longrightarrow_R = R^{-1}$ ). 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  $\longrightarrow_R$  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 confluence).** *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

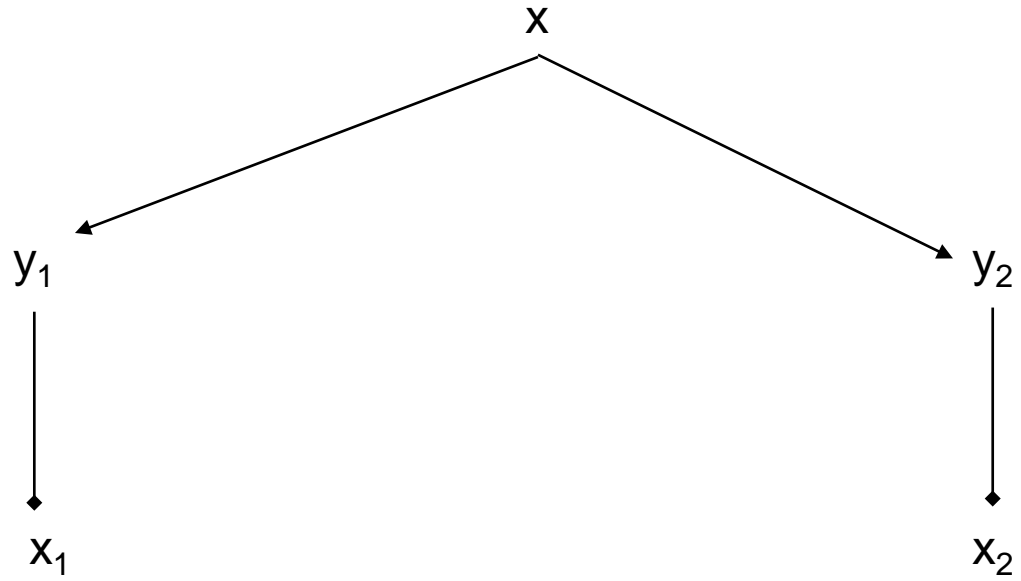
LEMMA (Newman's Lemma). *Let  $R$  be a terminating relation on  $X$ . If  $R$  is locally confluent, then  $R$  is confluent.*

*Proof.* By well founded (Noetherian) induction.

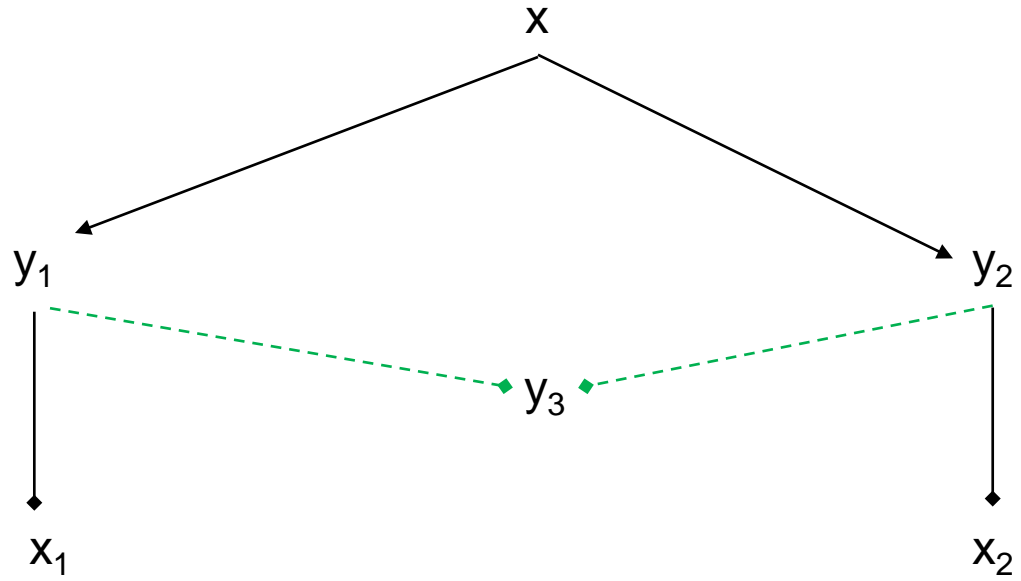
Assume  $x \twoheadrightarrow_R x_1$  and  $x \twoheadrightarrow_R x_2$ . If  $x$  is minimal (i.e. there is no  $y \in X$  such that  $x \twoheadrightarrow_R y$ ), the claim is true, since we can take  $x_1 = x_2 = x$ . So assume  $x$  is not minimal. If either  $x = x_1$  or  $x = x_2$ , the claim 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.  $\square$

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.

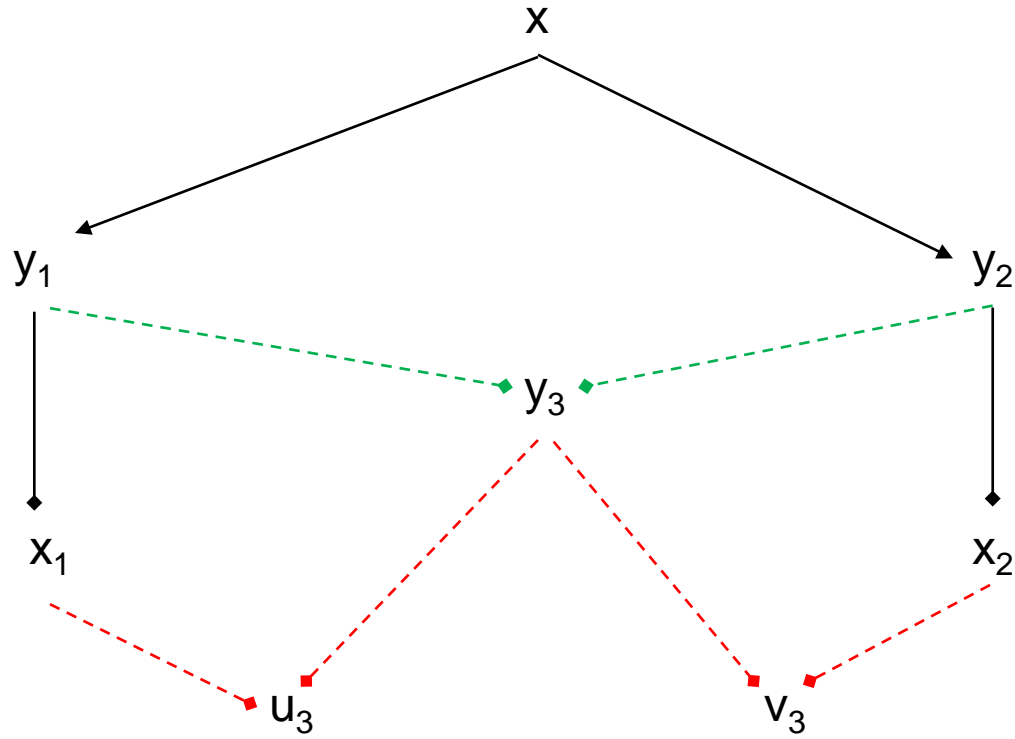
Initial situation



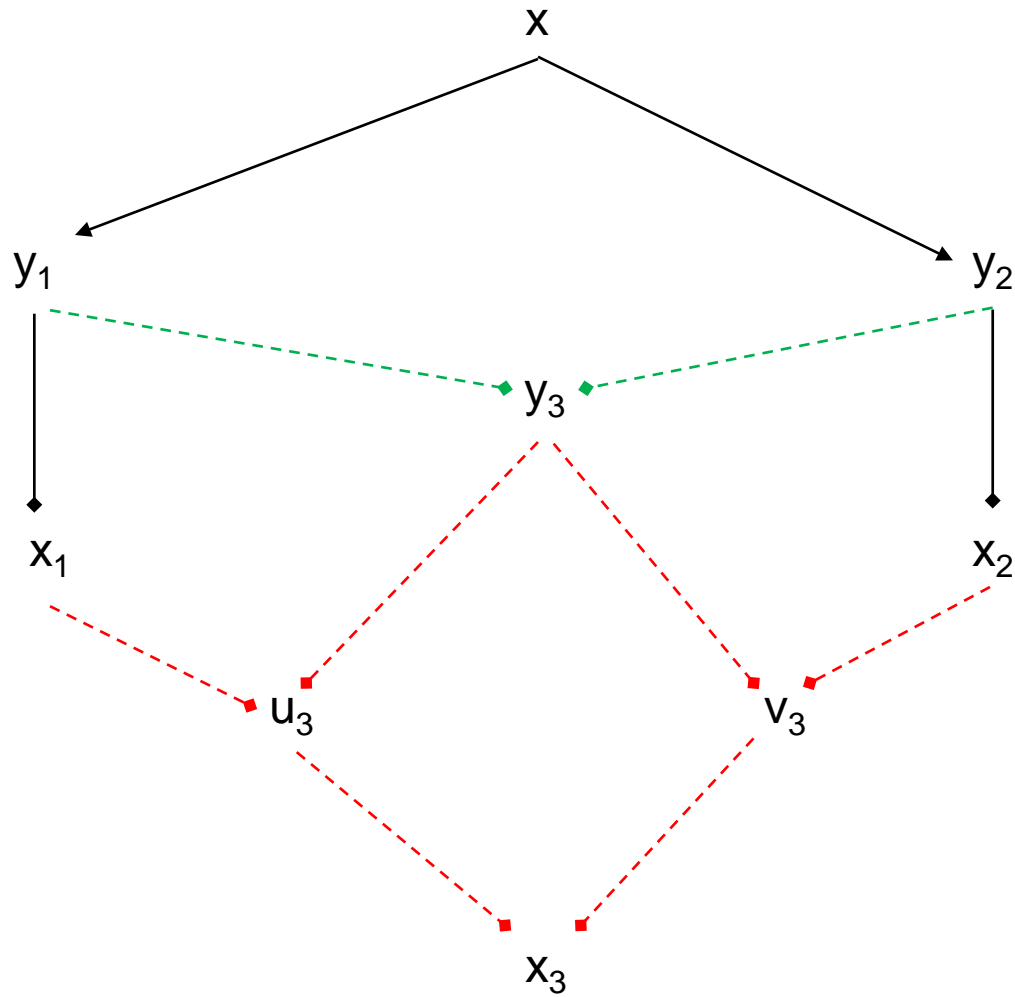
## Local confluence



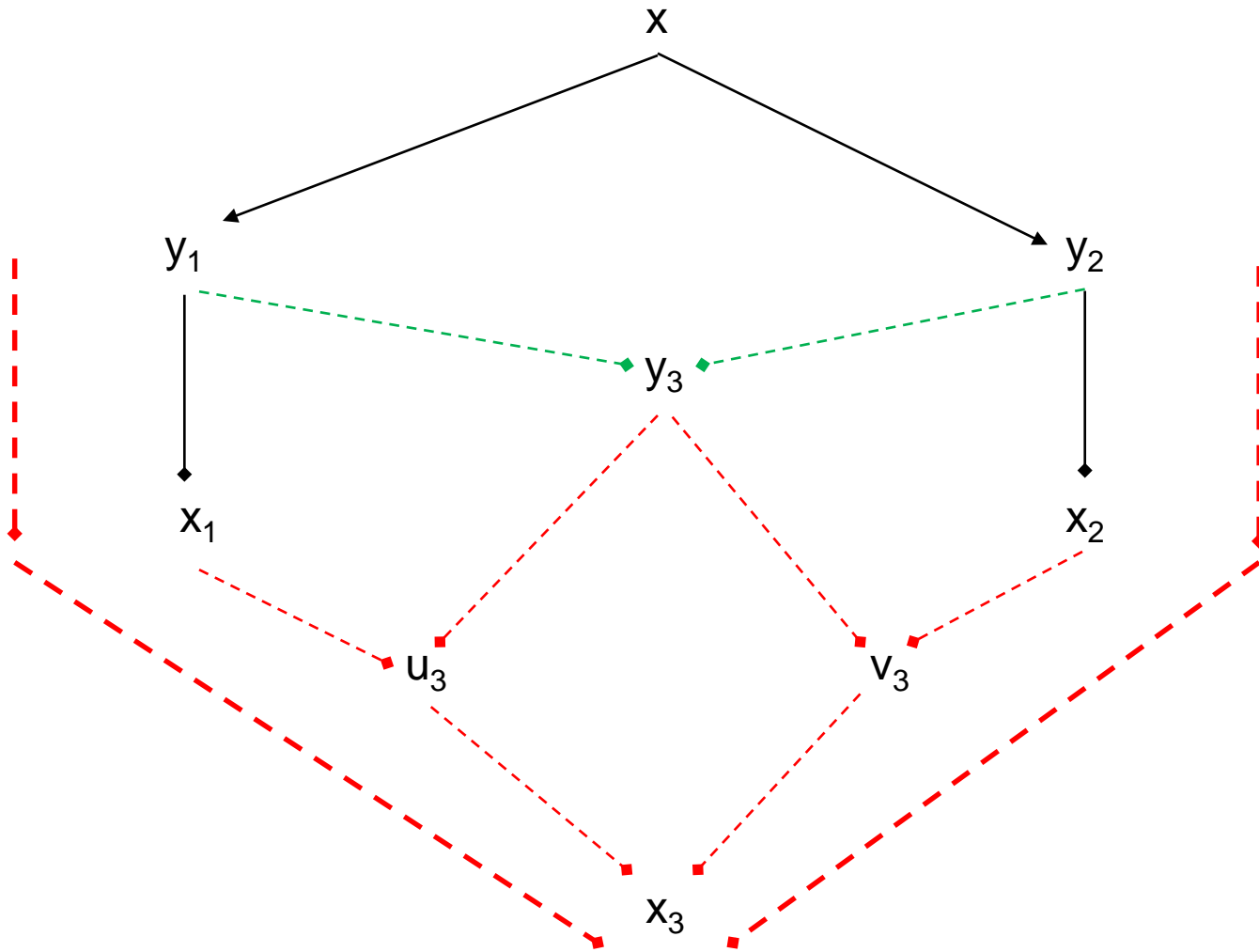
Induction hypothesis (twice)!



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

---

<sup>1</sup>Let  $R$  be a relation on  $\Lambda$ . The *transitive closure* of  $R$  is the least relation  $R^*$  satisfying:

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

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

$$\begin{array}{l} PRP' \quad \Rightarrow \quad PR^-P' \\ PR^-P \end{array}$$

# Diamond property

1.4.2. LEMMA. *Let  $>$  be a relation on  $\Lambda$  and suppose that its transitive closure<sup>1</sup> 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  $M_1 > \dots > M_n$  implies that there are  $N_2, \dots, N_n$  such that  $N_1 > N_2 > \dots > N_n$  and  $M_n > N_n$ .

Using this property, show by induction on  $m$  that if  $N_1 > \dots > N_m$  and  $N_1 >^* M_1$  then there are  $M_2, \dots, M_m$  such that  $M_1 > M_2 > \dots > M_m$  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  $M_1 > \dots > M_2$  and  $M_1 > \dots > M_3$ . By what was shown above, we can find  $M_4$  such that  $M_2 > \dots > M_4$  and  $M_3 > \dots > M_4$ . 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  $\Lambda$  defined by:

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

# 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  $M$ . □

# Parallel reduction has diamond property

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

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

# Parallel reduction and beta reduction

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

PROOF. Clearly<sup>2</sup>

$$(\twoheadrightarrow_{\beta})^{\overline{=}} \subseteq \twoheadrightarrow_l \subseteq \twoheadrightarrow_{\beta}$$

Then

$$\twoheadrightarrow_{\beta} = ((\twoheadrightarrow_{\beta})^{\overline{=}})^* \subseteq \twoheadrightarrow_l^* \subseteq (\twoheadrightarrow_{\beta})^* = \twoheadrightarrow_{\beta}$$

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  $\beta$ -normal form, then  $N_1 = N_2$ .*

1.4.10. COROLLARY. *For all  $M, N \in \Lambda$ , if there are  $\beta$ -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