

# Type Theory and Coq

Herman Geuvers

Meta-Theory of Type Theory and Church-Rosser

# Overview of today's lecture

- ▶ What do we want to prove **about** type systems?  
Meta Theory
- ▶ Church-Rosser (confluence) of reduction

# Meta theory of type systems

- ▶ Subject Reduction (or Closure, or Preservation of typing)  
If  $\Gamma \vdash M : A$  and  $M \rightarrow_{\beta} N$ , then  $\Gamma \vdash N : A$
- ▶ Church-Rosser for  $\beta$ -reduction (this lecture)  
If  $M \twoheadrightarrow_{\beta} P_1$  and  $M \twoheadrightarrow_{\beta} P_2$ , then  $\exists Q(P_1 \twoheadrightarrow_{\beta} Q \wedge P_2 \twoheadrightarrow_{\beta} Q)$ .
- ▶ Normalization (next lecture)
  - ▶ Weak Normalization, WN, a term  $M$  is WN if  $\exists P \in \text{NF}(M \twoheadrightarrow_{\beta} P)$ .  
NB. NF is the set of **normal forms**, terms that cannot be reduced.
  - ▶ Strong Normalization, SN, a term  $M$  is SN if  
 $\neg \exists (P_i)_{i \in \mathbb{N}}(M = P_0 \rightarrow_{\beta} P_1 \rightarrow_{\beta} P_2 \rightarrow_{\beta} \dots)$ .
- ▶ Progress  
If  $\vdash M : A$ , then either  $\exists P(M \rightarrow_{\beta} P)$  or  $M$  is a **value**

## Subject Reduction

LEMMA If  $\Gamma \vdash M : A$  and  $M \rightarrow_{\beta} N$ , then  $\Gamma \vdash N : A$

PROOF By induction on  $M$ . The base case is when  $M = (\lambda x:B.P)Q \rightarrow_{\beta} P[x := Q] = N$ . This is also the only interesting case. It goes roughly as follows

$$\frac{\frac{\Gamma, x:B \vdash P : C}{\Gamma \vdash \lambda x:B.P : \Pi x:B.C} \quad \Gamma \vdash Q : B}{\Gamma \vdash (\lambda x:B.P)N : C[x := Q]}$$

And we need to prove that  $\Gamma \vdash P[x := Q] : C[x := Q]$ .

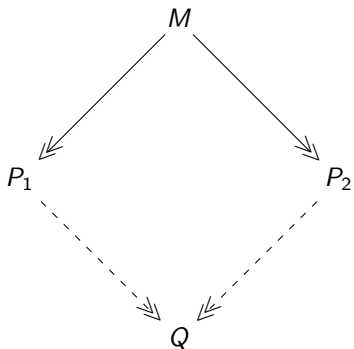
This is proved by proving a **Substitution Lemma**:

SUBSTITUTION LEMMA: If  $\Gamma, x : B, \Delta \vdash P : C$  and  $\Gamma \vdash Q : B$ , then  $\Gamma, \Delta[x := Q] \vdash P[x := Q] : C[x := Q]$ .

PROOF By induction on the derivation of  $\Gamma, x : B, \Delta \vdash P : C$ .

NB. For SR one only needs a weaker variant of the Substitution Lemma: If  $\Gamma, x : B \vdash P : C$  and  $\Gamma \vdash Q : B$ , then  $\Gamma \vdash P[x := Q] : C[x := Q]$ . However, this cannot be proved directly by induction.

## Church-Rosser property, CR



CHURCH-ROSSER THEOREM for  $\beta$ -reduction,  $CR_\beta$ .

If  $M \twoheadrightarrow_\beta P_1$  and  $M \twoheadrightarrow_\beta P_2$ , then  $\exists Q (P_1 \twoheadrightarrow_\beta Q \wedge P_2 \twoheadrightarrow_\beta Q)$

NB.  $M \twoheadrightarrow P$  denotes the reflexive transitive closure of  $M \rightarrow P$ , that is:  
 $M \twoheadrightarrow P$  iff there is a multi-step (0 or more) reduction from  $M$  to  $P$ .

We will prove the Church-Rosser Theorem for  $\beta$ -reduction in this lecture.

## Church-Rosser (for $\beta$ ) example

$$(\lambda x. y x x)(\mathbf{II})$$

## General setting: Rewriting systems

DEFINITION A rewriting system is a pair  $(A, \rightarrow_R)$ , with  $A$  a set and  $\rightarrow_R \subseteq A \times A$  a relation on  $A$ .

Some notation:

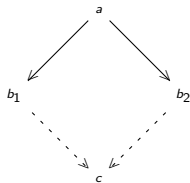
- ▶  $a \rightarrow_R a'$  if  $(a, a') \in \rightarrow_R$ .
- ▶  $\twoheadrightarrow_R$  denotes the reflexive transitive closure of  $\rightarrow_R$ . (Multistep rewriting; 0 or more steps of  $\rightarrow_R$ )
- ▶  $=_R$  denotes the symmetric transitive closure of  $\twoheadrightarrow_R$ . (Smallest equivalence relation containing  $\twoheadrightarrow_R$ .)  
This is similar to  $\beta$ -reduction in  $\lambda$ -calculus, where we have  $\rightarrow_\beta$ ,  $\twoheadrightarrow_\beta$  and  $=_\beta$ .
- ▶  $a \in A$  is in  $\rightarrow_R$ -normal form if  $\neg \exists b \in A (a \rightarrow_R b)$ .

## How can one prove the Church-Rosser property? (I)

DEFINITION The rewriting system  $(A, \rightarrow_R)$  satisfies the **Diamond Property**, DP, if

$$\forall a, b_1, b_2 \in A (a \rightarrow_R b_1 \wedge a \rightarrow_R b_2 \implies \exists c \in A (b_1 \rightarrow_R c \wedge b_2 \rightarrow_R c)).$$

In a diagram:



Note:  $CR(\rightarrow_R) := DP(\rightarrow_R)$

LEMMA  $DP(\rightarrow_R)$  implies  $CR(\rightarrow_R)$

PROOF

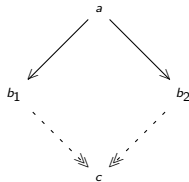


## How can one prove the Church-Rosser property? (II)

DEFINITION The rewriting system  $(A, \rightarrow_R)$  satisfies the **Weak Church-Rosser Property**, WCR, if

$$\forall a, b_1, b_2 \in A (a \rightarrow_R b_1 \wedge a \rightarrow_R b_2 \implies \exists c \in A (b_1 \twoheadrightarrow_R c \wedge b_2 \twoheadrightarrow_R c)).$$

In a diagram:



Note!:  $\text{WCR}(\rightarrow_R)$  does not imply  $\text{CR}(\rightarrow_R)$

But we do have

NEWMAN'S LEMMA  $\text{WCR}(\rightarrow_R) + \text{SN}(\rightarrow_R)$  implies  $\text{CR}(\rightarrow_R)$

But for type theory, we need first  $\text{CR}(\rightarrow_\beta)$ , which will be used in the meta theory and in the proof of  $\text{SN}(\rightarrow_\beta)$ .

## Intermezzo: proof of Newman's Lemma

NEWMAN'S LEMMA  $WCR + SN$  implies  $CR$

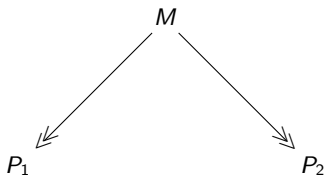
PROOF Constructive proof. By induction on  $M \in SN$ , we prove that  $M$  is  $CR$ .

$$\frac{M \in NF}{M \in SN} \text{ (base)}$$

$$\frac{\forall P, (\text{if } M \rightarrow_R P \text{ then } P \in SN)}{M \in SN} \text{ (step)}$$

## Corollaries of the Church-Rosser property

THEOREM  $\text{CR}(\rightarrow_R)$  implies  $\text{UN}(\rightarrow_R)$  (Uniqueness of Normal forms)



If  $P_1$  and  $P_2$  are in normal form, then  $P_1 = P_2$ , due to CR.

THEOREM  $\text{CR}(\rightarrow_R) + \text{SN}(\rightarrow_R)$  implies  $=_R$  is decidable.

PROOF: To decide  $a =_R b$ , just rewrite  $a$  and  $b$  until you find their normal forms  $a'$  and  $b'$ . Due to UN (which follows from CR), we have  $a =_R b$  iff  $a' = b'$ .

NB. Decidability of  $=_\beta$  is crucial for decidability of type checking!  
Remember the conversion rule:

$$\frac{\Gamma \vdash M : A \quad \Gamma \vdash B : s}{\Gamma \vdash M : B} A =_\beta B$$

# We prove $CR(\beta)$ for untyped $\lambda$ -calculus

Untyped  $\lambda$ -calculus

$$M, N ::= x \mid M N \mid \lambda x.M$$

Reduction:

$$\frac{}{(\lambda x.M)P \rightarrow_{\beta} M[x := P]} (\beta) \qquad \frac{M \rightarrow_{\beta} M'}{M P \rightarrow_{\beta} M' P} (\text{app-l})$$

$$\frac{M \rightarrow_{\beta} M'}{\lambda x.M \rightarrow_{\beta} \lambda x.M'} (\lambda) \qquad \frac{M \rightarrow_{\beta} M'}{P M \rightarrow_{\beta} P M'} (\text{app-r})$$

NB.  $DP(\beta)$  fails due to redex erasure or redex duplication:

$$(\lambda x.y)(\mathbf{II})$$

$$(\lambda x.y \ x \ x)(\mathbf{II})$$

## Parallel reduction in untyped $\lambda$ -calculus

We prove  $\text{CR}(\beta)$  using **parallel reduction**, a method due to Tait and Martin-Löf and refined by Takahashi.

Parallel reduction  $M \Longrightarrow P$  allows to contract several redexes in  $M$  in one step. It can be defined inductively.

DEFINITION

$$\frac{M \Longrightarrow M' \quad P \Longrightarrow P'}{(\lambda x.M)P \Longrightarrow M'[x := P']} (\beta)$$

$$\frac{M \Longrightarrow M' \quad P \Longrightarrow P'}{MP \Longrightarrow M'P'} (\text{app})$$

$$\frac{M \Longrightarrow M'}{\lambda x.M \Longrightarrow \lambda x.M'} (\lambda)$$

$$\frac{}{x \Longrightarrow x} (\text{var})$$

Examples:

$$(\lambda x.y)(\mathbf{II})$$

$$(\lambda x.y \ x \ x)(\mathbf{II})$$

## Properties of parallel reduction

$$\frac{M \Longrightarrow M' \quad P \Longrightarrow P'}{(\lambda x.M)P \Longrightarrow M'[x := P']} (\beta)$$

$$\frac{M \Longrightarrow M' \quad P \Longrightarrow P'}{MP \Longrightarrow M'P'} (\text{app})$$

$$\frac{M \Longrightarrow M'}{\lambda x.M \Longrightarrow \lambda x.M'} (\lambda)$$

$$\frac{}{x \Longrightarrow x} (\text{var})$$

### THEOREM

1.  $M \Longrightarrow M$
2. If  $M \rightarrow_{\beta} P$ , then  $M \Longrightarrow P$
3. If  $M \Longrightarrow P$ , then  $M \rightarrow_{\beta} P$ .

PROOF The proof of (1) is by induction on  $M$ . The proofs of (2) and (3) are by induction on the derivation, where the proof of (2) uses (1).

# Parallel reduction satisfies a strong Diamond Property (I)

THEOREM

$$\forall M \exists Q \forall P (\text{if } M \Longrightarrow P \text{ then } P \Longrightarrow Q).$$

This immediately implies  $\text{DP}(\Longrightarrow)$ .

We can even define this  $Q$  inductively from  $M$ ; it will be called  $M^*$ .

So we have

$$\forall M, P (\text{if } M \Longrightarrow P \text{ then } P \Longrightarrow M^*).$$

Note: This implies  $\forall M (M \Longrightarrow M^*)$ .

DEFINITION

$$\begin{aligned} x^* &:= x \\ (\lambda x.M)^* &:= \lambda x.M^* \\ (MN)^* &:= P^*[x := N^*] \text{ if } M = \lambda x.P \\ &:= M^* N^* \text{ otherwise.} \end{aligned}$$

## Parallel reduction satisfies a strong Diamond Property (II)

THEOREM

$$\forall M, P \text{ (if } M \Longrightarrow P \text{ then } P \Longrightarrow M^* \text{)}.$$

PROOF by induction on the derivation of  $M \Longrightarrow P$ . There are 4 cases.

case (1)

$$\frac{}{x \Longrightarrow x} \text{ (var)}$$

Then indeed  $x \Longrightarrow x^*$  (because  $x^* = x$ ).

case (2)

$$\frac{M \Longrightarrow M'}{\lambda x.M \Longrightarrow \lambda x.M'} (\lambda)$$

IH:  $M' \Longrightarrow M^*$

We need to prove:  $\lambda x.M' \Longrightarrow (\lambda x.M)^*$  and we know  $(\lambda x.M)^* = \lambda x.M^*$ .

This follows immediately from IH and the definition of  $\Longrightarrow$ .



# Parallel reduction satisfies a strong Diamond Property (III)

THEOREM

$$\forall M, P \text{ (if } M \Longrightarrow P \text{ then } P \Longrightarrow M^*).$$

PROOF continued

case (3)

$$\frac{M \Longrightarrow M' \quad P \Longrightarrow P'}{M P \Longrightarrow M' P'} \text{ (app)}$$

IH:  $M' \Longrightarrow M^*$  and  $P' \Longrightarrow P^*$ . To prove:  $M' P' \Longrightarrow (M P)^*$ .

- ▶ case  $M = \lambda x.Q$ . Then  $M' = \lambda x.Q'$  with  $Q \Longrightarrow Q'$  and we have a further IH:  $Q' \Longrightarrow Q^*$ .

Furthermore,  $(M P)^* = ((\lambda x.Q) P)^* = Q^*[x := P^*]$ . Then indeed, by the rules for  $\Longrightarrow$ :

$$\frac{Q' \Longrightarrow Q^* \quad P' \Longrightarrow P^*}{(\lambda x.Q')P' \Longrightarrow Q^*[x := P^*]} (\beta)$$

- ▶ case  $M \neq \lambda x.\dots$ . Now  $(M P)^* = M^* P^*$ , and we have  $M' P' \Longrightarrow M^* P^*$  by the rules for  $\Longrightarrow$ , so we are done.

# Parallel reduction satisfies a strong Diamond Property (IV)

THEOREM

$$\forall M, P \text{ (if } M \Longrightarrow P \text{ then } P \Longrightarrow M^* \text{)}.$$

PROOF continued

case (4)

$$\frac{M \Longrightarrow M' \quad P \Longrightarrow P'}{(\lambda x.M) P \Longrightarrow M'[x := P']}$$

IH:  $M' \Longrightarrow M^*$  and  $P' \Longrightarrow P^*$ .

We need to prove:  $M'[x := P'] \Longrightarrow ((\lambda x.M) P)^* = M^*[x := P^*]$ .

To prove this we need a separate

SUBSTITUTION LEMMA If  $M \Longrightarrow M'$  and  $P \Longrightarrow P'$ , then  $M[x := P] \Longrightarrow M'[x := P']$ .

This is proved by induction on the structure of  $M$ .

Yet another example

$$(\lambda z.z z) (\mathbf{I} (\mathbf{I} x))$$

## The same example again

$$\begin{aligned}x^* &:= x \\(\lambda x.M)^* &:= \lambda x.M^* \\(M N)^* &:= P^*[x := N^*] \text{ if } M = \lambda x.P \\ &:= M^* N^* \text{ otherwise.}\end{aligned}$$

$$(\lambda z.z z) (\mathbf{I} (\mathbf{I} x))$$

# This is a flexible proof of Church-Rosser

- ▶ Methods works for proving CR for reduction in Combinatory Logic
- ▶ Methods works for proving CR for  $\beta$  on pseudo-terms of Pure Type Systems
- ▶ Method extends to typed lambda calculus with data types, for example natural numbers:

$$M, N := x \mid M N \mid \lambda x.M \mid 0 \mid \mathbf{succ} M \mid \mathbf{nrec} M N P$$

with

$$\begin{aligned} \mathbf{nrec} M N 0 &\rightarrow M \\ \mathbf{nrec} M N (\mathbf{succ} P) &\rightarrow N P (\mathbf{nrec} M N P) \end{aligned}$$

- ▶ Method extends to  $\eta$ -reduction:

$$\lambda x.M x \rightarrow_{\eta} M \quad \text{if } x \notin \text{FV}(M)$$