Type Theory and Coq

Herman Geuvers

Meta-Theory of Type Theory and Church-Rosser

Overview of todays 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 $M \to_\beta N$, then $\Gamma \vdash N : A$
- Church-Rosser for β-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 $\exists P \in \mathrm{NF}(M \twoheadrightarrow_\beta P)$.
    NB. NF is the set of normal forms, terms that cannot be reduced.
  - Strong Normalization, SN, a term M is SN if
    $\neg\exists(P_i)_{i\in\mathbb{N}}(M = P_0 \to_\beta P_1 \to_\beta P_2 \to_\beta \ldots)$.
- Progress
  If $\vdash M : A$, then either $\exists P(M \to_\beta P)$ or M is a value

Subject Reduction

LEMMA If $\Gamma \vdash M : A$ and $M \to_\beta N$, then $\Gamma \vdash N : A$

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

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

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 $\Gamma \vdash P[x := N] : C[x := N]$.
However, this cannot be proved directly by induction.

Church-Rosser property, CR

$$\begin{tikzcd}
& M \arrow[dl, two heads] \arrow[dr, two heads] & \\
P_1 \arrow[dr, dashed, two heads] & & P_2 \arrow[dl, dashed, two heads] \\
& Q &
\end{tikzcd}$$

Church-Rosser Theorem for β-reduction, CR_β.
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 $M \to P$, 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 β-reduction in this lecture.

Church-Rosser (for β) example

$$(\lambda x.y\,x\,x)(\mathbf{I}\,\mathbf{I})$$

General setting: Rewriting systems

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

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

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

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

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

In a diagram:

$$\begin{tikzcd}
& a \arrow[dl] \arrow[dr] & \\
b_1 \arrow[dr, dashed] & & b_2 \arrow[dl, dashed] \\
& c &
\end{tikzcd}$$

Note: $\mathrm{CR}(\to_R) := \mathrm{DP}(\twoheadrightarrow_R)$

LEMMA $\mathrm{DP}(\to_R)$ implies $\mathrm{CR}(\to_R)$

PROOF

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

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

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

In a diagram:

$$\begin{tikzcd}
& a \arrow[dl] \arrow[dr] & \\
b_1 \arrow[dr, dashed, two heads] & & b_2 \arrow[dl, dashed, two heads] \\
& c &
\end{tikzcd}$$

Note!: WCR($\to_R$) does not imply CR($\to_R$)

But we do have
NEWMAN'S LEMMA WCR($\to_R$) + SN($\to_R$) implies CR($\to_R$)

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

Intermezzo: proof of Newman's Lemma

NEWMAN'S LEMMA WCR + SN implies CR

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

$$\frac{M \in \mathsf{NF}}{M \in \mathsf{SN}}\,(\text{base}) \qquad\qquad \frac{\forall P, (\text{if } M \to_R P \text{ then } P \in \mathsf{SN})}{M \in \mathsf{SN}}\,(\text{step})$$

Corollaries of the Church-Rosser property

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

$$\begin{tikzcd} & M \arrow[dl, two heads] \arrow[dr, two heads] & \\ P_1 & & P_2 \end{tikzcd}$$

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

THEOREM $\mathsf{CR}(\rightarrow_R) + \mathsf{SN}(\rightarrow_R)$ 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 form CR), we have $a =_R b$ iff $a' = b'$.

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

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

We prove CR(β) for untyped λ-calculus

Untyped λ-calculus

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

Reduction:

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

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

NB. DP(β) fails due to redex erasure or redex duplication:

$$(\lambda x.y)(\mathbf{I}\,\mathbf{I}) \qquad\qquad (\lambda x.y\,x\,x)(\mathbf{I}\,\mathbf{I})$$

Parallel reduction in untyped λ-calculus

We prove CR(β) 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

$$\frac{M \Longrightarrow M' \qquad P \Longrightarrow P'}{(\lambda x.M)P \Longrightarrow M'[x := P']}\,(\beta) \qquad \frac{M \Longrightarrow M' \qquad P \Longrightarrow P'}{M\,P \Longrightarrow M'\,P'}\,(\mathsf{app})$$

$$\frac{M \Longrightarrow M'}{\lambda x.M \Longrightarrow \lambda x.M'}\,(\lambda) \qquad \frac{}{x \Longrightarrow x}\,(\mathsf{var})$$

Examples:

$$(\lambda x.y)(\mathbf{I}\,\mathbf{I}) \qquad (\lambda x.y\,x\,x)(\mathbf{I}\,\mathbf{I})$$

Properties of parallel reduction

$$\frac{M \Longrightarrow M' \qquad P \Longrightarrow P'}{(\lambda x.M)P \Longrightarrow M'[x := P']}\,(\beta) \qquad\qquad \frac{M \Longrightarrow M' \qquad P \Longrightarrow P'}{M\,P \Longrightarrow M'\,P'}\,(\mathsf{app})$$

$$\frac{M \Longrightarrow M'}{\lambda x.M \Longrightarrow \lambda x.M'}\,(\lambda) \qquad\qquad \frac{}{x \Longrightarrow x}\,(\mathsf{var})$$

Theorem

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

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 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

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

Parallel reduction satisfies a strong Diamond Property (II)

Theorem

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

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)

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

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 $\Longrightarrow$:

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

- case $M \neq \lambda x. \ldots$. 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

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

PROOF continued

case (4)

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

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

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

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

This is a flexible proof of Church-Rosser

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

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

with

$$\begin{array}{rcl} \mathbf{nrec}\,M\,N\,0 & \to & M \\ \mathbf{nrec}\,M\,N\,(\mathbf{suc}\,P) & \to & N\,P\,(\mathbf{nrec}\,M\,N\,P) \end{array}$$

- Method extends to η-reduction:

$$\lambda x.M\,x \to_\eta M \qquad \text{if } x \notin \mathrm{FV}(M)$$