

Foundations of Proof Systems

PRFSYS

Benjamin Werner — Dominik Kirst

LIX, Ecole polytechnique

Team Partout, Inria Saclay

Oct. 2nd 2026

A λ -term *realizes* a proposition $t \Vdash_{\mathcal{I}} A$ (interpretation of variables $\mathcal{I}(x) \in \mathbb{N}$)

Here we take for t the language of system T with prods and sums, but not necessarily typed (other choices are possible).

$$t \Vdash_{\mathcal{I}} A \wedge B \iff t \triangleright_{\beta^*} (a, b), \quad a \Vdash_{\mathcal{I}} A \quad \text{and} \quad b \Vdash_{\mathcal{I}} B$$

$$t \Vdash_{\mathcal{I}} A \vee B \iff (t \triangleright_{\beta^*} i(a) \wedge a \Vdash_{\mathcal{I}} A) \quad \text{or} \quad (t \triangleright_{\beta^*} j(b) \wedge b \Vdash_{\mathcal{I}} B)$$

$$t \Vdash_{\mathcal{I}} A \Rightarrow B \iff \forall u \Vdash_{\mathcal{I}} A, \quad (t \, u) \Vdash_{\mathcal{I}} B$$

$$t \Vdash_{\mathcal{I}} n = m \iff t \triangleright_{\beta^*} () \quad \text{and} \quad n_{\mathcal{I}} =_{\mathbb{R}} m_{\mathcal{I}}$$

$$t \Vdash_{\mathcal{I}} \perp$$

never true

(no realizer of $2=3$)

$$t \Vdash_{\mathcal{I}} \forall x. A \iff \forall n, \quad (t \, n) \Vdash_{\mathcal{I}} A[x \setminus n]$$

$$t \Vdash_{\mathcal{I}} \exists x. A \iff t \triangleright_{\beta^*} (n, u) \quad \text{and} \quad u \Vdash_{\mathcal{I}} A[x \setminus n]$$

Remarks

$$t \Vdash_{\mathcal{I}} A \wedge B \iff t \triangleright_{\beta}^* (a, b), \quad a \Vdash_{\mathcal{I}} A \quad \text{and} \quad b \Vdash_{\mathcal{I}} B$$

$$t \Vdash_{\mathcal{I}} A \vee B \iff (t \triangleright_{\beta}^* i(a) \wedge a \Vdash_{\mathcal{I}} A) \quad \text{or} \quad (t \triangleright_{\beta}^* j(b) \wedge b \Vdash_{\mathcal{I}} B)$$

$$t \Vdash_{\mathcal{I}} A \Rightarrow B \iff \forall u \Vdash_{\mathcal{I}} A, \quad (t \ u) \Vdash_{\mathcal{I}} B$$

$$t \Vdash_{\mathcal{I}} n = m \iff t \triangleright_{\beta}^* () \quad \text{and} \quad n_{\mathcal{I}} =_R m_{\mathcal{I}}$$

$$t \Vdash_{\mathcal{I}} \perp \quad \text{never true}$$

$$t \Vdash_{\mathcal{I}} \forall x. A \iff \forall n, \quad (t \ n) \Vdash_{\mathcal{I}} A[x \setminus n]$$

$$t \Vdash_{\mathcal{I}} \exists x. A \iff t \triangleright_{\beta}^* (n, u) \quad \text{and} \quad u \Vdash_{\mathcal{I}} A[x \setminus n]$$

(1) if $t \Vdash_{\mathcal{I}} A$ and $t \triangleright_{\beta} t'$, then $t' \Vdash_{\mathcal{I}} A$. Actually if $t =_{\beta} t'$, then $t' \Vdash_{\mathcal{I}} A$

(2) $t[x \setminus n] \Vdash_{\mathcal{I}} A[x \setminus n]$ iff $t' \Vdash_{\mathcal{I}; x \leftarrow n} A$.

Provability entails realizability

Main idea: If $\vdash A$, then there exists t , s.t. $t \Vdash A$

► generalize for assumptions:

if $A_1; \dots; A_n \vdash A$, there exists t , s.t. for all $\mathcal{I}$,

if $t_1 \Vdash_{\mathcal{I}} A_1, \dots, t_n \Vdash_{\mathcal{I}} A_n$, then $t[x_1 \backslash t_1 \dots x_n \backslash t_n] \Vdash_{\mathcal{I}} A$

► Which term t ?

Here we can take the term we associated to the derivation of $A_1; \dots; A_n \vdash A$.

$$\frac{\sigma}{A_1; \dots; A_n \vdash A}$$

We wrote it $\|\sigma\|$. I will call it t in the next slides

- ▶ Axiom if $t_i \Vdash_{\mathcal{I}} A_i$, then $x_i[x_i \setminus t_i] \Vdash_{\mathcal{I}} A_i$
- ▶ $\wedge$ -I if $u[\sigma] \Vdash_{\mathcal{I}} A$ and $v[\sigma] \Vdash_{\mathcal{I}} B$, then $(u, v)[\sigma] \Vdash_{\mathcal{I}} A \wedge B$
- ▶ $\wedge$ -E, $\Rightarrow$ -E, $\vee$ -I... similar, easy
- ▶ $\Rightarrow$ -I $\forall u \Vdash_{\mathcal{I}} A, t[\sigma; x \setminus u] \Vdash_{\mathcal{I}} B.$

Take $u \Vdash_{\mathcal{I}} A$. show that $((\lambda x.t)[\sigma] u) \Vdash_{\mathcal{I}} B$

we have $(\lambda x.t)[\sigma] u \triangleright_{\beta} t[\sigma; x \setminus u]$

- ▶ $\vee$ -E
- $$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \text{ } \vee\text{-E}$$
- $t[\sigma] \triangleright_{\beta}^* i(t_A) \text{ or } j(t_B)$
- $u[\sigma; x^A \leftarrow t_A] \Vdash_{\mathcal{I}} C$
- $v[\sigma; y^B \leftarrow t_B] \Vdash_{\mathcal{I}} C$
- $\delta(t, x^A.u, y^B.v)[\sigma] \triangleright_{\beta}^* u[\sigma; x^A \leftarrow t_A] \text{ or } v[\sigma; y^B \leftarrow t_B]$
- so $\delta(t, x^A.u, y^B.v)[\sigma] \Vdash_{\mathcal{I}} C$

Proof (2)

$$t \Vdash_{\mathcal{I}} \forall x. A \quad \Leftrightarrow$$

$$\forall n, (t \ n) \mathcal{R} A[x \setminus n]$$

$$t \Vdash_{\mathcal{I}} \exists x. A \quad \Leftrightarrow$$

$$t \triangleright_{\beta}^* (n, u) \text{ and } u \mathcal{R} A[x \setminus n]$$

$$t \Vdash_{\mathcal{I}} \perp$$

never true

$\perp$ -E : $t [x^{A_1} \setminus t_1 \dots x^{A_n} \setminus t_n] \Vdash_{\mathcal{I}} \Gamma \vdash \perp$ means there is no $(t_1, \dots, t_n)$

$\forall$ -I : we have $t \Vdash_{\mathcal{I}} A$ so for all n , $t[x \setminus n] \Vdash_{\mathcal{I}} A[x \setminus n]$

and $(\lambda x. t \ n) \Vdash_{\mathcal{I}} A[x \setminus n]$

$\exists$ -I : unfold definitions

What can one talk about in Arithmetic ?

Define $F(x,y,z)$ such that:

$$F(x,0,z) \Leftrightarrow z = 1$$

$$F(x,y,z) \Leftrightarrow F(x, S(y), x \times z)$$

We can prove: $\forall x. \forall y. \exists z. F(x,y,z)$

The term realizing the proof will « compute » x^y

but it is not practical:

- to talk about x^y
- we cannot use the computation in the proofs (like for $2+2=4$)

Proofs as Objects of the Formalism or Dependent Types

Time to switch to contexts for typing

$$\begin{array}{c}
 \frac{}{\Gamma \vdash x : A} \text{ if } (x:A) \in \Gamma \qquad \frac{\Gamma (x : A) \vdash t : B}{\Gamma \vdash \lambda x:A. t : A \rightarrow B} \qquad \frac{\Gamma \vdash t : A \rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash t u : B} \\
 \\
 \frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash (t,u) : A \times B} \qquad \frac{\Gamma \vdash t : A}{\Gamma \vdash i_B(t) : A + B} \qquad \frac{\Gamma \vdash u : B}{\Gamma \vdash j_A(t) : A + B} \\
 \\
 \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_1(t) : A} \qquad \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_2(t) : B} \qquad \frac{\Gamma \vdash t : A + B \quad \Gamma(x:A) \vdash u:C \quad \Gamma(y:B) \vdash v:C}{\Gamma \vdash \delta(t, x.u, y.v) : C}
 \end{array}$$

Annotations to keep type uniqueness / type inference

Given Γ and t , one can decide whether there exists T s.t. $\Gamma \vdash t:T$

A (canonical)
proof of...

... is:

- ▶ $A \wedge B$ (a, b) where a is a proof of A , b a proof of B
- ▶ $A \vee B$ (ε, c) with $\varepsilon=0$ and c proof of A or $\varepsilon=1$ and c proof of B
- ▶ $A \Rightarrow B$ f , with $f(a)$ proof of B for any proof a of A
- ▶ $\forall x . A$ f , with $f(t) : A[x \backslash t]$ for any object t
- ▶ $\exists x . A$ (t, a) with a a proof of $A[x \backslash t]$

Realizability

$t \Vdash_{\mathcal{I}} A \wedge B$	$\Leftrightarrow$	$t \triangleright_{\beta}^* (a, b), a \Vdash_{\mathcal{I}} A \text{ and } b \Vdash_{\mathcal{I}} B$
$t \Vdash_{\mathcal{I}} A \vee B$	$\Leftrightarrow$	$(t \triangleright_{\beta}^* i(a) \wedge a \Vdash_{\mathcal{I}} A) \text{ or } (t \triangleright_{\beta}^* j(b) \wedge b \Vdash_{\mathcal{I}} B)$
$t \Vdash_{\mathcal{I}} A \Rightarrow B$	$\Leftrightarrow$	$\forall u \Vdash_{\mathcal{I}} A, (t \ u) \Vdash_{\mathcal{I}} B$
$t \Vdash_{\mathcal{I}} n = m$	$\Leftrightarrow$	$t \triangleright_{\beta}^* () \text{ and } n_{\mathcal{I}} =_R m_{\mathcal{I}}$
$t \Vdash_{\mathcal{I}} \perp$		never true
$t \Vdash_{\mathcal{I}} \forall x. A$	$\Leftrightarrow$	$\forall n, (t \ n) \Vdash_{\mathcal{I}} A[x \setminus n]$
$t \Vdash_{\mathcal{I}} \exists x. A$	$\Leftrightarrow$	$t \triangleright_{\beta}^* (n, u) \text{ and } u \Vdash_{\mathcal{I}} A[x \setminus n]$

A (canonical)
proof of...

... is:

- ▶ $A \wedge B$ (a, b) where $a : A$, $b : B$
- ▶ $A \vee B$ (ε, c) with $\varepsilon=0$ and $c : A$ or $\varepsilon=1$ and $c : B$
- ▶ $A \Rightarrow B$ f , with $f(a) : B$ for any $a : A$
- ▶ $\forall x . A$ f , with $f(t) : A[x \backslash t]$ for any object t
- ▶ $\exists x . A$ (t, a) with $a : A[x \backslash t]$

Implicational Fragment

$$\frac{}{\Gamma \vdash x : A} \text{ if } (x:A) \in \Gamma$$

$$\frac{\Gamma (x : A) \vdash t : B}{\Gamma \vdash \lambda x:A. t : A \rightarrow B}$$

$$\frac{\Gamma \vdash t : A \rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash t u : B}$$

$$\text{Axiom } \frac{}{\Gamma \vdash x : A} \text{ if } (x:A) \in \Gamma$$

$$\Rightarrow -i \quad \frac{\Gamma (x : A) \vdash t : B}{\Gamma \vdash \lambda x:A. t : A \Rightarrow B}$$

$$\Rightarrow -e \quad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash t u : B}$$

$$\begin{array}{c} [] \text{ wf} \quad \frac{\Gamma \vdash T : s}{\Gamma (x:T) \text{ wf}} \quad \frac{\Gamma \text{ wf}}{\Gamma \vdash x : T} \text{if } (x:T) \in \Gamma \quad \frac{\Gamma \text{ wf}}{\Gamma \vdash \text{Type} : \text{Kind}}\end{array}$$

$$\frac{\Gamma \vdash A : \text{Type} \quad \Gamma (x:A) \vdash B : s}{\Gamma \vdash \Pi x : A . B : s} \quad \frac{\Gamma \vdash t : A \quad \Gamma \vdash B : s}{\Gamma \vdash t : B} A =_{\beta} B$$

$$\frac{\Gamma \vdash \Pi x : A . B : \text{Type} \quad \Gamma(x:A) \vdash t : B}{\Gamma \vdash \lambda x : A . t : \Pi x : A . B} \quad \frac{\Gamma \vdash t : \Pi x : A . B \quad \Gamma \vdash u : A}{\Gamma \vdash (t \ u) : B [x \setminus u]}$$

No unicity of typing ! (modulo only beta-conversion)

$$1. \Gamma \Delta \text{ wf} \Rightarrow \Gamma \text{ wf} \quad \text{and} \quad \Gamma \vdash t:T \Rightarrow \Gamma \Delta \vdash t:T$$

$$2. \Gamma(x:T)\Delta \vdash u:U \wedge \Gamma \vdash t:T \Rightarrow \Gamma \Delta[x \backslash t] \vdash u[x \backslash t] : U[x \backslash t]$$
$$\text{and} \quad \Gamma(x:T)\Delta \text{ wf} \wedge \Gamma \vdash t:T \Rightarrow \Gamma \Delta[x \backslash t] \text{ wf}$$

3. Inversion lemma :

- ▶ If $\Gamma \vdash x : T$ then $(x:T') \in \Gamma$, $T =_{\beta} T'$ and $\Gamma \vdash T' : s$
- ▶ If $\Gamma \vdash \lambda x:A.t : B$ then $B =_{\beta} \Pi x:A.C$ and $\Gamma(x:A) \vdash t : C$
- ▶ If $\Gamma \vdash (t \ u) : C$ then $\Gamma \vdash t : \Pi x:A.B$, $\Gamma \vdash u : A$ and $C =_{\beta} B[x \backslash u]$
- ▶ If $\Gamma \vdash \Pi x:A.B : T$ then $\Gamma \vdash A : \text{Type}$, $\Gamma(x:A) \vdash B : s$ and $T =_s$

If $\Gamma \vdash t : T$ and $\Gamma \vdash t : U$ then $T =_{\beta} U$

Adding disjoint sum types

$$t ::= x \mid \lambda x : t . t \mid (t \ t) \mid \Pi x : t . t \mid t + t \mid \underset{t}{i}(t) \mid \underset{t}{j}(t) \mid \delta(t, t, t)$$

$$\frac{\Gamma \vdash A : \text{Type} \quad \Gamma \vdash B : \text{Type}}{\Gamma \vdash A+B : \text{Type}}$$

$$\frac{\Gamma \vdash A+B : \text{Type} \quad \Gamma \vdash t : A}{\Gamma \vdash \underset{B}{i}(t) : A+B}$$

$$\frac{\Gamma \vdash A+B : \text{Type} \quad \Gamma \vdash t : B}{\Gamma \vdash \underset{A}{j}(t) : A+B}$$

$$\frac{\Gamma \vdash t : A+B \quad \Gamma \vdash C : \text{Type} \quad \Gamma \vdash u : A \rightarrow C \quad \Gamma \vdash v : B \rightarrow C}{\Gamma \vdash \delta(t, u, v) : C}$$

for decidability of type checking / inference

Adding Sigma types

$$t ::= x \mid \lambda x : t . t \mid (t \ t) \mid \Pi x : t . t \mid t + t \mid i(t) \mid j(t) \mid \delta(t, t, t) \\ \mid \Sigma x : t . t \mid \underbrace{(t, t)}_{\Sigma x : t . t} \mid \pi_1(t) \mid \pi_2(t)$$

$$\frac{\Gamma \vdash A : \text{Type} \quad \Gamma(x:A) \vdash B : \text{Type}}{\Gamma \vdash \Sigma x : A . B : \text{Type}}$$

$\Sigma x : A . B$ written $A \times B$
when $x \notin FV(B)$

$$\frac{\Gamma \vdash \Sigma x : A . B : \text{Type} \quad \Gamma \vdash t : A \quad \Gamma \vdash u : B[x \setminus t]}{\Gamma \vdash \underbrace{(t, u)}_{\Sigma x : A . B} : \Sigma x : A . B}$$

$$\frac{\Gamma \vdash t : \Sigma x : A . B}{\Gamma \vdash \pi_1(t) : A} \qquad \frac{\Gamma \vdash t : \Sigma x : A . B}{\Gamma \vdash \pi_2(t) : B[x \setminus \pi_1(t)]}$$

for decidability of type checking / inference

1. $\Gamma \Delta \text{ wf} \Rightarrow \Gamma \text{ wf}$ and $\Gamma \vdash t:T \Rightarrow \Gamma \Delta \vdash t:T$
2. $\Gamma(x:T)\Delta \vdash u:U \wedge \Gamma \vdash t:T \Rightarrow \Gamma \Delta[x \setminus t] \vdash u[x \setminus t] : U[x \setminus t]$
and $\Gamma(x:T)\Delta \text{ wf} \wedge \Gamma \vdash t:T \Rightarrow \Gamma \Delta[x \setminus t] \text{ wf}$
3. Inversion lemma :
 - ▶ If $\Gamma \vdash x : T$ then $(x:T') \in \Gamma, T =_{\beta} T'$ and $\Gamma \vdash T' : s$
 - ▶ If $\Gamma \vdash \lambda x:A.t : B$ then $B =_{\beta} \Pi x:A.C$ and $\Gamma(x:A) \vdash t : C$
 - ▶ If $\Gamma \vdash (t \ u) : C$ then $\Gamma \vdash t : \Pi x:A.B \ \Gamma \vdash u : A$ and $C =_{\beta} B[x \setminus u]$
 - ▶ If $\Gamma \vdash \Pi x:A.B : T$ then $\Gamma \vdash A : \text{Type}, \Gamma(x:A) \vdash B : s$ and $T = s$
 - ▶ If $\Gamma \vdash (t, u)_{\Sigma x:A.B} : C$ then $\Gamma \vdash t:A, \Gamma \vdash u:B[x \setminus t], C =_{\beta} \Sigma x:A.B$
 - ▶ If $\Gamma \vdash \Sigma x:A.B : T$ then $\Gamma \vdash A : \text{Type}, \Gamma(x:A) \vdash B : s$ and $T = \text{Type}$

If $\Gamma \vdash t : T$ and $\Gamma \vdash t : U$ then $T =_{\beta} U$ (same for $A+B$)

$$\begin{array}{c} [] \text{ wf} \quad \frac{\Gamma \vdash T : s}{\Gamma (x:T) \text{ wf}} \quad \frac{\Gamma \text{ wf}}{\Gamma \vdash x : T} \quad \frac{\Gamma \text{ wf}}{\Gamma \vdash \text{Type} : \text{Kind}}\end{array}$$

$$\frac{\Gamma \vdash A : \text{Type} \quad \Gamma (x:A) \vdash B : s}{\Gamma \vdash \Pi x : A . B : s}$$

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

$$\frac{\Gamma \vdash \Pi x : A . B : \text{Type} \quad \Gamma(x:A) \vdash t : B}{\Gamma \vdash \lambda x : A . t : \Pi x : A . B}$$

$$\frac{\Gamma \vdash t : \Pi x : A . B \quad \Gamma \vdash u : A}{\Gamma \vdash (t \ u) : B [x \setminus u]}$$

If Γ wf and $(x:T) \in \Gamma$, then $\Gamma \vdash T:s$

Let us write $(\alpha:K)$ when $K:Kind$ and $(x:T)$ when $T:Type$

If $\Gamma \vdash t:T$, then $\Gamma \vdash T:s$ (or $T=kind$)

Let us write $T:K$ when $K:Kind$ and $t:T$ when $T:Type$

We have a stratification of (typed) terms:

- | | |
|------------------------|---|
| – Kind | Kind |
| – $K : Kind$ (kinds) | $Type, \Pi x : T. K, \Pi x_1:T_1. \dots \Pi x_n:T_n.Type$ |
| – $T : K$ (predicates) | $\alpha, \Pi x:T_1.T_2 (T t), \lambda x:T_1.T_2$ |
| – $t : T$ (proofs) | $x, (t_1 t_2), \lambda x:T.t$ |

Going further: System T

Adding primitive natural numbers and a recursor

In Coq:

```
Inductive nat : Type :=  
  | 0 : nat  
  | S : nat -> nat.
```

Additional atomic type: N

Additional constants: $0 : N$, $S : N \rightarrow N$

Additional operators: $R_T : N \rightarrow T \rightarrow (N \rightarrow T \rightarrow T) \rightarrow T$

$R\ 0\ t_0\ ts \quad \triangleright \quad t_0$

$R\ (S\ n)\ t_0\ ts \quad \triangleright \quad ts\ n\ (R\ n\ t_0\ ts)$

A terminating programming language

- ▶ Incomplete (no chance to have all algorithms)
- ▶ But quite expressive
- ▶ Can be made even more expressive (general inductive types, System F...)

$$\text{add} = \lambda n. \lambda m. (R_N \ n \ m \ \lambda p. \lambda r. S(r))$$

$$\text{mul} = \lambda n. \lambda m. (R_N \ n \ 0 \ \lambda p. \lambda r. (\text{add } m \ r))$$

quite straightforward for all primitive recursive functions

From $\lambda \rightarrow \Sigma+$ to Type Theory

We have:

- Dependent types, encodes FOL up to cut-elimination for logical cuts (for $\wedge, \vee, \Rightarrow, \forall, \exists$)
- System T: allows the definition of complex computations

$$R_T : T \rightarrow (N \rightarrow T \rightarrow T) \rightarrow N \rightarrow T$$

Let us add the induction axiom :

$$R_P : (P\ 0) \rightarrow (\Pi\ x : N . (P\ n) \rightarrow (P\ (S\ n))) \rightarrow \Pi\ n : N . (P\ n)$$

$$(R_P\ p_0\ p_S\ 0) \triangleright p_0$$

$$(R_P\ p_0\ p_S\ (S\ n)) \triangleright p_{S\ n}\ (R_P\ p_0\ p_S\ n)$$

Subject reduction

$$(R_P \ p_0 \ p_S \ 0) \triangleright p_0$$

$$R_P : (P \ 0) \rightarrow (\Pi \ x : N . (P \ n) \rightarrow (P \ (S \ n))) \rightarrow \Pi \ n : N . (P \ n)$$

Suppose $(R_P \ p_0 \ p_S \ 0) : T$

so $p_0 : (P \ 0)$

so $p_S : (\Pi \ x : N . (P \ n) \rightarrow (P \ (S \ n)))$

so $0 : N$ (it is)

so $T =_\beta P \ 0$

so $p_0 : T$

Obviously similar for

$$(R_P \ p_0 \ p_S \ (S \ n)) \triangleright p_S \ n \ (R_P \ p_0 \ p_S \ n)$$