Assistants de Preuve
Architecture / Modèles 1

Bruno Barras et Christine Paulin-Mohring

INRIA, Université Paris-Sud 11

6/1/09

Plan

Critères de classification

- critère de de Bruijn : noyau
- principe de Poincaré : 2+2=4 “par calcul”
- logique / méta-logique
- représentation des preuves
- construction interactive des preuves : tactiques
- automatisation

Quelques systèmes : Isabelle, HOL, Mizar, PVS, ACL2, Meta-PRL, Coq

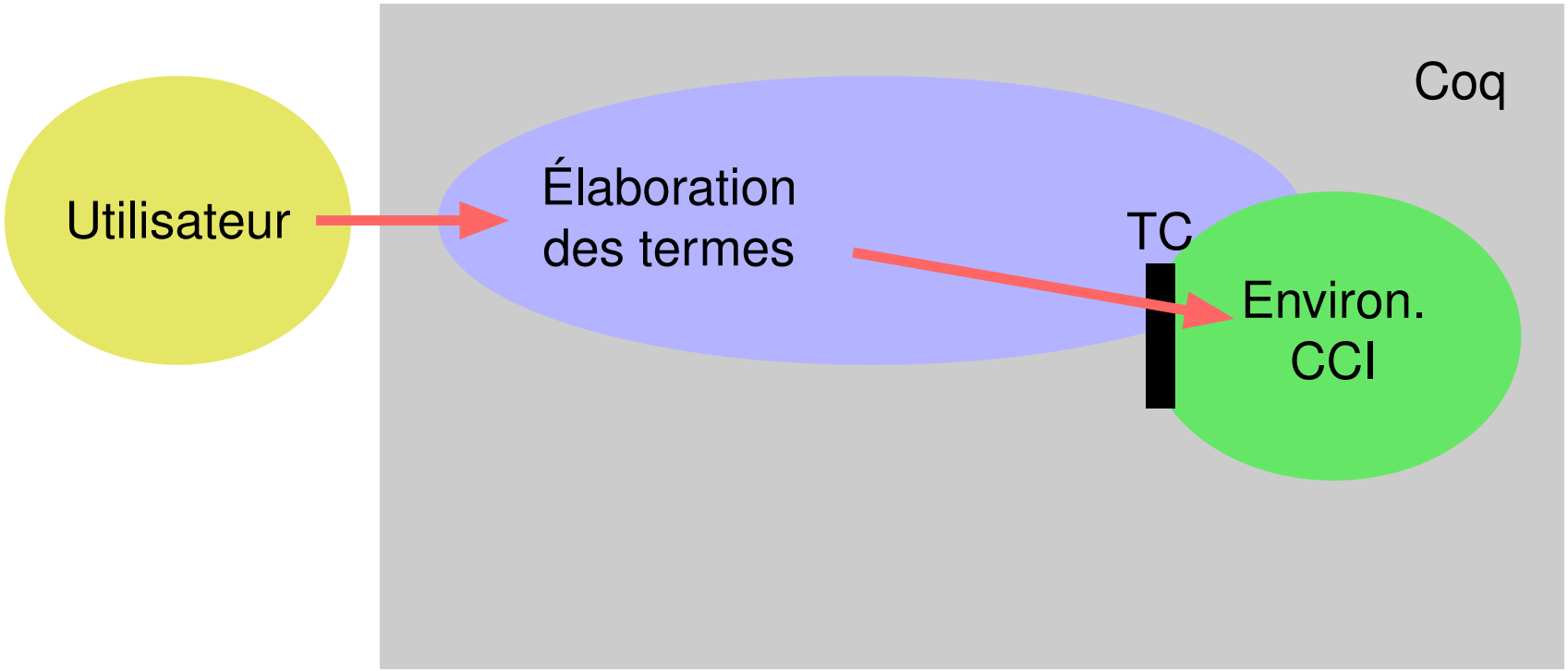
Architecture de Coq

- Noyau : implante les règles du CCI
- Élaboration : traduit des termes “à trous” en termes CCI
- Tactiques primitives : règles de déduction naturelle
- Tactiques composées : automatisation, macros
- Ltac : langage de programmation

Interactions avec l'utilisateur

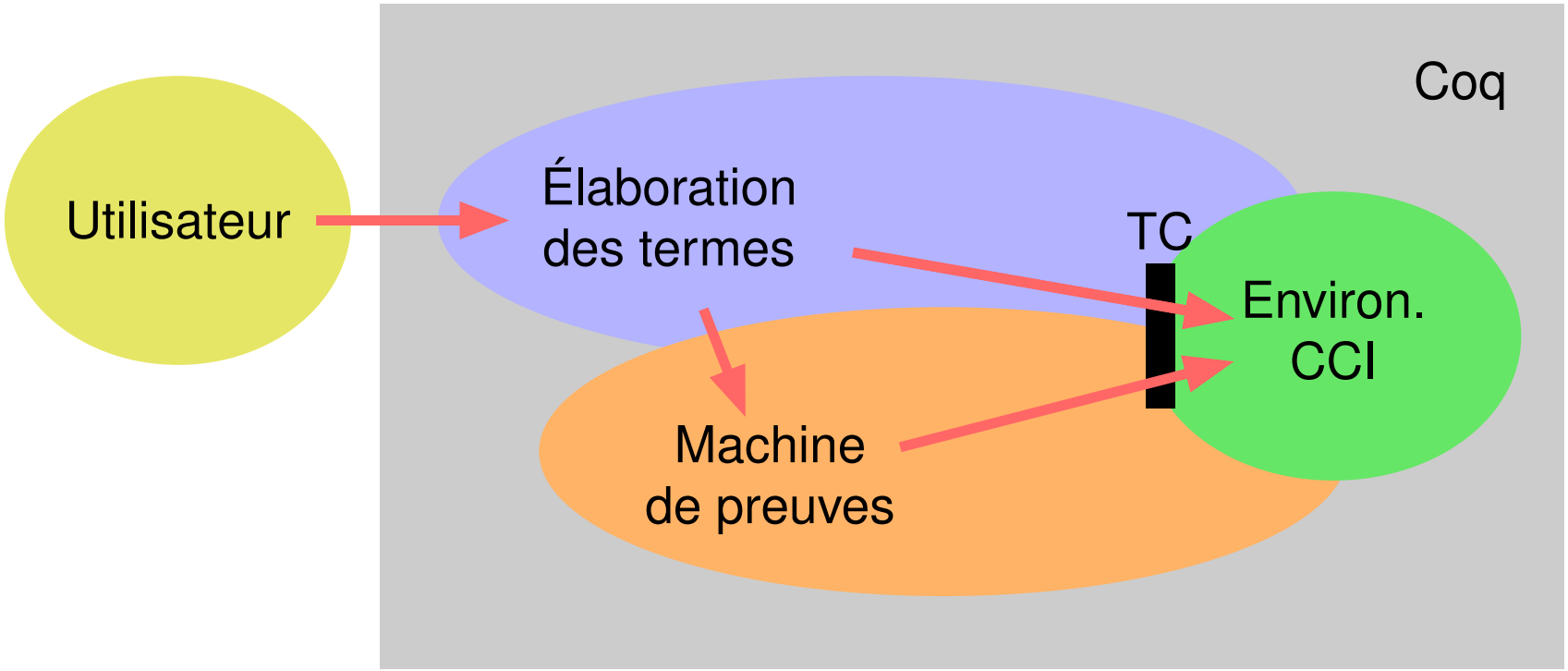
Invariant : environnement bien typé dans CCI

Interactions avec l'utilisateur



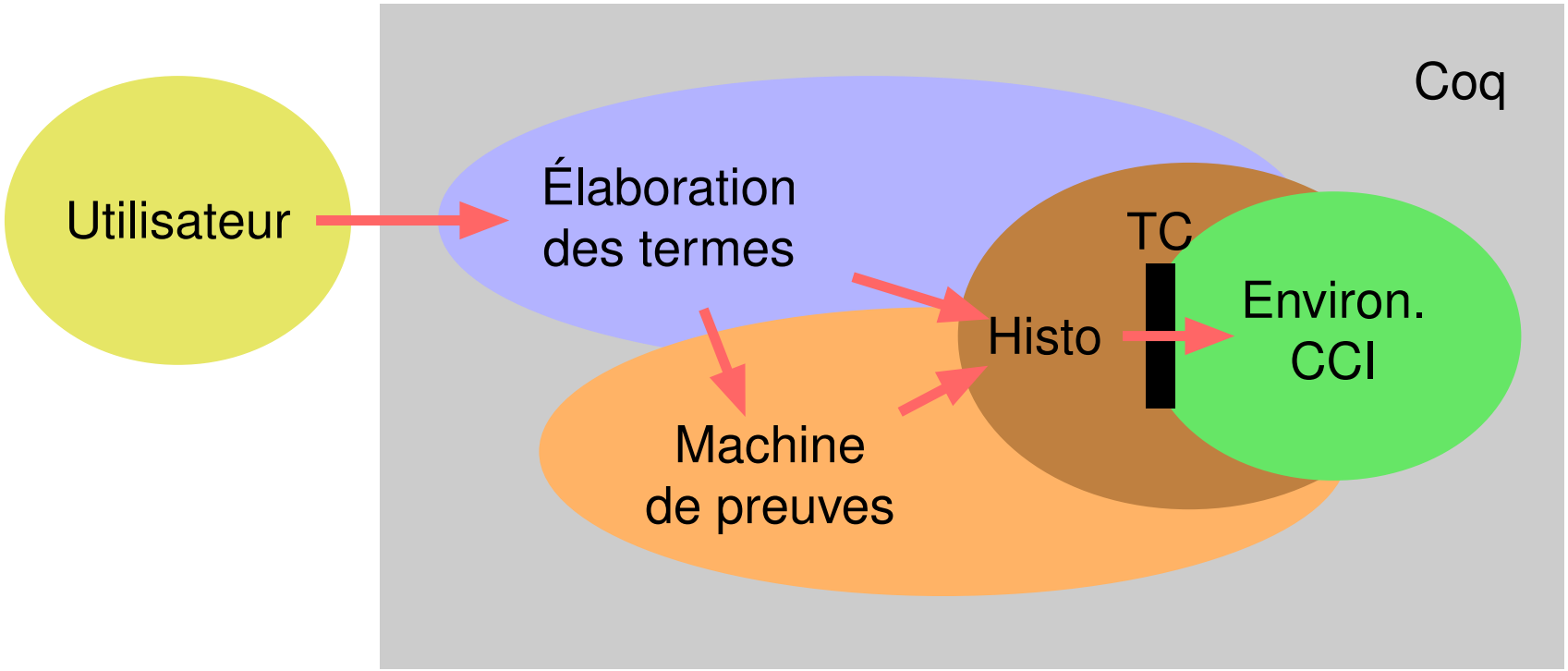
Syntaxe plus proche de l'utilisateur (notations, noms courts)

Interactions avec l'utilisateur



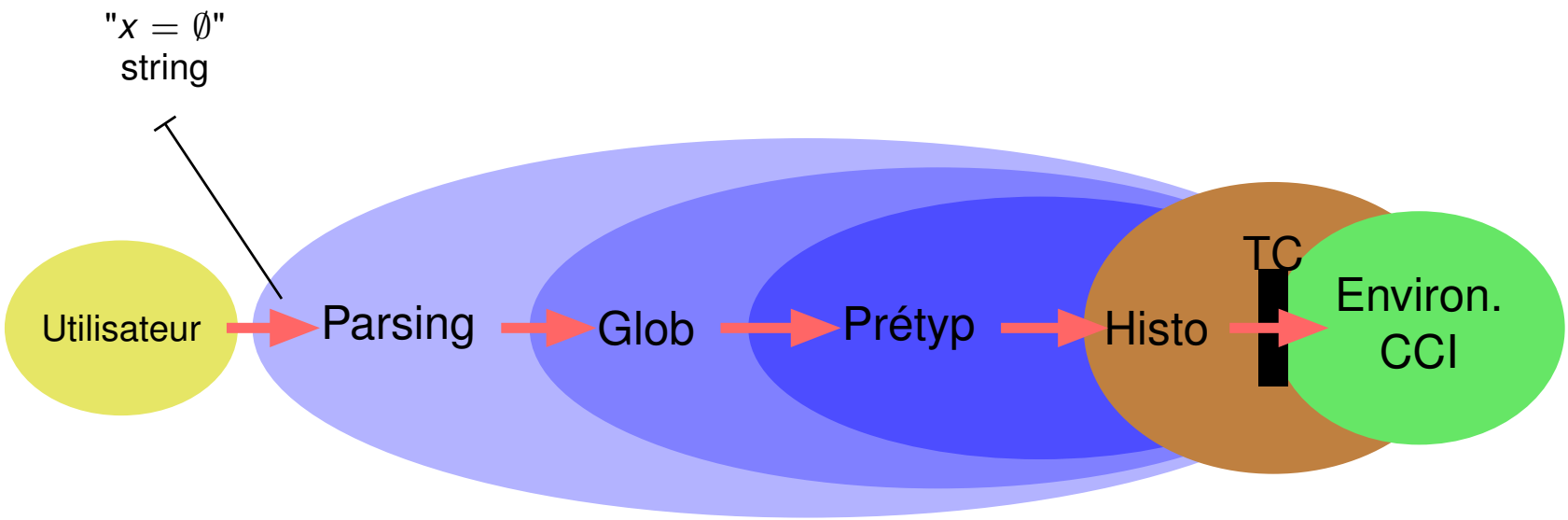
Preuves construites interactivement (tactiques)

Interactions avec l'utilisateur

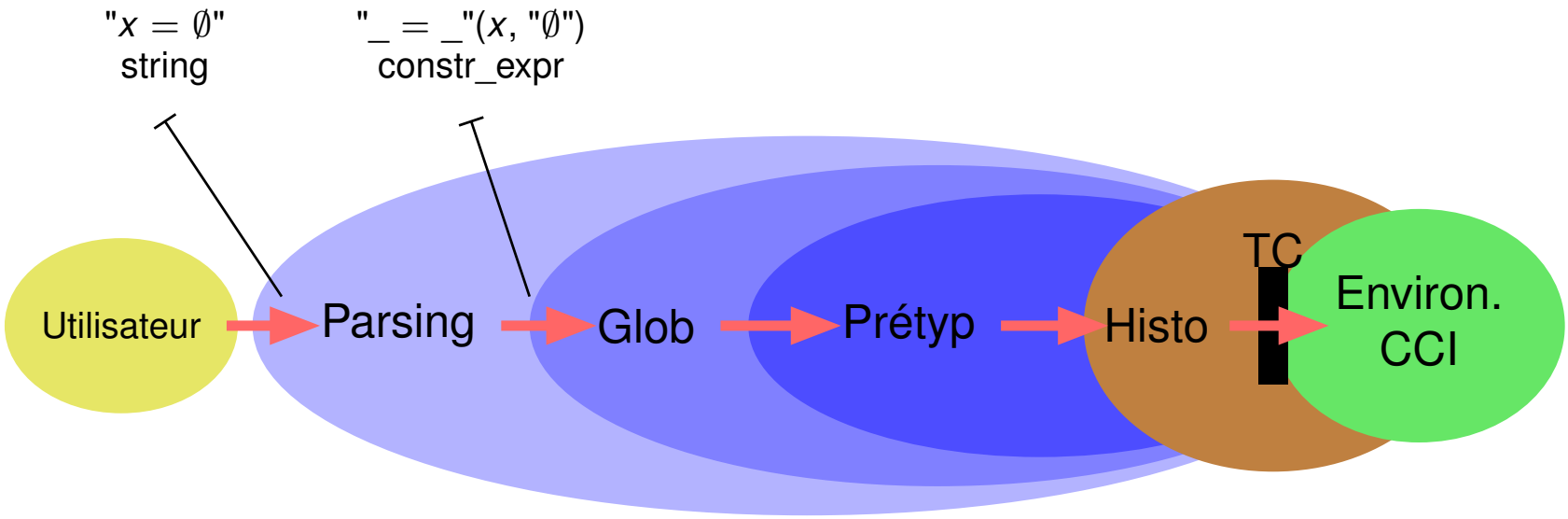


Modularité Coq, sections

Élaboration d'un terme

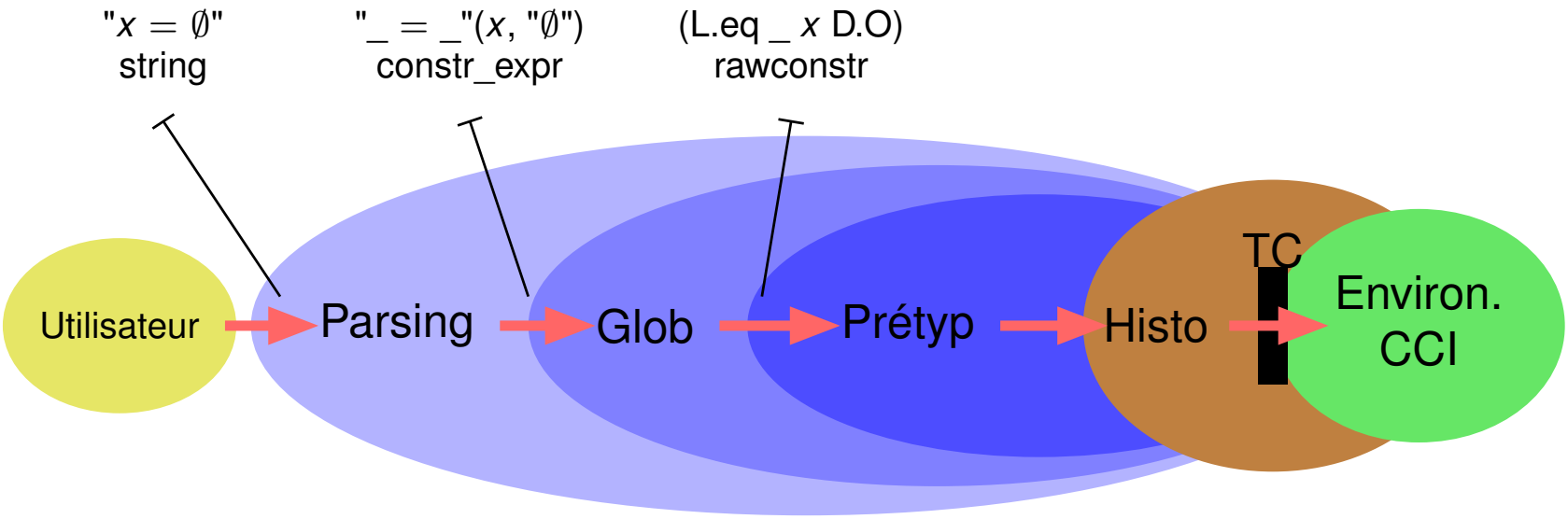


Élaboration d'un terme



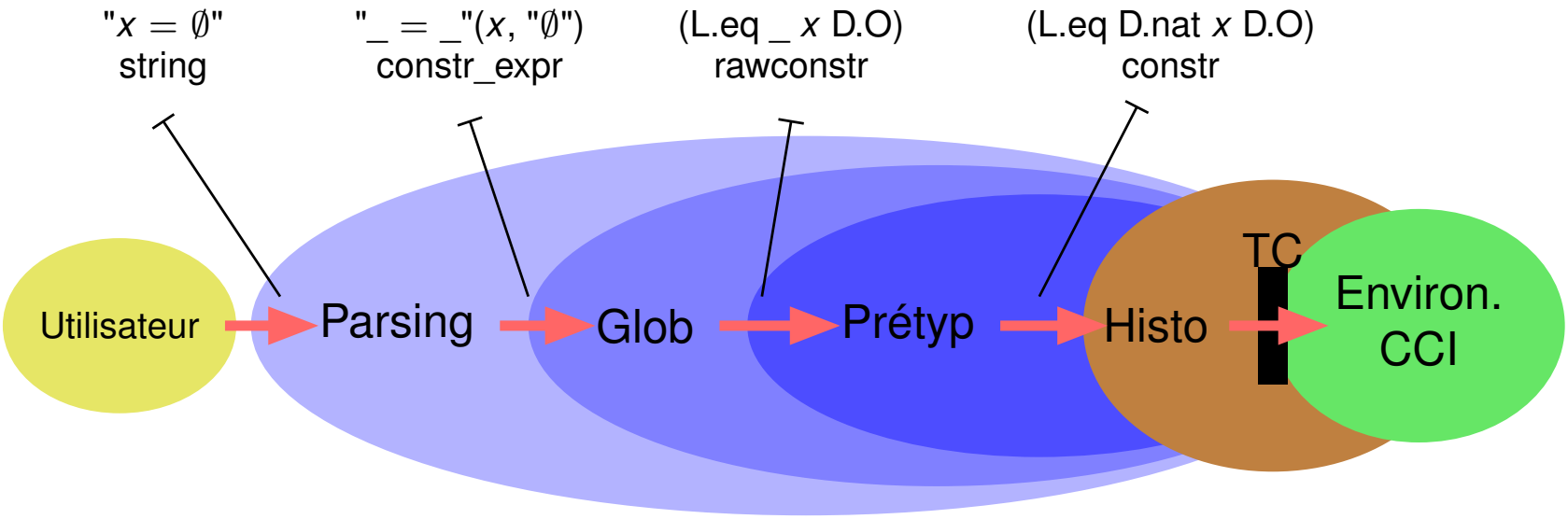
Analyse syntaxique (Camlp4)

Élaboration d'un terme



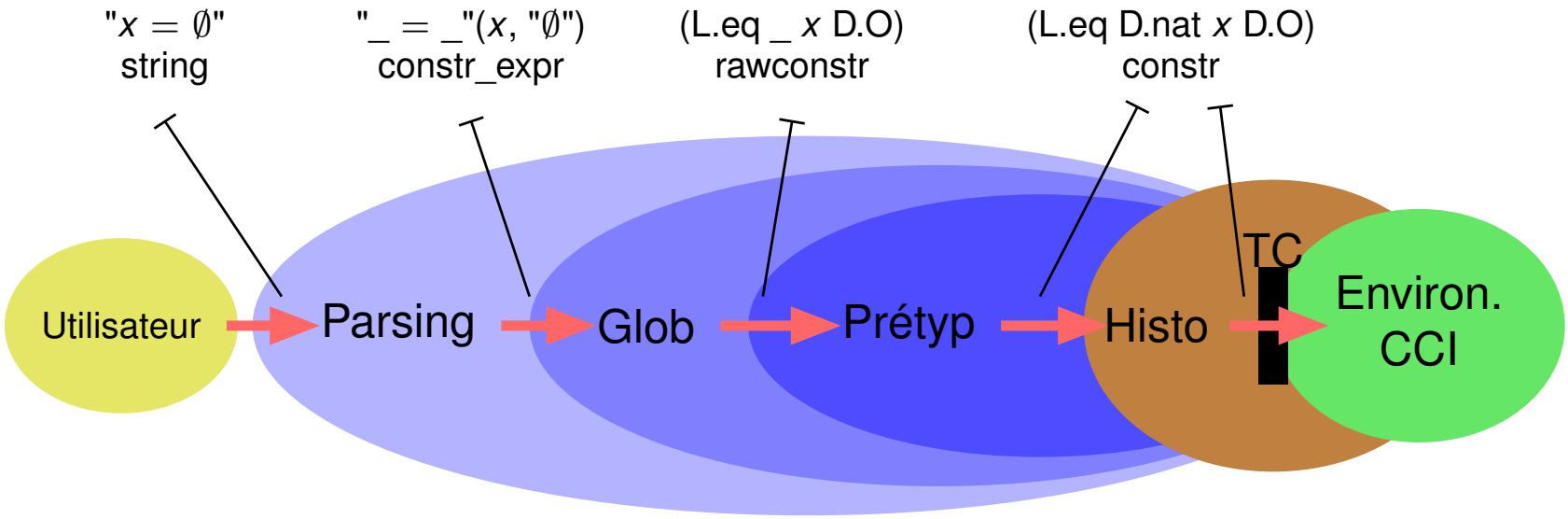
Globalisation, notations, expansion des implicites

Élaboration d'un terme



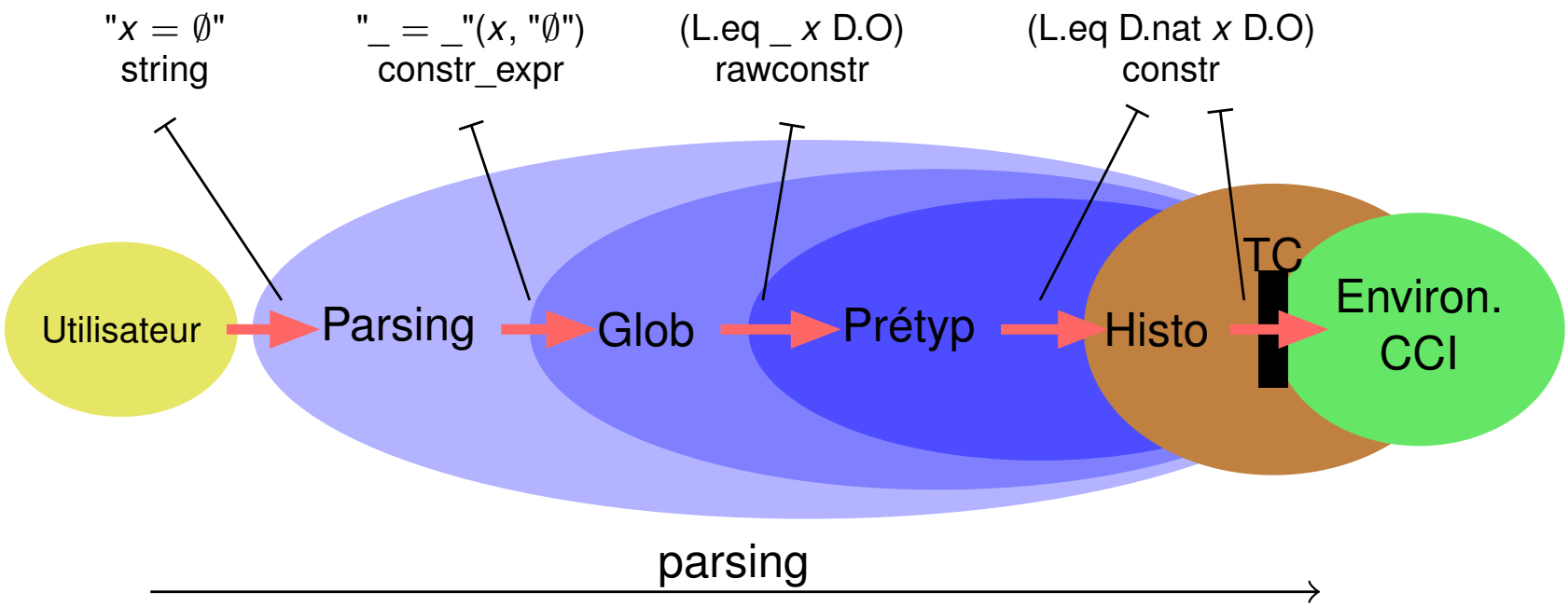
Résolution des implicites, compilation filtrage, coercions

Élaboration d'un terme

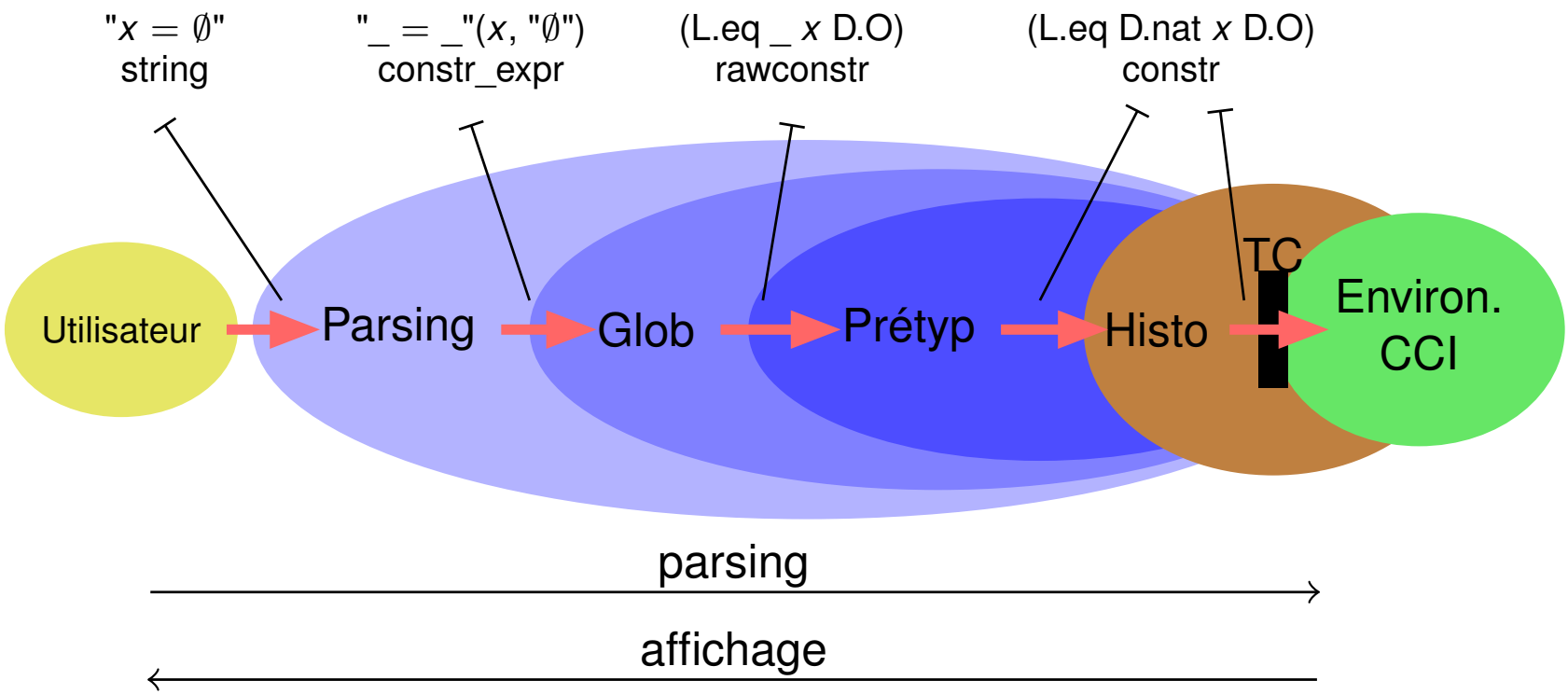


Contraintes d'univers

Élaboration d'un terme



Élaboration d'un terme



Arbre de preuve

- Historique arborescent de tactiques
- Rend compte de la décomposition des tactiques

Modèles : pour quoi faire ?

Montrer qu'un théorème n'est pas prouvable : $\not\vdash A$ pour A un énoncé donné
Exemples :

- Cohérence de CC : $\not\vdash \bot$
- Cohérence de CC + classique : $\forall A : Prop.(A \vee \neg A) \not\vdash_{CC} \bot$
- Non dérivabilité de $0 \neq 1$ dans CC

Modèles booléens

Cas propositionnel :

- À toute formule A est associée une valeur de vérité $[\![A]\!] : \mathit{bool}$
- On prouve $\vdash A \Rightarrow [\![A]\!] = \mathit{true}$
- Si $[\![\bot]\!] = \mathit{false}$, alors on a prouvé la cohérence

Cas général :

- On interprète un séquent $\Gamma \vdash t : T$ par une proposition $[\![\Gamma \vdash t : T]\!]$
- On prouve $\Gamma \vdash t : T \Rightarrow [\![\Gamma \vdash t : T]\!]$
- Si $[\![\vdash t : \bot]\!]$ est faux, alors le système est cohérent

Modèles booléens

Intuition :

- Définir $[T]$ comme une traduction de T en un ensemble
- $[\mathrm{Prop}] = \{\emptyset, \bullet\}$ et $[\forall P : \mathrm{Prop}, P] = \emptyset$
- $[\![t : T]\!]$ signifie $[t] \in [T]$

Plus généralement :

- L'interprétation dépend d'une valuation ρ, et on a $[x]_\rho = \rho(x)$
- $[\![\Gamma \vdash t : T]\!] = \forall \rho \in [\![\Gamma]\!], [t]_\rho \in [T]_\rho$, avec $[\![\Gamma]\!] = \{\rho \mid \forall (x : T) \in \Gamma, \rho(x) \in [T]_\rho\}$