ABOUT COQ……

张恒若

提纲

- Coq源码分析
- Coq的应用——CertiKOS
- Coq的应用——CertiUcosII
- （安利某实验室

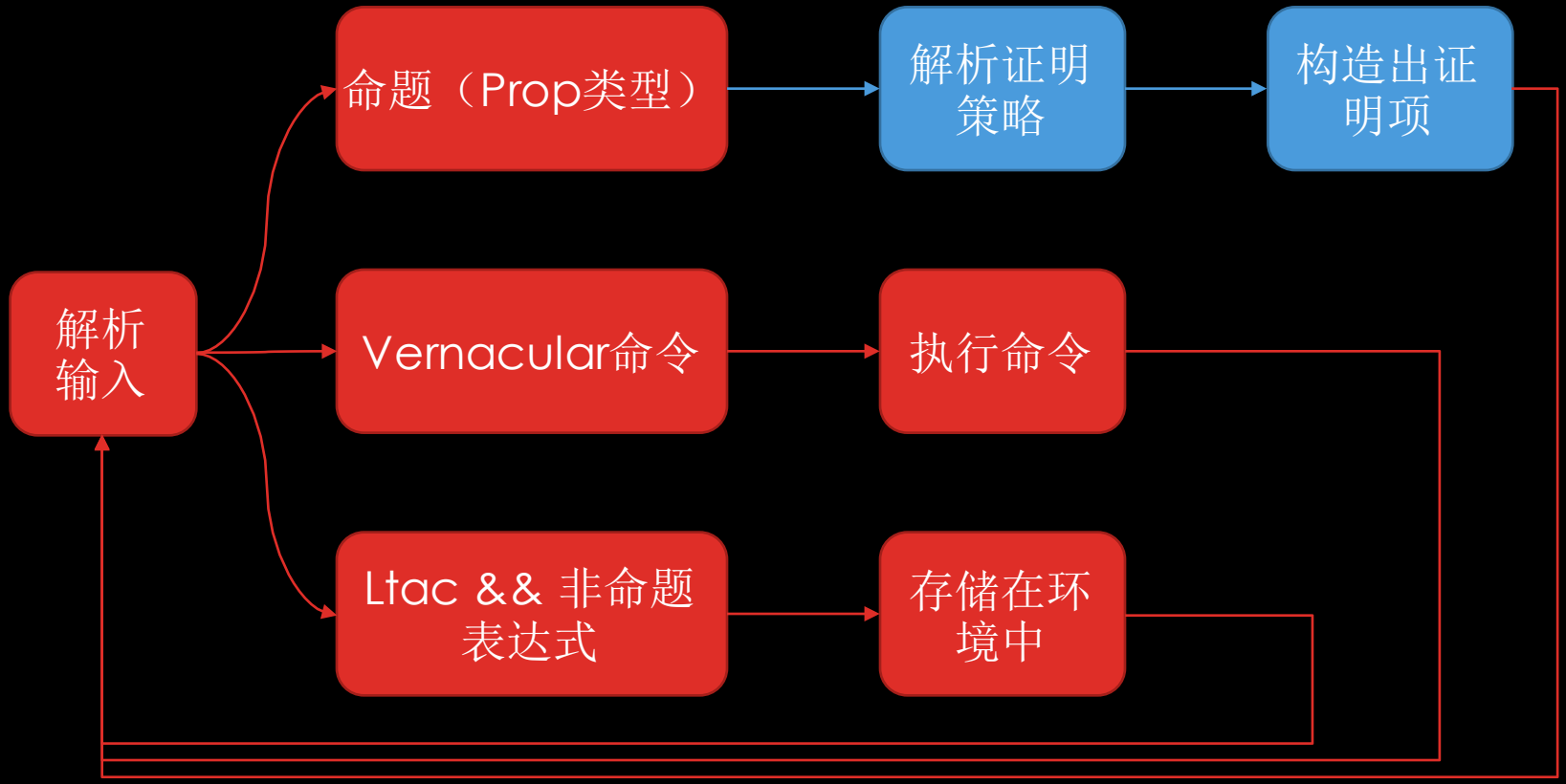
提纲

- Coq源码分析
- Coq的应用——CertiKOS与CertiUcosII
- （安利某实验室

COQ代码

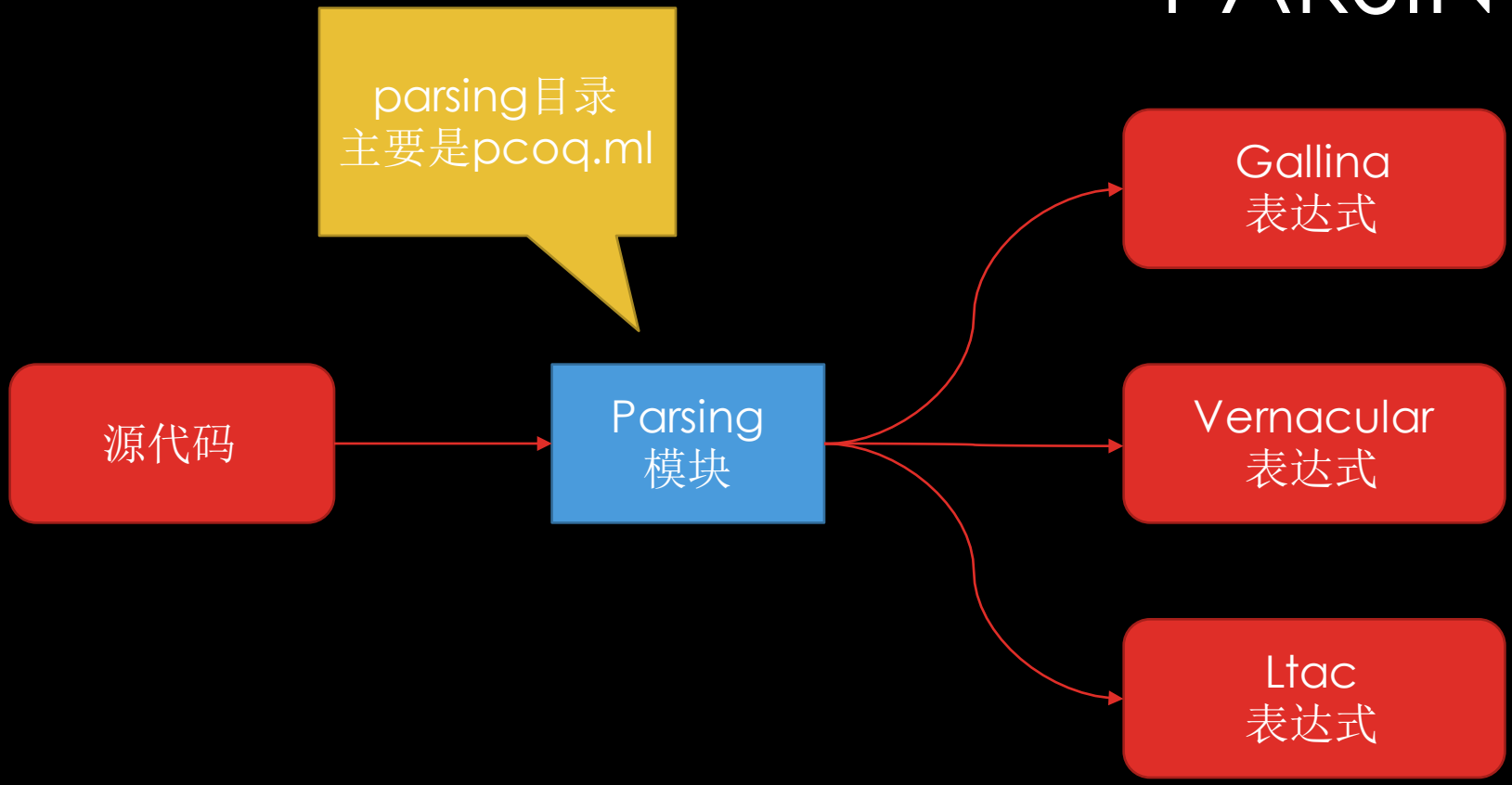
```
Inductive nat : Set :=
| O : nat
| S : nat -> nat.

Ltac tac1:=
intros;subst;reflexivity.

Theorem th1:.
forall p q r:nat, p = q -> q = r -> p = r.
Proof.
tac1.
Qed.
```

REPL

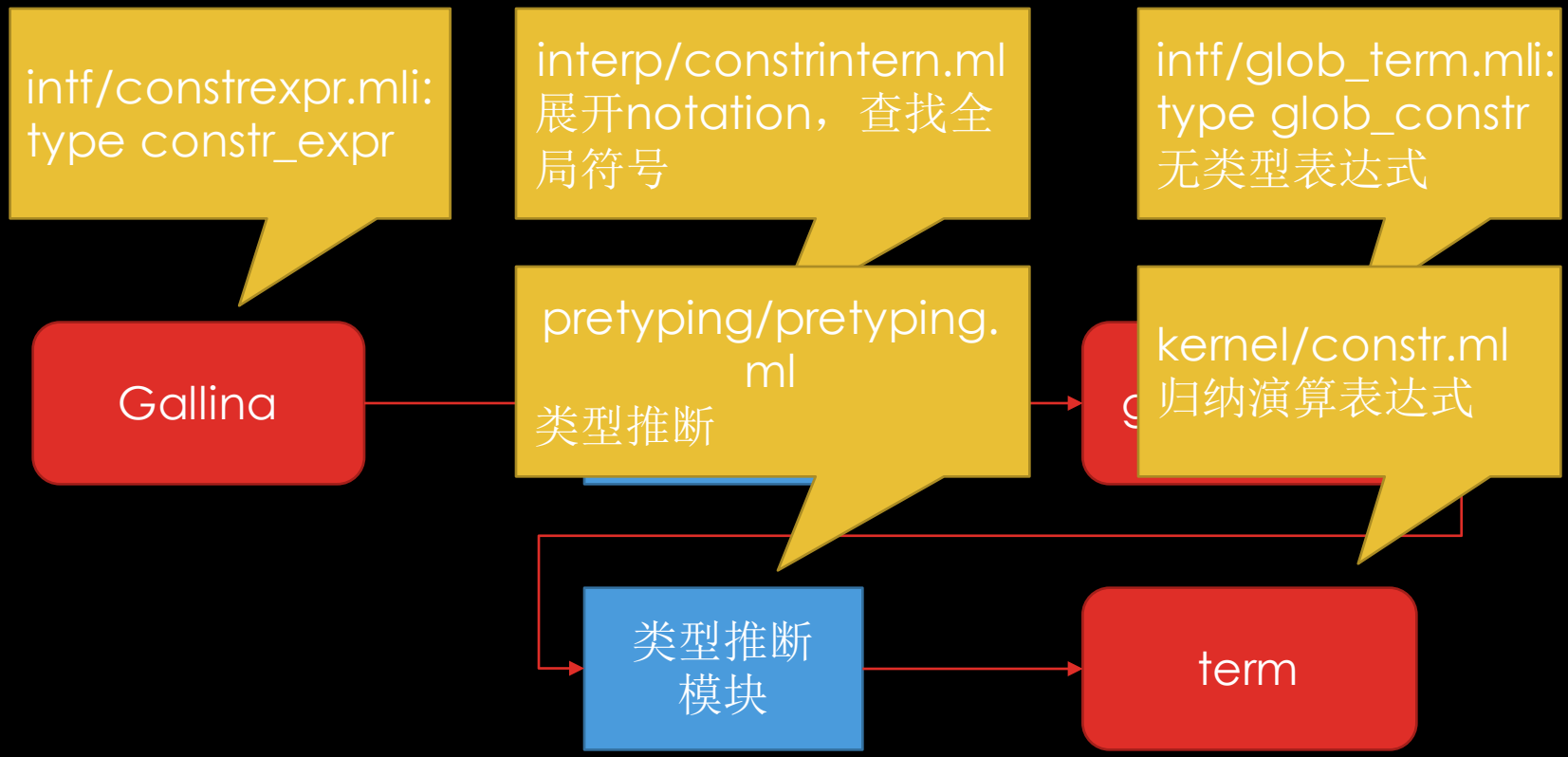


toplevel目录下的coqloop.ml文件

PARSING


parsing目录
主要是pcoq.ml
源代码
Parsing
模块
Gallina
表达式
Vernacular
表达式
Ltac
表达式

PARSING - GALLINA



- intf：interface，对外的Coq接口，目前还非常不成熟……
- interp： interpretation，翻译有关的函数
- pretyping：类型推断

PARSING - VERNACULAR

- parsing/g_vernac.ml4中定义语法
- toplevel/vernac.ml进行parse
- toplevel/command.ml执行相关功能

PARSING - LTAC

- 相关函数都在ltac目录下
- parsing/pcoq.ml发现“Ltac”标记之后转入ltac/pltac.ml
- pltac是主要的parser

环境

- 位于kernel/environ.ml，原始定义在kernel/pre_env.ml

- 内容：
  - 全局定义的符号，公理（kernel/constr.ml中的term类型）
  - 归纳类型（kernel/inductive.ml）
  - 非直谓标志
  - 当前证明环境的前提条件
  - ……

构造证明项

- engine/proofview.ml文件中的proofview类型储存证明的上下文
- tactic目录下有很多和tactic有关的操作（主要在tacmach.ml文件中）

COQ未来的展望

- 丰富开发文档（dev/doc/下很多TODO）
- 丰富API，更加模块化，接口化（向lean学习）
- 让tactic更像函数；monad化方便组合

CERTIKOS VS CERTIUCOS

- CertiKOS
  - 理论基础：并发分离逻辑
  - Yale FLINT实验室
- CertiUcosII
  - 理论基础：Rely-Guarantee Sep
  - 软件安全实验室

（安利环节

- 冯新宇老师主页：http://staff.ustc.edu.cn/~xyfeng

谢谢！