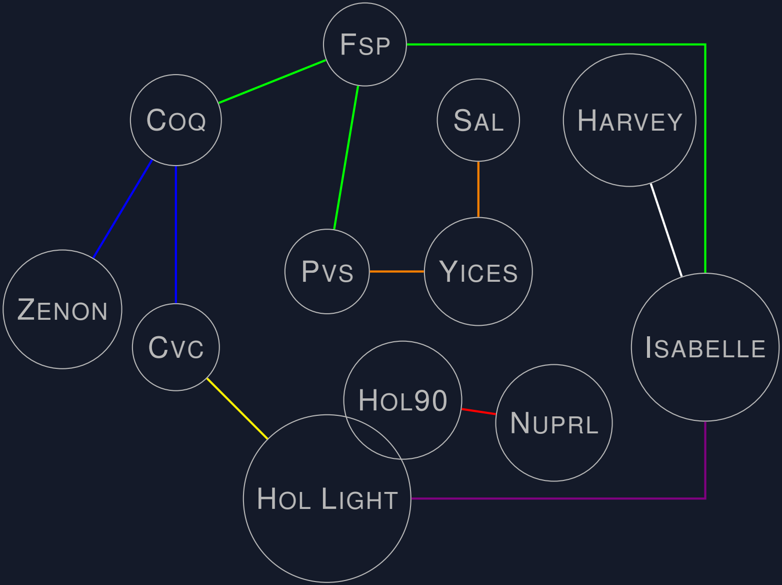
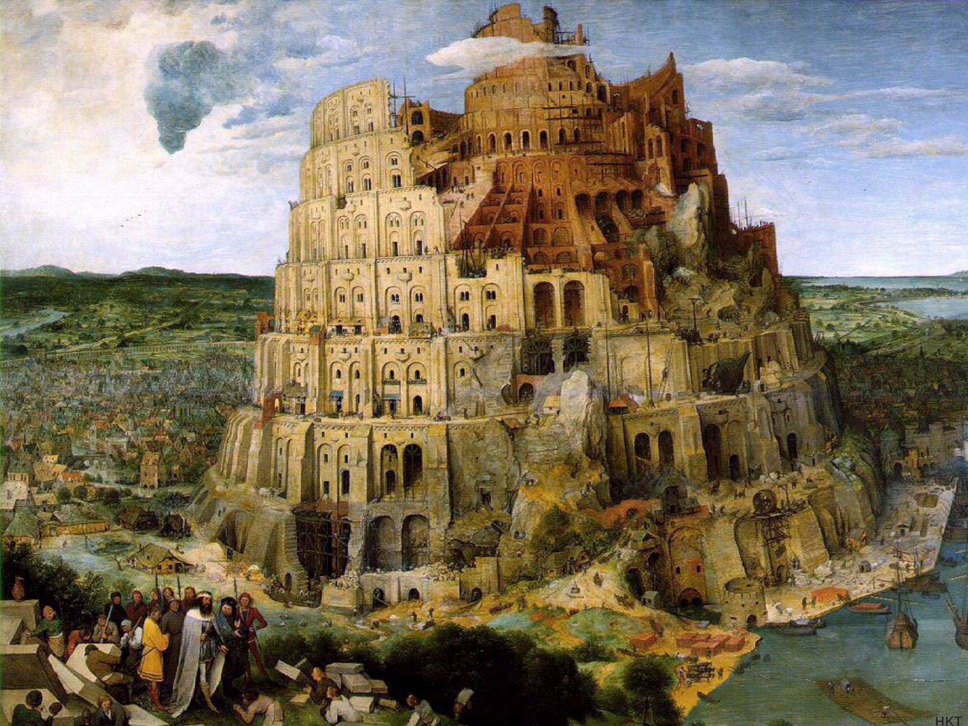
Distributing Formal Verification: The Evidential Tool Bus

Florent Kirchner

—

Computer Science Laboratory
SRI International


Fsp
Coq
Sal
Harvey
Zenon
Pvs
Yices
Cvc
Isabelle
Hol90
Nuprl
Hol Light


HKT

•–– •••• • •–• •

•– •–• –

– •••• ––– ••–

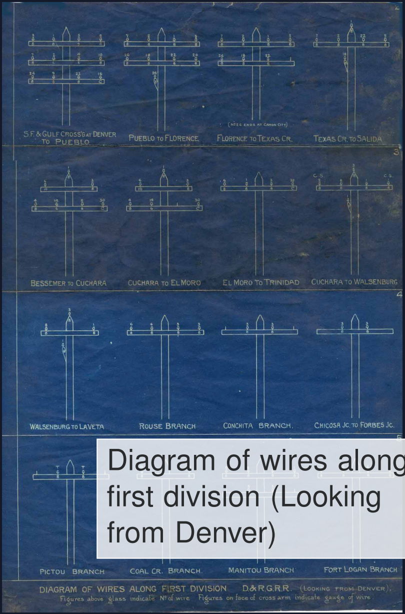
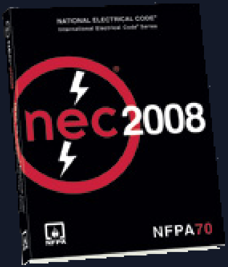
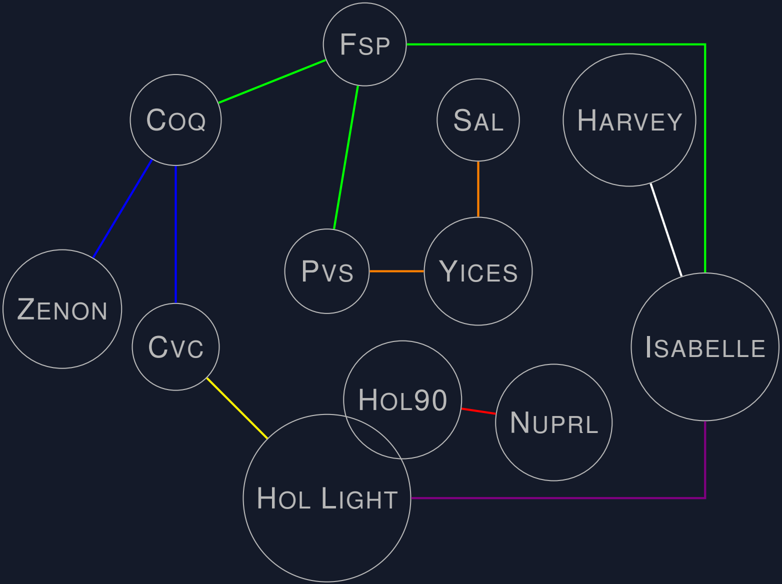

S.F. & GULF CROSS'G AT DENVER TO PUEBLO
PUEBLO TO FLORENCE
(No 24 ENDS AT CANON CITY)
FLORENCE TO TEXAS CR.
TEXAS CR. TO SALIDA
BESSEMER TO CUCHARA
CUCHARA TO EL MORO
EL MORO TO TRINIDAD
C.S.
CUCHARA TO WALSENBURG
WALSENBURG TO LAVETA
ROUSE BRANCH
CONCHITA BRANCH.
CHICOSA JC. TO FORBES JC.
PICTOU BRANCH
COAL CR. BRANCH.
MANITOU BRANCH
FORT LOGAN BRANCH
DIAGRAM OF WIRES ALONG FIRST DIVISION D&R.G.R.R. (LOOKING FROM DENVER).
Figures above glass indicate No of wire. Figures on face of cross arm indicate gauge of wire.

Diagram of wires along first division (Looking from Denver)

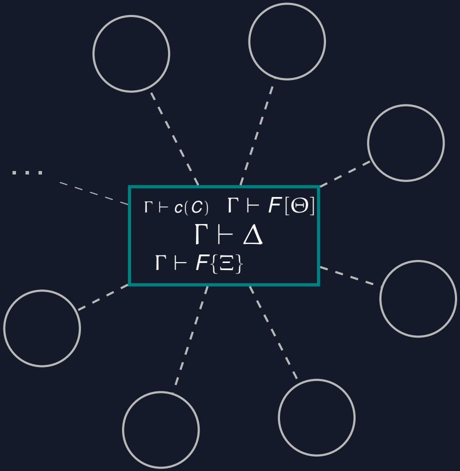


ANSI/NFPA 70
National Electrical Code

Heterogeneous pipes and mappings



Distributed framework for formal verification tools



$\Gamma \vdash c(C)$ $\Gamma \vdash F[\Theta]$

$\Gamma \vdash \Delta$

$\Gamma \vdash F\{\Xi\}$

$\Gamma \vdash c(C)$ $\quad$ $\Gamma \vdash F[\Theta]$

$$\Gamma \vdash \Delta$$

$\Gamma \vdash F\{\Xi\}$

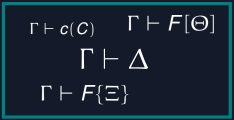
Blackboard

- Store proof obligations
- Record proof discharges
- Trace proof developments

$\Gamma \vdash c(C)$ $\Gamma \vdash F[\Theta]$

$$\Gamma \vdash \Delta$$

$\Gamma \vdash F\{\Xi\}$



$\Gamma \vdash c(C)$

$\Gamma \vdash F[\Theta]$

$\Gamma \vdash \Delta$

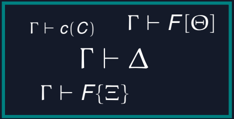
$\Gamma \vdash F\{\Xi\}$

Blackboard

- Store proof obligations
- Record proof discharges
- Trace proof developments

Language DB

- Register formal language declarations
- Query dialect intersections



$\Gamma \vdash c(C)$ $\Gamma \vdash F[\Theta]$

$$\Gamma \vdash \Delta$$

$\Gamma \vdash F\{\Xi\}$

Blackboard

- Store proof obligations
- Record proof discharges
- Trace proof developments

Language DB

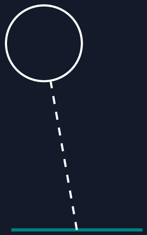
- Register formal language declarations
- Query dialect intersections

Facilitator

- Register agent capabilities
- Resolve and route requests
- Abstract network geometry

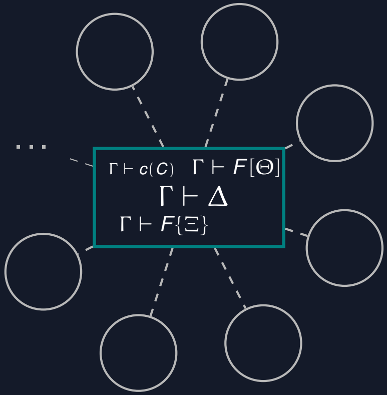
```
default namespace = "http://etb.csl.sri.com/ns/foa"
datatypes xsd = "http://www.w3.org/2001/XMLSchema-datatypes"

start = element-sequent

element-sequent = element sequent {
    attribute   structure       {"set"}
  & element     antecedent      {element-formula}*
  & element     consequent      {element-formula}*
  & element     activeformula   {xsd:anyURI}?
}
...
element-connectives = {
    element and {
      element-formula, element-formula}
  | element implies {
      element-formula, element-formula}
  | element forall {
      element-formula}
```

```
default namespace = "http://etb.csl.sri.com/ns/foa"
datatypes xsd = "http://www.w3.org/2001/XMLSchema-datatypes"

# scli: revised 2008-01-21 2008-01-24 2008-02-06 # YYYY-MM-DD
# scli: status experimental # official|experimental|private|obsolete
# scli: shelf-life 2008-12-31 # YYYY-MM-DD

start = element-sequent

element-sequent = element sequent {
    attribute   structure       {"set"}
  & element     antecedent      {element-formula}*
  & element     consequent      {element-formula}*
  & element     activeformula   {xsd:anyURI}?
}
...
element-connectives = {
    element and {
      # scli: G,and(A,B)|-D <==> G,A,B|-D # multiplicative conjunction
      element-formula, element-formula}
  | element implies {
      # scli: G|-implies(A,B),D <==> G,A|-B,D # classical implication
      element-formula, element-formula}
  | element forall {
      # scli: G|-forall(A),D <==> all(t) G|-A{1<-t},D
      element-formula}
```



Agent interface

- Declare formal language
- Declare agent capabilities
- Use standard rpc



$\cdots$

$\Gamma \vdash c(C) \quad \Gamma \vdash F[\Theta]$

$\Gamma \vdash \Delta$

$\Gamma \vdash F\{\Xi\}$

- CEGAR loop: predicate abstractor, model-checker, SAT-solver
- CSP specification: deadlock detector, code generator, trace monitors
- Autocode certificates: certification browser, automatic checker
- Regulation analysis: UML, Z, Roz, Jaza Animator, Alloy Analyzer
- Numerical + Predicate abstraction: NEXPoint, NTBDD, NDD checkers
- Verifying compiler: proof assistant, VC generator, automated prover

- *Open Agent Architecture*, DARPA CALO Project (A. Cheyer et al.)
- *Evidential Tool Bus*, Java, Perl, Scheme, Relax-NG, XML
- *SAL – Yices*, Callback procedure integrated into the ETB
- *Cybertrail*, NSF Medium Project Proposal (N. Shankar, A. Gehani)

•— — •••• • •—• •

•— •—• —

— •••• — — — ••—

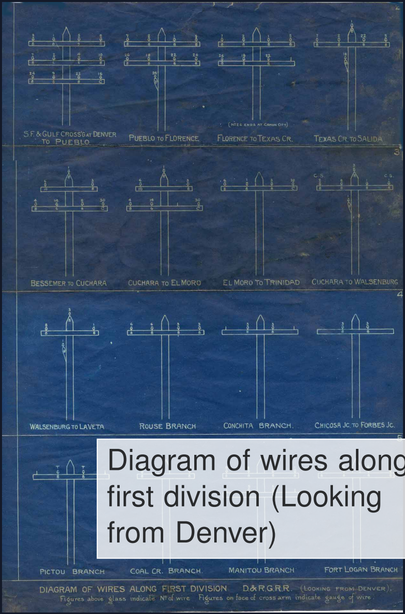

S.F. & GULF CROSS'G AT DENVER TO PUEBLO
PUEBLO TO FLORENCE
(No 24 ENDS AT CANON CITY)
FLORENCE TO TEXAS CR.
TEXAS CR. TO SALIDA
BESSEMER TO CUCHARA
CUCHARA TO EL MORO
EL MORO TO TRINIDAD
CUCHARA TO WALSENBURG
WALSENBURG TO LAVETA
ROUSE BRANCH
CONCHITA BRANCH.
CHICOSA JC. TO FORBES JC.
PICTOU BRANCH
COAL CR. BRANCH.
MANITOU BRANCH
FORT LOGAN BRANCH
DIAGRAM OF WIRES ALONG FIRST DIVISION D.&R.G.R.R. (LOOKING FROM DENVER).
Figures above glass indicate No of wire Figures on face of cross arm indicate gauge of wire.

Diagram of wires along first division (Looking from Denver)

Semantic Interoperability

Facets	Logical frameworks and embeddings Semantical formalisms for checkers / solvers
Objectives	Meta-logical backdrops for PVS, Isabelle and Coq Proof trace generation for Yices Translations and embeddings
With	Logical, Protheo, University of Warsow SRI International, DCS, Mosel

Formal Distribution

Facets	Formalizing the distribution framework Distributed proofs authentication Coordination languages
Objectives	Interaction model and semantics Distributed proof validation system Description tool for coordination scenarios
With	SRI International, Harvard, Mosel, Phoenix

Implementation

Facets	Extension of the distributed ecosystem Applications and performance
Objectives	Integrate PVS, Isabelle and Harvey, Coq and Why Verification of aeronautical systems
With	Mosel, University of Munich NASA, DGAC, Dassault