KeYmaera Improving the Proof Experience

Corwin de Boor

Cyber-Physical Systems

- Safety-critical
- Verification
- Proof assistance
- Proof assistants
- Proof experience

Proof Experience Issues

- High iteration cost
  - Verification is slow
  - Tactics are brittle
- Limited introspection

Demo

https://www.youtube.com/watch?v=JgBitYfgY2A

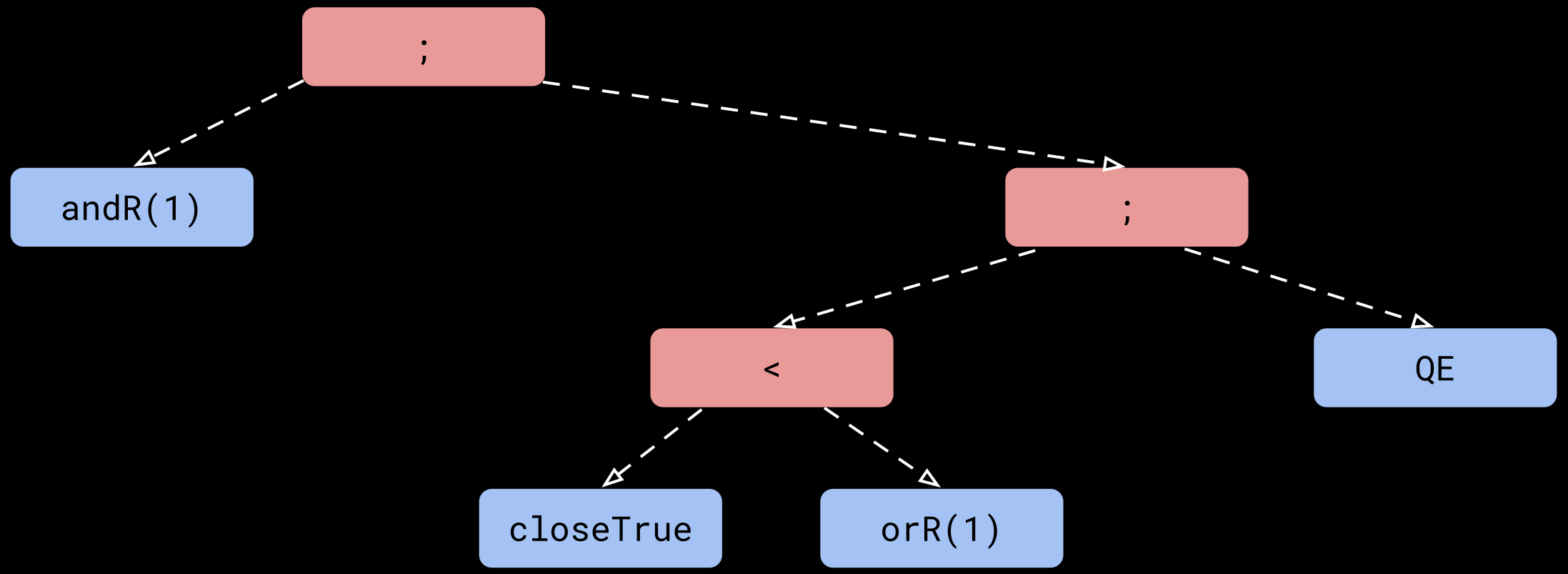
Step-by-Step Interpreter

- Goals
  - Store proof as tactic is executed
  - Keep state if tactic fails

- Strategy: Tree Transformation
  - Syntax Tree
  - Derivation Tree

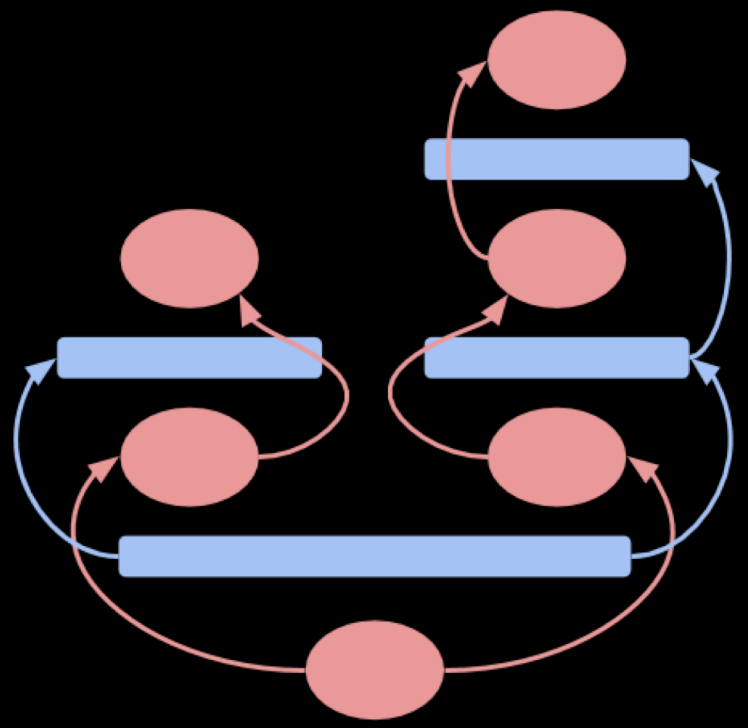
Syntax Tree

```
andR(1); <( closeTrue, orR(1) ); QE
```

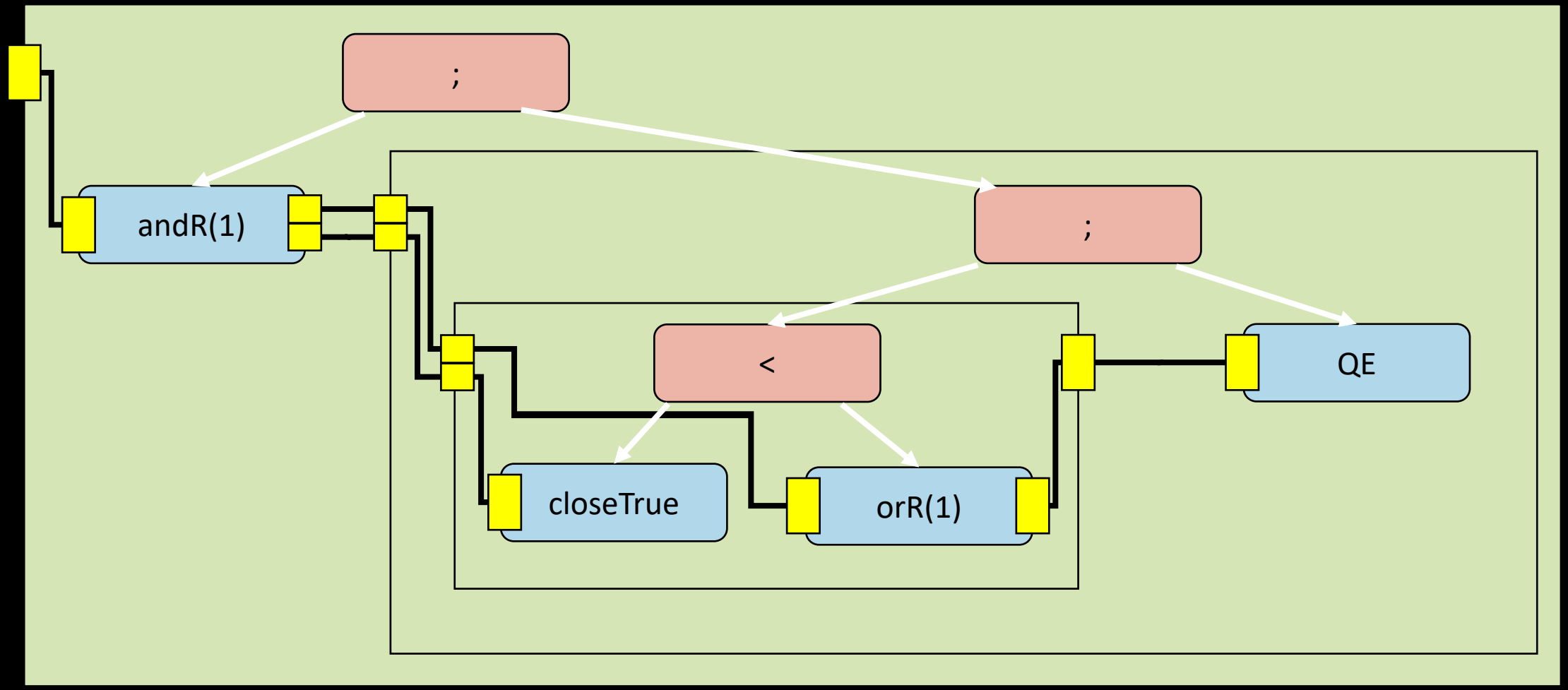


Derivation Tree

$$\dfrac{\dfrac{\dfrac{*}{\vdash \texttt{true}}\ \texttt{closeTrue} \qquad \dfrac{\dfrac{*}{\vdash x \geq 0, x < 0}\ \texttt{QE}}{\vdash x \geq 0 \lor x < 0}\ \texttt{orR(1)}}{\vdash \texttt{true} \land (x \geq 0 \lor x < 0)}\ \texttt{andR(1)}$$



Transformation Process



Feature Summary

- Interactive interpreter
  - Step-by-step listener
  - Pending tactics
  - Minimal editing
- Proof introspection
  - Highlight path to goal
  - View prior sequent

Questions?