Traf: Coqでの対話的証明と連動した証明木描画ツール

PPL2018

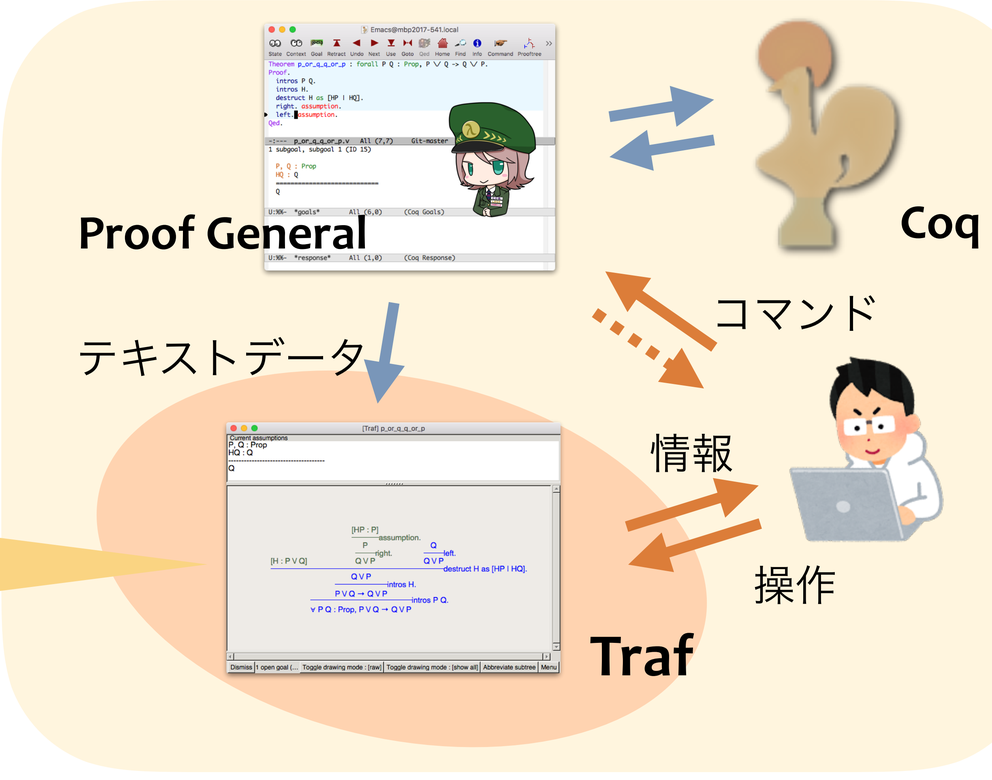
木村 麻衣　田中 雄太*　川端 英之　弘中 哲夫　　広島市立大学（* 現在，関電システムソリューションズ）

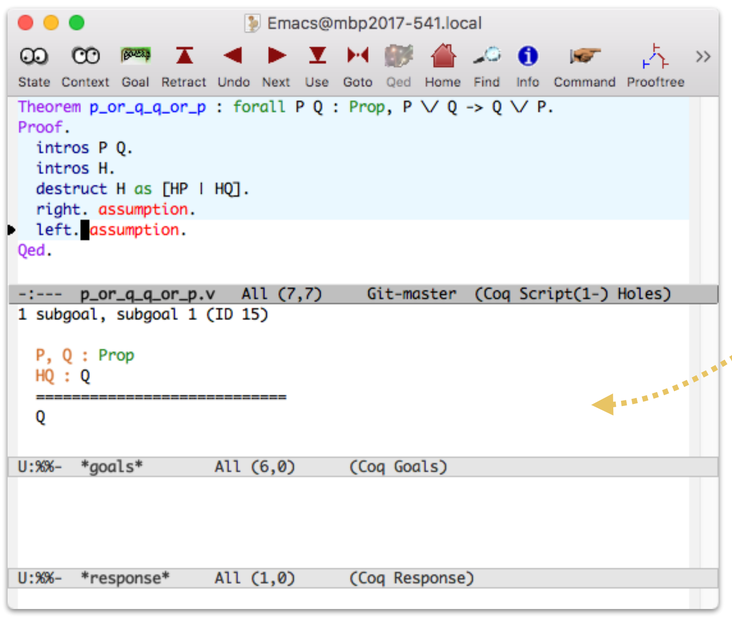
定理証明支援系（例えばCoq）・・・

- 証明スクリプトが手続き的で可読性が高いとは言い難い
- 証明スクリプトが宣言的に書けても，途中の様子が分かりにくい
- 証明の流れを図示するツール（例えばprooftree）は大雑把過ぎる

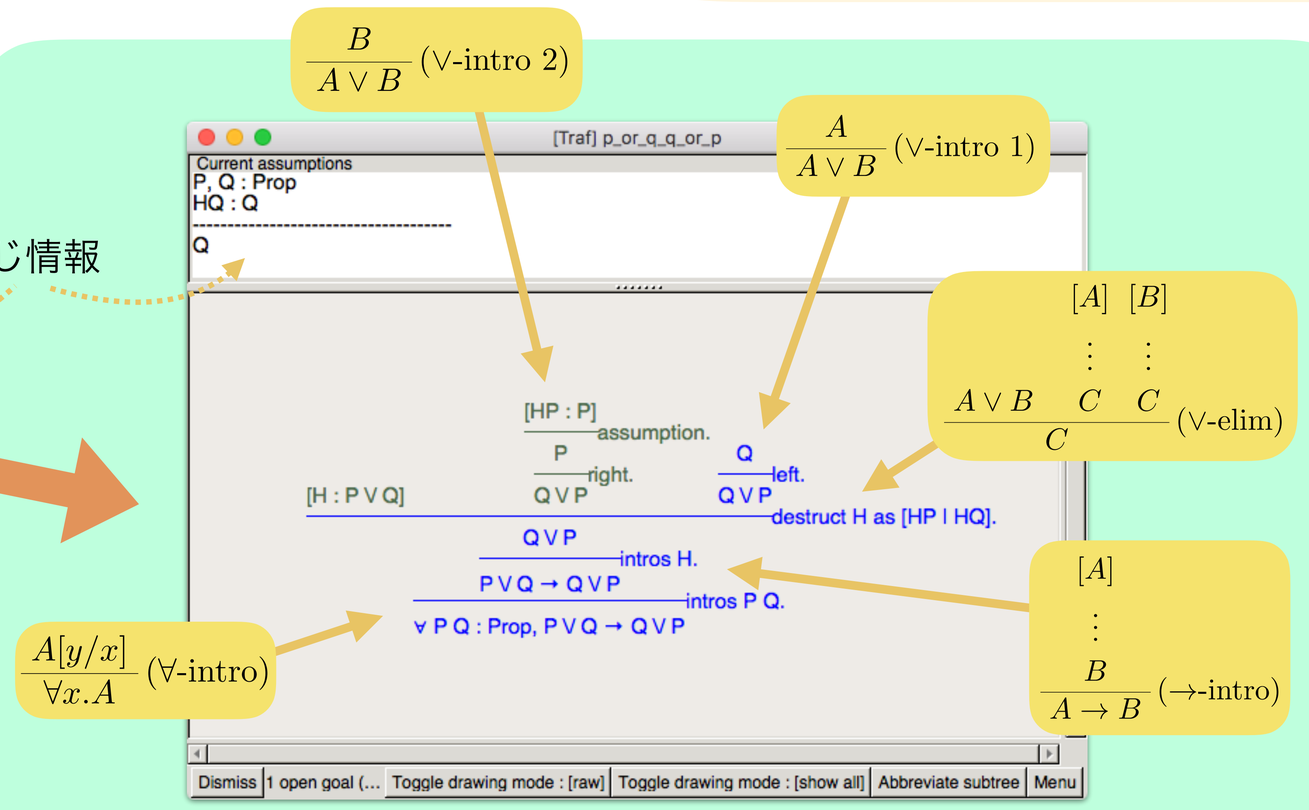
Traf　誰もが使える証明木描画ツール

- ✓ Coqでの対話的証明と連動した証明木描画の実現
- ✓ 自然演繹の証明木の簡略表現・必要十分な情報量
- ✓ prooftree を改造して実現・Proof General 経由で使用
- ✓ LaTeX 組版用記述の出力が可能





同じ情報



$\frac{B}{A \vee B}$ (∨-intro 2)

$\frac{A}{A \vee B}$ (∨-intro 1)

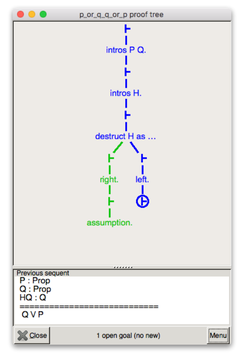
$\frac{[A]\ [B]}{A \vee B \quad C \quad C}$ (∨-elim)

$\frac{A[y/x]}{\forall x.A}$ (∀-intro)

$\frac{[A]}{B}$ (→-intro)

Trafによる証明木描画：自然演繹の証明図のスタイル

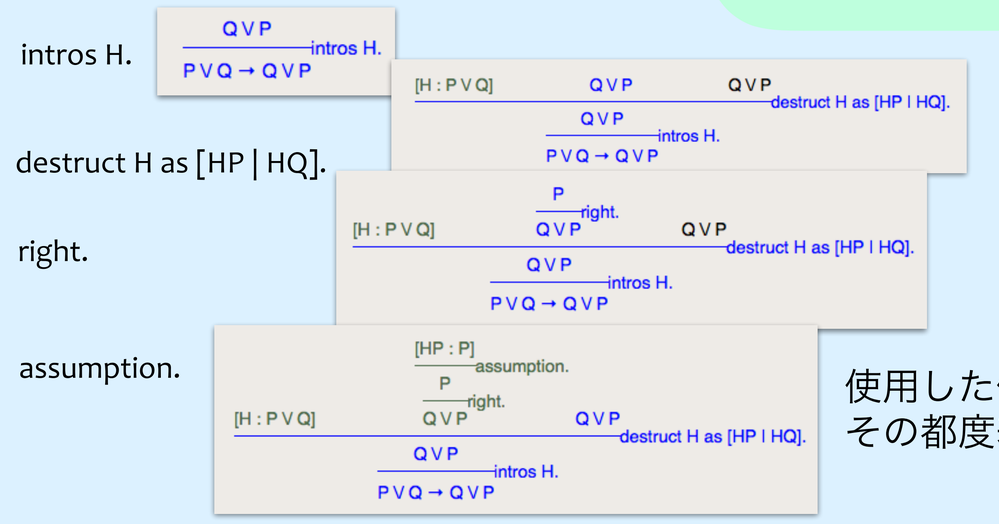
動作環境例
Coq (8.6.1)
Proof General (4.3)
OCaml (4.05.0)
LablGTK2 (2.18.5)
GTK+2 (2.24.31)



prooftree 0.13
の場合

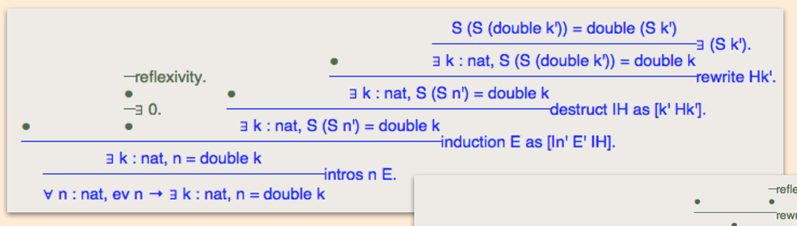
対話的証明の様子

Theorem p_or_q (P Q : Prop) : P ∨ Q → Q ∨ P.



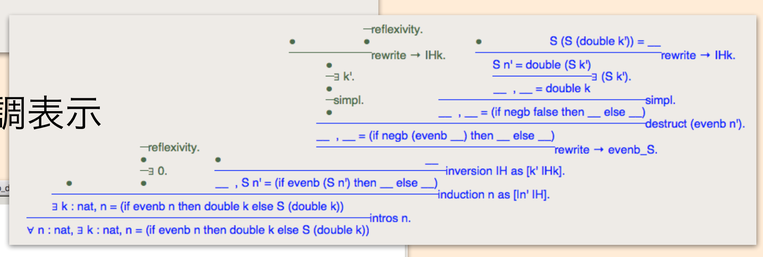
使用した仮定を
その都度表示

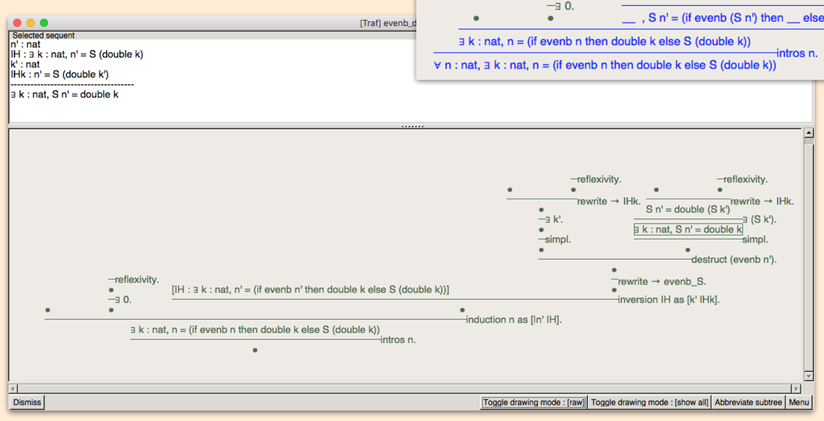
インタラクティブツールならではの機能



カレントゴールへの
パスの表示

変化箇所の強調表示





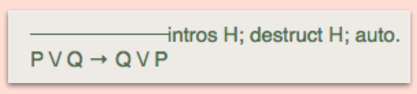
任意箇所の省略

LaTeX 組版用記述の出力機能

$$\dfrac{\dfrac{\dfrac{[\mathrm{HP}\ :\ \mathrm{P}]}{\mathrm{P}}\ \text{assumption.} \quad \dfrac{[\mathrm{HQ}\ :\ \mathrm{Q}]}{\mathrm{Q}}\ \text{assumption.}}{\mathrm{Q}\ \vee\ \mathrm{P}}\ \text{right.} \quad \dfrac{}{\mathrm{Q}\ \vee\ \mathrm{P}}\ \text{left.}}{\mathrm{Q}\ \vee\ \mathrm{P}}\ \text{destruct H as [HP | HQ].}}{\mathrm{P}\ \vee\ \mathrm{Q}\ \rightarrow\ \mathrm{Q}\ \vee\ \mathrm{P}}\ \text{intros H.}}{\forall\ \mathrm{P}\ \mathrm{Q}\ :\ \mathrm{Prop},\ \mathrm{P}\ \vee\ \mathrm{Q}\ \rightarrow\ \mathrm{Q}\ \vee\ \mathrm{P}}\ \text{intros P Q.}$$

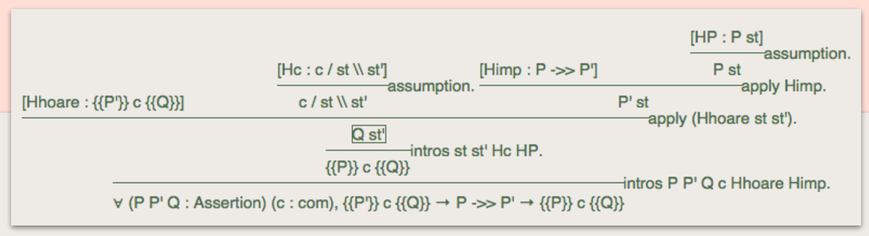
prftreeパッケージを使用

証明木の表示例

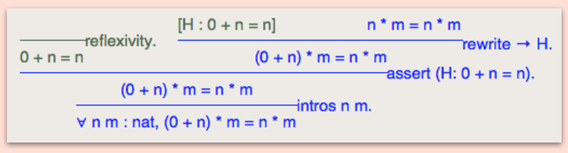


タクティカル / オートメーション

Notation の使用

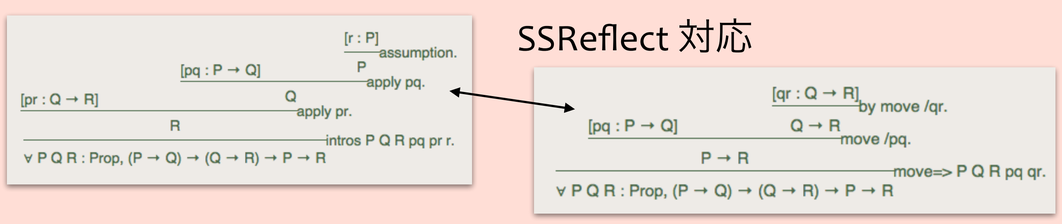


多数の枝分かれ



assert 使用時

SSReflect 対応



今後の課題

- 情報提示手法
  - 仮定の書き換え
  - 長大なコマンドに対する描画方法
  - オートメーション使用時の描画方法
- 複数の証明や定義の相互参照機能
- ユーザ定義構文の把握