

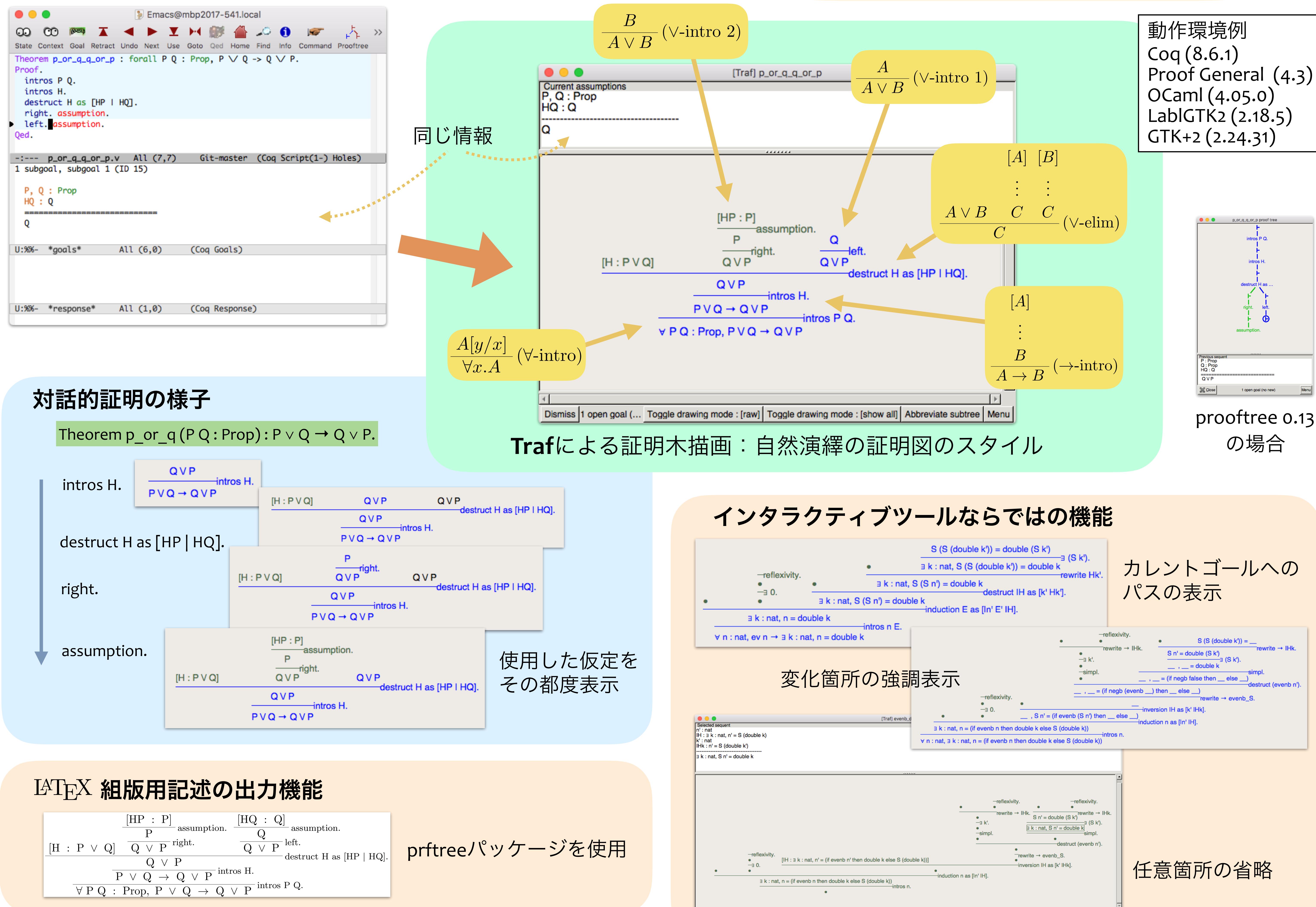
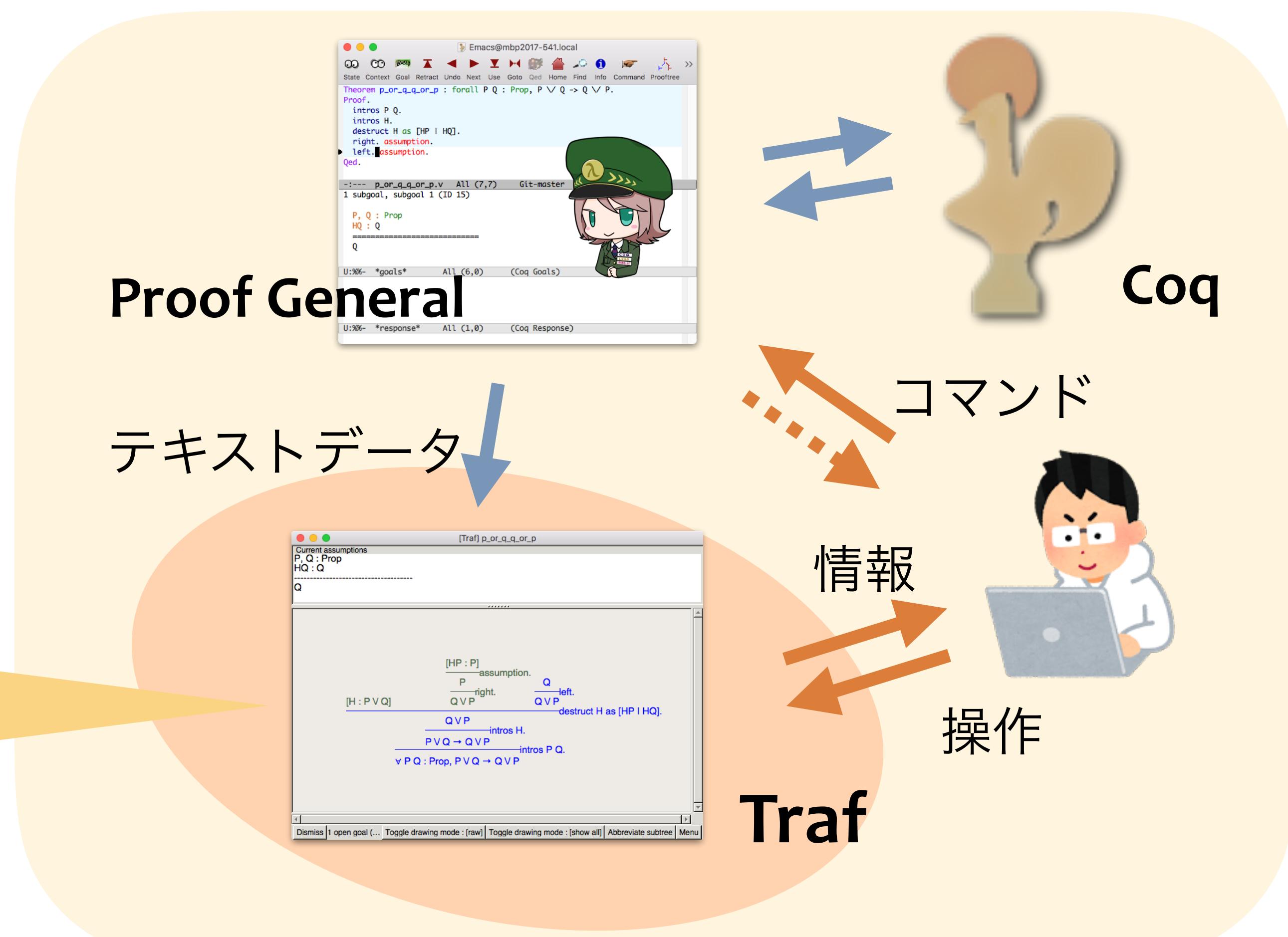
木村 麻衣 田中 雄太* 川端 英之 弘中 哲夫 広島市立大学 (* 現在, 関電システムソリューションズ)

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
 - ✓ L^AT_EX 組版用記述の出力が可能



$\frac{[HP : P]}{P}$ assumption. $\frac{[HQ : Q]}{Q}$ assumption

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

```

graph TD
    A[apply hoare_ski_assumption] --> B[eapply hoare_co...]
    B --> C["{{P}\$ SKIP {{a}}}"]
    C --> D["{{P}\$ extract d1 :: extract d2 {{post d2}}}"]
    D --> E[apply IHd2.]
    E --> F[clear H.]
    F --> G[inversion H as ...]
    G --> H[apply H2.]
    H --> I[apply IH.]
    I --> J[eapply hoare_s]
  
```

· 使用時

intros P Q R.

The diagram illustrates the correspondence between Coq's proof tactic `intros` and SSReflect's move tactic. It consists of two columns separated by a vertical double-headed arrow.

Left Column (Coq):

$$\frac{\frac{\frac{[pq : P \rightarrow Q]}{Q} \quad \frac{[pr : Q \rightarrow R]}{R}}{R} \quad [r : P]}{P} \text{ intros P Q R pq pr r.}$$

- Top rule: $\frac{[r : P]}{P}$ labeled "assumption."
- Middle rule: $\frac{[pr : Q \rightarrow R]}{R}$ labeled "apply pr."
- Bottom rule: $\frac{Q}{\frac{[pq : P \rightarrow Q]}{P}}$ labeled "apply pq."

Right Column (SSReflect):

$$\frac{[pq : P \rightarrow Q]}{P \rightarrow R} \text{ move /pq.}$$

- Top rule: $\frac{[qr : Q \rightarrow R]}{Q \rightarrow R}$ labeled "by move /qr."
- Bottom rule: $\frac{Q \rightarrow R}{P \rightarrow R}$ labeled "move /pq."

A large double-headed arrow connects the two columns, indicating that the proof structures are equivalent.

今後の課題

- ・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