4K-01

定理証明支援系 Coq と連携した証明木図示ツールにおける大域的および局所的な情報把握支援機能の改善

古谷夢都† 川端英之‡ 弘中哲夫‡
広島市立大学情報科学部情報工学科† 広島市立大学大学院情報科学研究科‡

1 はじめに

定理の証明やソフトウェア検証の場面で，形式的に証明する [1] ために定理証明支援系 Coq[2] が広く利用される．Coq を用いた証明スクリプトは，手続き型の記述が行われるため，可読性が高いとは言い難く，証明全体を詳細に見通し確認する行為は労力を要する．我々の研究目的は，Coq を用いて証明を遂行するユーザへの情報の把握支援である．証明木全体の概要を見通す大域的な支援と証明時点のサブゴールに対して推論規則を適用するための局所的な支援の二つの視点での支援が重要である．

大域的もしくは，局所的な情報を個々に支援可能なツール [3][4] は存在する．本稿では，それらの研究と異なり大域的かつ局所的な支援の両立を可能にした証明図示ツールの実現を目標とする．目標を実現するツールとして，大域的かつ局所的な情報支援が可能な Traf[5] が開発されている．しかし，Traf は表記スタイルや仮定に対する識別子の把握支援に対して，改善の余地がある．

我々は，ユーザが手続き的な記述を採用している Coq と対話的に証明を行うにあたって，局所的・大域的な情報把握可能な証明木図示ツールを開発した．

本発表では，証明情報全体を見通しつつ証明情報の細部を把握できる証明木図示ツールの設計と実装について報告する．

2 証明木図示ツール Traf[5]

2.1 Traf の概要

Traf は，ユーザが ProofGeneral を介して Coq と対話的に証明を行うにあたって，証明木を自動的に構築して図示するツールである．ユーザは Traf が図示する証明木を見ることで手続き的な記述である証明スクリプトの証明情報把握を支援される．証明木を図示することで，ユーザに対して手続き的な記述でなされた証明の把握を支援する．

図 1 は，Traf を用いて証明を遂行する様子である．Traf は上方向へ伸びる簡略化された自然演繹の表記スタイルの証明木を採用していて，ユーザが証明木全体の概要を

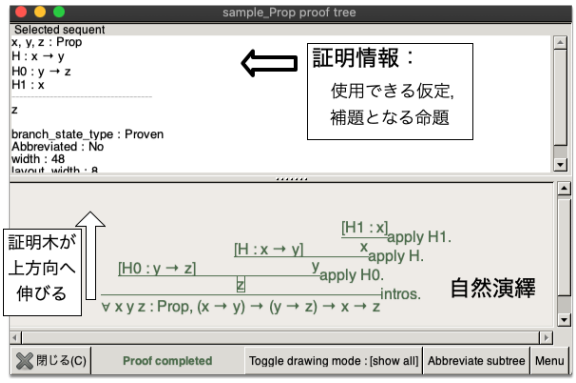

図 1: Coq での証明の際に Traf を用いた様子

図 2: Traf が図示する証明木が極度に横方向へ長い例

見通すことを補助している．Traf が図示する証明木のノードは各時点の論理式やタクティックからなり，ユーザがノードを指定する事で証明情報の確認が可能である．

2.2 Traf の改善

Traf に対して改善すべき点が二点ある．一点目は，証明によって極度に証明木が横方向へ長くなる点である．Traf は部分木を省略する機能を持つが，タクティックの適用で複数のサブゴールが横方向に列挙され，証明木は縦と横の両方向に長くなる．二次元的に大きくなった証明木は，縦と横の両方向のスクロールを行いサブゴールを比較する必要がある．図 2 は証明木が横へ長くなった Traf の出力例である．さらに証明を進めると上方向に証明木が長くなる．

二点目は，仮定に対する識別子の生成と使用関係を把握するための補助が不十分な点である．ユーザが識別子を使用する場面で Traf は対応する仮定の内容を出力するが，認識を容易にするためのハイライト等の補助がない．Coq を用いた証明は，タクティックと公理や仮定を組み合わせ，証明時点のサブゴールに対して推論規則を適用することで進められる．ユーザが仮定の生成箇所を知ることは，その仮定が使用可能な範囲を知り，証明の全体構造を把握する上で重要である．また，証明スクリプトで識別子名を明記せずに使用した場合には，証明スクリプトに識別子名の記載がないため，生成と使用の関係を把握することが困難となる．

Improvement of a Proof Tree Viewer Cooperating with Coq to Help the user Access Global and Local Information of Proofs
Mutsu Furutani† Hideyuki Kawabata‡ Tetsuo Hironaka‡
†Department of Computer and Network Engineering, Hiroshima City University
‡Graduate School of Information Sciences, Hiroshima City University

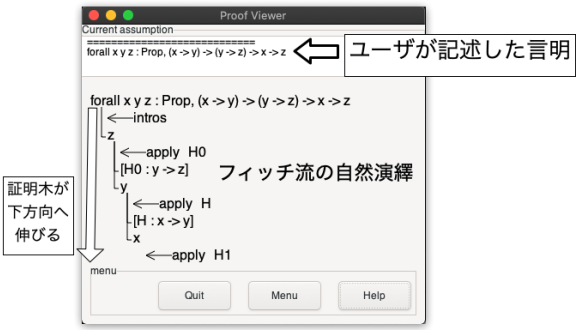

図 3: 改善を施した証明木図示ツールの出力

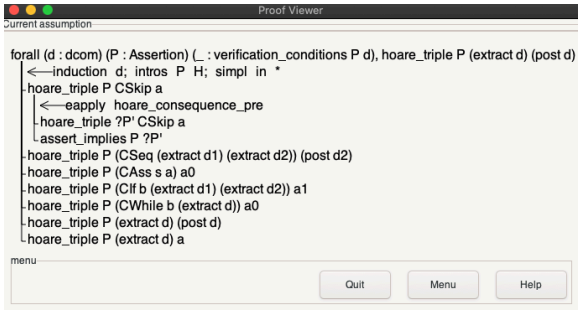

図 4: 証明木が極度に横方向へ長くなる例の改善後の様子

3 情報把握の支援機能を改善した証明木図示ツール

3.1 ツールのシステム構成

本ツールは ProofGeneral，証明木構造構築部，証明木描画部の三部で構成される．ユーザは ProofGeneral を通じて Coq を使用する．証明木構造構築部は ProofGeneral が標準出力する各ステップの証明情報を受け取り証明木の木構造を構築する．証明木描画部は構築された証明木の木構造を受け取りユーザに図示する．

本ツールの証明木構造構築部と証明木描画部は C++[6] を用いて記述され，証明木描画部は GUI ライブラリの Gtk– –[7] を用いて描画している．

3.2 縦並びに基づく証明木表示機能

図 2 のように証明によって極度に証明木が横方向へ長くなる問題を解決するために，本ツールはフィッチ流 (Fitch style)[8] の自然演繹の簡略化した表記スタイルの証明木を採用する．命題やサブゴール，タクティックの記述を縦方向に列挙するフィッチ流の表記スタイルは，横方向の 1 行が一つの意味を表しており，Coq を用いた証明に対して経験の浅い人でも親しみやすいと考えられる．

図 3 は本ツールを用いて証明を遂行する様子を表した図である．言明を画面左上に配置し，「←」の右側に書いた文字列はユーザが記述した証明スクリプトの一部である．命題に対して，推論のために必要な仮定やサブゴールを縦方向に列挙し，線で繋いでいる．

証明木の分岐が発生する場合には，線を用いて複数のサブゴールをつなぎ，サブゴールの左先頭の位置を揃える配置にした．その結果，図 4 のように縦方向へ並列されることで主に縦スクロールでサブゴール間の比較が容易となる．

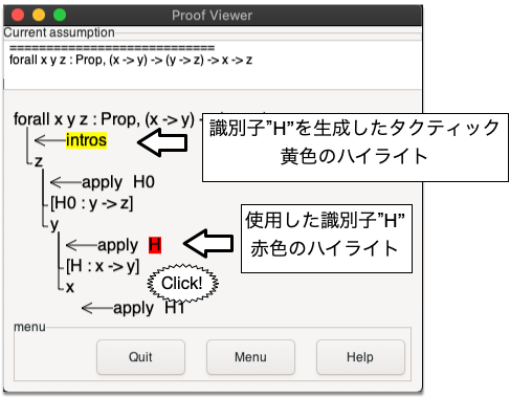

図 5: 使用された識別子をクリックした時の様子

3.3 識別子の生成および使用箇所の提示機能

本ツールでは，識別子名が証明時点において使用可能か判断する補助や，識別子名の生成過程を把握するために識別子名の使用箇所および生成箇所をユーザへ提示する機能を導入した．

図 5 は証明の過程において識別子名の生成と使用の関係をユーザが把握しようとする状況を表した図である．赤色でハイライトされた識別子名 (図では “H”) は，ユーザが指定した識別子名で，黄色でハイライトされたタクティック (図では “intros”) は，指定した識別子名を生成するタクティックである．“simpl in H” の識別子 “H” のような生成と使用の両方の性質を持った識別子を指定すると対応する生成箇所と使用箇所の両方がハイライトされる．

4 まとめと今後の課題

本研究では，表記スタイルと識別子の生成および使用の関係に対する改善を加えた証明木を図示することで，ユーザに対して手続き的な記述でなされた証明の把握を支援するツールを開発した．今後の課題として，被験者実験を行い詳細な評価と考察を行うことが挙げられる．

参考文献

[1] Harrison, J.: Formal Proof – Theory and Practice, *Notices of the American Mathematical Society*, Vol. 55, pp. 1395–1406 (2008).
[2] The Coq Proof Assistant. ⟨https://coq.inria.fr/⟩
[3] 中野恵太: 定理証明支援系 Coq における証明木を操作可能なインタフェースの設計および実装，修士論文，電気通信大学，(2018).
[4] Proof General. ⟨http://proofgeneral.github.io/⟩
[5] Hideyuki Kawabata, Yuta Tanaka, Mai Kimura, Tetsuo Hironaka: Traf: A Graphical Proof Tree Viewer Cooperating with Coq Through Proof General, APLAS 2018, LNCS 11275, pp. 157–165 (2018/12/2).
[6] Stroustrup, B.: *The C++ Programming Language: The C++ Programm Lang_p4* (2013).
[7] Gtk– –.⟨https://www.gtkmm.org/en/⟩
[8] Fitch, F. B.: *Symbolic Logic: An Introduction* (1977).