XII Summer Workshop in Mathematics

Interactively Proving Mathematical Theorems

Section 1: Propositional Deduction

Thaynara Arielly de Lima (IME) UFG

Mauricio Ayala-Rincón (CIC-MAT) UnB

In collaboration with:

Ariane Alves de Almeida and Gabriel Ferreira Silva and Thiago Mendonça Ferreira Ramos

Funded by FAPDF DE grant 00193.0000.2144/2018-81, CNPq Research Grant 307672/2017-4

February 10 - 14, 2020

Talk's Plan

1. Section 1
   - Deduction à la Gentzen
   - The Prototype Verification System (PVS)
   - Exercises - propositional logic
   - Gentzen Deductive Rules vs PVS Proof Commands

Gentzen Calculus

Sequents:

$$\Gamma \quad \Rightarrow \quad \Delta$$

$$\uparrow \qquad\qquad \uparrow$$

antecedent succedent

Gentzen Calculus

Table: RULES OF DEDUCTION *à la* GENTZEN FOR PREDICATE LOGIC

Left rules	Right rules
Axioms:	
$\Gamma, \varphi \Rightarrow \varphi, \Delta \quad (Ax)$	$\bot, \Gamma \Rightarrow \Delta \quad (L_\bot)$
Structural rules:	
$\dfrac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta} \; (LWeakening)$	$\dfrac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi} \; (RWeakening)$
$\dfrac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta} \; (LContraction)$	$\dfrac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi} \; (RContraction)$

Gentzen Calculus

Table: Rules of deduction *à la* Gentzen for predicate logic

Left rules	Right rules
Logical rules:	
$$\frac{\varphi_{i\in\{1,2\}}, \Gamma \Rightarrow \Delta}{\varphi_1 \wedge \varphi_2, \Gamma \Rightarrow \Delta} \; (L_\wedge)$$	$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi} \; (R_\wedge)$$
$$\frac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta} \; (L_\vee)$$	$$\frac{\Gamma \Rightarrow \Delta, \varphi_{i\in\{1,2\}}}{\Gamma \Rightarrow \Delta, \varphi_1 \vee \varphi_2} \; (R_\vee)$$
$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \rightarrow \psi, \Gamma \Rightarrow \Delta} \; (L_\rightarrow)$$	$$\frac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi} \; (R_\rightarrow)$$
$$\frac{\varphi[x/t], \Gamma \Rightarrow \Delta}{\forall_x \varphi, \Gamma \Rightarrow \Delta} \; (L_\forall)$$	$$\frac{\Gamma \Rightarrow \Delta, \varphi[x/y]}{\Gamma \Rightarrow \Delta, \forall_x \varphi} \; (R_\forall), \quad y \notin \mathtt{fv}(\Gamma, \Delta)$$
$$\frac{\varphi[x/y], \Gamma \Rightarrow \Delta}{\exists_x \varphi, \Gamma \Rightarrow \Delta} \; (L_\exists), \quad y \notin \mathtt{fv}(\Gamma, \Delta)$$	$$\frac{\Gamma \Rightarrow \Delta, \varphi[x/t]}{\Gamma \Rightarrow \Delta, \exists_x \varphi} \; (R_\exists)$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \to \psi) \to \psi) \to \psi$

$$\varphi \Rightarrow \varphi \ \ (Ax)$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \to \psi) \to \psi) \to \psi$

$$(RW)\ \frac{\varphi \Rightarrow \varphi \ \ (Ax)}{\varphi \Rightarrow \varphi, \psi}$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \to \psi) \to \psi) \to \psi$

$$
(R_{\to})\ \dfrac{(RW)\ \dfrac{\varphi \Rightarrow \varphi\ \ (Ax)}{\varphi \Rightarrow \varphi, \psi}}{\Rightarrow \varphi, \varphi \to \psi}
$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \to \psi) \to \psi) \to \psi$

$$\dfrac{(RW)\ \dfrac{\varphi \Rightarrow \varphi \ \ (Ax)}{\varphi \Rightarrow \varphi, \psi}}{\Rightarrow \varphi, \varphi \to \psi}\ (R_{\to}) \qquad \varphi \Rightarrow \varphi \ \ (Ax)$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \to \psi) \to \psi) \to \psi$

$$\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi \;\; (Ax)}{\varphi \Rightarrow \varphi, \psi}\,(RW)}{\Rightarrow \varphi, \varphi \to \psi}\,(R_{\to}) \qquad \varphi \Rightarrow \varphi \;\; (Ax)}{(\varphi \to \psi) \to \varphi \Rightarrow \varphi}\,(L_{\to})$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \to \psi) \to \psi) \to \psi$

$$\dfrac{\dfrac{(R_\to)\,\dfrac{(RW)\,\dfrac{\varphi \Rightarrow \varphi \quad (Ax)}{\varphi \Rightarrow \varphi, \psi}}{\Rightarrow \varphi, \varphi \to \psi} \qquad \varphi \Rightarrow \varphi \quad (Ax)}{(\varphi \to \psi) \to \varphi \Rightarrow \varphi}\,(L_\to)}{\Rightarrow ((\varphi \to \psi) \to \varphi) \to \varphi}\,(L_\to)$$

Gentzen Calculus

Cut rule:

$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma' \Rightarrow \Delta'}{\Gamma\Gamma' \Rightarrow \Delta\Delta'} \ (Cut)$$

Gentzen Calculus - dealing with negation: c-equivalence

$$\varphi, \Gamma \Rightarrow \Delta \text{ one-step c-equivalent } \Gamma \Rightarrow \Delta, \neg\varphi$$

$$\Gamma \Rightarrow \Delta, \varphi \text{ one-step c-equivalent } \neg\varphi, \Gamma \Rightarrow \Delta$$

The c-equivalence is the equivalence closure of this relation.

Lemma 1 (One-step c-equivalence)

(i) $\vdash_G \varphi, \Gamma \Rightarrow \Delta$, *iff* $\vdash_G \Gamma \Rightarrow \Delta, \neg\varphi$;

(ii) $\vdash_G \neg\varphi, \Gamma \Rightarrow \Delta$, *iff* $\vdash_G \Gamma \Rightarrow \Delta, \varphi$.

Gentzen Calculus - dealing with negation

Proof.

1. **Necessity**:

$$\dfrac{\dfrac{\varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta, \bot}\,(\mathrm{RW})}{\Gamma \Rightarrow \Delta, \neg\varphi}\,(\mathrm{R}_{\rightarrow})$$

Sufficiency:

$$\dfrac{(\mathrm{LW})\,\dfrac{\Gamma \Rightarrow \Delta, \neg\varphi}{\varphi, \Gamma \Rightarrow \Delta, \neg\varphi} \qquad \dfrac{(Ax)\ \varphi, \Gamma \Rightarrow \Delta, \varphi \qquad \bot, \varphi, \Gamma \Rightarrow \Delta\ (L_{\bot})}{\neg\varphi, \varphi, \Gamma \Rightarrow \Delta}\,(\mathrm{L}_{\rightarrow})}{\varphi, \Gamma \Rightarrow \Delta}\,(\textsc{Cut})$$

Gentzen Calculus - dealing with negation

(ii) **Necessity**:

$$\dfrac{\dfrac{\dfrac{\dfrac{(Ax)\ \varphi, \Gamma \Rightarrow \Delta, \varphi, \varphi, \bot}{\Gamma \Rightarrow \Delta, \varphi, \varphi, \neg\varphi}\,(\mathrm{R}_{\to}) \qquad \bot, \Gamma \Rightarrow \Delta, \varphi, \varphi\ (L_{\bot})}{\neg\neg\varphi, \Gamma \Rightarrow \Delta, \varphi, \varphi}\,(\mathrm{L}_{\to})}{\Gamma \Rightarrow \Delta, \varphi, \neg\neg\varphi \to \varphi}\,(\mathrm{R}_{\to}) \qquad \dfrac{\dfrac{\dfrac{\neg\varphi, \Gamma \Rightarrow \Delta}{\neg\varphi, \Gamma \Rightarrow \Delta, \varphi, \bot}\,(\mathrm{RW})}{\Gamma \Rightarrow \Delta, \varphi, \neg\neg\varphi}\,(\mathrm{R}_{\to}) \qquad \varphi, \Gamma \Rightarrow \Delta, \varphi\ (Ax)}{\neg\neg\varphi \to \varphi, \Gamma \Rightarrow \Delta, \varphi}\,(\mathrm{L}_{\to})}{\Gamma \Rightarrow \Delta, \varphi}\,(\mathrm{CUT})$$

Sufficiency:

$$\dfrac{\Gamma \Rightarrow \Delta, \varphi \qquad \bot, \Gamma \Rightarrow \Delta}{\neg\varphi, \Gamma \Rightarrow \Delta}\,(\mathrm{L}_{\to})$$

□

The Prototype Verification System (PVS)

PVS is a verification system, developed by the SRI International Computer Science Laboratory, which consists of

1. a *specification language*:
   - based on *higher-order logic*;
   - a type system based on Church's simple theory of types augmented with *subtypes* and *dependent types*.
2. an *interactive theorem prover*:
   - based on **sequent calculus**; that is, goals in PVS are sequents of the form $\Gamma \vdash \Delta$, where Γ and Δ are finite sequences of formulae, with the usual Gentzen semantics.

The Prototype Verification System (PVS) — Libraries

- The `prelude` library
  - It is a collection of basic *theories* containing specifications about:
    - functions;
    - sets;
    - predicates;
    - logic; among others.
  - The theories in the prelude library are visible in all PVS contexts;
  - It provides the infrastructure for the PVS typechecker and prover, as well as much of the basic mathematics needed to support specification and verification of systems.

The Prototype Verification System (PVS) — Libraries

- NASA LaRC PVS library (`nasalib`)
  - It includes the *theories*
    - ★ structures, analysis, algebra, graphs, digraphs,
    - ★ real arithmetic, floating point arithmetic, groups, interval arithmetic,
    - ★ linear algebra, measure integration, metric spaces,
    - ★ orders, probability, series, sets, topology,
    - ★ term rewriting systems, unification, etc. etc.
  - The `nasalib` is maintaned by the NASA LaRC formal methods group;
  - The `nasalib` is result of research developed by the NASA LaRC formal methods group and the cientific comunity in general.

Sequent Calculus in PVS

A sequent of the form $\Gamma \vdash \Delta$ (or $A_1, A_2, ..., A_n \vdash B_1, B_2, ..., B_m$, since Γ and Δ are finite sequences of formulae) is:

- interpreted as:
  $A_1 \wedge A_2 \wedge ... \wedge A_n \vdash B_1 \vee B_2 \vee ... \vee B_m$,
  that is, from the conjunction of the antecedent formulae one obtains the disjunction of the succedent formulae.

- represented in PVS as:

$$
\begin{array}{l}
\texttt{[-1]} \; A_1 \\
\vdots \\
\texttt{[-n]} \; A_n \\
\texttt{|----------} \\
\texttt{[1]} \; B_1 \\
\vdots \\
\texttt{[m]} \; B_m
\end{array}
$$

Sequent Calculus in PVS

- Inference rules
  - Premises and conclusions are simultaneously constructed:

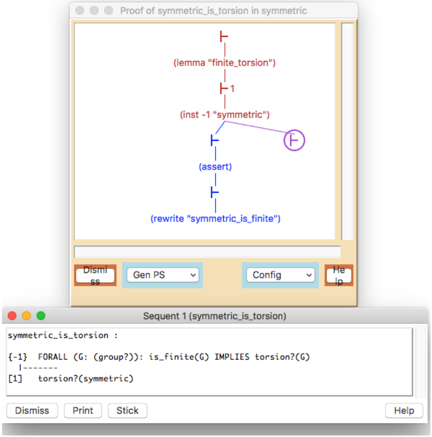
$$\frac{\Gamma \vdash \Delta}{\Gamma' \vdash \Delta'}$$

  - A PVS proof command corresponds to the application of an inference rule. In general:

$$\frac{\Gamma \vdash \Delta}{\Gamma_1 \vdash \Delta_1 \ldots \Gamma_n \vdash \Delta_n} \quad \textbf{(Rule Name)}$$

- Goal: $\vdash \Delta$.

- Proof tree: each node is labelled by a sequent



Some inference rules in PVS

- Structural:

Deduction rule	PVS command
$\dfrac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}$ $(LContraction)$	$\dfrac{\varphi, \Gamma \vdash \Delta}{\varphi, \varphi, \Gamma \vdash \Delta}$ $(copy)$

$$\begin{array}{c} \vdots \\ [-i]\ A \wedge \neg B \\ \vdots \\ |------- \\ \vdots \\ [j]\ \neg C \to D \\ \vdots \end{array} \quad (\texttt{copy} - \texttt{i}) \quad \rightsquigarrow \quad \begin{array}{c} [-1]\ A \wedge \neg B \\ \vdots \\ [-(i+1)]\ A \wedge \neg B \\ \vdots \\ |------- \\ \vdots \\ [j]\ \neg C \to D \\ \vdots \end{array}$$

Some inference rules in PVS

- Structural:

Deduction rule	PVS command
$\dfrac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}$ $(LWeakening)$	$\dfrac{\varphi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}$ $(hide)$

$$
\begin{array}{l}
[-1]\ A \wedge \neg B \\
\quad\vdots \\
[-(i+1)]\ A \wedge \neg B \\
\quad\vdots \\
|-------\\
\quad\vdots \\
[j]\ \neg C \rightarrow D \\
\quad\vdots
\end{array}
\qquad (\mathtt{hide}-(\mathtt{i}+\mathtt{1})) \qquad \rightsquigarrow \qquad
\begin{array}{l}
[-1]\ A \wedge \neg B \\
\quad\vdots \\
|-------\\
\quad\vdots \\
[j]\ \neg C \rightarrow D \\
\quad\vdots
\end{array}
$$

Some inference rules in PVS

- Propositional:

$|-------$

$[1]\ A \wedge B \to (C \vee D \to C \vee (A \wedge C))$

$\downarrow$ (flatten)

$[-1]\ A$

$[-2]\ B$

$[-3]\ C \vee D$

$|-------$

$[1]\ C$

$[2]\ A \wedge C$

Deduction rule		PVS command (*flatten*)
$\dfrac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \to \psi}$	$(R_{\to})$	$\dfrac{\Gamma \vdash \Delta, \varphi \to \psi}{\varphi, \Gamma \vdash \Delta, \psi}$
$\dfrac{\varphi_1, \varphi_2, \Gamma \Rightarrow \Delta}{\varphi_1 \wedge \varphi_2, \Gamma \Rightarrow \Delta}$	$(L_{\wedge})$	$\dfrac{\varphi_1 \wedge \varphi_2, \Gamma \vdash \Delta}{\varphi_{i\in\{1,2\}}, \Gamma \vdash \Delta}$
$\dfrac{\Gamma \Rightarrow \Delta, \varphi_{i\in\{1,2\}}}{\Gamma \Rightarrow \Delta, \varphi_1 \vee \varphi_2}$	$(R_{\vee})$	$\dfrac{\Gamma \vdash \Delta, \varphi_1 \vee \varphi_2}{\Gamma \vdash \Delta, \varphi_1, \varphi_2}$

Some inference rules in PVS

- Propositional:

Deduction rule	PVS command
$\dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \to \psi, \Gamma \Rightarrow \Delta}\ (L_\to)$	$\dfrac{\varphi \to \psi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi \quad \psi, \Gamma \vdash \Delta}\ (split)$

$[-1]\ (A \to B) \to A$

$|------$ (split −1)

$[1]\ A$

$\swarrow \qquad \searrow$

$[-1]\ A$

$|------$

$[1]\ A$

$|------$

$[1]\ A \to B$

$[2]\ A$

Some inference rules in PVS

- Propositional:

$|------$ (case "m ≥ n")

$[1]\ \gcd(m,n) = \gcd(n,m)$

$\rightsquigarrow$

$[-1]\ m \geq n$

$|------$

$[1]\ \gcd(m,n) = \gcd(n,m)$

$|------$

$[1]\ m \geq n$

$[2]\ \gcd(m,n) = \gcd(n,m)$

Some inference rules in PVS

- Propositional - semantics of PVS instructions:

$$\frac{\dfrac{a, \Gamma \,|\!\text{---}\, \Delta, b}{\Gamma \,|\!\text{---}\, \Delta, a \to b}\ (\texttt{flatten}) \qquad \dfrac{\Gamma \,|\!\text{---}\, \Delta, a, c}{\Gamma \,|\!\text{---}\, \Delta, \neg a \to c}\ (\texttt{flatten})}{\Gamma \,|\!\text{---}\, \Delta, \textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ endif}}\ (\texttt{split})$$

$$\frac{\dfrac{a, b, \Gamma \,|\!\text{---}\, \Delta}{a \wedge b, \Gamma \,|\!\text{---}\, \Delta}\ (\texttt{flatten}) \qquad \dfrac{c, \Gamma \,|\!\text{---}\, \Delta, a}{\neg a \wedge c, \Gamma \,|\!\text{---}\, \Delta}\ (\texttt{flatten})}{\textbf{if } a \textbf{ then } b \textbf{ else } c \textbf{ endif}, \Gamma \,|\!\text{---}\, \Delta}\ (\texttt{split})$$

Some inference rules in PVS

- Propositional (propax):

$$\frac{\Gamma, A \,|\!\!-\!\!-\!\!-\; A, \Delta}{} \quad \textbf{(Ax)}$$

$$\frac{\Gamma, FALSE \vdash \Delta}{} \quad \textbf{(FALSE |---)}$$

$$\frac{\Gamma \,|\!\!-\!\!-\!\!-\; TRUE, \Delta}{} \quad \textbf{(}\vdash\textbf{ TRUE)}$$

Exercises - propositional logic

See the file `prop_algebra.pvs` in Exercises directory

Summary - Gentzen Deductive Rules vs Proof Commads

Table: STRUCTURAL LEFT RULES VS PROOF COMMANDS

Structural left rules	PVS commands
$\frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}$ $(LWeakening)$	$\frac{\varphi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}$ $(hide)$
$\frac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}$ $(LContraction)$	$\frac{\varphi, \Gamma \vdash \Delta}{\varphi, \varphi, \Gamma \vdash \Delta}$ $(copy)$

Summary - Gentzen Deductive Rules vs Proof Commads

Table: Structural Right Rules vs Proof Commands

Structural right rules	PVS commands
$\dfrac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi}$ $(RWeakening)$	$\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta}$ $(hide)$
$\dfrac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi}$ $(RContraction)$	$\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \varphi, \varphi}$ $(copy)$

Summary - Gentzen Deductive Rules vs Proof Commads

Table: Logical Left Rules vs Proof Commands

Left rules	PVS commands
$\dfrac{\varphi_1, \varphi_2, \Gamma \Rightarrow \Delta}{\varphi_1 \wedge \varphi_2, \Gamma \Rightarrow \Delta}\ (L_\wedge)$	$\dfrac{\varphi_1 \wedge \varphi_2, \Gamma \vdash \Delta}{\varphi_{i\in\{1,2\}}, \Gamma \vdash \Delta}\ (flatten)$
$\dfrac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta}\ (L_\vee)$	$\dfrac{\varphi \vee \psi, \Gamma \vdash \Delta}{\varphi, \Gamma \vdash \Delta \quad \psi, \Gamma \vdash \Delta}\ (split)$
$\dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \to \psi, \Gamma \Rightarrow \Delta}\ (L_\to)$	$\dfrac{\varphi \to \psi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi \quad \psi, \Gamma \vdash \Delta}\ (split)$

Summary - Gentzen Deductive Rules vs Proof Commads

Table: Logical Right Rules vs Proof Commands

Right rules	PVS commands
$\dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi} \ (R_\wedge)$	$\dfrac{\Gamma \vdash \Delta, \varphi \wedge \psi}{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi} \ (split)$
$\dfrac{\Gamma \Rightarrow \Delta, \varphi_{i \in \{1,2\}}}{\Gamma \Rightarrow \Delta, \varphi_1 \vee \varphi_2} \ (R_\vee)$	$\dfrac{\Gamma \vdash \Delta, \varphi_1 \vee \varphi_2}{\Gamma \vdash \Delta, \varphi_1, \varphi_2} \ (flatten)$
$\dfrac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \to \psi} \ (R_\to)$	$\dfrac{\Gamma \vdash \Delta, \varphi \to \psi}{\varphi, \Gamma \vdash \Delta, \psi} \ (flatten)$