Mechanizing Mathematics

The Prototype Verification System vs Sequent Calculus

Universidad Nacional de Colombia - Sede Manizales

Facultad de Ciencias Exactas y Naturales

Thaynara Arielly de Lima (IME) UFG

Mauricio Ayala-Rincón (CIC-MAT) UnB

Funded by the Brazilian agencies CNPq, grants Universal 409003/21-2; FAPDF, grant DE 00193-00001175/2021-11 and

FAPEG, grant 202310267000223.

May 29 - June 02 , 2023

Talk's Plan

1. The Prototype Verification System (PVS)
   - Gentzen Deductive Rules vs PVS Proof Commands

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 $\mathbf{\Gamma} \vdash \mathbf{\Delta}$, where $\mathbf{\Gamma}$ and $\mathbf{\Delta}$ 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:

```
[-1] A1
  ⋮
[-n] An
|----------
[1] B1
  ⋮
[m] Bm
```

Sequent Calculus in PVS

- Inference rules
  - Premises and conclusions are simultaneously constructed:

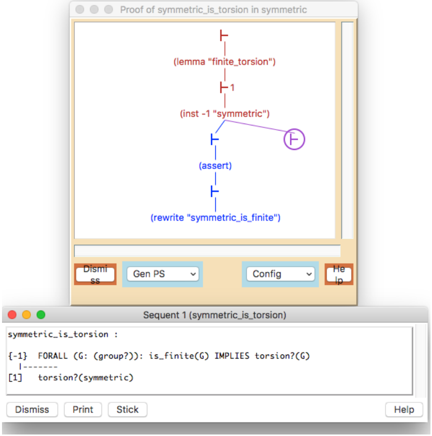
$$\frac{\Gamma \vdash \Delta}{\Gamma' \vdash \Delta'}$$

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

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

- Goal: $\vdash \Delta$.

- Proof tree: each node is labelled by a sequent



Some inference rules in PVS

- Structural:

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

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

Some inference rules in PVS

- Structural:

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

$$[-1]\ A \wedge \neg B$$
$$\vdots$$
$$[-(i+1)]\ A \wedge \neg B$$
$$\vdots$$
$$|-------$$
$$\vdots$$
$$[j]\ \neg C \to D$$
$$\vdots$$

$$(\mathtt{hide} - (\mathtt{i} + \mathtt{1})) \quad \rightsquigarrow$$

$$[-1]\ A \wedge \neg B$$
$$\vdots$$
$$|-------$$
$$\vdots$$
$$[j]\ \neg C \to D$$
$$\vdots$$

Some inference rules in PVS

- Propositional:

$|-------$

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

$\downarrow$ (**flatten**)

$[-1]\ A$

$[-2]\ B$

$[-3]\ C \vee D$

$|-------$

$[1]\ C$

$[2]\ A \wedge C$

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

Some inference rules in PVS

- Propositional:

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

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

$$|------ \qquad (\texttt{split} -1)$$

$$[1]\ A$$

↙ ↘

$$[-1]\ A$$

$$|------$$

$$[1]\ A$$

$$|------$$

$$[1]\ A \to B$$

$$[2]\ A$$

Some inference rules in PVS

- Propositional:

$|-------$ (case "m $\geq$ 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:

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

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

Some inference rules in PVS

- Propositional (propax):

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

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

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

Some inference rules in PVS

- Predicate:

Deduction rule	PVS command
$\dfrac{\varphi[x/y], \Gamma \Rightarrow \Delta}{\exists_x \varphi, \Gamma \Rightarrow \Delta}\ (L_\exists), \quad y \notin \mathtt{fv}(\Gamma, \Delta)$	$\dfrac{\exists_x \varphi, \Gamma \vdash \Delta}{\varphi[x/y], \Gamma \vdash \Delta}\ (skolem), \quad y \notin \mathtt{fv}(\Gamma, \Delta)$
$\dfrac{\varphi[x/t], \Gamma \Rightarrow \Delta}{\forall_x \varphi, \Gamma \Rightarrow \Delta}\ (L_\forall)$	$\dfrac{\forall_x \varphi, \Gamma \vdash \Delta}{\varphi[x/t], \Gamma \vdash \Delta}\ (inst)$

$[-1]\ \forall_{x:T} : P(x)$

$[-2]\ \exists_{x:T} : \neg P(x)$ $\quad$ (skolem −2 "z") $\quad \rightsquigarrow \quad$ $[-1]\ \forall_{x:T} : P(x)$

|---

$[1]\ P(z)$

$[-1]\ \forall_{x:T} : P(x)$

|--- $\quad$ (inst −1 "z") $\quad \rightsquigarrow \quad$ $\left([-1]\ P(z) \quad |\text{---} \quad [1]\ P(z) \right)$ Q.E.D.

$[1]\ P(z)$

Summary - Gentzen Deductive Rules vs Proof Commads

Table: Structural Left Rules vs Proof Commands

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

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
$\dfrac{\varphi_1, \varphi_2, \Gamma \Rightarrow \Delta}{\varphi_1 \wedge \varphi_2, \Gamma \Rightarrow \Delta} \ (L_\wedge)$	$\dfrac{\varphi_1 \wedge \varphi_2, \Gamma \vdash \Delta}{\varphi_{i \in \{1,2\}}, \Gamma \vdash \Delta} \ (flatten)$
$\dfrac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta} \ (L_\vee)$	$\dfrac{\varphi \vee \psi, \Gamma \vdash \Delta}{\varphi, \Gamma \vdash \Delta \quad \psi, \Gamma \vdash \Delta} \ (split)$
$\dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \rightarrow \psi, \Gamma \Rightarrow \Delta} \ (L_\rightarrow)$	$\dfrac{\varphi \rightarrow \psi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi \quad \psi, \Gamma \vdash \Delta} \ (split)$
$\dfrac{\varphi[x/t], \Gamma \Rightarrow \Delta}{\forall_x \varphi, \Gamma \Rightarrow \Delta} \ (L_\forall)$	$\dfrac{\forall_x \varphi, \Gamma \vdash \Delta}{\varphi[x/t], \Gamma \vdash \Delta} \ (inst)$
$\dfrac{\varphi[x/y], \Gamma \Rightarrow \Delta}{\exists_x \varphi, \Gamma \Rightarrow \Delta} \ (L_\exists), \quad y \notin \mathtt{fv}(\Gamma, \Delta)$	$\dfrac{\exists_x \varphi, \Gamma \vdash \Delta}{\varphi[x/y], \Gamma \vdash \Delta} \ (skolem), \quad y \notin \mathtt{fv}(\Gamma, \Delta)$

Summary - Gentzen Deductive Rules vs Proof Commads

Table: Logical Right Rules vs Proof Commands

Right rules	PVS commands
$\dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}\ (R_\wedge)$	$\dfrac{\Gamma \vdash \Delta, \varphi \wedge \psi}{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi}\ (split)$
$\dfrac{\Gamma \Rightarrow \Delta, \varphi_{i\in\{1,2\}}}{\Gamma \Rightarrow \Delta, \varphi_1 \vee \varphi_2}\ (R_\vee)$	$\dfrac{\Gamma \vdash \Delta, \varphi_1 \vee \varphi_2}{\Gamma \vdash \Delta, \varphi_1, \varphi_2}\ (flatten)$
$\dfrac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi}\ (R_\rightarrow)$	$\dfrac{\Gamma \vdash \Delta, \varphi \rightarrow \psi}{\varphi, \Gamma \vdash \Delta, \psi}\ (flatten)$
$\dfrac{\Gamma \Rightarrow \Delta, \varphi[x/y]}{\Gamma \Rightarrow \Delta, \forall_x \varphi}\ (R_\forall), \quad y \notin \mathtt{fv}(\Gamma, \Delta)$	$\dfrac{\Gamma \vdash \Delta, \forall_x \varphi}{\Gamma \vdash \Delta, \varphi[x/y]}\ (skolem), \quad y \notin \mathtt{fv}(\Gamma, \Delta)$
$\dfrac{\Gamma \Rightarrow \Delta, \varphi[x/t]}{\Gamma \Rightarrow \Delta, \exists_x \varphi}\ (R_\exists)$	$\dfrac{\Gamma \vdash \Delta, \exists_x \varphi}{\Gamma \vdash \Delta, \varphi[x/t]}\ (inst)$

Summary - Completing the GC vs PVS rules

	(hide)	(copy)	(flatten)	(split)	(skolem)	(inst)	(lemma) (case) $\times$
(LW)	$\times$						
(LC)		$\times$					
$(L_\wedge)$			$\times$				
$(L_\vee)$				$\times$			$\times$
$(L_\rightarrow)$				$\times$			
$(L_\forall)$						$\times$	
$(L_\exists)$					$\times$		
(RW)	$\times$						
(RC)		$\times$					
$(R_\wedge)$				$\times$			
$(R_\vee)$			$\times$				
$(R_\rightarrow)$			$\times$				
$(R_\forall)$					$\times$		
$(R_\exists)$						$\times$	
(Cut)							$\times$