

Sequent Calculus & PVS

©2001 M. Lawford

Review: Key Results used by PVS

Commutative & Associative rules for \wedge, \vee

Implication: $\models (\phi \rightarrow \psi) \leftrightarrow \neg\phi \vee \psi$

Iff: $\models (\phi \leftrightarrow \psi) \leftrightarrow (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$

Double negation: $\models \phi \leftrightarrow \neg(\neg\phi)$

Identity rules: $\models \phi \wedge \top \leftrightarrow \phi, \models \phi \vee \perp \leftrightarrow \phi$

Dominance rules: $\models \phi \vee \top \leftrightarrow \top, \models \phi \wedge \perp \leftrightarrow \perp$

Rule of adjunction: $\wedge i$

$\Gamma \vdash \psi \wedge \chi$ iff $\Gamma \vdash \psi$ and $\Gamma \vdash \chi$

Rule of alternative proof: $\vee e$

$\Gamma, \phi \vee \psi \vdash \chi$ iff $\Gamma, \phi \vdash \chi$ and $\Gamma, \psi \vdash \chi$

and Theorems:

Deduction Theorem: $\Gamma, \phi \vdash \psi$ iff $\Gamma \vdash \phi \rightarrow \psi$

Completeness & Consistency: $\Gamma \vdash \psi$ iff $\Gamma \models \psi$

2

Outline

- Review
- Order of precedence & logical operators in PVS
- Sequent Calculus
- PVS commands: (FLATTEN), (SPLIT) & (BDDSIMP)
- Checking validity of arguments
- Checking consistency of premises
- Unprovable sequents & counter examples

1

	introduction	elimination
\wedge	$\frac{\phi \quad \psi}{\phi \wedge \psi} \wedge i$	$\frac{\phi \wedge \psi}{\phi} \wedge e_1 \quad \frac{\phi \wedge \psi}{\psi} \wedge e_2$
\vee	$\frac{\phi}{\phi \vee \psi} \vee i_1 \quad \frac{\psi}{\phi \vee \psi} \vee i_2$	$\frac{\begin{array}{ c } \hline \phi \\ \vdots \\ \chi \\ \hline \end{array} \quad \begin{array}{ c } \hline \psi \\ \vdots \\ \chi \\ \hline \end{array}}{\phi \vee \psi \quad \chi} \vee e$
\rightarrow	$\frac{\phi \quad \phi \rightarrow \psi}{\psi} \rightarrow e$	$\frac{\begin{array}{ c } \hline \phi \\ \vdots \\ \psi \\ \hline \end{array}}{\phi \rightarrow \psi} \rightarrow i$
\leftrightarrow	$\frac{\phi \rightarrow \psi \quad \psi \rightarrow \phi}{\phi \leftrightarrow \psi} \leftrightarrow i$	$\frac{\phi \leftrightarrow \psi}{\phi \rightarrow \psi} \leftrightarrow e_1 \quad \frac{\phi \leftrightarrow \psi}{\psi \rightarrow \phi} \leftrightarrow e_2$
\neg	$\frac{\begin{array}{ c } \hline \phi \\ \vdots \\ \perp \\ \hline \end{array}}{\neg\phi} \neg i$	$\frac{\phi \quad \neg\phi}{\perp} \neg e$
$\neg\neg$	$\frac{\phi}{\neg\neg\phi} \neg\neg i$	$\frac{\neg\neg\phi}{\phi} \neg\neg e$
\perp	see $\neg e$	$\frac{\perp}{\phi} \perp e$

3

Order of Precedence in PVS

Recall: We use precedence of logical connectives and associativity of $\wedge, \vee, \leftrightarrow$ to drop parentheses it is understood that this is shorthand for the fully parenthesized expressions.

Rubin uses order of precedence:

$$\neg, \wedge, \rightarrow, \vee, \leftrightarrow$$

PVS uses order of precedence:

$$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$$

Additional Proof Rules

$$\frac{\phi \rightarrow \psi}{\neg\phi \vee \psi} \rightarrow 2V \quad \frac{\neg\phi \vee \psi}{\phi \rightarrow \psi} \vee 2 \rightarrow$$

$$\frac{\phi \rightarrow \psi \quad \neg\psi}{\neg\phi} \text{MT}$$

$$\frac{\boxed{\begin{array}{c} \neg\phi \\ \vdots \\ \perp \end{array}}}{\phi} \text{RAA}$$

$$\frac{}{\phi \vee \neg\phi} \text{LEM}$$

Logical Operators in PVS

Propositional constants and variables have type "bool" in PVS

bool={TRUE, FALSE}

\neg - NOT, not

\wedge - AND, and, &

\vee - OR, or

\rightarrow - IMPLIES, implies, \Rightarrow

\leftrightarrow - IFF, iff, \Leftrightarrow

Sequent Calculus

$\phi_1, \phi_2, \dots, \phi_n \vdash \psi_1 \vee \psi_2 \vee \dots \vee \psi_m$
 is another way of stating
 $\phi_1 \wedge \phi_2 \wedge \dots \wedge \phi_n \vdash \psi_1 \vee \psi_2 \vee \dots \vee \psi_m$

In sequent calculus it is written as:

$$\frac{\begin{array}{c} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{array}}{\begin{array}{c} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_m \end{array}}$$

There are implicit \wedge 's between the premises and implicit \vee 's between the conclusions.

Assuming all the ϕ_i 's are true, we are trying to prove at least one ψ_j is true.

Def: We call $\phi_1 \wedge \dots \wedge \phi_n \rightarrow \psi_1 \vee \dots \vee \psi_m$ the *characteristic formula* for the sequent because it is a tautology iff $\phi_1, \dots, \phi_n \vdash \psi_1 \vee \dots \vee \psi_m$

Sequent Calculus Special Cases

No premises: $\frac{}{\psi_1 \vdash \psi_1 \vee \dots \vee \psi_m}$

No conclusions: $\frac{\phi_1 \vdash \perp}{\phi_1 \wedge \dots \wedge \phi_n \vdash \perp}$

You can always add/remove TRUE (\top) to/from the premises or FALSE (\perp) to/from the conclusions without changing the meaning of the sequent.

Why? Hint: Identity laws

Proofs in Sequent Calculus

Proofs are done by transforming the sequent until one of the following forms is obtained:

$$\frac{\begin{array}{c} \dots \\ \phi \\ \dots \end{array}}{\phi} \text{ i.e. } \Gamma, \phi \vdash \phi \vee \dots$$

which is a case of Rule Premise and $\forall i_1$

$$\frac{}{\top} \text{ i.e. } \Gamma \vdash \top \vee \dots$$

which is a case of Dominance of \top

$$\frac{}{\perp} \text{ i.e. } \Gamma, \perp \vdash \dots$$

Which is a case of \perp_e .

PVS commands: (FLATTEN)

(FLATTEN) eliminates \wedge in the premises (by \wedge_e) and \vee in the conclusions (by $\forall i_1, \forall i_2$):

$$\frac{\begin{array}{c} \phi_1 \wedge \phi_2 \\ \vdots \\ \psi_1 \vee \psi_2 \\ \vdots \end{array}}{\vdots} \text{ becomes } \frac{\begin{array}{c} \phi_1 \\ \phi_2 \\ \vdots \\ \psi_1 \\ \psi_2 \\ \vdots \end{array}}{\vdots}$$

(FLATTEN) also eliminates \rightarrow in the conclusions:

$$\frac{\phi}{\psi_1 \rightarrow \psi_2} \text{ becomes } \frac{\phi}{\psi_1} \vdash \psi_2$$

Why?

PVS commands: (FLATTEN)

(FLATTEN) eliminates negations:

$$\frac{\begin{array}{|l} \phi_1 \\ \hline \neg\psi \\ \psi_1 \\ \psi_2 \end{array}}{\text{becomes}} \frac{\begin{array}{|l} \phi_1 \\ \hline \psi \\ \psi_1 \\ \psi_2 \end{array}}$$

Why? $\phi_1 \vdash \neg\psi \vee \psi_1 \vee \psi_2$ iff $\phi_1 \vdash \psi \rightarrow (\psi_1 \vee \psi_2)$
 iff $\phi_1, \psi \vdash \psi_1 \vee \psi_2$

Similarly $\phi_1, \neg\phi \vdash \psi_1 \vee \psi_2$ iff $\phi_1 \vdash \neg\phi \rightarrow \psi_1 \vee \psi_2$
 iff $\phi_1 \vdash \neg\phi \vee (\psi_1 \vee \psi_2)$ iff $\phi_1 \vdash \phi \vee (\psi_1 \vee \psi_2)$

$$\frac{\begin{array}{|l} \phi_1 \\ \hline \neg\phi \\ \psi_1 \\ \psi_2 \end{array}}{\text{becomes}} \frac{\begin{array}{|l} \phi_1 \\ \hline \phi \\ \psi_1 \\ \psi_2 \end{array}}$$

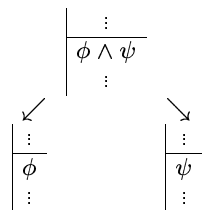
(SPLIT) also splits \leftrightarrow in the conclusions since:

$$(\phi \leftrightarrow \psi) \equiv (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$$

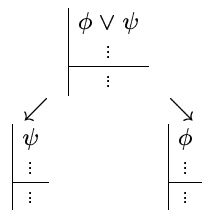
and splits \rightarrow in the premises (why?).

PVS commands: (SPLIT)

(SPLIT) uses "AND introduction" ($\wedge i$) to "split" a \wedge in the conclusions into two subproofs (i.e. $\Gamma \vdash \phi \wedge \psi$ iff $\Gamma \vdash \phi$ and $\Gamma \vdash \psi$)



(SPLIT) uses "OR elimination" ($\vee e$) to "split" a \vee in the premises into two subproofs (i.e. $\Gamma, \phi \vee \psi \vdash r$ iff $\Gamma, \phi \vdash r$ and $\Gamma, \psi \vdash r$)



PVS commands: (BDDSIMP)

The BDDSIMP command, in effect,

1. creates the truth table for the characteristic formula of the sequent. If it is a tautology the proof is done because

$$\models \phi \rightarrow \psi \text{ iff } \vdash \phi \rightarrow \psi \text{ iff } \phi \vdash \psi$$

(take $\phi : \phi_1 \wedge \dots \wedge \phi_n$ and $\psi : \psi_1 \vee \dots \vee \psi_m$).
 Otherwise BDDSIMP

2. obtains the CNF representation,
3. simplifies it with the help of the distributive law, and
4. applies the Rule of Adjunction to split the sequent into one sub-proof for each uninterrupted sequence of disjuncts and flattens all negations.

NOTE: BDDs - (ordered) Binary Decision Diagrams, are type of data structure representing a formula that can be algorithmically reduced to a canonical representation.

(BDDSIMP) Example

Applying (BDDSIMP) to sequent $\vdash p \rightarrow q \wedge r$:

1. Create Truth Table for $p \rightarrow q \wedge r$.
2. Get DNF for $\neg(p \rightarrow q \wedge r)$ then negate and "De Morgan it to death" to get (full) CNF or write down CNF directly:

$$(\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$$

3. Simplify to: $(\neg p \vee q) \wedge (\neg p \vee r)$
4. Split to get $\frac{}{\neg p \vee q}$ and $\frac{}{\neg p \vee r}$ then

$$\text{flatten to } \frac{p}{q} \text{ and } \frac{p}{r}$$

15

Checking Validity of Arguments in PVS

By Theorems on Soundness and Completeness

$$\phi_1, \phi_2, \dots, \phi_n \models \psi \text{ iff} \\ \models \phi_1 \wedge \dots \wedge \phi_n \rightarrow \psi$$

i.e. $\phi_1 \wedge \dots \wedge \phi_n \rightarrow \psi$ is a tautology.

Therefore to check if ϕ_1, \dots, ϕ_n are a valid argument for ψ , use PVS to prove the theorem:

V1: THEOREM $\phi_1 \& \dots \& \phi_n$ IMPLIES ψ

16

Fill in details of $\vdash p \rightarrow q \wedge r$ (BDDSIMP) example.

15

Checking Consistency of Premises in PVS

The set of premises ϕ_1, \dots, ϕ_n is inconsistent iff $\phi_1, \dots, \phi_n \vdash \psi \wedge \neg \psi$ for some ψ iff $\phi_1, \dots, \phi_n \vdash \perp$

But then by the deduction theorem ($\rightarrow i$):

$$\vdash \phi_1 \rightarrow (\phi_2 \rightarrow (\phi_3 \rightarrow (\dots \rightarrow (\phi_n \rightarrow \perp) \dots))) \\ \text{iff} \\ \vdash \phi_1 \wedge \phi_2 \wedge \phi_3 \dots \wedge \phi_n \rightarrow \perp \\ \text{iff} \\ \vdash \neg(\phi_1 \wedge \phi_2 \wedge \phi_3 \dots \wedge \phi_n)$$

Therefore propositional premises ϕ_1, \dots, ϕ_n are inconsistent iff you can prove the PVS theorem:

V1: THEOREM $\phi_1 \& \dots \& \phi_n$ IMPLIES *FALSE* or equivalently

V2: THEOREM $\neg(\phi_1 \& \dots \& \phi_n)$

17

Unprovable Sequents & Counter Examples

Consider the following example:

Use PVS to check if the argument following argument is valid & find a counter example if it is not:

$$q \rightarrow m \vee v, m, v \rightarrow q \stackrel{?}{=} q$$

E1 : THEOREM (q IMPLIES m OR v) & m & (v IMPLIES q) IMPLIES q

Trying (BDDSIMP) gives unprovable sequent.

```
{-1}  m
      |-----
{1}   q
{2}   v
```

which has characteristic formula $m \rightarrow (q \vee v)$. This formula is false when $m = T$ and $q = v = F$. Check that this provides a counter example showing the argument is not valid.

18

Applying disjunctive simplification to flatten sequent, this simplifies to:
a2i :

```
{-1} ((p => q) => q)
{-2} (q => p)
      |-----
{1}  p
```

Note that if

```
(p -> q) -> q, (q -> p) ⊢ p
      Then by → i
      (p -> q) -> q ⊢ (q -> p) -> p
And also by → i
      ⊢ (p -> q) -> q
      → ((q -> p) -> p)
```

Thus it suffices to show

```
(p -> q) -> q, (q -> p) ⊢ p
```

20

Example: Understanding PVS

Use PVS to show:

$$\vdash ((p \rightarrow q) \rightarrow q) \rightarrow ((q \rightarrow p) \rightarrow p)$$

Explain the proof steps.

Solution: In PVS file we have

```
p,q:bool
a2i:theorem ((p=>q)=>q)=>((q=>p)=> p)
```

Invoking the prover:

```
|-----
{1} ((p => q) => q) => ((q => p) => p)
```

Rule? (FLATTEN)

19

a2i :

```
{-1} ((p => q) => q)
{-2} (q => p)
      |-----
{1}  p
```

Rule? (SPLIT -1)
Splitting conjunctions,
this yields 2 subgoals:
a2i.1 :

```
{-1} q
[-2] (q => p)
      |-----
[1]  p
```

Rule? (SPLIT)

21

Splitting conjunctions,
this yields 2 subgoals:
a2i.1.1 :

```
{-1} p
[-2] q
 |-----
[1]  p
```

which is trivially true.
This completes the proof of a2i.1.1.

a2i.1.2 :

```
[-1] q
 |-----
{1}  q
[2]  p
```

which is trivially true.
This completes the proof of a2i.1.2.
This completes the proof of a2i.1.

22

This completes the proof of a2i.1.
a2i.2.2 :

```
|-----
{1}  q
[2]  (p => q)
[3]  p
```

Rule? (flatten)
Applying disjunctive simplification
to flatten sequent.

This completes the proof of a2i.2.2.

This completes the proof of a2i.2.

Q.E.D.

©2001 M. Lawford

a2i.2 :

```
[-1] (q => p)
 |-----
{1}  (p => q)
[2]  p
```

Rule? (split -1)
Splitting conjunctions,
this yields 2 subgoals:
a2i.2.1 :

```
{-1} p
 |-----
[1]  (p => q)
[2]  p
```

which is trivially true.
This completes the proof of a2i.2.1.

23