Tema 1: Cálculo proposicional en PVS

José A. Alonso Jiménez

Jose-Antonio.Alonso@cs.us.es
http://www.cs.us.es/∼jalonso

Dpto. de Ciencias de la Computación e Inteligencia Artificial

Universidad de Sevilla

Historia de PVS

- **PVS:**
  - Nombre: ***P**rototype **V**erification **S**ystem*
  - Autores: N. Shankar, S. Owre y J.M. Rushby (SRI, USA)
  - Def: “PVS is a verification system: that is, a specification language integrated with support tools and a theorem prover”
  - Historia: HDM (70), EHDM (84), PVS (91), PVS 2.4 (25-Nov-2001), PVS 3.0
- **Propósitos:**
  - The primary purpose of PVS is to provide formal support for conceptualization and debugging in the early stages of the lifecycle of the design of a hardware or software system
  - The primary emphasis in the PVS proof checker is on supporting the construction of readable proofs

El cálculo de secuentes proposicional

- **La sintaxis y la semántica proposicional**
- **Secuentes proposicionales**
  - Sintaxis: $\mathbf{\Gamma \Longrightarrow \Delta}$, con $\mathbf{\Gamma}$ y $\mathbf{\Delta}$ conjuntos de fórmulas proposicionales
  - Semántica de $\mathbf{\Gamma \Longrightarrow \Delta}$: $\bigwedge \mathbf{\Gamma} \to \bigvee \mathbf{\Delta}$
  - Antecedente de $\mathbf{\Gamma \Longrightarrow \Delta}$: $\mathbf{\Gamma}$
  - Consecuente de $\mathbf{\Gamma \Longrightarrow \Delta}$: $\mathbf{\Delta}$
- **Axiomas**

$$\frac{}{\mathbf{\Gamma}, \boldsymbol{A} \Longrightarrow \boldsymbol{A}, \mathbf{\Delta}}\ [\mathbf{Ax}]$$

El cálculo de secuentes proposicional

- Reglas

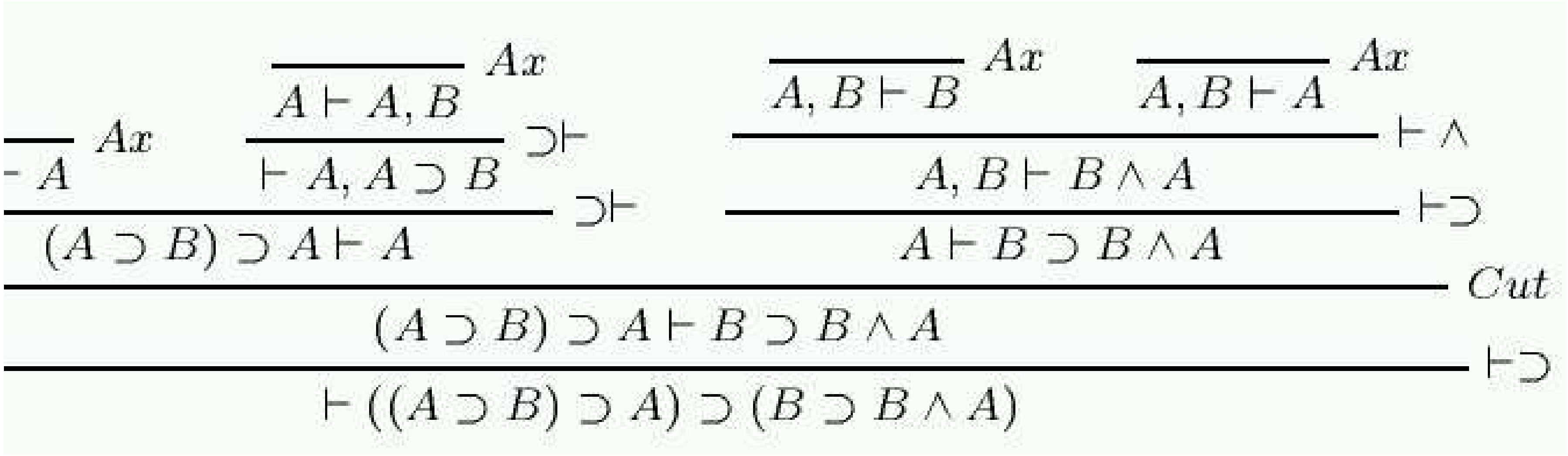
Izquierda	Derecha
$\dfrac{\Gamma \Longrightarrow A, \Delta}{\Gamma, \neg A \Longrightarrow \Delta}$ [¬I]	$\dfrac{\Gamma, A \Longrightarrow \Delta}{\Gamma \Longrightarrow \neg A, \Delta}$ [¬D]
$\dfrac{\Gamma, A \Longrightarrow \Delta \quad \Gamma, B \Longrightarrow \Delta}{\Gamma, A \vee B \Longrightarrow \Delta}$ [∨I]	$\dfrac{\Gamma \Longrightarrow A, B, \Delta}{\Gamma \Longrightarrow A \vee B, \Delta}$ [∨D]
$\dfrac{\Gamma, A, B \Longrightarrow \Delta}{\Gamma, A \wedge B \Longrightarrow \Delta}$ [∧I]	$\dfrac{\Gamma \Longrightarrow A, \Delta \quad \Gamma \Longrightarrow B, \Delta}{\Gamma \Longrightarrow A \wedge B, \Delta}$ [∧D]
$\dfrac{\Gamma, B \Longrightarrow \Delta \quad \Gamma \Longrightarrow A, \Delta}{\Gamma, A \rightarrow B \Longrightarrow \Delta}$ [→I]	$\dfrac{\Gamma, A \Longrightarrow B, \Delta}{\Gamma \Longrightarrow A \rightarrow B, \Delta}$ [→D]
$\dfrac{\Gamma, A \rightarrow B, B \rightarrow A \Longrightarrow \Delta}{\Gamma, A \leftrightarrow B \Longrightarrow \Delta}$ [↔I]	$\dfrac{\Gamma \Longrightarrow A \rightarrow B, \Delta \quad \Gamma \Longrightarrow B \rightarrow A, \Delta}{\Gamma \Longrightarrow A \leftrightarrow B, \Delta}$ [↔D]

$$\frac{\Gamma, \Longrightarrow A, \Delta \quad \Gamma, A \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta} \ \text{[Corte]}$$

Demostraciones

$$\dfrac{\dfrac{\dfrac{}{A \vdash B, A}\,Ax}{A \vdash B \vee A}\,\vdash \vee}{\vdash A \supset (B \vee A)}\,\vdash \supset \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash B}\,Ax \qquad \dfrac{}{A \vdash A, B}\,Ax}{A, A \supset B \vdash B}\,\supset \vdash}{A \wedge (A \supset B) \vdash B}\,\wedge \vdash}{\vdash (A \wedge (A \supset B)) \supset B}\,\vdash \supset$$

Demostraciones con corte



$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A}\,Ax \qquad \dfrac{\dfrac{}{A \vdash A, B}\,Ax}{\vdash A, A \supset B}\,\supset\vdash}{(A \supset B) \supset A \vdash A}\,\supset\vdash \qquad \dfrac{\dfrac{\dfrac{}{A, B \vdash B}\,Ax \qquad \dfrac{}{A, B \vdash A}\,Ax}{A, B \vdash B \wedge A}\,\vdash\wedge}{A \vdash B \supset B \wedge A}\,\vdash\supset}{(A \supset B) \supset A \vdash B \supset B \wedge A}\,Cut}{\vdash ((A \supset B) \supset A) \supset (B \supset B \wedge A)}\,\vdash\supset$$

Teoría PVS

```
proposicional: THEORY
 BEGIN

  A, B, C: bool

  ej1: LEMMA
   A IMPLIES (B OR A)

  ej2: LEMMA
   (A AND (A IMPLIES B)) IMPLIES B

  ej3: LEMMA
   ((A IMPLIES B) IMPLIES A) IMPLIES (B IMPLIES (B AND A))

  ej4: CONJECTURE
   (A OR B) IMPLIES (B OR C)

 END proposicional
```

Táctica `flatten-disjunct` acotada

- **Prueba del `ej1` con `flatten-disjunct` acotada**

```
ej1 :
  |-------
{1}   A IMPLIES (B OR A)

Rule? (flatten-disjunct :depth 1)
Applying disjunctive simplification to flatten sequent, this simplifies to:
ej1 :
{-1}  A
  |-------
{1}   (B OR A)

Rule? (flatten-disjunct :depth 1)
Applying disjunctive simplification to flatten sequent, this simplifies to:
ej1 :
[-1]  A
  |-------
{1}   B
{2}   A
which is trivially true. Q.E.D.
```

Táctica `flatten-disjunct`

- **Prueba del `ej1` con `flatten-disjunct`**

```
ej1 :

  |-------
{1}   A IMPLIES (B OR A)

Rule? (flatten-disjunct)
Applying disjunctive simplification to flatten sequent, this simplifies to:
ej1 :

{-1}  A
  |-------
{1}   B
{2}   A

which is trivially true.
Q.E.D.
```

Táctica `flatten`

- **Prueba del `ej1` con `flatten`**

```
ej1 :

  |-------
{1}   A IMPLIES (B OR A)

Rule? (flatten)
Applying disjunctive simplification to flatten sequent,
Q.E.D.
```

- **Tácticas usadas y reglas de inferencia**
  - **La táctica `flatten-disjunct` aplica las reglas $\vee$D, $\wedge$I, $\rightarrow$D, $\leftrightarrow$I, $\neg$I y $\neg$D.**
  - **La táctica `flatten` equivale a `flatten-disjunct` sin límite de profundidad**

Táctica split

- **Prueba del ej2 con flatten y split**

```
ej2 :

  |-------
{1}   (A AND (A IMPLIES B)) IMPLIES B

Rule? (flatten)
Applying disjunctive simplification to flatten sequent, this simplifies to:
ej2 :

{-1}  A
{-2}  (A IMPLIES B)
  |-------
{1}   B

Rule? (split)
Splitting conjunctions, this yields  2 subgoals:
```

Táctica split

```
ej2.1 :

{-1}  B
[-2]  A
  |-------
[1]   B

which is trivially true. This completes the proof of ej2.1.

ej2.2 :

[-1]  A
  |-------
{1}   A
[2]   B

which is trivially true. This completes the proof of ej2.2.
Q.E.D.
```

- **La táctica** `split` **aplica las reglas $\lor$I, $\land$D, $\to$I, $\leftrightarrow$D**

La estrategia `prop`

- **Prueba del `ej2` con `prop`**

```
ej2 :

  |-------
{1}   (A AND (A IMPLIES B)) IMPLIES B

Rule? (prop)
Applying propositional simplification,
Q.E.D.
```

- **Definición de `prop`:**

```
(try (flatten) (prop$) (try (split) (prop$) (skip)))
```

La estrategia prop$

- **Prueba del `ej2` con `prop$`**

```
ej2 :

  |-------
{1}   (A AND (A IMPLIES B)) IMPLIES B

Rule? (prop$)
Applying disjunctive simplification to flatten sequent, this simplifies to:
ej2 :

{-1}  A
{-2}  (A IMPLIES B)
  |-------
{1}   B

No change on: (FLATTEN)
...
```

La estrategia prop$

```
Splitting conjunctions, this yields  2 subgoals:
ej2.1 :

{-1}  B
[-2]  A
  |-------
[1]   B

which is trivially true. This completes the proof of ej2.1.

ej2.2 :

[-1]  A
  |-------
{1}   A
[2]   B

which is trivially true. This completes the proof of ej2.2.
Q.E.D.
```

La táctica `case` para cortes

- **Prueba del `ej3` con `case`**

```
ej3 :

  |-------
{1}   ((A IMPLIES B) IMPLIES A) IMPLIES (B IMPLIES (B AND A))

Rule? (flatten-disjunct :depth 1)
Applying disjunctive simplification to flatten sequent, this simplifies to:
ej3 :

{-1}  ((A IMPLIES B) IMPLIES A)
  |-------
{1}   (B IMPLIES (B AND A))

Rule? (case "A")
Case splitting on A, this yields  2 subgoals:
```

La táctica `case` para cortes

```
ej3.1 :

{-1}  A
[-2]  ((A IMPLIES B) IMPLIES A)
  |-------
[1]   (B IMPLIES (B AND A))

Rule? (hide -2)
Hiding formulas: -2, this simplifies to:
ej3.1 :

[-1]  A
  |-------
[1]   (B IMPLIES (B AND A))

Rule? (flatten)
Applying disjunctive simplification to flatten sequent, this simplifies to:
```

La táctica case para cortes

```
ej3.1 :

[-1]  A
{-2}  B
  |-------
{1}   (B AND A)

Rule? (split)
Splitting conjunctions, this yields  2 subgoals:
ej3.1.1 :

[-1]  A
[-2]  B
  |-------
{1}   B

which is trivially true.

This completes the proof of ej3.1.1.
```

La táctica case para cortes

```
ej3.1.2 :

[-1]  A
[-2]  B
  |-------
{1}   A

which is trivially true.

This completes the proof of ej3.1.2.

This completes the proof of ej3.1.

ej3.2 :

[-1]  ((A IMPLIES B) IMPLIES A)
  |-------
{1}   A
[2]   (B IMPLIES (B AND A))
```

La táctica `case` para cortes

```
Rule? (hide 2)
Hiding formulas:  2, this simplifies to:
ej3.2 :

[-1]  ((A IMPLIES B) IMPLIES A)
  |-------
[1]   A

Rule? (split)
Splitting conjunctions, this yields  2 subgoals:
ej3.2.1 :

{-1}  A
  |-------
[1]   A

which is trivially true.

This completes the proof of ej3.2.1.
```

La táctica `case` para cortes

```
ej3.2.2 :

  |-------
{1}   (A IMPLIES B)
[2]   A

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

This completes the proof of ej3.2.2.


This completes the proof of ej3.2.

Q.E.D.
```

La táctica `case` para cortes

- **Prueba del `ej3` con `prop`**

```
ej3 :

  |-------
{1}   ((A IMPLIES B) IMPLIES A) IMPLIES (B IMPLIES (B AND A))

Rule? (prop)
Applying propositional simplification,
Q.E.D.
```

Búsqueda de contramodelos

- **Cáculo de contramodelo del `ej4`**

```
ej4 :

  |-------
{1}   (A OR B) IMPLIES (B OR C)

Rule? (prop)
Applying propositional simplification,
this simplifies to:
ej4 :

{-1}  A
  |-------
{1}   B
{2}   C
```

- **Contramodelo: $v(A) = 1, v(B) = v(C) = 0$**

Bibliografía

- **J. Crow, S. Owre, J. Rushby, N. Shankar y M. Srivas *A Tutorial Introduction to PVS* (SRI International, 1995)**
- **M. Hofmann *Razonamiento asistido por computadora (2001–02)***
- **N. Shankar *Mechanized verification methodologies***