

# PPA

Un asistente de demostración para lógica de primer orden con extracción de testigos usando la traducción de Friedman

Manuel Panichelli

Departamento de Computación, FCEyN, UBA

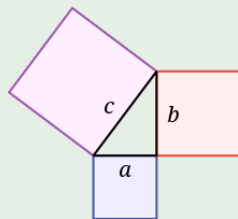
Diciembre 2024

## Introducción

- **Teorema:** Afirmación que puede ser *demostrada*.
- **Demostración** de un teorema:
  - *Argumento* que establece que el teorema es cierto
  - Usa *reglas de inferencia* a partir de *axiomas* y otros teoremas probados anteriormente.
- **Axiomas:** Afirmaciones que son siempre válidas (sin demostración).

## Ejemplo (Teorema de Pitágoras)

$$a^2 + b^2 = c^2.$$



- **Sistema:** Geometría euclidiana
- Un axioma: se puede dibujar una línea recta entre dos puntos

- Los **asistentes de demostración** son herramientas que facilitan la escritura y el chequeo de demostraciones por computadora.
- Usos usuales:
  - Formalización de teoremas matemáticos.
  - Verificación de programas.

---

<sup>1</sup>Terrence Tao - Machine Assisted Proof

- Los **asistentes de demostración** son herramientas que facilitan la escritura y el chequeo de demostraciones por computadora.
- Usos usuales:
  - Formalización de teoremas matemáticos.
  - Verificación de programas.
- Ventajas:<sup>1</sup>
  - Facilitan la colaboración a gran escala (mediante la confianza en el asistente).

---

<sup>1</sup>Terrence Tao - Machine Assisted Proof

- Los **asistentes de demostración** son herramientas que facilitan la escritura y el chequeo de demostraciones por computadora.
- Usos usuales:
  - Formalización de teoremas matemáticos.
  - Verificación de programas.
- Ventajas:<sup>1</sup>
  - Facilitan la colaboración a gran escala (mediante la confianza en el asistente).
  - Habilitan generación automática de demostraciones con IA. Por ej. un *LLM* (como *ChatGPT*) suele devolver alucinaciones, que pueden ser filtradas automáticamente con un asistente.

---

<sup>1</sup>Terrence Tao - Machine Assisted Proof

Constructivos



Coq  
(Type theory)



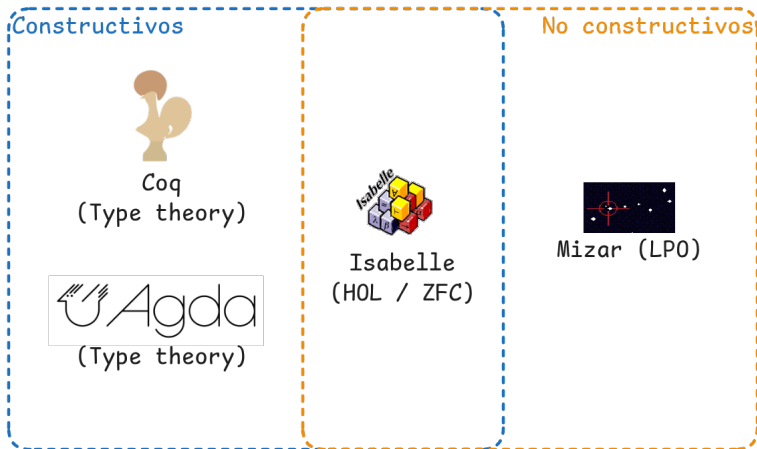
Isabelle  
(HOL / ZFC)

No constructivos

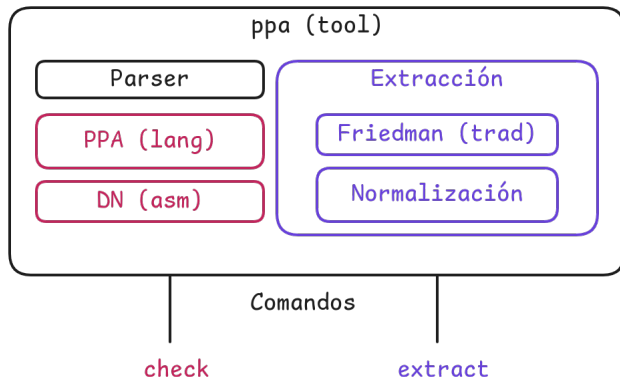


Mizar (LPO)





**Extracción de testigos:** De una demo de  $\exists x.p(x)$ , encontrar  $t$  tq  $p(t)$ .  
Lógica constructiva = sencillo, no constructiva = complicado.



Diseñamos e implementamos en Haskell la herramienta `ppa` (*Pani's Proof Assistant*): un asistente de demostración para LPO clásica. Dos partes:

- El lenguaje **PPA** para escribir demostraciones.
- **Extracción de testigos** (Aporte principal).

¿Cómo representamos las demostraciones? Ejemplo:

- Tenemos dos premisas
  - 1 Los alumnos que faltan a los exámenes, los reprueban.
  - 2 Si se reprueba un final, se recursa la materia.
- A partir de ellas, podríamos demostrar que si un alumno falta a un final, entonces recursa la materia.

# Representación de demostraciones

¿Cómo representamos las demostraciones? Ejemplo:

- Tenemos dos premisas
  - 1 Los alumnos que faltan a los exámenes, los reprueban.
  - 2 Si se reprueba un final, se recursa la materia.
- A partir de ellas, podríamos demostrar que si un alumno falta a un final, entonces recursa la materia.

## Teorema

*Si ((falta entonces reprueba) y (reprueba entonces recursa)) y falta, entonces recursa*

## Demostración.

- Asumo que falta. Quiero ver que recursa.
- Sabemos que si falta, entonces reprueba. Por lo tanto reprobó.
- Sabemos que si reprueba, entonces recursa. Por lo tanto recursó.



- **Problema:** Poco precisa. No se puede representar rigurosamente.
- Necesitamos **sistemas deductivos**: sistemas lógicos formales usados para escribir demostraciones
- Usamos **deducción natural**
  - **Lenguaje formal:** lógica de primer orden.
  - **Reglas de inferencia:** Por ejemplo,
    - *modus ponens*: si es cierto  $A \rightarrow B$  y  $A$ , se puede concluir  $B$
    - *modus tollens*: si es cierto  $A \rightarrow B$  y  $\neg B$ , se puede concluir  $\neg A$

## Definición (Términos)

Los términos están dados por la gramática:

$$\begin{array}{ll} t ::= x & \text{(variables)} \\ \quad | f(t_1, \dots, t_n) & \text{(funciones)} \end{array}$$

## Definición (Fórmulas)

Las fórmulas están dadas por la gramática:

$$\begin{array}{ll} A, B ::= p(t_1, \dots, t_n) & \text{(predicados)} \\ \quad | \perp \mid \top & \text{(falso o } bottom \text{ y verdadero o } top) \\ \quad | A \wedge B \mid A \vee B & \text{(conjunción y disyunción)} \\ \quad | A \rightarrow B \mid \neg A & \text{(implicación y negación)} \\ \quad | \forall x.A \mid \exists x.A & \text{(cuantificador universal y existencial)} \end{array}$$

## Deducción natural

## Ejemplo (Demostración en DN)

Notamos:

- $X \equiv \text{reprueba}(\text{juan}, \text{final}(\text{logica}))$
- $R \equiv \text{recurso}(\text{juan}, \text{logica})$
- $F \equiv \text{falta}(\text{juan}, \text{final}(\text{logica}))$

Queremos probar

$$\left( (F \rightarrow X) \wedge (X \rightarrow R) \right) \rightarrow (F \rightarrow R)$$



## Ejemplo (Demostración en DN)

$$\frac{\frac{\frac{\Gamma \vdash (F \rightarrow X) \wedge (X \rightarrow R)}{\Gamma \vdash X \rightarrow R} \text{Ax}}{\Gamma = (F \rightarrow X) \wedge (X \rightarrow R), F \vdash R} \text{E}_{\wedge 1} \quad \frac{\Gamma \vdash X}{\Gamma \vdash R} \text{E}_{\rightarrow}}{\frac{(F \rightarrow X) \wedge (X \rightarrow R) \vdash F \rightarrow R}{\vdash ((F \rightarrow X) \wedge (X \rightarrow R)) \rightarrow (F \rightarrow R)} \text{I}_{\rightarrow}} \text{I}_{\rightarrow}$$

donde

$$\Pi = \frac{\frac{\Gamma \vdash (F \rightarrow X) \wedge (X \rightarrow R)}{\Gamma \vdash F \rightarrow X} \text{E}_{\wedge 2} \quad \frac{}{\Gamma \vdash F} \text{Ax}}{\Gamma \vdash X} \text{E}_{\rightarrow}$$

## Definición (Contexto de demostración)

$\Gamma$  es un **contexto de demostración**, conjunto de fórmulas que se asumen válidas.

**Notación:**  $\Gamma, \varphi = \Gamma \cup \{\varphi\}$

## Definición (Contexto de demostración)

$\Gamma$  es un **contexto de demostración**, conjunto de fórmulas que se asumen válidas.

**Notación:**  $\Gamma, \varphi = \Gamma \cup \{\varphi\}$

## Definición (Relación de derivabilidad)

- $\vdash$  es la **relación de derivabilidad** definida a partir de las *reglas de inferencia*.
- Permite escribir juicios  $\Gamma \vdash \varphi$ . Intuición: “ $\varphi$  es una consecuencia de las suposiciones de  $\Gamma$ ”
- Es cierto si en una cantidad finita de pasos podemos concluir  $\varphi$  a partir de las fórmulas de  $\Gamma$ , los axiomas y las reglas de inferencia.

## Definición (Reglas de inferencia)

$$\frac{}{\Gamma, A \vdash A} \text{Ax}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \text{I} \rightarrow$$

$$\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \text{E} \rightarrow$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \text{I} \wedge$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \text{E} \wedge_1$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \text{E} \wedge_2$$

Dos tipos para cada conector y cuantificador, dada una fórmula formada con un conector:

- **Introducción:** ¿Cómo la demuestro?
- **Eliminación:** ¿Cómo la uso para demostrar otra?

## Otras reglas de inferencia

- $E\perp$ ,  $IT$
- $I\neg$ ,  $E\neg$
- $IV_1$ ,  $IV_2$ ,  $EV$
- $I\forall$ ,  $E\forall$
- $I\exists$ ,  $E\exists$
- LEM

## Otras reglas de inferencia

- $E\perp$ ,  $IT$
- $I\neg$ ,  $E\neg$
- $IV_1$ ,  $IV_2$ ,  $EV$
- $I\forall$ ,  $E\forall$
- $I\exists$ ,  $E\exists$
- LEM

## Alfa equivalencia

- Podemos usar  $\exists x.p(x)$  y  $\exists y.p(y)$  intercambiablemente.
- Son  $\alpha$ -equivalentes (renombrando variables ligadas de forma apropiada, son iguales).

# Reglas admisibles

- Mencionamos *modus tollens* pero no aparece en las reglas de inferencia.
- Queremos un sistema lógico **minimal**: no agregamos las reglas **admisibles**, derivables a partir de las existentes.
- Se implementan como funciones o *macros*.

## Lema (Modus tollens)

$$\frac{\frac{\frac{}{\Gamma \vdash (A \rightarrow B) \wedge \neg B} Ax}{\Gamma \vdash \neg B} E\wedge_2 \quad \frac{\frac{\frac{}{\Gamma \vdash (A \rightarrow B) \wedge \neg B} Ax}{\Gamma \vdash A \rightarrow B} E\wedge_1 \quad \frac{}{\Gamma \vdash A} Ax}{\Gamma \vdash B} E\rightarrow}{\Gamma = (A \rightarrow B) \wedge \neg B, A \vdash \perp} E\neg}{(A \rightarrow B) \wedge \neg B \vdash \neg A} I\neg}{\vdash (A \rightarrow B \wedge \neg B) \rightarrow \neg A} I\rightarrow$$

## Definición (Sustitución)

Notamos como  $A\{x := t\}$  a la sustitución de todas las ocurrencias libres de la variable  $x$  por el término  $t$  en la fórmula  $A$ .

## Eliminación de universal

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A\{x := t\}} E\forall$$

## Capturas

Evitamos automáticamente la **captura de variables**

$(\forall y.p(x))\{x := y\} \neq \forall y.p(y)$  (capturada)

$(\forall y.p(x))\{x := y\} = \forall z.p(y)$  (renombrada)



PPA

*Mathematical Vernacular*<sup>2</sup> = Mizar + Isar (Isabelle)

Forma *natural* de representar demostraciones matemáticas. Ideas:

- **Deducción natural en estilo de *Fitch***. Notación equivalente, demostraciones como listas de fórmulas en lugar de árboles.

---

<sup>2</sup>De Freek Wiedijk

*Mathematical Vernacular*<sup>2</sup> = Mizar + Isar (Isabelle)

Forma *natural* de representar demostraciones matemáticas. Ideas:

- **Deducción natural en estilo de *Fitch***. Notación equivalente, demostraciones como listas de fórmulas en lugar de árboles.
- **Reglas de inferencia *declarativas***: Afirmer

$$A_1, \dots, A_n \vdash A$$

sin tener que demostrarlo a mano (automático).

---

<sup>2</sup>De Freek Wiedijk

$$\textit{Mathematical Vernacular}^2 = \text{Mizar} + \text{Isar (Isabelle)}$$

Forma *natural* de representar demostraciones matemáticas. Ideas:

- **Deducción natural en estilo de *Fitch***. Notación equivalente, demostraciones como listas de fórmulas en lugar de árboles.
- **Reglas de inferencia *declarativas***: Afirmar

$$A_1, \dots, A_n \vdash A$$

sin tener que demostrarlo a mano (automático).

- **Sintaxis similar a un lenguaje de programación** en lugar al lenguaje natural.

---

<sup>2</sup>De Freek Wiedijk

*Lenguaje PPA, inspirado en el Mathematical Vernacular.*

Ejemplo demostración

```
1 axiom falta_reprueba: forall A . forall E .  
2   falta(A, E) -> reprueba(A, E)  
3 axiom reprueba_recura: forall A . forall M .  
4   reprueba(A, final(M)) -> recursa(A, M)
```

Lenguaje PPA, inspirado en el *Mathematical Vernacular*.

### Ejemplo demostración

```
1  axiom falta_reprueba: forall A . forall E .  
2      falta(A, E) -> reprueba(A, E)  
3  axiom reprueba_recura: forall A . forall M .  
4      reprueba(A, final(M)) -> recursa(A, M)  
5  
6  theorem falta_entonces_recura: forall A . forall M .  
7      falta(A, final(M)) -> recursa(A, M)  
8  proof
```

Lenguaje PPA, inspirado en el *Mathematical Vernacular*.

### Ejemplo demostración

```
1  axiom falta_reprueba: forall A . forall E .  
2      falta(A, E) -> reprueba(A, E)  
3  axiom reprueba_recura: forall A . forall M .  
4      reprueba(A, final(M)) -> recursa(A, M)  
5  
6  theorem falta_entonces_recura: forall A . forall M .  
7      falta(A, final(M)) -> recursa(A, M)  
8  proof  
9      let A  
10     let M
```

Lenguaje PPA, inspirado en el *Mathematical Vernacular*.

### Ejemplo demostración

```
1  axiom falta_reprueba: forall A . forall E .  
2      falta(A, E) -> reprueba(A, E)  
3  axiom reprueba_recura: forall A . forall M .  
4      reprueba(A, final(M)) -> recursa(A, M)  
5  
6  theorem falta_entonces_recura: forall A . forall M .  
7      falta(A, final(M)) -> recursa(A, M)  
8  proof  
9      let A  
10     let M  
11     suppose falta: falta(A, final(M))
```



Lenguaje PPA, inspirado en el *Mathematical Vernacular*.

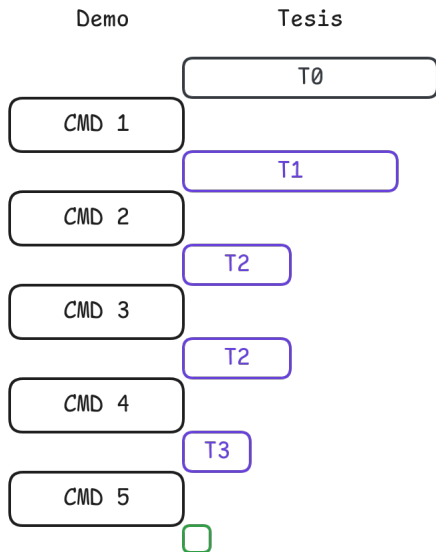
### Ejemplo demostración

```
1  axiom falta_reprueba: forall A . forall E .  
2      falta(A, E) -> reprueba(A, E)  
3  axiom reprueba_recura: forall A . forall M .  
4      reprueba(A, final(M)) -> recursa(A, M)  
5  
6  theorem falta_entonces_recura: forall A . forall M .  
7      falta(A, final(M)) -> recursa(A, M)  
8  proof  
9      let A  
10     let M  
11     suppose falta: falta(A, final(M))  
12     have reprueba: reprueba(A, final(M)) by falta_reprueba, falta
```

Lenguaje PPA, inspirado en el *Mathematical Vernacular*.

### Ejemplo demostración

```
1  axiom falta_reprueba: forall A . forall E .  
2      falta(A, E) -> reprueba(A, E)  
3  axiom reprueba_recura: forall A . forall M .  
4      reprueba(A, final(M)) -> recursa(A, M)  
5  
6  theorem falta_entonces_recura: forall A . forall M .  
7      falta(A, final(M)) -> recursa(A, M)  
8  proof  
9      let A  
10     let M  
11     suppose falta: falta(A, final(M))  
12     have reprueba: reprueba(A, final(M)) by falta_reprueba, falta  
13     thus recursa(A, M) by reprueba_recura, reprueba  
14 end
```



Lista de **comandos** que reducen sucesivamente la *tesis* (fórmula a demostrar) hasta agotarla.

`<form> by <h1>, ..., <hn>`

- Demuestra **automáticamente** que la fórmula es consecuencia lógica de la justificación
- Por debajo usa un *solver* completo para lógica proposicional pero *heurístico* para primer orden.
- Toma las hipótesis del **contexto**: fórmulas asumidas (axiomas) o demostradas (teoremas y comandos que demuestran hipótesis auxiliares).

# Thus y Have

**thus** <form> **by** <h1>, ..., <hn>

Si <form> es *parte* de la tesis, y el *solver* puede demostrar la implicación, lo demuestra automáticamente y lo descarga de la tesis.

**have** <name>: <form> **by** <h1>, ..., <hn>

Análogo a **thus**, pero introduce una afirmación *auxiliar* sin reducir la tesis, agregándola al contexto.

# Comandos y reglas de inferencia

Regla	Comando
LEM	<b>cases</b>
$Ax$	<b>by</b>
$I\exists$	<b>take</b>
$E\exists$	<b>consider</b>
$I\forall$	<b>let</b>
$E\forall$	<b>by</b>
$I\forall_1$	<b>by</b>
$I\forall_2$	<b>by</b>
$E\forall$	<b>cases</b>

Regla	Comando
$I\wedge$	<b>by</b>
$E\wedge_1$	<b>by</b>
$E\wedge_2$	<b>by</b>
$I\rightarrow$	<b>suppose</b>
$E\rightarrow$	<b>by</b>
$I\neg$	<b>suppose</b>
$E\neg$	<b>by</b>
$IT$	<b>by</b>
$E\perp$	<b>by</b>

**equivalently** <form>

Permite reducir la tesis a una fórmula equivalente

**claim** <name>: <form>

Análogo a **have** pero con una sub-demostración.

Esquema de claim

```
theorem t: <form1>
```

```
proof
```

```
  claim <name>: <form2>
```

```
  proof
```

```
    // Demostración de <form2>.
```

```
  end
```

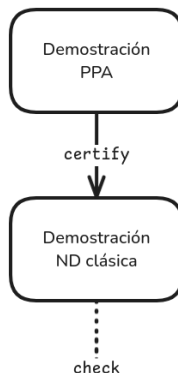
```
  // Demostración de <form1> refiriéndose a <name>.
```

```
end
```

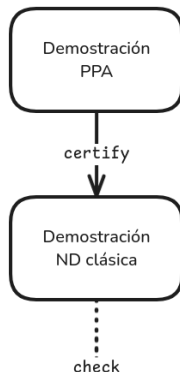
Certificador



- Las demostraciones de PPA se *certifican* generando una demostración de deducción natural.
- Evita confiar en la implementación del asistente.



- Las demostraciones de PPA se *certifican* generando una demostración de deducción natural.
- Evita confiar en la implementación del asistente.



## Criterio de de Bruijn

Un asistente de demostración cumple con el criterio de de Bruijn si satisface que sus demostraciones puedan ser chequeadas por un programa independiente, pequeño y confiable.

# Contexto global

Se generan  $N$  demostraciones de deducción natural para cada programa, y se guardan en el *contexto global*. El chequeo se extiende a contextos.

```
1  axiom ax1: q
2  axiom ax2: q -> p
3  axiom ax3: p -> r
4
5  theorem t1: p
6  proof
7    thus p by ax1, ax2
8  end
9
10 theorem t2: r
11 proof
12   thus r by t1, ax3
13 end
```

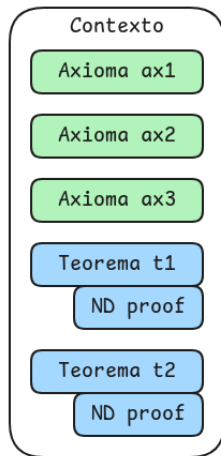


Figura: Contexto resultante de certificar un programa

El certificado de una demostración es recursivo:

```
1 theorem t:  
2   p(v) -> exists X . p(X)  
3 proof  
4   suppose h: p(v)  
5   take X := v  
6   thus p(v) by h  
7 end
```

$$\frac{\frac{h : p(v) \vdash p(v)}{h : p(v) \vdash \exists x.p(X)} \text{Ax}_h \mid \exists}{\vdash p(v) \rightarrow \exists x.p(X)} \mid \rightarrow_h$$

Figura: Ejemplo de certificado generado para un programa

# Contexto local

Cada demostración tiene un contexto local a ella con las hipótesis agregadas por ciertos comandos (**suppose**, **consider**, **have**, **claim**, etc.).

```
1 axiom ax1:  $p \rightarrow q$ 
2 theorem t:  $(q \rightarrow r) \rightarrow p \rightarrow r$ 
3 proof
4   suppose h1:  $(q \rightarrow r)$ 
5   suppose h2:  $p$ 
6   then tq:  $q$  by ax1
7   hence r by h1
8 end
```

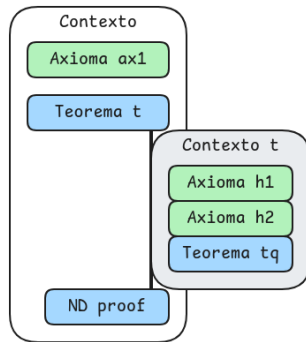


Figura: Ejemplo de contexto local

## Certificado del by

Teniendo  $\Gamma = \{h_1 : B_1, \dots, h_n : B_n\}$ , para **thus**  $A$  **by**  $h_1, \dots, h_n$ :

- 1 Buscamos las hipótesis en el contexto. Queremos demostrar

$$B_1 \wedge \dots \wedge B_n \rightarrow A$$

Teniendo  $\Gamma = \{h_1 : B_1, \dots, h_n : B_n\}$ , para **thus** A **by**  $h_1, \dots, h_n$ :

- 1 Buscamos las hipótesis en el contexto. Queremos demostrar

$$B_1 \wedge \dots \wedge B_n \rightarrow A$$

- 2 **Razonamos por el absurdo:** Asumiendo la negación buscamos una contradicción

$$\begin{aligned}\neg(B_1 \wedge \dots \wedge B_n \rightarrow A) &\equiv \neg(\neg(B_1 \wedge \dots \wedge B_n) \vee A) \\ &\equiv B_1 \wedge \dots \wedge B_n \wedge \neg A\end{aligned}$$

Teniendo  $\Gamma = \{h_1 : B_1, \dots, h_n : B_n\}$ , para **thus** A **by**  $h_1, \dots, h_n$ :

- 1 Buscamos las hipótesis en el contexto. Queremos demostrar

$$B_1 \wedge \dots \wedge B_n \rightarrow A$$

- 2 **Razonamos por el absurdo:** Asumiendo la negación buscamos una contradicción

$$\begin{aligned}\neg(B_1 \wedge \dots \wedge B_n \rightarrow A) &\equiv \neg(\neg(B_1 \wedge \dots \wedge B_n) \vee A) \\ &\equiv B_1 \wedge \dots \wedge B_n \wedge \neg A\end{aligned}$$

- 3 Convertimos la negación a forma normal disyuntiva (**DNF**)

$$(a_1 \wedge \dots \wedge a_n) \vee \dots \vee (b_1 \wedge \dots \wedge b_m)$$



# Certificado del by

Teniendo  $\Gamma = \{h_1 : B_1, \dots, h_n : B_n\}$ , para **thus** A **by**  $h_1, \dots, h_n$ :

- 1 Buscamos las hipótesis en el contexto. Queremos demostrar

$$B_1 \wedge \dots \wedge B_n \rightarrow A$$

- 2 **Razonamos por el absurdo**: Asumiendo la negación buscamos una contradicción

$$\begin{aligned}\neg(B_1 \wedge \dots \wedge B_n \rightarrow A) &\equiv \neg(\neg(B_1 \wedge \dots \wedge B_n) \vee A) \\ &\equiv B_1 \wedge \dots \wedge B_n \wedge \neg A\end{aligned}$$

- 3 Convertimos la negación a forma normal disyuntiva (**DNF**)

$$(a_1 \wedge \dots \wedge a_n) \vee \dots \vee (b_1 \wedge \dots \wedge b_m)$$

- 4 Buscamos una **contradicción** refutando cada cláusula individualmente. Será refutable si

# Certificado del by

Teniendo  $\Gamma = \{h_1 : B_1, \dots, h_n : B_n\}$ , para **thus** A **by**  $h_1, \dots, h_n$ :

- 1 Buscamos las hipótesis en el contexto. Queremos demostrar

$$B_1 \wedge \dots \wedge B_n \rightarrow A$$

- 2 **Razonamos por el absurdo**: Asumiendo la negación buscamos una contradicción

$$\begin{aligned}\neg(B_1 \wedge \dots \wedge B_n \rightarrow A) &\equiv \neg(\neg(B_1 \wedge \dots \wedge B_n) \vee A) \\ &\equiv B_1 \wedge \dots \wedge B_n \wedge \neg A\end{aligned}$$

- 3 Convertimos la negación a forma normal disyuntiva (**DNF**)

$$(a_1 \wedge \dots \wedge a_n) \vee \dots \vee (b_1 \wedge \dots \wedge b_m)$$

- 4 Buscamos una **contradicción** refutando cada cláusula individualmente. Será refutable si
  - Contiene  $\perp$  o dos fórmulas opuestas  $(a, \neg a)$ ,

# Certificado del by

Teniendo  $\Gamma = \{h_1 : B_1, \dots, h_n : B_n\}$ , para **thus** A **by**  $h_1, \dots, h_n$ :

- 1 Buscamos las hipótesis en el contexto. Queremos demostrar

$$B_1 \wedge \dots \wedge B_n \rightarrow A$$

- 2 **Razonamos por el absurdo**: Asumiendo la negación buscamos una contradicción

$$\begin{aligned}\neg(B_1 \wedge \dots \wedge B_n \rightarrow A) &\equiv \neg(\neg(B_1 \wedge \dots \wedge B_n) \vee A) \\ &\equiv B_1 \wedge \dots \wedge B_n \wedge \neg A\end{aligned}$$

- 3 Convertimos la negación a forma normal disyuntiva (**DNF**)

$$(a_1 \wedge \dots \wedge a_n) \vee \dots \vee (b_1 \wedge \dots \wedge b_m)$$

- 4 Buscamos una **contradicción** refutando cada cláusula individualmente. Será refutable si

- Contiene  $\perp$  o dos fórmulas opuestas  $(a, \neg a)$ ,
- Eliminando existenciales consecutivos y reiniciando el proceso, se consigue una refutación  $(\neg p(k), \forall x.p(x))$

## Ejemplo sin cuantificadores (1/2)

By sin cuantificadores

```
1 axiom ax1: a -> b
2 axiom ax2: a
3 theorem t: b
4 proof
5   thus b by ax1, ax2
6 end
```

## Ejemplo sin cuantificadores (1/2)

By sin cuantificadores

```
1 axiom ax1: a -> b
2 axiom ax2: a
3 theorem t: b
4 proof
5   thus b by ax1, ax2
6 end
```

- ❶ Para certificar **thus** b **by** ax1, ax2 hay que generar una demostración para la implicación

$$((a \rightarrow b) \wedge a) \rightarrow b$$

## Ejemplo sin cuantificadores (1/2)

By sin cuantificadores

```
1 axiom ax1: a -> b
2 axiom ax2: a
3 theorem t: b
4 proof
5   thus b by ax1, ax2
6 end
```

- 1 Para certificar **thus** b **by** ax1, ax2 hay que generar una demostración para la implicación

$$((a \rightarrow b) \wedge a) \rightarrow b$$

- 2 Negamos la fórmula y buscamos una contradicción.

$$\neg [((a \rightarrow b) \wedge a) \rightarrow b]$$

## Ejemplo sin cuantificadores (2/2)

### 3 La convertimos a DNF

$$\begin{aligned} & \neg[(a \rightarrow b) \wedge a \rightarrow b] \\ & \equiv \neg[\neg((a \rightarrow b) \wedge a) \vee b] && (A \rightarrow B \equiv \neg A \vee B) \\ & \equiv \neg\neg((a \rightarrow b) \wedge a) \wedge \neg b && (\neg(A \vee B) \equiv \neg A \wedge \neg B) \\ & \equiv ((a \rightarrow b) \wedge a) \wedge \neg b && (\neg\neg A \equiv A) \\ & \equiv (\neg a \vee b) \wedge a \wedge \neg b && (A \rightarrow B \equiv \neg A \vee B) \\ & \equiv (\neg a \vee b) \wedge a \wedge \neg b && ((A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)) \\ & \equiv (\neg a \wedge a \wedge \neg b) \vee \\ & \quad (b \wedge a \wedge \neg b) \end{aligned}$$

## Ejemplo sin cuantificadores (2/2)

### 3 La convertimos a DNF

$$\begin{aligned} & \neg[(a \rightarrow b) \wedge a \rightarrow b] \\ & \equiv \neg[\neg((a \rightarrow b) \wedge a) \vee b] && (A \rightarrow B \equiv \neg A \vee B) \\ & \equiv \neg\neg((a \rightarrow b) \wedge a) \wedge \neg b && (\neg(A \vee B) \equiv \neg A \wedge \neg B) \\ & \equiv ((a \rightarrow b) \wedge a) \wedge \neg b && (\neg\neg A \equiv A) \\ & \equiv (\neg a \vee b) \wedge a \wedge \neg b && (A \rightarrow B \equiv \neg A \vee B) \\ & \equiv (\neg a \vee b) \wedge a \wedge \neg b && ((A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)) \\ & \equiv (\neg a \wedge a \wedge \neg b) \vee \\ & \quad (b \wedge a \wedge \neg b) \end{aligned}$$

### 4 Refutamos cada cláusula

$$(\neg a \wedge a \wedge \neg b) \vee (b \wedge a \wedge \neg b)$$





## Ejemplo con cuantificadores (1/3)

By con cuantificadores

```
1 axiom ax1: forall X . p(X) -> q(X)
2 axiom ax2: p(k)
3 theorem t: q(k)
4 proof
5   thus q(k) by ax1, ax2
6 end
```

## Ejemplo con cuantificadores (1/3)

By con cuantificadores

```
1 axiom ax1: forall X . p(X) -> q(X)
2 axiom ax2: p(k)
3 theorem t: q(k)
4 proof
5   thus q(k) by ax1, ax2
6 end
```

- ❶ Para certificar **thus**  $q(k)$  **by**  $ax1, ax2$  hay que generar una demostración para la implicación

$$\left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \rightarrow q(k)$$

## Ejemplo con cuantificadores (1/3)

By con cuantificadores

```
1 axiom ax1: forall X . p(X) -> q(X)
2 axiom ax2: p(k)
3 theorem t: q(k)
4 proof
5   thus q(k) by ax1, ax2
6 end
```

- ❶ Para certificar **thus**  $q(k)$  **by**  $ax1, ax2$  hay que generar una demostración para la implicación

$$\left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \rightarrow q(k)$$

- ❷ Negamos la fórmula

$$\neg \left[ \left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \rightarrow q(k) \right]$$

## Ejemplo con cuantificadores (2/3)

- 3 La convertimos a DNF

$$\begin{aligned}& \neg \left[ \left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \rightarrow q(k) \right] \\& \equiv \neg \left[ \neg \left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \vee q(k) \right] \\& \equiv \neg \neg \left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \wedge \neg q(k) \\& \equiv (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \wedge \neg q(k)\end{aligned}$$

como a los ojos de DNF un  $\forall$  es opaco, a pesar de que dentro tenga una implicación, la fórmula ya está en forma normal.

## Ejemplo con cuantificadores (2/3)

- 3 La convertimos a DNF

$$\begin{aligned}& \neg \left[ \left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \rightarrow q(k) \right] \\& \equiv \neg \left[ \neg \left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \vee q(k) \right] \\& \equiv \neg \neg \left( (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \right) \wedge \neg q(k) \\& \equiv (\forall x. (p(x) \rightarrow q(x))) \wedge p(k) \wedge \neg q(k)\end{aligned}$$

como a los ojos de DNF un  $\forall$  es opaco, a pesar de que dentro tenga una implicación, la fórmula ya está en forma normal.

- 4 Buscamos una contradicción refutando cada cláusula. No hay forma encontrando literales opuestos o  $\perp$ , por ej. la cláusula  $p(a)$  no es refutable.

## Ejemplo con cuantificadores (3/3)

- 5 Probamos eliminando  $\forall x.(p(x) \rightarrow q(x))$ . Reemplazamos  $x$  por una meta-variable fresca  $u$ .

$$(p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k)$$

## Ejemplo con cuantificadores (3/3)

- 5 Probamos eliminando  $\forall x.(p(x) \rightarrow q(x))$ . Reemplazamos  $x$  por una meta-variable fresca  $u$ .

$$(p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k)$$

- 6 Convertimos a DNF

$$\begin{aligned} & (p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k) \\ & \equiv (\neg p(u) \vee q(u)) \wedge p(k) \wedge \neg q(k) \\ & \equiv ((\neg p(u) \wedge p(k)) \vee (q(u) \wedge p(k))) \wedge \neg q(k) \\ & \equiv (\neg p(u) \wedge p(k) \wedge \neg q(k)) \vee \\ & \quad (q(u) \wedge p(k) \wedge \neg q(k)) \end{aligned}$$

## Ejemplo con cuantificadores (3/3)

- 5 Probamos eliminando  $\forall x.(p(x) \rightarrow q(x))$ . Reemplazamos  $x$  por una meta-variable fresca  $u$ .

$$(p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k)$$

- 6 Convertimos a DNF

$$\begin{aligned} & (p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k) \\ & \equiv (\neg p(u) \vee q(u)) \wedge p(k) \wedge \neg q(k) \\ & \equiv ((\neg p(u) \wedge p(k)) \vee (q(u) \wedge p(k))) \wedge \neg q(k) \\ & \equiv (\neg p(u) \wedge p(k) \wedge \neg q(k)) \vee \\ & \quad (q(u) \wedge p(k) \wedge \neg q(k)) \end{aligned}$$

- 7 Buscamos una contradicción refutando cada cláusula. Los literales opuestos tienen que *unificar* en lugar de ser iguales.



## Ejemplo con cuantificadores (3/3)

- 5 Probamos eliminando  $\forall x.(p(x) \rightarrow q(x))$ . Reemplazamos  $x$  por una meta-variable fresca  $u$ .

$$(p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k)$$

- 6 Convertimos a DNF

$$\begin{aligned} & (p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k) \\ & \equiv (\neg p(u) \vee q(u)) \wedge p(k) \wedge \neg q(k) \\ & \equiv ((\neg p(u) \wedge p(k)) \vee (q(u) \wedge p(k))) \wedge \neg q(k) \\ & \equiv (\neg p(u) \wedge p(k) \wedge \neg q(k)) \vee \\ & \quad (q(u) \wedge p(k) \wedge \neg q(k)) \end{aligned}$$

- 7 Buscamos una contradicción refutando cada cláusula. Los literales opuestos tienen que *unificar* en lugar de ser iguales.
- $\neg p(u) \wedge p(k) \wedge \neg q(k)$  tenemos  $p(u) \doteq p(k)$  con  $\{u := k\}$

## Ejemplo con cuantificadores (3/3)

- 5 Probamos eliminando  $\forall x.(p(x) \rightarrow q(x))$ . Reemplazamos  $x$  por una meta-variable fresca  $u$ .

$$(p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k)$$

- 6 Convertimos a DNF

$$\begin{aligned} & (p(u) \rightarrow q(u)) \wedge p(k) \wedge \neg q(k) \\ & \equiv (\neg p(u) \vee q(u)) \wedge p(k) \wedge \neg q(k) \\ & \equiv ((\neg p(u) \wedge p(k)) \vee (q(u) \wedge p(k))) \wedge \neg q(k) \\ & \equiv (\neg p(u) \wedge p(k) \wedge \neg q(k)) \vee \\ & \quad (q(u) \wedge p(k) \wedge \neg q(k)) \end{aligned}$$

- 7 Buscamos una contradicción refutando cada cláusula. Los literales opuestos tienen que *unificar* en lugar de ser iguales.
- $\neg p(u) \wedge p(k) \wedge \neg q(k)$  tenemos  $p(u) \doteq p(k)$  con  $\{u := k\}$
  - $q(u) \wedge p(k) \wedge \neg q(k)$  tenemos  $q(u) \doteq q(k)$  con  $\{u := k\}$

## Desafío

¡Hay que generar una demostración en deducción natural!

### Pasos

- **Razonamiento por el absurdo:** mediante las *reglas admisibles* cut y eliminación de la doble negación ( $E_{\neg\neg}$ ).
- **Conversión a DNF:** mediante la implementación de un *sistema de reescritura*.
- **Contradicciones:** mediante la *regla admisible*  $E_{\wedge\varphi} + E_{\vee} + I_{\neg}$ .
- **Eliminación de cuantificadores universales:** mediante unificación y  $E_{\forall}$ .

# Razonamiento por el absurdo

## Razonamiento por el absurdo en DNF

$$\vdash B_1 \wedge \dots \wedge B_n \rightarrow A \overset{?}{\rightsquigarrow} \neg(B_1 \wedge \dots \wedge B_n \rightarrow A) \vdash \perp$$

# Razonamiento por el absurdo

## Razonamiento por el absurdo en DNF

$$\vdash B_1 \wedge \dots \wedge B_n \rightarrow A \overset{?}{\rightsquigarrow} \neg(B_1 \wedge \dots \wedge B_n \rightarrow A) \vdash \perp$$

### Teorema (DNeg Elim)

$$\frac{\frac{}{\neg\neg A \vdash A}}{E_{\neg\neg}}$$

### Teorema (cut)

$$\frac{\frac{\Gamma, B \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A}}{cut}$$

## Lema (Razonamiento por el absurdo)

$$\frac{\frac{\vdots}{\Gamma, \neg A \vdash \perp} \quad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A} \quad I_{\neg}}{cut, E_{\neg\neg}}$$

# Conversión a DNF

Implementamos una traducción mediante el siguiente sistema de reescritura. **Algoritmo:** reescribir de a un paso hasta que no cambie (clausura de Kleene)

$$\neg\neg a \rightsquigarrow a$$

eliminación de  $\neg\neg$

$$\neg\perp \rightsquigarrow \top$$

$$\neg\top \rightsquigarrow \perp$$

$$a \rightarrow b \rightsquigarrow \neg a \vee b$$

definición de implicación

$$\neg(a \vee b) \rightsquigarrow \neg a \wedge \neg b$$

distributiva de  $\neg$  sobre  $\wedge$

$$\neg(a \wedge b) \rightsquigarrow \neg a \vee \neg b$$

distributiva de  $\neg$  sobre  $\vee$

$$(a \vee b) \wedge c \rightsquigarrow (a \wedge c) \vee (b \wedge c)$$

distributiva de  $\wedge$  sobre  $\vee$  (der)

$$c \wedge (a \vee b) \rightsquigarrow (c \wedge a) \vee (c \wedge b)$$

distributiva de  $\wedge$  sobre  $\vee$  (izq)

$$a \vee (b \vee c) \rightsquigarrow (a \vee b) \vee c$$

asociatividad de  $\vee$

$$a \wedge (b \wedge c) \rightsquigarrow (a \wedge b) \wedge c$$

asociatividad de  $\wedge$

## Conversión a DNF - Congruencias

Para reescribir una sub-fórmula (trivial sintácticamente), hay que demostrar las congruencias de los conectivos.

$$a \vee \neg(b \vee c) \vdash a \vee (\neg b \wedge \neg c)$$

## Conversión a DNF - Congruencias

Para reescribir una sub-fórmula (trivial sintácticamente), hay que demostrar las congruencias de los conectivos.

$$a \vee \neg(b \vee c) \vdash a \vee (\neg b \wedge \neg c)$$

### Congruencias

$$\begin{array}{ll} A \vdash A' \Rightarrow A \wedge B \vdash A' \wedge B & B \vdash B' \Rightarrow A \wedge B \vdash A \wedge B' \\ A \vdash A' \Rightarrow A \vee B \vdash A' \vee B & B \vdash B' \Rightarrow A \vee B \vdash A \vee B' \\ A' \vdash A \Rightarrow \neg A \vdash \neg A' & \end{array}$$



## Conversión a DNF - Congruencias

Para reescribir una sub-fórmula (trivial sintácticamente), hay que demostrar las congruencias de los conectivos.

$$a \vee \neg(b \vee c) \vdash a \vee (\neg b \wedge \neg c)$$

### Congruencias

$$\begin{array}{ll} A \vdash A' \Rightarrow A \wedge B \vdash A' \wedge B & B \vdash B' \Rightarrow A \wedge B \vdash A \wedge B' \\ A \vdash A' \Rightarrow A \vee B \vdash A' \vee B & B \vdash B' \Rightarrow A \vee B \vdash A \vee B' \\ A' \vdash A \Rightarrow \neg A \vdash \neg A' & \end{array}$$

### $\neg$ es contravariante

Para demostrar  $\neg A \vdash \neg A'$  no necesitamos una demostración de  $A \vdash A'$  (covariante), sino de  $A' \vdash A$  (contravariante).

## Conversión a DNF - Congruencias

Para reescribir una sub-fórmula (trivial sintácticamente), hay que demostrar las congruencias de los conectivos.

$$a \vee \neg(b \vee c) \vdash a \vee (\neg b \wedge \neg c)$$

### Congruencias

$$\begin{array}{ll} A \vdash A' \Rightarrow A \wedge B \vdash A' \wedge B & B \vdash B' \Rightarrow A \wedge B \vdash A \wedge B' \\ A \vdash A' \Rightarrow A \vee B \vdash A' \vee B & B \vdash B' \Rightarrow A \vee B \vdash A \vee B' \\ A' \vdash A \Rightarrow \neg A \vdash \neg A' & \end{array}$$

### $\neg$ es contravariante

Para demostrar  $\neg A \vdash \neg A'$  no necesitamos una demostración de  $A \vdash A'$  (*covariante*), sino de  $A' \vdash A$  (*contravariante*).

$\Rightarrow$  para todas las reescrituras, incluso las congruencias, tenemos que demostrarlas en ambos sentidos.

# Conversión a DNF - Reglas admisibles

## Reglas admisibles para conversión a DNF

### Pasos base

$$\neg\neg a \dashv\vdash a$$

$$\neg\perp \dashv\vdash \top$$

$$\neg\top \dashv\vdash \perp$$

$$a \rightarrow b \dashv\vdash \neg a \vee b$$

$$\neg(a \vee b) \dashv\vdash \neg a \wedge \neg b$$

$$\neg(a \wedge b) \dashv\vdash \neg a \vee \neg b$$

$$(a \vee b) \wedge c \dashv\vdash (a \wedge c) \vee (b \wedge c)$$

$$c \wedge (a \vee b) \dashv\vdash (c \wedge a) \vee (c \wedge b)$$

$$a \vee (b \vee c) \dashv\vdash (a \vee b) \vee c$$

$$a \wedge (b \wedge c) \dashv\vdash (a \wedge b) \wedge c$$

### Pasos recursivos de congruencia (con $A \dashv\vdash A'$ )

$$A \wedge B \dashv\vdash A' \wedge B$$

$$A \vee B \dashv\vdash A' \vee B$$

$$\neg A \dashv\vdash \neg A'$$

**¡26 demostraciones!**

## Ejemplo

$$\begin{array}{c}
 \text{Ax} \frac{}{(\neg a \wedge a \wedge \neg b)} \quad \quad \quad \Pi_L \quad \quad \quad \frac{\Gamma_1 \vdash b \wedge a \wedge \perp}{\Gamma, b \wedge a \wedge \perp \vdash \perp} \text{Ax} \\
 \Gamma \vdash \vee (b \wedge a \wedge \perp) \quad \Gamma, \neg a \wedge a \wedge \neg b \vdash \perp \quad \frac{}{\Gamma, b \wedge a \wedge \perp \vdash \perp} \text{E}\wedge_{\perp} \\
 \hline
 \Gamma = (\neg a \wedge a \wedge \neg b) \vee (b \wedge a \wedge \perp) \vdash \perp \quad \text{E}\vee
 \end{array}$$

donde

$$\begin{array}{c}
 \frac{\Gamma_1 \vdash \neg a \wedge a \wedge \neg b}{\Gamma_1 \vdash \neg a} \text{Ax} \quad \frac{\Gamma_1 \vdash \neg a \wedge a \wedge \neg b}{\Gamma_1 \vdash a} \text{Ax} \\
 \text{E}\wedge_{\neg a} \quad \text{E}\wedge_a \\
 \Pi_L = \frac{\Gamma_1 \vdash \neg a \quad \Gamma_1 \vdash a}{\Gamma_1 = \Gamma, b \wedge a \wedge \perp \vdash \perp} \text{E}\neg
 \end{array}$$

## Ejemplo

$$\begin{array}{c}
 \text{Ax} \frac{}{(\neg a \wedge a \wedge \neg b)} \quad \Pi_L \quad \frac{\Gamma_1 \vdash b \wedge a \wedge \perp}{\Gamma, b \wedge a \wedge \perp \vdash \perp} \text{Ax} \\
 \frac{\Gamma \vdash \vee (b \wedge a \wedge \perp) \quad \Gamma, \neg a \wedge a \wedge \neg b \vdash \perp}{\Gamma = (\neg a \wedge a \wedge \neg b) \vee (b \wedge a \wedge \perp) \vdash \perp} \text{E}\vee \quad \text{E}\wedge_{\perp}
 \end{array}$$

donde

$$\Pi_L = \frac{\frac{\Gamma_1 \vdash \neg a \wedge a \wedge \neg b}{\Gamma_1 \vdash \neg a} \text{Ax} \quad \frac{\Gamma_1 \vdash \neg a \wedge a \wedge \neg b}{\Gamma_1 \vdash a} \text{Ax}}{\Gamma_1 = \Gamma, b \wedge a \wedge \perp \vdash \perp} \text{E}\neg$$

## Lema (Regla admisible $E\wedge_{\varphi}$ )

$$\frac{\Gamma \vdash \varphi_1 \wedge \dots \wedge \varphi_i \wedge \dots \wedge \varphi_n \quad n \in \mathbb{N}}{\Gamma \vdash \varphi_i} E\wedge_{\varphi_i}$$

- **Completo** para lógica proposicional y **heurístico** para primer orden.
- Esto es aceptable, la validez de LPO es indecidible (Teorema de Church).
- Elimina los  $\forall$  consecutivos de a lo sumo una hipótesis. Pero le faltan más cosas.

Ejemplo de falla en eliminación

```
1 axiom ax1: forall X . p(X) -> q(X)
2 axiom ax2: forall X . p(X)
3 theorem t: q(a)
4 proof
5   thus q(a) by ax1, ax2
6 end
```

# Descarga de conjunciones

Si la tesis es una conjunción, se puede probar un subconjunto de ella y se reduce el resto.

Descarga

```
1  axiom "a": a
2  axiom "b": b
3  axiom "c": c
4  axiom "d": d
5  axiom "e": e
6  theorem "and discharge":
7      (a & b) & ((c & d) & e)
8  proof
9      thus a & e by "a", "e"
10     thus d by "d"
11     thus b & c by "b", "c"
12 end
```

(TODO: Agregar esto)



## Extracción de testigos

## Extracción simple

```
1 axiom ax: es_bajo(juan)
2 theorem t: exists Alguien . es_bajo(Alguien)
3 proof
4   take Alguien := juan
5   thus es_bajo(juan) by ax
6 end
```

## Extracción simple

```
1 axiom ax: es_bajo(juan)
2 theorem t: exists Alguien . es_bajo(Alguien)
3 proof
4   take Alguien := juan
5   thus es_bajo(juan) by ax
6 end
```

**take** <var> := <term>

$$\frac{\Gamma \vdash A\{x := t\}}{\Gamma \vdash \exists x.A} \text{I}\exists$$

# Extracción indirecta con instanciación

## Extracción con instanciación

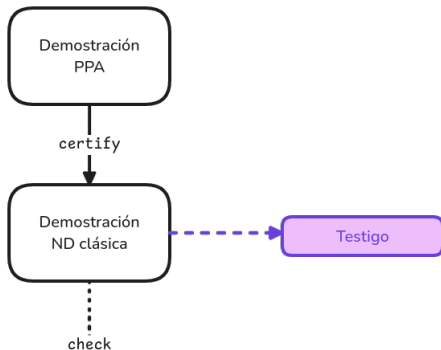
```
1  axiom cero_min: forall N . cero < N
2  axiom lt_leq: forall N . forall M . M < N -> M <= N
3
4  theorem todo_numero_tiene_lt: forall N. exists M . M < N
5  proof
6      let N
7      take M := cero
8      thus cero < N by cero_min
9  end
10
11 theorem todo_numero_tiene_leq: forall N. exists M . M <= N
12 proof
13     let N'
14     consider Min st h: Min < N' by todo_numero_tiene_lt
15     take M := Min
16     thus Min <= N' by h, lt_leq
17 end
```

# Extracción por el absurdo

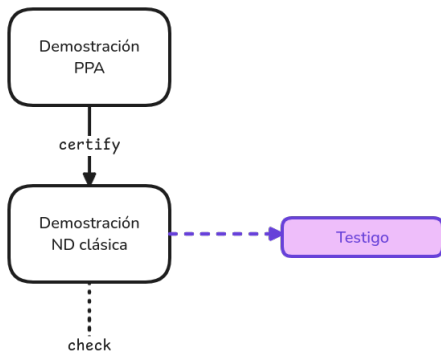
## Extracción por el absurdo

```
1 axiom juanEsBajo: bajo(juan)
2
3 theorem noTodoElMundoEsAlto: ~forall X. ~bajo(X)
4 proof
5   suppose todosSonAltos: forall X. ~bajo(X)
6   thus false by juanEsBajo, todosSonAltos
7 end
8
9 theorem hayAlguienBajo: exists X. bajo(X)
```

- En general  $\exists x. \varphi \equiv \neg \forall x. \neg \varphi$ .
- Sin **take** ( $\exists$ ) explícito, igual podemos extraer el testigo a partir del **theorem** hayAlguienBajo: juan.
- La implementación no es tan directa como buscar un  $\exists$  en el árbol de la demostración.



- Buscamos un mecanismo general que nos permita extraer testigos a partir de demostraciones en **deducción natural clásica**



- Buscamos un mecanismo general que nos permita extraer testigos a partir de demostraciones en **deducción natural clásica**
- Pero la lógica clásica **no es constructiva**, por LEM:

$$\frac{}{\Gamma \vdash A \vee \neg A} \text{LEM}$$

# Demostración no constructiva

## Ejemplo (Fórmula sin demostración constructiva)

Sea  $C$  algo indecidible (tipo HALT), queremos ver que vale

$$\exists y. (y = 1 \wedge C) \vee (y = 0 \wedge \neg C)$$



## Ejemplo (Fórmula sin demostración constructiva)

Sea  $C$  algo indecidible (tipo HALT), queremos ver que vale

$$\exists y. (y = 1 \wedge C) \vee (y = 0 \wedge \neg C)$$

podemos demostrarlo por LEM, sabemos que vale  $C \vee \neg C$

- Supongamos que vale  $C$ . Tomo  $y = 1$ .
- Supongamos que vale  $\neg C$ . Tomo  $y = 0$ .



## Ejemplo (Fórmula sin demostración constructiva)

Sea  $C$  algo indecidible (tipo HALT), queremos ver que vale

$$\exists y.(y = 1 \wedge C) \vee (y = 0 \wedge \neg C)$$

podemos demostrarlo por LEM, sabemos que vale  $C \vee \neg C$

- Supongamos que vale  $C$ . Tomo  $y = 1$ .
- Supongamos que vale  $\neg C$ . Tomo  $y = 0$ . □

¡No nos dice cual es cierto! No es *constructiva*. No tenemos forma de saber si es cierto  $C$  o  $\neg C$  (indecidible).

## Ejemplo (Fórmula sin demostración constructiva)

Sea  $C$  algo indecidible (tipo HALT), queremos ver que vale

$$\exists y. (y = 1 \wedge C) \vee (y = 0 \wedge \neg C)$$

podemos demostrarlo por LEM, sabemos que vale  $C \vee \neg C$

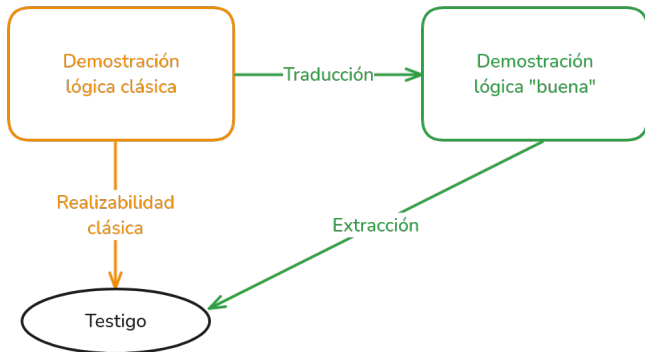
- Supongamos que vale  $C$ . Tomo  $y = 1$ .
- Supongamos que vale  $\neg C$ . Tomo  $y = 0$ . □

¡No nos dice cual es cierto! No es *constructiva*. No tenemos forma de saber si es cierto  $C$  o  $\neg C$  (indecidible).

¿Entonces por qué lógica clásica?

- Existen fórmulas que admiten demostraciones constructivas y no constructivas, y otras *solo no constructivas* (i.e. clásicas).
- Lógica clásica permite razonar por el absurdo, con  $E_{\neg\neg} \equiv \text{LEM}$

# Clases de estrategias de extracción



Clases de estrategias de extracción de demostraciones en lógica clásica:

- **Directas:** Extraer directamente de demostraciones clásicas. Técnicas de *realizabilidad clásica* (Semánticas de  $\lambda$ -cálculos clásicos).
- **Indirectas:** Convertir la demostración a una lógica que se porte mejor y extraer de ahí.

**lógica intuicionista** = lógica clásica – LEM

Características:

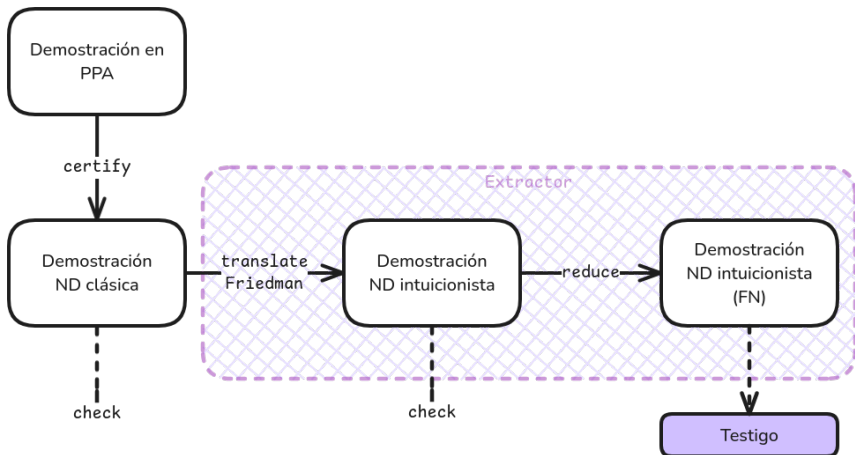
- No tiene LEM<sup>3</sup>, entonces siempre es constructiva.
- Siempre permite hacer extracción de testigos: proceso de normalización con *forma normal* buena, una demostración de un  $\exists$  debería comenzar con  $I\exists$  y de ahí sacás el testigo.

$$\frac{\Gamma \vdash A\{x := t\}}{\Gamma \vdash \exists x.A} I\exists$$

---

<sup>3</sup>Ni principios de razonamiento equivalentes, como  $E\neg\neg$

# Estrategia de extracción indirecta



# Traducción de doble negación relativizada

## Definición (Traducción de doble negación relativizada)

Sea  $\neg_R A \equiv A \rightarrow R$ , se define la traducción de doble negación relativizada:

$$\perp^{\neg\neg} = \perp$$

$$A^{\neg\neg} = \neg_R \neg_R A \quad \text{con } A \text{ atómica}$$

$$(\neg A)^{\neg\neg} = \neg_R A^{\neg\neg}$$

$$(A \wedge B)^{\neg\neg} = A^{\neg\neg} \wedge B^{\neg\neg}$$

$$(A \vee B)^{\neg\neg} = \neg_R (\neg_R A^{\neg\neg} \wedge \neg_R B^{\neg\neg})$$

$$(A \rightarrow B)^{\neg\neg} = A^{\neg\neg} \rightarrow B^{\neg\neg}$$

$$(\forall x. A)^{\neg\neg} = \forall x. A^{\neg\neg}$$

$$(\exists x. A)^{\neg\neg} = \neg_R \forall x. \neg_R A^{\neg\neg}$$

## Teorema

Si  $\Pi \triangleright \Gamma \vdash_C A$ , luego  $\Pi^{\neg\neg} \triangleright \Gamma^{\neg\neg} \vdash_I A^{\neg\neg}$

# Traducción de doble negación relativizada

## Definición (Traducción de doble negación relativizada)

Sea  $\neg_R A \equiv A \rightarrow R$ , se define la traducción de doble negación relativizada:

$$\perp^{\neg\neg} = \perp$$

$$A^{\neg\neg} = \neg_R \neg_R A \quad \text{con } A \text{ atómica}$$

$$(\neg A)^{\neg\neg} = \neg_R A^{\neg\neg}$$

$$(A \wedge B)^{\neg\neg} = A^{\neg\neg} \wedge B^{\neg\neg}$$

$$(A \vee B)^{\neg\neg} = \neg_R (\neg_R A^{\neg\neg} \wedge \neg_R B^{\neg\neg})$$

$$(A \rightarrow B)^{\neg\neg} = A^{\neg\neg} \rightarrow B^{\neg\neg}$$

$$(\forall x. A)^{\neg\neg} = \forall x. A^{\neg\neg}$$

$$(\exists x. A)^{\neg\neg} = \neg_R \forall x. \neg_R A^{\neg\neg}$$

## Teorema

Si  $\Pi \triangleright \Gamma \vdash_C A$ , luego  $\Pi^{\neg\neg} \triangleright \Gamma^{\neg\neg} \vdash_I A^{\neg\neg}$



## Definición (Fórmulas conjuntivas)

$$C ::= \perp \mid \top \mid p(t_1, \dots, t_n) \mid C \wedge C$$

## Teorema (Traducción de Friedman)

Sea  $\varphi$  una fórmula **conjuntiva**. Si tenemos

$$\Pi \triangleright \Gamma \vdash_C \forall y_1 \dots \forall y_n. \exists x. \varphi(x, y_1, \dots, y_n),$$

*podemos generar una demostración intuicionista de la misma fórmula.*

# El truco de Friedman

## Definición (Fórmulas conjuntivas)

$$C ::= \perp \mid \top \mid p(t_1, \dots, t_n) \mid C \wedge C$$

## Teorema (Traducción de Friedman)

Sea  $\varphi$  una fórmula **conjuntiva**. Si tenemos

$$\Pi \triangleright \Gamma \vdash_C \forall y_1 \dots \forall y_n. \exists x. \varphi(x, y_1, \dots, y_n),$$

*podemos generar una demostración intuicionista de la misma fórmula.*

## Lema (Traducción de Friedman simplificada)

Sea  $\varphi$  una fórmula conjuntiva. Si tenemos  $\Pi \triangleright \Gamma \vdash_C \exists x. \varphi$ , podemos generar una demostración intuicionista de la misma fórmula.

## Demostración.

Aplicando la traducción con  $R = \exists x.\varphi$ , tenemos que

$$(\Pi \triangleright \Gamma \vdash_C \exists x.\varphi)^{\neg\neg} \Leftrightarrow \Pi^{\neg\neg} \triangleright \Gamma^{\neg\neg} \vdash_I \neg_R \forall x. \neg_R \varphi^{\neg\neg}$$

Luego,

# El truco de Friedman

## Demostración.

Aplicando la traducción con  $R = \exists x.\varphi$ , tenemos que

$$(\Pi \triangleright \Gamma \vdash_C \exists x.\varphi)^{\neg\neg} \Leftrightarrow \Pi^{\neg\neg} \triangleright \Gamma^{\neg\neg} \vdash_I \neg_R \forall x. \neg_R \varphi^{\neg\neg}$$

Luego,

$$\frac{\Pi^{\neg\neg} \quad \frac{\frac{\frac{\overline{\Gamma^{\neg\neg}, \varphi \vdash_I \varphi} \text{Ax}}{\Gamma^{\neg\neg}, \varphi \vdash_I R = \exists x.\varphi} \text{I}\exists}{\Gamma^{\neg\neg} \vdash_I \neg_R \varphi} \text{I}\rightarrow}{\Gamma^{\neg\neg} \vdash_I \neg_R \varphi^{\neg\neg}} \text{cut, I}(\neg_R \cdot \neg\neg)}{\Gamma^{\neg\neg} \vdash_I \forall x \neg_R \varphi^{\neg\neg}} \text{I}\forall}{\Gamma^{\neg\neg} \vdash_I \exists x.\varphi} \text{E}\rightarrow$$



## Lema (Introducción de $\neg_R$ )

*Si  $A$  es conjuntiva, entonces vale  $\neg_R A \vdash_I \neg_R A^{\neg\neg}$  y lo notamos con la regla admisible  $I(\neg_R \cdot \neg\neg)$ .*

# Introducción de negación relativizada

## Lema (Introducción de $\neg_R$ )

Si  $A$  es conjuntiva, entonces vale  $\neg_R A \vdash_I \neg_R A^{\neg\neg}$  y lo notamos con la regla admisible  $I(\neg_R \cdot \neg\neg)$ .

## Demostración.

Por inducción estructural en la fórmula. Intuición:

- Atómicas trivial. Para predicados,

$$\neg_R A \vdash_I \neg_R A^{\neg\neg} \iff \neg_R A \vdash_I \neg_R \neg_R \neg_R A$$

sale con *eliminación de triple negación*.

- Conjunción tiene algunos trucos.



## Teorema

*Si  $\Pi \triangleright \Gamma \vdash_C A$ , luego  $\Pi^{\neg\neg} \triangleright \Gamma^{\neg\neg} \vdash_I A^{\neg\neg}$*

## Teorema

Si  $\Pi \triangleright \Gamma \vdash_C A$ , luego  $\Pi^{\neg\neg} \triangleright \Gamma^{\neg\neg} \vdash_I A^{\neg\neg}$

## Demostración.

Inducción estructural sobre la demostración. **Estrategia:** traducimos recursivamente las partes de  $\Pi$  y las usamos para construir una nueva demostración de  $A^{\neg\neg}$ .

- $I\wedge$ ,  $E\wedge_1$ ,  $E\wedge_2$ ,  $I\rightarrow$ ,  $E\rightarrow$ ,  $I\vee_1$ ,  $I\vee_2$ ,  $I\forall$ ,  $E\forall$ ,  $I\neg$ ,  $E\neg$ ,  $IT$ ,  $Ax$ ,  $I\exists$  fáciles.
- **LEM** interesante.
- $E\perp$  inducción estructural sobre la fórmula.
- $E\forall$  y  $E\exists$  son análogos y requieren un truco: usar la eliminación de la doble negación. No vale  $E\neg\neg$  pero si  $E\neg\neg_R$  (probado por inducción estructural sobre la fórmula).





# Traducción de introducción de conjunción

## Lema (Traducción de $I_{\wedge}$ )

$$\frac{\begin{array}{c} \Pi_A \\ \Gamma \vdash_I A \end{array} \quad \begin{array}{c} \Pi_B \\ \Gamma \vdash_I B \end{array}}{\Gamma \vdash_I A \wedge B} I_{\wedge}$$

*Es posible demostrar*  
 $(A \wedge B)^{\neg\neg} = A^{\neg\neg} \wedge B^{\neg\neg}$ .

## Demostración.

Usando la HI:  $\Pi_A^{\neg\neg} \triangleright \Gamma^{\neg\neg} \vdash_I A^{\neg\neg}$  y  $\Pi_B^{\neg\neg} \triangleright \Gamma^{\neg\neg} \vdash_I B^{\neg\neg}$ , generamos

$$\frac{\begin{array}{c} \Pi_A^{\neg\neg} \\ \Gamma^{\neg\neg} \vdash_I A^{\neg\neg} \end{array} \quad \begin{array}{c} \Pi_B^{\neg\neg} \\ \Gamma^{\neg\neg} \vdash_I B^{\neg\neg} \end{array}}{\Gamma^{\neg\neg} \vdash_I A^{\neg\neg} \wedge B^{\neg\neg}} I_{\wedge}$$



# Problema con axiomas

## Lema (Traducción de Friedman simplificada)

Sea  $\varphi$  una fórmula conjuntiva. Si tenemos  $\Gamma \vdash_C \exists x.\varphi$ , podemos generar una demostración intuicionista de la misma fórmula  $\Gamma^{\neg\neg} \vdash_I \exists x.\varphi$ .

**Problema:** la demostración normalizada no puede comenzar con  $\exists$

$$p(v)^{\neg\neg} \vdash_I \exists x.p(x) \iff \neg_R \neg_R p(v) \vdash_I \exists x.p(x)$$

Nos gustaría *mantener el contexto original*:  $p(v) \vdash_I \exists x.p(x)$

## Manteniendo el contexto

Luego de la traducción, antes de reducir, reemplazamos cada cita  $(Ax)$  de un axioma  $h : \varphi^{\neg\neg}$  por la demostración  $\varphi \vdash_I \varphi^{\neg\neg}$ .

## Lema (Introducción de la traducción $\neg\neg$ )

Si  $\varphi$  es una F-fórmula, vale  $\varphi \vdash_I \varphi^{\neg\neg}$ .

## F-fórmulas

$$A ::= \perp \mid \top \mid p(t_1, \dots, t_n)$$
$$F ::= A$$
$$\mid F \wedge F \mid F \vee F$$
$$\mid \forall x.F \mid \exists x.F$$
$$\mid C \rightarrow F \mid \neg C$$
$$C ::= A \mid C \wedge C$$

- $A$ : Fórmulas atómicas
- $F$ : F-fórmulas
- $C$ : Fórmulas conjuntivas

## F-fórmulas

$$A ::= \perp \mid \top \mid p(t_1, \dots, t_n)$$
$$F ::= A$$
$$\mid F \wedge F \mid F \vee F$$
$$\mid \forall x.F \mid \exists x.F$$
$$\mid C \rightarrow F \mid \neg C$$
$$C ::= A \mid C \wedge C$$

- $A$ : Fórmulas atómicas
- $F$ : F-fórmulas
- $C$ : Fórmulas conjuntivas

## Fórmulas de Harrop

$$G ::= A$$
$$\mid G \wedge G \mid G \vee G$$
$$\mid \forall x.G \mid \exists x.G$$
$$\mid H \rightarrow G$$
$$H ::= A \mid H \wedge H$$
$$\mid \forall x.H$$
$$\mid G \rightarrow A$$

- $G$ : G-fórmulas
- $H$ : Fórmulas Harrop Hereditarias
- Generalización de cláusulas de Horn, usadas para realizabilidad

**Motivación:** evitar “desvíos superfluos”.

## Ejemplo

$$\frac{\frac{\frac{}{A \vdash A} \text{Ax}}{\vdash A \rightarrow A} \text{I} \rightarrow \quad \frac{\frac{}{B \vdash B} \text{Ax}}{\vdash B \rightarrow B} \text{I} \rightarrow}{\vdash (A \rightarrow A) \wedge (B \rightarrow B)} \text{I} \wedge \quad \rightsquigarrow \quad \frac{\frac{}{A \vdash A} \text{Ax}}{\vdash A \rightarrow A} \text{I} \rightarrow}$$
$$\frac{}{\vdash A \rightarrow A} \text{E} \wedge_1$$

**Motivación:** evitar “desvíos superfluos”.

## Ejemplo

$$\frac{\frac{\frac{}{A \vdash A} Ax}{\vdash A \rightarrow A} I \rightarrow \quad \frac{\frac{}{B \vdash B} Ax}{\vdash B \rightarrow B} I \rightarrow}{\vdash (A \rightarrow A) \wedge (B \rightarrow B)} I \wedge \quad \rightsquigarrow \quad \frac{\frac{}{A \vdash A} Ax}{\vdash A \rightarrow A} I \rightarrow$$

$E \wedge_1$

- Se van a ver todos de esa forma: Una **eliminación** demostrada inmediatamente por su **introducción** correspondiente.
- Ejemplo:  $E \wedge_1$  demostrada por  $I \wedge$ .
- Idea: Simplificarlos sucesivamente hasta que no haya más y esté en **forma normal**.

- **Isomorfismo Curry-Howard:** correspondencia entre demostraciones en deducción natural y términos de  $\lambda$ -cálculo.
- Normalización de demostraciones corresponde a semántica de  $\lambda$ -cálculo

## Ejemplo

Conjunciones como el tipo de las tuplas, y las eliminaciones como proyecciones.

$$\pi_1(\langle M_1, M_2 \rangle) \rightsquigarrow M_1$$

$$\pi_2(\langle M_1, M_2 \rangle) \rightsquigarrow M_2$$

$$\frac{\frac{\frac{\Pi_1}{\Gamma \vdash A_1} \quad \frac{\Pi_2}{\Gamma \vdash A_2}}{\Gamma \vdash A_1 \wedge A_2} I_{\wedge} \quad \rightsquigarrow \quad \frac{\Pi_i}{\Gamma \vdash A_i} E_{\wedge_i}}{\Gamma \vdash A_i} E_{\wedge_i}$$

$$\frac{\frac{\Pi_B}{\Gamma, h : A \vdash B} \mid \rightarrow_h \quad \frac{\Pi_A}{\Gamma \vdash A} \quad \text{E} \rightarrow}{\Gamma \vdash B} \rightsquigarrow \frac{\Pi_B}{\Gamma \vdash B}$$

- Primer idea:  $\Pi_B \triangleright \Gamma \vdash B$



# Normalización de implicación

$$\frac{\frac{\Pi_B}{\Gamma, h : A \vdash B} \text{I} \rightarrow_h \quad \frac{\Pi_A}{\Gamma \vdash A} \text{E} \rightarrow}{\Gamma \vdash B} \text{E} \rightarrow \rightsquigarrow \frac{\Pi_B \{h := \Pi_A\}}{\Gamma \vdash B}$$

- Primer idea:  ~~$\Pi_B \triangleright \Gamma \vdash B$~~
- $\Pi_B$  requiere  $h : A$ , agregada por  $\text{I} \rightarrow_h$
- Correcto: usar  $\Pi_B$ , pero *sustituyendo* todas las ocurrencias de la hipótesis  $h$  por la demostración  $\Pi_A$  (sin capturas).

Además, hay reglas para

- $E\exists$  con  $I\exists$ ,
- $E\forall$  con  $I\forall$ ,
- $E\neg$  con  $I\neg$ ,
- $E\vee$  con  $I\vee$

**Idea original:** reducir en un paso sucesivamente hasta que sea irreducible.

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \text{I}\wedge$$

$$\vdots$$
$$\Pi$$

reducíamos de a un paso a la vez  $A \rightsquigarrow A_1 \rightsquigarrow A_2 \rightsquigarrow \dots \rightsquigarrow A^*$  hasta llegar a  $A^*$  irreducible y recién ahí aplicamos mismo para  $B$ . En cada paso se recorría todo el árbol.

Problema: Muy lento

# Estrategia de reducción

Dos tipos de estrategias:

- Un paso
- Muchos pasos
  - **Gross Knuth**: reduce en muchos pasos todos los sub-términos posibles al mismo tiempo.

En un solo paso, reducimos

$$\frac{\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge I}{\vdots} \Pi \quad \rightsquigarrow \quad \frac{\frac{\Gamma \vdash A^* \quad \Gamma \vdash B^*}{\Gamma \vdash A \wedge B} \wedge I}{\vdots} \Pi$$

- **Incompleta:** no contempla *reducciones permutativas* (mezclando introducciones y eliminaciones de conectivos distintos).

- **Incompleta:** no contempla *reducciones permutativas* (mezclando introducciones y eliminaciones de conectivos distintos).
  - *Mejora:* Implementarlas.

- **Incompleta:** no contempla *reducciones permutativas* (mezclando introducciones y eliminaciones de conectivos distintos).
  - *Mejora:* Implementarlas.
- **Ineficiente:** en cada paso reinicia la búsqueda de todos los focos de evaluación.

- **Incompleta:** no contempla *reducciones permutativas* (mezclando introducciones y eliminaciones de conectivos distintos).
  - *Mejora:* Implementarlas.
- **Ineficiente:** en cada paso reinicia la búsqueda de todos los focos de evaluación.
  - *Mejora:* Usar una máquina abstracta que implemente reducción a forma normal, Crégut para reducción *call-by-name* fuerte o la máquina de Biernacka para reducción *call-by-need* fuerte.



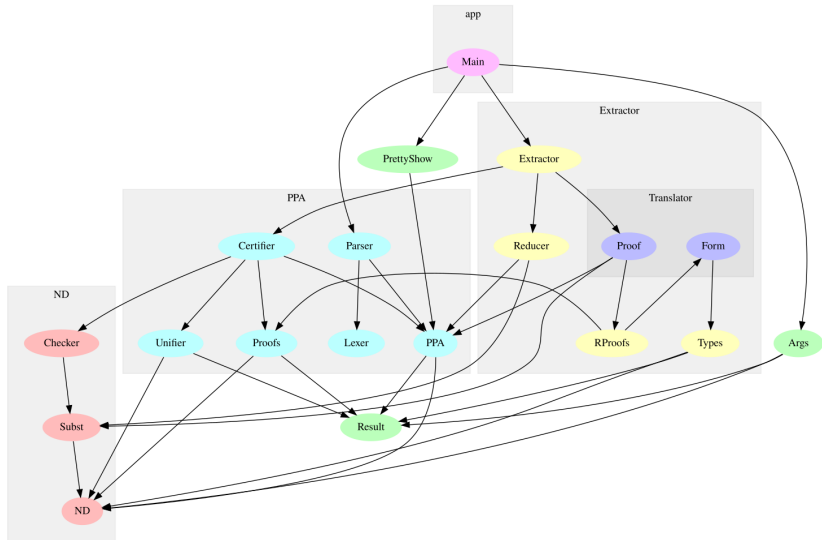
# Programa con falla de extracción

```
1 axiom ax_1: roba(tuco) | mata(tuco)
2 axiom ax_2: forall X . roba(X) -> criminal(X)
3 axiom ax_3: forall X . mata(X) -> criminal(X)
4
5 theorem t: exists X . criminal(X)
6 proof
7   take X := tuco
8   cases by ax_1
9     case roba(tuco)
10       hence criminal(tuco)
11         by ax_2
12
13     case mata(tuco)
14       hence criminal(tuco)
15         by ax_3
16   end
17 end
```

Certifica el programa generando una demostración que en lugar de comenzar con  $\exists$ , comienza con  $\forall$  y en cada rama introduce el existencial dos veces, con el mismo término

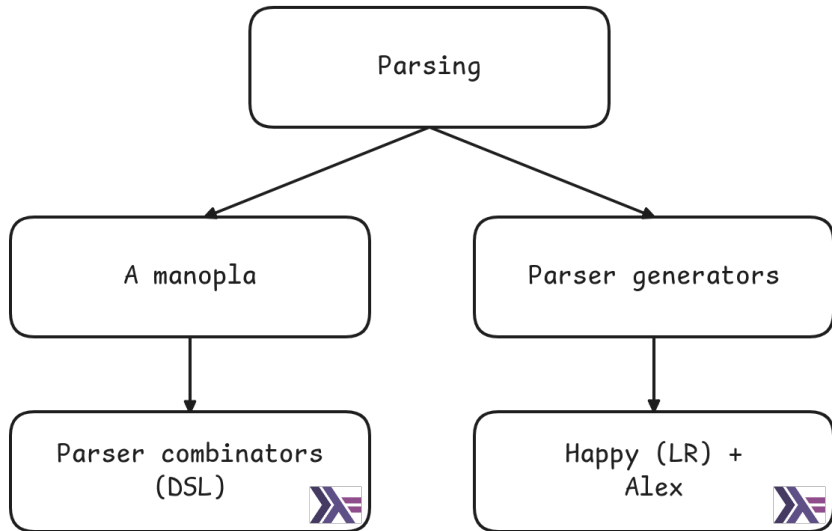
## Detalles de implementación

# La herramienta ppa



Haskell, 19 módulos con 330 tests

String -> Estructura



## Trabajo futuro

- Sofisticar el *solver heurístico* del **by** (recursivo, eliminar más de una hipótesis).

- Sofisticar el *solver heurístico* del **by** (recursivo, eliminar más de una hipótesis).
- Extender traducción de Friedman a más de un existencial.

- Sofisticar el *solver heurístico* del **by** (recursivo, eliminar más de una hipótesis).
- Extender traducción de Friedman a más de un existencial.
- Refinar fórmulas conjuntivas. Profundizar vínculo con Harrop.



- Sofisticar el *solver heurístico* del **by** (recursivo, eliminar más de una hipótesis).
- Extender traducción de Friedman a más de un existencial.
- Refinar fórmulas conjuntivas. Profundizar vínculo con Harrop.
- Sofisticar reducción de demostraciones: hacer completa (reglas permutativas) y más eficiente (implementando máquina abstracta).

- Sofisticar el *solver heurístico* del **by** (recursivo, eliminar más de una hipótesis).
- Extender traducción de Friedman a más de un existencial.
- Refinar fórmulas conjuntivas. Profundizar vínculo con Harrop.
- Sofisticar reducción de demostraciones: hacer completa (reglas permutativas) y más eficiente (implementando máquina abstracta).
- Mejorar PPA como lenguaje de programación: módulos, importar archivos, biblioteca estándar.

- Sofisticar el *solver heurístico* del **by** (recursivo, eliminar más de una hipótesis).
- Extender traducción de Friedman a más de un existencial.
- Refinar fórmulas conjuntivas. Profundizar vínculo con Harrop.
- Sofisticar reducción de demostraciones: hacer completa (reglas permutativas) y más eficiente (implementando máquina abstracta).
- Mejorar PPA como lenguaje de programación: módulos, importar archivos, biblioteca estándar.
- Extender PPA con tipos (usando LPO *many-sorted* con géneros).

- Sofisticar el *solver heurístico* del **by** (recursivo, eliminar más de una hipótesis).
- Extender traducción de Friedman a más de un existencial.
- Refinar fórmulas conjuntivas. Profundizar vínculo con Harrop.
- Sofisticar reducción de demostraciones: hacer completa (reglas permutativas) y más eficiente (implementando máquina abstracta).
- Mejorar PPA como lenguaje de programación: módulos, importar archivos, biblioteca estándar.
- Extender PPA con tipos (usando LPO *many-sorted* con géneros).
- Modelar de forma nativa inducción (segundo orden) e igualdad.

- Sofisticar el *solver heurístico* del **by** (recursivo, eliminar más de una hipótesis).
- Extender traducción de Friedman a más de un existencial.
- Refinar fórmulas conjuntivas. Profundizar vínculo con Harrop.
- Sofisticar reducción de demostraciones: hacer completa (reglas permutativas) y más eficiente (implementando máquina abstracta).
- Mejorar PPA como lenguaje de programación: módulos, importar archivos, biblioteca estándar.
- Extender PPA con tipos (usando LPO *many-sorted* con géneros).
- Modelar de forma nativa inducción (segundo orden) e igualdad.
- Mejorar reporte de errores (muy bajo nivel).

- QR con la página
- Preguntas