Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales
Departamento de Computación

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

Tesis de Licenciatura en Ciencias de la Computación

Manuel Panichelli

Director: Pablo Barenbaum

Buenos Aires, 2024

PPA - UN ASISTENTE DE DEMOSTRACIÓN PARA LÓGICA DE PRIMER ORDEN CON EXTRACCIÓN DE TESTIGOS USANDO LA TRADUCCIÓN DE FRIEDMAN

La princesa Leia, líder del movimiento rebelde que desea reinstaurar la República en la galaxia en los tiempos ominosos del Imperio, es capturada por las malévolas Fuerzas Imperiales, capitaneadas por el implacable Darth Vader. El intrépido Luke Skywalker, ayudado por Han Solo, capitán de la nave espacial "El Halcón Milenario", y los androides, R2D2 y C3PO, serán los encargados de luchar contra el enemigo y rescatar a la princesa para volver a instaurar la justicia en el seno de la Galaxia (aprox. 200 palabras).

Palabras claves: Guerra, Rebelión, Wookie, Jedi, Fuerza, Imperio (no menos de 5).

PPA - A PROOF-ASSISTANT FOR FIRST-ORDER LOGIC WITH WITNESS EXTRACTION USING FRIEDMAN'S TRANSLATION

In a galaxy far, far away, a psychopathic emperor and his most trusted servant – a former Jedi Knight known as Darth Vader – are ruling a universe with fear. They have built a horrifying weapon known as the Death Star, a giant battle station capable of annihilating a world in less than a second. When the Death Star's master plans are captured by the fledgling Rebel Alliance, Vader starts a pursuit of the ship carrying them. A young dissident Senator, Leia Organa, is aboard the ship & puts the plans into a maintenance robot named R2-D2. Although she is captured, the Death Star plans cannot be found, as R2 & his companion, a tall robot named C-3PO, have escaped to the desert world of Tatooine below. Through a series of mishaps, the robots end up in the hands of a farm boy named Luke Skywalker, who lives with his Uncle Owen & Aunt Beru. Owen & Beru are viciously murdered by the Empire's stormtroopers who are trying to recover the plans, and Luke & the robots meet with former Jedi Knight Obi-Wan Kenobi to try to return the plans to Leia Organa's home, Alderaan. After contracting a pilot named Han Solo & his Wookiee companion Chewbacca, they escape an Imperial blockade. But when they reach Alderaan's coordinates, they find it destroyed - by the Death Star. They soon find themselves caught in a tractor beam & pulled into the Death Star. Although they rescue Leia Organa from the Death Star after a series of narrow escapes, Kenobi becomes one with the Force after being killed by his former pupil - Darth Vader. They reach the Alliance's base on Yavin's fourth moon, but the Imperials are in hot pursuit with the Death Star, and plan to annihilate the Rebel base. The Rebels must quickly find a way to eliminate the Death Star before it destroys them as it did Alderaan (aprox. 200 palabras).

Keywords: War, Rebellion, Wookie, Jedi, The Force, Empire (no menos de 5).

AGRADECIMIENTOS

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce sapien ipsum, aliquet eget convallis at, adipiscing non odio. Donec porttitor tincidunt cursus. In tellus dui, varius sed scelerisque faucibus, sagittis non magna. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Mauris et luctus justo. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Mauris sit amet purus massa, sed sodales justo. Mauris id mi sed orci porttitor dictum. Donec vitae mi non leo consectetur tempus vel et sapien. Curabitur enim quam, sollicitudin id iaculis id, congue euismod diam. Sed in eros nec urna lacinia porttitor ut vitae nulla. Ut mattis, erat et laoreet feugiat, lacus urna hendrerit nisi, at tincidunt dui justo at felis. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Ut iaculis euismod magna et consequat. Mauris eu augue in ipsum elementum dictum. Sed accumsan, velit vel vehicula dignissim, nibh tellus consequat metus, vel fringilla neque dolor in dolor. Aliquam ac justo ut lectus iaculis pharetra vitae sed turpis. Aliquam pulvinar lorem vel ipsum auctor et hendrerit nisl molestie. Donec id felis nec ante placerat vehicula. Sed lacus risus, aliquet vel facilisis eu, placerat vitae augue.

Índice general

1. INTRODUCCIÓN

En este trabajo implementamos una asistente de demostración "PPA" (*Pani's proof assistant*) inspirado en Mizar.

PPA se puede referir a varias cosas: el lenguaje para escribir demostraciones, la herramienta (junto con su extracción de testigos).

1.1. Teoremas

In mathematics and formal logic, a theorem is a statement that has been proven, or can be proven.[a][2][3] The proof of a theorem is a logical argument that uses the inference rules of a deductive system to establish that the theorem is a logical consequence of the axioms and previously proved theorems.

In mainstream mathematics, the axioms and the inference rules are commonly left implicit, and, in this case, they are almost always those of Zermelo–Fraenkel set theory with the axiom of choice (ZFC), or of a less powerful theory, such as Peano arithmetic.[b] Generally, an assertion that is explicitly called a theorem is a proved result that is not an immediate consequence of other known theorems. Moreover, many authors qualify as theorems only the most important results, and use the terms lemma, proposition and corollary for less important theorems.

Completar con https://en.wikipedia.org/wiki/Theorem

1.2. Asistentes de demostraciones

- Son programs que asisten al usuario a la hora de escribir una demostración. Permiten representarlas en un programa.
- Aplicaciones: formalización de teoremas, verificación formal de programas, etc.
- Ejemplos: Coq, isabelle (isar), Mizar
- Reseña histórica de Mizar
- Ventajas: colaboración a gran escala (confianza en el checker), chequear el output de los LLMs

1.3. Arquitectura de PPA

- Por qué certificados (criterio de De Brujin)
- Certificados están en deducción natural. Sistema lógico que permite construir demostraciones mediante reglas de inferencia.
- PPA es un lenguaje que genera demostraciones "de bajo nivel"ND.
- razón de ser: Más práctico que demos de bajo nivel
- Implementado en Haskell

Principalmente hace dos cosas: certificar y extraer testigos.

1.4. Lógica de primer orden

Suponemos dados,

- Un conjunto infinito numerable de **variables** $\{x, y, z, \dots\}$
- Un conjunto infinito numerable de **símbolos de función** $\{f, g, h, \dots\}$
- Un conjunto infinito numerable de **símbolos de predicado** $\{p, q, r, \dots\}$

Def. 1 (Términos)**.** Los términos están dados por la gramática

$$\begin{aligned} t ::= {} & x && \text{(variables)} \\ \mid {} & f(t_1, \dots, t_n) && \text{(funciones)} \end{aligned}$$

Def. 2 (Fórmulas)**.** Las fórmulas están dadas por la gramática

$$\begin{aligned} A, B ::= {} & p(t_1, \dots, t_n) && \text{(predicados)} \\ \mid {} & \bot, \top && \text{(verdadero y falso)} \\ \mid {} & A \wedge B && \text{(conjunción)} \\ \mid {} & A \vee B && \text{(disyunción)} \\ \mid {} & A \to B && \text{(implicación)} \\ \mid {} & \neg A && \text{(negación)} \\ \mid {} & \forall x.A && \text{(cuantificador universal)} \\ \mid {} & \exists x.A && \text{(cuantificador existencial)} \end{aligned}$$

Los predicados son **fórmulas atómicas**. Los de aridad 0 además son llamados *variables proposicionales.*

Def. 3 (Variables libres y ligadas)**.** Las variables pueden ocurrir libres o ligadas. Los cuantificadores ligan a las variables, y usamos $fv(()A)$ para referirnos a las variables libres de una fórmula. Se define por inducción estructural de la siguiente forma.

- Términos

$$\begin{aligned} fv(x) &= \{x\} \\ fv(f(t_1, \dots, t_n)) &= \bigcup_{i \in 1 \dots n} fv(t_i) \end{aligned}$$

- Fórmulas

$$\begin{aligned} fv(\bot) &= \emptyset \\ fv(\top) &= \emptyset \\ fv(p(t_1, \dots, t_n)) &= \bigcup_{i \in 1 \dots n} fv(t_i) \\ fv(A \wedge B) &= fv(A) \cup fv(B) \\ fv(A \vee B) &= fv(A) \cup fv(B) \\ fv(A \to B) &= fv(A) \cup fv(B) \\ fv(\neg A) &= fv(A) \\ fv(\forall x.A) &= fv(A) \setminus x \\ fv(\exists x.A) &= fv(A) \setminus x \end{aligned}$$

2. DEDUCCIÓN NATURAL

Comencemos por las fundaciones: queremos armar un programa que permita escribir teoremas y demostraciones, pero, ¿cómo se representa una demostración en la computadora? No alcanza con hacerlo de la misma forma que escribimos demostraciones en papel (como en el Ejemplo 1). Debe ser una representación más precisa.

En el área de estudio de *teoría de pruebas*, en la cuál las demostraciones son un objeto matemático formal que puede ser estudiado, aparecen los *sistemas de inferencia* o *deductivos*: sistemas lógicos formales que permiten demostrar sentencias. Nos son útiles pues pueden ser modelados como un tipo abstracto de datos, por lo que son representables en la computadora.

Por ejemplo, supongamos que tenemos la siguiente *teoría* sobre exámenes en la facultad, que iremos iterando a lo largo de la tesis. Por ahora, en su versión proposicional. Si un alumno reprueba un final, entonces recursa. Si un alumno falta, entonces reprueba. Con estas dos, podríamos demostrar que si un alumno falta a un final, entonces recursa. Veamos cómo podría ser una demostración en lenguaje natural.

Ejemplo 1. 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. □

¿Cómo podrá ser formalizada en un *sistema de inferencia*?

2.1. El sistema de deducción natural

Los sistemas de inferencia en general están compuestos por

- **Lenguaje formal**: el conjunto L de fórmulas admitidas por el sistema. En nuestro caso, lógica de primer orden.
- **Reglas de inferencia**: lista de reglas que se usan para probar teoremas de axiomas y otros teoremas. Por ejemplo, *modus ponens* (si es cierto $A \to B$ y A, se puede concluir B) o *modus tollens* (si es cierto $A \to B$ y $\neg B$, se puede concluir $\neg A$)
- **Axiomas**: fórmulas de L que se asumen válidas. Todos los teoremas se derivan de axiomas. Por ejemplo, como usamos lógica clásica, vale el axioma *LEM* (Law of Excluded Middle): $A \vee \neg A$

El sistema particular que usamos se conoce como **deducción natural**, introducido por Gerhard Gentzen en [Gen35]. Tiene dos tipos de *reglas de inferencia* para cada conectivo ($\wedge$, $\vee$, $\exists$, ...) y cuantificador ($\forall$, $\exists$), que nos permite razonar de dos formas distintas.

- **Regla de introducción**: ¿Cómo demuestro una fórmula formada por este conectivo?
- **Regla de eliminación**: ¿Cómo uso una fórmula formada por este conectivo para demostrar otra?

Por ejemplo, la regla I$\wedge$ nos va a permitir *introducir* una conjunción, demostrarla. E$\vee$ *eliminar* una disyunción, usarla para demostrar otra fórmula. Primero vemos algunas definiciones preliminares, luego las reglas de inferencia, un ejemplo de una demostración, y finalmente explicamos cada regla en detalle.

Def. 4 (Contexto de demostración)**.** Definimos,

- Los **contextos de demostración** Γ como un conjunto de fórmulas, compuesto por las hipótesis que se asumen a lo largo de una demostración.
- Para algunas reglas es necesario conocer las variables libres de un contexto, que se definen de la forma esperable:

$$fv(\Gamma) = \bigcup_{A \in \Gamma} fv(A)$$

Def. 5 (Relación de consecuencia)**.** Las reglas de inferencia de la Figura 2.1 definen la relación de consecuencia $\vdash$, que nos permite escribir *juicios* $\Gamma \vdash A$. Intuitivamente pueden ser interpretados como "A es una consecuencia de las suposiciones de Γ"

Más precisamente, el juicio será cierto si en una cantidad finita de pasos podemos, a partir de las fórmulas de Γ, los axiomas y las reglas de inferencia, concluir A. En ese caso decimos que A es *derivable* a partir de Γ.

Cuando el contexto es omitido, $\vdash A$ se usa como abreviación de $\emptyset \vdash A$.

Def. 6 (Sustitución)**.** Notamos la **sustitución sin capturas** de todas las ocurrencias libres de la variable x por el término t en la fórmula A como

$$A\{x := t\}$$

Se explora en más detalle en la Subsección 2.5.3 Sustitución sin capturas

2.1.1. Reglas de inferencia

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,\mathrm{E}\bot \qquad \frac{}{\Gamma \vdash \top}\,\mathrm{I}\top$$

$$\frac{}{\Gamma \vdash A \vee \neg A}\,\mathrm{LEM} \qquad \frac{}{\Gamma, A \vdash A}\,\mathrm{Ax}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,\mathrm{I}\wedge$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,\mathrm{E}\wedge_1 \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,\mathrm{E}\wedge_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,\mathrm{I}\vee_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,\mathrm{I}\vee_2$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,\mathrm{E}\vee$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\,\mathrm{I}\to \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,\mathrm{E}\to$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,\mathrm{I}\neg \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,\mathrm{E}\neg$$

$$\frac{\Gamma \vdash A \qquad x \notin fv(\Gamma)}{\Gamma \vdash \forall x.A}\,\mathrm{I}\forall \qquad \frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A\{x := t\}}\,\mathrm{E}\forall$$

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

$$\frac{\Gamma \vdash \exists x.A \qquad \Gamma, A \vdash B \qquad x \notin fv(\Gamma, B)}{\Gamma \vdash B}\,\mathrm{E}\exists$$

Fig. 2.1: Reglas de inferencia para deducción natural de lógica clásica de primer orden

2.1.2. Ejemplo introductorio

Ejemplo 2. Demostración de Ejemplo 1 en deducción natural. Lo modelamos para un solo alumno y materia, sin cuantificadores. Notamos

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

Queremos probar entonces

$$\Big((X \to R) \wedge (F \to X)\Big) \to (F \to R)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash (X \to R) \wedge (F \to X)}\,\text{Ax}}{\Gamma \vdash X \to R}\,\text{E}\wedge_1 \quad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash (X \to R) \wedge (F \to X)}\,\text{Ax}}{\Gamma \vdash F \to X}\,\text{E}\wedge_2 \quad \dfrac{}{\Gamma \vdash F}\,\text{Ax}}{\Gamma \vdash X}\,\text{E}\to}{\dfrac{\Gamma = (X \to R) \wedge (F \to X),\ F \vdash R}{(X \to R) \wedge (F \to X) \vdash F \to R}\,\text{I}\to}\,\text{I}\to}{\vdash \Big((X \to R) \wedge (F \to X)\Big) \to (F \to R)}$$

Fig. 2.2: Demostración de $\big((X \to R) \wedge (F \to X)\big) \to (F \to R)$ en deducción natural

Las demostraciones en deducción natural son un árbol, en el que cada juicio está justificado por una regla de inferencia, que puede tener sub-árboles de demostración. La raíz es la fórmula a demostrar. Paso por paso,

- I→: *introducimos* la implicación. Para demostrarla, asumimos el antecedente y en base a eso demostramos el consecuente. Es decir asumimos $(X \to R) \wedge (F \to X)$, y en base a eso queremos deducir $F \to R$.
- I→: asumimos F, nos queda probar R. Nombramos el *contexto* de hipótesis como Γ.
- La estrategia para probar R es usando la siguiente cadena de implicaciones: $F \to X \to R$, y sabemos que vale F. Como tenemos que probar R, vamos de derecha a izquierda.
- E→: *eliminamos* una implicación, la usamos para deducir su conclusión demostrando el antecedente. Esta regla de inferencia tiene dos partes, probar la implicación $(X \to R)$, y probar el antecedente (X).
  - Para probar la implicación, tenemos que usar la hipótesis *eliminando* la conjunción y especificando cuál de las dos cláusulas estamos usando.
  - Para probar el antecedente X, es un proceso análogo pero usando la otra implicación y el hecho de que vale F por hipótesis.
- Las hojas del árbol, los casos base, suelen ser aplicaciones de la regla de inferencia Ax, que permite deducir fórmulas citando hipótesis del contexto.

2.2. Intuición detrás de las reglas

A continuación se explican brevemente las reglas de inferencia listadas en Figura 2.1.

2.2.1. Reglas base

$$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}\,\text{E}\bot \qquad \dfrac{}{\Gamma \vdash \top}\,\text{I}\top$$

$$\dfrac{}{\Gamma \vdash A \vee \neg A}\,\text{LEM} \qquad \dfrac{}{\Gamma, A \vdash A}\,\text{Ax}$$

- E⊥: a partir de $\bot$, algo que es falso, vamos a poder deducir cualquier fórmula.
- I⊤: $\top$ trivialmente vale siempre

- LEM: el *principio del tercero excluido* que vale en lógica clásica. Incluir este axioma es lo que hace que este sistema sea clásico.
- Ax: como ya vimos en el Ejemplo 2 , lo usamos para deducir fórmulas que ya tenemos como hipótesis.

2.2.2. Reglas de conjunciones y disyunciones

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\, \mathrm{I}\wedge$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\, \mathrm{E}\wedge_1 \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\, \mathrm{E}\wedge_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\, \mathrm{I}\vee_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\, \mathrm{I}\vee_2$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\, \mathrm{E}\vee$$

- I$\wedge$: para demostrar una conjunción, debemos demostrar ambas fórmulas.
- E$\wedge_1$/ E$\wedge_2$: a partir de una conjunción podemos deducir cualquiera de las dos fórmulas que la componen, porque ambas valen. Se modela con dos reglas.
- I$\vee_1$/ I$\vee_2$: para demostrar una disyunción, alcanza con demostrar una de sus dos fórmulas. Se modela con dos reglas al igual que la eliminación de conjunción.
- E$\vee$: nos permite deducir una conclusión a partir de una disyunción dando sub demostraciones que muestran que sin importar cual de las dos valga, asumiéndolas por separado, se puede demostrar.

2.2.3. Reglas de implicación y negación

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\, \mathrm{I}\to \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\, \mathrm{E}\to$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\, \mathrm{I}\neg \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\, \mathrm{E}\neg$$

- I$\to$: para demostrar una implicación, asumimos el antecedente (agregándolo a las hipótesis) y en base a eso se demuestra el consecuente.
- E$\to$: también conocida como *modus ponens*. A partir de una implicación, si podemos demostrar su antecedente, entonces vale su consecuente.
- I$\neg$: para demostrar una negación, lo hacemos por el absurdo: asumimos que vale la fórmula y llegamos a una contradicción.
- E$\neg$: podemos concluir un absurdo demostrando que vale una fórmula y su negación.

2.2.4. Reglas de cuantificadores

Las reglas de $\forall$ y $\exists$ se pueden ver como extensiones a las de $\wedge$ y $\vee$. Un $\forall$ se puede pensar como una conjunción con un elemento por cada uno del dominio sobre el cual se cuantifica, y análogamente un $\exists$ como una disyunción.

$$\frac{\Gamma \vdash A \qquad x \notin fv(\Gamma)}{\Gamma \vdash \forall x.A}\ \mathrm{I}\forall \qquad\qquad \frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A\{x := t\}}\ \mathrm{E}\forall$$

- I$\forall$: para demostrar un $\forall x.A$, quiero ver que sin importar el valor que tome x yo puedo demostrar A. Pero para eso en el contexto Γ no tengo que tenerlo ligado a nada, sino no lo estaría demostrando en general.
- E$\forall$: para usar un $\forall x.A$ para demostrar, como vale para todo x, puedo instanciarlo en *cualquier término* t.

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

$$\frac{\Gamma \vdash \exists x.A \qquad \Gamma, A \vdash B \qquad x \notin fv(\Gamma, B)}{\Gamma \vdash B}\ \mathrm{E}\exists$$

- I$\exists$: para demostrar un $\exists$, alcanza con instanciar x en un término t para el que sea cierto.
- E$\exists$: para usar un $\exists$ para demostrar, es parecido a E$\vee$. Como tenemos que ver que vale para cualquier x, podemos concluir B tomando como hipótesis A con x sin instanciar.

Ejemplo 3. Para ejemplificar el uso de las reglas de cuantificadores, extendemos el Ejemplo 2 para usar cuantificadores. Usamos

- Usamos las siguientes funciones 0-arias: a representa un alumno, m una materia y e un examen.
- $X(a, e) \equiv \text{reprueba}(a, e)$
- $R(a, m) \equiv \text{recursa}(a, m)$
- $F(a, e) \equiv \text{falta}(a, e)$

Vamos a tomar los siguientes como *axiomas*, que van a formar parte del contexto inicial de la demostración. Es lo mismo que haremos en PPA al modelar teorías de primer orden.

- **Axioma 1**: si un alumno reprueba el final de una materia, entonces recursa

$$\forall a.\ \forall m.\ (X(a, \text{final}(m)) \to R(a, m))$$

- **Axioma 2**: si un alumno falta a un examen, lo reprueba

$$\forall a.\ \forall e.\ (F(a, e) \to X(a, e))$$

Definimos

$$\Gamma_0 = \{\forall a.\ \forall m.\ X(a, \text{final}(m)) \to R(a, m), \forall a.\ \forall e.\ F(a, e) \to X(a, e)\}$$

Luego, queremos probar $\Gamma_0 \vdash \forall a.\ \forall m.\ F(a, \text{final}(m)) \to R(a, m)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_1 \vdash \forall a \forall m.\ X(a, \text{final}(m)) \to R(a,m)}\,\text{Ax}}{\Gamma_1 \vdash \forall m.\ X(a, \text{final}(m)) \to R(a,m)}\,\text{E}\forall}{\Gamma_1 \vdash X(a, \text{final}(m)) \to R(a,m)}\,\text{E}\forall \qquad \Pi}{\dfrac{\dfrac{\dfrac{\Gamma_1 = \Gamma_0, F(a, \text{final}(m)) \vdash R(a,m)}{\Gamma_0 \vdash F(a, \text{final}(m)) \to R(a,m)}\,\text{I}\to}{\Gamma_0 \vdash \forall m.\ F(a, \text{final}(m)) \to R(a,m)}\,\text{I}\forall}{\Gamma_0 \vdash \forall a.\ \forall m.\ F(a, \text{final}(m)) \to R(a,m)}\,\text{I}\forall}\,\text{E}\to$$

Con

$$\Pi = \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_1 \vdash \forall a.\ \forall e.\ F(a,e) \to X(a,e)}\,\text{Ax}}{\Gamma_1 \vdash \forall e.\ F(a,e) \to X(a,e)}\,\text{E}\forall}{\Gamma_1 \vdash F(a, \text{final}(m)) \to X(a, \text{final}(m))}\,\text{E}\forall \qquad \dfrac{}{\Gamma_1 \vdash F(a, \text{final}(m))}\,\text{Ax}}{\Gamma_1 \vdash X(a, \text{final}(m))}\,\text{E}\to$$

Fig. 2.3: Demostración con cuantificadores en deducción natural

2.3. Ajustes para generación de demostraciones

PPA genera demostraciones en deducción natural, pero no usa exactamente el sistema descrito en la Figura 2.1, sino que tiene algunos ajustes.

2.3.1. Hipótesis etiquetadas

Sección re-redactada!

En las secciones anteriores presentamos a los contextos Γ como *conjuntos* de fórmulas. Pero en realidad vamos a querer que las hipótesis estén nombradas para proveer mayor claridad en las demostraciones. Para permitirlo, cada regla que introduce una hipótesis tiene que darle nombre, y cada regla que la usa, tiene que explicitar qué nombre tiene.

- Los contextos Γ se redefinen como conjuntos de *pares* $h : A$ de etiquetas y fórmulas.
- Las reglas que hacen uso de hipótesis, lo hacen nombrándolas.

$$\dfrac{\boldsymbol{h} : A \in \Gamma}{\Gamma \vdash A}\,\text{Ax}_{\boldsymbol{h}} \qquad \dfrac{\Gamma, \boldsymbol{h} : A \vdash B}{\Gamma \vdash A \to B}\,\text{I}\to_{\boldsymbol{h}} \qquad \dfrac{\Gamma, \boldsymbol{h} : A \vdash \bot}{\Gamma \vdash \neg A}\,\text{I}\neg_{\boldsymbol{h}}$$

$$\dfrac{\Gamma \vdash \exists x.A \qquad \Gamma, \boldsymbol{h} : A \vdash B \qquad x \notin fv(\Gamma, B)}{\Gamma \vdash B}\,\text{E}\exists_{\boldsymbol{h}}$$

Obs. 1. Las reglas están decoradas con el nombre de la hipótesis porque esto hace que según cual se use, el uso de la regla y por lo tanto la demostración sea diferente. Por lo que si por ejemplo demostramos $A \to A \to A$, con etiquetas hay dos demostraciones distintas (dependiendo de si se usa la primera o segunda asunción) y sin habría una sola (como el contexto es un conjunto, se combinan ambas hipótesis en una).

2.3.2. Variables libres en contexto

Re-redactado!

Las reglas I$\forall$ y E$\exists$ validan que la variable del cuantificador no esté libre en el contexto. Cuando sí aparece, el algoritmo de chequeo debe reportar un error. El usuario debería re-escribir la demostración para corregir el uso de variables evitando conflictos.

Pero esto representó un problema para la generación de demostraciones, pues se daban conflictos en casos inofensivos: si tenemos una demostración de un teorema que usa las variables x, y, y lo citamos en otro que también las usa, el conflicto sería accidental, no estamos queriendo razonar de forma inválida. Al chequear la demostración citada, ya se usaron las variables en el anterior, llevando a un error. Para evitarlo manteniendo las reglas como están, habría que renombrar con cuidado las variables de forma automática.

La reformulamos para evitarlo de una forma más simple: en lugar de validar que la variable no esté no esté, directamente se remueve del contexto todas las hipótesis que contengan libre esa variable en la sub-demostración. Cada sub-demostración tiene un contexto "limpio". Esto permite que si el conflicto era accidental, la demostración siga chequeando (porque no se usaban las hipótesis que generaban conflicto). Pero si se usaban, seguiría fallando pero con un error diferente (hipótesis inexistente).

Definimos

$$\Gamma \ominus x = \{A \in \Gamma \mid x \notin fv(A)\}$$

Luego, las reglas son re-definidas como

$$\frac{\boldsymbol{\Gamma \ominus x} \vdash A}{\Gamma \vdash \forall x.A}\ \mathrm{I}\forall$$

$$\frac{\boldsymbol{\Gamma \ominus x} \vdash \exists x.A \qquad \boldsymbol{\Gamma \ominus x}, h : A \vdash B \qquad x \notin fv(B)}{\Gamma \vdash B}\ \mathrm{E}\exists_h$$

(NOTA: Lo re-redacté para dar un argumento un poco más robusto, si hace falta demostrar la inter-derivabilidad me decís y lo charlamos.)

2.4. Reglas admisibles

Antes mencionamos *modus tollens* como regla de inferencia, pero no aparece en la Figura 2.1. Esto es porque nos va a interesar tener un sistema lógico minimal: no vamos a agregar reglas de inferencia que se puedan deducir a partir de otras, es decir, *reglas admisibles*. Nos va a servir para simplificar el resto de PPA, dado que vamos a generar demostraciones en deducción natural y operar sobre ellas. Mientras más sencillas sean las partes con las que se componen, mejor. Las reglas admisibles las podemos demostrar para cualquier fórmula, así luego podemos usarlas como *macros*.

Ejemplo 4 (*Modus tollens*)**.** Se puede demostrar como regla admisible.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash (A \to B) \wedge \neg B}\,\mathrm{Ax}}{\Gamma \vdash \neg B}\,\mathrm{E}\wedge_2 \qquad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash (A \to B) \wedge \neg B}\,\mathrm{Ax}}{\Gamma \vdash A \to B}\,\mathrm{E}\wedge_1 \qquad \dfrac{}{\Gamma \vdash A}\,\mathrm{Ax}}{\Gamma \vdash B}\,\mathrm{E}\to}{\Gamma = (A \to B) \wedge \neg B, A \vdash \bot}\,\mathrm{E}\neg}{(A \to B) \wedge \neg B \vdash \neg A}\,\mathrm{I}\neg}{\vdash (A \to B \wedge \neg B) \to \neg A}\,\mathrm{I}\to$$

2.5. Algoritmos

A continuación describimos los algoritmos que son necesarios para la implementación de deducción natural. El chequeo de las demostraciones, alfa equivalencia de fórmulas, sustitución sin capturas, y variables libres

2.5.1. Chequeador

Sección reescrita!

El algoritmo de chequeo de una demostración en deducción natural consiste en recorrer recursivamente el árbol de demostración, asegurando que todas las inferencias sean válidas y manteniendo un contexto Γ en el camino. Se chequea que cada regla se use con el conectivo que le corresponde (no un I$\wedge$ para un $\vee$) y que cumple con las condiciones impuestas.

El módulo que se encarga de implementarlo es el `Checker`, su función principal es

```
check :: Env -> Proof -> Form
```

donde **`Env`** es el contexto Γ, **`Proof`** es el término de demostración en deducción natural y **`Form`** es la fórmula que demuestra.

2.5.2. Alfa equivalencia

Si tenemos una hipótesis $\exists x.f(x)$, sería ideal poder usarla para demostrar a partir de ella una fórmula $\exists y.f(y)$. Si bien no son exactamente iguales, son **alfa-equivalentes**: su estructura es la misma, pero tienen nombres diferentes para variables *ligadas* (no libres)

Def. 7 (Alfa equivalencia)**.** Se define la relación $\overset{\alpha}{=}$ como la que permite renombrar variables ligadas evitando capturas. Es la congruencia más chica que cumple con

$$(\forall x.A) \overset{\alpha}{=} (\forall y.A') \iff A\{x := z\} \overset{\alpha}{=} A'\{y := z\} \text{ con } z \text{ fresca}$$
$$(\exists x.A) \overset{\alpha}{=} (\exists y.A') \iff A\{x := z\} \overset{\alpha}{=} A'\{y := z\} \text{ con } z \text{ fresca}$$

Para implementarlo, un algoritmo naíf podría ser cuadrático: chequeamos recursivamente la igualdad estructural de ambas fórmulas. Si nos encontramos con un cuantificador con variables con nombres distintos, digamos x e y, elegimos una nueva variable *fresca* (para evitar capturas) y lo renombramos recursivamente en ambos. Luego continuamos con el algoritmo. Si en la base nos encontramos con dos variables, tienen que ser iguales.

Para hacerlo un poco más eficiente, se implementó un algoritmo lineal en la estructura de la fórmula. Mantenemos dos sustituciones de variables, una para cada fórmula. Si nos encontramos con $\exists x.f(x)$ y $\exists y.f(y)$, vamos a elegir una variable fresca igual que antes (por ejemplo z), pero en vez de renombrar recursivamente, que lo hace cuadrático, insertamos en cada sustitución los renombres $x \mapsto z$ y $y \mapsto z$. Luego, cuando estemos comparando dos variables libres, chequeamos que *sus renombres* sean iguales. En este ejemplo son alfa equivalentes, pues

$$\begin{aligned}
(\exists x.f(x)) \overset{\alpha}{=} (\exists y.f(y)) &\iff f(x) \overset{\alpha}{=} f(y) && \{x \mapsto z\}, \{y \mapsto z\} \\
&\iff x \overset{\alpha}{=} y && \{x \mapsto z\}, \{y \mapsto z\} \\
&\iff z = z. &&
\end{aligned}$$

2.5.3. Sustitución sin capturas

Notamos la sustitución de todas las ocurrencias libres de la variable x por un término t en una fórmula A como $A\{x := t\}$. Esto se usa en algunas reglas de inferencia,

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

Pero queremos evitar **captura de variables**. Por ejemplo, en

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

si sustituimos sin más, estaríamos involuntariamente "capturando" a y. Si hiciéramos que falle, tener que escribir las demostraciones con estos cuidados puede ser muy frágil y propenso a errores, por lo que es deseable que se resuelva *automáticamente*: cuando nos encontramos con una captura, sustituimos la variable ligada de forma que no ocurra.

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

donde z es una variable *fresca*.

Def. 8 (Sustitución sin capturas)**.** Corregido! Se define por inducción estructural.

- Términos

$$x\{y := t\} = \begin{cases} t & \text{si } x = y \\ x & \text{si no} \end{cases}$$
$$f(t_1, \ldots, t_n)\{y := t\} = f(t_1\{y := t\}, \ldots, t_n\{y := t\})$$

- Fórmulas

$$\begin{aligned}
\bot\{y := t\} &= \bot \\
\top\{y := t\} &= \top \\
p(t_1, \ldots, t_n)\{y := t\} &= p(t_1\{y := t\}, \ldots, t_n\{y := t\}) \\
(A \wedge B)\{y := t\} &= A\{y := t\} \wedge B\{y := t\} \\
(A \vee B)\{y := t\} &= A\{y := t\} \vee B\{y := t\} \\
(A \to B)\{y := t\} &= A\{y := t\} \to B\{y := t\} \\
(\neg A)\{y := t\} &= \neg A\{y := t\} \\
(\forall x.A)\{y := t\} &= \begin{cases} \forall x.A & \text{si } x = y \\ \forall z.(A\{x := z\})\{y := t\} & \text{si } x \in fv(t), \text{ con } z \text{ fresca} \\ \forall x.A\{y := t\} & \text{si no} \end{cases} \\
(\exists x.A)\{y := t\} &= \begin{cases} \exists x.A & \text{si } x = y \\ \exists z.(A\{x := z\})\{y := t\} & \text{si } x \in fv(t), \text{ con } z \text{ fresca} \\ \exists x.A\{y := t\} & \text{si no} \end{cases}
\end{aligned}$$

Para implementarlo, cada vez que nos encontramos con una captura, vamos a *renombrar* la variable del cuantificador por una nueva, fresca. Al igual que la alfa igualdad, esto se puede implementar de forma naíf cuadrática pero lo hicimos lineal. Mantenemos un único mapeo a lo largo de la sustitución, y cada vez que nos encontramos con una variable libre, si son iguales la sustituimos por el término, y si está mapeada la renombramos.

Def. 9 (Variables libres de una demostración)**.** Sea Π una demostración. $fv(\Pi)$ son las variables libres de todas las fórmulas que la componen. Por ejemplo, para la siguiente

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\, \mathrm{I}\wedge$$

se tiene $fv(\Pi) = fv(A) \cup fv(B)$

3. EL LENGUAJE PPA

El lenguaje PPA (*Pani's Proof Assistant*) se construye sobre las fundaciones de deducción natural. Es un asistente de demostración que permite escribir de una forma práctica demostraciones de cualquier teoría de lógica clásica de primer orden. En este capítulo nos vamos a centrar en el lenguaje, la interfaz del programa `ppa`, vista desde el punto de vista de un usuario que busca escribir demostraciones. Los detalles teóricos de cómo está implementado son abordados en el Capítulo 4, y los de implementación y su instalación en el Capítulo 6. Para introducirlo veamos un ejemplo: en la Figura 3.1 representamos el mismo de alumnos del Ejemplo 3 pero con un poco más de sofisticación.

Diseccionemos parte por parte. La primera de todo programa en PPA es definir los axiomas de la *teoría de primer orden* con la que se está trabajando. Como no se chequean tipos, no es necesario definir explícitamente los símbolos de predicados y de función. Pero se pueden agregar a modo informativo como un comentario. Consisten en fórmulas que son siempre consideradas como válidas. Definimos,

- **axiom** `reprueba_recu_parcial_recursa`: si un alumno reprueba el parcial y el recuperatorio de una materia, la recursa.
- **axiom** `reprobo_rinde`: si un alumno reprobó un examen, es porque lo rindió.
- **axiom** `rinde_recu_reprobo_parcial`: si un alumno rinde el recu de un parcial, es porque reprobó la primer instancia.
- **axiom** `falta_reprueba`: si un alumno falta a un exámen, lo reprueba.

```
/* Teoría de alumnos y exámenes

Predicados
   - reprueba(A, P): El alumno A reprueba el parcial P
   - recursa(A, M): El alumno A recursa la materia M

Funciones
   - parcial(M): El parcial de una materia
   - recu(P): El recuperatorio de un parcial
*/

axiom reprueba_recu_parcial_recursa: forall A. forall M.
   (reprueba(A, parcial(M)) & reprueba(A, recu(parcial(M))))
      -> recursa(A, M)

axiom rinde_recu_reprobo_parcial: forall A. forall P.
   rinde(A, recu(P)) -> reprueba(A, P)

axiom reprobo_rinde: forall A. forall P.
   reprueba(A, P) -> rinde(A, P)

axiom falta_reprueba: forall A. forall P.
   falta(A, P) -> reprueba(A, P)
```

En base a eso demostramos dos teoremas. El primero, **theorem** `reprueba_recu_recursa`, nos permite concluir que un alumno recursa solo a partir de que reprueba el recuperatorio. Esto es porque a partir de esto, con el resto de los axiomas, podemos deducir que también reprobó el parcial: si reprueba el recuperatorio es porque lo rindió, y si rindió el recuperatorio, es porque reprobó el parcial.

```
axiom reprueba_recu_parcial_recursa: forall A. forall M.
   (reprueba(A, parcial(M)) & reprueba(A, recu(parcial(M))))
      -> recursa(A, M)

axiom rinde_recu_reprobo_parcial: forall A. forall P.
   rinde(A, recu(P)) -> reprueba(A, P)

axiom reprobo_rinde: forall A. forall P.
   reprueba(A, P) -> rinde(A, P)

axiom falta_reprueba: forall A. forall P.
   falta(A, P) -> reprueba(A, P)

theorem reprueba_recu_recursa:
   forall A. forall M.
      reprueba(A, recu(parcial(M))) -> recursa(A, M)
proof
   let A
   let M
   suppose reprueba_recu: reprueba(A, recu(parcial(M)))

   claim reprueba_p: reprueba(A, parcial(M))
   proof
      have rinde_recu: rinde(A, recu(parcial(M)))
         by reprueba_recu, reprobo_rinde

      hence reprueba(A, parcial(M))
         by rinde_recu_reprobo_parcial
   end

   hence recursa(A, M)
      by reprueba_recu,
         reprueba_p,
         reprueba_recu_parcial_recursa
end

theorem falta_recu_recursa:
   forall A. forall M.
      falta(A, recu(parcial(M))) -> recursa(A, M)
proof
   let A
   let M

   suppose falta_recu: falta(A, recu(parcial(M)))

   have reprueba_recu: reprueba(A, recu(parcial(M)))
      by falta_recu, falta_reprueba

   hence recursa(A, M) by reprueba_recu_recursa
end
```

Fig. 3.1: Programa de ejemplo completo en PPA. Demostraciones de alumnos y parciales.

```
24 theorem reprueba_recu_recursa:
25    forall A. forall M.
26       reprueba(A, recu(parcial(M))) -> recursa(A, M)
27 proof
28    let A
29    let M
30    suppose reprueba_recu: reprueba(A, recu(parcial(M)))
31
32    claim reprueba_p: reprueba(A, parcial(M))
33    proof
34       have rinde_recu: rinde(A, recu(parcial(M)))
35          by reprueba_recu, reprobo_rinde
36
37       hence reprueba(A, parcial(M))
38          by rinde_recu_reprobo_parcial
39    end
40
41    hence recursa(A, M)
42       by reprueba_recu,
43          reprueba_p,
44          reprueba_recu_parcial_recursa
45 end
```

Para demostrar un teorema, tenemos que agotar su *tesis* reduciéndola sucesivamente con *proof steps*. Una demostración es correcta si todos los pasos son lógicamente correctos, y luego de ejecutarlos todos, la tesis se reduce por completo.

- **`let`** permite demostrar un **`forall`**, asignando un nombre a la variable general, y *reduce* la tesis a su fórmula.
- **`suppose`** permite demostrar una implicación. Agrega como hipótesis al contexto el antecedente, permitiendo nombrarlo, y reduce la tesis al consecuente.
- **`claim`** permite agregar una sub-demostración, cuya fórmula se agrega como hipótesis.
- **`have`** agrega una hipótesis auxiliar, sin reducir la tesis.
- **`by`** es el mecanismo principal de demostración. Permite deducir fórmulas a partir de otras. Es completo para lógica proposicional, y heurístico para primer orden. Unifica las variables de los **`forall`**.
- **`thus`** permite reducir parte o la totalidad de la tesis.
- **`hence`** es igual a thus, pero incluye implícitamente la hipótesis anterior a las justificaciones del **`by`**.

Finalmente, a partir del teorema anterior y **`axiom`** `falta_reprueba` podemos demostrar que si un alumno falta a un recuperatorio, recursa la materia.

```
46 theorem falta_recu_recursa:
47    forall A. forall M.
48       falta(A, recu(parcial(M))) -> recursa(A, M)
49 proof
50    let A
51    let M
52
53    suppose falta_recu: falta(A, recu(parcial(M)))
54
55    have reprueba_recu: reprueba(A, recu(parcial(M)))
56       by falta_recu, falta_reprueba
57
58    hence recursa(A, M) by reprueba_recu_recursa
59 end
```

Al ejecutarlo con `ppa`, se *certifica* la demostración, generando un certificado de deducción natural, y luego se chequea que sea correcto. Si se escribió una demostración que no es lógicamente válida, el certificador reporta el error. No debería fallar nunca el chequeo sobre el certificado.

3.1. Interfaz

PPA es un lenguaje que permite escribir demostraciones de cualquier teoría de lógica de primer orden. Está inspirado en el *mathematical vernacular* introducido por Freek Wiedijk [Wie]. En esta sección nos concentramos en la interfaz de usuario, sin entrar en detalle en cómo está implementada.

Un programa de PPA consiste en una lista de **declaraciones**: axiomas y teoremas, que se leen en orden el inicio hasta el final.

- Los axiomas se asumen válidos, se usan para modelar la *teoría de primer orden* sobre la cual hacer demostraciones

  ```
  axiom <name> : <form>
  ```

- Los teoremas deben ser demostrados, y se pueden citar todas las hipótesis previas, que consideran ciertas.

  ```
  theorem <name> : <form>
  proof
     <steps>
  end
  ```

3.1.1. Identificadores

Los identificadores se dividen en tres tipos:

- **Variables** (`<var>`). Son descritas por la siguiente expresión regular

  ```
  (\_|[A-Z])[a-zA-Z0-9\_\-]*(\')*
  ```

- **Identificadores** (`<id>`). Son descritos por la siguiente expresión regular

```
[a-zA-Z0-9\_\-\?!#\$\%\*\+\<\>\=\?\@\^]+(\')*
```

- **Nombres** (`<name>`): pueden ser identificadores, o *strings* arbitrarios encerrados por comillas dobles (`"..."`), que son descritos por la siguiente expresión regular

```
\"[^\"]*\"
```

3.1.2. Comentarios

Se pueden escribir comentarios de una sola línea (`//...`) o multilínea (`/* ... */`)

3.1.3. Fórmulas

Las fórmulas están compuestas por,

- **Términos**
  - **Variables**: `<var>`. Ejemplos: `_x`, `X`, `X'''`, `Alumno`.
  - **Funciones**: `<id>(<term>, ..., <term>)`. Los argumentos son opcionales, pudiendo tener funciones 0-arias (constantes). Ejemplos: `c`, `f(_x, c, X)`.
- **Predicados**: `<id>(<term>, ..., <term>)`. Los argumentos son opcionales, pudiendo tener predicados 0-arios (variables proposicionales). Ejemplos: `p(c, f(w), X)`, `A`, `<(n, m)`
- **Conectivos binarios**.
  - `<form> & <form>` (conjunción)
  - `<form> | <form>` (disyunción)
  - `<form> -> <form>` (implicación)
- **Negación** `~<form>`
- **Cuantificadores**
  - **`exists`** `<var> . <form>`
  - **`forall`** `<var> . <form>`
- **`true`**, **`false`**
- **Paréntesis**: `(<form>)`

3.2. Demostraciones

Las demostraciones consisten en una lista de *proof steps* o comandos que pueden reducir sucesivamente la *tesis* (fórmula a demostrar) hasta agotarla por completo. Corresponden aproximadamente a reglas de inferencia de deducción natural.

3.2.1. Contexto

Las demostraciones llevan asociado un *contexto* con todas las hipótesis que fueron asumidas (como los axiomas), o demostradas: tanto teoremas anteriores como sub-teoremas y otros comandos que agregan hipótesis a él.

3.2.2. by - el mecanismo principal de demostración

El mecanismo principal de demostración directa o *modus ponens* es el **by**, que afirma que un hecho es consecuencia de una lista de hipótesis (su "justificación"). Esto permite eliminar universales e implicaciones. Por detrás hay un solver completo para lógica proposicional pero heurístico para primer orden (elimina todos los foralls de a lo sumo una hipótesis, no intenta con más de una). Exploramos las limitaciones en Subsección 4.3.5 Poder expresivo.

En general, `[...] by <justification>` se interpreta como que `[...]` es una consecuencia lógica de las fórmulas que corresponden a las hipótesis de `<justification>`, que deben estar declaradas anteriormente y ser parte del contexto. Ya sea por axiomas o teoremas, u otros comandos que agreguen hipótesis (como **suppose**). Puede usarse de dos formas principales, **thus** y **have**

- **thus** `<form>` **by** `<justification>`.

  Si `<form>` es *parte* de la tesis (ver Subsección 3.2.4 Descarga de conjunciones), y es consecuencia lógica de las justificaciones, lo demuestra automáticamente y lo descarga de la tesis.

  Por ejemplo, para eliminación de implicaciones

```
1  axiom ax1: a -> b
2  axiom ax2: b -> c
3
4  theorem t1: a -> c
5  proof
6     suppose a: a
7
8     // La tesis ahora es c
9     thus c by a, ax1, ax2
10 end
```

  Y para eliminación de cuantificadores universales

```
1  axiom ax: forall X . f(X)
2
3  theorem t: f(n)
4  proof
5     thus f(n) by ax
6  end
```

- **have** `<form>` **by** `<justification>`.

  Igual a **thus**, pero permite introducir afirmaciones *auxiliares* que no son parte de la tesis, sin reducirla, y las agrega a las hipótesis para usar luego. Por ejemplo, la demostración anterior la hicimos en un solo paso con el **thus**, pero podríamos haberla hecho en más de uno con una afirmación auxiliar intermedia.

```
axiom ax1: a -> b
axiom ax2: b -> c

theorem t1: a -> c
proof
   suppose a: a
   have b: b by a, ax1
   thus c by b, ax2
end
```

Ambas tienen su contraparte con *azúcar sintáctico* que agrega automáticamente la hipótesis anterior a la justificación, a la que también se puede referir con guión medio (`-`).

Comando	Alternativo	¿Reduce la tesis?
thus	**hence**	Si
have	**then**	No

Por ejemplo,

```
axiom ax1: a -> b
axiom ax2: b -> c

theorem t1: a -> c
proof
   suppose a: a
   have b: b by a, ax1
   thus c by b, ax2
end
```

```
theorem t1': a -> c
proof
   suppose a: a
   have b: b by -, ax1
   thus c by -, ax2
end

theorem t1'': a -> c
proof
   suppose -: a
   then -: b by ax1
   hence c by ax2
end
```

En todos, el **by** es opcional. En caso de no especificarlo, debe ser una tautología.

```
theorem "distributiva de negación sobre disyunción":
   ~(a | b) <-> ~a & ~b
proof
   thus ~(a | b) <-> ~a & ~b
end
```

3.2.3. Comandos y reglas de inferencia

Muchas reglas de inferencia de deducción natural (2.1) tienen una correspondencia directa con comandos. Como se puede ver en Tabla 3.1 Reglas de inferencia y comandos, la mayor parte del trabajo manual, detallista y de bajo nivel de escribir demostraciones en deducción natural resuelve automáticamente con el uso **by**.

Regla	Comando
I∃	**take**
E∃	**consider**
I∀	**let**
E∀	**by**
I∨$_1$	**by**
I∨$_2$	**by**
E∨	**cases**
I∧	**by**
E∧$_1$	**by**
E∧$_2$	**by**
I→	**suppose**
E→	**by**
I¬	**suppose**
E¬	**by**
I⊤	**by**
E⊥	**by**
LEM	**by**
Ax	**by**

Tab. 3.1: Reglas de inferencia y comandos

- **suppose** (I→/ I¬)

  Si la tesis es una implicación $A \to B$, agrega el antecedente A como hipótesis con el nombre dado y reduce la tesis al consecuente B. Viendo la negación como una implicación $\neg A \equiv A \to \bot$, se puede usar para introducir negaciones, tomando $B = \bot$.

```
theorem "suppose":
   a -> (a -> b) -> b
proof
   suppose h1: a
   suppose h2: a -> b
   thus b by h1, h2
end
```

```
theorem "not intro":
   ~b & (a -> b) -> ~a
proof
   suppose h: ~b & (a -> b)
   suppose a: a
   hence false by h, a
end
```

- **cases** (E∨)

  Permite razonar por casos. Para cada uno se debe demostrar la tesis en su totalidad por separado.

```
theorem "cases":
   (a & b) | (c & a) -> a
proof
   suppose h: (a & b) | (c & a)
   cases by h
      case a & b
         hence a
      case right: a & c
         thus a by right
```

```
10    end
11 end
```

No es necesario que los casos sean exactamente iguales a como están presentados en la hipótesis, solo debe valer que la disyunción de ellos sea consecuencia de ella. Es decir, para poder usar

```
cases by h1, ..., hn
   case c1
   ...
   case cm
end
```

Tiene que valer `c1 | ... | cm by h1, ..., hn`.

Por lo que en el ejemplo anterior, podríamos haber usado el mismo case incluso si la hipótesis fuera `~((~a | ~b) & (~c | ~a))`, pues es equivalente a `(a & b) | (c & a)`.

- **take** (I∃)

  Introduce un existencial instanciando su variable y reemplazándola por un término. Si la tesis es `exists X . p(X)`, luego de `take X := a`, se reduce a `p(a)`.

- **consider** (E∃)

  Permite razonar sobre una variable que cumpla con un existencial. Si se puede justificar `exists X. p(X)`, permite razonar sobre `X`.

  El comando `consider X st h: p by ...` agrega `p` como hipótesis al contexto para el resto de la demostración. El `by` debe justificar `exists X. p(X)`.

  Valida que `X` no esté libre en la tesis.

  También es posible usar una fórmula α-equivalente, por ejemplo si podemos justificar `exists X. p(X)`, podemos usarlo para `consider Y st h: p(Y) by ...`

- **let** (I∀)

  Permite demostrar un cuantificador universal. Si se tiene `forall X. p(X)`, luego de `let X` la tesis se reduce a `p(X)` con un `X` genérico. Puede ser el mismo nombre de variable o uno diferente.

3.2.4. Descarga de conjunciones

Si la tesis es una conjunción, se puede probar solo una parte de ella y se reduce al resto.

Fig. 3.2: Descarga de conjunción simple

```
1  theorem "and discharge" : a -> b -> (a & b)
2  proof
3     suppose "a" : a
4     suppose "b" : b
5     // La tesis es a & b
6     hence b by "b"
7
8     // La tesis es a
9     thus a by "a"
10 end
```

Esto puede ser prácticamente en cualquier orden.

Fig. 3.3: Descarga de conjunción compleja

```
axiom "a": a
axiom "b": b
axiom "c": c
axiom "d": d
axiom "e": e
theorem "and discharge" : (a & b) & ((c & d) & e)
proof
   thus a & e by "a", "e"
   thus d by "d"
   thus b & c by "b", "c"
end
```

3.2.5. Otros comandos

- **equivalently**: permite reducir la tesis a una fórmula equivalente. Útil para usar descarga de conjunciones.

```
axiom a1: ~a
axiom a2: ~b

theorem "ejemplo" : ~(a | b)
proof
   equivalently ~a & ~b
   thus ~a by a1
   thus ~b by a2
end
```

- **claim**: permite demostrar una afirmación auxiliar. Útil para ordenar las demostraciones sin tener que definir otro teorema. Ejemplo en Figura 3.1 Programa de ejemplo completo en PPA. Demostraciones de alumnos y parciales

```
theorem t: <form>
proof
   claim <name>: <form>
   proof
      <proof>
   end
end
```

4. EL CERTIFICADOR DE PPA

En la sección anterior vimos cómo usar PPA para demostrar teoremas. Pero, ¿cómo funciona por detrás? ¿Como asegura la validez lógica de las demostraciones escritas por el usuario?

4.1. Certificados

Los programas de PPA se **certifican**, generando una demostración en deducción natural. ¿Por qué? El lenguaje es complejo, la implementación no es trivial. Si se programa una demostración, para confiar en que es correcta hay que confiar en la implementación de PPA. Si generara una demostración de bajo nivel, que use las reglas de un sistema lógico simple y conocido, entonces cualquiera que desconfíe podría fácilmente escribir un chequeador, o usar uno confiable. Al generar demostraciones en deducción natural, cumple con esto, que se llama **criterio de de Bruijn**.

Def. 10 (Criterio de de Bruijn [BW05])**.** Un asistente de demostración que satisface que sus demostraciones puedan ser chequeadas por un programa independiente, pequeño y confiable se dice que cumple con el criterio de de Bruijn.

El módulo de PPA que *certifica* las demostraciones de alto nivel de PPA generando una demostración en deducción natural es el `Certifier`. Si bien toda demostración que genere debería ser correcta, para atajar posibles errores siempre se chequean con el `Checker` de DN.

(DUDA: Para pablo: pero si emite certificados que no corresponden a la demo original y chequean siempre, por ej. siempre el mismo, no estaría mal igual? Tenés que confiar también en la parte que emite el certificado.)

4.2. Certificador

El `Certifier` en realidad no genera una sola demostración de deducción natural, sino que al poder haber más de un teorema en un archivo PPA, el certificado en realidad es un **contexto** compuesto por una lista ordenada de **hipótesis** de dos tipos:

- **Teoremas**: son fórmulas con demostraciones de deducción natural asociadas.
- **Axiomas**: son fórmulas que se asumen válidas (pueden ser usadas para modelar una teoría)

```
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
```

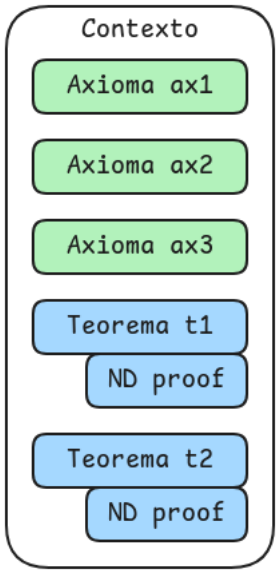

Fig. 4.1: Contexto resultante de certificar de un programa

Por lo tanto, en vez de chequear demostraciones, se chequean contextos: Una demostración será válida en el *prefijo estricto del contexto* que la contiene. Es decir, a la hora de chequear la demostración de un teorema, se deben asumir como ciertas todas las hipótesis que fueron definidas antes que él.

Pero no solo los axiomas y teoremas declarados en el programa se agregan al contexto. Cada demostración de un teorema tendrá además un *contexto local* que extiende al anterior, solo al alcance de su demostración (y se omiten en el certificado). Las afirmaciones auxiliares que no afectan la tesis (**`have`**, **`claim`**, **`consider`**, etc.) se agregan como teoremas. Por lo tanto, cuando se citen, se pegan sus demostraciones. Por otro lado, algunos comandos agregan axiomas, los mismos que en deducción natural agregan fórmulas al contexto (**`suppose`** y **`consider`**). Es correcto asumir como ciertas esas hipótesis, porque lo mismo se hará durante el chequeo de la demostración generada de deducción natural.

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

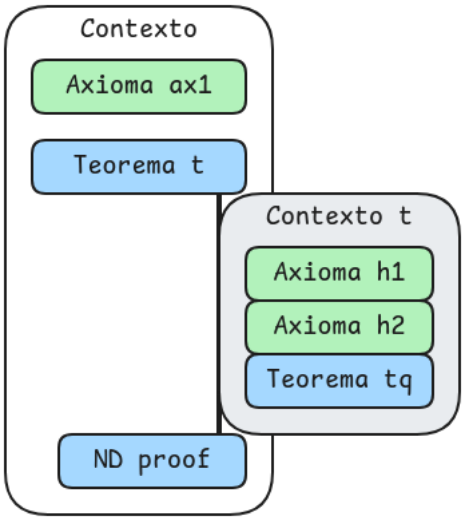

Fig. 4.2: Contexto local

4.3. Funcionamiento del by

El **by** es el mecanismo principal de demostración en PPA, y el corazón del `Certifier`. Muchas funcionalidades están implementadas a su alrededor. Genera **automáticamente** una demostración de que una fórmula es consecuencia lógica de una lista de hipótesis. Es un *solver heurístico* para lógica de primer orden.

Sea A una fórmula. Supongamos que queremos demostrar **thus** `A` **by** `h1, ..., hn` y que en el contexto tenemos que las hipótesis h_i corresponden a fórmulas B_i, con $i \in \{1, ..., n\}, n \in \mathbb{N}$. Primero veamos la idea general de la estrategia y luego profundizamos en cada paso. Los pasos para certificar un **by** son los siguientes.

- Queremos demostrar la implicación de las hipótesis a la fórmula.

  $$B_1 \wedge \ldots \wedge B_n \to A$$

  A esta fórmula la llamamos **tesis**.

- Razonamos por el absurdo: asumiendo la negación de la tesis encontramos una contradicción

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

- Convertimos la negación de la tesis a forma normal disyuntiva (DNF), una disyunción de conjunciones de literales ("cláusulas").

  $$(a_1^1 \wedge \ldots \wedge a_{n_1}^1) \vee \ldots \vee (a_1^m \wedge \ldots \wedge a_{n_m}^m)$$

  donde $m \in \mathbb{N}$ es el número de cláusulas, $n_1, \ldots, n_m \in \mathbb{N}$ es la cantidad de fórmulas de cada cláusula y a_j^i es la j-ésima fórmula de la i-ésima cláusula.

  (DUDA: Me parece que me compliqué de más con esta notación. Estaría OK dejarlo como $(a_1 \wedge \ldots \wedge a_n) \vee \ldots \vee (b_1 \wedge \ldots \wedge b_m)$?)

- Buscamos una contradicción refutando cada cláusula individualmente. Una cláusula $a_1 \wedge \ldots \wedge a_n$ será refutable si cumple una de las siguientes condiciones.
  - Contiene $\bot$
  - Contiene dos fórmulas opuestas $(a, \neg a)$
  - Eliminando existenciales consecutivos y re-convirtiendo a DNF, se consigue una refutación $(\neg p(k), \forall x.\ p(x))$

La complejidad del mecanismo no reside solo en tener que realizar todos estos pasos, sino que el desafío principal fue **generar la demostración en deducción natural**. Veamos un ejemplo sin generar la demostración, y sin eliminar existenciales.

Ejemplo 5 (Ejemplo sin cuantificadores)**.** Tenemos el siguiente programa

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

Para certificar `thus b by ax1, ax2` hay que generar una demostración para la implicación $\big((a \to b) \wedge a\big) \to b$.

1. Negamos la fórmula
$$\neg[\big((a \to b) \wedge a\big) \to b]$$
2. La convertimos a DNF
$$\begin{aligned}
&\neg[\big((a \to b) \wedge a\big) \to b] && \\
&\equiv \neg[\neg\big((a \to b) \wedge a\big) \vee b] && (A \to B \equiv \neg A \vee B) \\
&\equiv \neg\neg\big((a \to b) \wedge a\big) \wedge \neg b && (\neg(A \vee B) \equiv \neg A \wedge \neg B) \\
&\equiv \big((a \to b) \wedge a\big) \wedge \neg b && (\neg\neg A \equiv A) \\
&\equiv (\neg a \vee b) \wedge a \wedge \neg b && (A \to B \equiv \neg A \vee B) \\
&\equiv (\neg a \vee b) \wedge a \wedge \neg b && ((A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)) \\
&\equiv (\neg a \wedge a \wedge \neg b) \vee (b \wedge a \wedge \neg b) &&
\end{aligned}$$
3. Buscamos una contradicción refutando cada cláusula
   - En $(\neg a \wedge a \wedge \neg b)$ tenemos $\neg a$ y a.
   - En $(b \wedge a \wedge \neg b)$ tenemos b y $\neg b$.

4.3.1. Razonamiento por el absurdo

Queremos asumir que no vale la fórmula original, es decir $\neg(B_1 \wedge \ldots \wedge B_n \to A)$, y llegar a una contradicción. Pero en la demostración que estamos generando de deducción natural, tenemos que demostrar $(B_1 \wedge \ldots \wedge B_n \to A)$. ¿Cómo se puede razonar por el absurdo?

De la misma forma que en la Sección 2.4 se introduce *modus tollens* como una regla admisible, para razonar por el absurdo vamos a usar la **eliminación de la doble negación**. Es un principio de razonamiento clásico que es equivalente a LEM.

Teorema 1 (Eliminación de la doble negación)**.** Sea A una fórmula cualquiera. Vale $\neg\neg A \vdash A$, y lo notamos como regla admisible

$$\dfrac{}{\neg\neg A \vdash A}\,\mathrm{E}\neg\neg$$

Demostración. En deducción natural,

$$\mathrm{LEM}\ \dfrac{\dfrac{}{\neg\neg A \vdash A \vee \neg A} \quad \dfrac{}{\neg\neg A, A \vdash A}\,\mathrm{Ax} \qquad \mathrm{Ax}\ \dfrac{\dfrac{}{\neg\neg A, \neg A \vdash \neg\neg A} \quad \dfrac{}{\neg\neg A, \neg A \vdash \neg A}\,\mathrm{Ax}}{\neg\neg A, \neg A \vdash A}\,\mathrm{E}\neg}{\neg\neg A \vdash A}\,\mathrm{E}\vee$$

□

¿Cómo lo usamos? Introducimos otra regla admisible: **cut**, que nos permite "pegar" demostraciones entre sí. Si estamos queriendo demostrar A, y queremos reducir el problema a B que sí podemos probar, esta regla nos permite hacerlo.

Teorema 2 (Cut)**.** La siguiente regla de inferencia es admisible

$$\dfrac{\Gamma, B \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A}\,\mathrm{cut}$$

Demostración. La regla cut se puede ver como un *macro* que por atrás genera la siguiente demostración

$$\dfrac{\dfrac{\Gamma, B \vdash A}{\Gamma \vdash B \to A}\,\mathrm{I}\to \qquad \Gamma \vdash B}{\Gamma \vdash A}\,\mathrm{E}\to$$

□

Ejemplo 6. Cut nos permite continuar la demostración por otra fórmula a partir de la cual podamos demostrar la original. Sean $\Pi_{B\to A}$ una demostración de $B \vdash A$ y Π_B una demostración de B (la continuación). Podemos usar cut de la siguiente manera.

$$\dfrac{\begin{array}{cc}\Pi_{B\to A} & \Pi_B \\ \Gamma, B \vdash A & \Gamma \vdash B\end{array}}{\Gamma \vdash A}\,\mathrm{cut}$$

Que es certificado como

$$\dfrac{\dfrac{\begin{array}{c}\Pi_{B\to A} \\ \Gamma, B \vdash A\end{array}}{\Gamma \vdash B \to A}\,\mathrm{I}\to \qquad \begin{array}{c}\Pi_B \\ \Gamma \vdash B\end{array}}{\Gamma \vdash A}\,\mathrm{E}\to$$

Lema 1 (Razonamiento por el absurdo)**.** Imaginemos que queremos demostrar A por el absurdo. Podemos juntar con cut con la eliminación de la doble negación, pasando a demostrar $\neg\neg A$, que para introducirla, debemos demostrar el juicio $\Gamma, \neg A \vdash \bot$. Es decir, asumiendo que no es cierta la fórmula, deducimos una contradicción. Justo lo que estábamos buscando para razonar por el absurdo.

$$\dfrac{\dfrac{}{\Gamma, \neg\neg A \vdash A}\,\mathrm{E}\neg\neg \qquad \dfrac{\vdots}{\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash \neg\neg A}\,\mathrm{I}\neg}}{\Gamma \vdash A}\,\mathrm{cut}$$

Obs. 2. A E$\neg\neg$ La formulamos como $\neg\neg A \vdash A$ y la usamos con **cut**, pero otra alternativa equivalente, levemente más tediosa para generar demostraciones, hubiera sido demostrarla como $\neg\neg A \to A$ y usarla con E$\to$ directamente.

4.3.2. DNF

Tenemos que generar una demostración de que la negación de la tesis genera una contradicción, pero lo queremos hacer a partir de la tesis en DNF. ¿Cómo la convertimos?

Def. 11 (DNF)**.** Una fórmula está en **forma normal disyuntiva** o DNF (*disjunctive normal form*) si es una disyunción de conjunciones de literales. Llamamos **cláusulas** a las conjunciones que la componen. Un literal será un predicado, una negación de un predicado o una fórmula cualquiera que comienza con un cuantificador. Ejemplos:

- $a \land b$ está en DNF
- $(a \land c) \lor (a \land b)$ también
- $(a \to b) \lor (a \land b)$ no lo está
- $\big(\forall x.(a \to b)\big) \lor (a \land b)$ si.

Teorema 3 (Conversión a DNF)**.** Para toda fórmula A, existe A_{DNF} su equivalente en DNF. Y vale $A \vdash A_{\mathrm{DNF}}$.

Obs. 3. Continuamos la demostración por la refutación de la fórmula en DNF mediante el uso de cut.

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \Gamma, A, A_{\mathrm{DNF}} \vdash \bot & \Gamma, A \vdash A_{\mathrm{DNF}}\end{array}}{\Gamma, A \vdash \bot}\,\mathrm{cut}$$

Para convertir una fórmula cualquiera a DNF, vamos a implementar una traducción *small-step* implementando el siguiente sistema de reescritura.

$\neg\neg a \rightsquigarrow a$	eliminación de $\neg\neg$
$\neg\bot \rightsquigarrow \top$	
$\neg\top \rightsquigarrow \bot$	
$a \to b \rightsquigarrow \neg a \vee b$	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 $\wedge$

Fig. 4.3: Sistema de reescritura para conversión a DNF de forma sintáctica

Pero no podemos hacerlo meramente de forma sintáctica, sino que tenemos *generar una demostración* para cada equivalencia.

Congruencias

Hay casos en donde tenemos que reemplazar una sub-fórmula por una equivalente. Por ejemplo para reescribir $a \vee \boldsymbol{\neg(b \vee c)} \rightsquigarrow a \vee \boldsymbol{(\neg b \wedge \neg c)}$ reescribimos la sub-fórmula $\neg(b \vee c) \rightsquigarrow \neg b \wedge \neg c$. Esto de forma sintáctica sería trivial, basta con hacerlo recursivamente. Pero para demostrarlo hay que usar la la *congruencia* de los conectivos, que también hay que demostrar.

$$A \vdash A' \Rightarrow A \wedge B \vdash A' \wedge B$$
$$A \vdash A' \Rightarrow A \vee B \vdash A' \vee B$$
$$A' \vdash A \Rightarrow \neg A \vdash \neg A'$$

No hay regla de congruencia para $\to$ pues se convierte en un $\vee$. Es sumamente importante observar que $\neg$ es *contravariante*, para demostrar $\neg A \vdash \neg A'$ no necesitamos una demostración de $A \vdash A'$, sino de $A' \vdash A$. Esto quiere decir que para todas las equivalencias, incluso las congruencias, no nos alcanza con demostrarlas en un solo sentido, sino que vamos a necesitar ambos, la ida y la vuelta: para $\neg(a \vee b) \rightsquigarrow \neg a \wedge \neg b$ necesitamos $\neg(a \vee b) \vdash \neg a \wedge \neg b$ y $\neg a \wedge \neg b \vdash \neg(a \vee b)$. lo notamos como

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

Algoritmo

Finalmente, el algoritmo para generar la demostración de la conversión de una fórmula en DNF se implementa de forma *small-step*. La conversión es la clausura de hacer un "paso", que puede o bien ser un paso de reescritura, o uno de congruencia reescribiendo una sub-fórmula. En cada uno se usa una de las siguientes demostraciones.

Pasos base

$$\begin{aligned}
\neg\neg a &\dashv\vdash a \\
\neg\bot &\dashv\vdash \top \\
\neg\top &\dashv\vdash \bot \\
a \to b &\dashv\vdash \neg a \vee b \\
\neg(a \vee b) &\dashv\vdash \neg a \wedge \neg b \\
\neg(a \wedge b) &\dashv\vdash \neg a \vee \neg b \\
(a \vee b) \wedge c &\dashv\vdash (a \wedge c) \vee (b \wedge c) \\
c \wedge (a \vee b) &\dashv\vdash (c \wedge a) \vee (c \wedge b) \\
a \vee (b \vee c) &\dashv\vdash (a \vee b) \vee c \\
a \wedge (b \wedge c) &\dashv\vdash (a \wedge b) \wedge c
\end{aligned}$$

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

$$\begin{aligned}
A \wedge B &\dashv\vdash A' \wedge B \\
A \vee B &\dashv\vdash A' \vee B \\
\neg A &\dashv\vdash \neg A'
\end{aligned}$$

Fig. 4.4: Pasos de conversión a DNF

En total son 26 demostraciones. Nos ahorramos los detalles porque son bien conocidas (por ej. DeMorgan).

(DUDA: Demostración de que termina? De que es correcto? Al menos una cita para que sea más confiable el sistema de reescritura? O se asume como bien conocido?)

4.3.3. Contradicciones

Tenemos la fórmula traducida a DNF. Debemos demostrar una contradicción a partir de ella. Si tenemos las cláusulas $C_1 \vee C_2$, podemos demostrar $C_1 \vee C_2 \vdash \bot$ usando E$\vee$ y asumiendo cada una, llegar a una contradicción. Esto se generaliza a N cláusulas mediante el uso de E$\vee$ anidados. Por esto decimos que hay que *"refutar cada cláusula"*. El método tiene tres formas de refutarlas

- Contienen fórmulas opuestas: $A \wedge \neg A$ (con E$\neg$)
- Contienen $\bot$
- Eliminando cuantificadores universales consecutivos (próxima sección)

Para los primeros dos, es necesario demostrar a partir de la cláusula una fórmula. Pero como pueden tener una cantidad arbitraria, según cómo esté asociado el $\wedge$, una demostración a mano de $A_1 \wedge \ldots \wedge A_i \wedge \ldots \wedge A_n \vdash A_i$, puede ser muy laboriosa. Como las reglas son binarias, hay que usar E$\wedge_1$ y E$\wedge_2$ anidados. Para simplificarlo demostramos otra regla admisible, la proyección de un elemento E$\wedge_\alpha$.

Teorema 4 (Regla admisible E$\wedge_\alpha$)**.** Sea α alguna fórmula de la conjunción $\alpha_1 \wedge \ldots \wedge \alpha_i$. Notamos por E$\wedge_\alpha$ a la proyección *de la fórmula*, sin importar en qué posición de la conjunción está.

$$\dfrac{\Gamma \vdash \alpha_1 \wedge \ldots \wedge \alpha_i \wedge \ldots \wedge \alpha_n \qquad n \in \mathbb{N}}{\Gamma \vdash \alpha_i}\, \mathrm{E}\wedge_{\alpha_i}$$

Demostración. Para generar la demostración correspondiente usando E$\wedge_1$ y E$\wedge_2$, basta con identificar el camino hacia α_i, y luego caminar recursivamente el $\wedge$ usando E$\wedge_1$ si el camino continúa por la izquierda y E$\wedge_2$ si sigue por la derecha. □

Ejemplo 7 (Contradicción)**.** Veamos un ejemplo de las primeras dos formas de refutar cláusulas. Los cuantificadores universales los veremos en la siguiente sección.

$$\dfrac{\mathrm{Ax}\dfrac{}{\Gamma \vdash (\neg a \wedge a \wedge \neg b) \vee (b \wedge a \wedge \bot)} \qquad \Pi_L \quad \Gamma, \neg a \wedge a \wedge \neg b \vdash \bot \qquad \dfrac{\dfrac{}{\Gamma_1 \vdash b \wedge a \wedge \bot}\,\mathrm{Ax}}{\Gamma, b \wedge a \wedge \bot \vdash \bot}\,\mathrm{E}\wedge_\bot}{\Gamma = (\neg a \wedge a \wedge \neg b) \vee (b \wedge a \wedge \bot) \vdash \bot}\,\mathrm{E}\vee$$

donde

$$\Pi_L = \dfrac{\dfrac{\dfrac{}{\Gamma_1 \vdash \neg a \wedge a \wedge \neg b}\,\mathrm{Ax}}{\Gamma_1 \vdash \neg a}\,\mathrm{E}\wedge_{\neg a} \qquad \dfrac{\dfrac{}{\Gamma_1 \vdash \neg a \wedge a \wedge \neg b}\,\mathrm{Ax}}{\Gamma_1 \vdash a}\,\mathrm{E}\wedge_a}{\Gamma_1 = \Gamma, b \wedge a \wedge \bot \vdash \bot}\,\mathrm{E}\neg$$

(DUDA: No se si me convence la notación E$\wedge_\alpha$, después de todo es una proyección y se suele notar con Π, pero ese símbolo lo estamos usando para representar demostraciones (ej. Π_L).)

4.3.4. Eliminación de cuantificadores universales

Hasta ahora logramos razonar por el absurdo, convertir la fórmula a DNF, y encontrar una contradicción siempre que no haya que eliminar cuantificadores universales. Pero es usual que en una teoría de primer orden, los axiomas contengan cuantificadores universales y sea necesario eliminarlos para poder demostrar un **by**. Al eliminarlos, vamos a reemplazar las ocurrencias de su variable por *meta-variables*: aquellas que pueden ser unificadas.

Def. 12 (Unificación)**.** Sean A, B dos fórmulas. Decimos que *unifican* y lo notamos $A \doteq B$ si existe una sustitución de meta-variables tal que $A = B$. Veamos algunos ejemplos. Sean u, v meta-variables.

- $p(\mathrm{u}) \doteq p(a)$ con $\{\mathrm{u} := a\}$
- $p(\mathrm{u}) \not\doteq q(a)$
- $p(\mathrm{u}) \wedge q(b) \doteq p(a) \wedge q(\mathrm{v})$ con $\{\mathrm{u} := a, \mathrm{v} := b\}$
- $p(\mathrm{u}) \to q(b) \not\doteq p(a) \wedge q(\mathrm{v})$

(DUDA: Hace falta agregar el algoritmo de unificación que implementamos?)

Ejemplo 8 (Ejemplo de by con cuantificadores)**.** Tenemos el siguiente programa

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

Para certificar `thus q(a) by ax1, ax2` hay que generar una demostración para la implicación $\Big(\big(\forall x.(p(x) \to q(x))\big) \land p(a)\Big) \to q(a)$.

1. Negamos la fórmula
$$\neg \left[\Big(\big(\forall x.(p(x) \to q(x))\big) \land p(a)\Big) \to q(a)\right].$$

2. La convertimos a DNF
$$\begin{aligned}
&\neg \left[\Big(\big(\forall x.(p(x) \to q(x))\big) \land p(a)\Big) \to q(a)\right] \\
&\equiv \neg \left[\neg\Big(\big(\forall x.(p(x) \to q(x))\big) \land p(a)\Big) \lor q(a)\right] && (A \to B \equiv \neg A \lor B) \\
&\equiv \neg\neg\Big(\big(\forall x.(p(x) \to q(x))\big) \land p(a)\Big) \land \neg q(a) && (\neg(A \lor B) \equiv \neg A \land \neg B) \\
&\equiv \big(\forall x.(p(x) \to q(x))\big) \land p(a) \land \neg q(a) && (\neg\neg A \equiv A)
\end{aligned}$$
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.

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

4. Probamos eliminando $\forall x.(p(x) \to q(x))$. Reemplazamos x por una meta-variable fresca u.
$$(p(\mathrm{u}) \to q(\mathrm{u})) \land p(a) \land \neg q(a)$$
¡No está en DNF! Hay que volver a convertir.

5. Convertimos a DNF
$$\begin{aligned}
&(p(\mathrm{u}) \to q(\mathrm{u})) \land p(a) \land \neg q(a) \\
&\equiv (\neg p(\mathrm{u}) \lor q(\mathrm{u})) \land p(a) \land \neg q(a) && (A \to B \equiv \neg A \lor B) \\
&\equiv ((\neg p(\mathrm{u}) \land p(a)) \lor (q(\mathrm{u}) \land p(a))) \land \neg q(a) && ((A \lor B) \land C \equiv (A \land C) \lor (A \land C)) \\
&\equiv (\neg p(\mathrm{u}) \land p(a) \land \neg q(a)) \lor && ((A \lor B) \land C \equiv (A \land C) \lor (A \land C)) \\
&\quad (q(\mathrm{u}) \land p(a) \land \neg q(a))
\end{aligned}$$

6. Buscamos una contradicción refutando cada cláusula. Esta vez, no podemos volver a eliminar un forall (por motivos de eficiencia) y los literales opuestos tienen que *unificar* en lugar de ser iguales. Las sustituciones tienen que ser compatible entre todas las cláusulas (no pueden asignar valores diferentes a la misma meta-variable)

   - $\neg p(\mathrm{u}) \land p(a) \land \neg q(a)$ tenemos $p(\mathrm{u}) \doteq p(a)$ con $\{\mathrm{u} := a\}$
   - $q(\mathrm{u}) \land p(a) \land \neg q(a)$ tenemos $q(\mathrm{u}) \doteq q(a)$ con $\{\mathrm{u} := a\}$

Algoritmo

1. Si la cláusula no puede ser refutada por contener $\bot$ ni literales opuestos
2. Para cada fórmula, si comienza con $\forall$ (ej. $\forall x_0.\forall x_1 \ldots \forall x_n.p(x_0, \ldots, x_n)$) se busca una refutación sin generar la demostración.
   - Para combinación de prefijos de $\forall$ consecutivos, se reemplaza su variable por una meta-variable fresca, se re-convierte a DNF y se intenta encontrar una refutación (unificando con $\alpha-$equivalencia)
     - $\forall x_1 \ldots \forall x_n.p(u_0, \ldots, x_n)$
     - $\ldots$
     - $p(u_0, \ldots, u_n)$
   - Se usa la menor cantidad de eliminaciones posibles.
   - Si puede ser refutada, nos da como resultado una sustitución que asigna a cada meta-variable u_i un término t_i.
3. Se usa E$\forall$ reemplazando cada variable por el término asignado a la meta-variable correspondiente, para obtener la fórmula con los $\forall$ eliminados, y luego se genera la demostración de la refutación de la forma usual.

Ejemplo 9 (Eliminación consecutiva minimal)**.** Si se tiene

$$(\forall x.\forall y.p(x) \vee q(y)) \wedge \neg p(a) \wedge \neg q(b)$$

se reemplazarían tanto x como y por meta-variables frescas u_0 y u_1, quedando así $(p(u_0) \vee q(u_1)) \wedge \neg p(a) \wedge \neg q(b)$ que se podrá refutar. En cambio, en

$$(\forall x.\forall y.p(x) \wedge q(y)) \wedge \neg(\forall z.p(a) \wedge q(z))$$

es necesario eliminar solamente $\forall x$. Y la unificación será capaz de tener en cuenta la alpha equivalencia, así puede unificar $\forall y.p(u_0) \wedge q(y) \doteq \forall z.p(a) \wedge q(z)$.

Ejemplo 10 (Eliminación de una sola fórmula)**.** Se eliminan los $\forall$ consecutivos de una sola fórmula de la cláusula. Por ejemplo, en la siguiente o bien eliminamos $\forall x.p(x)$ o $\forall y.q(y)$ pero no ambos.

$$(\forall x.p(x)) \wedge (\forall y.q(y)) \wedge \neg p(a) \wedge \neg q(b)$$

Compatibilidad de sustituciones

Como cada cláusula se refuta por separado, hay que asegurar que las sustituciones de cada una sean compatibles entre sí. Es decir, que no asignen términos diferentes a las mismas meta-variables. Por ejemplo, en

Esto quiere decir que debemos probar con todas las sustituciones posibles, porque puede haber combinaciones que la hagan incompatible. Por ejemplo, en las siguientes cláusulas hay más de una sustitución candidata para cada una.

- $f(u_0) \wedge \neg f(a) \wedge \neg f(b)$ tenemos $\{u_0 := a\}$, $\{u_0 := b\}$
- $f(u_0) \wedge \neg f(b)$ solo $\{u_0 := b\}$

Si en la primera nos quedamos con $\{u_0 := a\}$, no podríamos refutar la 2da.

4.3.5. Poder expresivo

(DUDA: Está bien decir poder expresivo?)

El solver implementado es **completo para lógica proposicional**, pero heurístico para lógica de primer orden. Esto es aceptable, puesto que la satisfacibilidad de lógica de primer orden es indecidible (por el teorema de Church [Par]), y además el objetivo del trabajo no fue dar el mejor solver, sino dar alguno que se pueda certificar.

Teorema 5. El solver es **completo** para lógica proposicional.

Demostración. (DUDA: Citar Hilbert 1950?) Lo hacemos semánticamente. Sea α una fórmula proposicional cualquiera, supongamos que es válida ($\vdash \alpha$). Queremos argumentar que el solver va a poder generar una demostración para ello. Esto es cierto $\iff$ $\neg\alpha$ es insatisfactible.

Siempre vamos a poder convertir $\neg\alpha$ a DNF, por lo que tenemos $(a_1 \wedge \ldots \wedge a_n) \vee \ldots \vee (b_1 \wedge \ldots \wedge b_m)$. Para que sea insatisfactible, por definición sobre $\vee$ todas las cláusulas tienen que serlo. Para que una claúsula lo sea, no tiene que haber una valuación que la haga verdadera. Supongamos que lo es y existe una valuación v. Esta valuación está unívocamente determinada, al ser una conjunción, tiene que asignar a cada literal p_1 un 1 si es positivo o un 0 si es negativo. Para que no sea verdadera, necesariamente debe aparecer la misma variable dos veces, una vez negada y la otra sin negar, o bien debe aparecer false.

Esto es exactamente lo que busca el solver, por lo que si es refutable, siempre va a poder refutarla.

(DUDA: Está suficientemente bien escrito esto? Supongo que no. En la intro hay que agregar las definiciones de la semántica de LPO.) □

Teorema 6. El solver es **incompleto** para lógica de primer orden.

Demostración. El siguiente es un contra ejemplo, que no encuentra la refutación porque para ello debería eliminar ambos $\forall$, pero elimina a lo sumo los de una fórmula.

```
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
```

Pero esto no es lo único que le falta para ser completo. También se podría dar un contra ejemplo más burdo que requiera un *SAT solver* completo. □

4.3.6. Azúcar sintáctico

Antes mencionamos que se puede usar **hence** en lugar de **thus** referenciando automáticamente a la hipótesis anterior, y análogamente lo mismo para **have** y **then**. Esto se implementa desde el *parser*, todo se compila como los comandos base, y se agrega la hipótesis anterior (`-`) cuando es necesario. Esto simplifica al certificador permitiendo que solo conozca a **have** y **thus**.

4.4. Descarga de conjunciones

¿Cómo podemos certificar el siguiente programa?

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

Veamos en particular el primer comando de la demostración. La tesis es una conjunción que está asociada de una forma particular, y se quiere demostrar $a \wedge e$ que es parte de la tesis.

1. Se convierte la conjunción y lo que se demuestra en conjuntos

$$(a \wedge b) \wedge ((c \wedge d) \wedge e) \rightsquigarrow \{a, b, c, d, e\}$$
$$(a \wedge e) \rightsquigarrow \{a, e\}$$

2. Si está contenido, se separa lo demostrado y el resto

$$\{a, b, c, d, e\} \rightsquigarrow \{b, c, d\}\{a, e\}$$

3. Se construye una *nueva tesis* reordenando la fórmula de forma tal que sea sencillo hacer I$\wedge$ (poniendo a la izquierda lo demostrado aislado de lo demás)

$$(a \wedge e) \wedge (b \wedge c \wedge d)$$

   De esa forma, al usar la regla

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \mathrm{I}\wedge$$

   la demostración de $a \wedge e$ se hace de la forma usual con by, y se reduce la tesis a $b \wedge c \wedge d$ continuando la certificación por allí, insertando la demostración resultante en $\Gamma \vdash B$.

4. Para demostrar la equivalencia entre la tesis vieja y su versión re-ordenada se usa el mismo solver que el by. Al ser completo para proposicional, también puede resolver equivalencias por asociatividad y re-orden.

Finalmente, queda certificado como

$$\dfrac{\text{solver}\ \dfrac{}{\Gamma \vdash (a \wedge e) \wedge (b \wedge c \wedge d) \to (a \wedge b) \wedge ((c \wedge d) \wedge e)} \qquad \dfrac{\dfrac{}{\Gamma \vdash a \wedge e}\ \text{by} \qquad \begin{array}{c}\vdots\\ \Gamma \vdash b \wedge c \wedge d\end{array}}{\Gamma \vdash (a \wedge e) \wedge (b \wedge c \wedge d)}\ \mathrm{I}\wedge}{\Gamma \vdash (a \wedge b) \wedge ((c \wedge d) \wedge e)}\ \mathrm{E}\to$$

4.5. Comandos correspondientes a reglas de inferencia

Como se puede ver en Tabla 3.1 Reglas de inferencia y comandos, el resto de los comandos se corresponden directamente con reglas de inferencia, por lo que su traducción es directa.

- **`take`** (I∃)

  Si la tesis es **`exists`** `X . a`, el comando **`take`** `X := t` la reduce a `a` con x reemplazado por t y la certifica como

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

  insertando la demostración certificada del resto en en $\Gamma \vdash A\{x := t\}$

- **`consider`** (E∃)

  El comando **`consider`** `X` **`st`** `h: a` **`by`** `h1, ... hn` se certifica como

  $$\frac{\Gamma \vdash \exists x.A \qquad \Gamma, A \vdash B \qquad x \notin fv(\Gamma, B)}{\Gamma \vdash B}\ \text{E}\exists$$

  - $\Gamma \vdash \exists x.A$ se demuestra mediante el by.
  - Se agrega la hipótesis `h: a` al contexto como axioma, se continúa la certificación y se inserta la demostración resultante en $\Gamma, A \vdash B$.

- **`let`** (I∀)

  Si la tesis es **`forall`** `X. a`, el comando **`let`** `X` reduce la tesis a `a` y continúa la certificación, insertando el resultado en la demostración de $\Gamma \vdash A$

  $$\frac{\Gamma \vdash A \qquad x \notin fv(\Gamma)}{\Gamma \vdash \forall x.A}\ \text{I}\forall$$

- **`cases`** (E∨)

  El comando

  ```
  cases by h1, ..., hn
    case c1
    ...
    case cm
  end
  ```

  se certifica como varios E∨ anidados, en donde el primer ∨ se certifica mediante by. Cada rama certifica la sub-demostración agregando la hipótesis del caso al contexto como axioma.

  $$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ \text{E}\vee$$

- **`suppose`** (I→, I¬)

  Si la tesis es `a -> b`, el comando **`suppose`** `h: a` reduce la tesis a `b` y agrega al contexto la hipótesis `h: a` como axioma. La certifica como

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

  insertando el resto de la demostración certificada en su sub-demostración.

  Si la tesis es `~a`, es análogo pero interpretándolo como `a -> false`.

4.6. Comandos adicionales

- **`equivalently`**

  Si la tesis es a, el comando **`equivalently`** `a'` usa el mismo solver que el by para demostrar $a' \to a$ y reduce la tesis a a'.

- **`claim`**

  La certificación del comando

```
claim h: f
proof
   ...
end
```

  Consiste en certificar la sub-demostración y agregar la hipótesis `h: f` como teorema al contexto.

5. EXTRACCIÓN DE TESTIGOS DE EXISTENCIALES

Puntos a abordar
- mencionar realizabilidad clásica. Related work capaz en la conclusión - hacer una investigación de otras formas de hacer witness extraction. Capaz no es original lo nuestro (y capaz Coq lo banca con realizabilidad).

- Motivación, limitaciones de lógica clásica. Demostración sqrt 2
- Lógica intuicionista
- Como necesitamos reducir en ND, necesitamos la demo en ND. Escribirla en este caso.
- También queremos para Π_2^0, mostrar la extensión en ND.
- En realidad no nos sirve $\Gamma^{\neg\neg}$, queremos dejarlo como está y demostrar que los axiomas demuestran sus traducciones. Pero no vale siempre (buscar c.ej), caracterizar cuando.
- Sumarizar cómo queda, vincular con reducción. Mostrar ejemplos en PPA que funcionan y ejemplos que no.
- Extensión a demostraciones. Mostrar algunos ejemplos interesantes (y los que usen los lemas dNegRElim y rElim)
- Lemas para demostraciones: dNegRElim (relacionar con 4.3.1), rElim, tNegRElim
- Reducción (buena explicación https://plato.stanford.edu/entries/natural-deduction/). En realidad se conoce como **normalization**.
  - Similitud con reducción en cálculo lambda.
  - Ejemplos de LP y todo LPO
  - substHyp, substVar en proofs
  - Argumentos de que es correcto y completo?
  - Small step vs big step

Queremos, dado un teorema, *extraer testigos de un existencial*. Por ejemplo, si tenemos una demostración de $\exists x.p(x)$ la extracción nos debería instanciar x en un término t tal que $p(t)$. Imaginemos que tenemos el siguiente programa de PPA

```
axiom ax: p(v)
theorem thm: exists X . p(X)
proof
    take X := v
    thus p(v) by ax
end
```

¿Cómo hacemos para extraer La demostración generada por el certificador es **clásica**. La forma más fácil de extraer un testigo de una demostración es normalizarla y obtener el testigo de su forma normal. Pero esto no se puede hacer en general para lógica clásica, porque las demostraciones en general no son **constructivas**.

En la lógica clásica vale el *principio del tercero excluido*, comúnmente conocido por sus siglas en inglés, LEM (*law of excluded middle*).

Prop. 1 (LEM)**.** Para toda fórmula A, es verdadera ella o su negación

$$A \vee \neg A$$

Las demostraciones que usan este principio suelen dejar aspectos sin concretizar, como muestra el siguiente ejemplo bien conocido:

Teorema 7. Existen dos números irracionales, a, b tales que a^b es irracional

Demostración. Considerar el número $\sqrt{2}^{\sqrt{2}}$. Por LEM, es o bien racional o irracional.

- Supongamos que es racional. Como sabemos que $\sqrt{2}$ es irracional, podemos tomar $a = b = \sqrt{2}$.
- Supongamos que es irracional. Tomamos $a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$. Ambos son irracionales, y tenemos

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

que es racional.

□

Como se puede ver, la prueba no nos da forma de saber cuales son a y b. Es por eso que en general, tener una demostración de un teorema que afirma la existencia de un objeto que cumpla cierta propiedad, no necesariamente nos da una forma de encontrar tal objeto. Entonces tampoco vamos a poder extraer un testigo.

En el caso de Teorema 7 , lo demostramos de una forma no constructiva pero existen formas constructivas de hacerlo (TODO: citar). Pero hay casos en donde no. Por ejemplo, si consideramos la fórmula

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

y pensamos en C como algo indecidible, por ejemplo `HALT`, trivialmente podemos demostrarlo de forma no constructiva (LEM con $C \vee \neg C$) pero no de forma constructiva.

5.1. Lógica intuicionista

Para solucionar estos problemas existe la lógica **intuicionista**, que se puede definir como la lógica clásica sin LEM. Al no contar con ese principio, las demostraciones son constructiva. Esto permite por un lado para tener interpretaciones computacionales (como la *BHK*) y además que exista la noción de *forma normal* de uan demostración. Existen métodos bien conocidos para reducir prueba hacia su forma normal con un proceso análogo a una reducción de cálculo λ. Luego en la forma normal se esperaría que toda demostración de un $\exists$ sea mediante I$\exists$, explicitando el testigo.

Al no tener LEM, tampoco valen principios equivalentes, como la eliminación de la doble negación (TODO: hablar un poco más de esto)

5.2. Traducción de Friedman

5.2.1. Traducción de doble negación

Queremos extraer testigos de las demostraciones generadas por el certificador de PPA, pero son en lógica clásica. Sabemos que podemos hacerlo para lógica intuicionista. ¿Cómo conciliamos ambos mundos?

Existen muchos métodos que permiten embeber la lógica clásica en la intuicionista (TODO: citar). Un mecanismo general es la traducción de **doble negación**, que intuitivamente consiste en agregar una doble negación recursivamente a toda la fórmula. Por ejemplo

Def. 13 (Traducción *Gödel-Gentzen*)**.** Dada una fórmula A se asocia con otra A^{N}. La traducción se define inductivamente en la estructura de la fórmula de la siguiente forma

$$\begin{aligned}
\bot^{\mathrm{N}} &= \bot \\
A^{\mathrm{N}} &= \neg\neg A \quad \text{con } A \neq \bot \text{ atómica} \\
(A \wedge B)^{\mathrm{N}} &= A^{\mathrm{N}} \wedge B^{\mathrm{N}} \\
(A \vee B)^{\mathrm{N}} &= \neg(\neg A^{\mathrm{N}} \wedge \neg B^{\mathrm{N}}) \\
(A \to B)^{\mathrm{N}} &= A^{\mathrm{N}} \to B^{\mathrm{N}} \\
(\forall x.A)^{\mathrm{N}} &= \forall x.A^{\mathrm{N}} \\
(\exists x.A)^{\mathrm{N}} &= \neg\forall x.\neg A^{\mathrm{N}}
\end{aligned}$$

Teorema 8. Si tenemos $\vdash_C A$, luego $\vdash_I A^{\mathrm{N}}$

Esto significa que dada una demostración en lógica clásica, podemos obtener una en lógica intuicionista de su traducción. Pero esto no es exactamente lo que queremos, porque por ejemplo

$$(\exists x.p(x))^{\mathrm{N}} = \neg\forall x.\neg\neg\neg p(x)$$

Que al no ser una demostración de un $\exists$, al reducirla no necesariamente obtendremos un testigo.

5.2.2. El truco de Friedman

La idea de Friedman [Miq11] es generalizar la traducción Gödel-Gentzen reemplazando la negación intuicionista $\neg A \equiv A \to \bot$ por una relativa $\neg_R A \equiv A \to R$ que está parametrizada por una fórmula arbitraria R. Esto nos va a permitir, con una elección particular de R, traducir una demostración clásica de una fórmula Σ^0_1 (e incluso Π^0_2) a una intuicionista, y usarla para demostrar **la fórmula original**. Finalmente podremos reducirla y hacer la extracción de forma usual.

Def. 14 (Traducción de doble negación relativizada)**.**

$$\begin{aligned}
\bot^{\neg\neg} &= \bot \\
A^{\neg\neg} &= \neg_R\neg_R A \quad \text{con } A \neq \bot \text{ atómica} \\
(A \wedge B)^{\neg\neg} &= A^{\neg\neg} \wedge B^{\neg\neg} \\
(A \vee B)^{\neg\neg} &= \neg_R(\neg_R A^{\neg\neg} \wedge \neg_R B^{\neg\neg}) \\
(A \to B)^{\neg\neg} &= A^{\neg\neg} \to B^{\neg\neg} \\
(\forall x.A)^{\neg\neg} &= \forall x.A^{\neg\neg} \\
(\exists x.A)^{\neg\neg} &= \neg_R\forall x.\neg_R A^{\neg\neg}
\end{aligned}$$

Teorema 9. Si $\Gamma \vdash_C A$, luego $\Gamma^{\neg\neg} \vdash_I A^{\neg\neg}$

Veremos esta extensión de la traducción a contextos y demostraciones más adelante.

Veamos cómo podemos usarla para, dada una demostración clásica de $\exists x A$ obtener una intuicionista.

Prop. 2. Sea Π una demostración clásica de $\exists x.A$, y A una fórmula atómica. Si tenemos

$$\Gamma \vdash_C \exists x.A,$$

luego

$$\Gamma^{\neg\neg} \vdash_I \exists x.A.$$

Demostración. Aplicando la traducción, tenemos que

$$\frac{\Pi}{\Gamma \vdash_C \exists x.A}$$

se traduce a

$$\frac{\Pi^{\neg\neg}}{\Gamma^{\neg\neg} \vdash_I \neg_R\forall x.\neg_R\neg_R\neg_R A}$$

luego, tomando R como la fórmula que queremos probar, $\exists x.A$

$$\begin{aligned}
\Pi^{\neg\neg} \rhd \Gamma^{\neg\neg} &\vdash_I \neg_R\forall x.\neg_R\neg_R\neg_R A \\
&\iff \Gamma^{\neg\neg} \vdash_I \neg_R\forall x.\neg_R A && (2) \\
&= \Gamma^{\neg\neg} \vdash_I (\forall x.(A \to R)) \to R \\
&= \Gamma^{\neg\neg} \vdash_I (\forall x.(A \to \exists x.A)) \to \exists x.A && (R = \exists x A) \\
&\Rightarrow \Gamma^{\neg\neg} \vdash_I \exists x.A && (4)
\end{aligned}$$

□

Lema 2. $\neg_R\neg_R\neg_R A \iff \neg_R A$

Demostración. (TODO: En deducción natural) □

Obs. 4. $\vdash_I \forall x(A \to \exists x A)$

(TODO: IDem pero en ND, y también para $\forall$)

6. LA HERRAMIENTA PPA

```haskell
type VarId = String
type FunId = String
type PredId = String
type HypId = String

data Term
    = TVar VarId
    | TMetavar Metavar
    | TFun FunId [Term]
```

```haskell
data Form
    = FPred PredId [Term]
    | FAnd Form Form
    | FOr Form Form
    | FImp Form Form
    | FNot Form
    | FTrue
    | FFalse
    | FForall VarId Form
    | FExists VarId Form
```

Fig. 6.1: Modelado de fórmulas y términos de LPO

Las meta-variables se usan para unificación, que es parte del solver de PPA. Ver más en Subsección 4.3.4 Eliminación de cuantificadores universales

```
data Proof =
    | PAx HypId
    | PAndI
        { proofLeft :: Proof
        , proofRight :: Proof
        }
    | PAndE1
        { right :: Form
        , proofAnd :: Proof
        }
    | PAndE2
        { left :: Form
        , proofAnd :: Proof
        }
    | POrI1
        { proofLeft :: Proof
        }
    | POrI2
        { proofRight :: Proof
        }
    | POrE
        { left :: Form
        , right :: Form
        , proofOr :: Proof
        , hypLeft :: HypId
        , proofAssumingLeft :: Proof
        , hypRight :: HypId
        , proofAssumingRight :: Proof
        }
    | PImpI
        { hypAntecedent :: HypId
        , proofConsequent :: Proof
        }
    | PImpE
        { antecedent :: Form
        , proofImp :: Proof
        , proofAntecedent :: Proof
        }
    | PNotI
        { hyp :: HypId
        , proofBot :: Proof
        }
    | PNotE
        { form :: Form
        , proofNotForm :: Proof
        , proofForm :: Proof
        }
    | PTrueI
    | PFalseE
        { proofBot :: Proof
        }
    | PLEM
    | PForallI
        { newVar :: VarId
        , proofForm :: Proof
        }
    | PForallE
        { var :: VarId
        , form :: Form
        , proofForall :: Proof
        , termReplace :: Term
        }
    | PExistsI
        { inst :: Term
        , proofFormWithInst :: Proof
        }
    | PExistsE
        { var :: VarId
        , form :: Form
        , proofExists :: Proof
        , hyp :: HypId
        , proofAssuming :: Proof
        }
```

Fig. 6.2: Modelado de reglas de inferencia para demostraciones

El modelado de las reglas de inferencia omite varios detalles que están implícitos y serán inferidos por el algoritmo de chequeo. De esa forma las demostraciones son más fáciles de escribir y generar. Por ejemplo, `PImpI` no especifica en su modelo cuál es la implicación que se está introduciendo, dado que durante el chequeo debería ser la fórmula actual a demostrar

6.1. Compiladores

- Primer de compiladores en general y sus frontends
- Parser generators en general. LR/LALR
- Happy. Alex.
- Sintaxis BNF en apéndice (el archivo). Incluir el archivo Alex/happy? Es cortito

7. CONCLUSIONES

- (TODO: Al final de la tesis)

Trabajo futuro

- Inducción como axioma de deducción natural, permite demostrar más cosas. Implica tocar todo
- Sofisticación del by para eliminación de foralls más compleja que consecutivos. (elimina un solo forall, pero no intenta recursivamente eliminar todos)
- Sofisticación de PPA como lenguaje de programación, implementar más comandos .Permitir importar archivos/módulos. Hacer una standard library de teorías y teoremas.
- Mejorar la extracción de testigos?
- Mejorar reporting de errores, muy rústico.

BIBLIOGRAFíA

[BW05] Henk Barendregt y Freek Wiedijk. «The challenge of computer mathematics». En: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 363.1835 (sep. de 2005), págs. 2351-2375. ISSN: 1471-2962. DOI: 10.1098/rsta.2005.1650. URL: http://dx.doi.org/10.1098/rsta.2005.1650.

[Gen35] Gerhard Gentzen. «Untersuchungen über das logische Schließen. I». En: *Mathematische Zeitschrift* 39.1 (dic. de 1935), págs. 176-210. ISSN: 1432-1823. DOI: 10.1007/BF01201353. URL: https://doi.org/10.1007/BF01201353.

[Miq11] Alexandre Miquel. «Existential witness extraction in classical realizability and via a negative translation». En: *Log. Methods Comput. Sci.* 7.2 (2011). DOI: 10.2168/LMCS-7(2:2)2011. URL: https://doi.org/10.2168/LMCS-7(2:2)2011.

[Par] Rohit Parikh. «Church's theorem and the decision problem». En: *Routledge Encyclopedia of Philosophy*. Routledge. ISBN: 9780415250696. DOI: 10.4324/9780415249126-y003-1. URL: http://dx.doi.org/10.4324/9780415249126-Y003-1.

[Wie] Freek Wiedijk. *Mathematical Vernacular*. https://www.cs.ru.nl/~freek/notes/mv.pdf.