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

2. DEDUCCIÓN NATURAL

3. EL LENGUAJE PPA

4. EL CERTIFICADOR DE PPA

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

En los capítulos anteriores vimos como el lenguaje PPA puede ser usado para escribir demostraciones de alto nivel, que son certificadas generando demostraciones de bajo nivel usando el sistema lógico de deducción natural. Ahora vamos a introducir una nueva funcionalidad: la **extracción de testigos**.

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

Fig. 5.1: Extracción simple

```
axiom ax: forall Y . p(Y, v)
theorem t:
   forall X. exists V . p(X, V)
proof
   let X
   take V := v
   thus p(X, v) by ax
end
```

Fig. 5.2: Extracción con instanciación

```
axiom ax1: q(m)
axiom ax2: forall X. q(X) -> p(X)

theorem t1: exists X. q(X)
proof
   take X := m
   thus q(m) by ax1
end

theorem t2: exists X. p(X)
proof
   consider Y st h: q(Y) by t1
   take X := Y
   hence p(Y) by ax2
end
```

Fig. 5.3: Extracción indirecta

Por ejemplo, en el programa Figura 5.1 Extracción simple la extracción nos permitirá encontrar un término t que sea testigo de $\exists x.p(x)$, es decir que cumpla $p(t)$. En este caso es fácil encontrarlo a ojo sobre la demostración de PPA, sería `v`. Pero puede haber casos en donde no sea tan trivial, como en el programa Figura 5.3 Extracción indirecta, en donde se instancia la variable en un término de forma indirecta. Además, también querríamos poder extraer en casos donde haya cuantificadores universales, como en Figura 5.2 Extracción con instanciación. Buscamos un mecanismo general, que nos permita a partir de cualquier demostración una fórmula de la pinta $\forall x_0 \dots \forall x_n \exists y.\alpha$ extraer un testigo. Vamos a hacerlo a partir de los certificados de deducción natural.

5.1. La lógica clásica no es constructiva

El objetivo es extraer el testigo de las demostraciones generadas por el certificador, pero estas son en lógica clásica, que tiene el gran problema de que en general, **no es constructiva**. ¿Qué quiere decir? Que en general, puede suceder que una demostración de $\exists x.p(x)$ no nos diga quien es x, y por lo tanto no podamos extraer un testigo. Esto es porque en la lógica clásica vale el *principio del tercero excluido* o LEM

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.

□

La prueba no nos da forma de saber cuales son a y b. Es por eso que en general, en lógica clásica, 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 elegimos demostrarlo de forma no constructiva, pero existen formas constructivas de hacerlo (TODO: citation needed). Pero hay casos en donde no.

Ejemplo 11 (Demostración no constructiva)**.** Si consideramos la fórmula

$$\exists x.((x = 1 \land C) \lor (x = 0 \land \neg C))$$

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

5.2. Lógica intuicionista

Como alternativa a la lógica clásica existe existe la lógica **intuicionista**, que se puede definir como la lógica clásica sin LEM[1]. Al no contar con ese principio, las demostraciones son constructivas. Esto permite por un lado tener interpretaciones computacionales (como la *BHK*) y además que exista la noción de *forma normal* de una demostración. Existen métodos bien conocidos para reducir prueba hacia su forma normal con un proceso análogo a una reducción de cálculo λ.

Esto permite usar como estrategia de extracción la siguiente: normalizar la demostración y obtener el testigo de la forma normal. En ella, se esperaría que toda demostración de un $\exists$ sea mediante I$\exists$, explicitando el testigo.

[1] Al no tener LEM, tampoco valen principios de razonamiento clásicos equivalentes, como la eliminación de la doble negación.

5.3. Estrategia de extracción de testigos

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 métodos que permiten *embeber* la lógica clásica en la intuicionista. Uno de ellos es la **traducción de Friedman** que se aborda en la siguiente sección. La estrategia general entonces es la siguiente (esquematizada en Figura 5.4), dada una demostración en PPA como por ejemplo de Figura 5.1:

1. La certificamos generando una demostración clásica en deducción natural, usando el `Certifier`. Nos da un contexto con una demostración por teorema.

2. Generamos una única demostración haciendo *inline* de las demostraciones de otros teoremas citados, así cuando se reduce, se reduce la demostración completa y no una parte.

3. Usamos la traducción de Friedman para obtener una demostración intuicionista de la misma fórmula.

   Restricción: La fórmula a demostrar debe ser de la forma $\forall y_0 \ldots \forall y_n . \exists x . A$.

4. Instanciamos las variables de los $\forall$ en términos proporcionados por el usuario, quedando una fórmula de la forma $\exists x . A$.

5. Normalizamos la demostración.

   Limitación: No vamos a poder llevar cualquier demostración a su forma normal.

6. Al ser una demostración normalizada de un $\exists$, debe comenzar con I$\exists$, que especifica el término que hace cierta la fórmula. Este es precisamente el testigo que estábamos buscando.

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

En las siguientes secciones vemos en detalle la traducción de Friedman y la normalización (o reducción) de demostraciones.

5.4. Traducción de Friedman

5.4.1. Traducción de doble negación

Existen muchos métodos que permiten embeber la lógica clásica en la intuicionista. Un mecanismo general es la traducción de **doble negación**, que tiene distintas variaciones. Una es la *Gödel-Gentzen* [AF98]

Def. 13 (Traducción *Gödel-Gentzen*)**.** Dada una fórmula A se asocia con otra A^{N}. La

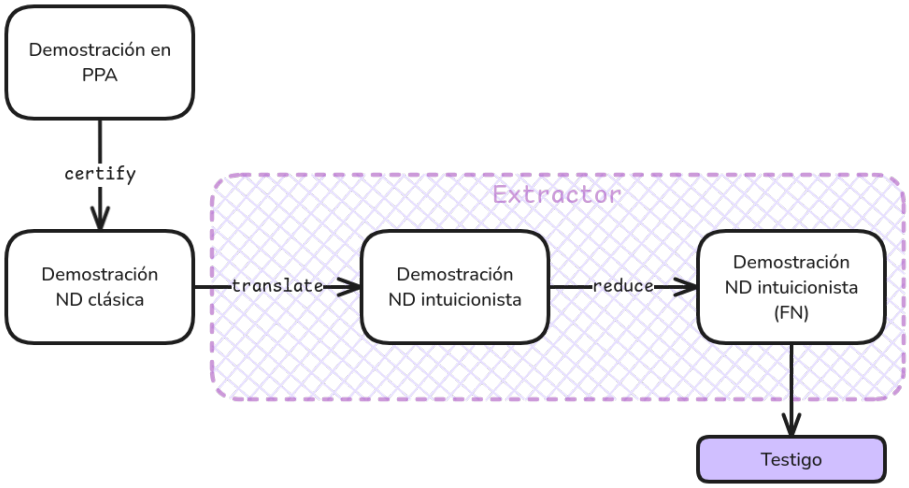

Fig. 5.4: Estrategia de extracción de testigos

traducción se define por inducción estructural.

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

Def. 14 (Traducción de contextos)**.** Se extiende a contextos de la forma esperable

$$\Gamma^{\mathrm{N}} = \{A^{\mathrm{N}} \mid A \in \Gamma\}.$$

Notación. Notamos,

- $\vdash_C$ para expresar que un juicio es derivable en lógica clásica, y $\vdash_I$ para intuicionista.
- $\Pi \rhd \Gamma \vdash A$ para expresar que Π es una demostración de $\Gamma \vdash A$. Equivalente a $\dfrac{\Pi}{\Gamma \vdash A}$

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

Dada una demostración en lógica clásica, podemos obtener una en lógica intuicionista de su traducción. Pero esto no es exactamente lo que queremos, pues si quisiéramos extraer un testigo de una demostración de la fórmula $\exists x.p(x)$, al traducirla nos quedaría $(\exists x.p(x))^{\mathrm{N}} = \neg\forall x.\neg\neg\neg p(x)$, que si bien su demostración sería intuicionista (y por lo tanto constructiva), como no es de un $\exists$ al normalizarla no podremos hacer la extracción.

5.4.2. 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 inteligente de R, traducir una demostración clásica de una fórmula a una intuicionista, y usarla para demostrar **la fórmula original**. Esto nos permite reducirla y hacer la extracción. No va a ser posible para cualquier fórmula, sino las de una clase particular (de la forma $\forall y_1 \dots \forall y_m . \exists x_1 \dots \exists x_k . A$ o Π^0_2)

Def. 15 (Traducción de doble negación relativizada)**.**

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

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

Demostración. Dada una demostración en deducción natural clásica $\Gamma \vdash_C A$, podemos traducirla recursivamente extendiendo la traducción de fórmulas a reglas de inferencia, así generando una demostración de $\Gamma^{\neg\neg} \vdash_I A^{\neg\neg}$. Este proceso está descrito en detalle en Subsección 5.4.4 Traducción de demostraciones □

Vamos a enunciar diferentes versiones de la traducción de Friedman en orden de sofisticación, según para qué clase de fórmulas funcionan. No solo ayuda a entenderla, sino que también fue el mismo enfoque con el que las implementamos. Cada una incluye a la anterior, por lo que en PPA solo quedó implementada la última.

Def. 16 (Jerarquía aritmética de fórmulas)**.** Clasifica las fórmulas en dos clases: Π^0_n y Σ^0_n. Se define por inducción en n.

- Si φ es equivalente a una fórmula sin cuantificadores, está en Π^0_0 y Σ^0_0.
- Sean las clasificaciones Π^0_n y Σ^0_n. Definimos para $n+1$.
  - Si φ es equivalente a una formula de la forma $\exists x_1 \dots \exists x_k . \psi$ donde ψ es Π^0_n, entonces φ es asignada la clasificación Σ^0_{n+1}.
  - Si φ es equivalente a una formula de la forma $\forall x_1 \dots \forall x_k . \psi$ donde ψ es Σ^0_n, entonces φ es asignada la clasificación Π^0_{n+1}.

Una fórmula de Σ^0_n es equivalente a una que comienza con cuantificadores existenciales y alterna $n-1$ veces entre series de universales y existenciales. Mientras que una Π^0_n es análoga pero comenzando con universales.

Las dos que más nos interesan son:

- Σ^0_1: fórmulas de la pinta $\exists x_1 \dots \exists x_k.\varphi$.
- Π^0_2: fórmulas de la pinta $\forall y_1 \dots \forall y_m.\exists x_1 \dots \exists x_k.\varphi$

Una intuición detrás de los nombres de las clases puede ser

- Σ es una sumatoria, que se puede interpretar como disyunciones (en el sentido del álgebra de Boole), y generalizar con un existencial.
- Π análogamente pero con productoria, conjunciones y universales.

5.4.3. Versiones de la traducción

1. **Fórmulas Σ^0_1 atómicas** (Teorema 10):

$$\exists x.A(x) \text{ con } A(x) \text{ atómica.}$$

2. **Fórmulas Π^0_2 atómicas** (Teorema 11):

$$\forall y_1 \dots \forall y_n.\exists x.A(x, y_1, \dots, y_n) \text{ con } A(\dots) \text{ atómica.}$$

3. **Fórmulas Π^0_2 no atómicas** (Teorema 12):

$$\forall y_1 \dots \forall y_n.\exists x.\varphi(x, y_1, \dots, y_n) \text{ con } \varphi(\dots) \text{ no atómica.}$$

   Por ejemplo, podría ser $p(x) \wedge q(y_1, \dots, y_n)$. Pero no podrá ser cualquier fórmula, por ej. no $\neg(p(x) \wedge q(y_1, \dots, y_n))$. En (TODO: Cita) damos una caracterización.

Teorema 10 (Traducción de Friedman para fórmulas Σ^0_1)**.** Sea Π una demostración clásica de $\exists x.A$, y A una fórmula atómica. Si tenemos

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

luego, podemos generar una demostración intuicionista de *la misma fórmula*

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

Demostración. Aplicando la traducción, tenemos que

$$\begin{array}{c} \left(\Pi \rhd \Gamma \vdash_C \exists x.A\right)^{\neg\neg} \\ \| \\ \Pi^{\neg\neg} \rhd \Gamma^{\neg\neg} \vdash_I \neg_R \forall x.\neg_R \neg_R \neg_R A \end{array}$$

luego, tomando $R = \exists x.A$ la fórmula que buscamos probar,

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

En deducción natural,

$$\dfrac{\dfrac{\Pi^{\neg\neg}}{\Gamma^{\neg\neg} \vdash_I \neg_R \forall x \neg_R A^{\neg\neg}} \quad \dfrac{\dfrac{\dfrac{}{\Gamma^{\neg\neg} \vdash_I \neg_R \neg_R \neg_R A}\, \mathrm{I}\neg_R\neg_R\neg_R \quad \dfrac{\dfrac{}{\Gamma^{\neg\neg}, A \vdash_I A}\,\mathrm{Ax}}{\dfrac{\Gamma^{\neg\neg}, A \vdash_I R = \exists x A}{\Gamma^{\neg\neg} \vdash_I \neg_R A}\,\mathrm{I}\to}\,\mathrm{I}\exists}{\Gamma^{\neg\neg}, \neg_R A \vdash_I \neg_R \neg_R \neg_R A}\,\mathrm{cut}}{\Gamma^{\neg\neg} \vdash_I \forall x \neg_R A^{\neg\neg}}\,\mathrm{I}\forall}{\Gamma^{\neg\neg} \vdash_I \exists x.A}\,\mathrm{E}\to$$

□

Obs. 3. En la demostración del Teorema 10 y las de esta sección, luego de la traducción de Friedman, todas las demostraciones deben ser intuicionistas para que sigan siendo constructivas.

Lema 2 (Eliminación de triple negación relativa)**.** $\neg_R \neg_R \neg_R A \iff \neg_R A$ y lo demostramos como dos reglas admisibles, una para cada lado

$$\dfrac{}{\neg_R \neg_R \neg_R A \vdash_I \neg_R A}\,\mathrm{E}\neg_R\neg_R\neg_R \qquad \dfrac{}{\neg_R A \vdash_I \neg_R \neg_R \neg_R A}\,\mathrm{I}\neg_R\neg_R\neg_R$$

Demostración. Primero $\mathrm{I}\neg_R\neg_R\neg_R$

$$\dfrac{\dfrac{\dfrac{}{\neg_R A, \neg_R \neg_R A \vdash_I \neg_R \neg_R A}\,\mathrm{Ax} \quad \dfrac{}{\neg_R A, \neg_R \neg_R A \vdash_I \neg_R A}\,\mathrm{Ax}}{\neg_R A, \neg_R \neg_R A \vdash_I R}\,\mathrm{E}\to}{\neg_R A \vdash_I \neg_R \neg_R \neg_R A}\,\mathrm{I}\to$$

Ahora $\mathrm{E}\neg_R\neg_R\neg_R$

$$\dfrac{\dfrac{}{\neg_R \neg_R \neg_R A, A \vdash_I \neg_R \neg_R \neg_R A}\,\mathrm{Ax} \quad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash_I \neg_R A}\,\mathrm{Ax} \quad \dfrac{}{\Gamma \vdash_I A}\,\mathrm{Ax}}{\Gamma = \neg_R \neg_R \neg_R A, A, \neg_R A \vdash_I R}\,\mathrm{E}\to}{\neg_R \neg_R \neg_R A, A \vdash_I \neg_R \neg_R A}\,\mathrm{I}\to}{\neg_R \neg_R \neg_R A, A \vdash_I R}\,\mathrm{E}\to$$

$$\dfrac{}{\neg_R \neg_R \neg_R A \vdash_I \neg_R A}\,\mathrm{I}\to$$

□

Obs. 4. $\vdash_I \forall x(A \to \exists x A)$. Trivialmente, para cualquier x si vale A entonces va a existir un x tal que valga A.

Teorema 11 (Traducción de Friedman para fórmulas Π^0_2 atómicas)**.** Sea Π una demostración clásica de $\forall y_1 \ldots \forall y_n . \exists x . A(x, y_1, \ldots, y_n)$ y $A(\ldots)$ una fórmula atómica

Si tenemos

$$\Gamma \vdash_C \forall y_1 \ldots \forall y_n . \exists x . A(x, y_1, \ldots, y_n),$$

podemos generar una demostración intuicionista de la misma fórmula

$$\Gamma^{\neg\neg} \vdash_I \forall y_1 \ldots \forall y_n . \exists x . A(x, y_1, \ldots, y_n).$$

Demostración. Lo demostramos en deducción natural para un solo $\forall$. La demostración para una cantidad arbitraria es análoga y fácilmente generalizable a partir de esta. La estrategia consiste en primero introducir el $\forall$ reemplazando su variable por una fresca, para evitar conflictos con las variables usadas en la demostración original. Luego se procede a demostrar el $\exists$ de forma análoga al Teorema 10, usando la traducción de la demostración pero usando

como R no la fórmula original, sino el $\exists$ con la variable ligada por el $\forall$ reemplazada por la fresca.

Tomando $R = \exists x.A(x, y_0)$ y aplicando la traducción, tenemos que

$$\begin{array}{c} \big(\Pi \rhd \Gamma \vdash_C \forall y \exists x.A(x,y)\big)^{\neg\neg} \\ \| \\ \Pi^{\neg\neg} \rhd \Gamma^{\neg\neg} \vdash_I \forall y \neg_R \forall x.\neg_R \neg_R \neg_R A(x,y) \end{array}$$

Luego

$$\dfrac{\dfrac{\dfrac{\Pi^{\neg\neg}}{\Gamma^{\neg\neg} \vdash_I \forall y \neg_R \forall x.\neg_R A(x,y_0)^{\neg\neg}}\,\mathrm{E}\forall \qquad \dfrac{\Pi_\forall}{\Gamma^{\neg\neg} \vdash_I \forall x.\neg_R A(x,y_0)^{\neg\neg}}}{\Gamma^{\neg\neg} \vdash_I \neg_R \forall x.\neg_R A(x,y_0)^{\neg\neg}}\,\mathrm{E}\to}{\Gamma^{\neg\neg} \vdash_I \exists x.A(x,y_0)}\,\mathrm{I}\forall}{\Gamma^{\neg\neg} \vdash_I \forall y \exists x.A(x,y)}$$

donde

$$\mathrm{I}\neg_R\neg_R\neg_R\,\dfrac{\dfrac{}{\Gamma^{\neg\neg}, \neg_R A(x,y_0) \vdash_I \neg_R\neg_R\neg_R A(x,y_0)} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma^{\neg\neg}, A(x,y_0) \vdash_I A(x,y_0)}\,\mathrm{Ax}}{\Gamma^{\neg\neg}, A(x,y_0) \vdash_I R = \exists x.A(x,y_0)}\,\mathrm{I}\exists}{\Gamma^{\neg\neg} \vdash_I \neg_R A(x,y_0)}\,\mathrm{I}\to}{\dfrac{\Gamma^{\neg\neg} \vdash_I \neg_R\neg_R\neg_R A(x,y_0)}{\Gamma^{\neg\neg} \vdash_I \forall x.\neg_R A(x,y_0)^{\neg\neg}}\,\mathrm{I}\forall = \Pi_\forall}\,\mathrm{cut}$$

□

Corolario 1 (Instanciación de $\forall$)**.** El Teorema 11 nos permite realizar la instanciación de las variables del $\forall$ eliminandolo e instanciando con el término que querramos. De esa forma, la demostración final es sobre un $\exists$, requerido para poder hacer la extracción sobre la demostración normalizada. Por ejemplo,

$$\dfrac{\dfrac{(11)}{\Gamma^{\neg\neg} \vdash_I \forall y \exists x.A(x,y)}}{\Gamma^{\neg\neg} \vdash_I \exists x.A(x,t)}\,\mathrm{E}\forall$$

Formulas no atómicas

Hasta ahora usamos la traducción de Friedman para traducir las demostraciones de una fórmula de clásica a intuicionista, manteniendo esa fórmula, siempre y cuando su subfórmula Σ^0_0 sea **atómica**. Pero queremos generalizarlo a fórmulas como $\forall y \exists x.\varphi(x,y)$ donde φ no sea atómica, por ejemplo $A(x) \wedge B(y)$. Para ello, la única diferencia es en el uso de cut. Para fórmulas atómicas, tenemos

$$\mathrm{I}\neg_R\neg_R\neg_R\,\dfrac{\dfrac{}{\Gamma^{\neg\neg}, \neg_R A \vdash_I \neg_R\neg_R\neg_R A} \qquad \begin{array}{c}\vdots\\ \Gamma^{\neg\neg} \vdash_I \neg_R A\end{array}}{\Gamma^{\neg\neg} \vdash_I \neg_R A^{\neg\neg} = \neg_R\neg_R\neg_R A^{\neg\neg}}\,\mathrm{cut}$$

Que en donde aprovechamos que la traducción de fórmulas atómicas es $\neg_R A^{\neg\neg} = \neg_R\neg_R\neg_R A^{\neg\neg}$ y podemos llevarla a $\neg_R A$ mediante la eliminación de la triple negación. Pero esto no es así para fórmulas que no sean atómicas. Para ello, enunciamos el Lema 5, el cual podemos usar para demostrar la traducción en el Teorema 12.

Lema 3 (Congruencia de $\neg_R\neg_R$)**.** Si $A \vdash_I A'$, luego $\neg\neg A \vdash_I \neg\neg A'$.

Lema 4 (Distributividad del $\neg_R$ sobre $\wedge$)**.** $\neg_R A \vee \neg_R B \vdash_I \neg_R(A \wedge B)$

Lema 5 (Introducción de $\neg_R$)**.** Para algunas fórmulas A, vale $\neg_R A \vdash_I \neg_R A^{\neg\neg}$ y lo notamos con la regla admisible $\mathrm{I}(\neg_R^{\neg\neg})$.

No vale siempre, ya que en ese caso podríamos usar la traducción de Friedman para todas las fórmulas. Lo demostramos para las fórmulas descritas por la siguiente gramática (conjunciones y fórmulas atómicas)

$$A, B ::= \bot \mid \top \mid p(t_1, \ldots, t_n) \mid A \wedge B$$

Demostración. La demostración se hace por inducción estructural en la fórmula.

- $\bot, \top$ son triviales. Predicados con $\mathrm{I}\neg_R\neg_R\neg_R$.
- $\neg, \vee, \to, \exists, \forall$ no están demostradas. Debería ser posible para algunas, pero no es claro.
- $\wedge$ es cierta para sub-fórmulas que cumplan con la hipótesis inductiva. Tiene algunos trucos.

Veamos esquemáticamente la demostración del $\wedge$. En la Figura 5.5 se puede ver el esquema en deducción natural.

- Debemos probar $\neg_R(A \wedge B) \vdash_I \neg_R(A \wedge B)^{\neg\neg}$
- Intuitivamente, queremos llevarlo a $\neg_R(A \wedge B) \vdash_I \neg_R A^{\neg\neg} \vee \neg_R B^{\neg\neg}$. Pero esta demostración requiere el uso de $\mathrm{E}\neg\neg$ para razonar por el absurdo, que no es cierto para lógica intuicionista (la demostración de esta equivalencia de De Morgan es clásica).
- Pero podemos usar un truco para razonar por el absurdo.
  - Tenemos que $\neg_R(A \wedge B)^{\neg\neg}$ es siempre equivalente a $\neg_R\neg_R(\neg_R(A \wedge B)^{\neg\neg})$ por eliminación de triple negación.
  - Podemos usar dos lemas auxiliares: $\neg_R A^{\neg\neg} \vee \neg_R B^{\neg\neg} \vdash_I \neg_R(A \wedge B)^{\neg\neg}$ y la congruencia de la doble negación, que al ser doble es covariante: $A \vdash_I A' \Rightarrow \neg_R\neg_R A \vdash_I \neg_R\neg_R A'$ para demostrar

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

- Esto nos permite llevar $\neg_R(A \wedge B) \vdash_I \neg_R(A \wedge B)^{\neg\neg}$ a

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

que se puede demostrar por el absurdo de forma análoga a la demostración clásica bien conocida.

□

Teorema 12 (Traducción de Friedman para fórmulas Σ^0_1 en general)**.** Sea Π una demostración clásica de $\forall y_1 \dots \forall y_n.\exists x.\varphi(x, y_1, \dots, y_n)$, y $\varphi(x, y_1, \dots, y_n)$ una fórmula no atómica. Si tenemos

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

podemos generar una demostración intuicionista de la misma fórmula

$$\Gamma^{\neg\neg} \vdash_I \forall y_1 \dots \forall y_n.\exists x.\varphi(x, y_1, \dots, y_n).$$

Demostración. Al igual que el Teorema 11 lo demostramos para un solo $\forall$. La demostración es análoga con la diferencia del uso del Lema 5: $\mathrm{I}(\neg_R^{\neg\neg})$. En lugar de tener

$$\mathrm{I}\neg_R\neg_R\neg_R \dfrac{\dfrac{}{\Gamma^{\neg\neg}, \neg_R A \vdash_I \neg_R\neg_R\neg_R A} \qquad \begin{array}{c}\vdots\\ \Gamma^{\neg\neg} \vdash_I \neg_R A\end{array}}{\Gamma^{\neg\neg} \vdash_I \neg_R A^{\neg\neg} = \neg_R\neg_R\neg_R A^{\neg\neg}}\,\mathrm{cut}$$

tenemos

$$\mathrm{I}(\neg_R^{\neg\neg}) \dfrac{\dfrac{}{\Gamma^{\neg\neg}, \neg_R\varphi \vdash_I \neg_R\varphi^{\neg\neg}} \qquad \begin{array}{c}\vdots\\ \Gamma^{\neg\neg} \vdash_I \neg_R\varphi\end{array}}{\Gamma^{\neg\neg} \vdash_I \neg_R\varphi^{\neg\neg}}\,\mathrm{cut}$$

□

5.4.4. Traducción de demostraciones

Ya vimos como podemos usar la traducción de Friedman para, dada una traducción de la demostración, usarla para demostrar la misma fórmula. Pero aún no ahondamos en un detalle importante. En el Teorema 9 se introduce la necesidad de extender la traducción de doble negación relativizada de fórmulas a demostraciones, para poder traducir una demostración clásica a intuicionista. En esta sección lo vemos más en detalle.

La conversión se efectúa por inducción estructural en la demostración. Para cada regla de inferencia que demuestra A, se genera una demostración a partir de ella para demostrar $A^{\neg\neg}$. La estrategia para hacerlo es similar para todas: usar la hipótesis inductiva para convertir las sub-demostraciones, y usarlas para generar la nueva demostración. Pero hay algunas que requieren un truco. Solo mostramos las interesantes.

- I$\wedge$ (Lema 6), E$\wedge_1$, E$\wedge_2$, I$\to$, E$\to$, I$\vee_1$, I$\vee_2$, I$\forall$, E$\forall$, I$\neg$, E$\neg$, I$\top$, Ax son todas similares entre sí, por lo que solo mostramos una.
- I$\exists$ (Lema 7) es una regla simple pero más interesante que las anteriores, por la traducción de $\exists$.
- LEM (Lema 8) es sumamente interesante, ya que se encuentra en el corazón de la traducción al ser la parte clave: ¿cómo traducimos el principio de razonamiento clásico que lo separa de la lógica intuicionista?
- E$\bot$ (Lema 9) se prueba como lema por inducción estructural en la fórmula a demostrar.

- E$\vee$ (Lema 11) y E$\exists$ son análogos y requieren un truco: usar la eliminación de la doble negación. Si bien al ser un principio de razonamiento clásico no vale para lógica intuicionista (por ser equivalente a LEM), lo que si vale es la eliminación de la doble negación relativizada: E$\neg_R\neg_R$ (Lema 10).

Lema 6 (Traducción de I$\wedge$)**.** Dada una aparición de la regla I$\wedge$,

$$\dfrac{\begin{array}{cc}\Pi_A & \Pi_B\\ \Gamma \vdash_I A & \Gamma \vdash_I B\end{array}}{\Gamma \vdash_I A \wedge B}\,\mathrm{I}\wedge$$

es posible traducirla generando una demostración de $(A \wedge B)^{\neg\neg} = A^{\neg\neg} \wedge B^{\neg\neg}$.

Demostración. Por hipótesis inductiva, tenemos que

- $\Pi_A^{\neg\neg} \rhd \Gamma^{\neg\neg} \vdash_I A^{\neg\neg}$ y
- $\Pi_B^{\neg\neg} \rhd \Gamma^{\neg\neg} \vdash_I B^{\neg\neg}$

Luego, podemos generar una demostración de $A^{\neg\neg} \wedge B^{\neg\neg}$

$$\dfrac{\begin{array}{cc}\Pi_A^{\neg\neg} & \Pi_B^{\neg\neg}\\ \Gamma^{\neg\neg} \vdash_I A^{\neg\neg} & \Gamma^{\neg\neg} \vdash_I B^{\neg\neg}\end{array}}{\Gamma^{\neg\neg} \vdash_I A^{\neg\neg} \wedge B^{\neg\neg}}\,\mathrm{I}\wedge$$

□

Lema 7 (Traducción de I$\exists$)**.** Dada una aparición de la regla I$\exists$,

$$\dfrac{\begin{array}{c}\Pi\\ \Gamma \vdash A\{x := t\}\end{array}}{\Gamma \vdash \exists x.A}\,\mathrm{I}\exists$$

es posible traducirla generando una demostración de $\exists x.A^{\neg\neg} = \neg_R\forall x.\neg_R A^{\neg\neg}$.

Demostración. Por hipótesis inductiva, tenemos que $\Pi^{\neg\neg} \rhd \Gamma^{\neg\neg} \vdash_I (A\{x := t\})^{\neg\neg}$
Luego, podemos generar una demostración de $\neg_R\forall x.\neg_R A^{\neg\neg}$

$$\dfrac{\dfrac{\dfrac{}{\Gamma_1 \vdash_I \neg_R\forall x A^{\neg\neg}}\,\mathrm{Ax}}{\Gamma_1 \vdash_I \neg_R A\{x := t\}^{\neg\neg}}\,\mathrm{E}\forall \qquad \begin{array}{c}\Pi^{\neg\neg}\\ \Gamma_1 \vdash_I A\{x := t\}^{\neg\neg}\end{array}}{\dfrac{\Gamma_1 = \Gamma^{\neg\neg}, \forall x.\neg_R A^{\neg\neg} \vdash_I R}{\Gamma^{\neg\neg} \vdash_I \neg_R\forall x.\neg_R A^{\neg\neg}}\,\mathrm{I}\to}\,\mathrm{E}\to$$

□

Lema 8 (Traducción de LEM)**.** Dada una aparición de la regla LEM,

$$\dfrac{}{\Gamma \vdash A \vee \neg A}\,\mathrm{LEM}$$

es posible traducirla generando una demostración de

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

Demostración. Como no hay HI, podemos demostrarlo para cualquier contexto Γ.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_1 \vdash_I \neg_R A^{\neg\neg} \wedge \neg_R \neg_R A^{\neg\neg}}\,\mathrm{Ax}}{\Gamma_1 \vdash_I \neg_R \neg_R A^{\neg\neg}}\,\mathrm{E}\wedge_2 \quad \dfrac{\dfrac{}{\Gamma_1 \vdash_I \neg_R A^{\neg\neg} \wedge \neg_R \neg_R A^{\neg\neg}}\,\mathrm{Ax}}{\Gamma_1 \vdash_I \neg_R A^{\neg\neg}}\,\mathrm{E}\wedge_1}{\Gamma_1 \vdash_I \neg_R A^{\neg\neg} \wedge \neg_R \neg_R A^{\neg\neg}}\,\mathrm{E}\to}{\Gamma_1 = \Gamma, \neg_R A^{\neg\neg} \wedge \neg_R \neg_R A^{\neg\neg} \vdash_I R}\,\mathrm{I}\to}{\Gamma \vdash_I \neg_R(\neg_R A^{\neg\neg} \wedge \neg_R \neg_R A^{\neg\neg})}\,\mathrm{I}\to$$

□

Lema 9 (Traducción de E⊥)**.** Dada una aparición de la regla E⊥,

$$\dfrac{\begin{array}{c}\Pi_\bot \\ \Gamma \vdash \bot\end{array}}{\Gamma \vdash \varphi}\,\mathrm{E}\bot$$

es posible generar una demostración de $\varphi^{\neg\neg}$ a partir de $\bot^{\neg\neg} = R$.

Demostración. Por hipótesis inductiva (de inducción estructural sobre la demostración), tenemos que

$$\begin{array}{c}\Pi_\bot^{\neg\neg} \rhd \Gamma^{\neg\neg} \vdash_I \bot^{\neg\neg} \\ \| \\ \Pi_R \rhd \Gamma^{\neg\neg} \vdash_I R\end{array}$$

Pero no es posible demostrar de forma directa $\varphi^{\neg\neg}$ a partir de R. Lo hacemos por inducción estructural en φ. Todos los casos son parecidos. Por ejemplo, veamos un caso inductivo y uno base.

- Dada una conjunción $A \wedge B$, su traducción es $A^{\neg\neg} \wedge B^{\neg\neg}$. Por HI (de inducción estructural sobre la fórmula) a partir de Π_R podemos probar $A^{\neg\neg}$ al igual que $B^{\neg\neg}$. Luego,

$$\dfrac{\begin{array}{cc}\text{(HI)} & \text{(HI)} \\ \Gamma^{\neg\neg} \vdash_I B^{\neg\neg} & \Gamma^{\neg\neg} \vdash_I A^{\neg\neg}\end{array}}{\Gamma^{\neg\neg} \vdash_I A^{\neg\neg} \wedge B^{\neg\neg}}\,\mathrm{I}\wedge$$

- Dada una disyunción $A \vee B$, su traducción es $\neg_R(\neg_R A^{\neg\neg} \wedge \neg_R B^{\neg\neg})$. Luego, podemos demostrarlo sin usar la HI.

$$\dfrac{\begin{array}{c}\Pi_R \\ \Gamma^{\neg\neg}, \neg_R A^{\neg\neg} \wedge \neg_R B^{\neg\neg} \vdash_I R\end{array}}{\Gamma^{\neg\neg} \vdash_I \neg_R(\neg_R A^{\neg\neg} \wedge \neg_R B^{\neg\neg})}\,\mathrm{I}\to$$

El resto de los casos son análogos. □

Lema 10 (Eliminación de doble negación relativizada (E$\neg_R\neg_R$))**.** (TODO: Enunciar y demostrar)

Lema 11 (Traducción de E∨)**.** (TODO: Enunciar y demostrar)

5.5. Normalización (o reducción)

Repasemos en dónde estamos parados. Queremos extraer un testigo de la demostración de un existencial (i.e extraer de una demostración de $\exists x.p(x)$ a un t tal que $p(t)$). Partimos de una demostración escrita en el lenguaje de alto nivel PPA, que se certifica a una demostración en deducción natural *clásica* (que tiene el problema para la reducción que no es constructiva). Mediante la traducción de Friedman, para cierto tipo de fórmulas (Π^0_2), podemos convertir la demostración a *intuicionista*. Ahora, queremos extraer el testigo a partir de ella. Eso lo podemos lograr **normalizando** la demostración. ¿De qué trata?

Intuitivamente, la estrategia que empleamos consiste en evitar *desvíos superfluos* en una demostración, sucesivamente simplificándolos hasta que queda una demostración en forma normal. Por ejemplo, en la siguiente demostración se prueba $A \to A$ usando $(A \to A) \wedge (B \to B)$ y demostrándo ambos por separado. Pero se puede demostrar de forma más directa, insertando directo la demostración de $A \to A$ y eliminado el desvío por el $\wedge$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathrm{Ax}}{\vdash A \to A}\,\mathrm{I}\to \quad \dfrac{\dfrac{}{B \vdash B}\,\mathrm{Ax}}{\vdash B \to B}\,\mathrm{I}\to}{\vdash (A \to A) \wedge (B \to B)}\,\mathrm{I}\wedge}{\vdash A \to A}\,\mathrm{E}\wedge_1 \quad \rightsquigarrow \quad \dfrac{\dfrac{}{A \vdash A}\,\mathrm{Ax}}{\vdash A \to A}\,\mathrm{I}\to$$

Fig. 5.6: Ejemplo de desvío y su normalización

Todos los desvíos que normalizamos se ven de esta forma: una **eliminación** seguida inmediatamente de su **introducción** correspondiente. Por ejemplo, E$\wedge_1$ seguida de I$\wedge$.

Este proceso es análogo a las reducciones de cálculo λ. Más aún, existe un isomorfismo entre demostraciones en deducción natural y términos de cálculo λ: El isomorfismo Curry-Howard [SU10]. Con él, la normalización de demostraciones es el isomorfismo de las reducciones en cálculo λ, su semántica. Por ejemplo, el isomorfismo nos permite pensar en una conjunción como una tupla, y las eliminaciones como proyecciones. Luego, podemos ver cómo la regla de normalización de la conjunción es isomorfa a la regla de reducción de las proyecciones.

$$\pi_1(\langle M_1, M_2\rangle) \rightsquigarrow M_1$$
$$\pi_2(\langle M_1, M_2\rangle) \rightsquigarrow M_2$$

$$\dfrac{\dfrac{\Pi_1 \qquad \Pi_2}{\Gamma \vdash A_1 \qquad \Gamma \vdash A_2}\,\mathrm{I}\wedge}{\Gamma \vdash A_1 \wedge A_2}\,\mathrm{E}\wedge_i \quad \rightsquigarrow \quad \begin{array}{c}\Pi_i\\ \Gamma \vdash A_i\end{array}$$

Fig. 5.7: Relación entre conjunciones y tuplas

De acá en adelante presentamos las reducciones directamente en deducción natural, dado que es lo implementado en PPA. Usamos de forma intercambiable *reducción* y *normalización*, pues en el fondo, son lo mismo.

Obs. 5. Es interesante notar que en las reducciones mencionadas en esta sección, no se explicita ni $\vdash_I$ ni $\vdash_C$ a diferencia de la traducción de Friedman. Esto es porque la normalización se puede ejecutar en ambos casos, con la diferencia de que si lo hacemos para una demostración de lógica clásica que use LEM, se traba cuando llega ahí y su forma normal no es muy útil.

5.5.1. Sustituciones

No todas las reglas de reducción son igual de sencillas que $\wedge$. Veamos el caso de la implicación. Una eliminación seguida de una introducción tiene la siguiente forma.

$$\dfrac{\dfrac{\begin{matrix}\Pi_B\\ \Gamma, h : A \vdash B\end{matrix}}{\Gamma \vdash A \to B}\,\mathrm{I}{\to_h} \qquad \begin{matrix}\Pi_A\\ \Gamma \vdash A\end{matrix}}{\Gamma \vdash B}\,\mathrm{E}{\to}$$

Para eliminar el desvío, uno podría estar tentado a hacer directamente $\Pi_B \rhd \Gamma \vdash B$ pero ¡**no sería correcto**! La demostración Π_B requiere la hipótesis $h : A$. Lo correcto sería usar Π_B, pero reemplazando todas las ocurrencias de la hipótesis h por la demostración Π_A. A continuación introducimos esa noción.

Def. 17 (Hipótesis libres)**.** Una hipótesis ocurre libre en una demostración si se cita sin ser definida. Las reglas que etiquetan y agregan hipótesis al contexto son las que las ligan (i.e. las mencionadas en Subsección 2.3.1 Hipótesis etiquetadas: Ax_h, $\mathrm{I}{\to_h}$, $\mathrm{I}{\neg_h}$, $\mathrm{E}{\vee_h}$, $\mathrm{E}{\exists_h}$)

Def. 18 (Hipótesis citadas por una demostración)**.** Definimos el conjunto de hipótesis citadas por una demostración $\mathrm{hyps}(\Pi)$ como todas las hipótesis ligadas y libres que aparecen en ella.

Def. 19 (Sustitución de hipótesis)**.** Notamos como $\Pi\{h := \Pi'\}$ a la sustitución sin capturas de todas las ocurrencias libres de una hipótesis h por una demostración Σ en otra demostración Π. Una *captura* ocurriría si en Π se liga una hipótesis $h_2 \neq h$ tal que $h_2 \in \mathrm{hyps}(\Sigma)$, se cite en Σ.

Para evitar la captura, al igual que en la sustitución de variables, no podemos renombrar en Σ (porque la hipótesis está "libre"), sino que la reemplazamos por una hipótesis fresca en donde se liga la que genera el conflicto, en la sub-demostración de Π.

Además, para la reducción del $\exists$ y $\forall$, necesitaremos extender la sustitución usual de variables (Def. 8) por términos a demostraciones. La implementación es análoga, evitando capturas y haciéndolo en una pasada de forma lineal.

Def. 20 (Sustitución de variables en demostraciones)**.** Notamos como $\Pi\{x := t\}$ a la sustitución sin capturas de todas las ocurrencias libres de una variable x por un término t en todas las partes de una demostración Π. Incluyendo los contextos.

(DUDA: Hace falta definirlo más?)

(DUDA: Pensamiento: Si no tuvieramos etiquetas, esta sustitución sería más fácil, no? Porque en lugar de reemplazar por ocurrencias de la etiqueta, reemplazas por veces que citas en un axioma una *fórmula*, entonces si lo estás capturando te da igual, total es la misma fórmula. O se podrá romper?)

5.5.2. Algoritmo de reducción

A partir de todas las reglas de reducción (Figura 5.8), dado que son *pasos* que acercan la demostración sucesivamente a su versión normalizada, podemos implementarlo de forma análoga a DNF (Sección 4.3.2) como la clausura reflexiva transitiva de la reducción de un paso (aplicarla 0 o más veces hasta que esté en forma normal). Al igual que DNF, también necesitaremos reglas de congruencia: si no hay una eliminación de una introducción para simplificar, se intentan de reducir recursivamente las sub-demostraciones.

En una primera implementación las sub-demostraciones las reducíamos en un paso, de izquierda a derecha. Por ejemplo, si teníamos una introducción de una conjunción, reducíamos de a un paso a la vez $A \rightsquigarrow A_1 \rightsquigarrow A_2 \rightsquigarrow \ldots \rightsquigarrow A^*$ hasta llegar a A^* irreducible. Luego, lo mismo para B.

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

Pero esto resultó demasiado lento, dado que las demostraciones que reducimos son muy grandes (pues son generadas automáticamente), y si por ejemplo la sub-demostración que había que reducir estaba muy anidada, había que recorrerla toda para efectuar cada paso.

$$\dfrac{\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\, \mathrm{I}\wedge}{\vdots}$$
$$\Pi$$

Además, las demostraciones eran de mayor profundidad por una mayor cantidad de iteraciones del algoritmo, lo que hacía que realizar sustituciones también sea costoso (pues hay que recorrer el árbol entero para ver las hipótesis citadas y realizar la sustitución).

Para solucionar este problema, implementamos una reducción en muchos pasos. En la literatura se pueden encontrar muchas *estrategias de reducción* alternativas, que se clasifican en si reducen en un paso o muchos para cada iteración de la clausura. Dentro de las de muchos, la que implementamos fue **Gross-Knuth**, que reduce en muchos pasos todos los sub-términos posibles al mismo tiempo. Aplicado a demostraciones, quiere decir que en un único paso de reducción, al mismo tiempo reduciríamos $A \wedge B \rightsquigarrow A^* \wedge B^*$. Esto hace que la convergencia sea mucho más rápida.

(DUDA: Probablemente falta rigurosidad en esta sección.)

5.5.3. Limitaciones

Implementamos una reducción sencilla, que solamente normaliza eliminaciones de introducciones de la misma regla. Pero hay otros patrones que dejamos afuera, para los cuales no llegamos a una forma normal. Entonces no siempre podremos extraer un testigo. Por ejemplo, en Figura 5.9 Ejemplo de demostración no normalizada, se puede observar una demostración sencilla que usa **`cases`**. Pero al certificarla, traducirla y reducirla, no queda en una forma normal. Se repite dos veces I$\exists$, cuando se podría mover hacia la raíz del árbol y evitar repetirlo en cada rama del E$\vee$. Esto hace que al intentar de extraer un testigo, el programa reporte una falla al no poder normalizar la demostración. Para soportar estos casos es necesario sofisticar la reducción, agregando otro tipo de reglas, que quedó fuera del alcance del trabajo.

(a) Programa de PPA

```
1  axiom ax_1: p(k) | q(k)
2  axiom ax_2: p(k) -> r(k)
3  axiom ax_3: q(k) -> r(k)
4
5  theorem t: exists Y . r(Y)
6  proof
7     take Y := k
8     cases by ax_1
9        case p(k)
10          hence r(k) by ax_2
11
12       case q(k)
13          hence r(k) by ax_3
14    end
15 end
```

(b) Demostración traducida y reducida

$$\dfrac{\dfrac{}{\Gamma \vdash_I p(k) \vee q(k)}\,\mathrm{Ax} \qquad \begin{matrix}\Pi_L & \Pi_R \\ \Gamma, p(k) \vdash_I \exists y.r(y) & \Gamma, q(k) \vdash_I \exists y.r(y)\end{matrix}}{\Gamma \vdash_I \exists y.r(y)}\,\mathrm{E}\vee$$

con Π_L definido de la siguiente forma, y Π_R simétrico.

$$\Pi_L = \dfrac{\dfrac{}{\Gamma, p(k) \vdash_I p(k) \to r(k)}\,\mathrm{Ax} \quad \dfrac{}{\Gamma, p(k) \vdash_I p(k)}\,\mathrm{Ax}}{\dfrac{\Gamma, p(k) \vdash_I r(k)}{\Gamma, p(k) \vdash_I \exists y.r(y)}\,\mathrm{I}\exists}$$

(c) Demostración en forma normal

$$\dfrac{\dfrac{}{\Gamma \vdash_I p(k) \vee q(k)}\,\mathrm{Ax} \qquad \begin{matrix}\Pi_L & \Pi_R \\ \Gamma, p(k) \vdash_I r(y) & \Gamma, q(k) \vdash_I r(k)\end{matrix}}{\dfrac{\Gamma \vdash_I r(k)}{\Gamma \vdash_I \exists y.r(y)}\,\mathrm{I}\exists}\,\mathrm{E}\vee$$

con Π_L y Π_R análogas al caso anterior, pero sin I$\exists$.

Fig. 5.9: Ejemplo de demostración no normalizada

5.6. Manteniendo el contexto

Problema con normalización: axiomas, hay que traducirlos para que la traducción de Friedman funcione. Solución? Dejar los axiomas originales y demostrar su traducción. No funciona siempre.

Lema 12 (Introducción de la traducción $\neg\neg$)**.** Se reduce a transintro

(TODO: Enunciar y demostrar)

5.7. Otros métodos de extracción

(TODO: Hablar sobre y citar classical realizability, no tengo ni idea.)

Buena intro acá https://www.degruyter.com/document/doi/10.1515/9783110324921.11/html?lang=en

In the past years, many computational interpretations of Classical Arithmetic havebeen put forward. Under a first classification, they fall into two large categories:directandindirectinterpretations. Among the indirect interpretations one findsthe negative translations followed either by Dialectica interpretations [13], [30](see e.g. Kohlenbach [19]) or by intuitionistic realizability interpretations com-bined with Friedman's translation [13] (see e.g. Berger and Schwichtenberg [10]).Among the direct interpretations, there are different versions of Classical Realiz-ability (Krivine's [22] and Avigad's [6]), there is Coquand game semantics [11],

$$\dfrac{\dfrac{\Pi_1}{\neg_R(A\wedge B)\vdash_I \neg_R\neg_R\neg_R(A\wedge B)^{\neg\neg}} \qquad \dfrac{}{\neg_R\neg_R\neg_R(A\wedge B)^{\neg\neg}\vdash_I \neg_R(A\wedge B)^{\neg\neg}}\,\mathrm{E}\neg_R\neg_R\neg_R}{\neg_R(A\wedge B)\vdash_I \neg_R(A\wedge B)^{\neg\neg}}\,\mathrm{cut}$$

Donde,

$$\Pi_1 = \dfrac{\dfrac{\dfrac{}{\neg_R A^{\neg\neg}\vee\neg_R B^{\neg\neg}\vdash_I \neg_R(A\wedge B)^{\neg\neg}}\,(\text{Lema 4})}{\neg_R\neg_R(\neg_R A^{\neg\neg}\vee\neg_R B^{\neg\neg})\vdash_I \neg_R\neg_R\neg_R(A\wedge B)^{\neg\neg}}\,(\text{Lema 3}) \qquad \begin{array}{c}\textit{(demostración por el absurdo)}\\ \neg_R(A\wedge B)\vdash_I \neg_R\neg_R(\neg_R A^{\neg\neg}\vee\neg_R B^{\neg\neg})\end{array}}{\neg_R(A\wedge B)\vdash_I \neg_R\neg_R\neg_R(A\wedge B)^{\neg\neg}}\,\mathrm{cut}$$

Fig. 5.5: Esquema de demostración de introducción de $\neg_R$ para el caso de $\wedge$, ver Lema 5

.

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ \Gamma \vdash A_1\end{array} \quad \begin{array}{c}\Pi_2\\ \Gamma \vdash A_2\end{array}}{\Gamma \vdash A_1 \wedge A_2}\,\mathrm{I}\wedge}{\Gamma \vdash A_i}\,\mathrm{E}\wedge_i \quad \rightsquigarrow \quad \begin{array}{c}\Pi_i\\ \Gamma \vdash A_i\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\Pi_B\\ \Gamma, h : A \vdash B\end{array}}{\Gamma \vdash A \to B}\,\mathrm{I}\to_h \quad \begin{array}{c}\Pi_A\\ \Gamma \vdash A\end{array}}{\Gamma \vdash B}\,\mathrm{E}\to \quad \rightsquigarrow \quad \left(\begin{array}{c}\Pi_B\\ \Gamma, h : A \vdash B\end{array}\right)\{h := \Pi_A\}$$

(DUDA: Por qué no directamente así? $\begin{array}{c}\Pi_B\{h := \Pi_A\}\\ \Gamma \vdash B\end{array}$)

$$\dfrac{\dfrac{\begin{array}{c}\Pi_{A_i}\\ \Gamma \vdash A_i\end{array}}{\Gamma \vdash A_1 \vee A_2}\,\mathrm{I}\vee_i \quad \begin{array}{c}\Pi_1\\ \Gamma, h_1 : A_1 \vdash B\end{array} \quad \begin{array}{c}\Pi_2\\ \Gamma, h_2 : A_2 \vdash B\end{array}}{\Gamma \vdash B}\,\mathrm{E}\vee$$
$$\rightsquigarrow \quad \left(\begin{array}{c}\Pi_i\\ \Gamma, h_i : A_i \vdash B\end{array}\right)\{h_i := \Pi_{A_i}\}$$

$$\dfrac{\dfrac{\begin{array}{c}\Pi_\bot\\ \Gamma, h : A \vdash \bot\end{array}}{\Gamma \vdash \neg A}\,\mathrm{I}\neg \quad \begin{array}{c}\Pi_A\\ \Gamma \vdash A\end{array}}{\Gamma \vdash \bot}\,\mathrm{E}\neg \quad \rightsquigarrow \quad \left(\begin{array}{c}\Pi_\bot\\ \Gamma, h : A \vdash \bot\end{array}\right)\{h := \Pi_A\}$$

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \Gamma \vdash A\end{array}}{\Gamma \vdash \forall.xA}\,\mathrm{I}\forall}{\Gamma \vdash A\{x := t\}}\,\mathrm{E}\forall \quad \rightsquigarrow \quad \left(\begin{array}{c}\Pi\\ \Gamma \vdash A\end{array}\right)\{x := t\}$$

$$\dfrac{\dfrac{\begin{array}{c}\Pi_A\\ \Gamma \vdash A\{x := t\}\end{array}}{\Gamma \vdash \exists x.A}\,\mathrm{I}\exists \quad \begin{array}{c}\Pi_B\\ \Gamma, h : A \vdash B\end{array}}{\Gamma \vdash B} \quad \rightsquigarrow \quad \left(\left(\begin{array}{c}\Pi_B\\ \Gamma, h : A \vdash B\end{array}\right)\{x := t\}\right)\{h := \Pi_A\}$$

Fig. 5.8: Reglas de reducción

6. LA HERRAMIENTA PPA

7. CONCLUSIONES

BIBLIOGRAFíA

[AF98] Jeremy Avigad y Solomon Feferman. «Godel's Functional Interpretation». En: *Handbook of proof theory*. Ed. por Samuel R. Buss. Elsevier, 1998, págs. 337-405. URL: https://philpapers.org/rec/FEFOFD.

[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.

[SU10] Morten Sørensen y Paweł Urzyczyn. «Lectures on the Curry-Howard Isomorphism». En: *Studies in Logic and the Foundations of Mathematics* 149 (oct. de 2010). DOI: 10.1016/S0049-237X(06)80005-4. URL: https://disi.unitn.it/~bernardi/RSISE11/Papers/curry-howard.pdf.

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