Tesis de licenciatura

Manuel Panichelli

7 de octubre de 2024

Capítulo 1

Deducción natural

(TODO: cambiar el nombre)

Capítulo 2

Extracción de testigos de existenciales

2.1. Lógica clásica

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 1. 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 1, 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

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

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

2.1.1. 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)

2.2. Traducción de Friedman

2.2.1. 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. 1. (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 2. 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.

2.2.2. 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. 2. (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 3. 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, $\exists x.A$

$$\begin{aligned}
\Pi^{\neg\neg} \rhd \Gamma^{\neg\neg} &\vdash_I \neg_R \forall x.\neg_R \neg_R \neg_R A \\
&\iff \Gamma^{\neg\neg} \vdash_I \neg_R \forall x.\neg_R A && (1) \\
&= \Gamma^{\neg\neg} \vdash_I (\forall x.(A \to R)) \to R \\
&= \Gamma^{\neg\neg} \vdash_I (\forall x.(A \to \exists x.A)) \to \exists x.A && (R = \exists x A) \\
&\Rightarrow \Gamma^{\neg\neg} \vdash_I \exists x.A && (1)
\end{aligned}$$

□

Lema 1. $\neg_R \neg_R \neg_R A \iff \neg_R A$

Demostración. (TODO: En deducción natural) □

Obs. 1. $\vdash_I \forall x(A \to \exists x A)$

(TODO: IDem pero en ND, y también para $\forall$)
Puntos que falta abordar

- Como necesitamos reducir en ND, necesitamos la demo en ND. Escribirla en este caso.
- También queremos para Π^0_2, 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.

Bibliografía

[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.