

Tesis de licenciatura

Manuel Panichelli

6 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
```

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 racional

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.

□

2.2. LÓGICA INTUICIONISTA Y DEMOSTRACIÓN DE TESTIGOS DE EXISTENCIALES

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**). En cambio, si consideramos la fórmula

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

pensando 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.

2.2. Lógica intuicionista

Para solucionar estos problemas existe la lógica **intuicionista**, que se puede definir como la lógica clásica sin LEM. Al ser siempre constructiva, sirve para tener interpretaciones computacionales (como la *BHK*). En esta lógica, podemos reducir la prueba hacia una 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.

[\[Miq11\]](#)

[\[Sel92\]](#)

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](https://doi.org/10.2168/LMCS-7(2:2)2011). URL: [https : // doi . org / 10 . 2168 / LMCS - 7 \(2 : 2 \) 2011](https://doi.org/10.2168/LMCS-7(2:2)2011).
- [Sel92] Peter Selinger. «Friedman’s A-Translation». En: (1992). URL: [https : // www . mscs . dal . ca / ~ selinger / papers / papers / friedman . pdf](https://www.mscs.dal.ca/~selinger/papers/papers/friedman.pdf).