Unidad II: Lógica de Primer Orden

Teorías y Gödel

Clase 14 - Lógica para Ciencia de la Computación/Teoría de la Computación

Prof. Miguel Romero

Un problema fundamental:

¿Es φ consecuencia lógica de Σ?

Recordatorio:

Decimos que φ es **consecuencia lógica** de Σ, denotado por $\Sigma \vDash \varphi$, si para **toda** $\mathcal{L}$-estructura $\mathfrak{A}$ y asignación σ para $\mathfrak{A}$, se tiene que:

$$(\mathfrak{A}, \sigma) \vDash \Sigma \implies (\mathfrak{A}, \sigma) \vDash \varphi.$$

Recordatorio:

- $\Sigma \vDash \varphi \iff \Sigma \cup \{\neg\varphi\}$ es inconsistente.
- Si Σ es inconsistente, entonces $\Sigma \vDash \varphi$, para todo φ.
- Sea α una fórmula no satisfacible.

$$\Sigma \text{ es inconsistente} \iff \Sigma \vDash \alpha.$$

- φ es válida $\iff \varnothing \vDash \varphi$.

¿Es posible capturar la noción de consecuencia lógica de manera sintáctica?

Sistemas deductivos:

- Define la noción de demostración:

  φ puede ser demostrado a partir de Σ.

- Una demostración es un objeto finito.
- Un caso común:
  secuencia de fórmulas conectadas por reglas de inferencia fijas.

¿Es posible capturar consecuencia lógica con algún sistema deductivo?

Un sistema de Hilbert para LPO consta de los siguientes dos elementos:

- Axiomas básicos:
  Un conjunto finito de axiomas básicos.
  - Un axioma básico genera fórmulas válidas de cierta forma.

Ejemplos:

- $(\exists x\, \varphi) \leftrightarrow (\neg \forall x \neg \varphi)$, para cada fórmula φ.
- $(\forall x\, \varphi(x)) \rightarrow \varphi(t)$, para cada fórmula φ y cada término t.
- $\forall x\, (x = x)$.
- $\varphi \rightarrow (\psi \rightarrow \varphi)$, para cada fórmula φ y ψ.

Un sistema de Hilbert para LPO consta de los siguientes dos elementos:

- Reglas de inferencia:
  Un conjunto finito de reglas de inferencia.

  Cada regla de inferencia nos dice:
  "si tengo cierto conjunto de fórmulas, puedo derivar cierta fórmula nueva".

Ejemplos:

- Modus Ponens:

$$\frac{\varphi \to \psi \quad \varphi}{\psi}$$

Cada regla de inferencia debe ser **correcta**:
debe corresponder a una consecuencia lógica.

Dado: sistema de Hilbert fijo.

Definición:

Sea un conjunto de fórmulas Σ y una fórmula φ.
Una demostración de φ desde Σ, es una secuencia de fórmulas φ_1, φ_2, ..., φ_n tal que:

- Para cada $1 \leq i \leq n$:
  - $\varphi_i \in \Sigma$ o
  - φ_i es un axioma en el sistema o
  - φ_i se puede derivar aplicando alguna regla de inferencia a algunas de las fórmulas anteriores $\varphi_1, \ldots, \varphi_{i-1}$.
- $\varphi_n = \varphi$

Notación: Si existe tal demostración, escribimos $\Sigma \vdash \varphi$.

Todo sistema de Hilbert es correcto:

$$\Sigma \vdash \varphi \implies \Sigma \vDash \varphi.$$

Teorema (Completitud de Gödel)

Existe un sistema de Hilbert correcto y **completo**. Es decir, se cumple:

$$\Sigma \vdash \varphi \iff \Sigma \vDash \varphi.$$

"ser consecuencia lógica" y "ser demostrable" son lo mismo en LPO!

Teorema:

VAL es recursivamente enumerable.

Demostración:

Tenemos que φ es válida $\iff \varnothing \vDash \varphi$.

Por el teorema de completitud de Gödel: φ es válida $\iff \varnothing \vdash \varphi$.

Algoritmo para VAL:

Sobre entrada $\langle \varphi \rangle$:

1. Iterar sobre todas las secuencias finitas π de fórmulas.
   (en orden lexicográfico.)
2. Si π es una demostración de φ desde $\varnothing$, **aceptar**.

Observación: La misma idea demuestra que CONS está en RE.

Teorema de compacidad:

Un conjunto de oraciones Σ es satisfacible si y sólo si es finitamente satisfacible.

Demostración:

Basta demostrar: Σ no es satisfacible $\implies$ Σ no es finitamente satisfacible.

Si Σ no es satisfacible, entonces $\Sigma \vDash \alpha$, con α cualquier oración no satisfacible. (e.g. $\alpha = \exists x(\neg x = x)$.)

Por completitud de Gödel, existe demostración $\varphi_1, \ldots, \varphi_n$ de α desde Σ. (en particular, $\varphi_n = \alpha$.)

Sea $\Delta = \{\varphi_i \mid 1 \leq i \leq n \text{ y } \varphi_i \in \Sigma\}$. Notar que $\Delta \subseteq \Sigma$ es finito.

Tenemos que $\Delta \vdash \alpha$ y por correctitud $\Delta \vDash \alpha$. Sigue que Δ no es satisfacible.

Concluimos que Σ no es finitamente satisfacible.

Una teoría es un cuerpo de conocimiento sobre un tema.

- Debe estar libre de contradicciones.
- Debe ser cerrada con respecto a lo que se puede deducir de ella.

Definición:

Sea $\mathcal{L}$ un vocabulario. Una **teoría** es un conjunto Σ de $\mathcal{L}$-oraciones tal que:

- Σ es consistente (es decir, satisfacible).
- Σ es cerrado bajo consecuencia lógica:

$$\Sigma \vDash \varphi \implies \varphi \in \Sigma \qquad \text{para toda } \mathcal{L}\text{-oración } \varphi$$

¿Cómo podemos definir una teoría?

Dada una $\mathcal{L}$-estructura $\mathfrak{A}$, la teoría de $\mathfrak{A}$ se define como:

$$\mathrm{Th}(\mathfrak{A}) = \{\varphi \mid \varphi \text{ es una } \mathcal{L}\text{-oración tal que } \mathfrak{A} \vDash \varphi\}.$$

Proposición:

$\mathrm{Th}(\mathfrak{A})$ es una teoría, para toda $\mathcal{L}$-estructura $\mathfrak{A}$.

Demostración:

$\mathrm{Th}(\mathfrak{A})$ es consistente: $\mathfrak{A} \vDash \mathrm{Th}(\mathfrak{A})$.

$\mathrm{Th}(\mathfrak{A})$ es cerrada bajo consecuencia lógica: $\mathrm{Th}(\mathfrak{A}) \vDash \varphi \Rightarrow \mathfrak{A} \vDash \varphi \Rightarrow \varphi \in \mathrm{Th}(\mathfrak{A})$.

Tomemos el vocabulario $\mathcal{L} = \{0, 1, suc, +, \cdot, <\}$ y las estructuras:

$$\mathfrak{N} = (\mathbb{N}, 0^{\mathfrak{N}}, 1^{\mathfrak{N}}, suc^{\mathfrak{N}}, +^{\mathfrak{N}}, \cdot^{\mathfrak{N}}, <^{\mathfrak{N}})$$
$$\mathfrak{R} = (\mathbb{R}, 0^{\mathfrak{R}}, 1^{\mathfrak{R}}, suc^{\mathfrak{R}}, +^{\mathfrak{R}}, \cdot^{\mathfrak{R}}, <^{\mathfrak{R}})$$

Dos teorías fundamentales:

- Aritmética: $\mathrm{Th}(\mathfrak{N})$.
- Teoría de los números reales: $\mathrm{Th}(\mathfrak{R})$.

Sea Ax conjunto consistente de $\mathcal{L}$-oraciones. La teoría generada por Ax es:

$$\mathrm{Th}(\mathrm{Ax}) = \{\varphi \mid \varphi \text{ es una } \mathcal{L}\text{-oración tal que } \mathrm{Ax} \vDash \varphi\}.$$

Proposición:

Th(Ax) es una teoría, para todo conjunto consistente de $\mathcal{L}$-oraciones Ax.

Demostración:

Th(Ax) es consistente:

Ax es consistente $\Rightarrow$ existe $\mathfrak{A}$ tal que $\mathfrak{A} \vDash \mathrm{Ax}$.

Para todo $\varphi \in \mathrm{Th}(\mathrm{Ax})$, tenemos por definición $\mathrm{Ax} \vDash \varphi$, y luego $\mathfrak{A} \vDash \varphi$.

Obtenemos que $\mathfrak{A} \vDash \mathrm{Th}(\mathrm{Ax})$.

Th(Ax) es cerrada bajo consecuencia lógica:

Sea φ tal que $\mathrm{Th}(\mathrm{Ax}) \vDash \varphi$. Veamos que $\varphi \in \mathrm{Th}(\mathrm{Ax})$, es decir, $\mathrm{Ax} \vDash \varphi$.

Sea $\mathfrak{A}$ tal que $\mathfrak{A} \vDash \mathrm{Ax}$. Por el argumento de arriba, sabemos que $\mathfrak{A} \vDash \mathrm{Th}(\mathrm{Ax})$.

Por hipótesis, obtenemos que $\mathfrak{A} \vDash \varphi$.

La teoría generada por un conjunto axiomas: ejemplos

Sea $\mathcal{L} = \{e, \circ\}$ y Gr el siguiente conjunto de axiomas:

$$\forall x \forall y \forall z \left(x \circ (y \circ z) = (x \circ y) \circ z\right)$$
$$\forall x \left(x \circ e = x \wedge e \circ x = x\right)$$
$$\forall x \exists y \left(x \circ y = e \wedge y \circ x = e\right).$$

Podemos tomar Th(Gr), lo cual se conoce como la teoría de grupos.

¿Qué cumplen las estructuras $\mathfrak{A}$ que satisfacen Gr?

- $\circ$ es una operación asociativa.
- e es elemento neutro para $\circ$.
- todo elemento tiene un inverso con respecto a $\circ$.

La teoría generada por un conjunto axiomas: ejemplos

Sea $\mathcal{L} = \{e, \circ\}$ y Gr el siguiente conjunto de axiomas:

$$\forall x \forall y \forall z \left(x \circ (y \circ z) = (x \circ y) \circ z\right)$$
$$\forall x \left(x \circ e = x \wedge e \circ x = x\right)$$
$$\forall x \exists y \left(x \circ y = e \wedge y \circ x = e\right).$$

Podemos tomar Th(Gr), lo cual se conoce como la teoría de grupos.

¿Cuáles de las siguientes oraciones pertenece a Th(Gr)?

- $\forall z \left(\left(\forall x \left(x \circ z = x \wedge z \circ x = x\right)\right) \rightarrow z = e\right)$.
- $\forall x \forall y \left(x \circ y = y \circ x\right)$.

Definición:

Una teoría Σ sobre vocabulario $\mathcal{L}$ es **completa** si para cada $\mathcal{L}$-oración φ:

$$\varphi \in \Sigma \quad \text{o} \quad \neg\varphi \in \Sigma.$$

Equivalentemente:

Σ es completa si para cada $\mathcal{L}$-oración φ:

$$\Sigma \vDash \varphi \quad \text{o} \quad \Sigma \vDash \neg\varphi.$$

Proposición:

$\mathrm{Th}(\mathfrak{A})$ es completa, para toda $\mathcal{L}$-estructura $\mathfrak{A}$.

Demostración:

Para toda $\mathcal{L}$-oración φ se tiene $\mathfrak{A} \vDash \varphi$ o $\mathfrak{A} \nvDash \varphi$, es decir, $\mathfrak{A} \vDash \varphi$ o $\mathfrak{A} \vDash \neg\varphi$.
Luego $\varphi \in \mathrm{Th}(\mathfrak{A})$ o $\neg\varphi \in \mathrm{Th}(\mathfrak{A})$.

Corolario: $\mathrm{Th}(\mathfrak{N})$ y $\mathrm{Th}(\mathfrak{R})$ son completas.

¿Las teorías Th(Ax) generadas a partir de axiomas son siempre completas?

- ¿Funciona el argumento anterior para Th(Ax)?

Proposición:

Th(Gr) no es completa.

Demostración:

Sea la oración $\varphi = \forall x \forall y (x \circ y = y \circ x)$. Demostraremos que:

$$\varphi \notin \mathrm{Th}(\mathrm{Gr}) \text{ y } \neg\varphi \notin \mathrm{Th}(\mathrm{Gr}).$$

¿Qué significa esto en términos de grupos?

Demostración (continuación):

Veamos que $\neg\varphi \notin \mathrm{Th}(\mathrm{Gr})$, es decir, $Gr \not\models \neg\varphi$.

- Basta ver que existe un grupo conmutativo.

Sea $\mathfrak{A} = (\mathbb{Z}, e^{\mathfrak{A}}, \circ^{\mathfrak{A}})$, donde:

- $e^{\mathfrak{A}} = 0$.
- $a \circ^{\mathfrak{A}} b = a + b$.

Tenemos que $\mathfrak{A} \models Gr$ y $\mathfrak{A} \models \varphi$, es decir, $\mathfrak{A} \not\models \neg\varphi$.

- Concluimos que $Gr \not\models \neg\varphi$.

Demostración (continuación):

Veamos ahora que $\varphi \notin \mathrm{Th}(\mathrm{Gr})$, es decir, $Gr \not\models \varphi$.

- Basta ver que existe un grupo **no** conmutativo.

Sea $\mathfrak{B} = (B, e^{\mathfrak{B}}, \circ^{\mathfrak{B}})$, donde:

- $B = \{f : \{1,2,3\} \to \{1,2,3\} \mid f \text{ es biyectiva}\}$.
- $e^{\mathfrak{B}}$ es la función identidad.
- $\circ^{\mathfrak{B}}$ es la composición de funciones.

$$(f_1 \circ^{\mathfrak{B}} f_2)(x) = f_1(f_2(x))$$

¿Está bien definida $\circ^{\mathfrak{B}}$?

Demostración (continuación):

Tenemos que $\mathfrak{B} \vDash \mathrm{Gr}$, es decir, $\mathfrak{B}$ es un grupo.

- $\circ^{\mathfrak{B}}$ es asociativa: $(f_1 \circ^{\mathfrak{B}} f_2) \circ^{\mathfrak{B}} f_3 = f_1 \circ^{\mathfrak{B}} (f_2 \circ^{\mathfrak{B}} f_3)$, para todo $f_1, f_2, f_3 \in B$.
- $e^{\mathfrak{B}}$ es neutro: $(f \circ^{\mathfrak{B}} e^{\mathfrak{B}}) = f = (e^{\mathfrak{B}} \circ^{\mathfrak{B}} f)$, para todo $f \in B$.
- $\circ^{\mathfrak{B}}$ tiene inversos: $(f \circ^{\mathfrak{B}} f^{-1}) = e^{\mathfrak{B}} = (f^{-1} \circ^{\mathfrak{B}} f)$, para todo $f \in B$.

Pero $\mathfrak{B} \nvDash \varphi$. Tomemos los siguientes elementos de B:

$$\begin{array}{lcllcl} f_1(1) & = & 2 & f_2(1) & = & 1 \\ f_1(2) & = & 3 & f_2(2) & = & 3 \\ f_1(3) & = & 1 & f_2(3) & = & 2 \end{array}$$

$$\begin{array}{lcllcl} g(1) & = & 2 & h(1) & = & 3 \\ g(2) & = & 1 & h(2) & = & 2 \\ g(3) & = & 3 & h(3) & = & 1 \end{array}$$

Tenemos que $(f_1 \circ^{\mathfrak{B}} f_2) = g$ y $(f_2 \circ^{\mathfrak{B}} f_1) = h$.

- Concluimos que $Gr \nvDash \varphi$.

Definición:

Dos $\mathcal{L}$-estructuras $\mathfrak{A}$ y $\mathfrak{B}$ son **elementamente equivalentes** si para toda $\mathcal{L}$-oración:

$$\mathfrak{A} \vDash \varphi \iff \mathfrak{B} \vDash \varphi.$$

Observación:

Si $\mathfrak{A}$ y $\mathfrak{B}$ son isomorfas, entonces $\mathfrak{A}$ y $\mathfrak{B}$ son elementalmente equivalentes.
(teorema de isomorfismo)

Teorema:

Una teoría Σ es completa si y sólo si para todo par de estructuras $\mathfrak{A}$ y $\mathfrak{B}$:

$$\mathfrak{A} \vDash \Sigma \text{ y } \mathfrak{B} \vDash \Sigma \implies \mathfrak{A} \text{ y } \mathfrak{B} \text{ son elementalmente equivalentes.}$$

Demostración: Propuesta.

Una teoría Σ es **decidible** si el lenguaje $\{\langle\varphi\rangle \mid \varphi \in \Sigma\}$ es decidible.

Una teoría Σ es **finitamente axiomatizable** si existe un conjunto consistente finito Ax tal que $\Sigma = \mathrm{Th}(\mathrm{Ax})$.

Ejemplo:

$\mathrm{Th}(\mathrm{Gr})$ es una teoría finitamente axiomatizable.

Una teoría Σ es **recursivamente axiomatizable** si existe un conjunto consistente decidible Ax tal que $\Sigma = \mathrm{Th}(\mathrm{Ax})$.

Ejemplo:

La teoría de conjuntos ZFC es recursivamente axiomatizable.

Observación:

Toda teoría finitamente axiomatizable es recursivamente axiomatizable.

Teorema:

Si una teoría es completa y recursivamente axiomatizable, entonces es decidible.

Demostración:

Sea Σ una teoría completa y recursivamente axiomatizable con conjunto consistente decidible Ax con $\Sigma = \mathrm{Th}(\mathrm{Ax})$. El siguiente algoritmo decide Σ:

Sobre entrada $\langle\varphi\rangle$:

1. Iterar sobre todas las secuencias finitas de fórmulas π.
   (en orden lexicigráfico.)
2. Si π es una demostración de φ desde Ax, **aceptar**.
3. Si π es una demostración de $\neg\varphi$ desde Ax, **rechazar**.

(basta ocupar cualquier sistema deductivo completo, e.g., sistemas de Hilbert).

Sabemos que $\mathrm{Th}(\mathfrak{N})$ es completa.
¿Es $\mathrm{Th}(\mathfrak{N})$ recursivamente axiomatizable?

Teorema (Incompletitud de Gödel):

Para todo conjunto de axiomas Ax consistente y decidible, existe una oración φ tal que:

$$\varphi \in \mathrm{Th}(\mathfrak{N}) \qquad \text{y} \qquad \mathrm{Ax} \nvdash \varphi.$$

En particular, $\mathrm{Th}(\mathfrak{N})$ no es recursivamente axiomatizable.

Esto también es consecuencia directa del siguiente resultado:

Teorema:

$\mathrm{Th}(\mathfrak{N})$ es indecidible.