Teorema de incompletitud e intro a lógica de segundo orden

Semana $(14)_2 = 1110$

Lógica para Ciencia de la Computación - IIC2213

Prof. Sebastián Bugedo

Programa

Programa

Teorías decidibles

Definición

Una teoría Σ sobre un vocabulario $\mathcal{L}$ es **decidible** si existe un algoritmo tal que para cualquier $\mathcal{L}$-oración φ, verifica si $\varphi \in \Sigma$.

¿Cómo demostramos decidibilidad?

Una técnica para decidibilidad

Definición

Una teoría Σ **admite eliminación de cuantificadores** si para toda $\mathcal{L}$-fórmula $\varphi(x_1, \ldots, x_k)$, existe una $\mathcal{L}$-fórmula φ^{sc} sin cuantificadores tal que

$$\Sigma \models \forall x_1 \cdots \forall x_k \big[\varphi(x_1, \ldots, x_k) \leftrightarrow \varphi^{\mathsf{sc}}(x_1, \ldots, x_k)\big]$$

Ojo: la posibilidad de eliminar cuantificadores es una característica de **la teoría**, no de fórmulas específicas!

Hacia la decidibilidad

Teorema

Si una teoría Σ cumple

1. admite eliminación de cuantificadores
2. existe algoritmo que construye φ^{sc} desde φ, para toda fórmula φ

entonces Σ es decidible.

Proposición

Sea Σ una teoría tal que para toda fórmula de la forma

$$\varphi(x_1, \dots, x_k) = \exists y(\alpha_0 \wedge \cdots \wedge \alpha_m)$$

con α_i sin cuantificadores, existe φ^{sc} sin cuantificadores tal que

$$\Sigma \ \vDash \ \forall x_1 \cdots \forall x_k \big[\varphi(x_1, \dots, x_k) \leftrightarrow \varphi^{\mathsf{sc}}(x_1, \dots, x_k)\big]$$

Entonces Σ admite eliminación de cuantificadores.

Una teoría decidible

Sea $\mathcal{L} = \{<\}$ y $\mathrm{Th}(\mathfrak{R}_<) = \langle \mathbb{R}, <^{\mathfrak{R}_<} \rangle$ que interpreta $<$ de forma usual

Teorema

$\mathrm{Th}(\mathfrak{R}_<)$ admite eliminación de cuantificadores y además, existe un algoritmo que construye φ^{sc} a partir de φ

Corolario

$\mathrm{Th}(\mathfrak{R}_<)$ es decidible

La clase pasada motivamos la demostración de este resultado

Más teorías decidibles

Hay más teorías que admiten eliminación de cuantificadores

Teorema (Tarski)

$\mathrm{Th}(\mathfrak{R})$ admite eliminación de cuantificadores. Además, existe un algoritmo que construye φ^{sc} a partir de φ.

Corolario

$\mathrm{Th}(\mathfrak{R})$ es decidible

¿Toda teoría que hemos estudiado es decidible?
¿Para todas sirve esta estrategia?

Playlist Unidad IV y Orquesta

Playlist: LogiWawos #4

Además sigan en instagram:
@orquesta_tamen

Objetivos de la clase

- Argumentar que hay varias teorías decidibles
- Conocer el teorema de incompletitud de Gödel
- Comprender la necesidad de una lógica más expresiva para axiomatizar $\mathrm{Th}(\mathfrak{N})$
- Conocer elementos de lógica de segundo orden

Programa

Obertura

Acto único

- ¿Th($\mathfrak{N}$) decidible?
- Teorema de incompletitud
- Lógica de segundo orden

Epílogo

Resultados favorables

Sea $\mathcal{L} = \{0, s\}$ con s símbolo de función unaria y $\mathfrak{N}_s$ la $\mathcal{L}$-estructura con dominio $\mathbb{N}$ que interpreta 0 y s como la estructura $\mathfrak{N}$

Teorema

$\mathrm{Th}(\mathfrak{N}_s)$ admite eliminación de cuantificadores y además, existe un algoritmo que construye φ^{sc} a partir de φ

Corolario

$\mathrm{Th}(\mathfrak{N}_s)$ es decidible

¿Qué hay que hacer en la demo de este teorema?

Resultados *favorables*

Sea $\mathcal{L} = \{0, s, +, <\}$ con símbolos usuales y $\mathfrak{N}_+$ la $\mathcal{L}$-estructura con dominio $\mathbb{N}$ que interpreta los símbolos de $\mathcal{L}$ como la estructura $\mathfrak{N}$

¿Qué nos gustaría demostrar?

Empiezan los problemas

- ¿Podemos usar eliminación de cuantificadores en $\mathrm{Th}(\mathfrak{N}_+)$?
- ¡No admite eliminación de cuantificadores!

Ejemplo

En la teoría $\mathrm{Th}(\mathfrak{N}_+)$, no es posible eliminar cuantificadores de

$$\varphi(x) = \exists y(x = y + y)$$

Extendiendo el vocabulario

¡No todo está perdido!

- Añadiremos una relación binaria
- La interpretaremos de forma adecuada

Ejemplo

Consideremos el vocabulario $\mathcal{L}' = \mathcal{L} \cup \{\equiv_2\}$

La estructura de naturales que interpreta el símbolo $\equiv_2$ como congruencia módulo 2 permite reescribir sin cuantificadores la fórmula del ejemplo anterior

$$\varphi(x) = \exists y(x = y + y) \qquad \varphi^{sc}(x) = (x \equiv_2 0)$$

¿Podemos extender esta idea para otros módulos?

Aritmética de Presburger

Sea $\mathcal{L}_{\equiv} = \mathcal{L} \cup \{\equiv_k \mid k \geq 2\}$

Sea además $\mathfrak{N}_{\equiv}$ la $\mathcal{L}$-estructura tal que

- Tiene dominio $\mathbb{N}$
- Los símbolos de $\mathcal{L}$ se interpretan tal como en $\mathfrak{N}$
- Para $k \geq 2$, $\equiv_k$ se interpreta como congruencia módulo k

Teorema (Presburger)

$\mathrm{Th}(\mathfrak{N}_{\equiv})$ admite eliminación de cuantificadores y además, existe un algoritmo que construye φ^{sc} a partir de φ

Aritmética de Presburger

Teorema (Presburger)

$\mathrm{Th}(\mathfrak{N}_{\equiv})$ admite eliminación de cuantificadores y además, existe un algoritmo que construye φ^{sc} a partir de φ

Corolario

$\mathrm{Th}(\mathfrak{N}_{\equiv})$ es decidible

Corolario

$\mathrm{Th}(\mathfrak{N}_{+})$ es decidible

¿De dónde sale esto?

Naturales con suma

Demostración del último corolario

Sean $\mathcal{L}$ y $\mathcal{L}_{\equiv}$ los vocabularios mencionados. Sea φ una $\mathcal{L}$-oración, es decir, sabemos que no incluye ninguno de los símbolos $\equiv_k$.

Como $\mathrm{Th}(\mathfrak{N}_{\equiv})$ es decidible, existe un algoritmo $\mathcal{A}$ que decide si una $\mathcal{L}_{\equiv}$-oración es parte de $\mathrm{Th}(\mathfrak{N}_{\equiv})$. Además, toda aparición de $x \equiv_k y$ se puede escribir como

$$\exists z(x = \underbrace{z + \cdots + z}_{k\text{-veces}} + y)$$

Dada φ, notemos que ella también es una $\mathcal{L}_{\equiv}$-oración y que

$$\mathfrak{N}_{\equiv} \models \varphi \text{ si y solo si } \mathfrak{N}_{+} \models \varphi$$

Luego, la respuesta del algoritmo $\mathcal{A}$ sirve para decir $\mathrm{Th}(\mathfrak{N}_{+})$. Concluimos que esta última teoría es también decidible.

Teorías decidibles

Con eliminación de cuantificadores, hemos dicho que las siguientes teorías son decidibles

- $\mathrm{Th}(\mathfrak{R}_<)$
- $\mathrm{Th}(\mathfrak{R})$
- $\mathrm{Th}(\mathfrak{N}_s)$
- $\mathrm{Th}(\mathfrak{N}_\equiv)$
- $\mathrm{Th}(\mathfrak{N}_+)$

¿Podemos usar una estrategia similar para $\mathrm{Th}(\mathfrak{N})$?

Programa

Obertura

Acto único

- ¿Th($\mathfrak{N}$) decidible?
- Teorema de incompletitud
- Lógica de segundo orden

Epílogo

Una propiedad fundamental

Definición

Una teoría Σ es **finitamente axiomatizable** si existe un conjunto finito A de $\mathcal{L}$-oraciones tal que

- Σ es consistente
- $\Sigma = \mathrm{Th}(A)$

Teorema

Si una teoría es finitamente axiomatizable y completa, entonces es decidible

¿Podremos axiomatizar $\mathrm{Th}(\mathfrak{N})$?

Teorema de incompletitud de Gödel

Teorema (Gödel)

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

Corolario

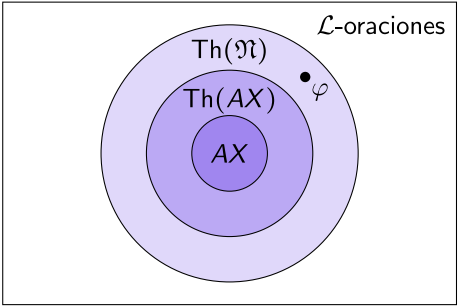
$\mathrm{Th}(\mathfrak{N})$ no es finitamente axiomatizable

¿Qué significa que no sea axiomatizable?

Visualizando el teorema de incompletitud

Corolario

$\mathrm{Th}(\mathfrak{N})$ no es finitamente axiomatizable



Todo conjunto de axiomas finito AX que busquemos para $\mathrm{Th}(\mathfrak{N})$ va a dejar fuera alguna oración consecuencia de $\mathrm{Th}(\mathfrak{N})$

Teorema de incompletitud de Gödel

Teorema (Gödel) [Reformulación]

Para todo conjunto de $\mathcal{L}$-oraciones Σ que es consistente y decidible, existe una $\mathcal{L}$-oración φ tal que

$$\varphi \in \mathsf{Th}(\mathfrak{N}) \quad \text{y} \quad \Sigma \not\models \varphi$$

Esta forma del teorema es equivalente a que $\varphi \in \mathsf{Th}(\mathfrak{N})$ sea indecidible

Teorema de incompletitud de Gödel

Teorema (Gödel)

$\mathsf{Th}(\mathfrak{N})$ es indecidible

Corolario

$\mathsf{Th}(\langle \mathbb{N}, +, \cdot \rangle)$ es indecidible

¿Para qué nos sirve este último corolario?

Al fin...

Pati-Reflexión

Sea $\mathcal{L} = \{+\}$, donde $+$ es símbolo de función binaria. Sea $\mathfrak{A} = \langle \mathbb{N}, +^{\mathfrak{A}} \rangle$ con la interpretación usual de suma en los naturales

El siguiente conjunto no es definibile

$$\mathcal{S} = \{(a, b, c) \in \mathbb{N}^3 \mid a \cdot b = c\}$$

Teorema de isomorfismo NO SIRVE AQUÍ

¿Qué pasaría si pudiéramos definir la multiplicación en $\langle \mathbb{N}, +^{\mathfrak{A}} \rangle$?

Una caracterización de la aritmética

Ya sabemos que **no se puede** axiomatizar la aritmética en LPO

Pero **sí se puede** con lógicas más expresivas

¿Tendrá algún contra usar una lógica más expresiva?

Programa

Obertura

Acto único

- ¿Th($\mathfrak{N}$) decidible?
- Teorema de incompletitud
- Lógica de segundo orden

Epílogo

Lógica de segundo orden

Llamaremos **lógica de segundo orden (LSO)** a nuestra nueva herramienta que usará

- conectivos lógicos
- paréntesis
- relación binaria de igualdad
- variables de **primer y segundo orden**
  - Primer orden: x representa un elemento del dominio
  - Segundo orden: R representa una **relación**
- cuantificadores

Veremos que la sintaxis y semántica es muy similar

Lógica de segundo orden

Ejemplo

Sea $\mathcal{L} = \varnothing$. La siguiente es una $\mathcal{L}$-oración en LSO

$$\begin{aligned}\exists R \quad \big[& \forall x \exists y \; R(x,y) \; \wedge \\ & \forall x \forall y \forall z (R(x,y) \wedge R(x,z) \rightarrow y = z) \; \wedge \\ & \forall x \forall y \forall z (R(y,x) \wedge R(z,x) \rightarrow y = z) \; \wedge \\ & \exists y \forall x \; \neg R(x,y) \big]\end{aligned}$$

Notemos que no necesitamos símbolos de relaciones,
pues ahora son variables que son instanciables con cuantificadores

Sintaxis de LSO: fórmulas

La definición de $\mathcal{L}$-términos es igual que en LPO

Definición

El conjunto de **$\mathcal{L}$-fórmulas** en LSO se define usando las reglas de LPO junto con

- Si $t_1, \ldots, t_k$ son $\mathcal{L}$-términos, y R es una variable de segundo orden de aridad k, enmtonces $R(t_1, \ldots, t_k)$ es $\mathcal{L}$-fórmula
- Si φ es $\mathcal{L}$-fórmula que menciona la variable R, entonces $(\exists R.\ \varphi)$ y $(\forall R.\ \varphi)$ son $\mathcal{L}$-fórmulas

La semántica se extiende de forma similar.
Notemos que la definición de $\mathcal{L}$-estructura no cambia

Axiomatizando $\mathfrak{N}$ en LSO

Sea $\mathcal{L} = \{0, 1, s, +, \cdot, <\}$

Mostraremos oraciones de un conjunto AP tal que

- AP será finito y consistente
- Si $\mathfrak{A} \models AP$, entonces $\mathfrak{A} \cong \mathfrak{N}$

El conjunto AP puede considerarse
una axiomatización de la aritmética

Axiomatizando $\mathfrak{N}$ en LSO

Ejemplo

Consideremos las dos primeras oraciones

$$\neg\exists x(s(x) = 0)$$
$$\forall x \forall y(s(x) = s(y) \rightarrow x = y)$$

¿Qué dicen estas oraciones?

Ejemplo

Axioma de inducción

$$\forall P\big[\big(P(0) \land \forall x(P(x) \to P(s(x)))\big) \to \forall x\ P(x)\big]$$

Como esta oración debe ser satisfecha **para toda** relación P, consideremos

$$P = \{a \in A \mid \text{existe } k \in \mathbb{N} \text{ tal que } a = \underbrace{s(s(\dots s}_{k\text{-veces}}(0)))\}$$

Este conjunto exige que $A = \{0, s(0), s(s(0)), \dots\}$ para cualquier estructura $\mathfrak{A}$ tal que $\mathfrak{A} \models AP$

Axiomatizando $\mathfrak{N}$ en LSO

Ejemplo

Axiomas para definir la suma

$$\forall x(x + 0 = x)$$
$$\forall x \forall y(x + s(y) = s(x + y))$$

Axiomas para definir la multiplicación

$$\forall x(x \cdot 0 = x)$$
$$\forall x \forall y(x \cdot s(y) = x \cdot y + x)$$

Axiomas para fijar el 1 y $<$

$$1 = s(0)$$
$$\forall x \forall y(x < y \leftrightarrow \exists z(\neg z = 0 \wedge x + z = y))$$

A este listado se le conoce como **Axiomas de Peano**
(ojo, hay algunos implícitos en la definición de estructura)

Teorema de Dedekind

Teorema (Dedekind)

Si $\mathfrak{A} \models AP$, entonces $\mathfrak{A} \cong \mathfrak{N}$

Nos falta llevarlo a la teoría de la aritmética

Teorema de Dedekind

Definición

La **teoría de segundo orden** de AP se define como

$$\mathrm{Th}_{\mathrm{SO}}(AP) = \{\varphi \mid \varphi \text{ oración en LSO y } AP \models \varphi\}$$

Proposición

Para toda oración en LPO φ,

$$\varphi \in \mathrm{Th}(\mathfrak{N}) \quad \text{si y solo si} \quad \varphi \in \mathrm{Th}_{\mathrm{SO}}(AP)$$

Hay una mala noticia para la LSO...

¿Sistema deductivo en LSO?

Corolario

No existe un sistema deductivo correcto y completo para la lógica de segundo orden

Tal sistema permitiría decidir $\varphi \in \mathrm{Th}_{\mathsf{SO}}(AP)$
y por consiguiente, a $\varphi \in \mathrm{Th}(\mathfrak{N})$

Programa

Actividad Espiritual Complementaria #2

Objetivos de la clase

- □ Argumentar que hay varias teorías decidibles
- □ Conocer el teorema de incompletitud de Gödel
- □ Comprender la necesidad de una lógica más expresiva para axiomatizar $\mathrm{Th}(\mathfrak{N})$
- □ Conocer elementos de lógica de segundo orden

¿Qué aprendí hoy? ¿Comentarios?

Ve a

www.menti.com

Introduce el código

5676 4833

O usa el código QR