Teorema de incompletitud de Gödel

Theorem (Gödel)

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

Corolario

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

Ejercicio

Demuestre el corolario.

Una idea (moderna) de la demostración

Considere el problema:

$$U = \{w' \in \{0,1\}^* \mid \text{existe una MT } M \text{ y } w \in A^* \text{ tal que } w' = C(M)0000w \text{ y } M \text{ se detiene con entrada } w\}$$

Sabemos que U es indecidible.

- Queremos reducir U a $\mathrm{Th}(\mathfrak{N})$

Vale decir, dada una MT $M = (Q, \{0,1\}, q_0, \delta, F)$ y una entrada $w \in \{0,1\}^*$ para M, queremos construir una oración $\varphi_{M,w}$ tal que:

M se detiene con entrada w si y sólo si $\varphi_{M,w} \in \mathrm{Th}(\mathfrak{N})$

Primer ingrediente de la demostración

Existe una cantidad infinita de números $n \in \mathbb{N}$ tales que $n = \alpha_0 \alpha_1 \cdots \alpha_k$, donde:

- Cada α_i representa a una configuración de M con un número finito de celdas seleccionadas
- Para cada α_i y α_j se tiene que estos números tienen el mismo largo
  - α_i y α_j representan entonces configuraciones con el mismo número de celdas
- α_0 representa a la configuración inicial de M (con w como entrada)
- α_{i+1} debe ser la configuración obtenida a partir de α_i según la función de transición δ

Segundo ingrediente de la demostración

Suponga que $*$ es un símbolo reservado que no se menciona en Q.

De un orden lineal arbitrario a $\{0, 1, \mathtt{B}\} \times (Q \cup \{*\})$.

Asigne a cada par $(a, q) \in \{0, 1, \mathtt{B}\} \times (Q \cup \{*\})$ un número de la forma 1ℓ, donde ℓ es la posición de (a, q) en el orden partiendo desde el 0.

- Agregue los símbolos 0 necesarios después del 1 inicial para que todos los valores asignados tengan el mismo largo.

Segundo ingrediente de la demostración

Ejemplo

Suponga que $Q = \{q_0, q_1, q_2\}$, y suponga que el siguiente orden lineal es dado a los pares en $\{0, 1, \mathtt{B}\} \times \{q_0, q_1, q_2, *\}$:

$$(0,*) < (1,*) < (\mathtt{B},*) < (0,q_0) < (1,q_0) < (\mathtt{B},q_0) < (0,q_1) < (1,q_1) < (\mathtt{B},q_1) < (0,q_2) < (1,q_2) < (\mathtt{B},q_2)$$

Entonces los siguientes son los números asignados a los pares:

$(0,*)$	$\mapsto$	100	$(0,q_1)$	$\mapsto$	106
$(1,*)$	$\mapsto$	101	$(1,q_1)$	$\mapsto$	107
$(\mathtt{B},*)$	$\mapsto$	102	$(\mathtt{B},q_1)$	$\mapsto$	108
$(0,q_0)$	$\mapsto$	103	$(0,q_2)$	$\mapsto$	109
$(1,q_0)$	$\mapsto$	104	$(1,q_2)$	$\mapsto$	110
$(\mathtt{B},q_0)$	$\mapsto$	105	$(\mathtt{B},q_2)$	$\mapsto$	111

Segundo ingrediente de la demostración

Representamos cada celda de una configuración con un par $(a, q) \in \{0, 1, \mathtt{B}\} \times (Q \cup \{*\})$

- a es el contenido de la celda
- Si $q = *$, entonces la cabeza lectora no se encuentra en esta celda
- Si $q \in Q$, entonces la cabeza lectora se encuentra en esta celda y M está en estado q

Una configuración es representada entonces como la secuencia de números asignados a los pares que representan sus celdas.

Segundo ingrediente de la demostración

Ejemplo

Suponga que se quiere representar una configuración de M en la cual tenemos el siguiente contenido en la cinta (omitiendo los otros valores B):

$$\texttt{B011B}$$

Además, suponga que M se encuentra en estado q_2 y que su cabeza lectora está en la celda con el primer símbolo 1 (de izquierda a derecha).

Está configuración de M es representada por la siguiente secuencia de pares:

$$(\texttt{B}, *)(0, *)(1, q_2)(1, *)(\texttt{B}, *)$$

Si asignamos números a los pares como en el ejemplo anterior, entonces el siguiente número representa la configuración descrita:

$$102100110101102$$

Tercer ingrediente de la demostración

Necesitamos una fórmula que nos permitan extraer un bloque desde un número en una posición dada como parámetro.

- Si un número n representa una secuencia de configuraciones, un bloque de n es una configuración
- Si un número m representa una configuración, un bloque de m es una celda

Vamos a definir dos fórmula:

$\varphi_{\text{bloq}}(x, y, z)$	:	es cierta si x se puede dividir en y bloques de largo z
$\varphi_{\text{bloq\_ind}}(x, y, z, w)$	:	es cierta si x se puede dividir en bloques de largo y, y el z-ésimo de estos bloques es w (contando desde 0 de izquierda a derecha)

La definición de $\varphi_{\text{bloq}}(x, y, z)$

Considere las siguientes fórmulas auxiliares:

$$\begin{aligned} \varphi_{\text{div}}(x, y, z) &= \exists u\,(x = z \cdot y + u \wedge 0 \leq u \wedge u < y) \\ \varphi_{\text{menos}}(x, y, z) &= x = y + z \end{aligned}$$

Además suponga que la fórmula $\varphi_{\text{exp10}}(x, y)$ es verdad si $y = 10^x$

- Está fórmula es definida de manera analoga a $\varphi_{\text{exp}}(x, y)$

La definición de $\varphi_{\text{bloq}}(x, y, z)$

Utilizando las fórmulas anteriores definimos la siguiente fórmula:

$$\varphi_{\text{largo}}(x, y) \;=\; \exists z \exists u \exists v \, (\varphi_{\text{menos}}(y, 1, z) \wedge \varphi_{\text{exp10}}(z, u) \wedge \varphi_{\text{exp10}}(y, v) \wedge u \leq x \wedge x < v)$$

¿Cuál es la relación entre x e y en este caso?

Definimos finalmente:

$$\varphi_{\text{bloq}}(x, y, z) \quad = \quad \exists u \, (\varphi_{\text{largo}}(x, u) \wedge u = y \cdot z)$$

La definición de $\varphi_{\text{bloq\_ind}}(x, y, z, w)$

Utilizamos la función β de Gödel y la fórmula φ_{mod} definida anteriormente:

$$
\begin{aligned}
&\exists u \exists \ell \exists i \exists a_1 \exists b_1 \exists a_2 \exists b_2 \Big[\\
&\quad \varphi_{\text{bloq}}(x, u, y) \wedge 0 \leq z \wedge z < u \wedge \varphi_{\text{exp10}}(y, \ell) \wedge \\
&\quad \forall u_1 \left(\varphi_{\text{mod}}(x, \ell, u_1) \rightarrow \varphi_\beta(a_1, b_1, 0, u_1)\right) \wedge \\
&\quad \forall u_2 \left(\varphi_{\text{div}}(x, \ell, u_2) \rightarrow \varphi_\beta(a_2, b_2, 0, u_2)\right) \wedge \\
&\quad \forall u_3 \forall u_4 \forall u_5 \forall u_6 \Big(\big(0 \leq u_3 \wedge s(u_3) < u \wedge \varphi_\beta(a_2, b_2, u_3, u_4) \wedge \\
&\qquad\qquad \varphi_{\text{mod}}(u_4, \ell, u_5) \wedge \varphi_{\text{div}}(u_4, \ell, u_6)\big) \rightarrow \\
&\qquad\qquad \big(\varphi_\beta(a_1, b_1, s(u_3), u_5) \wedge \varphi_\beta(a_2, b_2, s(u_3), u_6)\big) \Big) \wedge \\
&\quad \varphi_{\text{menos}}(u, s(z), i) \wedge \varphi_\beta(a_1, b_1, i, w) \Big]
\end{aligned}
$$

Un corolario de la demostración

Corolario

Th($\mathfrak{N}$) *no es recursivamente enumerable.*

Ejercicio

De una reducción de $\overline{U}$ a Th($\mathfrak{N}$).

Una reformulación del Teorema de incompletitud de Gödel

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

Teorema (Gödel)

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

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

Ejercicio

Demuestre que las dos formulaciones del teorema son equivalentes.

Teorema de incompletitud de Gödel: Un corolario

El teorema de isomorfismo no puede usarse directamente para demostrar que la multiplicación no es definible en $\langle \mathbb{N}, + \rangle$

- ¿Por qué?

Pero de los resultados anteriores obtenemos:

Corolario

La multiplicación no es definible en $\langle \mathbb{N}, + \rangle$

Ejercicio

Demuestre el corolario.

Una caracterización de la aritmética

Vimos que la aritmética no puede ser axiomatizada en lógica de primer orden.

Pero la aritmética puede ser caracterizada usando lógicas más expresivas.

- Vamos a ver una axiomatización en lógica de segundo orden
- Esta lógica pierde alguna de las buenas propiedades de la lógica de primer orden

Lógica de segundo orden

Las fórmulas de la lógica de segundo orden se construyen usando:

- Conectivos lógicos: $\neg$, $\vee$, $\wedge$, $\rightarrow$ y $\leftrightarrow$
- Paréntesis: (y)
- Relación binaria $=$
- Variables de primer y segundo orden:
  - Primer orden: x representa un elemento del dominio
  - Segundo orden: R representa una relación sobre el dominio
- Cuantificadores: $\forall$ y $\exists$

Lógica de segundo orden: Ejemplo

Sea $\mathcal{L}$ el vocabulario vacío. La siguiente es una $\mathcal{L}$-oración en lógica de segundo orden:

$$\exists R \Big[\forall x \exists y \, R(x,y) \wedge$$
$$\forall x \forall y \forall z \, (R(x,y) \wedge R(x,z) \rightarrow y = z) \wedge$$
$$\forall x \forall y \forall z \, (R(y,x) \wedge R(z,x) \rightarrow y = z) \wedge$$
$$\exists y \forall x \, \neg R(x,y) \Big]$$

¿Qué propiedad define esta oración?

Sintaxis de la lógica de segundo orden

Suponga dadas una lista infinita de variables de primer orden y una lista infinita de variables de segundo orden.

- Cada variable de segundo orden tiene una aridad asociada

Sea $\mathcal{L}$ un vocabulario.

- La definición de $\mathcal{L}$-término no cambia

Sintaxis de la lógica de segundo orden (continuación)

Definición

El conjunto de $\mathcal{L}$-fórmulas en lógica de segundo orden se define utilizando las reglas para primer orden junto con las reglas:

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

Semántica de la lógica de segundo orden

Sea $\mathcal{L}$ un vocabulario.

- La definición de $\mathcal{L}$-estructura no cambia

Dada una estructura $\mathfrak{A}$ con dominio A, una asignación σ es una función tal que:

- Para cada variable de primer orden x: $\sigma(x) \in A$
- Para cada variable de segundo orden R de aridad k: $\sigma(R) \subseteq A^k$

Dada una variable R de segundo orden de aridad k y $C \subseteq A^k$:

$$\sigma[R/C](X) = \begin{cases} C & X = R \\ \sigma(X) & X \neq R \end{cases}$$

Semántica de la lógica de segundo orden (continuación)

Definición

$(\mathfrak{A}, \sigma) \models \varphi$ *se define utilizando las de reglas de satisfacción para primer orden junto con las reglas:*

- $\varphi = R(t_1, \ldots, t_k)$, *donde* R *es una variable de segundo orden de aridad* k, *y* $(\sigma(t_1), \ldots, \sigma(t_k)) \in \sigma(R)$
- $\varphi = (\exists R\, \psi)$, *donde* R *es una variable de segundo orden de aridad* k, *y existe* $C \subseteq A^k$ *tal que* $(\mathfrak{A}, \sigma[R/C]) \models \psi$
- $\varphi = (\forall R\, \psi)$, *donde* R *es una variable de segundo orden de aridad* k, *y para todo* $C \subseteq A^k$ *se tiene que* $(\mathfrak{A}, \sigma[R/C]) \models \psi$

Caracterizando $\mathfrak{N}$ en lógica de segundo orden

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

Vamos a construir un conjunto finito y consistente AP de $\mathcal{L}$-oraciones en lógica de segundo orden tal que:

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

AP puede considerarse una axiomatización de la aritmética.

Caracterizando $\mathfrak{N}$ en lógica de segundo orden

Los dos primeros axiomas de AP:

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

Si una estructura satisface AP, entonces tiene un dominio infinito.

- Al menos contiene los elementos 0, $s(0)$, $s(s(0))$, $\ldots$,
- $\underbrace{s(s(s(\cdots s}_{i \text{ símbolos } s}(0)\cdots))) \neq \underbrace{s(s(s(\cdots s}_{j \text{ símbolos } s}(0)\cdots)))$ si $i \neq j$

Caracterizando $\mathfrak{N}$ en lógica de segundo orden

AP contiene un axioma de inducción:

$$\forall P \left[\Big(P(0) \wedge \forall x \, (P(x) \rightarrow P(s(x))) \Big) \rightarrow \forall x \, P(x) \right]$$

Si $\mathfrak{A} \models \text{AP}$, entonces $\mathfrak{A}$ tiene como dominio $A = \{0, s(0), s(s(0)), s(s(s(0))), \ldots\}$

- Para demostrar esto considere el conjunto:

$$P \quad = \quad \{a \in A \mid \text{existe } k \in \mathbb{N} \text{ tal que } a = \underbrace{s(s(s(\cdots s}_{k \text{ símbolos } s}(0) \cdots)))\}$$

Caracterizando $\mathfrak{N}$ en lógica de segundo orden

AP contiene axiomas que definen la suma:

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

AP contiene axiomas que definen la multiplicación:

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

Caracterizando $\mathfrak{N}$ en lógica de segundo orden

Finalmente, AP contiene axiomas que definen los símbolos 1 y $<$:

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

Teorema (Dedekind)

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

Ejercicio

Demuestre el teorema.

Teoremas de Gödel y Dedekind: Un corolario fundamental

La noción de consecuencia lógica se define para la lógica de segundo orden como para el caso de primer orden.

La teoría de segundo orden de AP se define como:

$$\mathrm{Th}_{\mathrm{SO}}(\mathrm{AP}) = \{\varphi \mid \varphi \text{ es una } \mathcal{L}\text{-oración en lógica de segundo orden y AP} \models \varphi\}$$

Proposición

Para cada $\mathcal{L}$-oración φ en lógica de primer orden: $\varphi \in Th(\mathfrak{N})$ si y sólo si $\varphi \in Th_{SO}(AP)$

Teoremas de Gödel y Dedekind: Un corolario fundamental

Corolario

No puede existir un sistema de deducción correcto y completo (como el sistema de Hilbert) para la lógica de segundo orden.

Demostración: Si existiera este sistema, entonces $\mathrm{Th}_{\mathrm{SO}}(\mathrm{AP})$ sería decidible.

- ¿Por qué?

De la proposición obtenemos que $\mathrm{Th}(\mathfrak{N})$ es decidible.

- Obtenemos una contradicción ya que desde el teorema de Gödel sabemos que $\mathrm{Th}(\mathfrak{N})$ es indecidible □

Lógica de segundo orden: Un segundo resultado negativo

No se puede demostrar que el teorema de compacidad es válido para la lógica de segundo orden como en el caso de primer orden.

- Por el corolario anterior

De hecho, es posible demostrar que el teorema de compacidad no es válido para la lógica de segundo orden.

Proposición

Existe un conjunto inconsistente de oraciones de segundo orden sobre el vocabulario vacío que es finitamente satisfacible.

Compacidad no es válido para segundo orden: Demostración

Sea $\mathcal{L}$ el vocabulario vacío y Φ la siguiente $\mathcal{L}$-oración:

$$\forall R \Bigg[\Big(\forall x \exists y \, R(x,y) \wedge \forall x \forall y \forall z \, (R(x,y) \wedge R(x,z) \rightarrow y = z) \wedge \forall x \forall y \forall z \, (R(y,x) \wedge R(z,x) \rightarrow y = z) \Big) \rightarrow \forall y \exists x \, R(x,y) \Bigg]$$

Además, para cada $n \geq 2$, sea λ_n la siguiente $\mathcal{L}$-oración:

$$\exists x_1 \cdots \exists x_n \left(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \right)$$

Compacidad no es válido para segundo orden: Demostración

Sea $\Sigma = \{\Phi\} \cup \{\lambda_n \mid n \geq 2\}$

Se tiene que Σ es inconsistente.

- ¿Por qué?

Además, se tiene que Σ es finitamente satisfacible.

- ¿Por qué?