Teorías axiomatizables: Una definición más general

Recuerde que un conjunto de oraciones Γ sobre un vocabulario $\mathcal{L}$ es decidible si existe un algoritmo que, dada una $\mathcal{L}$-oración φ, verifica si $\varphi \in \Gamma$

- Vale decir, si Γ es decidible cuando es considerado como un lenguaje

Teorías axiomatizables: Una definición más general

Recuerde que un conjunto de oraciones Γ sobre un vocabulario $\mathcal{L}$ es decidible si existe un algoritmo que, dada una $\mathcal{L}$-oración φ, verifica si $\varphi \in \Gamma$

- Vale decir, si Γ es decidible cuando es considerado como un lenguaje

Sea Σ una teoría sobre $\mathcal{L}$.

Teorías axiomatizables: Una definición más general

Recuerde que un conjunto de oraciones Γ sobre un vocabulario $\mathcal{L}$ es decidible si existe un algoritmo que, dada una $\mathcal{L}$-oración φ, verifica si $\varphi \in \Gamma$

- Vale decir, si Γ es decidible cuando es considerado como un lenguaje

Sea Σ una teoría sobre $\mathcal{L}$.

Definición

Σ es recursivamente axiomatizable si existe un conjunto consistente y decidible Ax de $\mathcal{L}$-oraciones tal que $\Sigma = Th(Ax)$

Teorías recursivamente axiomatizables: Una propiedad fundamental

Cada teoría finitamente axiomatizable es una teoría recursivamente axiomatizable.

- ¿Por qué son interesantes las teorías recursivamente axiomatizables?

Teorías recursivamente axiomatizables: Una propiedad fundamental

Cada teoría finitamente axiomatizable es una teoría recursivamente axiomatizable.

- ¿Por qué son interesantes las teorías recursivamente axiomatizables?

Teorema

Si una teoría es recursivamente axiomatizable y completa (categórica), entonces es decidible

Teorías recursivamente axiomatizables: Una propiedad fundamental

Cada teoría finitamente axiomatizable es una teoría recursivamente axiomatizable.

- ¿Por qué son interesantes las teorías recursivamente axiomatizables?

Teorema

Si una teoría es recursivamente axiomatizable y completa (categórica), entonces es decidible

Ejercicio

Demuestre el teorema.

Teorías axiomatizables: Una definición aun más general

Sea Σ una teoría sobre un vocabulario $\mathcal{L}$.

Teorías axiomatizables: Una definición aun más general

Sea Σ una teoría sobre un vocabulario $\mathcal{L}$.

Definición

Σ es axiomatizable si existe un conjunto consistente y recursivamente enumerable Ax de $\mathcal{L}$-oraciones tal que $\Sigma = Th(Ax)$

Teorías axiomatizables: Una propiedad fundamental

Teorema

Si una teoría es axiomatizable y completa (categórica), entonces es decidible

Teorías axiomatizables: Una propiedad fundamental

Teorema

Si una teoría es axiomatizable y completa (categórica), entonces es decidible

Ejercicio

Demuestre el teorema.

Pregunta pendiente: ¿Es $\mathrm{Th}(\mathfrak{N})$ decidible?

Hemos desarrollado algunas técnicas para demostrar que una teoría es decidible.

- Ya mencionamos que $\mathrm{Th}(\mathfrak{N})$ no admite eliminación de cuantificadores

Pregunta pendiente: ¿Es $\mathrm{Th}(\mathfrak{N})$ decidible?

Hemos desarrollado algunas técnicas para demostrar que una teoría es decidible.

- Ya mencionamos que $\mathrm{Th}(\mathfrak{N})$ no admite eliminación de cuantificadores

Un posible enfoque para demostrar que $\mathrm{Th}(\mathfrak{N})$ es dedicible:

Demostrar que $\mathrm{Th}(\mathfrak{N})$ es axiomatizable

Pregunta pendiente: ¿Es $\mathrm{Th}(\mathfrak{N})$ decidible?

Hemos desarrollado algunas técnicas para demostrar que una teoría es decidible.

- Ya mencionamos que $\mathrm{Th}(\mathfrak{N})$ no admite eliminación de cuantificadores

Un posible enfoque para demostrar que $\mathrm{Th}(\mathfrak{N})$ es dedicible:

Demostrar que $\mathrm{Th}(\mathfrak{N})$ es axiomatizable

¿Funciona este enfoque?

Pregunta pendiente: ¿Es $\mathrm{Th}(\mathfrak{N})$ decidible?

Hemos desarrollado algunas técnicas para demostrar que una teoría es decidible.

- Ya mencionamos que $\mathrm{Th}(\mathfrak{N})$ no admite eliminación de cuantificadores

Un posible enfoque para demostrar que $\mathrm{Th}(\mathfrak{N})$ es dedicible:

Demostrar que $\mathrm{Th}(\mathfrak{N})$ es axiomatizable

¿Funciona este enfoque?

Vamos a mostrar que no ...

Funciones recursivas en $\mathrm{Th}(\mathfrak{N})$

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

Queremos mostrar que cualquier función recursiva $f : \mathbb{N}^k \to \mathbb{N}$ es definible en $\mathfrak{N}$.

- Vale decir, existe una $\mathcal{L}$-fórmula $\varphi_f(x_1, \ldots, x_k, y)$ tal que para todo $a_1, \ldots, a_k, b \in \mathbb{N}$: $f(a_1, \ldots, a_k) = b$ si y sólo si $\mathfrak{N} \models \varphi_f(a_1, \ldots, a_k, b)$

Funciones recursivas en $\mathrm{Th}(\mathfrak{N})$

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

Queremos mostrar que cualquier función recursiva $f : \mathbb{N}^k \to \mathbb{N}$ es definible en $\mathfrak{N}$.

- Vale decir, existe una $\mathcal{L}$-fórmula $\varphi_f(x_1, \ldots, x_k, y)$ tal que para todo $a_1, \ldots, a_k, b \in \mathbb{N}$: $f(a_1, \ldots, a_k) = b$ si y sólo si $\mathfrak{N} \models \varphi_f(a_1, \ldots, a_k, b)$

Algunos ejemplos de funciones recursivas que sabemos como definir:

$$\text{Suma} \quad : \quad \begin{array}{rcl} x + 0 & = & x \\ x + s(y) & = & s(x + y) \end{array}$$

$$\text{Multiplicación} \quad : \quad \begin{array}{rcl} x \cdot 0 & = & 0 \\ x \cdot s(y) & = & (x \cdot y) + x \end{array}$$

Una formalización de la noción de función recursiva

Podemos generalizar las definiciones de la suma y la multiplicación.

Una formalización de la noción de función recursiva

Podemos generalizar las definiciones de la suma y la multiplicación.

Suponga que $k \geq 0$, $g : \mathbb{N}^k \to \mathbb{N}$ y $h : \mathbb{N}^{k+2} \to \mathbb{N}$

- Además, suponga que g y h son funciones que ya han sido definidas

Una formalización de la noción de función recursiva

Podemos generalizar las definiciones de la suma y la multiplicación.

Suponga que $k \geq 0$, $g : \mathbb{N}^k \to \mathbb{N}$ y $h : \mathbb{N}^{k+2} \to \mathbb{N}$

- Además, suponga que g y h son funciones que ya han sido definidas

Definimos $f : \mathbb{N}^{k+1} \to \mathbb{N}$ recursivamente a partir de g y h:

$$\begin{aligned} f(x_1, \ldots x_k, 0) &= g(x_1, \ldots, x_k) \\ f(x_1, \ldots, x_k, s(y)) &= h(x_1, \ldots, x_k, y, f(x_1, \ldots, x_k, y)) \end{aligned}$$

La función exponencial

Utilizamos la idea anterior para definir la función exponencial:

$$\begin{aligned} 2^0 &= 1 \\ 2^{s(y)} &= 2 \cdot 2^y \end{aligned}$$

La función exponencial

Utilizamos la idea anterior para definir la función exponencial:

$$\begin{aligned} 2^0 &= 1 \\ 2^{s(y)} &= 2 \cdot 2^y \end{aligned}$$

¿Cómo podemos definir la función exponencial en $\mathfrak{N}$?

La función exponencial

Utilizamos la idea anterior para definir la función exponencial:

$$\begin{aligned} 2^0 &= 1 \\ 2^{s(y)} &= 2 \cdot 2^y \end{aligned}$$

¿Cómo podemos definir la función exponencial en $\mathfrak{N}$?

- Vamos a utilizar la función β de Gödel para definir la función exponencial

La función exponencial

Utilizamos la idea anterior para definir la función exponencial:

$$\begin{aligned} 2^0 &= 1 \\ 2^{s(y)} &= 2 \cdot 2^y \end{aligned}$$

¿Cómo podemos definir la función exponencial en $\mathfrak{N}$?

- Vamos a utilizar la función β de Gödel para definir la función exponencial
- La función beta de Gödel nos va a permitir codificar cualquier función recursiva en $\mathfrak{N}$

La función β de Gödel

Definición (Función β de Gödel)

Dados $a, b, i \in \mathbb{N}$*:*

$$\beta(a, b, i) \quad = \quad a \ mod \ [b(i+1)+1]$$

La función β de Gödel

Definición (Función β de Gödel)

Dados $a, b, i \in \mathbb{N}$:

$$\beta(a, b, i) = a \bmod [b(i+1)+1]$$

Por ejemplo:

$$\begin{aligned} \beta(32, 7, 2) &= 32 \bmod [7(2+1)+1] \\ &= 32 \bmod 22 \\ &= 10 \end{aligned}$$

Una propiedad fundamental de la función β de Gödel

Lema

Para cada secuencia $r_0, r_1, \ldots, r_n$ de números naturales, existen números naturales a, b tales que:

$$\text{para cada } i \in \{0, \ldots, n\}: \ \beta(a, b, i) = r_i$$

Una propiedad fundamental de la función β de Gödel

Lema

Para cada secuencia $r_0, r_1, \ldots, r_n$ de números naturales, existen números naturales a, b tales que:

$$\text{para cada } i \in \{0, \ldots, n\}: \ \beta(a, b, i) = r_i$$

Ejemplo

Para la secuencia $r_0 = 2$, $r_1 = 6$, $r_2 = 3$ tenemos que:

$$\begin{aligned} \beta(1.651.320.463.326, 720, 0) &= 2 \\ \beta(1.651.320.463.326, 720, 1) &= 6 \\ \beta(1.651.320.463.326, 720, 2) &= 3 \end{aligned}$$

Vale decir, $a = 1.651.320.463.326$ y $b = 720$ en este caso.

La demostración del lemma

Considere una secuencia $r_0, r_1, \ldots, r_n$ de números naturales.

La demostración del lemma

Considere una secuencia $r_0, r_1, \ldots, r_n$ de números naturales.

Defina $b = \text{máx}\{n, r_0, r_1, \ldots, r_n\}$!

- Tenemos que $n \leq b$ y $r_i \leq b$ para cada $i \in \{0, \ldots, n\}$
- Además, para cada $0 < k \leq n$ tenemos que $k | b$

La demostración del lemma

Considere una secuencia $r_0, r_1, \ldots, r_n$ de números naturales.

Defina $b = \text{máx}\{n, r_0, r_1, \ldots, r_n\}$!

- Tenemos que $n \leq b$ y $r_i \leq b$ para cada $i \in \{0, \ldots, n\}$
- Además, para cada $0 < k \leq n$ tenemos que $k | b$

Defina $m_i = b(i+1) + 1$

La demostración del lemma

Considere una secuencia $r_0, r_1, \ldots, r_n$ de números naturales.

Defina $b = \text{máx}\{n, r_0, r_1, \ldots, r_n\}$!

- Tenemos que $n \leq b$ y $r_i \leq b$ para cada $i \in \{0, \ldots, n\}$
- Además, para cada $0 < k \leq n$ tenemos que $k|b$

Defina $m_i = b(i+1) + 1$

Vamos a demostrar que para cada $0 \leq i < j \leq n$, se tiene que m_i y m_j son primos relativos.

- Vale decir, $\text{MCD}(m_i, m_j) = 1$

La demostración del lemma

Considere una secuencia $r_0, r_1, \ldots, r_n$ de números naturales.

Defina $b = \text{máx}\{n, r_0, r_1, \ldots, r_n\}$!

- Tenemos que $n \leq b$ y $r_i \leq b$ para cada $i \in \{0, \ldots, n\}$
- Además, para cada $0 < k \leq n$ tenemos que $k|b$

Defina $m_i = b(i+1) + 1$

Vamos a demostrar que para cada $0 \leq i < j \leq n$, se tiene que m_i y m_j son primos relativos.

- Vale decir, $\text{MCD}(m_i, m_j) = 1$

Por contradicción, suponga que p es un primo tal que $p|m_i$ y $p|m_j$

La demostración del lemma

Tenemos entonces que $p|(m_j - m_i)$, vale decir, $p|b(j - i)$

- Por lo tanto $p|b$ o $p|(j - i)$

La demostración del lemma

Tenemos entonces que $p|(m_j - m_i)$, vale decir, $p|b(j-i)$

- Por lo tanto $p|b$ o $p|(j-i)$

Si p divide a b, entonces se tiene que $p|(m_i - b(i+1))$ dado que $p|m_i$

- Concluimos que $p|1$, lo cual es una contradicción

La demostración del lemma

Tenemos entonces que $p|(m_j - m_i)$, vale decir, $p|b(j-i)$

- Por lo tanto $p|b$ o $p|(j-i)$

Si p divide a b, entonces se tiene que $p|(m_i - b(i+1))$ dado que $p|m_i$

- Concluimos que $p|1$, lo cual es una contradicción

Tenemos entonces que $p|(j-i)$

La demostración del lemma

Tenemos entonces que $p|(m_j - m_i)$, vale decir, $p|b(j-i)$

- Por lo tanto $p|b$ o $p|(j-i)$

Si p divide a b, entonces se tiene que $p|(m_i - b(i+1))$ dado que $p|m_i$

- Concluimos que $p|1$, lo cual es una contradicción

Tenemos entonces que $p|(j-i)$

Dado que $0 < j - i \leq n$, tenemos que $(j-i)|b$

- Concluimos entonces que $p|b$ ya que $p|(j-i)$, lo cual nuevamente nos lleva a una contradicción

La demostración del lemma

Para terminar con la demostración usamos el teorema chino del resto.

La demostración del lemma

Para terminar con la demostración usamos el teorema chino del resto.

Dado que $\text{MCD}(m_i, m_j) = 1$ para cada $0 \leq i < j \leq n$, existe un número a tal que:

$$\text{para cada } i \in \{0, \ldots, n\}: \quad a \equiv r_i \bmod m_i$$

La demostración del lemma

Para terminar con la demostración usamos el teorema chino del resto.

Dado que MCD$(m_i, m_j) = 1$ para cada $0 \leq i < j \leq n$, existe un número a tal que:

$$\text{para cada } i \in \{0, \ldots, n\}: \quad a \equiv r_i \bmod m_i$$

Puesto que para cada $i \in \{0, \ldots, n\}$ se tiene que $r_i \leq b < m_i$, concluimos que $a \bmod m_i = r_i$

La demostración del lemma

Para terminar con la demostración usamos el teorema chino del resto.

Dado que $\text{MCD}(m_i, m_j) = 1$ para cada $0 \leq i < j \leq n$, existe un número a tal que:

$$\text{para cada } i \in \{0, \ldots, n\}: \quad a \equiv r_i \bmod m_i$$

Puesto que para cada $i \in \{0, \ldots, n\}$ se tiene que $r_i \leq b < m_i$, concluimos que $a \bmod m_i = r_i$

Por lo tanto, tenemos que $\beta(a, b, i) = r_i$ para cada $i \in \{0, \ldots, n\}$ □

La función β de Gödel en lógica de primer orden

Sea $\varphi_{\mathsf{mod}}(x, y, z)$ una fórmula definida de la siguiente forma:

$$\varphi_{\mathsf{mod}}(x, y, z) \quad = \quad \exists u\,(x = u \cdot y + z \wedge 0 \leq z \wedge z < y),$$

donde $0 \leq z$ es una abreviación de $(0 = z \vee 0 < z)$

La función β de Gödel en lógica de primer orden

Sea $\varphi_{\mathsf{mod}}(x, y, z)$ una fórmula definida de la siguiente forma:

$$\varphi_{\mathsf{mod}}(x, y, z) \quad = \quad \exists u\,(x = u \cdot y + z \wedge 0 \leq z \wedge z < y),$$

donde $0 \leq z$ es una abreviación de $(0 = z \vee 0 < z)$

¿Qué representa z en $\varphi_{\mathsf{mod}}(x, y, z)$?

La función β de Gödel en lógica de primer orden

Sea $\varphi_{\mathsf{mod}}(x, y, z)$ una fórmula definida de la siguiente forma:

$$\varphi_{\mathsf{mod}}(x, y, z) \quad = \quad \exists u\,(x = u \cdot y + z \wedge 0 \leq z \wedge z < y),$$

donde $0 \leq z$ es una abreviación de $(0 = z \vee 0 < z)$

¿Qué representa z en $\varphi_{\mathsf{mod}}(x, y, z)$?

La función β de Gödel entonces es definida en lógica de primer orden de la siguiente forma:

$$\varphi_{\beta}(x, y, z, w) \quad = \quad \varphi_{\mathsf{mod}}(x, y \cdot (z + 1) + 1, w)$$

Definiendo la función exponencial

Queremos definir una fórmula $\varphi_{\text{exp}}(y, z)$ tal que:

$$\mathfrak{N} \models \varphi_{\text{exp}}(a, b) \quad \text{si y sólo si} \quad b = 2^a$$

Definiendo la función exponencial

Queremos definir una fórmula $\varphi_{\text{exp}}(y, z)$ tal que:

$$\mathfrak{N} \models \varphi_{\text{exp}}(a, b) \quad \text{si y sólo si} \quad b = 2^a$$

Dada la definición recursiva de la función exponencial, nos gustaría definir $\varphi_{\text{exp}}(y, z)$ como la siguiente expresión:

$$\exists u_0 \exists u_1 \cdots \exists u_y \left[u_0 = 1 \wedge \forall v \Big((0 \leq v \wedge v < y) \rightarrow u_{v+1} = 2 \cdot u_v \Big) \wedge z = u_y \right]$$

Definiendo la función exponencial

Queremos definir una fórmula $\varphi_{\text{exp}}(y, z)$ tal que:

$$\mathfrak{N} \models \varphi_{\text{exp}}(a, b) \quad \text{si y sólo si} \quad b = 2^a$$

Dada la definición recursiva de la función exponencial, nos gustaría definir $\varphi_{\text{exp}}(y, z)$ como la siguiente expresión:

$$\exists u_0 \exists u_1 \cdots \exists u_y \left[u_0 = 1 \wedge \forall v \left((0 \leq v \wedge v < y) \rightarrow u_{v+1} = 2 \cdot u_v \right) \wedge z = u_y \right]$$

Pero ésta no es una fórmula en lógica de primer orden

- Dado que el número de variables en ella depende del valor de y

Definiendo la función exponencial

La función β de Gödel puede ser usada para solucionar el problema mencionado en la transparencia anterior.

Definiendo la función exponencial

La función β de Gödel puede ser usada para solucionar el problema mencionado en la transparencia anterior.

La función $\varphi_{\exp}(y, z)$ se define de la siguiente forma:

$$\exists a \exists b \Big[\varphi_\beta(a, b, 0, 1) \wedge \forall v \forall w \Big((0 \leq v \wedge v < y \wedge \varphi_\beta(a, b, v, w)) \rightarrow \varphi_\beta(a, b, s(v), 2 \cdot w) \Big) \wedge \varphi_\beta(a, b, y, z) \Big],$$

donde 2 es una abreviación de $(1 + 1)$

Generalizando la construcción

Considere una función $f : \mathbb{N}^{k+1} \to \mathbb{N}$ definida recursivamente:

$$\begin{aligned} f(x_1, \ldots x_k, 0) &= g(x_1, \ldots, x_k) \\ f(x_1, \ldots, x_k, s(y)) &= h(x_1, \ldots, x_k, y, f(x_1, \ldots, x_k, y)) \end{aligned}$$

Generalizando la construcción

Considere una función $f : \mathbb{N}^{k+1} \to \mathbb{N}$ definida recursivamente:

$$\begin{aligned} f(x_1, \ldots x_k, 0) &= g(x_1, \ldots, x_k) \\ f(x_1, \ldots, x_k, s(y)) &= h(x_1, \ldots, x_k, y, f(x_1, \ldots, x_k, y)) \end{aligned}$$

Queremos utilizar la función β de Gödel para construir una fórmula φ_f que defina f

- Suponemos que las funciones g y h son definidas por las fórmulas φ_g y φ_h, respectivamente

Generalizando la construcción

La función $\varphi_f(x_1, \ldots, x_k, y, z)$ se define de la siguiente forma:

$$\exists a \exists b \Big[\forall u \Big(\varphi_g(x_1, \ldots, x_k, u) \rightarrow \varphi_\beta(a, b, 0, u) \Big) \wedge$$
$$\forall v \forall w_1 \forall w_2 \Big((0 \leq v \wedge v < y \wedge \varphi_\beta(a, b, v, w_1) \wedge$$
$$\varphi_h(x_1, \ldots, x_k, v, w_1, w_2)) \rightarrow \varphi_\beta(a, b, s(v), w_2) \Big) \wedge$$
$$\varphi_\beta(a, b, y, z) \Big]$$