

Lógica de Predicados de Primer Orden

Seminario de Matemáticas

Julio Ariel Hurtado Alegría

2013

Material de Jorge Aranda – Pontificia
Universidad Católica de Chile

Lógica de Predicados de Primer Orden

- La lógica proposicional puede ser no apropiada para expresar ciertos tipos de conocimiento. Por ejemplo:

Algunas manzanas son rojas

- Esta afirmación no se refiere específicamente a ningún conjunto de manzanas, solo está diciendo que existe un conjunto de manzanas que son rojas.
- ¿cómo podríamos representar esta afirmación en LP?
- La LP también puede ser no apropiada para modelar cierto tipo de razonamiento.
- Veamos el siguiente razonamiento correcto:

Juan ayuda a todas las personas que gustan de la lógica.

A Juan es persona y le gusta la lógica.

Juan ayuda a Juan

- En estos ejemplos hemos visto que la LP no permite referirse en forma sencilla a todos los elementos de un dominio.
- Más aún, si los elementos del dominio son infinitos, simplemente no puede expresar conocimiento acerca de todos los individuos.
- La LP tampoco es capaz de representar propiedades de objetos, solo proposiciones.
- La lógica de primer orden (LPO) soluciona estos problemas en este sentido:
 - Permite hacer cuantificación sobre los objetos de un dominio. Ej: “Todos los perros son animales”, “Algunos sapos lloran”.
 - Permite representar propiedades a través de relaciones y funciones.
- Un lenguaje \mathcal{L} de la lógica de predicados esta compuesto por los siguientes elementos:
 - Un conjunto \mathbf{C} , finito o enumerable, de constantes para designar objetos. Ej:

$$\{C_1, C_2, \dots, C_n, \dots\},$$

Para evitar confusiones, usaremos siempre mayúsculas para denotar los símbolos constantes.

- Un conjunto \mathbf{F} , de símbolos de función. Ejemplo:

$$\{f, g, h, \dots\}.$$

A cada función se le asocia una *aridad*, que es un número natural y que corresponde a la cantidad de argumentos de la función.

- Un conjunto \mathbf{P} finito o infinito enumerable de símbolos para predicados

$$\{P, Q, R, S, \dots\},$$

que se utilizan para designar propiedades de objetos. A éstos también se les asocia una aridad positiva.

- Los tres conjuntos anteriores, se agrupan normalmente en un solo conjunto de símbolos $S = \langle \mathbf{P}, \mathbf{F}, \mathbf{C} \rangle$. En el que se ubican primero los predicados, luego las funciones y finalmente las constantes. En nuestro ejemplo,

$$S = \langle \langle P, Q, R, S, \dots \rangle, \langle f, g, h, \dots \rangle, \langle C_1, C_2, \dots \rangle \rangle$$

Además de estos elementos un lenguaje de primer está compuesto de fórmulas que pueden contener los siguientes elementos:

1. $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$: conectivos lógicos usuales.
2. $=$: un predicado especial para la igualdad.
3. \exists, \forall : cuantificadores existencial y universal.
4. x_1, x_2, \dots : conjunto enumerable de variables, el cual informalmente podríamos llamar por x, z, u , etc.
5. $(, ,,)$: símbolos de puntuación.

- Aún nos falta definir cómo se forman exactamente las fórmulas.
- Veamos ahora un pequeño adelanto:

Sea $S = \langle \langle A, GL \rangle, \langle padre \rangle, \langle Maria, Pedro, Andres, Juan \rangle \rangle$. Un conjunto de símbolos, donde

- GL , de aridad 1 tal que $GL(x)$ es verdadero ssi a x le gusta la lógica.
- A , de aridad 2 es tal que $A(x, y)$ es verdadero exactamente cuando x ayuda a y .

Además, la función $padre(x)$ representa al padre del objeto x .

¿Qué creen que expresan las siguientes fórmulas?

$$\forall y (GL(y) \rightarrow A(Juan, y))$$

$$\exists x A(x, Juan)$$

$$GL(Juan)$$

$$\exists y (A(Juan, y) \wedge \forall x (A(x, y)))$$

$$\exists y, z (A(Juan, y) \wedge z = padre(y) \wedge \forall x (A(z, x)))$$

- Aparte de especificar cómo se escriben las fórmulas debemos darle una semántica.
- Notemos que los lenguajes de primer orden hablan de objetos, propiedades y funciones. Estos elementos del lenguaje deben tener una contra parte, en cierto dominio real (dominio de discurso).
- Es posible usar el meta-lenguaje matemático para describir el dominio de discurso a través de *estructuras*. Veremos esto más adelante...

Sintaxis de LPOP

- Ahora definiremos formalmente la sintaxis de LPOP.
- Partiremos con la definición de qué es un **término**.

Definición 14. *Sea \mathcal{L} un lenguaje de primer orden construido a partir de un conjunto S de símbolos. Un término se forma a partir de la aplicación sucesiva de las siguientes reglas.*

1. *Toda constante de S es un término.*
2. *Toda variable es un término.*
3. *Si f es una función de aridad n ($f \in S$) y t_1, t_2, \dots, t_n son términos entonces $f(t_1, t_2, \dots, t_n)$ es un término.*

En nuestro ejemplo anterior, los siguientes son términos

$x_1, y, Juan, padre(padre(Juan))$

- Usando esto como base podemos definir una fórmula

Definición 15. Una fórmula se obtiene, solamente, mediante una aplicación finita de las siguientes reglas:

1. Si t_1 y t_2 son términos, entonces $t_1 = t_2$ es una fórmula.
 2. Si P es un símbolo de predicado n -ario y t_1, \dots, t_n son términos, entonces $P(t_1, t_2, \dots, t_n)$ es una fórmula.
 3. Si φ y ψ son fórmulas, entonces $\neg\varphi$ y $(\varphi * \psi)$ son fórmulas ($*$ es un conectivo binario).
 4. Si ϕ es una fórmula y x es una variable, entonces $\exists x\phi$ y $\forall x\phi$ también son fórmulas.
- El lenguaje de primer orden de todas las fórmulas que se generan a partir de un conjunto de símbolos S se anota como $L(S)$.
 - Continuando con nuestro ejemplo, las siguientes son fórmulas del lenguaje:

$$\forall x(A(x, z) \rightarrow A(x, \text{padre}(u))),$$

$$\forall x\forall yA(x, y), \tag{*}$$

$$\forall x(A(y, \text{Juan}) \rightarrow \exists y(GL(y) \wedge \neg A(y, x))),$$

$$\exists yA(x, y). \tag{**}$$

La fórmula (*) se acostumbra a escribir como $\forall xyA(x, y)$

En la fórmula (**) la variable x no está afectada por ningún cuantificador. En este caso decimos que x es una variable libre.

Además, las relaciones binarias también se pueden anotar con notación infija. De esta manera $A(x, y)$ se escribe como xAy .

- **Definición 16.** *Una fórmula del lenguaje φ es una oración. Si no tiene variables libres.*

Otro Ejemplo de LPOP

- Supongamos el siguiente conjunto de símbolos

$$S = \langle\langle <, > \rangle, \langle s, + \rangle, \langle 0, 1 \rangle\rangle,$$

- Podemos escribir el siguiente conjunto de fórmulas:

$$\forall x 0 < s(x)$$

$$\forall xyz((x < y \wedge y < z) \rightarrow x < z)$$

$$\forall x x + 1 = s(x)$$

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

$$\forall x x + 0 = x$$

- ¿De qué dominio real están hablando estas fórmulas?
- Si pensamos que estas fórmulas están hablando acerca de los naturales y que $s(x)$ representa al sucesor del natural x , entonces, estas fórmulas están describiendo propiedades de la desigualdad y de la suma.

Estructuras

- El dominio de discurso lo describiremos como una **estructura**.
- Una estructura es un conjunto formado por:
 - Un conjunto A no vacío de **objetos**. Si estamos hablando de los naturales, este conjunto es \mathbb{N}
 - Un conjunto \mathbf{R}^A de **relaciones**. Una relación R^A sobre A es n -aria si $R^A \subseteq A^n$. Estas son las relaciones que cumplen los elementos del dominio.
En el caso de los naturales, podríamos escoger la relación $<^{\mathbb{N}} \subseteq \mathbb{N} \times \mathbb{N}$ o la relación $\text{primo}^{\mathbb{N}} \subseteq \mathbb{N}$
 - Un conjunto \mathbf{F}^A de **funciones**. Una función n -aria f^A recibe elementos del dominio y retorna un elemento del dominio, es decir

$$f^A : A^n \rightarrow A.$$

En el caso de los naturales, podríamos escoger la multiplicación $(\cdot^{\mathbb{N}})$ y la suma $(+^{\mathbb{N}})$

- Un conjunto de **constantes** distinguidas. C^A puede denotar una constante en el conjunto A . Obviamente, $C^A \in A$.
En el caso de los naturales podríamos elegir a $0^{\mathbb{N}}$ y a $1^{\mathbb{N}}$.

Definición 17. *Una estructura se anota formalmente como una tupla*

$$\mathfrak{E} = \langle A, \langle R^A, \dots \rangle, \langle f^A, \dots \rangle, \langle C^A, \dots \rangle \rangle,$$

en la cual A es un conjunto y R^A , f^A y C^A son, respectivamente, una relación, una función y una constante sobre A con las características descritas anteriormente.

Por ejemplo, una estructura sobre los naturales puede ser la siguiente:

$$\mathfrak{N} = \langle \mathbb{N}, \langle \langle \cdot^{\mathbb{N}}, \text{primo}^{\mathbb{N}} \rangle, \langle +^{\mathbb{N}}, \cdot^{\mathbb{N}} \rangle, \langle 0^{\mathbb{N}}, 1^{\mathbb{N}} \rangle \rangle$$

- Si un lenguaje \mathcal{L} de primer orden habla acerca de cierta estructura, entonces el conjunto de símbolos S utilizados por el lenguaje debe ser **compatible** con los elementos de la estructura.

Por ejemplo, el conjunto de símbolos

$$S = \langle \langle R, \dots \rangle, \langle f, \dots \rangle, \langle C \rangle \rangle$$

es compatible con la estructura

$$\mathfrak{E} = \langle A, \langle R^A, \dots \rangle, \langle f^A, \dots \rangle, \langle C^A \rangle \rangle$$

cuando hay una correspondencia exacta entre los elementos y sus símbolos (incluyendo las aridades).

En este caso decimos que

- R es interpretado por R^A
- f es interpretado por f^A , y
- C es interpretado por C^A .

- Los siguientes son ejemplos de estructuras compatibles:

$$S = \langle \langle \langle, primo \rangle, \langle +, \cdot \rangle, \langle 0, 1 \rangle \rangle \text{ y } \mathfrak{N}_1 = \langle \mathbb{N}, \langle \langle^{\mathbb{N}}, primo^{\mathbb{N}} \rangle, \langle +^{\mathbb{N}}, \cdot^{\mathbb{N}} \rangle, \langle 0^{\mathbb{N}}, 1^{\mathbb{N}} \rangle \rangle$$

$$S = \langle \langle \langle, primo \rangle, \langle +, \cdot \rangle, \{0, 1\} \rangle \text{ y } \mathfrak{N}_2 = \langle \mathbb{N}, \langle \langle^{\mathbb{N}}, impar^{\mathbb{N}} \rangle, \langle +^{\mathbb{N}}, \cdot^{\mathbb{N}} \rangle, \langle 1^{\mathbb{N}}, 0^{\mathbb{N}} \rangle \rangle$$

- Nótese que en el segundo ejemplo no existe una correspondencia “natural” entre los símbolos utilizados y las propiedades que representan. Este fenómeno siempre ocurre en lógica simbólica.
- Siempre debemos recordar que los símbolos son solamente símbolos.
- Bajo este esquema en el cual la realidad es representada mediante símbolos nos preocupa ahora saber cuándo una fórmula es verdadera.

Por ejemplo, ¿qué significa la siguiente fórmula

$$\forall x (primo(x) \rightarrow primo(x + 2))$$

cuando la interpretamos con \mathfrak{N}_1 ?

¿qué significa cuando la interpretamos con \mathfrak{N}_2 ?

¿bajo qué interpretación esta fórmula es verdadera?

¿es \mathfrak{N}_2 la única estructura que hace a la fórmula verdadera?

¿podemos escribir un conjunto de fórmulas que sea hecho verdadero sólo por una interpretación dada por la estructura \mathfrak{N}_2 y por **ninguna** otra?

- Si queremos usar la lógica de primer orden para *razonar* acerca de lo que ocurre en el mundo, deberemos ser capaces de describir lógicamente el mundo sin que exista la posibilidad a que las teorías sean verdaderas en estructuras que no tienen nada que ver con el mundo que estamos modelando.
- Más adelante veremos que esto puede ser no trivial...
- De lo que sí debiéramos estar seguros es que para ser capaces de modelar dominios en forma lógica deberemos entender claramente cuándo una fórmula es verdadera en una cierta estructura.
- Antes de esto, refinaremos nuestro concepto de interpretación.

Interpretación de Términos

- Hasta el momento, tenemos una idea “más o menos” clara de cómo se interpretan las relaciones y funciones.
- La pregunta es ¿cómo interpretamos un término?
- Debemos dar una respuesta para los tres tipos de términos:
 - constantes,
 - variables,
 - $f(t_1, t_2, \dots, t_n)$, donde t_1, \dots, t_n son términos.
- Al menos para el caso de las constantes debería ser bastante claro...
- Sin embargo, necesitamos dar una interpretación a las variables. Si x es una variable, ¿qué objeto del dominio le corresponde?
- Necesitamos una función de asignación, que asigne valores a las variables.

- Sea

$$S = \{\langle R, \dots \rangle, \langle f, \dots \rangle, \langle C, \dots \rangle\}$$

un conjunto de símbolos. Si llamamos $Var(L(S))$ al conjunto de variables de un lenguaje de primer orden, entonces β es una función de asignación tal que

$$\beta : Var(L(S)) \rightarrow A.$$

- Formalmente, sea

$$S = \langle \langle R, \dots \rangle, \langle f, \dots \rangle, \langle C, \dots \rangle \rangle$$

un conjunto de símbolos y

$$\mathfrak{E} = \langle A, \langle R^A, \dots \rangle, \langle f^A, \dots \rangle, \langle C^A \rangle \rangle$$

una estructura compatible y β una función de asignación, entonces una **interpretación** es un par $\mathcal{I} = \langle \mathfrak{E}, \beta \rangle$, definida por:

1. $\mathcal{I}(C) := C^A$.
2. $\mathcal{I}(x) := \beta(x)$, con $x \in Var(L(S))$.
3. $\mathcal{I}(f(t_1, \dots, t_n)) := f^A(\mathcal{I}(t_1), \dots, \mathcal{I}(t_n))$, con $x \in Var(L(S))$.

Valor de Verdad de Fórmulas

- Tal como en el caso proposicional, nos interesa saber cuándo una fórmula es verdadera.
- En LP, definimos cuando una fórmula era verdadera dada una asignación de valor de verdad para cada una de las variables proposicionales del lenguaje. Es decir, definimos cuándo $\sigma \models \varphi$.
- En lógica de primer orden no hay valuaciones, sino interpretaciones, por lo tanto nos preocupamos de definir cuándo una fórmula es verdadera bajo una interpretación:

$$\mathcal{I} \models \varphi \quad (\varphi \in L(S)).$$

- Deberemos definir esto en forma inductiva para todas las fórmulas posibles del lenguaje.

Definición 18. *Sea $L(S)$ un lenguaje de primer orden y $\varphi \in L(S)$. Entonces:*

1. Si φ es de la forma $t = s$ entonces

$$\mathcal{I} \models \varphi \text{ ssi } \mathcal{I}(t) = \mathcal{I}(s)$$

2. Si φ es de la forma $R(t_1, \dots, t_n)$ entonces

$$\mathcal{I} \models \varphi \text{ ssi } (\mathcal{I}(t_1), \dots, \mathcal{I}(t_n)) \in R^A$$

3. Si φ es de la forma $\neg\psi$ entonces

$$\mathcal{I} \models \varphi \text{ ssi no se cumple que } \mathcal{I} \models \psi$$

4. Si φ es de la forma $\psi \wedge \chi$ entonces

$$\mathcal{I} \models \varphi \text{ ssi } \mathcal{I} \models \psi \text{ y } \mathcal{I} \models \chi$$

5. Si φ es de la forma $\psi \vee \chi$ entonces

$$\mathcal{I} \models \varphi \text{ ssi } \mathcal{I} \models \psi \text{ o } \mathcal{I} \models \chi$$

6. Si φ es de la forma $\psi \rightarrow \chi$ entonces

$$\mathcal{I} \models \varphi \text{ ssi } \mathcal{I} \models \chi \text{ o no se cumple que } \mathcal{I} \models \psi$$

7. Si φ es de la forma $\psi \leftrightarrow \chi$ entonces

$$\mathcal{I} \models \varphi \text{ ssi } \mathcal{I} \models \psi \text{ exactamente cuando } \mathcal{I} \models \chi$$

8. Si φ es de la forma $\exists x \psi$ entonces

$$\mathcal{I} \models \varphi \text{ ssi } \mathcal{I}_a^x \models \psi \text{ con } a \in A$$

Aquí, la notación \mathcal{I}_a^x implica reemplazar la asignación de valor de x por el objeto a en la función de asignación β .

9. Si φ es de la forma $\forall x \psi$ entonces

$$\mathcal{I} \models \varphi \text{ ssi } \mathcal{I}_a^x \models \psi \text{ para todo } a \in A$$

- **Definición 19.** Una fórmula φ de $L(S)$ es satisfacible si existe una interpretación $\mathcal{I} = \langle \mathfrak{E}, \beta \rangle$ tal que

$$\mathcal{I} \models \varphi$$

- **Definición 20.** *Una fórmula φ de $L(S)$ es válida en la estructura \mathfrak{E} (compatible con S) si ésta es hecha verdadera bajo cualquier asignación β .*

$$\mathfrak{E} \models \varphi \text{ ssi } \langle \mathfrak{E}, \beta \rangle \models \varphi \text{ para todo } \beta$$

- **Definición 21.** *Sea \mathcal{I} una interpretación que hace verdadera a una fórmula $\varphi \in L(P)$. Entonces se dice que \mathcal{I} es un **modelo** para esta fórmula.*
- **Definición 22.** *Sea Σ un conjunto de fórmulas en un lenguaje de primer orden $L(S)$, decimos que*

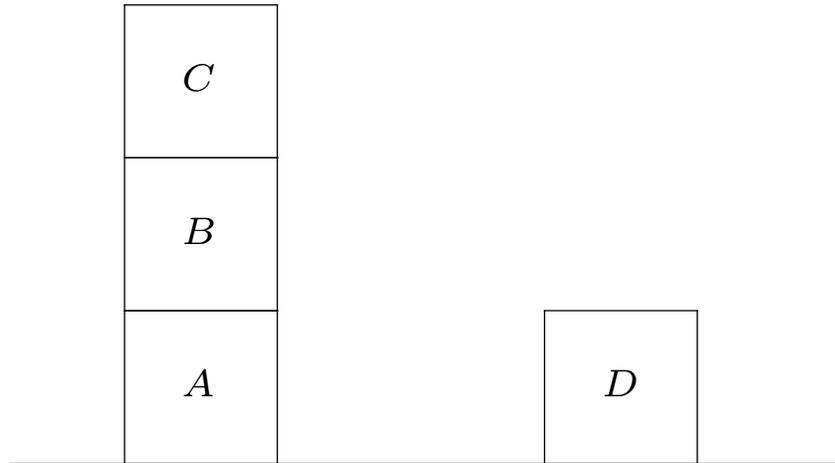
$$\mathcal{I} \models \Sigma \text{ ssi } \mathcal{I} \models \varphi \text{ para todo } \varphi \in \Sigma$$

- **Definición 23. [Consecuencia Lógica]** *Sea Σ un conjunto de oraciones en $L(S)$ y φ es una oración en $L(S)$. Entonces φ es consecuencia lógica de Σ ssi,*

$$\mathcal{I} \models \Sigma \text{ entonces } \mathcal{I} \models \varphi$$

Otro Ejemplo

- Supongamos las siguientes situaciones en el dominio de los bloques:



Podríamos usar la estructura $\mathfrak{B} = \langle U, \{Sobre^U\}, \{A, B, C, D, M\} \rangle$ para modelar este dominio, donde:

- $U = \{A, B, C, D, M\}$.
 - $Sobre^U = \{(A, M), (B, A), (C, B), (D, M)\}$
- La interpretación $\mathcal{I} = \langle \mathfrak{B}, \beta \rangle$, para un β arbitrario es modelo del siguiente conjunto de fórmulas sobre $S = \{\{Sobre\}, \{B_A, B_B, B_C, B_D, M\}\}$

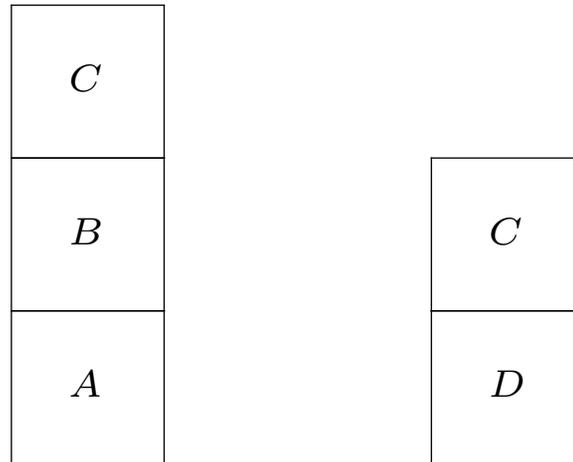
$$\forall x (Sobre(x, M) \rightarrow x = B_A \vee x = B_D)$$
$$Sobre(B_B, B_A) \wedge Sobre(B_C, B_B)$$

- Si consideramos, ahora, una relación binaria extra *ArribaDe*, tal que *ArribaDe*(*x*, *y*) es verdadera si y sólo si el objeto *x* está arriba de *y*, y agregamos el siguiente axioma:

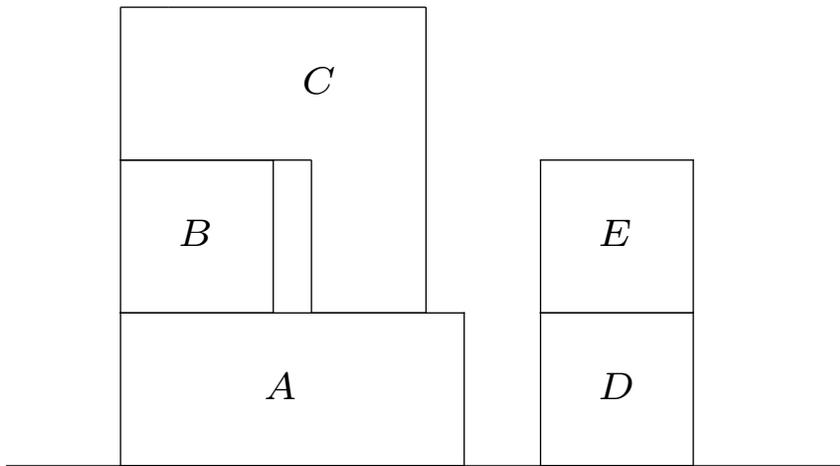
$$\forall xy (ArribaDe(x, y) \leftrightarrow Sobre(x, y) \vee Sobre(x, z) \wedge ArribaDe(z, y))$$

La interpretación, adecuadamente modificada, seguiría siendo modelo de la teoría.

- Una pregunta natural a hacerse es: ¿tiene esta teoría otro modelo? La respuesta es SÍ, y muchos más...



- Mostramos sólo dos de ellos:



- ¿Hay algún problema con la teoría?
- La respuesta a esta pregunta dependerá de qué es lo que queremos hacer con ella.

- Si esta representa hechos válidos, entonces es suficiente.
- Si queremos hacer deducción o **razonar** acerca de los hechos que son verdaderos en este dominio o no, necesitamos una mejor teoría.
- Dicha teoría debe *forzar* a que todas los modelos de esta representen el mundo que se quiere representar.
- Un arreglo para esta teoría es el siguiente:

$$\forall x(Sobre(x, M) \leftrightarrow x = B_A \vee x = B_D),$$

$$\forall x(Sobre(x, B_A) \leftrightarrow x = B_B),$$

$$\forall x(Sobre(x, B_B) \leftrightarrow x = B_C),$$

$$\forall x \neg Sobre(x, B_C),$$

$$\forall x \neg Sobre(x, B_D).$$

- Recordemos, además, que una interpretación podría asignar a un objeto del dominio dos símbolos de constante distintos del lenguaje. Por ejemplo, el objeto

A podría estar designado por B_A y B_B al mismo tiempo y la teoría seguiría teniendo un modelo.

- Esta distinción se hace agregando axiomas de nombres únicos. Los axiomas para este caso son varios. A continuación veremos algunos:

$$\begin{aligned}M \neq B_A, & \quad M \neq B_B \quad M \neq B_C, \\M \neq B_D, & \quad B_A \neq B_B, B_A \neq B_C, \\B_A \neq B_D, & \quad \dots\end{aligned}$$

- Lo que estamos logrando con esto es que cualquier modelo de la teoría tenga propiedades con la **misma extensión** para cada uno de sus predicados.
- Una condición suficiente para asegurar es que la teoría sea **definicional**, es decir, que defina por completo la extensión de los predicados.
- Esto se traduce en que para todo predicado n -ario P de la teoría exista un axioma que establece que

$$\forall \mathbf{x} (P(\mathbf{x}) \leftrightarrow \varphi),$$

donde φ es una fórmula que no tiene variables libres y \mathbf{x} es una tupla de n variables.

$$\forall x(Sobre(x, y) \leftrightarrow (y = M \wedge (x = B_A \vee x = B_D)) \vee \\ (y = B_A \wedge x = B_B) \\ (y = B_B \wedge x = B_C)).$$

y que hay axiomas de nombres únicos para objetos del dominio.

- Usando la semántica ya definida, podemos demostrar que la siguiente fórmula es consecuencia lógica de nuestra teoría.

$$\forall x \neg Sobre(x, x)$$

En efecto podemos demostrarlo por contradicción

Supongamos que hay un objeto z tal que $Sobre(z, z)$, del axioma de definición de $Sobre$ se tiene que

$$(z = M \wedge (z = B_A \vee z = B_D)) \vee (z = B_A \wedge z = B_B) \vee (z = B_B \wedge z = B_C)$$

Que evidentemente contradice a los axiomas de nombres únicos, por lo que no puede existir tal z y luego $\forall x \neg \text{Sobre}(x, x)$.

- La demostración que acabamos de hacer ha sido posible porque tenemos un conocimiento certero sobre los modelos de la teoría.
- Sería ideal que, tal como en el caso de LP, en LPOP tuviéramos un sistema formal deductivo, mediante el cual no requiramos evidencia explícita de las estructuras que lo modelan.
- A continuación, veremos un sistema deductivo para lógica de primer orden.

Un sistema deductivo para Lógica de Primer Orden

- Al igual que en LP, en LPO existen fórmulas que son siempre verdaderas.
- A partir de estas fórmulas, podremos construir un sistema deductivo, con el cual se podrán derivar fórmulas correctas.
- Por ejemplo, las siguientes fórmulas son universalmente válidas:

$$\models P(x) \rightarrow (Q(x) \rightarrow P(x)),$$

Esta fórmula es una instancia de una tautología de LP. En general, con cualquier instancia de tautología podremos obtener una fórmula universalmente.

- En particular, a partir del esquema de axiomas de Hilbert, podemos obtener:

$$(P(x) \rightarrow (Q(y) \rightarrow R(z))) \rightarrow ((P(x) \rightarrow Q(y)) \rightarrow (P(x) \rightarrow R(z)))$$

- Sin embargo, instanciaciones de estos esquemas de axiomas no son suficientes para realizar todo el razonamiento de primer orden.

- Veamos ahora algunas fórmulas universalmente válidas que involucran cuantificación:

$$(\forall x P(x) \rightarrow P(C)),$$

$$(P(y) \rightarrow \exists x P(x)),$$

$$(\forall y P(y) \rightarrow \exists x P(x)),$$

$$(\neg \forall x P(x) \rightarrow \exists x \neg P(x)).$$

- Las siguientes fórmulas, sin embargo, no lo son:

$$(\exists x P(x) \rightarrow \forall x P(x)),$$

$$\forall x (P(x) \rightarrow P(C)),$$

$$(\exists x \neg P(x) \rightarrow \neg \exists y P(y))$$

El sistema deductivo

- Un sistema deductivo de Hilbert para LPO consta de:
 - Esquemas axiomáticos
 - Reglas de deducción.
- Los esquemas axiomáticos para LPO son los de LP, más axiomas para la cuantificación universal ⁴:
 1. $\varphi \rightarrow (\psi \rightarrow \varphi)$.
 2. $(\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$
 3. $(\neg\varphi \rightarrow \neg\psi) \rightarrow ((\neg\varphi \rightarrow \psi) \rightarrow \varphi)$.
 4. $\forall x\varphi(x) \rightarrow \varphi(t)$
 5. $\varphi(t) \rightarrow \exists x\varphi(x)$
 6. $\exists x\varphi(x) \leftrightarrow \neg\forall x\neg\varphi(x)$.

⁴Aquí t denota un término arbitrario, en particular puede ser una variable o una constante

- Además, debemos agregar los siguientes axiomas para igualdad:

$$\forall x (x = x)$$

$$\forall x (x = y \rightarrow y = x)$$

$$\forall x (x = y \wedge y = z \rightarrow x = z)$$

Para todo predicado n -ario P y función m -aria f ⁵:

$$\forall \mathbf{x} \mathbf{y} P(\mathbf{x}) \wedge \mathbf{x} = \mathbf{y} \rightarrow P(\mathbf{y}),$$

$$\forall \mathbf{x} \mathbf{y} \mathbf{x} = \mathbf{y} \rightarrow f(\mathbf{x}) = f(\mathbf{y}).$$

- Las reglas de deducción son las siguientes:

1. Modus Ponens, igual que en LP

$$\frac{\varphi \rightarrow \psi, \varphi}{\psi}$$

⁵Aquí \mathbf{x} representa a una tupla de variables.

2. Regla de Generalización. Cuando y no aparece libre en φ

$$\frac{\varphi \rightarrow \psi(y)}{\varphi \rightarrow \forall x \psi(x)}$$

Nótese que φ puede ser una fórmula siempre válida, con lo que la regla de generalización:

$$\frac{\psi(y)}{\forall x \psi(x)}$$

es un caso particular de la anterior.

- Una demostración formal de una fórmula φ a partir de un conjunto de fórmulas Σ es una secuencia de fórmulas $\phi_1, \phi_2, \dots, \phi_n$ donde $\phi_n = \varphi$ y, para todo $1 \leq i \leq n$,
 - $\phi_i \in \Sigma$, o
 - ϕ_i es un axioma lógico, o
 - ϕ_i se obtiene de una regla de deducción a partir de fórmulas ϕ_k y ϕ_j ($k < j < i$)
- Cuando φ se obtiene de una demostración formal a partir de Σ , decimos que

$$\Sigma \vdash \varphi.$$

- Ejercicio: Demuestre que

$$\{\forall x (P(x) \rightarrow Q(x)), \forall x P(x)\} \vdash \forall x Q(x)$$

1. $\forall x (P(x) \rightarrow Q(x))$ (de Σ)
2. $(P(p) \rightarrow Q(p))$. (esquema de axioma 4 en 1)
3. $\forall x P(x)$ (de Σ)
4. $P(p)$. (esquema de axioma 4 en 3)
5. $Q(p)$. (modus ponens entre 2 y 4)
6. $\forall x Q(x)$ (generalización de 5)

Propiedades del Sistema Deductivo

- Cabe preguntarnos ahora, qué propiedades tiene este sistema deductivo.
- Veremos que, afortunadamente, muchas de las propiedades que se tenían en LP, también se cumplen en LPO.
- **Teorema 2. [de Corrección]** *Sea Σ un conjunto de oraciones y φ una oración, entonces*

$$\text{si } \Sigma \vdash \varphi \text{ entonces } \Sigma \models \varphi$$

La demostración de este teorema es idéntica a la de LP, puesto que los esquemas de axiomas y reglas de deducción siempre preservan la verdad.

- **Teorema 3. [de Compleción de Gödel]** *Sea Σ un conjunto de oraciones y φ una oración, entonces*

$$\text{si } \Sigma \models \varphi \text{ entonces } \Sigma \vdash \varphi$$

- **Teorema 4. [de Compacidad o Finitud]** *Sea Σ es un conjunto de oraciones y*

φ es una oración, entonces

Σ es satisfacible ssi todo subconjunto finito de Σ lo es

Fórmulas Prenex

- Es una forma normal de fórmulas de primer orden.
- Una fórmula prenex sólo tiene cuantificadores al comienzo de ésta. Por ejemplo:

$$\forall xy\exists z (P(x, y) \rightarrow R(x, y, z))$$

es una fórmula prenex.

- Formalmente, una fórmula prenex se escribe como

$$Q_1x_1Q_2x_2 \dots Q_nx_n \Psi,$$

donde Q_i ($1 \leq i \leq n$) representa algún cuantificador (\forall o \exists) y donde Ψ no tiene cuantificadores.

- **Teorema 5.** *Sea φ una fórmula arbitraria de $L(S)$. Entonces existe una fórmula prenex ψ equivalente.*

- Antes de demostrar este teorema, veamos algunos ejemplos:

la fórmula

$$\forall x (P(x) \rightarrow \forall y Q(x, y))$$

es equivalente a

$$\forall x \forall y (P(x) \rightarrow Q(x, y))$$

y

$$P(x) \wedge \forall y R(y)$$

equivalente a

$$\forall y (P(x) \wedge R(y))$$

¿cómo podemos hacer esto en general?

- Es posible demostrar que si φ y ψ son fórmulas y x es una variable que no aparece en ψ o está cuantificada en ψ , entonces las siguientes fórmulas son equivalentes:

1. $\neg Qx \varphi$ y $\overline{Q}x \neg \varphi$
2. $(Qx \varphi) \circ \psi$ y $Qx (\varphi \circ \psi)$
3. $\psi \circ (Qx \varphi)$ y $Qx (\psi \circ \varphi)$

donde Q representa a algún cuantificador (\forall o \exists), \overline{Q} representa al cuantificador complementario⁶ representado por Q y \circ representa a \wedge o \vee .

- ¿Qué pasa si ψ tiene a x como una variable libre? Ejemplo: Encuentre una fórmula equivalente a:

$$\forall x P(x) \wedge \forall y Q(y, z) \wedge P(x, y)$$

en este caso no podemos aplicar directamente la transformación, deberemos renombrar la variable libre x y luego aplicar la regla.

⁶El cuantificador complementario de \forall es \exists y vice versa.

Renombrando x por u e y por v obtenemos:

$$\forall x(P(x) \wedge \forall y Q(y, z) \wedge P(u, v))$$

y luego

$$\forall x(\forall y (P(x) \wedge Q(y, z) \wedge P(u, v)))$$

que es equivalente a

$$\forall x \forall y (P(x) \wedge Q(y, z) \wedge P(u, v))$$

- El teorema se demuestra justificando que la aplicación de las transformaciones de arriba son suficientes para llevar cualquier fórmula a forma normal prenex.

Resolución de Primer Orden

- Tal como en LP, nos interesa encontrar un algoritmo implementable que permita hacer demostraciones de teoremas de primer orden en forma automática.
- En 1965, J.A. Robinson descubrió un método de resolución para primer orden.
- El método es bastante parecido al de resolución de LP.

- Supongamos que tenemos las siguientes dos cláusulas de primer orden:

$$P(x) \vee Q(y, z) \vee R(x, f(w))$$

y la cláusula

$$S(y) \vee \neg P(u)$$

Observemos que:

- Las variables en ambas cláusulas aparecen como libres.
- Buscamos encontrar una correspondencia entre resolución y consecuencia lógica por lo cual supondremos que todas las fórmulas están implícitamente cuantificadas universalmente (no queremos variables libres).
- Dado que la primera fórmula se cumple para todo x , podríamos inferir que, en particular, se cumple para un objeto cualquiera C .
- Si lo mismo decimos acerca de la segunda cláusula tendremos que, se cumple que

$$P(C) \vee Q(y, z) \vee R(C, f(w))$$

y la cláusula

$$S(y) \vee \neg P(C)$$

- Dada tal sustitución, podemos utilizar la regla de resolución que ya conocemos y generar la siguiente cláusula:

$$S(y) \vee Q(y, z) \vee R(C, f(w))$$

¿Por qué?

- El proceso de asignar un valor a una variable, reemplazándola en toda la forma se llama **sustitución**.
- Si $\theta = \{x/b, y/f(a)\}$ y φ es una fórmula, entonces $\varphi\theta$ corresponde a la misma fórmula con todas las ocurrencias de x reemplazadas por b y todas las ocurrencias de y reemplazadas por $f(a)$.
- Formalmente, una sustitución es una función parcialmente definida $\theta : Var \rightarrow T(S)$, donde $T(S)$ es el conjunto de términos de un conjunto de símbolos S .
- Una sustitución que hace que dos fórmulas atómicas se hagan iguales se conoce como **unificador**.

Ejemplo:

La sustitución $\theta = \{x/f(A), y/g(u), z/A\}$ es un unificador para los literales⁷:

$$L_1 \equiv R(x, g(u)) \quad L_1 \equiv R(f(z), y)$$

porque $L_1\theta \equiv L_2\theta$.

- El sentido de igualdad (\equiv) usado aquí es meramente sintáctico y quiere decir que las expresiones son iguales caracter a caracter.

- Si θ es unificador, se usa

$$\{E_1, E_2, \dots, E_n\}\theta$$

para expresar el conjunto

$$\{E_1\theta, E_2\theta, \dots, E_n\theta\}$$

- Dos literales que unifican, pueden ser hechos unificar por muchas sustituciones. En nuestro ejemplo anterior, todas las siguientes sustituciones son unificadores

⁷Tal como en LP, un literal es una fórmula atómica o la negación de una.

de L_1 y L_2 :

$$\theta_1 = \{x/f(A), y/g(u), z/A\}$$

$$\theta_2 = \{x/f(z), y/g(u)\}$$

$$\theta_3 = \{x/f(f(B)), y/g(A), z/f(B), u/A\}$$

- De todos los unificadores posibles siempre existe al menos uno que es el menos restrictivo, en el sentido que es el que menos restringe futuras unificaciones.
- Este tipo de unificador se conoce como unificador más general (UMG).
- Un UMG asigna la menor cantidad de sustituciones posibles.
- Formalmente, un UMG θ de el conjunto de expresiones \mathbf{E} es tal que cualquier otro unificador θ' de \mathbf{E} se puede obtener primero mediante la aplicación de θ y después de alguna otra sustitución τ . Es decir,

$$\mathbf{E}\theta' = \mathbf{E}\theta\tau$$

- En nuestro ejemplo, θ_2 es el unificador más general. De hecho, si $\mathbf{E} = \{R(x, g(u)), R(f(z), y)\}$,

$$\mathbf{E}\theta_1 = (\mathbf{E}\theta_2)\{z/A\}$$

$$\mathbf{E}\theta_3 = (\mathbf{E}\theta_2)\{z/f(B), u/A\}$$

- Ahora estamos listos para formalizar una regla de resolución:

Sean $l_1 \vee l_2 \vee \dots \vee l_n$ y $l'_1 \vee l'_2 \vee \dots \vee l'_m$ cláusulas de primer orden. La regla de resolución es **aplicable** si existen l_i ($1 \leq i \leq n$) y l'_k ($1 \leq k \leq m$) tales que $l_i\theta$ y $l'_k\theta$ son uno la negación del otro (literales complementarios).

En este caso, la regla de resolución es la siguiente:

$$\frac{l_1 \vee l_2 \vee \dots \vee l_n \quad l'_1 \vee l'_2 \vee \dots \vee l'_m}{\bigvee_{i \in \{1, \dots, n\} - \{j\}} l_i\theta \vee \bigvee_{i \in \{1, \dots, m\} - \{k\}} l'_i\theta}$$

- Hasta el momento, tenemos un método de resolución que sirve para fórmulas de primer orden cuantificadas universalmente.

- ¿qué podemos hacer cuando queremos demostrar un hecho a partir de un conjunto de formulas con cuantificadores existenciales?
- La respuesta está en transformar una fórmula con cuantificadores varios a una que sólo tenga cuantificadores universales.
- Esto se puede hacer mediante **skolemización**.

Skolemización

- La *skolemización* (por Toraf Skolem) tiene por objeto transformar una fórmula a otra equivalente en forma normal prenex.
- Consideremos la siguiente fórmula:

$$\exists x P(x)$$

- Siempre podremos reemplazar la fórmula anterior por

$$P(C),$$

donde C es **una constante**.

- Pero, ¿cómo podemos transformar $\forall x \exists y R(x, y)$? Claramente, no nos sirve $\forall x R(x, C)$ ¿por qué?
- Sea φ una fórmula prenex, tal que

$$\forall x_1 \dots \forall x_k \exists x \varphi$$

es una oración.

La transformación de skolem le asocia a esta fórmula:

$$\forall x_1 \dots \forall x_k \varphi(x/f(x_1, \dots, x_k))$$

donde $\varphi(x/f(x_1, \dots, x_k))$ corresponde a la sustitución de x por $f(x_1, \dots, x_k)$ en φ .

f se conoce como una constante de Skolem, y es una constante nueva, que no debe tener ocurrencias en φ .

- Para la regla anterior, en caso que $k = 0$, se obtiene la fórmula

$$\exists x \varphi$$

la que se reemplaza por $\varphi(x/C)$ donde C es una constante nueva.

- Ejemplos:

1. $\forall x \forall y \exists z S(x, y, z)$ se transforma en $\forall x \forall y S(x, y, f(x, y))$.

2.

$$\forall x \exists y \forall z \exists u (P(x, y) \wedge Q(y, z) \rightarrow R(u))$$

se transforma en

$$\forall x \forall z (P(x, f(x)) \wedge Q(f(x), z) \rightarrow R(g(x, z)))$$

- **Teorema 6.** *Sea $\Sigma \in L(S)$ un conjunto de oraciones en forma normal prenex y sea Σ' un conjunto formado a partir de sucesivas aplicaciones de la transformación de Skolem. Entonces Σ tiene un modelo si y solo si Σ' también lo tiene.*

La demostración del teorema pasa por demostrar que

$$\forall x_1 \dots \forall x_k \exists x \varphi \leftrightarrow \forall x_1 \dots \forall x_k \varphi(x/f(x_1, \dots, x_k))$$

Lógica de Predicados de Primer Orden

Seminario de Matemáticas

Julio Ariel Hurtado Alegría

2013