Lógica y Computabilidad

2do cuatrimestre 2020 - **A DISTANCIA**

Departamento de Computación - FCEyN - UBA

Lógica de Primer Orden - clase 2

Lema de sustitución, sistema axiomático SQ, consecuencia sintáctica, teorema de la generalización, teorema de la generalización en constantes

Reemplazo de variables libres por términos

Sea $\mathcal{L} = \mathcal{C} \cup \mathcal{F} \cup \mathcal{P}$ un lenguaje fijo.

Sea $\varphi \in \mathrm{FORM}(\mathcal{L})$, $t \in \mathrm{TERM}(\mathcal{L})$ y $x \in \mathrm{VAR}$. $\varphi[x/t]$ es la fórmula obtenida a partir de φ sustituyendo todas las apariciones libres de la variable x por t

Por ejemplo, (para un lenguaje con símbolo de predicado binario P y símbolo de función unario f)

- $P(x,y)[x/f(z)] = P(f(z),y)$
- $P(x,y)[x/f(x)] = P(f(x),y)$
- $\big((\forall x)(\forall y)\ P(x,y)\big)[x/f(z)] = (\forall x)(\forall y)\ P(x,y)$
- $\big(P(x,y) \to (\forall x)(\forall y)\ P(x,y)\big)[x/f(z)] =$
  $P(f(z),y) \to (\forall x)(\forall y)\ P(x,y)$

Si $c \in \mathcal{C}$, $\varphi[c/t]$ es la fórmula obtenida a partir de φ sustituyendo todas las apariciones de la constante c por t

Variable reemplazable por un término

Sea $t \in \mathrm{TERM}(\mathcal{L})$, $x \in \mathrm{VAR}$, $\varphi \in \mathrm{FORM}(\mathcal{L})$.

Decimos que x es reemplazable por t en φ cuando

1. t es un término cerrado (i.e. no tiene variables) o
2. t tiene variables pero ninguna de ellas queda atrapada por un cuantificador en el reemplazo $\varphi[x/t]$

Por ejemplo, (para un lenguaje con símbolo de predicado unario P y símbolo de función binaria f)
En

$$(\forall y)\big((\forall x)P(x) \to P(x)\big)$$

- x es reemplazable por z: $(\forall y)\big((\forall x)P(x) \to P(z)\big)$
- x es reemplazable por $f(x,z)$: $(\forall y)\big((\forall x)P(x) \to P(f(x,z))\big)$
- x no es reemplazable por $f(x,y)$: $(\forall y)\big((\forall x)P(x) \to P(f(x,y))\big)$

Lema de Sustitución

Lema

Si x es reemplazable por t en φ entonces

$$\mathcal{A} \models (\varphi[x/t])[v] \quad \textit{sii} \quad \mathcal{A} \models \varphi[v(x = \tilde{v}(t))].$$

Demostración.

Por inducción en la complejidad de φ.
(a veces escribo v por $\tilde{v}$)

- $\varphi = P(u)$ es atómica (u es término; el caso n-ario es similar).
  $\mathcal{A} \models P(u[x/t])[v]$ sii $\tilde{v}(u[x/t]) \in P_{\mathcal{A}}$
  sii (lema auxiliar que dice $v(u[x/t]) = v(x = v(t))(u)$)
  $v[x = \tilde{v}(t)](u) \in P_{\mathcal{A}}$ sii $\mathcal{A} \models \varphi[v(x = \tilde{v}(t))]$.
- φ es de la forma $\neg\psi$ o de la forma $\psi \to \rho$. Directo.

(sigue $\to$)

$\square$

Lema de Sustitución

Demostración (cont.)

- φ es de la forma $(\forall y)\ \psi$.
  Sup. x no aparece libre en φ. Entonces v y $v[x = v(t)]$ coinciden en todas las variables que aparecen libres en φ. Además, $\varphi = \varphi[x/t]$. Inmediato.

  Sup. x aparece libre en φ. Como x es reemplazable por t en φ, y no ocurre en t. Luego para todo $d \in A$,
  $$v(t) = v(y = d)(t). \tag{1}$$
  Además, x es reemplazable por t en ψ. Como $x \neq y$,
  $$\varphi[x/t] = ((\forall y)\ \psi)[x/t] = (\forall y)\ (\psi[x/t]).$$
  Luego
  $$\begin{array}{lcl} \mathcal{A} \models \varphi[x/t][v] & \text{sii (def.)} & \text{para todo } d \in A,\ \mathcal{A} \models \psi[x/t][v(y = d)] \\ & \text{sii (HI)} & \text{para todo } d \in A,\ \mathcal{A} \models \psi[\underbrace{v(y = d)}_{w}(x = w(t))] \\ & \text{sii (1)} & \text{para todo } d \in A,\ \mathcal{A} \models \psi[v(y = d)(x = v(t))] \\ & \text{sii } (x \neq y) & \text{para todo } d \in A,\ \mathcal{A} \models \psi[v(x = v(t))(y = d)] \\ & \text{sii (def.)} & \mathcal{A} \models \varphi[v(x = v(t))] \end{array}$$

Mecanismo deductivo SQ (para un lenguaje fijo $\mathcal{L}$)

Para un lenguaje fijo $\mathcal{L}$

- axiomas. Sean $\varphi, \psi, \rho \in \text{FORM}(\mathcal{L})$, $x \in \text{VAR}$, $t \in \text{TERM}(\mathcal{L})$

  SQ1 $\varphi \to (\psi \to \varphi)$

  SQ2 $(\varphi \to (\psi \to \rho)) \to ((\varphi \to \psi) \to (\varphi \to \rho))$

  SQ3 $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$

  SQ4 $(\forall x)\varphi \to \varphi[x/t]$ si x es reemplazable por t en φ

  SQ5 $\varphi \to (\forall x)\varphi$ si x no aparece libre en φ

  SQ6 $(\forall x)(\varphi \to \psi) \to ((\forall x)\varphi \to (\forall x)\psi)$

  SQ7 si φ es un axioma entonces $(\forall x)\varphi$ también es un axioma

- regla de inferencia

  MP Sean $\varphi, \psi \in \text{FORM}(\mathcal{L})$. ψ es una consecuencia inmediata de $\varphi \to \psi$ y φ

Consecuencia sintáctica, demostraciones, teoremas, teorías

Fijamos un lenguaje $\mathcal{L}$. Sea $\Gamma \subseteq \mathsf{FORM}(\mathcal{L})$ y $\varphi \in \mathsf{FORM}(\mathcal{L})$

1. una demostración de φ en SQ es una cadena finita y no vacía

   $$\varphi_1, \dots, \varphi_n$$

   de fórmulas de $\mathcal{L}$ tal que $\varphi_n = \varphi$ y
   - φ_i es un axioma o
   - φ_i es una consecuencia inmediata de φ_k, φ_l, $k, l < i$

   En este caso, decimos que φ es un teorema ($\vdash \varphi$).

2. φ es una consecuencia sintáctica de Γ ($\Gamma \vdash \varphi$) si existe una cadena finita y no vacía

   $$\varphi_1, \dots, \varphi_n$$

   de fórmulas de $\mathcal{L}$ tal que $\varphi_n = \varphi$ y
   - φ_i es un axioma o
   - $\varphi_i \in \Gamma$ o
   - φ_i es una consecuencia inmediata de φ_k, φ_l, $k, l < i$

   Aquí, $\varphi_1, \dots, \varphi_n$ se llama derivación de φ a partir de Γ. Γ se llama teoría. Decimos que φ es un teorema de la teoría Γ.

Ejemplo $\Gamma = \{(\forall x)(\varphi[z/x])\} \vdash (\forall z)\varphi$ (x no aparece en φ)

1.	$(\forall z)\big((\forall x)(\varphi[z/x]) \to \varphi\big)$	SQ4+SQ7
2.	$(\forall z)\big((\forall x)(\varphi[z/x]) \to \varphi\big) \to \big((\forall z)(\forall x)(\varphi[z/x]) \to (\forall z)\varphi\big)$	SQ6
3.	$(\forall z)(\forall x)(\varphi[z/x]) \to (\forall z)\varphi$	MP 1,2
4.	$(\forall x)(\varphi[z/x]) \to (\forall z)(\forall x)(\varphi[z/x])$	SQ5
5.	$(\forall x)(\varphi[z/x])$	Γ
6.	$(\forall z)(\forall x)(\varphi[z/x])$	MP 4,5
7.	$(\forall z)\varphi$	MP 3,6

Observar

- paso 1: x es reemplazable por z en $\varphi[z/x]$
- paso 1: $\varphi[z/x][x/z] = \varphi$
- paso 4: z no aparece libre en $(\forall x)(\varphi[z/x])$

Correctitud y consistencia

Teorema (Correctitud)

El sistema SQ es correcto, i.e. si $\Gamma \vdash \varphi$ *entonces* $\Gamma \models \varphi$.

Teorema (Consistencia)

El sistema SQ es consistente, i.e. no existe $\varphi \in \mathrm{FORM}(\mathcal{L})$ *tal que*

$$\vdash \varphi \qquad \textit{y} \qquad \vdash \neg\varphi$$

Resultados similares a los de *SP*

Teorema (de la Deducción)

Si $\Gamma \cup \{\varphi\} \vdash \psi$ *entonces* $\Gamma \vdash \varphi \to \psi$

$\Gamma \subseteq \mathrm{FORM}(\mathcal{L})$ es consistente si no existe $\varphi \in \mathrm{FORM}(\mathcal{L})$ tal que

$$\Gamma \vdash \varphi \qquad \text{y} \qquad \Gamma \vdash \neg\varphi$$

Proposición

1. $\Gamma \cup \{\neg\varphi\}$ *es inconsistente sii* $\Gamma \vdash \varphi$
2. $\Gamma \cup \{\varphi\}$ *es inconsistente sii* $\Gamma \vdash \neg\varphi$

Teorema

Si Γ *es satisfacible, entonces* Γ *es consistente.*

Teorema

Si Γ *es inconsistente, entonces existe un subconjunto finito de* Γ *que es inconsistente.*

Instancias de esquemas tautológicos

- sea $\varphi(p_1, \ldots, p_n)$ una tautología de P con variables proposicionales $p_1, \ldots, p_n$.
- sean $\psi_1, \ldots, \psi_n$ fórmulas cualesquiera de primer orden
- $\varphi(\psi_1, \ldots, \psi_n)$ es una instancia de un esquema tautológico (reemplazar p_i por ψ_i en la fórmula original φ)

Proposición

Si φ es una instancia de un esquema tautológico entonces $\vdash \varphi$.

Por ejemplo, la fórmula de P

$$(p \wedge q) \rightarrow p$$

es tautología. Entonces

$$\vdash \big((\forall x)R(x) \wedge (\exists y)Q(y)\big) \rightarrow (\forall x)R(x)$$

Variantes alfabéticas

Sea $\mathcal{L} = \{0, S\}$ con igualdad y $\varphi \in \mathrm{FORM}(\mathcal{L})$ definida como

$$\varphi = x \neq 0 \to (\exists y)x = S(y)$$

En φ la variable x es reemplazable por z:

$$\varphi[x/z] = z \neq 0 \to (\exists y)z = S(y)$$

Sin embargo, la variable x no es reemplazable por y:

$$\varphi[x/y] = y \neq 0 \to (\exists y)y = S(y)$$

No habría habido problema si la fórmula original hubiese sido

$$\varphi' = x \neq 0 \to (\exists w)x = S(w)$$

φ' se llama variante alfabética de φ

Lema

Sea $\varphi \in \mathrm{FORM}(\mathcal{L})$. Dados $x \in \mathrm{VAR}$ y $t \in \mathrm{TERM}(\mathcal{L})$ podemos encontrar φ' (variante alfabética de φ) tal que

- $\{\varphi\} \vdash \varphi'$ *y* $\{\varphi'\} \vdash \varphi$
- *x es reemplazable por t en φ'*

Teorema de Generalización (TG)

Teorema

Si $\Gamma \vdash \varphi$ *y* x *no aparece libre en ninguna fórmula de* Γ*, entonces* $\Gamma \vdash (\forall x)\varphi$

Observar que es necesario pedir que x no aparezca libre en ninguna fórmula de Γ:

- $\{R(x)\} \not\models (\forall x)R(x)$
- entonces $\quad \{R(x)\} \nvdash (\forall x)R(x) \quad$ (por correctitud)

Demostración del teorema.

Planteo

> $P(n) =$ *para toda* ψ*,* Γ *y* x *tal que* $\Gamma \vdash \psi$ *y* x *no aparece libre en ninguna fórmula de* Γ*, si* $\psi_1, \ldots, \psi_n$ *es una derivación de* ψ *a partir de* Γ *entonces* $\Gamma \vdash (\forall x)\psi$

Demostración por inducción en n (detalles a continuación). $\square$

Demostración del TG (caso base)

$P(n)$ = para toda ψ, Γ y x tal que $\Gamma \vdash \psi$ y x no aparece libre en ninguna fórmula de Γ, si $\psi_1, \ldots, \psi_n$ es una derivación de ψ a partir de Γ entonces $\Gamma \vdash (\forall x)\psi$

Probamos $P(1)$:

- sea φ, Γ y x tal que x no aparece libre en Γ
- sea φ una derivación de φ a partir de Γ
- queremos ver que $\Gamma \vdash (\forall x)\varphi$

Hay 2 posibilidades:

1. φ es axioma de SQ $\overset{SQ7}{\Rightarrow} \vdash (\forall x)\varphi \Rightarrow \Gamma \vdash (\forall x)\varphi$
2. $\varphi \in \Gamma$ entonces
   - $\Gamma \vdash \varphi$
   - por hipótesis x no aparece libre en φ
   - por SQ5, $\vdash \varphi \rightarrow (\forall x)\varphi$
   - por MP, $\Gamma \vdash (\forall x)\varphi$

Demostración del TG (paso inductivo)

$P(n)$ = para toda ψ, Γ y x tal que $\Gamma \vdash \psi$ y x no aparece libre en ninguna fórmula de Γ, si $\psi_1, \dots, \psi_n$ es una derivación de ψ a partir de Γ entonces $\Gamma \vdash (\forall x)\psi$

Probamos $P(n)$:

- sea φ, Γ y x tal que x no aparece libre en Γ
- sea $\varphi_1, \dots, \varphi_n$ una derivación de φ a partir de Γ
- queremos ver que $\Gamma \vdash (\forall x)\varphi$
- HI: vale $P(m)$ para todo $m < n$

Hay 3 posibilidades:

1 y 2. φ es axioma de SQ o $\varphi \in \Gamma$: igual que en caso base.

3. φ se obtiene por MP de φ_i y φ_j ($i, j < n$): supongamos que $\varphi_j = \varphi_i \to \varphi$. Usamos HI 2 veces:
   - como $i < n$, vale $P(i)$, en particular, $\Gamma \vdash (\forall x)\varphi_i$
   - como $j < n$, vale $P(j)$, en particular, $\Gamma \vdash (\forall x)(\varphi_i \to \varphi)$

   por SQ6, $\vdash (\forall x)(\varphi_i \to \varphi) \to ((\forall x)\varphi_i \to (\forall x)\varphi)$
   usando MP 2 veces, $\Gamma \vdash (\forall x)\varphi$

Teorema de Generalización en Constantes (TGC)

Teorema

Supongamos que $\Gamma \vdash \varphi$ *y* c *es un símbolo de constante que no aparece en* Γ*. Entonces existe una variable* x *que no aparece en* φ *tal que* $\Gamma \vdash (\forall x)(\varphi[c/x])$*. Más aun, hay una derivación de* $(\forall x)(\varphi[c/x])$ *a partir de* Γ *en donde* c *no aparece.*

Idea de la demostración.

Sea $\varphi_1, \dots, \varphi_n$ una derivación de φ a partir de Γ.
Sea x la primera variable que no aparece en ninguna de las φ_i.

1. demostrar que $\varphi_1[c/x], \dots, \varphi_n[c/x]$
   1.1 es una derivación de $\varphi[c/x]$ a partir de Γ (por inducción en n)
   1.2 no contiene al símbolo de constante c
2. hay un $\Delta \subseteq \Gamma$ finito tal que $\Delta \vdash \varphi[c/x]$ con derivación que no usa c y tal que x no aparece libre en ninguna fórmula de Δ
   2.1 Δ es el conjunto de axiomas de Γ que se usan en $\varphi_1, \dots, \varphi_n$
3. por el TG, $\Delta \vdash (\forall x)(\varphi[c/x])$ con derivación que no usa c

$\square$

Consecuencias del TGC

Corolario

Supongamos que $\Gamma \vdash \varphi[z/c]$ *y* c *es un símbolo de constante que no aparece en* Γ *ni en* φ*. Entonces* $\Gamma \vdash (\forall z)\varphi$*. Más aun, hay una derivación de* $(\forall z)\varphi$ *a partir de* Γ *en donde* c *no aparece.*

Demostración.

- por el TGC, existe x tal que
  - x no aparece en $\varphi[z/c]$
  - $\Gamma \vdash (\forall x)\big(\varphi[z/c][c/x]\big)$
  - en esta última derivación no aparece c
- como c no aparece en φ, $\quad \varphi[z/c][c/x] = \varphi[z/x]$
- entonces $\quad \Gamma \vdash (\forall x)\big(\varphi[z/x]\big)$
- sabemos $\quad \vdash (\forall x)\big(\varphi[z/x]\big) \rightarrow (\forall z)\varphi$
  (aplicar el Teorema de la Deducción a derivación de hoja 8)
- por MP concluimos $\Gamma \vdash (\forall z)\varphi$
- en esta última derivación no aparece c

$\square$

Lenguajes con igualdad

Fijamos un lenguaje $\mathcal{L}$ con igualdad.
Para los lenguajes con igualdad, se considera el sistema $SQ^=$ con los axiomas y regla de inferencia de SQ, sumando estos dos axiomas

- axiomas adicionales para $SQ^=$. Sean $\varphi, \psi \in \text{FORM}(\mathcal{L})$, $x, y \in \text{VAR}$

  SQ$^=$1 $x = x$

  SQ$^=$2 $x = y \to (\varphi \to \psi)$ donde φ es atómica y ψ se obtiene de φ reemplazando x por y en cero o más lugares

Se puede probar que

- $SQ^=$ es consistente
- Si hay una derivación de φ en $SQ^=$ entonces φ es verdadera en toda $\mathcal{L}$-estructura en donde el $=$ se interpreta como la igualdad

Notas sobre computabilidad

Fijemos un lenguaje numerable $\mathcal{L}$. Se pueden codificar las fórmulas de FORM($\mathcal{L}$) con números naturales.

Igual que para la lógica proposicional:

- es computable la función

$$dem_{\mathcal{L}}(x) = \begin{cases} 1 & x \text{ es una demostración válida en } SQ \text{ para } \mathcal{L} \\ 0 & \text{si no} \end{cases}$$

- considerar el siguiente programa P:

$$\begin{array}{ll} [A] & \text{IF } dem_{\mathcal{L}}(D) = 1 \wedge D[|D|] = X \text{ GOTO } E \\ & D \leftarrow D + 1 \\ & \text{GOTO } A \end{array}$$

- φ es teorema de SQ para $\mathcal{L}$ sii $\#\varphi \in \text{dom}\Psi_P$
- el conjunto de teoremas del sistema SQ para $\mathcal{L}$ es c.e.
- ¿será el conjunto de teoremas de SQ para $\mathcal{L}$ computable?