Clase 25/09/2013

Tomado y editado de los apuntes de Pedro Sánchez Terraf

A pesar de haber ejercitado la realización de demostraciones en varias materias, es frecuente que el alumno consulte sobre la validez de una prueba, sobre la correctitud de un razonamiento. En este segmento estudiaremos formalmente el concepto de demostración, proporcionando elementos para que el alumno pueda decidir por sí mismo si una argumentación matemática es lógicamente correcta. Haremos esto para un fragmento relativamente simple de la lógica matemática llamado **Lógica Proposicional**.

Proposiciones

Las proposiciones representan afirmaciones. Estas afirmaciones se escriben con una notación muy particular: usamos conectivas lógicas como $\wedge$, $\vee$, $\to$, ... También se utilizan paréntesis como '(' y ')' para resolver ambigüedades, y variables proposicionales.

Es decir que las proposiciones serán ciertas secuencias, listas o cadenas (usamos estas tres palabras como sinónimos) de símbolos. Utilizaremos los siguientes símbolos. Al conjunto de símbolos permitidos se le llama *alfabeto*.

Alfabeto de la Lógica Proposicional

La lógica proposicional se escribirá con el siguiente alfabeto:

1. Símbolos proposicionales (en cantidad numerable): $p_0, p_1, \ldots, p_n, \ldots$;
2. Conectivos. Básicos: $\bot$, $\wedge$, $\to$. Derivados: $\neg$, $\vee$, $\leftrightarrow$, $\top$, $|$, ...;
3. Símbolos auxiliares: '(' y ')'.

Llamamos Σ al conjunto de estos símbolos, y Σ^* al conjunto de todas las cadenas de símbolos de Σ. Ejemplos de tales cadenas:

$p_0 p_3) \bot \wedge p_0$	$(()) \wedge \vee \to$	$p_0 \to p_1)$	$)p_0 \wedge p_5($	$(()p_3)$
$p_0 \wedge p_5$	$(p_0 \wedge p_5)$	$((p_0 \wedge p_5))$	p_3	(p_3)

Ejemplos de cadenas que **no** pertenecen a Σ^*:

llueve	$x \leq y$	$p \to q$	$p_0 \Rightarrow p_3$	$p_0 \to p_j$
$F \to V$	$\varphi \wedge \psi$	$(\varphi \wedge \psi)$	2 es par	$p_0 \,\square\, p_1$

Lenguaje de la Lógica Proposicional

No cualquier cadena de Σ^* denota una proposición.[1] A los *símbolos proposicionales* se los llama también *variables proposicionales*, y se define $\mathcal{V} = \{p_0, p_1, \ldots, p_n, \ldots\}$. Si agregamos el símbolo $\bot$, tenemos los *átomos* o *proposiciones atómicas*, y los designaremos con el nombre $At = \mathcal{V} \cup \{\bot\}$. El conectivo $\neg$ es unario, $\bot$ es nulario (corresponde a una *constante*) y el resto son binarios. Para designar un operador binario arbitrario, utilizaremos el meta-símbolo $\square$.[2]

Definición 1. El conjunto de las *proposiciones*, $PROP$, es el menor conjunto que cumple con las siguientes propiedades:

$\boxed{\varphi \in At}$ Para todo $\varphi \in At$, $\varphi \in PROP$.

$\boxed{(\neg\varphi)}$ Para toda φ en $PROP$, $(\neg\varphi)$ está en $PROP$.

$\boxed{(\varphi \square \psi)}$ Para todas φ, ψ en $PROP$, $(\varphi \square \psi)$ está en $PROP$.

Usaremos letras griegas φ, ψ, χ, ... para nombrar proposiciones arbitrarias. La última cláusula se vale del meta-símbolo $\square$ que representa un operador binario genérico y evita ser repetitivos. Si no deberíamos escribir una cláusula como esa para cada uno de los operadores binarios:

$\boxed{(\varphi \wedge \psi)}$ Para todas φ, ψ en $PROP$, $(\varphi \wedge \psi)$ está en $PROP$.

$\boxed{(\varphi \to \psi)}$ Para todas φ, ψ en $PROP$, $(\varphi \to \psi)$ está en $PROP$.

etcétera

Proposiciones por extensión

La definición dada establece que las siguientes cadenas son proposiciones:

1. Los átomos $\bot, p_0, p_1, \ldots, p_n, \ldots$ son las proposiciones atómicas.
2. Para cada proposición φ y ψ ya listada, y para cada conectivo binario $\square$, $(\neg\varphi)$ y $(\varphi \square \psi)$ son proposiciones un poco más complejas. Ejemplos: $(\neg\bot)$, $(\neg p_0)$, etc. Otros: $(\bot \wedge \bot)$, $(\bot \wedge p_0)$, etc.
3. Para cada proposición φ y ψ ya listada, y para cada conectivo binario $\square$, $(\neg\varphi)$ y $(\varphi \square \psi)$ son proposiciones un poco más complejas. Ejemplos: $(\neg(\neg\bot))$, $(\neg(\bot \wedge p_0))$, etc. Otros: $((\neg\bot) \wedge (p_0 \wedge p_1))$, $(\bot \wedge (p_0 \wedge p_1))$, etc.
4. etcétera

Esta enumeración de las **proposiciones por extensión** continúa indefinidamente, presentando en cada línea proposiciones más y más complejas porque en cada línea se puede concebir nuevas proposiciones de la forma $(\neg\varphi)$ y $(\varphi \square \psi)$ para cada proposición φ y ψ listada con anterioridad, y para cada operador binario $\square$. En efecto, todas las proposiciones de la primera línea son cadenas de un solo símbolo, en la segunda hay cadenas de cuatro símbolos y otras de cinco símbolos. En la tercera línea ya hay más variantes, pero en particular tenemos proposiciones de la forma $(\varphi \square \psi)$ donde φ y ψ denotan cadenas de cinco símbolos, por lo tanto $(\varphi \square \psi)$ denota otra cadena de trece símbolos. En la cuarta línea habrá nuevas cadenas de 29 símbolos, en la quinta de 61, en la sexta de 125, etc.

[1] ¿Cuáles de los ejemplos de cadenas de Σ^* enumeradas arriba lo hace?

[2] Le llamamos **meta** para indicar que no pertenece al alfabeto Σ.

Inducción y recursión

La definición del conjunto $PROP$ dice que es el **menor** conjunto que satisface las tres cláusulas ya explicadas. Ser el menor conjunto significa que $PROP$ no contiene ningún otro elemento que no sea producto de esas cláusulas. Nos permite deducir, por ejemplo, que p_0p_1 no pertenece a $PROP$ porque no es un átomo (y por ello no puede ser producto de la primera cláusula) ni comienza con un paréntesis que abre (y por ello, no puede ser producto de ninguna de las otras dos cláusulas). También nos permite deducir que las siguientes cadenas no pertenecen a $PROP$:

$p_0 \wedge p_1$	$((p_0 \wedge p_1))$	$\neg\bot$	(p_0)	$p_0 \wedge (p_0 \to p_1)$
$(p_0 \,\square\, p_1)$	$(\neg\varphi)$	$(\neg p_i)$	$(\ )$	$(\bot)$

Más interesante aún, que $PROP$ sea el **menor** conjunto que satisface las tres cláusulas implica que se puede demostrar propiedades sobre las proposiciones por inducción de la siguiente manera.

Teorema 2 (inducción en subfórmulas)**.** *Sea A un predicado sobre $PROP$. Luego $A(\varphi)$ es verdadero para toda $\varphi \in PROP$ si y sólo si:*

$\boxed{\varphi \in At}$ *Si φ es atómica, $A(\varphi)$ vale.*

$\boxed{(\neg\varphi)}$ *Si $A(\varphi)$ entonces $A((\neg\varphi))$.*

$\boxed{(\varphi \,\square\, \psi)}$ *Si $A(\varphi)$ y $A(\psi)$ entonces $A((\varphi \,\square\, \psi))$.*

Demostración. Sea $X = \{\varphi \in PROP : A(\varphi)\}$. X satisface las tres propiedades de la Definición 1, así que $PROP \subseteq X$ (pues $PROP$ es el **menor** conjunto con tales propiedades). Como $X \subseteq PROP$, tenemos $X = PROP$ y entonces $A(\varphi)$ vale para toda $\varphi \in PROP$. □

Por la misma razón, también es posible definir funciones f de $PROP$ en cualquier otro conjunto por recursión de la siguiente manera:

$\boxed{\varphi \in At}$ Si φ es atómica, se define $f(\varphi)$ de manera directa, sin llamadas recursivas.

$\boxed{(\neg\varphi)}$ Para definir $f((\neg\varphi))$ está permitido llamar recursivamente a $f(\varphi)$.

$\boxed{(\varphi \,\square\, \psi)}$ Para definir $f((\varphi \,\square\, \psi))$ está permitido llamar recursivamente a $f(\varphi)$ y a $f(\psi)$.

Dicho de otra manera, es posible definir una función f de $PROP$ en otro conjunto siguiendo el esquema:

$f(p_i)$	$=$	$\ldots$	caso base, sin llamadas a f
$f(\bot)$	$=$	$\ldots$	caso base, sin llamadas a f
$f((\neg\varphi))$	$=$	$\ldots f(\varphi) \ldots$	llamada recursiva permitida
$f((\varphi \,\square\, \psi))$	$=$	$\ldots f(\varphi) \ldots f(\psi) \ldots$	llamadas recursivas permitidas

Daremos algunos ejemplos de definiciones recursivas y luego de prueba por inducción.

Definiciones recursivas

A continuación definimos una función que calcula el número de símbolos de cada proposición, $\# : PROP \longrightarrow \mathbb{N}$:

$$\begin{array}{rcl} \#(p_i) & = & 1 \\ \#(\bot) & = & 1 \\ \#((\neg\varphi)) & = & \#(\varphi) + 3 \\ \#((\varphi \,\square\, \psi)) & = & \#(\varphi) + \#(\psi) + 3 \end{array}$$

Por ejemplo,

$$\begin{array}{rcl} \#((\neg(p_2 \to (\neg p_3)))) & = & \#((p_2 \to (\neg p_3))) + 3 \\ & = & \#(p_2) + \#((\neg p_3)) + 3 + 3 \\ & = & 1 + \#(p_3) + 3 + 3 + 3 \\ & = & 1 + 1 + 9 \\ & = & 11 \end{array}$$

El número de pares de conectivas lógicas de una proposición ($c : PROP \longrightarrow \mathbb{N}$):

$$\begin{array}{rcl} c(p_i) & = & 0 \\ c(\bot) & = & 1 \\ c((\neg\varphi)) & = & c(\varphi) + 1 \\ c((\varphi \,\square\, \psi)) & = & c(\varphi) + c(\psi) + 1 \end{array}$$

Por ejemplo $c(((\neg p_1) \wedge (p_2 \to (p_1 \vee p_3)))) = 4$.

El conjunto de variables o símbolos proposicionales que ocurren en una proposición ($vars : PROP \longrightarrow \mathcal{P}(\mathcal{V})$):

$$\begin{array}{rcl} vars(p_i) & = & \{p_i\} \\ vars(\bot) & = & \{\ \} \\ vars((\neg\varphi)) & = & vars(\varphi) \\ vars((\varphi \,\square\, \psi)) & = & vars(\varphi) \cup vars(\psi) \end{array}$$

Por ejemplo $vars(((\neg p_1) \wedge (p_2 \to (p_1 \vee p_3)))) = \{p_1, p_2, p_3\}$.

El conjunto de subfórmulas o subproposiciones de una proposición ($sub : PROP \longrightarrow \mathcal{P}(PROP)$):

$$\begin{array}{rcl} sub(p_i) & = & \{p_i\} \\ sub(\bot) & = & \{\bot\} \\ sub((\neg\varphi)) & = & sub(\varphi) \cup \{(\neg\varphi)\} \\ sub((\varphi \,\square\, \psi)) & = & sub(\varphi) \cup sub(\psi) \cup \{(\varphi \,\square\, \psi)\} \end{array}$$

Por ejemplo $sub(((\neg p_1) \to (p_1 \vee p_3))) = \{p_1, p_3, (\neg p_1), (p_1 \vee p_3), ((\neg p_1) \to (p_1 \vee p_3))\}$.

La sustitución del símbolo proposicional p_i por ψ en φ, que se denota por $\varphi[\psi/p_i]$

$$\begin{array}{rcl} p_j[\psi/p_i] & = & \begin{cases} \psi & \text{si } i = j \\ p_j & \text{si } i \neq j \end{cases} \\ \bot[\psi/p_i] & = & \bot \\ (\neg\varphi)[\psi/p_i] & = & (\neg\varphi[\psi/p_i]) \\ (\varphi \,\square\, \xi)[\psi/p_i] & = & (\varphi[\psi/p_i] \,\square\, \xi[\psi/p_i]) \end{array}$$

Por ejemplo,

$$\begin{array}{rcl} (p_1 \to (\neg p_2))[(\neg p_3)/p_1] & = & (p_1[(\neg p_3)/p_1] \to (\neg p_2)[(\neg p_3)/p_1]) \\ & = & ((\neg p_3) \to (\neg p_2[(\neg p_3)/p_1])) \\ & = & ((\neg p_3) \to (\neg p_2[(\neg p_3)/p_1])) \\ & = & ((\neg p_3) \to (\neg p_2)) \end{array}$$

Prueba por inducción

Veamos un ejemplo de prueba por inducción:

Definición 3. Una sucesión de proposiciones $\varphi_1, \ldots, \varphi_n$ es una *serie de formación* de $\varphi \in PROP$ si $\varphi_n = \varphi$ y para todo $i \leq n$, φ_i es:

- atómica, o bien
- igual a $(\neg\varphi_j)$ con $j < i$, ó
- igual a $(\varphi_j \,\square\, \varphi_k)$ con $j, k < i$.

Por ejemplo $p_1, p_2, p_3, (\neg p_1), ((\neg p_1) \wedge p_2), (p_1 \vee p_3), ((\neg p_1) \to (p_1 \vee p_3))\}$ es una serie de formación de $((\neg p_1) \to (p_1 \vee p_3))$, aunque no es la más corta posible. En cambio, si se elimina la segunda proposición, p_2, de la sucesión deja de ser una serie de formación. Si además se suprime la quinta proposición, obtenemos una nueva serie de formación de $((\neg p_1) \to (p_1 \vee p_3))$, esta vez de longitud mínima. ¿Es la única de longitud mínima?

Teorema 4. *Toda $\varphi \in PROP$ tiene serie de formación.*

Demostración. Analizamos cada caso:

$\boxed{\varphi \in At}$ φ es una serie de formación de φ.

$\boxed{(\neg\varphi)}$ Por hipótesis inductiva, φ tiene una serie de formación; sea $\varphi_1, \ldots, \varphi_{n-1}, \varphi$ una tal serie. Pero $\varphi_1, \ldots, \varphi_{n-1}, \varphi, (\neg\varphi)$ es una serie de formación de $(\neg\varphi)$.

$\boxed{(\varphi \,\square\, \psi)}$ Por hipótesis inductiva, φ y ψ tienen sus series de formación; llamémoslas $\varphi_1, \ldots, \varphi_{n-1}, \varphi$ y $\psi_1, \ldots, \psi_{m-1}, \psi$. Luego $\varphi_1, \ldots, \varphi_{n-1}, \varphi, \psi_1, \ldots, \psi_{m-1}, \psi, (\varphi \,\square\, \psi)$ es serie de formación de $(\varphi \,\square\, \psi)$.

Con esto se concluye la prueba. □