Notas de Clase para IL

4. Definición de Lógica de Primer Orden
Ejercicios resueltos

Rafel Farré, Robert Nieuwenhuis,
Pilar Nivela, Albert Oliveras, Enric Rodríguez

3 de septiembre de 2009

1. Ejercicios de la definición de LPO

1. (dificultad 1) Sea $\mathcal{F}$ el conjunto $\{c^0, f^1, g^2\}$. Evalúa los términos $f(f(g(c, f(c))))$ y $f(g(f(f(x)), g(c, f(c))))$ en las tres interpretaciones y asignaciones siguientes:

   a) La interpretación I se define por: $D_I = \mathbb{N}$, $c_I = 1$, $f_I(n) = n + 1$ y $g_I(n, m) = n + m$. La asignación α cumple $\alpha(x) = 7$.

   b) $D_I = P(\mathbb{N})$, c_I es el conjunto de los números pares, $f_I(A) = \mathbb{N} - A$ (el complementario de A) y $g_I(A, B) = A \cap B$. Además, $\alpha(x) = \emptyset$.

   c) El dominio D_I son las cadenas binarias, $c_I = 1$, $f_I(c) = c0$ y g_I es la concatenación. La asignación α cumple $\alpha(x) = 1111$.

---

a) Este primero lo haremos con todo detalle:

$$
\begin{array}{rcl}
eval_I^\alpha(f(f(g(c, f(c))))) & = & [\text{ def. de } eval_I^\alpha] \\
f_I(eval_I^\alpha(f(g(c, f(c))))) & = & [\text{ def. de } eval_I^\alpha\ ] \\
f_I(f_I(eval_I^\alpha(g(c, f(c))))) & = & [\text{ def. de } eval_I^\alpha\ ] \\
f_I(f_I(g_I(eval_I^\alpha(c), eval_I^\alpha(f(c))))) & = & [\text{ def. de } eval_I^\alpha\ ] \\
f_I(f_I(g_I(c_I, f_I(eval_I^\alpha(c))))) & = & [\text{ def. de } eval_I^\alpha\ ] \\
f_I(f_I(g_I(c_I, f_I(c_I)))) & = & [\text{ def. de } c_I\ ] \\
f_I(f_I(g_I(1, f_I(1)))) & = & [\text{ def. de } f_I] \\
f_I(f_I(g_I(1, 2))) & = & [\text{ def. de } g_I] \\
f_I(f_I(3)) & = & [\text{ def. de } f_I] \\
f_I(4) & = & [\text{ def. de } f_I] \\
5 & &
\end{array}
$$

Para el segundo caso aplicamos las definiciones de $eval_I^\alpha$ todas de golpe:

$$
\begin{array}{rcl}
eval_I^\alpha(f(g(f(f(x)), g(c, f(c))))) & = & [\text{ def. de } eval_I^\alpha] \\
f_I(g_I(f_I(f_I(\alpha(x))), g_I(c_I, f_I(c_I)))) & = & [\text{ def. de } \alpha \text{ y } c_I\ ] \\
f_I(g_I(f_I(f_I(7)), g_I(1, f_I(1)))) & = & [\text{ def. de } f_I\ ] \\
f_I(g_I(f_I(8), g_I(1, 2))) & = & [\text{ def. de } f_I \text{ y } g_I\ ] \\
f_I(g_I(9, 3)) & = & [\text{ def. de } g_I\ ] \\
f_I(12) & = & [\text{ def. de } f_I\ ] \\
13 & &
\end{array}
$$

b) Similarmente, si $\mathbb{P}$ es el conjunto de números pares e $\mathbb{I}$ es el conjunto de números impares tenemos

$$
\begin{array}{rcl}
eval_I^\alpha(f(f(g(c, f(c))))) & = & [\text{ def. de } eval_I^\alpha\ ] \\
f_I(f_I(g_I(c_I, f_I(c_I)))) & = & [\text{ def. de } c_I\ ] \\
f_I(f_I(g_I(\mathbb{P}, f_I(\mathbb{P})))) & = & [\text{ def. de } f_I\ ] \\
f_I(f_I(g_I(\mathbb{P}, \mathbb{I}))) & = & [\text{ def. de } g_I \text{ y } \mathbb{P} \cap \mathbb{I} = \emptyset\ ] \\
f_I(f_I(\emptyset)) & = & [\text{ def. de } f_I\ ] \\
f_I(\mathbb{N}) & = & [\text{ def. de } f_I\ ] \\
\emptyset & &
\end{array}
$$

El segundo término se evalúa como sigue:

$$\begin{array}{rcl}
eval_I^\alpha(f(g(f(f(x)),g(c,f(c))))) & = & [\text{ def. de } eval_I^\alpha] \\
f_I(g_I(f_I(f_I(\alpha(x))),g_I(c_I,f_I(c_I)))) & = & [\text{ def. de } \alpha \text{ y } c_I\ ] \\
f_I(g_I(f_I(f_I(\emptyset)),g_I(\mathbb{P},f_I(\mathbb{P})))) & = & [\text{ def. de } f_I] \\
f_I(g_I(f_I(\mathbb{N}),g_I(\mathbb{P},\mathbb{I}))) & = & [\text{ def. de } f_I \text{ y } g_I] \\
f_I(g_I(\emptyset,\emptyset)) & = & [\text{ def. de } g_I] \\
f_I(\emptyset) & = & [\text{ def. de } f_I] \\
\mathbb{N} & &
\end{array}$$

c) Para el caso de las cadenas binarias tenemos:

$$\begin{array}{rcl}
eval_I^\alpha(f(f(g(c,f(c))))) & = & [\text{ def. de } eval_I^\alpha\ ] \\
f_I(f_I(g_I(c_I,f_I(c_I)))) & = & [\text{ def. de } c_I\ ] \\
f_I(f_I(g_I(1,f_I(1)))) & = & [\text{ def. de } f_I\ ] \\
f_I(f_I(g_I(1,10))) & = & [\text{ def. de } g_I\ ] \\
f_I(f_I(110)) & = & [\text{ def. de } f_I\ ] \\
f_I(1100) & = & [\text{ def. de } f_I\ ] \\
11000 & &
\end{array}$$

El segundo término se evalúa así:

$$\begin{array}{rcl}
eval_I^\alpha(f(g(f(f(x)),g(c,f(c))))) & = & [\text{ def. de } eval_I^\alpha] \\
f_I(g_I(f_I(f_I(\alpha(x))),g_I(c_I,f_I(c_I)))) & = & [\text{ def. de } c_I \text{ y } \alpha] \\
f_I(g_I(f_I(f_I(1111)),g_I(1,f_I(1)))) & = & [\text{ def. de } f_I] \\
f_I(g_I(f_I(11110),g_I(1,10))) & = & [\text{ def. de } f_I \text{ y } g_I] \\
f_I(g_I(111100,110)) & = & [\text{ def. de } g_I] \\
f_I(111100110) & = & [\text{ def. de } f_I] \\
1111001100 & &
\end{array}$$

■

2. (dificultad 2) Este ejercicio es una continuación del anterior. Definimos los términos s_n y t_n recursivamente de la manera siguiente $s_0 := c$, $t_0 := c$, $s_{n+1} := f(s_n)$ y $t_{n+1} := f(g(t_n, t_n))$. Determina por inducción su evaluación en función de n en las tres interpretaciones anteriores (en la tercera interpretación evalúa sólo los 4 primeros términos t_n).

3. (dificultad 2) Sea el conjunto de símbolos de función $\mathcal{F} = \{+^2, s^1, z^0\}$. Consideremos también una interpretación I tal que D_I es $\mathbb{N}$ (los naturales), y los símbolos de función $+, s, z$ se interpretan como la suma en los naturales, el sucesor de un número natural y el número natural cero, respectivamente.

   a) Da dos términos distintos y sin variables tales que su evaluación en I sea 2.

   b) Demuestra que para todo número natural n existe un término t sin variables tal que la evaluación de t en I es n.

   c) Demuestra que dado un número natural n existen infinitos términos sin variables tales que su evaluación en I es n.

---

a) Por ejemplo, $+(s(z), s(z))$ y $s(s(z))$.

b) El término $\overbrace{s(s(\cdots s(}^{n} z)\cdots))$ cumple la propiedad requerida.

c) Para todo número natural m, el término

$$\overbrace{+(+(\cdots+(}^{m}\overbrace{s(s(\cdots s(}^{n} z)\cdots))\overbrace{,z),\cdots z),z)}^{m}$$

se evalúa a n en la interpretación considerada.

■

4. (dificultad 1) Dados los símbolos de función $\mathcal{F} = \{\ cero^0,\ suc^1,\ resta^2\}$ y los símbolos de predicado $\mathcal{P} = \{escero^1, espositivo^1, esmenor^2\}$ define interpretaciones I_1 a I_6 donde:

   - $D_{I_1} = \mathbb{Z}$, conjunto de los números enteros
   - $D_{I_2} = \{a, b\}$
   - $D_{I_3} = \{a\}$
   - $D_{I_4} = \mathcal{P}(\mathbb{N})$, el conjunto de todos los subconjuntos de $\mathbb{N}$
   - $D_{I_5} = \mathbb{N}^*$, el conjunto de todas las cadenas de naturales
   - $D_{I_6} = \mathbb{Z}$ *modulo* 3, el conjunto de las clases de equivalencia de los enteros módulo 3 (x e y están relacionados si x *mod* $3 = y$ *mod* 3, donde *mod* es el resto de la división entera).

   Para cada una de las interpretaciones anteriores, indica cuáles satisfacen las fórmulas

   - $\forall x\ escero(resta(x, x))$
   - $\forall x\ (espositivo(x) \rightarrow esmenor(cero, suc(x)))$
   - $\forall x\ (espositivo(x) \rightarrow esmenor(x, suc(x)))$
   - $\exists x \forall y\ (espositivo(y) \rightarrow esmenor(x, y))$

5. (dificultad 1) Sea F la fórmula $\exists x \exists y \exists z\ \ (p(x, y) \wedge p(z, y) \wedge p(x, z) \wedge \neg p(z, x))$. Cuáles de las siguientes interpretaciones son modelos de F?

   a) $D_I = \mathbb{N}$ y $p_I(m, n) = 1$ si y sólo si $m \leq n$.

   b) $D_I = \mathbb{N}$ y $p_I(m, n) = 1$ si y sólo si $n = m + 1$.

   c) $D_I = \mathcal{P}(\mathbb{N})$ (esto denota *partes de* $\mathbb{N}$, es decir, el conjunto de todos los subconjuntos de $\mathbb{N}$), y $p_I(A, B) = 1$ si y sólo si $A \subseteq B$.

---

   a) La interpretación es un modelo porque existen x, y y z cumpliendo que $x \leq y$, $z \leq y$, $x \leq z$, $z > x$; por ejemplo, $x = 0$, $y = 2$, $z = 1$.

b) La interpretación no es un modelo porque el sistema de ecuaciones $x + 1 = y$, $z + 1 = y$, $x + 1 = y$ no tiene solución.

c) La interpretación es un modelo. Tomando como referencia la solución del primer apartado y observando que $\{0, 1, ..., x\} \subseteq \{0, 1, ..., y\}$ si y sólo si $x \leq y$, vemos que podemos tomar $x = \{0\}$, $y = \{0, 1, 2\}$, $z = \{0, 1\}$.

■

6. (dificultad 2) Expresa con tres fórmulas las propiedades de reflexividad, simetría y transitividad de un predicado binario p y demuestra que ninguna de las tres fórmulas es consecuencia lógica de (la conjunción de) las otras dos.

- **Reflexividad:** $\forall x\ p(x, x)$
- **Simetría:** $\forall x\ \forall y\ \ (p(x, y) \rightarrow p(y, x))$
- **Transitividad:** $\forall x\ \forall y\ \forall z\ \ (p(x, y) \wedge p(y, z)\ \rightarrow\ p(x, z))$

La simetría no es consecuencia lógica de la reflexividad y de la transitividad: un contraejemplo consiste en la interpretación I cuyo dominio es $D_I = \mathbb{N}$ y donde $p_I(n, m) = 1$ si y sólo si $n \leq m$.

La transitividad no es consecuencia lógica de la reflexividad y de la simetría: un contraejemplo consiste en la interpretación I cuyo dominio son los naturales mayores o iguales a 2, o sea $D_I = \{2, 3, 4, 5, \ldots\}$ y donde $p_I(n, m) = 1$ si y sólo si n y m tienen algún factor primo común.

La reflexividad no es consecuencia lógica de la simetría y de la transitividad: un contraejemplo consiste en la interpretación I cuyo dominio es $D_I = \{a\}$ y donde p_I es siempre 0.

■

7. (dificultad 3) Sea $\mathcal{F}$ el conjunto $\{f^2, c^0\}$ y sea $\mathcal{P}$ el conjunto $\{p^2\}$. Consideremos una interpretación I tal que $D_I = \mathbb{N}$ y $p_I(n, m) = 1$ si y sólo si $n \leq m$. Encuentra tres interpretaciones distintas para f y c que satisfagan la fórmula

$$\forall x\ (\ p(f(x, c), x)\ \wedge\ p(x, f(x, c)\ )$$

y que sólo dos de ellas satisfagan la fórmula

$$\forall x \forall y\ (\ p(f(x, y), f(y, x)) \wedge p(f(y, x), f(x, y))\ )$$

8. (dificultad 2) Sea F la fórmula $\forall x \exists y\ p(x, y) \wedge \forall x \exists y\ \neg p(x, y)$. Demuestra que F es satisfactible.

Si I es una interpretación, decimos que *el número de elementos de* I es $|D_I|$, el número de elementos de D_I. Asimismo, decimos que I es un *modelo finito* cuando D_I es finito, y hablamos de *la cardinalidad de* I para referirnos a la cardinalidad de D_I.

¿Cual es el mínimo número de elementos que debe tener un modelo de F?

Sea I un modelo de F, y supongamos que tiene un solo elemento, que llamaremos a; o sea, $D_I = \{a\}$. Como $I \models \forall x \exists y\ p(x, y)$ y a es el único elemento de D_I, se tiene que cumplir que $p_I(a, a) = 1$. Similarmente, como $I \models \forall x \exists y\ \neg p(x, y)$ y a es el único elemento de D_I, se tiene que cumplir que $p_I(a, a) = 0$. Como esto es imposible, no puede existir ningún modelo de F con 1 elemento.

Por otra parte, sea I' la interpretación con dominio $D_{I'} = \{a, b\}$ y donde p se interpreta como la igualdad, esto es, $p_{I'}(a, a) = p_{I'}(b, b) = 1$, $p_{I'}(a, b) = p_{I'}(b, a) = 0$. Como para todo elemento del dominio existe un elemento del dominio que es igual a él mismo, y también existe otro que es distinto, esta interpretación es modelo de F. Por lo tanto los modelos de F tienen al menos 2 elementos.

■

9. (dificultad 3) Considera los conjuntos de símbolos y pares de interpretaciones I_1 e I_2 siguientes. Para cada caso, da una fórmula F que es cierta en una de ellas y falsa en la otra, y razona informalmente por qué es así.

   a) $\mathcal{P} = \{r^2\}$, I_1 tiene como dominio los naturales y el predicado se interpreta como el orden (es decir $r_I(n, m) = 1$ si y sólo si $n \leq m$); I_2 tiene como dominio los enteros y el predicado también se interpreta también como el orden;
   b) $\mathcal{P} = \{r^2\}$, I_1 tiene como dominio los enteros y el predicado se interpreta como el orden; I_2 tiene como dominio los racionales y el predicado se interpreta también como el orden.
   c) $\mathcal{P} = \{r^2\}$. El dominio tanto de I_1 como de I_2 son los números enteros, para I_1 el predicado r se interpreta como 'tener el mismo resto módulo 2' y para I_2 el predicado r se interpreta como 'tener el mismo resto módulo 3'.

---

   a) Consideremos la fórmula $\exists x \forall y\ r(x, y)$. Esta fórmula es cierta en los naturales porque los naturales tienen un *elemento mínimo*, el 0: existe un número, el 0, tal que para todo otro natural m, se tiene $0 \leq m$. En cambio, la fórmula no es cierta en los enteros, ya que los enteros no tienen mínimo: para todo entero n, podemos tomar $m = n - 1$ y entonces $n > m$.
   b) Consideremos la fórmula $\forall x \forall y\ (\neg r(y, x) \to \exists z\ (\neg r(z, x) \land \neg r(y, z)))$. Nótese que la fórmula viene a decir que si $x < y$ entonces hay un z con $x < z < y$. Es cierta en los racionales porque los racionales son *densos*: por ejemplo, se puede tomar z como $(x + y/2)$. En cambio, la fórmula no es cierta en los enteros.
   c) Consideremos la fórmula $\exists x \exists y \exists z\ (\neg r(x, y) \land \neg r(x, z) \land \neg r(y, z))$. Si interpretamos r como "tener el mismo resto módulo 3", la fórmula es cierta, ya que 0, 1 y 2 tienen resto distinto al dividirlos entre 3. En cambio, la fórmula no es cierta si r si interpreta como "tener el mismo resto módulo 2", ya que todo entero tiene resto o bien 0 o bien 1 al dividir entre 2; por lo tanto, no pueden existir tres enteros con restos módulo 2 distintos dos a dos.

■

10. (dificultad 2) Supón que en $\mathcal{P}$ sólo hay símbolos de predicado de aridad cero. Entonces, la sintaxis de las fórmulas, ¿en qué se diferencia de la de la lógica proposicional? ¿Y la semántica?

11. (dificultad 2) Sea F una fórmula con una única variable libre x. $\exists x\, F$ es consecuencia lógica de $\forall x\, F$? Demuéstralo aplicando la definición.

Sea I una interpretación tal que $I \models \forall x\, F$. Sea α una asignación arbitraria. Luego $1 = eval_I^\alpha(\forall x\, F) = \text{mín}\{\ eval_I^{\alpha[x\mapsto d]}(F) \ \mid\ d \in D_I\ \}$. Como $D_I \neq \emptyset$ por definición de interpretación, existe $a \in D_I$. Entonces $eval_I^{\alpha[x\mapsto a]}(F) = 1$, y $1 = \text{máx}\{\ eval_I^{\alpha[x\mapsto d]}(F) \ \mid\ d \in D_I\ \} = eval_I^\alpha(\exists x\, F)$. Por lo tanto $I \models \exists x\, F$; y como I es arbitraria, $\forall x\, F \models \exists x\, F$.

■

12. (dificultad 3) Sea F una fórmula y sean α y β dos asignaciones tales que $\alpha(x) = \beta(x)$ para toda variable libre x de F (en este caso se dice que α y β *coinciden* en las variables libres de F).

    Demuestra que $eval_I^\alpha(F) = eval_I^\beta(F)$. En particular, si F es cerrada el valor de $eval_I^\alpha(F)$ no depende de α y podemos escribir simplemente $eval_I(F)$.

    Ayuda: demuestra primero que $eval_I^\alpha(t) = eval_I^\beta(t)$ para todo término t tal que α y β coinciden en las variables de t.

Veamos primero que $eval_I^\alpha(t) = eval_I^\beta(t)$ para todo término t tal que α y β coinciden en las variables de t. Lo haremos por inducción sobre m el número de paréntesis de t:

- Caso base ($m = 0$): entonces o bien t es una variable o bien una constante. Si es una variable x entonces sabemos que $eval_I^\alpha(x) = \alpha(x) = \beta(x) = eval_I^\beta(x)$. Si es una constante c tenemos $eval_I^\alpha(c) = c_I = eval_I^\beta(c)$.
- Paso de inducción ($m > 0$ y asumo el enunciado cierto para todo $m' < m$): en este caso t será de la forma $f(t_1, \ldots, t_n)$. Tenemos entonces
  $eval_I^\alpha(f(t_1, \ldots, t_n)) = f_I(eval_I^\alpha(t_1), \ldots, eval_I^\alpha(t_n))$
  $eval_I^\beta(f(t_1, \ldots, t_n)) = f_I(eval_I^\beta(t_1), \ldots, eval_I^\beta(t_n))$
  Debido a que el número de paréntesis de cualquier t_i es menor que m y que las variables de cualquier t_i son un subconjunto de las variables de t, entonces podemos asegurar que $eval_I^\alpha(t_i) = eval_I^\beta(t_i)$, lo cual implica la igualdad de las dos evaluaciones.

Vayamos ahora a demostrar la propiedad para fórmulas. De forma similar lo haremos por inducción sobre m el número de conectivas (incluyendo cuantificadores) que aparecen en la fórmula:

- Caso base ($m = 0$): entonces F es de la forma p, siendo p símbolo de predicado de aridad cero, o bien de la forma $p(t_1, \ldots, t_n)$ con p símbolo de predicado de aridad $n > 0$. Si F es p el enunciado es cierto ya que $eval_I^\alpha(p) = p_I = eval_I^\beta(p)$. Si F es $p(t_1, \ldots, t_n)$ entonces tenemos que

$$\begin{aligned} eval_I^\alpha(p(t_1, \ldots, t_n)) &= p_I(eval_I^\alpha(t_1), \ldots, eval_I^\alpha(t_n)) \\ &= p_I(eval_I^\beta(t_1), \ldots, eval_I^\beta(t_n)) \\ &= eval_I^\beta(p(t_1, \ldots, t_n)) \end{aligned}$$

  Nótese que la segunda igualdad es cierta ya que al ser las variables de cualquier t_i un subconjunto de las libres de F, sabemos que α y β coinciden sobre las variables de cualquier t_i, y por lo tanto se cumple $eval_I^\alpha(t_i) = eval_I^\beta(t_i)$.

- Paso de inducción ($m > 0$ y asumo el enunciado cierto para todo $m' < m$): entonces F es de una de las siguientes formas: $\neg F_1$, $F_1 \vee F_2$, $F_1 \wedge F_2$, $\exists x F_1$, $\forall x F_1$. La demostración para los tres primeros casos es idéntica, así como la de los dos últimos casos. Por lo tanto, sólo haremos una de cada ($\vee$ y $\exists$).

  Si F es $F_1 \vee F_2$ entonces sabemos que tanto las variables libres de F_1 como las de F_2 son un subconjunto de las de F. Por lo tanto, α y β coincidirán sobre las libres de F_1 y F_2 y, al tener ambas fórmulas menos conectivas que m, puedo aplicar la hipótesis de inducción para concluir $eval_I^\alpha(F_1) = eval_I^\beta(F_1)$ y $eval_I^\alpha(F_2) = eval_I^\beta(F_2)$, con lo que tenemos $eval_I^\alpha(F_1 \vee F_2) = eval_I^\beta(F_1 \vee F_2)$.

  Si F es $\exists x F_1$, entonces las variables libres de F_1 son las de F más posiblemente x. Así pues, α y β coinciden en todas las variables libres de F_1 excepto a lo mejor en x. Pero nos fijamos que $eval_I^\alpha(\exists x F_1) = \text{máx}\{eval_I^{\alpha[x\mapsto d]}(F_1) \mid d \in D_I\}$ y que $eval_I^\beta(\exists x F_1) = \text{máx}\{eval_I^{\beta[x\mapsto d]}(F_1) \mid d \in D_I\}$. El argumento termina haciendo notar que ambas expresiones coinciden puesto que $eval_I^{\alpha[x\mapsto d]}(F_1) = eval_I^{\beta[x\mapsto d]}(F_1)$ al coincidir $\alpha[x \mapsto d]$ y $\beta[x \mapsto d]$ en todas las variables libres de F_1 y tener F_1 menos conectivas que m.

■

13. (dificultad 2) Vamos a extender la noción de equivalencia a fórmulas cualesquiera (no necesariamente cerradas). Diremos que dos fórmulas F y G *son equivalentes* (y lo denotaremos por $F \equiv G$) si $eval_I^\alpha(F) = eval_I^\alpha(G)$ para toda interpretación I y toda asignación α. Observa que esta nueva definición extiende la dada para fórmulas cerradas.

    a) Demuestra que la equivalencia de fórmulas en Lógica de primer orden es una relación de equivalencia (es decir, es reflexiva, simétrica y transitiva).

    b) Demuestra que si $F \equiv F'$ y $G \equiv G'$ entonces se cumplen:
    - $F \wedge G \equiv F' \wedge G'$
    - $F \vee G \equiv F' \vee G'$
    - $\neg F \equiv \neg F'$

- $\forall x F \equiv \forall x F'$
- $\exists x F \equiv \exists x F'$

14. (dificultad 4) Enuncia y demuestra el lema de sustitución para la lógica de primer orden.
Ayuda: ver el lema del mismo nombre en los ejercicios de lógica proposicional.

15. (dificultad 2) Las equivalencias de fórmulas que aparecen en los ejercicios de lógica proposicional (como por ejemplo, las leyes de De Morgan) son también ciertas para la lógica de primer orden. Demuestra alguna de ellas.

16. (dificultad 2) Demuestra alguna de las siguientes equivalencias:

$$
\begin{array}{lcl}
\neg\forall x F & \equiv & \exists x \neg F \\
\neg\exists x F & \equiv & \forall x \neg F \\
\forall x \forall y F & \equiv & \forall y \forall x F \\
\exists x \exists y F & \equiv & \exists y \exists x F \\
\forall x F \wedge \forall x G & \equiv & \forall x(F \wedge G) \\
\exists x F \vee \exists x G & \equiv & \exists x(F \vee G) \\
\forall x F \rightarrow \exists x G & \equiv & \exists x(F \rightarrow G) \\
\forall x F \vee G & \equiv & \forall x(F \vee G),\ \text{si } x \text{ no es libre en } G \\
\forall x F \wedge G & \equiv & \forall x(F \wedge G),\ \text{si } x \text{ no es libre en } G \\
\exists x F \vee G & \equiv & \exists x(F \vee G),\ \text{si } x \text{ no es libre en } G \\
\exists x F \wedge G & \equiv & \exists x(F \wedge G),\ \text{si } x \text{ no es libre en } G
\end{array}
$$

Demostremos algunas de estas equivalencias lógicas. Para ello, veamos que la función *eval* evalúa de la misma forma las fórmulas para toda interpretación I y para toda asignación α.

- Veamos que $\neg\forall x\, F \equiv \exists x\, \neg F$:

$$
\begin{array}{lcl}
eval_I^\alpha(\neg\forall x\, F) & = & [\text{por def. de } eval_I^\alpha] \\
1 - eval_I^\alpha(\forall x\, F) & = & [\text{por def. de } eval_I^\alpha] \\
1 - \text{mín}\{eval_I^{\alpha[x\to d]}(F) \mid d \in D_I\} & = & [\text{prop. de mín}] \\
1 + \text{máx}\{-eval_I^{\alpha[x\to d]}(F) \mid d \in D_I\} & = & [\text{prop. de máx}] \\
\text{máx}\{1 - eval_I^{\alpha[x\to d]}(F) \mid d \in D_I\} & = & [\text{por def. de } eval_I^\alpha] \\
\text{máx}\{eval_I^{\alpha[x\to d]}(\neg F) \mid d \in D_I\} & = & [\text{por def. de } eval_I^\alpha] \\
eval_I^\alpha(\exists x\, \neg F) & &
\end{array}
$$

- Veamos que $\forall x F \wedge \forall x G \equiv \forall x(F \wedge G)$.

$$
\begin{array}{lcl}
eval_I^\alpha(\forall x F \wedge \forall x G) & = & [\text{por def. de } eval_I^\alpha] \\
\text{mín}(eval_I^\alpha(\forall x F), eval_I^\alpha(\forall x G)) & = & [\text{por def. de } eval_I^\alpha] \\
\text{mín}(\text{mín}\{eval_I^{\alpha[x\to d]}(F) \mid d \in D_I\}, & & \\
\qquad \text{mín}\{eval_I^{\alpha[x\to d]}(G) \mid d \in D_I\}) & = & [\text{prop. de mín}] \\
\text{mín}\{\text{mín}(eval_I^{\alpha[x\to d]}(F), eval_I^{\alpha[x\to d]}(G)) \mid d \in D_I\} & = & [\text{por def. de } eval_I^\alpha] \\
\text{mín}\{eval_I^{\alpha[x\to d]}(F \wedge G) \mid d \in D_I\} & = & [\text{por def. de } eval_I^\alpha] \\
eval_I^\alpha(\forall x(F \wedge G)) & &
\end{array}
$$

- Veamos que $\forall xF \vee G \equiv \forall x(F \vee G)$ si x no es una variable libre de G.

$$
\begin{array}{lll}
eval_I^\alpha(\forall xF \vee G) & = & [\text{por def. de } eval_I^\alpha] \\
\text{máx}(eval_I^\alpha(\forall xF), eval_I^\alpha(G)) & = & [\text{por def. de } eval_I^\alpha] \\
\text{máx}(\text{mín}\{eval_I^{\alpha[x\to d]}(F) \mid d \in D_I\}, eval_I^\alpha(G)) & = & [\text{prop. de mín, máx}] \\
\text{mín}\{\text{máx}(eval_I^{\alpha[x\to d]}(F), eval_I^\alpha(G)) \mid d \in D_I\} & = & [\text{no es libre en } G] \\
\text{mín}\{\text{máx}(eval_I^{\alpha[x\to d]}(F), eval_I^{\alpha[x\to d]}(G)) \mid d \in D_I\} & = & [\text{por def. de } eval_I^\alpha] \\
\text{mín}\{eval_I^{\alpha[x\to d]}(F \vee G) \mid d \in D_I\} & = & [\text{por def. de } eval_I^\alpha] \\
eval_I^\alpha(\forall x(F \vee G)) & &
\end{array}
$$

■

17. (dificultad 2) Demuestra que las equivalencias siguientes **no** son ciertas en general (es decir, para cualquier par de fórmulas F, G):

    $\forall xF \vee \forall xG \equiv \forall x(F \vee G)$

    $\exists xF \wedge \exists xG \equiv \exists x(F \wedge G)$

    En ambos casos, hay alguna de la dos fórmulas que sea consecuencia lógica de la otra? (no hace falta que demuestres esto último, ya lo haremos cuando tengamos un cálculo deductivo).

Para ver que para ciertas fórmulas F y G se tiene $\forall x(F \vee G) \not\models \forall xF \vee \forall xG$ y que $\exists xF \wedge \exists xG \not\models \exists x(F \wedge G)$, basta con tomar $p(x)$ como F, $\neg p(x)$ como G y considerar la interpretación I con dominio $D_I = \{a, b\}$ y $p_I(a) = 0$, $p_I(b) = 1$.

En cambio, para cualesquiera F y G se cumple que

$\forall xF \vee \forall xG \models \forall x(F \vee G)$,

$\exists x(F \wedge G) \models \exists xF \wedge \exists xG$.

En el tema siguiente veremos un cálculo deductivo que nos permitirá demostrarlo fácilmente.

■

18. (dificultad 2) Demuestra que las fórmulas $\forall x\exists y\ F$ y $\exists y\forall x\ F$ no son equivalentes en general. ¿Hay alguna de la dos fórmulas que sea consecuencia lógica de la otra? (no hace falta que demuestres esto último, ya lo haremos cuando tengamos un cálculo deductivo).

Veamos que, para una cierta fórmula F, se tiene $\forall x\exists y\ F \not\models \exists y\forall x\ F$. Basta con tomar $p(x, y)$ como F y considerar la interpretación I con dominio $D_I = \mathbb{N}$ y $p_I(n, m) = 1$ si y sólo si $n \leq m$.

En cambio, para toda fórmula F se cumple que $\exists y\forall x\ F \models \forall x\exists y\ F$.

■

19. (dificultad 2) Las fórmulas $\exists x(F \rightarrow G)$ y $\exists xF \rightarrow \exists xG$, ¿son equivalentes? Responde a las mismas preguntas para las fórmulas $\forall x(F \rightarrow G)$ y $\forall xF \rightarrow \forall xG$.

20. (dificultad 3) Demuestra que la fórmula:

    $\exists x\,(p(x) \wedge q(x)) \;\wedge\; \exists x\,(p(x) \wedge \neg q(x)) \;\wedge\; \exists x\,(\neg p(x) \wedge q(x)) \;\wedge\; \exists x(\,\neg p(x) \wedge \neg q(x))$

    es satisfactible y que todo modelo tiene por lo menos 2^2 elementos. Da un modelo con exactamente 2^2 elementos. Escribe una fórmula con una propiedad análoga para 2^3 elementos. Generalízalo a 2^n.

21. (dificultad 3) Da una fórmula F_3 tal que todo modelo de F_3 tenga al menos 3 elementos. Generalízalo a n cualquiera.
    Ayuda: define la propiedad reflexiva de un símbolo de predicado binario p, y además expresa que hay pares de elementos e_i y e_j en el dominio tales que $p_I(e_i, e_j) = 0$.

La fórmula será una conjunción de dos subfórmulas. La primera será $\forall x \;\; p(x, x)$, que indica que p debe interpretarse como un símbolo de predicado reflexivo. La segunda subfórmula indica que existen tres elementos que son distintos dos a dos. Nótese que si p es un símbolo de predicado reflexivo entonces si $p_I(a, b) = 0$ en I, esto significa que a y b no pueden ser el mismo elemento del dominio. Así pues, escribiremos $\exists x \exists y \exists z\; (\neg p(x, y) \wedge \neg p(y, z) \wedge \neg p(x, z)\,)$ y la fórmula final

$$\forall x\; p(x, x) \;\wedge\; \exists x \exists y \exists z\; (\neg p(x, y) \wedge \neg p(y, z) \wedge \neg p(x, z)\,)$$

sólo puede ser cierta en modelos de cardinalidad al menos 3.

La generalización a cardinalidad al menos n es inmediata:

$$\forall x\; p(x, x) \;\wedge\; \exists x_1 \exists x_2 \ldots \exists x_n \left(\bigwedge_{1 \leq i < j \leq n} \neg p(x_i, x_j) \right)$$

■

22. (dificultad 5) Escribe una fórmula F tal que si $I \models F$ entonces D_I tiene infinitos elementos. Ayuda: piensa en la relación 'ser estrictamente menor que' y expresa (entre otras cosas) que 'no hay máximo' tal como ocurre en los naturales.

23. (dificultad 5) Demuestra que si una fórmula tiene modelos con n elementos, también tiene modelos con m elementos para cualquier $m \geq n$ e incluso modelos infinitos. Ayuda. Si I es una interpretación, tomar un elemento cualquiera a del dominio y añadir 'clones' de este elemento de la manera siguiente. Si A es un conjunto (el conjunto de los 'clones' de a) añadimos todos los elementos de A al dominio y extendemos la interpretación de un símbolo de predicado n-ario así: $(a_1, \ldots, a_n)$ evalúa el predicado a cierto si y sólo si evalúa el predicado a cierto en I al reemplazar cada uno de los clones por a. De manera análoga se define la interpretación de un símbolo de función. Llamemos I' a esta nueva interpretación.

Si $\alpha\colon \mathcal{X} \to D_{I'}$ es una asignación para I', consideramos la asignación $\alpha'\colon \mathcal{X} \to D_I$ consistente en reemplazar cada 'clon' por a. Ahora demostrad por inducción los hechos siguientes:

a) para cada término t, si $eval_{I'}^{\alpha}(t)$ es un elemento de D_I entonces $eval_{I'}^{\alpha}(t) = eval_I^{\alpha'}(t)$; si $eval_{I'}^{\alpha}(t)$ es un elemento de A entonces $eval_I^{\alpha'}(t) = a$.

b) para cada fórmula F no necesariamente cerrada se cumple que:

$$eval_{I'}^{\alpha}(F) = eval_I^{\alpha'}(F).$$

Observad que I e I' satisfacen exactamente las mismas fórmulas cerradas.

Dada una interpretación I definamos formalmente I'. Su dominio va a ser $D_{I'} = D_I \cup A$, donde A es tal que $A \cap D_I = \emptyset$. Recordemos que A es el conjunto de clones de un elemento $a \in D_I$. Notemos ahora que si consideramos una función $f_{proj} : D_{I'} \to D_I$ tal que $f_{proj}(e) = e$ si $e \in D_I$ y $f_{proj}(e) = a$ si $e \in A$, la α' del enunciado es precisamente $\alpha \circ f_{proj}$. Además, para facilitar la legibilidad escribiremos $\widehat{e}$ en lugar de $f_{proj}(e)$.

Ahora interpretemos los símbolos del lenguaje en I'. Para las constantes c definimos $c_{I'} = c_I$, y para los símbolos de función definimos $f_{I'}(a_1, \ldots, a_n) = f_I(\widehat{a_1}, \ldots, \widehat{a_n})$. Los símbolos de predicado p con aridad cero cumplirán $p_{I'} = p_I$ y para los de aridad mayor tendremos $p_{I'}(a_1, \ldots, a_n) = p_I(\widehat{a_1}, \ldots, \widehat{a_n})$.

Veamos ahora que se cumplen los dos apartados:

a) Lo demostramos por inducción sobre m el número de paréntesis de t.

- Caso base ($m = 0$): entonces o bien t es una constante c o una variable x. Si es una constante entonces $eval_{I'}^{\alpha}(c) = c_{I'} = c_I = eval_I^{\alpha'}(c)$, cumpliendo el resultado ya que $c_I \in D_I$. Si es una variable x distinguimos dos casos: si $\alpha(x) \notin D_I$ entonces $\alpha(x) \in A$ y tenemos $eval_{I'}^{\alpha}(x) = \alpha(x)$ y $eval_I^{\alpha'}(x) = \alpha'(x) = \widehat{\alpha(x)} = a$; en caso contrario $\alpha(x) \in D_I$, por lo que $\alpha(x) \notin A$, y se cumple $eval_{I'}^{\alpha}(x) = \alpha(x)$ y $eval_I^{\alpha'}(x) = \alpha'(x) = \widehat{\alpha(x)} = \alpha(x)$.
- Paso de inducción ($m > 0$ y asumo el enunciado cierto para todo $m' < m$): entonces t es $f(t_1, \ldots, t_n)$. Podemos notar primero que por la definición de I' tenemos $eval_{I'}^{\alpha}(t) \in D_I$. Además se cumple
$$\begin{aligned} eval_{I'}^{\alpha}(t) &= f_{I'}(eval_{I'}^{\alpha}(t_1), \ldots, eval_{I'}^{\alpha}(t_n)) \\ &= f_I(\widehat{eval_{I'}^{\alpha}(t_1)}, \ldots, \widehat{eval_{I'}^{\alpha}(t_n)}) \\ &= f_I(eval_I^{\alpha'}(t_1), \ldots, eval_I^{\alpha'}(t_n)) \\ &= eval_I^{\alpha'}(t) \end{aligned}$$
donde en la tercera igualdad hemos utilizado la hipótesis de inducción.

b) En este caso demostraremos el resultado por inducción sobre m el número de conectivas (incluyendo cuantificadores) de la fórmula:

- Caso base ($m = 0$): entonces o bien F es p o bien es $p(t_1, \ldots, t_n)$. Si es p entonces claramente $eval_{I'}^{\alpha}(p) = p_{I'} = p_I = eval_I^{\alpha'}(p)$. Para el otro caso tenemos

  $$\begin{array}{rcl} eval_{I'}^{\alpha}(F) & = & p_{I'}(eval_{I'}^{\alpha}(t_1), \ldots, eval_{I'}^{\alpha}(t_n)) \\ & = & p_I(\widehat{eval_{I'}^{\alpha}}(t_1), \ldots, \widehat{eval_{I'}^{\alpha}}(t_n)) \\ & = & p_I(eval_I^{\alpha'}(t_1), \ldots, eval_I^{\alpha'}(t_n)) \\ & = & eval_I^{\alpha'}(F) \end{array}$$

  donde en la tercera igualdad hemos utilizado el apartado anterior.

- Paso de inducción ($m > 0$ y asumo el enunciado cierto para todo $m' < m$): entonces F es de una de las siguientes formas: $\neg F_1$, $F_1 \vee F_2$, $F_1 \wedge F_2$, $\exists x F_1$, $\forall x F_1$. La demostración para los tres primeros casos es idéntica, así como la de los dos últimos casos. Por lo tanto, sólo haremos una de cada ($\vee$ y $\exists$).

  Si F es $F_1 \vee F_2$ entonces tenemos

  $$\begin{array}{rcl} eval_{I'}^{\alpha}(F_1 \vee F_2) & = & \text{máx}\{eval_{I'}^{\alpha}(F_1), eval_{I'}^{\alpha}(F_2)\} \\ & = & \text{máx}\{eval_I^{\alpha'}(F_1), eval_I^{\alpha'}(F_2)\} \\ & = & eval_I^{\alpha'}(F_1 \vee F_2) \end{array}$$

  donde en la tercera igualdad hemos utilizado la hipótesis de inducción.

  Sea ahora F de la forma $\exists x F_1$. El razonamiento va a ser el siguiente:

  $$\begin{array}{rcl} eval_{I'}^{\alpha}(\exists x F_1) & = & \text{máx}\{eval_{I'}^{\alpha[x \mapsto d]}(F_1) \mid d \in D_{I'}\} \\ & = & \text{máx}\{eval_I^{\alpha[x \mapsto d] \circ f_{proj}}(F_1) \mid d \in D_{I'}\} \\ & = & \text{máx}\{eval_I^{(\alpha \circ f_{proj})[x \mapsto d]}(F_1) \mid d \in D_I\} \\ & = & eval_I^{\alpha'}(\exists x F_1) \end{array}$$

  Aquí hemos utilizado en la segunda igualdad la hipótesis de inducción, pero falta argumentar la tercera igualdad:

  $$\underbrace{\text{máx}\{eval_I^{\alpha[x \mapsto d] \circ f_{proj}}(F_1) \mid d \in D_{I'}\}}_{L} = \underbrace{\text{máx}\{eval_I^{(\alpha \circ f_{proj})[x \mapsto d]}(F_1) \mid d \in D_I\}}_{R}$$

  Veamos primero que $L \geq R$: sea $d \in D_I$ donde se alcanza el máximo para R. Para esta d concreta no es difícil ver que se cumple que $\alpha[x \mapsto d] \circ f_{proj} = (\alpha \circ f_{proj})[x \mapsto d]$. Así pues $eval_I^{(\alpha \circ f_{proj})[x \mapsto d]}(F_1) = eval_I^{\alpha[x \mapsto d] \circ f_{proj}}(F_1)$ y, como $d \in D_I \subseteq D_{I'}$ sabemos que L deberá ser mayor o igual que R.
  Ahora veamos que $R \geq L$: sea $d \in D_{I'}$ donde se alcanza el máximo para L. Si $d \in D_I$ razonamos como en el caso anterior. Para el caso donde $d \notin D_I$ sabemos $d \in A$. Entonces $\alpha[x \mapsto d] \circ f_{proj} = (\alpha \circ f_{proj})[x \mapsto a]$ y por lo tanto $eval_I^{(\alpha \circ f_{proj})[x \mapsto a]}(F_1) = eval_I^{\alpha[x \mapsto d] \circ f_{proj}}(F_1)$. El argumento termina notando que $a \in D_I$ y por lo tanto R deberá ser mayor o igual que L.

■

1.1. Ejercicios de la definición de LPOI

24. (dificultad 2) Escribe una fórmula F que exprese que para todo modelo I de F:

a) hay como máximo 1 elemento en el dominio de I

b) hay como máximo 2 elementos en el dominio de I

c) hay como máximo n elementos en el dominio de I, para una n dada

d) hay exactamente n elementos en el dominio de I, para una n dada

¿Se podría hacer esto sin utilizar la igualdad? (ver el último ejercicio del apartado previo).

---

a) $\forall x\,(x = a)$.

b) $\forall x\,(x = a \lor x = b)$.

c) $\forall x\,(x = a_1 \lor x = a_2 \lor \cdots \lor x = a_n)$.

d) $\forall x\,(x = a_1 \lor x = a_2 \lor \cdots \lor x = a_n) \land \bigwedge_{1\le i<j\le n} a_i \neq a_j$.

Estas condiciones sobre los modelos no se podrían expresar en LPO *sin* igualdad porque, de acuerdo con el ejercicio anterior, si una fórmula sin igualdad tiene un modelo de cardinal n, entonces para todo m mayor que n tiene modelos de cardinal m, y también modelos infinitos.

■

25. (dificultad 1) En este ejercicio $\mathcal{F}$ consta de un único símbolo de función 1-aria f. Utilizando la igualdad, expresa con una fórmula F que f_I es inyectiva (es decir $I \models F$ si y sólo si f_I es inyectiva). Expresa que f_I es exhaustiva y también que f_I es biyectiva.

- f_I es inyectiva: $\forall x\,\forall y\,(x \neq y \rightarrow f(x) \neq f(y))$
- f_I es exhaustiva: $\forall y\,\exists x\, f(x) = y$
- f_I es biyectiva $\forall x\,\forall y\,(x \neq y \rightarrow f(x) \neq f(y)) \;\land\; \forall y\,\exists x\, f(x) = y$

■

26. (dificultad 2)

a) Sea p un símbolo de predicado unario. Escribe una fórmula F que exprese que hay un único elemento que cumple p. Esto quiere decir: que exprese que para todo modelo I de F hay un único elemento a en D_I con $p_I(a) = 1$.

b) Escribe otra F expresando que hay exactamente 2.

c) Generalízalo a un número natural n cualquiera.

d) Generalízalo más, considerando en vez de p una fórmula G con una única variable libre x: expresa que hay n elementos x tales que se cumple G.

---

a) La idea es que la fórmula exprese que existe un elemento que cumple p, y que además todo elemento que satisface p debe ser igual a éste. Por ejemplo:

$$\exists x\, (p(x) \wedge \forall y\, (p(y) \rightarrow y = x))$$

b) Ahora la idea es que la fórmula exprese que existen dos elementos distintos que cumplen p, y que además todo elemento que satisface p debe ser igual a uno de estos dos:

$$\exists x_1 \exists x_2\, (p(x_1) \wedge p(x_2) \wedge x_1 \neq x_2 \wedge \forall y\, (p(y) \rightarrow (y = x_1 \vee y = x_2)))$$

c) Similarmente al caso anterior, se trata de que la fórmula exprese que n elementos distintos cumplen p, y que además todo elemento que satisface p debe ser igual a uno de éstos:

$$\begin{aligned}\exists x_1 \exists x_2 \cdots \exists x_n \qquad & (p(x_1) \wedge p(x_2) \wedge \cdots \wedge p(x_n) \wedge \\ & \Big(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \Big) \wedge \\ & \forall y\, (p(y) \rightarrow (y = x_1 \vee y = x_2 \vee \cdots \vee y = x_n)))\end{aligned}$$

d) Denotamos por $G[z]$ la fórmula obtenida al sustituir las ocurrencias de la variable x en G por la variable z. Sin pérdida de generalidad, podemos asumir que las variables x_1, ..., x_n, y no aparecen en G (si no es así, las renombramos). Entonces la fórmula del apartado anterior también funciona para este caso, reemplazando p por G convenientemente:

$$\begin{aligned}\exists x_1 \exists x_2 \cdots \exists x_n \qquad & (G[x_1] \wedge G[x_2] \wedge \cdots \wedge G[x_n] \wedge \\ & \Big(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \Big) \wedge \\ & \forall y\, (G[y] \rightarrow (y = x_1 \vee y = x_2 \vee \cdots \vee y = x_n)))\end{aligned}$$

■

27. (dificultad 2) Un *monoide* es un modelo de la siguiente fórmula:

$$\forall x \forall y \forall z\ \ (x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \wedge \quad \forall x\ \ x \cdot e = x \quad \wedge \quad \forall x\ \ e \cdot x = x$$

donde $\cdot$ es un símbolo de función binaria y e es un símbolo de constante. Observa que hemos usado notación infija (como hacemos con el símbolo = para la igualdad). Con la notación habitual (y con f en vez de $\cdot$) la fórmula $\forall x \forall y \forall z\ \ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ se escribiría $\forall x \forall y \forall z\ \ f(f(x, y), z) = f(x, f(y, z))$.

Demuestra que las siguientes interpretaciones son monoides:

a) El dominio es el conjunto de los números racionales, $\cdot$ se interpreta como la suma y e se interpreta como 0.

b) El dominio es el conjunto de los números naturales, $\cdot$ se interpreta como el producto y y e se interpreta como 1.

c) El dominio es $\mathcal{P}(\mathbb{N})$ (el conjunto de los subconjuntos de $\mathbb{N}$), $\cdot$ se interpreta como la intersección y e se interpreta como $\mathbb{N}$.

d) El dominio es el conjunto de las cadenas binaria ('strings' de ceros y unos), $\cdot$ se interpreta como la concatenación y e se interpreta como la cadena vacía.

e) El dominio es $\{0, 1, \cdots, n-1\}$, $\cdot$ se interpreta como la suma módulo n (es decir $i \cdot_I i = i + j$ mod n) y e se interpreta como 0.

f) El dominio es el conjunto $\{\alpha, \beta\}$, $\cdot$ se interpreta mediante $\alpha \cdot_I \alpha = \alpha$, $\alpha \cdot_I \beta = \beta$, $\beta \cdot_I \alpha = \beta$, $\beta \cdot_I \beta = \alpha$, y e se interpreta como α.

---

a) Es un monoide porque para cualesquiera números racionales a, b y c, se cumple $(a + b) + c = a + (b + c)$, $a + 0 = 0 + a = a$.

b) Es un monoide porque para cualesquiera números naturales a, b y c, se cumple $(a \times b) \times c = a \times (b \times c)$, $a \times 1 = 1 \times a = a$.

c) Es un monoide porque para cualesquiera conjuntos de naturales R, S y T, se cumple $(R \cap S) \cap T = R \cap (S \cap T)$, $R \cap \mathbb{N} = \mathbb{N} \cap R = R$.

d) Es un monoide porque para cualesquiera cadenas binarias r, s y t, se cumple $(r \sharp s) \sharp t = r \sharp (s \sharp t)$, $r \sharp \lambda = \lambda \sharp r = r$ (donde $\sharp$ representa la concatenación y λ es la cadena vacía).

e) Es un monoide porque para cualesquiera números $a, b, c \in \{0, 1, \ldots, n-1\}$, se cumple $(a + b \bmod n) + c \bmod n = a + (b + c \bmod n) \bmod n$, $a + 0 \bmod n = 0 + a \bmod n = a$.

f) Es un monoide porque es un caso particular del ejemplo anterior con $n = 2$, donde α juega el papel de 0 y β el de 1.

■

28. (dificultad 2) Este ejercicio es una continuación del anterior. Un *grupo* es un monoide que además satisface la fórmula:

$$\forall x \exists y \ (\ x \cdot y = e \quad \wedge \quad y \cdot x = e \ )$$

¿Cuales de las interpretaciones anteriores eran grupos?

Un monoide se llama conmutativo o *Abeliano* cuando satisface la fórmula:

$$\forall x \forall y \ \ x \cdot y = y \cdot x$$

Cuales de las interpretaciones anteriores eran monoides Abelianos?

---

a) Es un grupo porque para cualquier número racional a, existe un número racional, $-a$, tal que $a + (-a) = (-a) + a = 0$. Además es Abeliano porque para cualquier par de números racionales a y b, se cumple $a + b = b + a$.

b) No es un grupo porque, por ejemplo, no hay inverso para 2 (en $\mathbb{N}$). Sin embargo es Abeliano porque para cualquier par de números naturales a y b, se cumple $a \times b = b \times a$.

c) No es un grupo porque, por ejemplo, no hay inverso para $\{0\}$. Sin embargo es Abeliano porque para cualquier par de conjuntos S y T, se cumple $S \cap T = T \cap S$.

d) No es un grupo porque, por ejemplo, no hay inverso para 0. Tampoco es Abeliano porque $0 \sharp 1 = 01$ y $1 \sharp 0 = 01$.

e) Es un grupo porque para cualquier número $a \in \{0, 1, ..., n-1\}$, existe un número $a' = (n - a) \bmod n \in \{0, 1, ..., n-1\}$, tal que $a + a' \bmod n = a' + a \bmod n = 0$. Además es Abeliano porque para cualquier par de números $a, b \in \{0, 1, ..., n-1\}$, se cumple $a + b \bmod n = b + a \bmod n$.

f) Es un grupo Abeliano porque es un caso particular del ejemplo anterior con $n = 2$, donde α juega el papel de 0 y β el de 1.

■

29. En este ejercicio $\mathcal{F}$ consta de dos símbolos de función 1-aria f, g.

   a) Utilizando la igualdad, expresa los hechos siguientes:

      1) (dificultad 1) Las funciones f_I y g_I son iguales.
      2) (dificultad 2) La función f_I es constante.
      3) (dificultad 2) La imagen de f_I está contenida en la imagen de g_I.
      4) (dificultad 2) La imagen de f_I y la de g_I son iguales.
      5) (dificultad 2) La imagen de f_I y la de g_I tienen un único elemento en común.
      6) (dificultad 3) La imagen de f_I contiene exactamente la imagen de g_I y 2 elementos más.

   b) Dadas las formulas:

      $F_1: \quad \forall x \quad f(x) = g(x)$
      $F_2: \quad \forall x\, \forall y \quad f(x) = g(y)$
      $F_3: \quad \forall x\, \exists y \quad f(x) = g(y)$
      $F_4: \quad \exists x\, \forall y \quad f(x) = g(y)$
      $F_5: \quad \exists x\, \exists y \quad f(x) = g(y)$

      construye un modelo de cada uno de las siguientes fórmulas:

      $F_1 \wedge \neg F_2, \quad F_2, \quad \neg F_1 \wedge F_3, \quad \neg F_1 \wedge F_4, \quad \neg F_3 \wedge \neg F_4 \wedge F_5, \quad \neg F_5.$

30. (dificultad 2) Demuestra, aplicando la definición, que la fórmula $\forall x \quad x = x$ es válida.

Tomemos una interpretación I y una asignación α cualesquiera. Veamos que $eval_I^\alpha(\forall x \;\; x = x) = 1$.

$$\begin{array}{rcll} eval_I^\alpha(\forall x\; x = x) & = & \text{mín}\,\{eval_I^{\alpha[x\mapsto d]}(x = x) \mid d \in D_I\} & [\text{ def. } eval_I^\alpha] \\ & = & \text{mín}\,\{igual_I(d,d) \mid d \in D_I\} & [\text{ def. } eval \text{ de } =] \\ & = & \text{mín}\,\{1 \mid d \in D_I\} & [\text{ def. } igual_I\,] \\ & = & 1 & \end{array} \qquad \blacksquare$$

31. (dificultad 2) Razona (puedes aplicar la semántica de manera informal sin necesidad de recurrir a la definición de *eval*) por qué la fórmula $\forall x \forall y\; (x = y \to f(x) = f(y))$ y la fórmula $\forall x \forall y\; (x = y \to (p(x) \leftrightarrow p(y)))$ son válidas. Demuestra que si en estas fórmulas reemplazamos la igualdad por un símbolo de predicado q de aridad 2 cualquiera dejan de ser fórmulas válidas. Expresa mediante fórmulas propiedades análogas para símbolos de función y predicado n-arios. Son también fórmulas válidas?

Ambas fórmulas son válidas porque, si x e y son elementos cualesquiera del dominio tales que $x = y$, entonces son el mismo, y por lo tanto las imágenes por f_I y p_I son la misma, o sea, se cumplen $f(x) = f(y)$ y $p(x) \leftrightarrow p(y)$ respectivamente.

Veamos por ejemplo que $\forall x \forall y\; (q(x,y) \to f(x) = f(y))$ no es válida. Para ello basta considerar la interpretación I con dominio $D_I = \{a, b\}$, $q_I(u, v) = 1$ para cualesquiera $u, v \in D_I$, y $f_I(a) = a$, $f_I(b) = b$.

Las generalizaciones a símbolos de función y de predicado de aridad n son las siguientes fórmulas, que también son válidas:

- $\forall x_1 \cdots \forall x_{i-1}\, \forall x_i\, \forall y_i\, \forall x_{i+1} \cdots \forall x_n$
  $(x_i = y_i \to f(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) = f(x_1, ..., x_{i-1}, x_i, y_{i+1}, ..., x_n))$
- $\forall x_1 \cdots \forall x_{i-1}\, \forall x_i\, \forall y_i\, \forall x_{i+1} \cdots \forall x_n$
  $(x_i = y_i \to (p(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) \leftrightarrow p(x_1, ..., x_{i-1}, y_i, x_{i+1}, ..., x_n)))$

donde $1 \le i \le n$.

■

32. Para los conjuntos de símbolos y pares de interpretaciones siguientes, escribe una fórmula que es cierta en una de ellas y falsa en la otra.

    a) (dificultad 2) $\mathcal{F} = \{f^2\}$, I_1 tiene como dominio los naturales y f se interpreta como el producto; I_2 tiene como dominio $P(\mathbb{N})$ y f se interpreta como la intersección.

    b) (dificultad 2) $\mathcal{F} = \{f^1\}$, el dominio de I_1 son los naturales y el de I_2 son los números enteros: En ambos casos el símbolo f se interpreta como la función 'siguiente', es decir $f_I(n) = n + 1$.

    c) (dificultad 4) $\mathcal{F} = \{f^2, g^2\}$. El dominio de I_1 son los números reales, f y g se interpretan como la suma y el producto respectivamente. I_2 es análogo salvo que ahora el dominio son los números racionales.
    Ayuda: fabrica el dos y expresa que raíz de dos existe.

---

a) Consideremos la fórmula $\forall x\ f(x,x) = x$. Es cierta en la interpretación I_2, porque la intersección de todo conjunto consigo es él mismo. Sin embargo no lo es en I_1, ya que por ejemplo $2 \times 2 \neq 2$.

b) Consideremos la fórmula $\forall x \exists y\ f(y) = x$. Es cierta en I_2, porque todo entero x es el siguiente de $x-1$. En cambio no lo es en I_1, ya que 0 no tiene 'anterior' en los naturales.

c) Consideremos la fórmula $\exists x \left(\forall y\, g(x,y) = y \ \wedge\ \exists z\, g(z,z) = f(x,x)\right)$. Intuitivamente, x juega el papel de 1, y z el de $\sqrt{2}$. La fórmula es cierta en I_1 y falsa en I_2 porque $\sqrt{2}$ existe en $\mathbb{R}$ pero no en $\mathbb{Q}$.

■

33. (dificultad 3) Tenemos los símbolos de constante $\{c_n \mid n \in \mathbb{N}\}$, los símbolos de predicado p^1, q^1, d^2, y los símbolos de función su^2, pr^2. Sea I la interpretación que tiene por dominio los números naturales, la constante c_n se interpreta como el número natural n, p se interpreta como 'ser número primo', q se interpreta como 'ser un cuadrado', d se interpreta como el predicado de divisibilidad, su y pr se interpretan respectivamente como la suma y el producto de naturales. Expresa con una fórmula las siguientes propiedades:

   a) El número 1 no es primo

   b) 2 es el único natural que es primo y par

   c) Todo número natural es suma de 4 cuadrados

   d) Ningún número primo es un cuadrado

   e) Todo cuadrado par es divisible por 4

   f) Todo número par mayor que 2 es suma de dos primos

   g) Hay números impares que no son primos

   h) Si un número impar es producto de otros dos, éstos también deben ser impares

   i) La suma de dos impares es par

   j) Si un número primo divide al producto de otros dos números, debe dividir alguno de ellos

---

En este ejercicio, $d(x,y)$ se interpreta como que x es divisible entre y. Las siguientes fórmulas expresan las propiedades anteriores:

a) $\neg p(c_1)$

b) $p(c_2) \wedge d(c_2, c_2) \wedge \forall x\ ((p(x) \wedge d(x, c_2)) \rightarrow x = c_2)$

c) $\forall x \exists y_1 \exists y_2 \exists y_3 \exists y_4\ (q(y_1) \wedge q(y_2) \wedge q(y_3) \wedge q(y_4) \wedge x = su(y_1, su(y_2, su(y_3, y_4))))$

d) $\neg\exists x\ (p(x) \wedge q(x))$

e) $\forall x\ ((q(x) \wedge d(x, c_2)) \rightarrow d(x, c_4))$

f) $\forall x\ ((d(x, c_2) \wedge x \neq c_0 \wedge x \neq c_2) \rightarrow \exists y_1 \exists y_2\ (p(y_1) \wedge p(y_2) \wedge x = su(y_1, y_2)))$

g) $\exists x\ (\neg d(x, c_2) \wedge \neg p(x))$

h) $\forall x \forall y \forall z\ ((\neg d(x, c_2) \wedge x = pr(y, z)) \rightarrow (\neg d(y, c_2) \wedge \neg d(z, c_2)))$

i) $\forall x \forall y\ ((\neg d(x, c_2) \wedge \neg d(y, c_2)) \rightarrow d(su(x, y), c_2))$

j) $\forall x \forall y \forall z((p(z) \wedge d(pr(x, y), z)) \rightarrow (d(x, z) \vee d(y, z)))$

■

34. (dificultad 4) Demuestra que si una fórmula no contiene ¬ ni ningún símbolo de predicado (salvo la igualdad) es cierta en toda interpretación cuyo dominio tiene un solo elemento.

35. (dificultad 5) Demuestra que la fórmula

$$\forall x \forall y\ (f(x) = f(y) \rightarrow x = y) \quad \wedge \quad \exists x \forall y\ x \neq f(y)$$

es satisfactible pero que todos sus modelos son infinitos.

En primer lugar veamos el siguiente resultado: si S es un conjunto finito, una función $g : S \rightarrow S$ es inyectiva si y sólo si es exhaustiva. En efecto: si S, T son conjuntos finitos y tenemos una función $g : S \rightarrow T$, entonces g es inyectiva si y sólo si $|g(S)| = |S|$, y es exhaustiva si y sólo si $|g(S)| = |T|$; en el caso particular en que $S = T$ se deduce que g inyectiva equivale a g exhaustiva.

La fórmula está expresando que f_I es una función inyectiva pero no exhaustiva. Por lo que acabamos de demostrar, necesariamente sus modelos tienen que ser infinitos. Uno de ellos, por ejemplo, es la interpretación I con dominio $D_I = \mathbb{N}$, y $f_I(n) = 2n$.

■

36. (dificultad 5) Sea F la fórmula $\forall x\ f(f(x)) = x$.

a) Demuestra que $\forall x \forall y\ (f(x) = f(y) \rightarrow x = y)$ es consecuencia lógica de F (puedes aplicar la semántica de manera informal, es decir sin necesidad de recurrir a la definición literal de *eval*). Ídem para $\forall x \exists y\ \ x = f(y)$.

b) Demuestra que $F \wedge \forall x\ f(x) \neq x$ es satisfactible y que todo modelo finito de dicha fórmula tiene un número par de elementos. Para cada $n \geq 1$ construye un modelo de dicha fórmula que tenga exactamente $2n$ elementos. Podría ocurrir lo mismo con una fórmula sin igualdad?

2. Ejercicios de formalización del lenguaje natural

37. (dificultad 2) Formaliza en lógica proposicional y estudia la validez lógica de la siguiente argumentación, esto es, si la conclusión es consecuencia lógica de la conjunción de las premisas:

    “Si Dios no existe y todo está permitido, entonces vamos inexorablemente hacia el caos. Dios no existe. No vamos hacia el caos. Luego, no todo está permitido”

    (Extraído de Hortalá, Leach, Rodríguez “Matemática discreta y lógica matemática, Ed. Complutense 2001)

38. (dificultad 2) Si tenemos los símbolos de predicado binario ami, con, pa (ami para ‘amigos’, con para ‘conocidos’, y pa para ‘ser padre de’) y los símbolos de constante m, e, r (m para Manuel, e para Enrique y r para Ramón) , formaliza la frases siguientes:

    a) Manuel es hijo de Enrique
    b) Manuel tiene amigos
    c) Ramón conoce a todos los amigos de sus hijos
    d) Enrique y Ramón tienen los mismos amigos
    e) Los amigos comunes de Ramón y Enrique son conocidos de Manuel
    f) Todos conocen a sus amigos pero no son amigos de todos sus conocidos
    g) Todos conocen a los amigos de sus hijos
    h) Todos los padres conocen a los padres de los amigos de sus hijos
    i) Hay padres que no conocen a todos los conocidos de sus hijos
    j) Si dos personas tienen los mismos amigos entonces también tienen los mismos conocidos
    k) Hay personas que tienen los mismos conocidos pero no los mismos amigos

---

En nuestra resolución $pa(x, y)$ significa “x es padre de y”.

a) $pa(e, m)$
b) $\exists x\ ami(m, x)$
c) $\forall x \forall y\ (pa(r, x) \land ami(x, y) \rightarrow con(r, y))$
d) $\forall x(ami(e, x) \leftrightarrow ami(r, x))$
e) $\forall x(ami(r, x) \land ami(e, x) \rightarrow con(m, x))$
f) $\forall x \forall y(ami(x, y) \rightarrow con(x, y)) \land \forall x \exists y(con(x, y) \land \neg ami(x, y))$
g) $\forall u \forall x \forall y\ (pa(u, x) \land ami(x, y) \rightarrow con(u, y))$
h) $\forall u \forall v \forall x \forall y\ (pa(u, x) \land ami(x, y) \land pa(v, y) \rightarrow con(u, v))$
i) $\exists x \exists y \exists z\ (pa(x, y) \land con(y, z) \land \neg con(x, z))$

j) $\forall x \forall y\ ((\forall z\ ami(x,z) \leftrightarrow ami(y,z)) \rightarrow (\forall z\ con(x,z) \leftrightarrow con(y,z)))$

k) $\exists x \exists y \left(\left(\forall z\ con(x,z) \leftrightarrow con(y,z) \right) \wedge \left(\exists z\ ami(x,z) \wedge \neg ami(y,z) \right) \right)$

■