(Undécima clase: Ejemplos de exponenciales)

Algunos ejemplos de lógica y computación.

Álgebras de Heyting. La clase pasada vimos que una álgebra de Boole, vista como categoría, es cartesiana cerrada definiendo $b^a = \neg a \vee b$ (que también se denota $a \Rightarrow b$). En realidad, para ser CCC, no es necesario que un poset sea un álgebra de Boole, alcanza con que sea un álgebra de Heyting:

Definición 224. *Un poset es un* ***álgebra de Heyting*** *si tiene*

1. *ínfimos finitos:* 1 *y* $p \wedge q$,
2. *supremos finitos:* 0 *y* $p \vee q$.
3. *exponenciales:* $p \Rightarrow q$ *tal que* $r \wedge p \leq q$ *sii* $r \leq p \Rightarrow q$.

El sii del tercer requerimiento dice que tiene exponenciales: que $r \wedge p \leq q$ implique $r \leq p \Rightarrow q$ nos da la transpuesta. Que $r \leq p \Rightarrow q$ implique $r \wedge p \leq q$, nos da la evaluación tomando $r = p \Rightarrow q$.

Por lo comprobado la clase pasada, un álgebra de Boole es un álgebra de Heyting. La inversa no es cierta, pero se puede obtener al menos distributividad:

$$\begin{aligned} (r \vee s) \wedge p \leq q \quad & \text{sii} \quad r \vee s \leq p \Rightarrow q \\ & \text{sii} \quad r \leq p \Rightarrow q \text{ y } s \leq p \Rightarrow q \\ & \text{sii} \quad r \wedge p \leq q \text{ y } s \wedge p \leq q \\ & \text{sii} \quad (r \wedge p) \vee (s \wedge p) \leq q \end{aligned}$$

De acá, tomando $q = (r \vee s) \wedge p$ obtenemos $(r \wedge p) \vee (s \wedge p) \leq (r \vee s) \wedge p$. Y tomando $q = (r \wedge p) \vee (s \wedge p)$ obtenemos $(r \vee s) \wedge p \leq (r \wedge p) \vee (s \wedge p)$.

No todos los reticulados distributivos son álgebras de Heyting. Sin embargo, los reticulados distributivos completos sí lo son.

Definición 225. *Un poset es* ***completo*** *si tiene ínfimos arbitrarios.*

Esto es equivalente a pedir supremos arbitrarios, ya que si tiene los unos tiene también los otros. Un reticulado, álgebra de Heyting o álgebra de Boole es completa si lo es como poset.

Prop 226. *Un reticulado completo es un álgebra de Heyting sii satisface la siguiente regla de distributividad:*

$$a \wedge (\bigvee_i b_i) = \bigvee_i (a \wedge b_i)$$

Un álgebra de Heyting satisface distributividad, es lo que demostramos un poco más arriba (la prueba es muy similar). Recíprocamente, si se define

$$p \Rightarrow q = \bigvee_{x \wedge p \leq q} x$$

veamos que es un álgegra de Heyting comprobando que $r \wedge p \leq q$ sii $r \leq p \Rightarrow q$. Por un lado tenemos el implica

$$r \wedge p \leq q \Longrightarrow r \leq \bigvee_{x \wedge p \leq q} x$$

que vale ya que r pertenece al rango del supremo. Por el otro

$$r \leq \bigvee_{x\wedge p\leq q} x \Longrightarrow r\wedge p \leq (\bigvee_{x\wedge p\leq q} x)\wedge p$$

Por distributividad podemos continuar:

$$(\bigvee_{x\wedge p\leq q} x)\wedge p = \bigvee_{x\wedge p\leq q}(x\wedge p) \leq \bigvee_{x\wedge p\leq q} q = q$$

Esto nos da el segundo implica: si $r \leq p \Rightarrow q$, entonces $r\wedge p\leq q$.

Como ya vimos, un álgebra de Boole es un álgebra de Heyting (tomando como hicimos $p\Rightarrow q = \neg p\vee q$). Pero no toda álgebra de Heyting es un álgebra de Boole (si se define $\neg p = p\Rightarrow 0$, como es lógico ya que $\neg p = \neg p \vee 0 = p\Rightarrow 0$, es posible que $\neg\neg p\neq p$ en un álgebra de Heyting).

Lógica proposicional intuicionista (IPC). Se define a través de reglas de inferencia, que establecen cuándo la fórmula q **se deduce de** la fórmula p (se escribe $p\vdash q$). Acá las fórmulas son las de la lógica proposicional: variables, $\top,\bot,p\wedge q,p\vee q$ y $p\Rightarrow q$. La relación $\vdash$ se define inductivamente por:

$$\frac{p\vdash q \quad p\vdash r}{p\vdash q\wedge r}\,a \qquad \frac{p\vdash q\wedge r}{p\vdash q}\,b \qquad \frac{p\vdash q\wedge r}{p\vdash r}\,c \qquad \frac{p\vdash r \quad q\vdash r}{p\vee q\vdash r}\,d \qquad \frac{p\vee q\vdash r}{p\vdash r}\,e \qquad \frac{p\vee q\vdash r}{q\vdash r}\,f$$

$$\frac{p\wedge q\vdash r}{p\vdash q\Rightarrow r}\,g \qquad \frac{p\vdash q\Rightarrow r}{p\wedge q\vdash r}\,h \qquad \frac{}{p\vdash\top}\,i \qquad \frac{}{\bot\vdash p}\,j \qquad \frac{}{p\vdash p}\,k \qquad \frac{p\vdash q \quad q\vdash r}{p\vdash r}\,l$$

La relación $\vdash$ así definida establece un preorden sobre el conjunto de fórmulas, y por lo tanto una categoría. Las reglas k (reflexividad) y l (transitividad) se corresponden con la flecha identidad y la composición.

Es una categoría cartesiana cerrada donde $\top$ es 1, y las siguiente derivaciones corresponden a las proyecciones

$$\frac{\dfrac{}{p\wedge q\vdash p\wedge q}\,k}{p\wedge q\vdash p}\,b \qquad \frac{\dfrac{}{p\wedge q\vdash p\wedge q}\,k}{p\wedge q\vdash q}\,c$$

mientras que la propiedad universal está dada por la regla a.

Se puede obtener la siguiente derivación:

$$\frac{\dfrac{}{p\Rightarrow q\vdash p\Rightarrow q}\,k}{(p\Rightarrow q)\wedge p\vdash q}\,h$$

que corresponde a la flecha evaluación, mientras que la transpuesta está dada por la regla g.

Es un juego interesante intentar obtener otros teoremas del cálculo proposicional intuicionista. Por ejemplo, modus ponens: obtener $p\vdash r$ a partir de $p\vdash q\Rightarrow r$ y $p\vdash q$:

$$\frac{\dfrac{\dfrac{}{p\vdash p}\,k \quad \dfrac{}{p\vdash q}}{p\vdash p\wedge q}\,a \qquad \dfrac{p\vdash q\Rightarrow r}{p\wedge q\vdash r}\,h}{p\vdash r}\,l$$

Las siguiente derivaciones dicen que p y $\top \wedge p$ son interdeducibles:

$$\dfrac{\dfrac{}{p \vdash \top}\,i \quad \dfrac{}{p \vdash p}\,k}{p \vdash \top \wedge p}\,a \qquad \dfrac{\dfrac{}{\top \wedge p \vdash \top \wedge p}\,k}{\top \wedge p \vdash p}\,c$$

La utilidad de fórmulas interdeducibles es que, gracias a la transitividad del $\vdash$, podemos reemplazar unas por otras: si $p \vdash p'$, $p' \vdash p$, $q \vdash q'$ y $q' \vdash q$, entonces $p \vdash q$ sii $p' \vdash q'$.

Decimos que una fórmula p es derivable cuando $\top \vdash p$ lo es.

Ejercicio 227. *Comprobar que los axiomas usuales de la conjunción*

- $(p \wedge q) \Rightarrow p$,
- $(p \wedge q) \Rightarrow q$, *y*
- $p \Rightarrow q \Rightarrow (p \wedge q)$

son derivables.

Estamos asumiendo que $\Rightarrow$ asocia a derecha.

Ejercicio 228. *Comprobar que los axiomas usuales de la implicación*

- $p \Rightarrow p$,
- $p \Rightarrow q \Rightarrow p$, *y*
- $(p \Rightarrow q \Rightarrow r) \Rightarrow (p \Rightarrow q) \Rightarrow p \Rightarrow r$

son derivables.

Ejercicio 229. *Comprobar que los axiomas usuales de la disyunción*

- $p \Rightarrow (p \vee q)$,
- $q \Rightarrow (p \vee q)$,
- $(p \vee q) \Rightarrow (p \Rightarrow r) \Rightarrow (q \Rightarrow r) \Rightarrow r$

son derivables.

Como se trata de un cálculo intuicionista, no es posible derivar $p \vee (p \Rightarrow \perp)$.

IPC y álgebras de Heyting. Existe una correspondencia entre IPC y álgebras de Heyting. Dado un cálculo intuicionista $\mathcal{L}$ construido con las conectivas que mencionamos a partir de un conjunto de variables, con las reglas dadas y tal vez con algunas fórmulas como axiomas, se puede construir el álgebra de Heyting $HA(\mathcal{L})$ (llamada álgebra de Lindenbaum-Tarski), cuyos elementos son clases de equivalencia $[p]$ de fórmulas :

$$[p] = [q] \text{ sii } p \vdash q \text{ y } q \vdash p$$

Se define un orden parcial entre clases

$$[p] \leq [q] \text{ sii } p \vdash q$$

que está bien definido por la observación que hicimos entre fórmulas interdeducibles. Las demás construcciones de un álgebra de Heyting no presentan sorpresas:

$$\begin{array}{rcl} 1 & = & [\top] \\ 0 & = & [\perp] \\ [p] \wedge [q] & = & [p \wedge q] \\ [p] \vee [q] & = & [p \vee q] \\ [p] \Rightarrow [q] & = & [p \Rightarrow q] \end{array}$$

Ejercicio 230. *Comprobar que* $\wedge$, $\vee$ *y* $\Rightarrow$ *están bien definidas.*

Una fórmula p es derivable en $\mathcal{L}$ sii $[p] = 1$, de donde se obtiene

Prop 231. *IPC es completo con respecto a los modelos en álgebras de Heyting.*

En efecto, sea p una fórmula verdadera en todas las álgebras de Heyting. En particular, p es verdadera en $HA(\mathcal{L})$. Luego $p = 1$ en $HA(\mathcal{L})$ y $\top \vdash p$.

Cálculo lambda. La correspondencia entre álgebras de Heyting y la lógica proposicional intuicionista es un caso particular de una correspondencia más general entre categorías cartesianas cerradas y cálculo lambda.

Recordemos la definición de cálculo lambda:

- Tipos

$$A, B \ ::= \ \text{ciertos tipos básicos} \mid A \longrightarrow B \mid A \times B \mid \ \ldots$$

- Términos

$$M, N \ ::= \ c \mid v \mid M \ N \mid \lambda v.M \mid (M, N) \mid fst(M) \mid snd(M) \mid \ \ldots$$

- Ecuaciones (además de renombre de variables ligadas, reflexividad, simetría, transitividad y congruencias)

$$\begin{array}{rcll} (\lambda x.\ M)\ N & = & M[N/x] & \\ \lambda x.\ M\ x & = & M & \quad \text{si } x \text{ no está libre en } M \\ fst((M,N)) & = & M & \\ snd((M,N)) & = & N & \\ (fst(M), snd(M)) & = & M & \end{array}$$

A partir de éste cálculo, obtuvimos una categoría:

- objetos $=$ tipos
- flechas de A a B $=$ clases de equivalencia de términos cerrados de tipo $A \to B$
- $1_A = \lambda x.x$ (con $x : A$)
- $M \circ N = \lambda x.M\ (N\ x)$

Luego definimos

- $\pi_1 = \lambda y.fst(y)$,
- $\pi_2 = \lambda y.snd(y)$, y
- $<M, N> = \lambda x.(M\ x, N\ x)$

que como demostramos determinan un producto en esa categoría. También se puede determinar un objeto exponencial:

- $B^A = A \to B$,
- $\epsilon = \lambda p.\ fst(p)\ snd(p)$, y
- $\widetilde{f} = \lambda z.\lambda x.\ f\ (z, x)$

Se puede comprobar fácilmente que el diagrama del exponencial conmuta:

$$\begin{aligned}
\epsilon \circ (\widetilde{f} \times 1_A) &= \epsilon \circ <\widetilde{f} \circ \pi_1, \pi_2> \\
&= \lambda x.\ \epsilon\ (<\widetilde{f} \circ \pi_1, \pi_2>\ x) \\
&= \lambda x.\ \epsilon\ (\widetilde{f}\ (\pi_1\ x), \pi_2\ x) \\
&= \lambda x.\ fst((\widetilde{f}\ (\pi_1\ x), \pi_2\ x))\ snd((\widetilde{f}\ (\pi_1\ x), \pi_2\ x)) \\
&= \lambda x.\ \widetilde{f}\ (\pi_1\ x)\ (\pi_2\ x) \\
&= \lambda x.\ \widetilde{f}\ (fst(x))\ (snd(x)) \\
&= \lambda x.\ f\ (fst(x), snd(x)) \\
&= \lambda x.\ f\ x \\
&= f
\end{aligned}$$

Para demostar unicidad, sea g que también hace conmutar el diagrama. Reiterando los pasos anteriores, asumir la conmutatividad del diagrama equivale a asumir la ecuación

$$\lambda x.\ g\ (fst(x))\ (snd(x)) = \lambda x.\ f\ (fst(x), snd(x))$$

que implica, para z y x

$$(\lambda x.\ g\ (fst(x))\ (snd(x)))\ (z, x) = (\lambda x.\ f\ (fst(x), snd(x)))\ (z, x)$$

que equivale a

$$g\ (fst((z, x)))\ (snd((z, x))) = f\ (fst(z, x), snd(z, x))$$

y esto a su vez a

$$g\ z\ x = f\ (z, x)$$

y esto a

$$\lambda z.\lambda x.\ g\ z\ x = \lambda z.\lambda x.\ f\ (z, x)$$

y finalmente, a

$$g = \lambda z.\lambda x.\ f\ (z, x)$$

que equivale a $g = \widetilde{f}$.

Por lo tanto, $\lambda\!\rightarrow$ es una CCC.

La categoría $\lambda\!\rightarrow$ y CCCs. Llamemos a un conjunto de tipos y términos básicos junto con sus ecuaciones una teoría en el cálculo lambda. Así como antes construimos $HA(\mathcal{L})$ a partir de un cálculo proposicional intuicionista $\mathcal{L}$, se puede construir una categoría cartesiana cerrada $\mathbf{C}(\mathcal{T})$ a partir una teoría $\mathcal{T}$.

Sea una categoría cartesiana cerrada $\mathbf{C}$. A cada tipo X se le debe asignar un objeto $[\![X]\!]$ de $\mathbf{C}$, y a cada término $M : A \rightarrow B$, una flecha $[\![M]\!]$ de $[\![A]\!] \rightarrow [\![B]\!]$. Una vez hecha para los tipos y términos básicos, para los demás se explota que $\mathbf{C}$ es CCC:

$$\begin{aligned}
[\![A \times B]\!] &= [\![A]\!] \times [\![B]\!] \\
[\![B^A]\!] &= [\![B]\!]^{[\![A]\!]} \\
&\dots \\
[\![<f, g>]\!] &= <[\![f]\!], [\![g]\!]> \\
&\dots
\end{aligned}$$

También se requiere que todas las ecuaciones de $\mathcal{T}$ sean satisfechas: si $a = b : A \rightarrow B$ vale en $\mathcal{T}$, entonces $[\![a]\!] = [\![b]\!] : [\![A]\!] \rightarrow [\![B]\!]$ debe valer en $\mathbf{C}$.

Por ejemplo, sea $\mathcal{T}$ la teoría que consiste de un tipo básico X y dos términos $u : X$ y $m : X \times X \to X$ con las ecuaciones

- $m\ (u, x) = x$,
- $m\ (x, u) = x$, y
- $m\ (x, m\ (y, z)) = m\ (m\ (x, y), z)$

es decir, las mismas que definen un monoide. Un modelo de $\mathcal{T}$ será una CCC $\mathbf{C}$ con un objeto M equipado con flechas $1 \xrightarrow{[\![u]\!]} M$ y $M \times M \xrightarrow{[\![m]\!]} M$ tales que el diagrama

$$\begin{tikzcd}
(M \times M) \times M \arrow[rr, "<\pi_1 \circ \pi_1, <\pi_2 \circ \pi_1, \pi_2>>"] \arrow[d, "{[\![m]\!] \times 1_M}"'] & & M \times (M \times M) \arrow[d, "{1_M \times [\![m]\!]}"] \\
M \times M \arrow[dr, "{[\![m]\!]}"'] & & M \times M \arrow[dl, "{[\![m]\!]}"] \\
& M &
\end{tikzcd}$$

que expresa asociatividad, conmute, y que el diagrama

$$\begin{tikzcd}
M \arrow[r, "{<[\![u]\!], 1_M>}"] \arrow[d, "{<1_M, [\![u]\!]>}"'] \arrow[dr, "1_M"] & M \times M \arrow[d, "{[\![m]\!]}"] \\
M \times M \arrow[r, "{[\![m]\!]}"'] & M
\end{tikzcd}$$

que expresa que $[\![\mathrm{u}]\!]$ sea neutro, conmute.

Prop 232. *Para toda teoría $\mathcal{T}$ en el cálculo lambda, y todos términos $a, b \in \mathcal{T}$, la ecuación $a = b$ puede deducirse en la teoría sii en todos los modelos de $\mathcal{T}$ en CCCs, $[\![a]\!] = [\![b]\!]$.*

Conclusión. Hay un parecido entre el cálculo lambda e IPC, por un lado, y CCC y álgebras de Heyting por el otro. El parecido consiste en ignorar el número de flechas y pensar que entre dos objetos puede haber a lo sumo una. Así, si del cálculo lambda suprimimos la posible multiplicidad de flechas (atendemos sólo la existencia de un término del tipo apropiado, pero sin importar cuáles son los términos, pretendiendo que es a lo sumo uno) obtenemos un cálculo equivalente a IPC. También si de una CCC, suprimimos dicha posible multiplicidad, obtenemos un álgebra de Heyting. Por ello, que una álgebra de Heyting sea modelo de IPC es un caso particular de que una CCC sea modelo del cálculo lambda.

La correspondencia que estamos observando es un ejemplode un fenómeno que se conoce como correspondencia o **isomorfismo de Curry-Howard**.