Teoría de la Prueba y Teoría de Categorías.

Juan Pablo Yamamoto Zazueta
(jpyamamoto@ciencias.unam.mx)

***Introducción*— La Teoría de Categorías es la rama que surge con la observación de que muchos conceptos matemáticos se pueden estudiar a través de diagramas de objetos y flechas entre estos. La belleza de esta área radica en el alto nivel de abstracción en que se estudia, permitiendo que estos resultados tengan aplicación en muchas otras áreas.**

En 1968, Joachim Lambek publicó su artículo *Deductive systems and categories* en el cuál por primera vez encontramos la formulación categórica de las pruebas formales en sistemas de deducción. Desde algunos años antes se había comenzado a estudiar en forma la Teoría de la Prueba, y ya se había comenzado a vislumbrar su conección con el cálculo λ de Alonzo Church, dando lugar a la Correspondencia Curry-Howard. Esta nueva forma de modelar los sistemas de deducción formal como categorías permitió extender la noción anterior a la Correspondencia Curry-Howard-Lambek. A continuación doy una corta introducción a los conceptos esenciales de teoría de Categorías para entender su conexión con Teoría de la Prueba.

I. CONCEPTOS BÁSICOS DE CATEGORÍAS

Una categoría $\mathfrak{C}$ se define a partir de 3 elementos:

- Una clase de objetos de la categoría, denotado $\operatorname{Obj}\mathfrak{C}$.
- Una clase de morfismos (flechas) entre los objetos de la clase, denotado $\operatorname{Hom}\mathfrak{C}$. En particular, a la subclase de morfismos que van de A a B, se le denota como $\operatorname{Hom}(A, B)$.
- Una operación binaria de composición $\circ : \operatorname{Hom}(B, C) \times \operatorname{Hom}(A, B) \to \operatorname{Hom}(A, C)$.

Los axiomas que debe cumplir una categoría $\mathfrak{C}$ son:

1) Identidad: Para cada objeto $A \in \operatorname{Obj}\mathfrak{C}$, existe $A \xrightarrow{1_A} A$ tal que para cualquier $A \xrightarrow{f} B$ sucede $1_B \circ f = f = f \circ 1_A$.
2) Asociatividad: Para cualesquiera 3 morfismos de la forma $A \xrightarrow{f} B, B \xrightarrow{g} C, C \xrightarrow{h} D$ sucede que $h \circ (g \circ f) = (h \circ g) \circ f$.

A. PRODUCTO DE OBJETOS

Dados dos objetos X, Y de una categoría $\mathfrak{C}$ denotamos el producto $X \times Y$ como un objeto Z en $\mathfrak{C}$ junto con los morfismos $Z \xrightarrow{\pi_1} X$ y $Z \xrightarrow{\pi_2} Y$. Además, debe cumplir que para cualesquiera $Z \xrightarrow{f} X, Z \xrightarrow{g} Y$ existe un único morfismo h tal que el siguiente diagrama conmuta:

$$\begin{tikzcd}
 & Z \arrow[dl, "f"'] \arrow[d, dashed, "h"] \arrow[dr, "g"] & \\
X & X \times Y \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & Y
\end{tikzcd}$$

B. EXPONENTE DE OBJETOS

Dados dos objetos X, Y de una categoría $\mathfrak{C}$ denotamos el exponente X^Y como un objeto en $\mathfrak{C}$ junto con el morfismo $\mathrm{eval} : (X^Y \times Y) \to X$. Debe cumplir que para cualesquiera $X \in \operatorname{Obj}\mathfrak{C}$ y $g : Z \times Y \to X$, existe un único morfismo $\overline{g} : Z \to X^Y$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd}
Z \times Y \arrow[d, dashed, "\overline{g} \times 1_Y"'] \arrow[dr, "g"] & \\
X^Y \times Y \arrow[r, "\mathrm{eval}"'] & X
\end{tikzcd}$$

C. *CATEGORÍA CERRADA*

Decimos que una categoría $\mathfrak{C}$ es cerrada si para cualesquiera $A, B \in \operatorname{Obj}\mathfrak{C}$ sucede que $\operatorname{Hom}(A, B)$ se puede considerar en si mismo un objeto de la categoría $\mathfrak{C}$.

Esta idea de colapsar todos los morfismos entre dos objetos nos va a permitir definir una relación de equivalencia (o congruencia), como veremos más adelante.

D. *CATEGORÍA CARTESIANA CERRADA*

Una categoría $\mathfrak{C}$ es cartesiana cerrada si cumple lo siguiente:

1) Tiene un objeto terminal. Un objeto $T \in \operatorname{Obj}\mathfrak{C}$ es terminal si para cualquier $X \in \operatorname{Obj}\mathfrak{C}$ existe un único morfismo $X \xrightarrow{O_X} T$.

2) Para cualesquiera $X, Y \in \operatorname{Obj}\mathfrak{C}$ se tiene $X \times Y \in \operatorname{Obj}\mathfrak{C}$.

3) Para cualesquiera $X, Y \in \operatorname{Obj}\mathfrak{C}$ sucede que $X^Y \in \operatorname{Obj}\mathfrak{C}$.

Es decir, tenemos productos, exponentes y un objeto terminal.

II. CORRESPONDENCIA ENTRE CATEGORÍAS Y PRUEBAS

Voy a dar una definición alternativa (pero equivalente) de la Categoría Cartesiana Cerrada con una notación ligeramente distinta a la que he utilizado hasta ahora para hacer más evidente la correspondencia a la que quiero llegar.

Una categoría cartesiana cerrada se define como $\mathcal{C} = (\mathfrak{C}, T, \wedge, \Rightarrow, O, (,), \mathrm{fst}, \mathrm{snd}, \mathrm{eval}, \mathrm{curry})$ que cumple lo siguiente:

1) $\mathfrak{C}$ es una categoría.

2) T es un objeto terminal.

3) O es la familia de morfismos que para cada $A \in \operatorname{Obj}\mathfrak{C}$ nos da $O_A : A \to T$.

4) $\wedge$ es la operación binaria de producto de objetos en la categoría, junto con sus proyecciones fst y snd.

5) $(,)$ es la operación binaria que construye el producto. Es decir, es el único morfismo tal que el siguiente diagrama conmuta:

$$\begin{tikzcd}
 & X \arrow[dl, "f"'] \arrow[d, "(f{,}g)"] \arrow[dr, "g"] & \\
Y & Y \wedge Z \arrow[l, "\mathrm{fst}"] \arrow[r, "\mathrm{snd}"'] & Z
\end{tikzcd}$$

6) $\Rightarrow$ es la operación binaria para exponentes, junto con su morfismo asociado eval.

7) curry es la operación que transforma un morfismo $A \wedge B \to C$ en $A \to B \Rightarrow C$.

Ahora queda más clara la correspondencia entre Lógica Intuicionista y Categorías Cartesianas Cerradas. Si tenemos que explicar esta correspondencia de forma concisa, podemos extender la frase popular: pruebas como programas (y como morfismos de una categoría cartesiana cerrada); proposiciones como tipos (y como objetos de una categoría cartesiana cerrada)

Entremos en algunos detalles que probablemente son evidentes, pero igual vale la pena enfatizar.

El valor de verdad “Verdadero” se captura a través del objeto terminal T. En lógica intuicionista tenemos que la presencia de una variable proposicional es un testigo de que esta variable existe. Al ser construible, podríamos interpretarla como "verdadera". Es decir, si podemos construir la variable proposicional A, podemos concluir $\top$ sin inconsistencias. Otra forma de verlo es: si tenemos $\top$, por introducción vacua de la implicación, $A \Rightarrow \top$. Esto mismo se captura a través del operador O en categorías, que nos dice que dado un objeto, siempre podemos encontrar un morfismo al objeto terminal.

Otro detalle es considerar qué interpretación tiene el morfismo 1_A. Recordando que este es un morfismo $A \xrightarrow{1_A} A$, podemos interpretarlo como el secuente inicial $A \vdash A$ o el axioma $A \Rightarrow A$.

Además, notemos que el tener un morfismo $A \xrightarrow{f} B$ se puede interpretar como tener una derivación de A a B, con nombre f (análogo a lo que hacemos en el cálculo λ al nombrar un λ término). De igual manera, un exponente A^B, bajo la nueva notación sería $B \Rightarrow A$. Volviendo a ver el diagrama conmutativo del exponente tenemos para cualquier $A \wedge B \xrightarrow{f} C$:

$$\begin{tikzcd} A \wedge B \arrow[d, "((\text{curry } f)\text{fst,snd})"'] \arrow[drr, "f"] & & \\ (B \Rightarrow C) \wedge B \arrow[rr, "\text{eval}"] & & C \end{tikzcd}$$

Nótese que eval es simplemente el *modus ponens* (o la aplicación de funciones si nos remitimos al cálculos λ). Es importante no confundir la notación $\rightarrow$ de morfismo (que se interpreta como tener una derivación) con la flecha $\Rightarrow$ de exponente (que se interpreta como una implicación). Si bien en la práctica es intercambiable, formalmente no es lo mismo.

Esto nos conduce a cuestionar cómo interpretamos la composición de morfismos. Si tenemos $A \xrightarrow{f} B$ y $B \xrightarrow{g} C$, entonces tenemos un morfismo $A \xrightarrow{f \circ g} C$. Esto es la regla de corte.

III. CERRADURA DE LA CATEGORÍA

Anteriormente mencionamos que para modelar un sistema de deducción natural íbamos a utilizar una categoría cartesiana cerrada. Sin embargo, hay un problema que no mencioné anteriormente y es que bajo la definición dada, no justificamos que los morfismos correspondan a objetos en la categoría $\mathfrak{C}$. Si bien los productos y exponentes sí generan objetos, tenemos que justificar que los morfismos $\text{curry}, \circ, \text{fst}, \text{snd}$ y $(,)$ también son objetos, y en qué casos.

Para solucionar esto y que la categoría sí sea cerrada, definimos una relación de equivalencia $\equiv$ y hablamos de "igualdad módulo $\equiv$".

Una forma de definir $\equiv$ es como: *la relación de equivalencia más pequeña tal que $\mathfrak{C}$ es una categoría cerrada*. Si bien es correcta la definición, por motivos que serán aparentes más adelante preferimos dar explícitamente cuáles son las reglas que inducen esa relación. Estas son las siguientes:

$$\frac{}{a \equiv a} \qquad \frac{a \equiv b \quad b \equiv c}{a \equiv c} \qquad \frac{a \equiv b \quad c \equiv d}{(a, c) \equiv (b, d)}$$

$$\frac{a \equiv b \quad c \equiv d}{a \circ c \equiv b \circ d} \qquad \frac{a \equiv b}{\text{curry}\, a \equiv \text{curry}\, b}$$

$$\frac{a \equiv b}{\text{fst}\, a \equiv \text{fst}\, b} \qquad \frac{a \equiv b}{\text{snd}\, a \equiv \text{snd}\, b}$$

Más adelante será posible demostrar que esto se puede interpretar como la noción de **normalidad**. Es decir, en la categoría de pruebas, si tenemos dos objetos tales que $A \equiv B$, bajo la correspondencia *Curry-Howard-Lambek* tendremos que A y B tienen una misma forma normal.

IV. VARIANTES

Nótese que he estado postergando hablar sobre dos elementos comúnmente presentes en la lógica intuicionista: el valor de verdad "Falso" y la conjunción. Y es que bajo la definición que hemos dado de categoría cartesiana cerrada, no es posible modelar esto.

Para ello es necesario un tipo de categoría más fuerte: la categoría bicartesiana cerrada. Esta va a introducir:

1) Un objeto inicial F. Es decir, para cualquier $A \in \operatorname{Obj} \mathfrak{C}$ existe un único morfismo $F \xrightarrow{\text{EFQ}_A} A$.

2) Co-productos. Dados dos objetos X, Y de una categoría $\mathfrak{C}$ denotamos el co-producto $X \vee Y$ como un objeto en $\mathfrak{C}$ junto con los morfismos $X \xrightarrow{\text{left}} X \vee Y$ y $Y \xrightarrow{\text{right}} X \vee Y$. Debe satisfacer que para cualesquiera $Z \in \operatorname{Obj} \mathfrak{C}$, $X \xrightarrow{f} Z$ y $Y \xrightarrow{g} Z$, existe un único morfismo $X \vee Y \xrightarrow{\text{case}} Z$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} X \arrow[r, "\text{left}"] \arrow[dr, "f"'] & X \vee Y \arrow[d, dashed, "\text{case}"] & Y \arrow[l, "\text{right}"'] \arrow[dl, "g"] \\ & Z & \end{tikzcd}$$

Resulta de interés notar que el co-producto se define invirtiendo el orden del diagrama conmutativo del producto. Esto hace evidente la noción de que la disyunción es el dual de la conjunción.

Otra variante propuesta por Berger en [1] es la generalización de las categorías cartesianas cerradas para contemplar lógicas proposicionales distintas a la intuicionista. Logra esto dando una manera de definir categorías que incluya distintos axiomas. Por ejemplo, una categoría que con el axioma $\{\top \vdash A\}$ para significar la categoría en donde se cumple A; o la categoría con el axioma $\{(A \Rightarrow B) \Rightarrow A \vdash A\}$ para modelar la lógica clásica con la ley de Pierce.

V. NORMALIZACIÓN

Utilizar la formulación categórica de los sistemas de deducción no es la forma más sencilla de mostrar que las proposiciones en la lógica intuicionista son normalizables, pues en gran medida recurre a dar la misma demostración que se utiliza en la codificación con el cálculo λ, cambiando la notación para ajustarse a la formulación categórica.

De cualquier manera, enuncio los pasos que se realizarían para demostrar que se poseé la propiedad de normalidad.

1) Se define una relación binaria R_1 entre objetos de $\mathfrak{C}$, análoga a la η reducción.

2) Se define una relación binaria R_2 entre objetos de $\mathfrak{C}$, análoga a la β reducción.

3) Se demuestra la propiedad de Church-Rosser.

4) Usando la propiedad de Church-Rosser, se demuestra que todo objeto de $\mathfrak{C}$ tiene una *forma normal reducida* (la aplicación de R_2 seguido de R_1).

5) Se muestra que $A \equiv B$ si y sólo si las formas normales reducidas de A y B son equivalentes bajo una cierta relación de equivalencia.

VI. APLICACIONES

Si bien acabamos de comentar que la formulación categórica de los sistemas de deducción no destaca particularmente por dar una mejor prueba de la propiedad de normalización, sí hay casos en donde vemos aplicaciones a esta correspondencia.

Una de las primeras aplicaciones que se exploraron fue la de resolver el "word problem" para ciertas categorías, dando una reducción a un problema de teoría de la prueba.

Posteriormente, también se utilizó la correspondencia Curry-Howard-Lambek para demostrar algunos Teoremas de Coherencia para ciertas categorías, que consiste en mostrar que bajo ciertas condiciones, los diagramas de morfismos conmutan.

Otra línea de investigación reciente es en Teoría de Tipos Homotópica que estudia las proposiciones y tipos, utilizando conceptos de teoría de categorías y topología.

REFERENCES

[1] Carsen Berger. A categorical approach to proofs-as-programs. 2010.

[2] C. R. MANNf. The connection between equivalence of proofs and cartesian closed categories. 1974.

[3] Grigorii E. Mints. *Closed categories and the theory of proofs*, page 183–212. Bibliopolis, 1992.

[4] Grigorii E. Mints. *Proof theory and category theory*, page 157–182. Bibliopolis, 1992.

[5] Cosimo Perini Brogi. Curry–howard–lambek correspondence for intuitionistic belief. *Studia Logica*, 109(6):1441–1461, 2021.