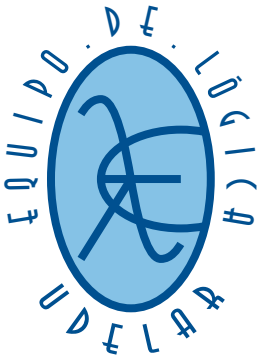
¿Qué es la verdad?

(Juan, 18:38)

Alexandre Miquel



30 de abril de 2024
Coloquio mensual del IMERL

Juan, 18:33–38

33 **Pilato:** ¿Eres tú el Rey de los judíos?

34 **Jesús:** ¿Dices tú esto por ti mismo, o te lo han dicho otros de mí?

35 **Pilato:** ¿Soy yo acaso judío? Tu nación, y los principales sacerdotes, te han entregado a mí. ¿Qué has hecho?

36 **Jesús:** Mi reino no es de este mundo; si mi reino fuera de este mundo, mis servidores pelearían para que yo no fuera entregado a los judíos; pero mi reino no es de aquí.

37 **Pilato:** ¿Luego, eres tú rey?

Jesús: Tú dices que yo soy rey. Yo para esto he nacido, y para esto he venido al mundo, para dar testimonio a la verdad. Todo aquel que es de la verdad, oye mi voz.

38 **Pilato:** ¿Qué es la verdad? [...]

La verdad en matemática (1/2)

Existen al menos dos nociones de verdad en matemática:

1. La verdad a partir de un cálculo de valor de verdad

La verdad como correspondencia entre un enunciado y el mundo externo (Aristóteles, Platón, Descartes, Leibniz, Hume, Kant, Tarski, Popper, ...)

Negación	
ϕ	$\neg\phi$
$\mathscr{V}$	$\mathscr{F}$
$\mathscr{F}$	$\mathscr{V}$

Conjunción		
ϕ	ψ	$\phi \wedge \psi$
$\mathscr{V}$	$\mathscr{V}$	$\mathscr{V}$
$\mathscr{V}$	$\mathscr{F}$	$\mathscr{F}$
$\mathscr{F}$	$\mathscr{V}$	$\mathscr{F}$
$\mathscr{F}$	$\mathscr{F}$	$\mathscr{F}$

Disyunción		
ϕ	ψ	$\phi \vee \psi$
$\mathscr{V}$	$\mathscr{V}$	$\mathscr{V}$
$\mathscr{V}$	$\mathscr{F}$	$\mathscr{V}$
$\mathscr{F}$	$\mathscr{V}$	$\mathscr{V}$
$\mathscr{F}$	$\mathscr{F}$	$\mathscr{F}$

Implicación		
ϕ	ψ	$\phi \Rightarrow \psi$
$\mathscr{V}$	$\mathscr{V}$	$\mathscr{V}$
$\mathscr{V}$	$\mathscr{F}$	$\mathscr{F}$
$\mathscr{F}$	$\mathscr{V}$	$\mathscr{V}$
$\mathscr{F}$	$\mathscr{F}$	$\mathscr{V}$

Equivalencia lógica		
ϕ	ψ	$\phi \Leftrightarrow \psi$
$\mathscr{V}$	$\mathscr{V}$	$\mathscr{V}$
$\mathscr{V}$	$\mathscr{F}$	$\mathscr{F}$
$\mathscr{F}$	$\mathscr{V}$	$\mathscr{F}$
$\mathscr{F}$	$\mathscr{F}$	$\mathscr{V}$

Cuantificación universal y existencial		
$\phi(x)$	$\forall x\, \phi(x)$	$\exists x\, \phi(x)$
$\phi(a)$ es $\mathscr{V}$ para todo a	$\mathscr{V}$	
$\phi(a)$ es $\mathscr{F}$ para algún a	$\mathscr{F}$	
$\phi(a)$ es $\mathscr{V}$ para algún a		$\mathscr{V}$
$\phi(a)$ es $\mathscr{F}$ para todo a		$\mathscr{F}$

La verdad en matemática (2/2)

Existen al menos dos nociones de verdad en matemática:

2. La verdad a partir de una demostración

(Axioma) $\dfrac{}{\Gamma \vdash \phi}$ si $\phi \in \Gamma$

(⇒) $\dfrac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi}$ $\qquad$ $\dfrac{\Gamma \vdash \phi \Rightarrow \psi \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi}$

(∧) $\dfrac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}$ $\qquad$ $\dfrac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}$ $\qquad$ $\dfrac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}$

(∨) $\dfrac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}$ $\qquad$ $\dfrac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}$ $\qquad$ $\dfrac{\Gamma \vdash \phi \vee \psi \quad \Gamma, \phi \vdash \chi \quad \Gamma, \psi \vdash \chi}{\Gamma \vdash \chi}$

(¬) $\dfrac{\Gamma, \phi \vdash \psi \quad \Gamma, \phi \vdash \neg\psi}{\Gamma \vdash \neg\phi}$ $\qquad$ $\dfrac{\Gamma, \neg\phi \vdash \psi \quad \Gamma, \neg\phi \vdash \neg\psi}{\Gamma \vdash \phi}$

(∀) $\dfrac{\Gamma \vdash \phi}{\Gamma \vdash \forall x\, \phi}$ si $x \notin FV(\Gamma)$ $\qquad$ $\dfrac{\Gamma \vdash \forall x\, \phi}{\Gamma \vdash \phi[x := t]}$

(∃) $\dfrac{\Gamma \vdash \phi[x := t]}{\Gamma \vdash \exists x\, \phi}$ $\qquad$ $\dfrac{\Gamma \vdash \exists x\, \phi \qquad \Gamma, \phi \vdash \psi}{\Gamma \vdash \psi}$ si $x \notin FV(\Gamma, \psi)$

Teorías y modelos

El punto de vista sintáctico: Una teoría $\mathscr{T}$ está definida por

- Un lenguaje $\mathscr{L}$ (definido por sus símbolos de constante/función/predicado)
- Un sistema de deducción (clásico o intuicionista)
- Un sistema de axiomas

El punto de vista semántico: Un modelo $\mathscr{M}$ está definido por:

- Un conjunto $\mathscr{M} \neq \varnothing$ (dominio de la interpretación)
- Elementos, funciones y relaciones (o funciones de verdad) en $\mathscr{M}$ para interpretar los símbolos del lenguaje $\mathscr{L}$
- $\mathscr{M}$ es un modelo de una teoría $\mathscr{T}$ (notación: $\mathscr{M} \models \mathscr{T}$) cuando $\mathscr{M}$ satisface todos los axiomas de $\mathscr{T}$

Propiedad deseada (Corrección)

Si $\mathscr{T} \vdash \phi$, entonces $\mathscr{M} \models \phi$ en todos los modelos $\mathscr{M} \models \mathscr{T}$

Teorías de primer orden

Definición (Teoría de primer orden)

Una teoría de primer orden $\mathscr{T}$ está definida por:

1. un lenguaje de 1er orden $\mathscr{L}$ (definido por sus símbolos de función/predicado)
2. un conjunto de fórmulas cerradas de $\mathscr{L}$: los axiomas de $\mathscr{T}$

Una fórmula cerrada ϕ es un teorema de $\mathscr{T}$ cuando tiene una derivación formal a partir de los axiomas de $\mathscr{T}$. Notación: $\mathscr{T} \vdash \phi$

Note: Derivaciones formales son objetos finitos (listas o árboles finitos) definidos a partir de uno de los sistemas de deducción (equivalentes) para la lógica clásica. Cada derivación formal solo usa un número finito de símbolos y de axiomas de $\mathscr{T}$

Ejemplos de teorías de primer orden:

- La teoría de los grupos
- La teoría de los cuerpos (etc.)
- La Aritmética de Peano (PA)
- La teoría de Zermelo-Fraenkel (ZF)

Interpretación de Tarski de un lenguaje de primer orden

Sea $\mathscr{L}$ un lenguaje de primer orden

Definición (Interpretación de Tarski del lenguaje $\mathscr{L}$)

Una interpretación de Tarski $\mathscr{M}$ de $\mathscr{L}$ está definida por:

- un conjunto no vacío $\mathscr{M} \neq \varnothing$ (el dominio de la interpretación)
- un elemento $c^{\mathscr{M}} \in \mathscr{M}$ para cada símbolo de constante c
- una función $f^{\mathscr{M}} : \mathscr{M}^k \to \mathscr{M}$ para cada símb. de función f (k-ario)
- una función $p^{\mathscr{M}} : \mathscr{M}^k \to \{0,1\}$ para cada símb. de predicado p (k-ario)

Dada una interpretación de Tarski $\mathscr{M}$ de un lenguaje $\mathscr{L}$, se interpretan:

- cada término $t(x_1, \ldots, x_n)$ (con parámetros $a_i \in \mathscr{M}$) por un elemento
$$[\![t]\!]^{\mathscr{M}}(a_1, \ldots, a_n) \qquad (\in \mathscr{M})$$
- cada fórmula $\phi(x_1, \ldots, x_n)$ (con parámetros $a_i \in \mathscr{M}$) por un valor
$$[\![\phi]\!]^{\mathscr{M}}(a_1, \ldots, a_n) \qquad (\in \{0,1\})$$

(interpretando cada conectiva por su tabla de verdad, y $\forall/\exists$ por $\min / \max$)

Modelos de Tarski

Sea $\mathscr{T}$ una teoría de primer orden sobre un lenguaje $\mathscr{L}$

Definición (Modelo de Tarski de $\mathscr{T}$)

Un modelo de Tarski de $\mathscr{T}$ es una interpretación $\mathscr{M}$ del lenguaje $\mathscr{L}$ que satisface todos los axiomas de $\mathscr{T}$. Notación: $\mathscr{M} \models \mathscr{T}$

Por supuesto, si $\mathscr{M} \models \mathscr{T}$, entonces $\mathscr{M}$ también satisface todos los teoremas de $\mathscr{T}$

Ejemplos:

- Los modelos (de Tarski) de la teoría de grupos son... los grupos
- Los modelos (de Tarski) de la teoría de cuerpos son... los cuerpos
- El conjunto $\mathbb{N}$ (equipado con las funciones adecuadas) es el modelo más pequeño de la Aritmética de Peano (PA): el modelo estándar...

  ... pero hay mucho más modelos de PA, de todos los cardinales infinitos
- Si la teoría de conjuntos de Zermelo-Fraenkel (ZF) es consistente, entonces tiene modelos... ¡inclusive modelos numerables!

Propiedades de los modelos de Tarski

Dada una teoría de primer orden $\mathscr{T}$ sobre un lenguaje $\mathscr{L}$:

1. **Completitud:** $\mathscr{T}$ es consistente sii $\mathscr{T}$ tiene un modelo

   Corolario: $\mathscr{T} \vdash \phi$ sii $\mathscr{M} \models \phi$ para todo $\mathscr{M} \models \mathscr{T}$

2. **Compacidad:** $\mathscr{T}$ tiene un modelo sii
   cada conjunto finito de axiomas de $\mathscr{T}$ tiene un modelo

3. **Löwenheim-Skolem:** Si $\mathscr{T}$ tiene un modelo infinito $\mathscr{M}_0$, entonces $\mathscr{T}$ tiene un modelo $\mathscr{M}_\kappa$ de cardinal κ para cada cardinal infinito $\kappa \geq \mathrm{Card}(\mathscr{L})$. Además, se puede construir $\mathscr{M}_\kappa$ tal que:
   - $\mathscr{M}_\kappa$ es elementalmente equivalente a $\mathscr{M}_0$
   - $\mathscr{M}_\kappa \subseteq \mathscr{M}_0$, cuando $\kappa \leq \mathrm{Card}(\mathscr{M}_0)$
   - $\mathscr{M}_\kappa \supseteq \mathscr{M}_0$, cuando $\kappa \geq \mathrm{Card}(\mathscr{M}_0)$

¿Qué es un álgebra de valores de verdad?

- Qué es un conjunto de números?
  - Un anillo, un cuerpo, etc.
- ¿Qué es un espacio de vectores?
  - Un espacio vectorial, un módulo, etc.
- ¿Qué es un espacio de puntos?
  - Un espacio afín, un espacio topológico
- ¿Qué es un álgebra de valores de verdad?
  - Un álgebra booleana
  - $\mathfrak{P}(P)$, donde $(P, \cdot)$ es una PCA
  - $\mathfrak{P}(\Pi)$, donde $(\Lambda, \Pi, \ldots, \perp\!\!\!\perp)$ es una AKS
  - Un álgebra implicativa

Plan

Plan

Intuición fundamental: el orden lógico

- Se define el (pre)orden lógico $\phi \leq \psi$ sobre las proposiciones y la equivalencia asociada $\phi \sim \psi$ por:

$$\begin{array}{lll} \phi \leq \psi & \text{sii} & \phi \Rightarrow \psi \text{ es verdadera} \\ \phi \sim \psi & \text{sii} & \phi \leq \psi \quad \text{y} \quad \psi \leq \phi \\ & \text{sii} & \phi \Leftrightarrow \psi \text{ es verdadera} \end{array}$$

- $\phi \wedge \psi$ (resp. $\phi \vee \psi$) es el ínfimo (resp. el supremo) de ϕ y ψ:

$$\frac{}{(\phi \wedge \psi) \leq \phi} \qquad \frac{}{(\phi \wedge \psi) \leq \psi} \qquad \frac{\chi \leq \phi \quad \chi \leq \psi}{\chi \leq (\phi \wedge \psi)}$$

$$\frac{}{\phi \leq (\phi \vee \psi)} \qquad \frac{}{\psi \leq (\phi \vee \psi)} \qquad \frac{\phi \leq \chi \quad \psi \leq \chi}{(\phi \vee \psi) \leq \chi}$$

- Negación: $\neg\neg\phi \sim \phi$ y $(\phi \leq \psi \quad \text{sii} \quad \neg\psi \leq \neg\phi)$
- Adjunción $\wedge/\rightarrow$: $(\phi \wedge \psi) \leq \chi \quad \text{sii} \quad \phi \leq (\psi \Rightarrow \chi)$

Álgebras booleanas

Definición (Álgebra booleana)

Un álgebra booleana es un conjunto ordenado $\mathscr{B} = (\mathscr{B}, \leq)$ tal que:

1. $\mathscr{B}$ tiene mínimo y máximo:

$$0 := \min(\mathscr{B}) \qquad \text{y} \qquad 1 := \max(\mathscr{B})$$

2. Cada dos elementos $x, y \in \mathscr{B}$ tienen ínfimo y supremo:

$$x \wedge y := \inf\{x, y\} \qquad \text{y} \qquad x \vee y := \sup\{x, y\}$$

3. $\wedge$ (resp. $\vee$) es distributiva con respecto a $\vee$ (resp. $\wedge$):

$$\begin{aligned} x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \\ x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) \end{aligned} \qquad (x, y, z \in \mathscr{B})$$

4. Cada elemento $x \in \mathscr{B}$ tiene un complemento $\neg x \in \mathscr{B}$, tal que:

$$x \wedge \neg x = 0 \qquad \text{y} \qquad x \vee \neg x = 1$$

Álgebra booleana = retículo acotado, distributivo y complementado

Observaciones (1/2)

Álgebra booleana = retículo acotado, distributivo y complementado

- Las dos leyes de distributividad son equivalentes

$$\begin{aligned} x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \\ x \vee (y \wedge z) &= (x \vee y) \vee (x \vee z) \end{aligned} \qquad (x, y, z \in \mathscr{B})$$

- Dichas leyes implican que el complemento $\neg x$ (de cada x) es único

  Es decir: $\neg x$ está definido por $x \wedge \neg x = 0$ y $x \vee \neg x = 1$

- La complementación $x \mapsto \neg x$ es una involución antítona:

$$\neg\neg x = x \qquad \text{y} \qquad (x \leq y \text{ sii } \neg y \leq \neg x)$$

- En particular, la complementación intercambia $\wedge$ con $\vee$:

$$\neg(x \wedge y) = \neg x \vee \neg y \qquad \text{y} \qquad \neg(x \vee y) = \neg x \wedge \neg y$$

Observaciones (2/2)

- Se definen la implicación $x \to y$ y la equivalencia $x \leftrightarrow y$ por:

$$x \to y \;:=\; \neg x \vee y \qquad \text{y} \qquad x \leftrightarrow y \;:=\; (x \to y) \wedge (y \to x)$$

- Tenemos que:

$$\neg(x \to y) \;=\; x \wedge \neg y \qquad \text{y} \qquad \neg(x \leftrightarrow y) \;=\; (x \wedge \neg y) \vee (y \wedge \neg x)$$

- Se puede caracterizar el orden $x \leq y$ mediante cada una de las operaciones $\wedge$, $\vee$ y $\to$:

$$\begin{array}{lll} x \leq y & \text{sii} & x \wedge y = x \\ & \text{sii} & x \vee y = y \\ & \text{sii} & x \to y = 1 \end{array}$$

- La igualdad $x = y$ se caracteriza mediante la operación $\leftrightarrow$:

$$x = y \qquad \text{sii} \qquad x \leftrightarrow y = 1$$

Ejemplos

- $\mathbf{1} := \{0 = 1\}$ (álgebra booleana degenerada)
- $\mathbf{2} := \{0, 1\}$ con $0 < 1$ (álgebra booleana trivial)
- $\mathfrak{P}(X)$ con $\subseteq$ (conjunto potencia)
  - Observar que $\mathbf{1} \simeq \mathfrak{P}(\varnothing)$ y $\mathbf{2} \simeq \mathfrak{P}(\{*\})$

Proposición (Álgebra booleana producto)

El producto $\prod_{i \in I} \mathscr{B}_i$ de una familia $(\mathscr{B}_i)_{i \in I}$ de álgebras booleanas (equipado con el orden producto) también es un álgebra booleana

- Observar que $\mathfrak{P}(X) \simeq \mathbf{2}^X = \prod_{\_ \in X} \mathbf{2}$

Proposición (Álgebras booleanas finitas)

Las álgebra booleanas finitas son las de la forma $\mathscr{B} \simeq \mathbf{2}^n$, con $n \in \mathbb{N}$

Filtros e ideales (1/2)

Sea $\mathscr{B}$ un álgebra booleana

Definición (Filtro / Ideal)

- Un filtro de $\mathscr{B}$ es un subconjunto $F \subseteq \mathscr{B}$ tal que:
  1. $1 \in F$ (F no es vacío)
  2. Si $x \in F$ e $y \geq x$, entonces $x \in F$ (F está cerrado superiormente)
  3. Si $x, y \in F$, entonces $x \wedge y \in F$ (F está cerrado por $\wedge$)
- Un ideal de $\mathscr{B}$ es un subconjunto $I \subseteq \mathscr{B}$ tal que:
  1. $0 \in I$ (I no es vacío)
  2. Si $x \in I$ e $y \leq x$, entonces $x \in I$ (I está cerrado inferiormente)
  3. Si $x, y \in I$, entonces $x \vee y \in I$ (I está cerrado por $\vee$)

Intuición: – Filtro = criterio de verdad = "entorno" de 1
– Ideal = criterio de falsedad = "entorno" de 0

Filtros e ideales (2/2)

- Filtros e ideales son duales, vía complementación:

$$\begin{array}{lll} F \text{ filtro} & \text{sii} & \neg F \text{ ideal} \\ I \text{ ideal} & \text{sii} & \neg I \text{ filtro} \end{array}$$

Escribiendo $\neg X := \{\neg x \mid x \in X\}$ (para $X \subseteq \mathscr{B}$)

- Se puede cocientar un álgebra booleana $\mathscr{B}$ por cualquier filtro $F \subseteq \mathscr{B}$ o por cualquier ideal $I \subseteq \mathscr{B}$ (por dualidad):

$$\begin{array}{rcll} \mathscr{B}/F & := & \mathscr{B}/\!\sim_F, & \text{con} \quad x \sim_F y :\equiv (x \leftrightarrow y) \in F \\ \mathscr{B}/I & := & \mathscr{B}/\!\sim_I, & \text{con} \quad x \sim_I y :\equiv (x \,\Delta\, y) \in I \end{array}$$

Nota: $x \Delta y := (x \wedge \neg y) \vee (y \wedge \neg x) = \neg(x \leftrightarrow y)$ (diferencia simétrica)

Proposición (Álgebra booleana cociente)

El cociente $\mathscr{B}/F$ (resp. $\mathscr{B}/I$) es un álgebra booleana

Otros ejemplos de álgebras booleanas

- Sea $\mathscr{B} := (\mathfrak{P}(X), \subseteq)$, con X infinito. Se definen:

$$\mathcal{I}_X := \{Y \subseteq X \mid Y \text{ finito}\} \quad \text{(conjuntos finitos de } X\text{)}$$
$$\mathcal{F}_X := \{Y \subseteq X \mid Y^c \text{ finito}\} = \neg\mathcal{I}_X \quad \text{(conjuntos cofinitos de } X\text{)}$$

  El álgebra cociente $\mathfrak{P}(X)/\mathcal{I}_X = \mathfrak{P}(X)/\mathcal{F}_X$ no tiene átomos, por lo tanto no es de la forma $\mathfrak{P}(Z)$ para ningún Z (a menos de iso)

- Sea Ω un conjunto. Toda σ-álgebra $\mathcal{A} \subseteq \Omega$ (equipada con $\subseteq$) es una σ-álgebra booleana (i.e. con todos los ínfimos y supremos numerables)

- Sea $(\Omega, \mathcal{A}, \mu)$ un espacio medido. El conjunto

$$[\mu = 0] := \{X \in \mathcal{A} \mid \mu(X) = 0\}$$

  es un σ-ideal de $\mathcal{A}$ (i.e. con todos los supremos numerables).

  El cociente $\mathcal{A}/[\mu = 0]$ también es una σ-álgebra booleana

Ultrafiltros

Proposición y definición (Ultrafiltro)

Para todo filtro $\mathcal{F} \subseteq \mathscr{B}$, las siguientes aserciones son equivalentes:

1. $\mathcal{F}$ es un filtro propio (i.e. $\neq \mathscr{B}$) maximal
2. $\mathcal{F}^c$ $(= \mathscr{B} - \mathcal{F})$ es un ideal de $\mathscr{B}$
3. $\mathcal{F}^c = \neg\mathcal{F}$
4. $\mathscr{B}/\mathcal{F} \simeq \mathbf{2}$

Cuando es el caso, se dice que $\mathcal{F}$ es un ultrafiltro

- El dual de un ultrafiltro es un ideal primo

Teorema del ultrafiltro

Todo filtro propio $\mathcal{F} \subsetneq \mathscr{B}$ se puede extender en un ultrafiltro $\mathcal{U} \supseteq \mathcal{F}$

- El teorema del ultrafiltro es consecuencia del axioma de elección (vía el lema de Zorn), pero es estrictamente más débil

Álgebras booleanas y cálculo proposicional

- Cualquier fórmula $\phi(p, q, r, \ldots)$ del cálculo proposicional se puede interpretar en cualquier álgebra booleana $\mathscr{B}$ por un elemento

$$[\![\phi(x, y, z, \ldots)]\!]^{\mathscr{B}} \in \mathscr{B},$$

usando parámetros $x, y, z, \ldots \in \mathscr{B}$ (arbitrarios) para interpretar las variables proposicionales $p, q, r, \ldots$ que aparecen en la fórmula

- Por ejemplo, si $\phi(p, q, r) \equiv (p \wedge q \Rightarrow r) \Leftrightarrow (\neg q \vee (\neg r \Rightarrow \neg p))$
  entonces $[\![\phi(x, y, z)]\!]^{\mathscr{B}} \equiv (x \wedge y \Rightarrow z) \leftrightarrow (\neg y \vee (\neg z \to \neg x))$

Proposición

Dada una fórmula $\phi(p, q, r, \ldots)$ del cálculo proposicional,
las dos aserciones siguientes son equivalentes:

1. La fórmula $\phi(p, q, r, \ldots)$ es una tautología
2. En toda álgebra booleana $\mathscr{B}$ y para todos $x, y, z, \ldots \in \mathscr{B}$, tenemos que $[\![\phi(x, y, z, \ldots)]\!]^{\mathscr{B}} = 1$

Interpretación de las cuantificaciones

- En un álgebra booleana $\mathscr{B}$, se interpretan las cuantificaciones $\forall x\, \phi(x)$ y $\exists x\, \phi(x)$ por ínfimos y supremos infinitarios:

$$[\![\forall x\, \phi(x)]\!]^{\mathscr{B}} := \bigwedge_{a \in \mathscr{M}} [\![\phi(a)]\!] \qquad [\![\exists x\, \phi(x)]\!]^{\mathscr{B}} := \bigvee_{a \in \mathscr{M}} [\![\phi(a)]\!]$$

  (donde $\mathscr{M}$ representa el dominio de interpretación)

- Para ello, se necesita trabajar en un álgebra booleana $\mathscr{B}$ completa, i.e. que tiene ínfimos/supremos arbitrarios

- **Ejemplos:**
  - El álgebra booleana $(\mathfrak{P}(X), \subseteq) \simeq \mathbf{2}^X$ es completa (para todo X)
  - Si $(\Omega, \mathcal{A}, \mu)$ es un espacio medido σ-finito, entonces el álgebra booleana cociente $\mathcal{A}/[\mu = 0]$ es completa

- **Observación:** En el marco de las álgebras booleanas:

$$\forall \;=\; \wedge \text{ infinitario}$$
$$\exists \;=\; \vee \text{ infinitario}$$

El álgebra de Tarski-Lindenbaum

Sea $\mathscr{T}$ una teoría de primer orden sobre un lenguaje $\mathscr{L}$

- Se equipa el conjunto Φ de las fórmulas cerradas de $\mathscr{L}$ con la relación de equivalencia $\sim$ definida por:

$$\phi \sim \psi \qquad \text{sii} \qquad \mathscr{T} \vdash \phi \Leftrightarrow \psi$$

- El cociente $\mathscr{B} := \Phi/\!\sim$, equipado con el orden definido por

$$[\phi] \leq [\psi] \qquad \text{sii} \qquad \mathscr{T} \vdash \phi \Rightarrow \psi$$

  es un álgebra booleana, llamada álgebra de Tarski-Lindenbaum de $\mathscr{T}$

- El álgebra de Tarski-Lindenbaum captura muchas propiedades de la teoría $\mathscr{T}$, por ejemplo:

$$\begin{aligned} \mathscr{B} &\approx \mathbf{1} && \text{ssi} && \mathscr{T} \text{ inconsistente} \\ \mathscr{B} &\approx \mathbf{2} && \text{ssi} && \mathscr{T} \text{ consistente y completa} \\ \#\mathscr{B} &> 2 && \text{ssi} && \mathscr{T} \text{ consistente e incompleta} \end{aligned}$$

Interpretación booleana de un lenguaje de primer orden

Sea $\mathscr{L}$ un lenguaje de primer orden

Definición (Interpretación booleana del lenguaje $\mathscr{L}$)

Una interpretación booleana $\mathscr{M}$ de $\mathscr{L}$ está definida por:

- un álgebra booleana completa $\mathscr{B}$ (conjunto de los valores de verdad)
- un conjunto no vacío $\mathscr{M} \neq \varnothing$ (dominio de la interpretación)
- un elemento $c^{\mathscr{M}} \in \mathscr{M}$ para cada símbolo de constante c
- una función $f^{\mathscr{M}} : \mathscr{M}^k \to \mathscr{M}$ para cada símbolo de función f (k-ario)
- una función $p^{\mathscr{M}} : \mathscr{M}^k \to \mathscr{B}$ para cada símbolo de predicado p (k-ario)

De modo similar a los modelos de Tarski, se interpretan:

- cada término $t(x_1, \ldots, x_n)$ (con parámetros $a_i \in \mathscr{M}$) por un elemento
$$[\![t]\!]^{\mathscr{M}}(a_1, \ldots, a_n) \qquad (\in \mathscr{M})$$
- cada fórmula $\phi(x_1, \ldots, x_n)$ (con parámetros $a_i \in \mathscr{M}$) por un valor
$$[\![\phi]\!]^{\mathscr{M}}(a_1, \ldots, a_n) \qquad (\in \mathscr{B})$$

Modelos booleanos

- Interpretación de las fórmulas en $\mathscr{B}$:

$$[\![p(t_1,\ldots,t_k)]\!]^{\mathscr{M}} := p^{\mathscr{M}}([\![t_1]\!],\ldots,[\![t_k]\!])$$

$$[\![\neg\phi]\!]^{\mathscr{M}} := \neg[\![\phi]\!]^{\mathscr{M}} \qquad [\![\phi\Rightarrow\psi]\!]^{\mathscr{M}} := [\![\phi]\!]^{\mathscr{M}} \to [\![\psi]\!]^{\mathscr{M}}$$

$$[\![\phi\wedge\psi]\!]^{\mathscr{M}} := [\![\phi]\!]^{\mathscr{M}} \wedge [\![\psi]\!]^{\mathscr{M}} \qquad [\![\phi\vee\psi]\!]^{\mathscr{M}} := [\![\phi]\!]^{\mathscr{M}} \vee [\![\psi]\!]^{\mathscr{M}}$$

$$[\![\forall x\,\phi(x)]\!]^{\mathscr{M}} := \bigwedge_{a\in\mathscr{M}} [\![\phi(a)]\!]^{\mathscr{M}} \qquad [\![\exists x\,\phi(x)]\!]^{\mathscr{M}} := \bigvee_{a\in\mathscr{M}} [\![\phi(a)]\!]^{\mathscr{M}}$$

- Sea $\mathscr{T}$ una teoría de primer orden sobre un lenguaje $\mathscr{L}$:

Definición (Modelo booleano de $\mathscr{T}$)

Un modelo booleano de $\mathscr{T}$ es una interpretación booleana $\mathscr{M}$ del lenguaje $\mathscr{L}$ tal que $[\![\phi]\!]^{\mathscr{M}} = 1_{\mathscr{B}}$ para cada axioma ϕ de $\mathscr{T}$

Más generalmente, tenemos que $[\![\phi]\!]^{\mathscr{M}} = 1_{\mathscr{B}}$ para cada teorema ϕ de $\mathscr{T}$

- Modelos de Tarski = modelo booleano sobre el álgebra $\mathbf{2}$

Operaciones sobre los modelos booleanos

(1) **Producto:** Si para cada $i \in I$, $\mathscr{M}_i$ es un modelo booleano de $\mathscr{T}$ sobre un álgebra $\mathscr{B}_i$, entonces:

$$\prod_{i\in I} \mathscr{M}_i \quad \text{es un modelo booleano de } \mathscr{T} \text{ sobre } \quad \prod_{i\in I} \mathscr{B}_i$$

(2) En particular, si $\mathscr{M}_i$ es un modelo de Tarski de $\mathscr{T}$ para todo $i \in I$:

$$\prod_{i\in I} \mathscr{M}_i \quad \text{es un modelo booleano (lleno) de } \mathscr{T} \text{ sobre } \quad \mathbf{2}^I$$

(3) **Cociente:** Si $\mathscr{M}$ es un modelo booleano (lleno) de $\mathscr{T}$ sobre un álgebra $\mathscr{B}$, y si $\mathcal{U} \subseteq \mathscr{B}$ es un ultrafiltro de $\mathscr{B}$, entonces:

$$\mathscr{M}/\mathcal{U} \quad \text{es un modelo de Tarski de } \mathscr{T}$$

(4) La construcción $\left(\prod_{i\in I} \mathscr{M}_i\right)/\mathcal{U}$ es un ultraproducto ((2) + (3))

Ejemplo: construcción de modelos no estándar

- Sean $\mathscr{M}$ un modelo de una teoría $\mathscr{T}$
  e I un conjunto infinito (por ejemplo $I = \mathbb{N}$)
- Por lo anterior, $\mathscr{M}^I$ es un modelo booleano (lleno) de la teoría $\mathscr{T}$ sobre el álgebra booleana $\mathbf{2}^I$ $(\simeq \mathfrak{P}(I))$
- Cocientando por un ultrafiltro $\mathcal{U} \subseteq \mathbf{2}^I$, se obtiene un nuevo modelo de Tarski:
  $$\mathscr{M}^I/\mathcal{U} \models \mathscr{T}$$ (ultraproducto)
- El ultraproducto $\mathscr{M}^I/\mathcal{U}$ es elementalmente equivalente a $\mathscr{M}$...
  ... pero en general contiene mucho más elementos que $\mathscr{M}$
- Tal construcción se usa para construir modelos de:
  - La aritmética no estándar $(\mathbb{N}^I/\mathcal{U})$
  - El análisis no estándar $(\mathbb{R}^I/\mathcal{U})$
  - La teoría de conjuntos no estándar

Modelos booleanos y forcing

Los modelos booleanos también sirven en forcing para construir extensiones genéricas de modelos de ZF(C)

(ZF = Teoría de conjuntos de Zermelo-Fraenkel, ZFC = ZF + Axioma de Elección)

¿Qué es el forcing?

- Método introducido (Cohen 1963) para demostrar la independencia de la hipótesis del continuo (HC) con respecto a ZFC

  Gödel 1938 ya había demostrado la consistencia relativa de HC, introduciendo los conjuntos constructibles

- Permite extender un modelo de Tarski $\mathscr{M}$ de ZF en otro modelo

  $$\mathscr{M}[G] \supseteq \mathscr{M} \qquad \text{(extensión genérica)}$$

  donde los conjuntos infinitos ($\mathbb{N}$, $\mathbb{R}$, etc.) tienen más subconjuntos

- Basado en la construcción de un modelo booleano particular $\mathscr{M}^{(\mathscr{B})}$ de ZF. Luego: $\mathscr{M}[G] := \mathscr{M}^{(\mathscr{B})}/\mathcal{U}$ ($\mathcal{U}$ = ultrafiltro genérico)

Plan

El intuicionismo de Brouwer

Luitzen Egbertus Jan **Brouwer** (1881–1966)

1908: *De onbetrouwbaarheid der logische principes*
(La desconfiabilidad de los principios de la lógica)

- Rechazo de principios no constructivos, tales como:
  - La ley del tercer excluido ($\phi \vee \neg\phi$)
  - El razonamiento por el absurdo (deducir ϕ de la absurdidad de $\neg\phi$)
  - El axioma de elección, en sus formas más fuertes (Zorn, Zermelo)
- Principios del intuicionismo:
  - Filosofía del sujeto creativo
  - Cada objeto matemático es una construcción de la mente.
    Las pruebas también son construcciones (métodos, reglas...)
  - Rechazo del formalismo de Hilbert (lógica sin reglas)

Brouwer también hizo contribuciones fundamentales en topología clásica...
... para ser aceptado en el mundo académico matemático

La lógica intuicionista (LJ)

Aunque Brouwer era fuertemente opuesto al formalismo, las reglas de la lógica intuicionista (LJ) fueron formalizadas por su estudiante Arend **Heyting** (1898–1980)

1930: *The formal rules of intuitionistic logic*

1956: *Intuitionism. An introduction*

Intuitivamente:

- Las fórmulas $\phi \wedge \psi$ y $\forall x\, \phi(x)$ mantienen su sentido usual, pero las fórmulas $\phi \vee \psi$ y $\exists x\, \phi(x)$ adquieren un sentido más fuerte:
  - Una prueba de $\phi \vee \psi$ tiene que contener una prueba de ϕ o de ψ
  - Una prueba de $\exists x\, \phi(x)$ tiene que contener un testigo x
- La implicación $\phi \Rightarrow \psi$ también adquiere un sentido algorítmico y la negación $\neg\phi$ (definida como $\phi \Rightarrow \bot$) ya no es involutiva

Técnicamente: LJ $\subset$ LK (LK = lógica clásica)

Álgebras de Heyting (1/2)

Ya vimos que: cálculo proposicional clásico $\Leftrightarrow$ álgebras booleanas

Similarmente: cálculo prop. intuicionista $\Leftrightarrow$ álgebras de Heyting

Definición (Álgebra de Heyting)

Un álgebra de Heyting es un conjunto ordenado $(\mathscr{H}, \leq)$ tal que:

1. $\mathscr{H}$ tiene mínimo y máximo:
$$0 := \min(\mathscr{H}) \quad \text{y} \quad 1 := \max(\mathscr{H})$$
2. Cada dos elementos $x, y \in \mathscr{H}$ tienen ínfimo y supremo:
$$x \wedge y := \inf\{x, y\} \quad \text{y} \quad x \vee y := \sup\{x, y\}$$
3. Cada dos elementos $x, y \in \mathscr{H}$ tienen pseudo-complemento relativo
$$x \to y := \max\{z \in \mathscr{H} : (z \wedge x) \leq y\}$$
caracterizado por la adjunción de Heyting:
$$z \leq (x \to y) \quad \Leftrightarrow \quad (z \wedge x) \leq y \qquad \text{(para todos } z \in \mathscr{H})$$

Álgebras de Heyting (2/2)

Álgebra de Heyting = retículo acotado con pseudo-compl. relativo

- La existencia de $x \to y$ implica las leyes de distributividad:

$$\begin{aligned} x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \\ x \vee (y \wedge z) &= (x \vee y) \vee (x \vee z) \end{aligned} \qquad (x, y, z \in \mathscr{H})$$

- Pseudo-complemento definido por $\neg x := x \to 0$. Tenemos que:

$$x \wedge \neg x = 0 \qquad \text{pero} \qquad x \vee \neg x \neq 1 \qquad \text{(en general)}$$

- De mismo modo, tenemos que $x < \neg\neg x$ (en general)

Hecho: $\mathscr{H}$ es un álgebra booleana sii $x \vee \neg x = 1$
sii $\neg\neg x = x$ (para todo $x \in \mathscr{H}$)

- Se pierde la dualidad entre filtros e ideales.
  Los cocientes solo se hacen con filtros: $\mathscr{H}/\mathcal{F}$

Interpretación de Brouwer-Heyting-Kolmogorov (1/3)

Filosofía del constructivismo: El significado de una fórmula ϕ es el conjunto $\boldsymbol{\mathcal{E}}(\phi)$ de las "evidencias" (sentido intuitivo) que ϕ se cumple:

Una evidencia de $\phi \wedge \psi$ es...

- un par $\langle a, b\rangle$, donde $a \in \boldsymbol{\mathcal{E}}(\phi)$ y $b \in \boldsymbol{\mathcal{E}}(\psi)$

... entonces $\boldsymbol{\mathcal{E}}(\phi \wedge \psi) = \boldsymbol{\mathcal{E}}(\phi) \times \boldsymbol{\mathcal{E}}(\psi)$ (Producto cartesiano)

Una evidencia de $\phi \vee \psi$ es o bien...

- de la forma $\mathtt{izq}(a)$, donde $a \in \boldsymbol{\mathcal{E}}(\phi)$, o
- de la forma $\mathtt{der}(b)$, donde $b \in \boldsymbol{\mathcal{E}}(\psi)$

... entonces $\boldsymbol{\mathcal{E}}(\phi \vee \psi) = \boldsymbol{\mathcal{E}}(\phi) + \boldsymbol{\mathcal{E}}(\psi)$ (Suma directa)

Una evidencia de $\phi \Rightarrow \psi$ es...

- una función f que transforma cada $a \in \boldsymbol{\mathcal{E}}(\phi)$ en algún $f(a) \in \boldsymbol{\mathcal{E}}(\psi)$

... entonces $\boldsymbol{\mathcal{E}}(\phi \Rightarrow \psi) = \boldsymbol{\mathcal{E}}(\phi) \to \boldsymbol{\mathcal{E}}(\psi)$ ("funciones computables")

Interpretación de Brouwer-Heyting-Kolmogorov (2/3)

Filosofía del constructivismo: El significado de una fórmula ϕ es el conjunto $\boldsymbol{\mathcal{E}}(\phi)$ de las "evidencias" (sentido intuitivo) que ϕ se cumple:

No hay evidencia de $\bot$...
... entonces $\boldsymbol{\mathcal{E}}(\bot) = \varnothing$ (Conjunto vacío)

Una evidencia de $\forall x\, \phi(x)$ es...

- una función f que asocia a cada objeto $x \in D$ una evidencia $a_x \in \boldsymbol{\mathcal{E}}(\phi(x))$

... entonces $\boldsymbol{\mathcal{E}}(\forall x\, \phi(x)) = \prod_{x \in D} \boldsymbol{\mathcal{E}}(\phi(x))$ ("Producto dependiente")

Una evidencia de $\exists x\, \phi(x)$ es...

- un par $\langle x, a \rangle$, donde $x \in D$ y $a \in \boldsymbol{\mathcal{E}}(\phi(x))$

... entonces $\boldsymbol{\mathcal{E}}(\exists x\, \phi(x)) = \sum_{x \in D} \boldsymbol{\mathcal{E}}(\phi(x))$ ("Suma dependiente")

Interpretación de Brouwer-Heyting-Kolmogorov (3/3)

Filosofía del constructivismo: El significado de una fórmula ϕ es el conjunto $\mathcal{E}(\phi)$ de las "evidencias" (sentido intuitivo) que ϕ se cumple:

$$\begin{aligned}
\mathcal{E}(\phi \wedge \psi) &= \mathcal{E}(\phi) \times \mathcal{E}(\psi) && \text{(Producto cartesiano)}\\
\mathcal{E}(\phi \vee \psi) &= \mathcal{E}(\phi) + \mathcal{E}(\psi) && \text{(Suma directa)}\\
\mathcal{E}(\phi \Rightarrow \psi) &= \mathcal{E}(\phi) \to \mathcal{E}(\psi) && \text{(funciones "computables")}\\
\mathcal{E}(\bot) &= \varnothing && \text{(Conjunto vacío)}\\
\mathcal{E}(\top) &= \{\bullet\} && \text{(Conjunto unitario)}\\
\mathcal{E}(\forall x\ \phi(x)) &= \prod_{x \in D} \mathcal{E}(\phi(x)) && \text{(Producto dependiente)}\\
\mathcal{E}(\exists x\ \phi(x)) &= \sum_{x \in D} \mathcal{E}(\phi(x)) && \text{(Suma dependiente)}
\end{aligned}$$

Ejemplo típico: $\forall x\ \exists y\ \phi(x, y)$

De la filosofía a la matemática

La interpretación (filosófica) de BHK se puede formalizar de modo matemático con la teoría de la realizabilidad [Kleene '45]

- Interpreta cada fórmula ϕ de la aritmética (intuicionista) de 1^{er} orden como el conjunto $[\![\phi]\!]$ de todos los "programas" que realizan ϕ
- **Teorema:** Si $\mathrm{HA} \vdash \phi$, entonces ϕ es realizable

Obs.: HA (Aritmética de Heyting) = Aritmética intuicionista de 1^{er} orden

La interpretación de realizabilidad se extiende a:

- La aritmética intuicionista de 2do orden / de orden superior
- La teoría de conjuntos intuicionista (IZF) [Myhill '73, Friedman '73, McCarty '84]
- Interpretación categórica de la realizabilidad + vínculo con la teoría de topos [Hyland-Johnstone-Pitts '80; Hyland '82]

Álgebras combinatorias parciales (PCA)

Cada interpretación de realizabilidad (de HA, HA2, HAω, IZF, etc.) está parametrizada por un lenguaje de programación abstracto

Definición (Álgebra combinatoria parcial)

Un álgebra combinatoria parcial (PCA) es un conjunto P equipado con una función parcial $(p, q) \mapsto p\,q$ de P^2 a P ("aplicación") tal que existen elementos ("combinadores") $\mathbf{K}, \mathbf{S} \in P$ tales que:

- $\mathbf{K}\,p$, $(\mathbf{K}\,p)\,q$ siempre están definidos, y $(\mathbf{K}\,p)\,q = p$
- $\mathbf{S}\,p$, $(\mathbf{S}\,p)\,q$ siempre está definido; y $((\mathbf{S}\,p)\,q)\,r$ está definido sii $(p\,r)\,(q\,r)$ está definido, y en este caso $((\mathbf{S}\,p)\,q)\,r = (p\,r)\,(q\,r)$

Ejemplos:

- $P := \mathbb{N}$, equipado con la aplicación de Kleene $n \cdot m := f_n(m)$ (donde f_n es la $n$ésima función recursiva parcial)
- $P := \Lambda/{=_\beta}$ (λ-términos cerrados, a menos de β-equivalencia), equipado con la aplicación del cálculo λ

Completitud combinatoria

Debido a los axiomas de $\mathbf{K}$ y $\mathbf{S}$, cada álgebra combinatoria parcial P es combinatoriamente completa, en el sentido en que:

Proposición (Completitud combinatoria)

Para cada expresión aplicativa $E[x_1, \ldots, x_n]$ que involucra las variables $x_1, \ldots, x_n$ (y parámetros en P), existe un combinador $\tilde{E} \in P$ tal que:

$(\cdots(\tilde{E}\, p_1)\cdots p_n)$ está definido sii $E[p_1, \ldots, p_n]$ está definido, y cuando es el caso: $(\cdots(\tilde{E}\, p_1)\cdots p_n) = E[p_1, \ldots, p_n]$

(para todos $p_1, \ldots, p_n \in P$)

Por lo tanto:

- Todos los términos λ cerrados son representables en P
- Todos los enteros $n \in \mathbb{N}$ son representables en P (notación: $\overline{n} \in P$)
- Todas las funciones recursivas parciales son representables en P

En este marco: $\boxed{\text{Álgebra de valores de verdad} = \mathfrak{P}(P)}$

Interpretar la aritmética intuicionista de 1er orden (HA)

Dada un álgebra combinatoria parcial $(P, \cdot)$, se interpretan las fórmulas cerradas de HA (con parámetros en $\mathbb{N}$) del modo siguiente:

$$[\![n = m]\!] := \begin{cases} \{\overline{0}\} & \text{si } n = m \\ \varnothing & \text{si } n \neq m \end{cases} \qquad [\![\bot]\!] := \varnothing$$

$$[\![\phi \wedge \psi]\!] := \{\langle p, q\rangle \ : \ p \in [\![\phi]\!] \ \text{ y } \ q \in [\![\psi]\!]\}$$

$$[\![\phi \vee \psi]\!] := \{\langle \overline{0}, p\rangle \ : \ p \in [\![\phi]\!]\} \cup \{\langle \overline{1}, q\rangle \ : \ q \in [\![\psi]\!]\}$$

$$[\![\phi \Rightarrow \psi]\!] := \{p \in P \ : \ \forall q \in [\![\phi]\!], \ \ p\,q\downarrow \ \text{ y } \ p\,q \in [\![\psi]\!]\}$$

$$[\![\forall x\, \phi(x)]\!] := \{p \in P \ : \ \forall n \in \mathbb{N}, \ \ p\,\overline{n}\downarrow \ \text{ y } \ p\,\overline{n} \in [\![\phi(n)]\!]$$

$$[\![\exists x\, \phi(x)]\!] := \{\langle \overline{n}, p\rangle \ : \ n \in \mathbb{N} \ \text{ y } \ p \in [\![\phi(n)]\!]\}$$

Relación de realizabilidad definida por: $p \Vdash \phi$ sii $p \in [\![\phi]\!]$

Teorema (Corrección) [Kleene '45]

Si $\mathrm{HA} \vdash \phi$, entonces $p \Vdash \phi$ para algún $p \in P$ (en cualquier PCA P)

De la demostración al programa

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\psi(x)\Rightarrow\chi(x)}\,g}{\forall x\,(\psi(x)\Rightarrow\chi(x))}}{\forall x\,(\phi(x)\Rightarrow\psi(x))\ \Rightarrow\ \forall x\,(\psi(x)\Rightarrow\chi(x))}\,\lambda g}{\forall x\,(\phi(x)\Rightarrow\psi(x))\ \Rightarrow\ \forall x\,(\psi(x)\Rightarrow\chi(x))\ \Rightarrow\ \forall x\,(\phi(x)\Rightarrow\chi(x))}\,\lambda f}$$

$$\lambda f\,.\,\lambda g\,.\,\lambda u\,.\,g\,(f\,u)$$

El eslabón perdido

	Forcing ($\wedge = \forall =$ ínfimo)	**Realizabilidad** ($\wedge = \times$, $\forall =$ ínfimo)
Lógica intuicionista	Modelos de Heyting (forcing de Kripke)	Realizabilidad intuicionista
Lógica clásica	Modelos booleanos (forcing de Cohen)	Realizabilidad clásica

- **En forcing:** $\wedge$ y $\forall$ tienen la misma naturaleza:
  - Ambos están interpretados como ínfimos (binarios o infinitarios)
- **En realizabilidad:** $\wedge$ y $\forall$ no tienen la misma naturaleza:
  - $\wedge$ está interpretado como un producto cartesiano
  - $\forall$ aún está interpretado como un ínfimo infinitario

¿Qué es la realizabilidad clásica? [Krivine '94, '00, '03, '09, '11, '12, ...]

- Una reformulación completa de los principios de la realizabilidad de Kleene para acomodarla con el razonamiento clásico

  Reformulación $\neq$ Extensión. Por diseño, la realizabilidad de Kleene es incompatible con la lógica clásica

- Basada en un vínculo entre el razonamiento clásico y los operadores de control descubierto por Griffin '90:

$$\text{call/cc} \ : \ ((\phi \Rightarrow \psi) \Rightarrow \phi) \Rightarrow \phi \qquad \text{(Ley de Peirce)}$$

- Inicialmente diseñada para PA2, pero se extiende a:
  - La aritmética de orden superior (PAω)
  - La teoría de conjuntos de Zermelo-Fraenkel (ZF)
  - Interpreta el Axioma de elección dependiente (DC)
- Vínculos profundos con el forcing de Cohen

Principios de la realizabilidad clásica (1/2)

- Se interpreta cada ϕ por 2 conjuntos: $\begin{cases} [\![\phi]\!]^{\perp\!\!\!\perp} \subseteq \Lambda & \text{(valor de verdad)} \\ [\![\phi]\!] \subseteq \Pi & \text{(valor de falsedad)} \end{cases}$

  donde Λ es el conjunto de los programas y Π el conjunto de las pilas

  (**Intuición:** programa $=$ defensor / pila $=$ atacante)

- Programas y pilas interactúan en procesos $p \star \pi$ $(\in \Lambda \times \Pi)$

- Valor de falsedad $[\![\phi]\!]$ definido por inducción sobre ϕ (noción primitiva)
  y valor de verdad definido por ortogonalidad: (noción derivada)

$$[\![\phi]\!]^{\perp\!\!\!\perp} := \{p \in \Lambda \ : \ \forall \pi \in [\![\phi]\!], \ \ p \star \pi \in \perp\!\!\!\perp\}$$

  donde $\perp\!\!\!\perp \subseteq \Lambda \times \Pi$ (el polo del modelo) es un conjunto de procesos que parametriza la construcción (las "contradicciones")

  (**Obs.:** La operación $[\![\phi]\!] \mapsto [\![\phi]\!]^{\perp\!\!\!\perp}$ es antítona)

Principios de la realizabilidad clásica (2/2)

- Valores de falsedad para $\Rightarrow$ y $\forall$: (punto de vista del atacante)

$$\begin{aligned} [\![\phi \Rightarrow \psi]\!] &:= [\![\phi]\!]^{\perp\!\!\perp} \cdot [\![\psi]\!] = \{p \cdot \pi \ : \ p \in [\![\phi]\!]^{\perp\!\!\perp},\ \pi \in [\![\psi]\!]\} \\ [\![\forall x\, \phi(x)]\!] &:= \bigcup_{v \in \mathscr{M}} [\![\phi(v)]\!] \end{aligned}$$

- Valores de verdad para $\Rightarrow$ y $\forall$: (punto de vista del defensor)

$$\begin{aligned} [\![\phi \Rightarrow \psi]\!]^{\perp\!\!\perp} &:= \left([\![\phi]\!]^{\perp\!\!\perp} \cdot [\![\psi]\!]\right)^{\perp\!\!\perp} \subseteq [\![\phi]\!]^{\perp\!\!\perp} \to [\![\psi]\!]^{\perp\!\!\perp} \\ [\![\forall x\, \phi(x)]\!]^{\perp\!\!\perp} &:= \left(\bigcup_{v \in \mathscr{M}} [\![\phi(v)]\!]\right)^{\perp\!\!\perp} = \bigcap_{v \in \mathscr{M}} [\![\phi(v)]\!]^{\perp\!\!\perp} \end{aligned}$$

- Se definen: $p \Vdash \phi$ sii $p \in [\![\phi]\!]^{\perp\!\!\perp}$
  sii $p \star \pi \in \perp\!\!\perp$ para todo $\pi \in [\![\phi]\!]$

Hecho observacional

Existe un programa $\mathfrak{cc} \Vdash ((\phi \Rightarrow \psi) \Rightarrow \phi) \Rightarrow \phi$ (ley de Peirce)

Máquinas abstractas de Krivine

Definición (Máquina abstracta de Krivine)

Una máquina abstracta de Krivine (AKM) está definida por:

- dos conjuntos Λ (programas) y Π (pilas) (defensores/atacantes)
- una operación $(p, q) \mapsto pq$ de Λ^2 a Λ (aplicación)
- una operación $(p, \pi) \mapsto p \cdot \pi$ de $\Lambda \times \Pi$ a Π ("push")
- una operación $\pi \mapsto [\pi]$ de Π a Λ ("store")
- tres combinadores $\mathbf{K}, \mathbf{S}, \text{cc} \in \Lambda$
- un preorden $\succ$ sobre $\Lambda \times \Pi$ (evaluación), tal que:

$$
\begin{array}{lcll}
pq \star \pi & \succ & p \star q \cdot \pi & (\textsc{Push}) \\
\mathbf{K} \star p \cdot q \cdot \pi & \succ & p \star \pi & (\mathbf{K}) \\
\mathbf{S} \star p \cdot q \cdot r \cdot \pi & \succ & p \star r \cdot qr \cdot \pi & (\mathbf{S}) \\
\text{cc} \star p \cdot \pi & \succ & p \star [\pi] \cdot \pi & (\textsc{Save}) \\
[\pi] \star p \cdot \pi' & \succ & p \star \pi & (\textsc{Restore})
\end{array}
$$

notando $p \star \pi$ al par (p, π)

Estructura abstracta de Krivine

Definición (Estructura abstracta de Krivine)

Una estructura abstracta de Krivine (AKS) es una máquina abstracta de Krivine $(\Lambda, \Pi, @, \cdot, [\_], \mathbf{K}, \mathbf{S}, \text{cc}, \succ)$ equipada con:

- un subconjunto $\mathrm{PL} \subseteq \Lambda$ conteniendo $\mathbf{K}$, $\mathbf{S}$, cc y cerrado por aplicación. Los elementos de PL se llaman casi-pruebas
- un subconjunto $\perp\!\!\!\perp \subseteq \Lambda \times \Pi$ (el polo) cerrado por antievaluación

$$\text{Si} \quad p * \pi \succ p' \star \pi' \quad \text{y} \quad p' \star \pi' \in \perp\!\!\!\perp, \quad \text{entonces} \quad p \star \pi \in \perp\!\!\!\perp$$

- Una fórmula ϕ está realizada cuando: $\quad [\![\phi]\!]^{\perp\!\!\!\perp} \cap \mathrm{PL} \neq \varnothing$

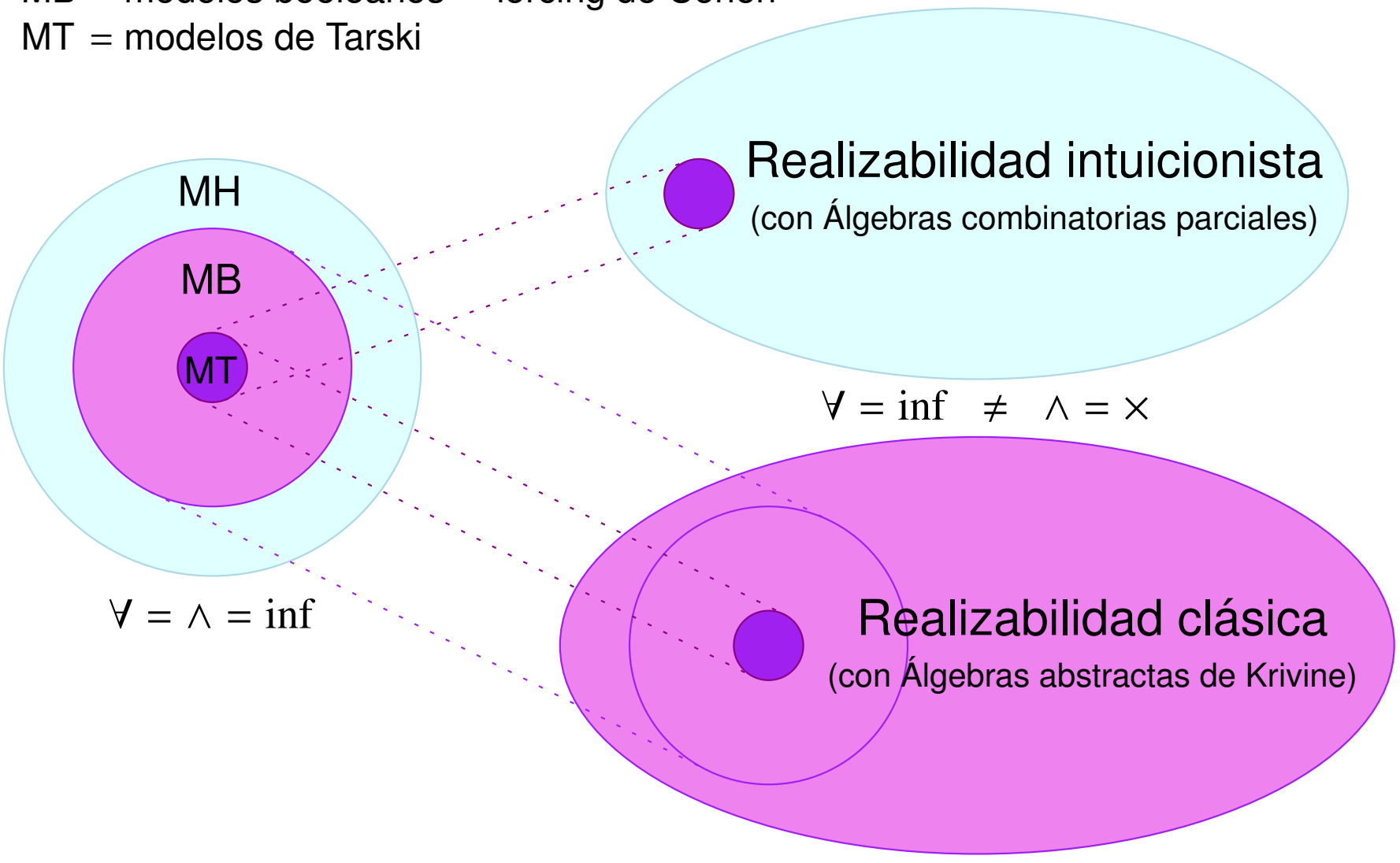
  es decir: $\quad p \Vdash \phi \quad$ para algún $p \in \mathrm{PL}$

En este marco: $\boxed{\text{Álgebra de valores de falsedad} = \mathfrak{P}(\Pi)}$

Plan

Una situación caótica

MH = modelos de Heyting $\approx$ forcing de Kripke
MB = modelos booleanos $\approx$ forcing de Cohen
MT = modelos de Tarski



¿Qué álgebra de valores de verdad?

¿Qué es un álgebra de valores de verdad? (en lógica intuicionista y clásica)

- ¿Un álgebra booleana completa? (forcing de Cohen)
- ¿Un álgebra de Heyting completa? (forcing de Kripke)
- ¿Un álgebra combinatoria parcial? (realizabilidad intuicionista)
- ¿Una estructura abstracta de Krivine? (realizabilidad clásica)

Una larga búsqueda hacia la unificación:

- Streicher '13: *Krivine's classical realizability from a categorical perspective*
- Ferrer *et al* '17: *Ordered combinatory algebras and realizability*
- M. '20: *Implicative algebras: a new foundation for realizability and forcing*

Principios subyacentes a las álgebras implicativas

1. La lógica está basada en **dos** órdenes (sobre los valores de verdad)
   - El orden (primitivo) del subtipado, escrito $a \preccurlyeq b$:

     "cada prueba de a también es una prueba de b" (identidad)
   - El orden (definido) de la consecuencia, escrito $a \vdash b$:

     "cada prueba de a se puede transformar en una prueba de b"

2. La cuantificación universal se deduce del subtipado

$$[\![\forall x\, \phi(x)]\!] = \bigwedge_{v \in \mathscr{M}} [\![\phi(v)]\!] \qquad \text{(ínfimo infinitario)}$$

3. La implicación es primitiva e independiente del subtipado. Las otras conectivas se derivan de la implicación, así como la consecuencia:

$$a \vdash b \qquad \text{sii} \qquad (a \to b) \in S$$

(donde S es un criterio de verdad adecuado)

Estructuras implicativas

Definición (Estructura implicativa)

Una estructura implicativa es una terna $(\mathscr{A}, \preccurlyeq, \to)$ donde

(1) $(\mathscr{A}, \preccurlyeq)$ es un retículo completo

(2) $(\to) : \mathscr{A}^2 \to \mathscr{A}$ es una operación binaria tal que:

(2a) $a' \preccurlyeq a, \;\; b \preccurlyeq b' \quad$ implica $\quad (a \to b) \preccurlyeq (a' \to b') \qquad (a, a', b, b' \in \mathscr{A})$

(2b) $\bigwedge_{b \in B} (a \to b) \;=\; a \to \bigwedge_{b \in B} b \qquad$ (para todo $B \subseteq \mathscr{A}$)

- Se escribe $\bot$ (resp. $\top$) al mínimo (resp. máximo) de $\mathscr{A}$
- Cuando $B = \varnothing$, el axioma (2b) da: $\quad (a \to \top) = \top \qquad (a \in \mathscr{A})$

Ejemplos de estructuras implicativas

- **Álgebras de Heyting completas** $(\mathscr{A}, \preccurlyeq)$, con $\to$ definida por:

  $$a \to b \;:=\; \max\{c \in \mathscr{A} \;:\; (c \curlywedge a) \preccurlyeq b\} \qquad \text{(implicación de Heyting)}$$

- **Álgebras booleanas completas** (como caso particular de lo anterior)

- Dada un álgebra combinatoria total $(P, \cdot)$, se definen:
  - $\mathscr{A} \;:=\; \mathfrak{P}(P)$
  - $a \preccurlyeq b \;:=\; a \subseteq b$
  - $a \to b \;:=\; \{x \in P : \forall z \in a,\; x \cdot z \in b\}$ (implicación de Kleene)

  Nota: si uno hace lo mismo con un álgebra combinatoria parcial, solo se obtiene una estructura casi implicativa, donde $(a \to \top) \neq \top$

- Dada una estructura abstracta de Krivine $(\mathbf{\Lambda}, \mathbf{\Pi}, ..., \perp\!\!\!\perp)$, se definen:
  - $\mathscr{A} \;:=\; \mathfrak{P}(\mathbf{\Pi})$
  - $a \preccurlyeq b \;:=\; a \supseteq b$
  - $a \to b \;:=\; a^{\perp\!\!\!\perp} \cdot b$ (implicación de Krivine)

Definición de las otras construcciones de la lógica

Se usan las codificaciones usuales al segundo orden:

Negación $\quad \neg a := a \to \bot$

Conjunción $\quad a \times b := \bigwedge_{c \in \mathscr{A}} ((a \to b \to c) \to c)$

Disyunción $\quad a + b := \bigwedge_{c \in \mathscr{A}} ((a \to c) \to (b \to c) \to c)$

Cuant. existencial $\quad \exists_{i \in I} a_i := \bigwedge_{c \in \mathscr{A}} \Big(\Big(\bigwedge_{i \in I} (a_i \to c) \Big) \to c \Big)$

Proposición

1. Estás codificaciones son correctas con respecto a las reglas de la lógica intuicionista y clásica
2. Cuando $(\mathscr{A}, \preccurlyeq, \to)$ es un álgebra de Heyting/Boole, tenemos:

$$a \times b = a \curlywedge b, \qquad a + b = a \curlyvee b, \qquad \exists_{i \in I} a_i = \bigvee_{i \in I} a_i$$

Derivando realizadores a partir de los valores de verdad

- Cada elemento $a \in \mathscr{A}$ representa un valor de verdad abstracto, independientemente de cualquier noción de realizador o de prueba

- Sin embargo, existe una codificación $t \mapsto t^{\mathscr{A}}$ del cálculo λ en $\mathscr{A}$, tal que: $t \twoheadrightarrow_\beta u$ implica $t^{\mathscr{A}} \preccurlyeq u^{\mathscr{A}}$

- **Eslogan:** valor de verdad $=$ realizador generalizado

- En una estructura implicativa, la relación $a \preccurlyeq b$ se puede leer:
  - a es un subtipo de b (viendo a y b as como valores de verdad)
  - a realiza b (viendo a como realizador, y b como valor de verdad)
  - a está más definido que b (viendo a y b como realizadores)

  ▶ orden de subtipado $\preccurlyeq$ $=$ orden definicional al revés $\sqsupseteq$

- **Adjunción fundamental:** $\boxed{ab \preccurlyeq c \quad \text{sii} \quad a \preccurlyeq b \to c}$

Definición de un criterio de verdad

Sea $\mathscr{A} = (\mathscr{A}, \preccurlyeq, \to)$ una estructura implicativa

Definición (Separador)

Un separador de $\mathscr{A}$ es un subconjunto $S \subseteq \mathscr{A}$ tal que:

(1) Si $a \in S$ y $a \preccurlyeq b$, entonces $b \in S$ (cerrado superiormente)

(2) $\mathbf{K}^{\mathscr{A}} = (\lambda xy\,.\,x)^{\mathscr{A}} \in S$ y $\mathbf{S}^{\mathscr{A}} = (\lambda xyz\,.\,xz(yz))^{\mathscr{A}} \in S$

(3) Si $(a \to b) \in S$ y $a \in S$, entonces $b \in S$ (modus ponens)

Se dice que $\mathbf{S}$ es consistente (resp. clásico) cuando $\bot \notin S$ (resp. $\mathbf{Peirce}^{\mathscr{A}} \in S$)

- **Intuición:** Separador $S \subseteq \mathscr{A}$ $=$ criterio de verdad (en $\mathscr{A}$)
- Cuando $\mathscr{A}$ es un álgebra de Heyting/Boole completa, la noción de separador coincide con la noción de filtro (pues $ab = a \curlywedge b$)

  Pero en general (i.e. afuera del forcing), los separadores no son filtros (no son cerrados por ínfimos binarios)

Álgebras implicativas

Definición (Álgebra implicativa)

Un álgebra implicativa es una cuádrupla $(\mathscr{A}, \preccurlyeq, \to, S)$ donde

- $(\mathscr{A}, \preccurlyeq, \to)$ es una estructura implicativa
- $S \subseteq \mathscr{A}$ es un separador

- El separador $S \subseteq \mathscr{A}$ induce un preorden de consecuencia:

$$a \vdash_S b \quad :\equiv \quad (a \to b) \in S \qquad \text{(para todos } a, b \in \mathscr{A}\text{)}$$

- El orden cociente de $(\mathscr{A}, \vdash_S)$ se escribe $\mathscr{A}/S$

Proposición

1. El orden cociente $\mathscr{A}/S$ es un álgebra de Heyting
2. Si $\mathbf{Peirce}^{\mathscr{A}} \in S$, entonces $\mathscr{A}/S$ es un álgebra booleana

Obs.: El álgebra de Heyting $\mathscr{A}/S$ es en general no completa

Construcciones

- Las estructuras (álgebras) implicativas se pueden manipular casi del mismo modo que las álgebras de Heyting o de Boole:
  - El producto de una familia de estructuras (resp. álgebras) implicativas es una estructura (resp. álgebra) implicativa
  - El análogo de los utrafiltros son los ultraseparadores
- Los modelos implicativos generalizan los modelos booleanos así como los modelos de realizabilidad (intuicionista y clásica):
  - Los modelos implicativos son cerrados por producto
  - El cociente de un modelo implicativo (lleno) de una teoría $\mathscr{T}$ por un ultraseparator clásico induce un modelo de Tarski de $\mathscr{T}$
- La construcción de los modelos booleanos y de realizabilidad de (I)ZF se generaliza a todas las álgebras implicativas [Maschio-M. '23]

El aspecto categórico

- Cada álgebra implicativa $\mathscr{A}$ induce un tripos $\mathbf{P}_{\mathscr{A}} : \mathbf{Set}^{\mathrm{op}} \to \mathbf{HA}$
  (= modelo categórico de la lógica de orden superior, expresado como un funtor)

- Esta construcción factoriza varias construcciones conocidas:
  - Los triposes de forcing, que corresponden al caso donde $(\mathscr{A}, \preccurlyeq, \to)$ es un álgebra de Heyting/Boole completa y $S = \{\top\}$ (i.e. sin cociente)
  - Los triposes inducidos por las álgebras combinatorias totales...
    ... inclusive por las álgebras combinatorias parciales, usando un truco de completación
  - Los triposes inducidos por las estructuras abstractas de Krivine

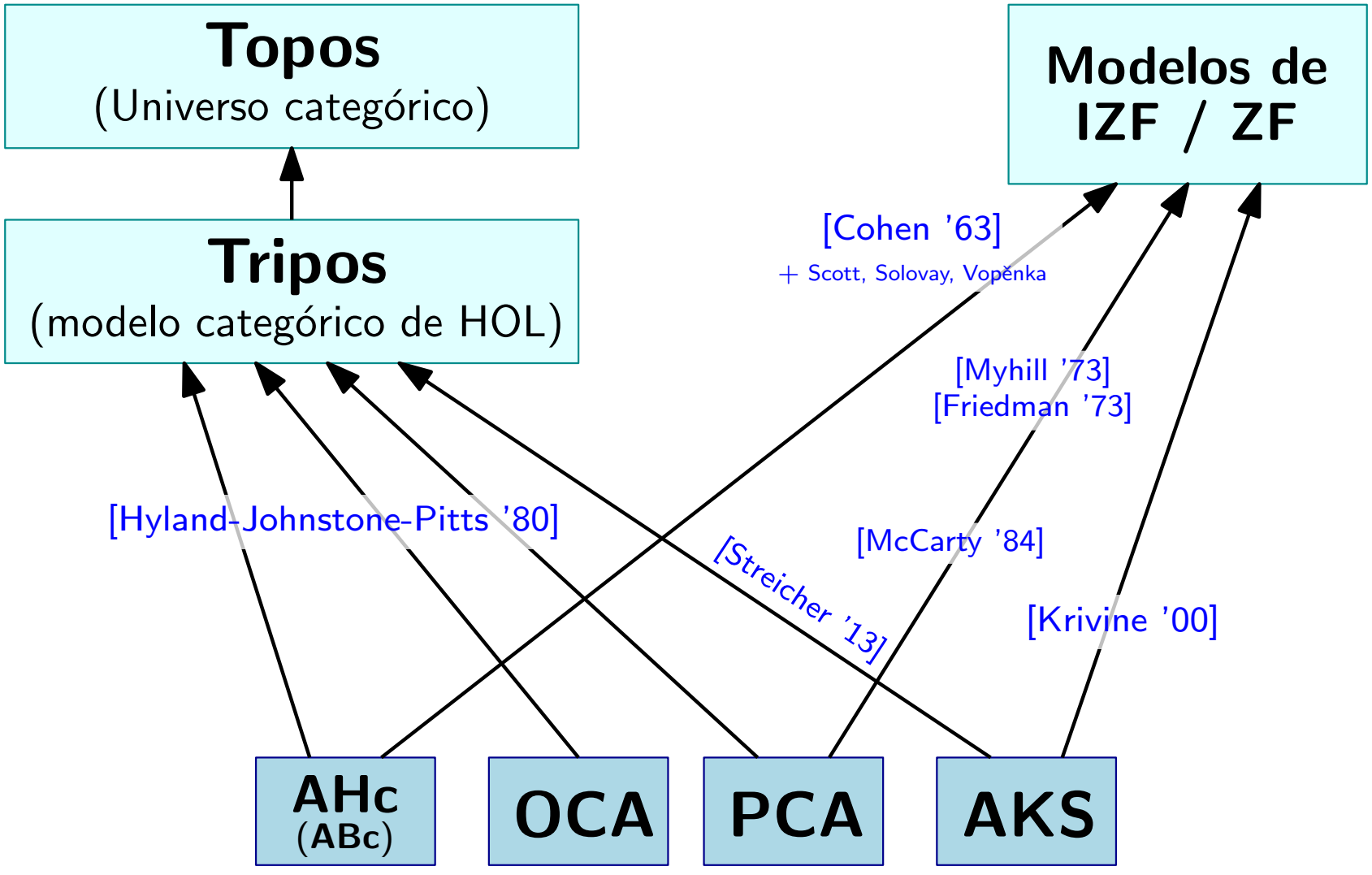
Teorema (Completitud / representación) [M. '20]

Todo tripos (sobre $\mathbf{Set}$) es isomorfo a un tripos implicativo

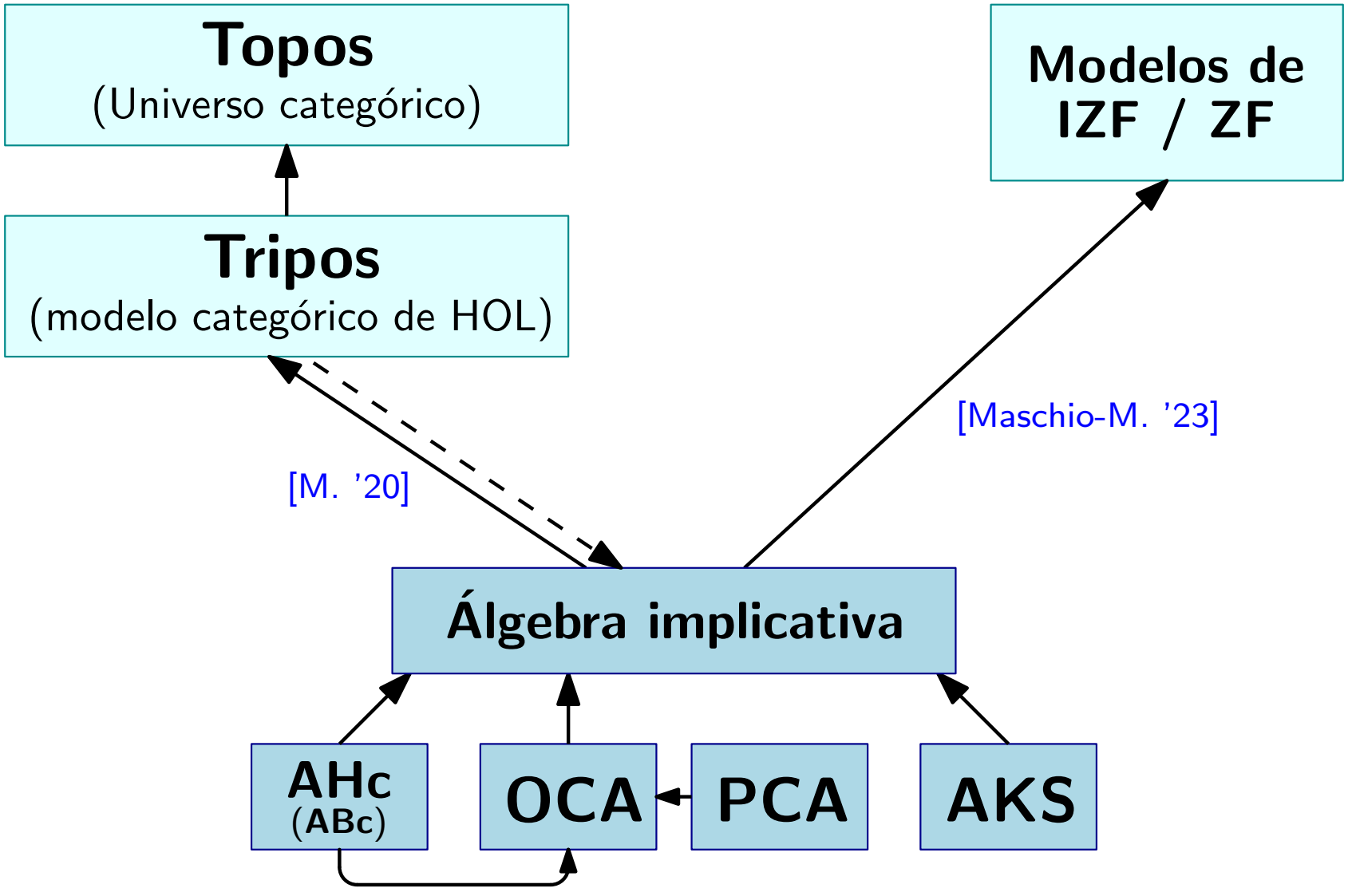
(Las álgebras implicativas constituyen una representación de los triposes)

- Las álgebras implicativas clásicas tienen la misma expresividad que la realizabilidad clásica (inducen exactamente los mismos triposes)

Resumen de la situación antes



Resumen de la situación ahora



¿Qué noción(es) de morfismo(s)?

Definición (Morfismo implicativo) [M. '20]

Sean $\mathscr{A}$ y $\mathscr{B}$ dos álgebras implicativas.
Un mapa $\phi : \mathscr{A} \to \mathscr{B}$ es un morfismo implicativo si:

(1) $\phi(S_{\mathscr{A}}) \subseteq \phi(S_{\mathscr{B}})$

(2) Existe $r_1 \in S_{\mathscr{B}}$ t.q. $a \preccurlyeq a'$ implica $r_1 \preccurlyeq \phi(a) \to \phi(a')$

(3) Existe $r_2 \in S_{\mathscr{B}}$ t.q. $r_2 \preccurlyeq \phi(a \to a') \to \phi(a) \to \phi(a')$

$(a, a' \in \mathscr{A})$

Teorema (Equivalencia de categorías) [Steinberg '23]

Álgebras implicativas
con morfismos implicativos
a menos de equiv. computacional

$\simeq$

Triposes
con transformaciones naturales
que preservan los ínfimos finitos

¿Qué noción de morfismo geométrico?

Una nueva prueba del teorema de completitud

En lógica de 1er orden, la noción de modelo implicativo generaliza los modelos de Tarski/Heyting/Boole. Además:

Teorema (Completitud fuerte para los modelos implicativos) [M. '22]

Para cada teoría clásica $\mathscr{T}$ (de 1er orden), existe un modelo implicativo $\mathscr{M}$ (sobre alguna álgebra implicativa) que captura la teoría $\mathscr{T}$:

$$\mathscr{T} \vdash \phi \qquad \text{sii} \qquad \mathscr{M} \models \phi \qquad (\phi \text{ cerrada})$$

Cocientando por un ultraseparador $U \supseteq S_{\mathscr{A}}$ (si la teoría $\mathscr{T}$ es consistente), se deduce un modelo de Tarski $\mathscr{M}/U$ de $\mathscr{T}$:

$$\mathscr{T} \vdash \phi \qquad \text{implica} \qquad \mathscr{M}/U \models \phi \qquad (\phi \text{ cerrada})$$

Factorization de la completitud de 1er orden

Teoría 1er orden		**Modelo implicativo**		**Modelo de Tarski**
$\boxed{\mathscr{T} \vdash \phi}$	$\Longleftrightarrow$	$\boxed{\mathscr{M} \models \phi}$	$\overset{U}{\Longrightarrow}$	$\boxed{\mathscr{M}/U \models \phi}$
	(constructivo)		(no constr.)	

Conclusión

Las álgebra implicativas permiten factorizar las construcciones de modelos subyacentes al forcing y a la realizabilidad (intuicionistas & clásicos)

- **Idea:** Valores de verdad $\approx$ realizadores generalizados

Demostración = Programa = Tipo = Fórmula

- Cada álgebra implicativa induce un tripos implicativo, y la correspondencia es sobreyectiva (a menos de isomorfismo)
- En esta estructura: forcing = realizabilidad no determinista

Trabajos en marcha:

- Álgebras conjuntivas & disyuntivas [Miquey '20]
- Evidenced Frames [Cohen-Miquey-Tate '22]
- Modelos implicativos de la teoría de conjuntos [Maschio-M. '23]
- Estructura categórica: morfismos implicativos [Steinberg '23]