Tesis de
Maestría en Matemática

PEDECIBA

Montevideo, Uruguay
2024

Una prueba de la independencia de la hipótesis del continuo con reales aleatorios

---

Francisco Carballal

Orientador:

Alexandre Miquel

Facultad de Ingeniería
Universidad de la República

Resumen

A partir de trabajos de Gödel [1] y Cohen [2, 3] del siglo XX , sabemos que la hipótesis del continuo es independiente de la teoría de conjuntos de ZF. En base a esto, tenemos formas de construir modelos donde la hipótesis del continuo se cumple y modelos donde no se cumple. Respecto a los modelos en los que la hipótesis del continuo no se cumple, si bien se demuestra que efectivamente esta no se cumple, no parece haber una intuición clara detrás de la construcción, más allá de aspectos abstractos de cardinalidad.

El objetivo motivador de este trabajo, fue dar una prueba de la consistencia relativa de la negación de la hipótesis del continuo en la que haya una explicación intuitiva de que esta no se cumple en el modelo considerado. Específicamente, construimos un modelo en el que la negación de la hipótesis del continuo se explica con intuiciones de probabilidad. Para esto nos basamos en un artículo de Scott [4], en el que realiza una prueba de la negación de la hipótesis del continuo a partir de álgebras booleanas que provienen de espacios de probabilidad . Esta prueba es en un marco más débil que la teoría de conjuntos de ZF, esencialmente en una teoría de reales de tercer orden (con reales, funciones y funcionales).

En este trabajo, generalizamos la construcción de Scott a una teoría de los números reales expresada en lógica de orden superior, usando una presentación en el estilo de la teoría de tipos simples de Church [5]. Para ello, introducimos la categoría de los B-conjuntos (a saber: conjuntos equipados con B-relaciones de equivalencia), en la cual modelamos nuestra teoría de orden superior. Finalmente, logramos adaptar la prueba de Scott para que la negación de la hipótesis del continuo tenga una explicación intuitiva en base a conceptos de reales aleatorios.

Estructura del documento

En el capítulo 1, presentamos las álgebras booleanas completas y un método para obtener una a partir de un espacio de probabilidad. Este tipo de álgebras booleanas son las que utilizaremos en el capítulo 4 para construir modelos en los que no se cumple la hipótesis del continuo.

En el capítulo 2, introducimos la categoría de los B-conjuntos (notación: B-Set), que brinda un marco algebraico para expresar las construcciones presentadas por Scott y permite naturalmente generalizarlas a un marco de orden superior. Demostramos además que se trata de una categoría cartesiana cerrada completa y estudiamos ciertos tipos de B-conjuntos: los reducidos y los mezclables.

En el capítulo 3, presentamos la lógica de orden superior, introducimos los modelos sobre la categoría B-Set y demostramos varias propiedades de estos modelos, algunas de las cuales son interesantes intrínsecamente y otras de las cuales serán útiles en lo siguiente.

En el capítulo 4, presentamos el B-conjunto $\mathcal{R}$ de los números reales aleatorios, y mostramos cómo dicho B-conjunto permite construir un modelo de nuestra teoría de los «números reales de orden superior» adentro de la categoría de los B-conjuntos. En particular, presentamos una nueva prueba de la negación de la hipótesis del continuo, basada en el estudio del subconjunto $\mathbb{R}$ (reales constantes) incluido en $\mathcal{R}$ (reales aleatorios).

Contribuciones

Las contribuciones de este trabajo son:

- Las nociones de B-conjunto y de B-conjunto mezclable (capítulo 2), así como el estudio de las categorías correspondientes.
- La extensión del modelo de Scott '67 [4] al orden superior (capítulos 3 y 4), usando la noción de B-conjunto mezclable para interpretar el axioma de elección.
- Un nuevo contraejemplo de la hipótesis del continuo (capítulo 4) en lógica de orden superior.

Índice general

Capítulo 1

Álgebras booleanas completas

En este capítulo presentamos las álgebras booleanas y algunas propiedades que utilizaremos frecuentemente durante el resto del trabajo. Luego, haremos la construcción del álgebra booleana completa inducida por un espacio de probabilidad. Este tipo de álgebras booleanas son las que en el capítulo 4 usaremos para construir modelos de los números reales en los que no se cumple la hipótesis del continuo.

1.1. Definiciones, ejemplos y propiedades

Comenzamos con la definición de álgebra booleana. Cada álgebra booleana se puede utilizar como conjunto de valores de verdad para la lógica clásica. La intuición es que tenemos un orden que va desde los elementos más falsos a los más verdaderos. Es decir, $a \leq b$ significará que a es más falso que b, o equivalentemente b más verdadero que a.

Definición 1.1.1. Un *álgebra booleana* es un conjunto ordenado $(B, \leq)$ que cumple:

1. Existen mínimo, denotado 0, y máximo, denotado 1.
2. Para todos $a, b \in B$ existen ínfimo y supremo de $\{a, b\}$, denotados $a \wedge b$ y $a \vee b$, respectivamente.
3. Cada una de las dos operaciones $\wedge$ y $\vee$ es distributiva con respecto a la otra, es decir, para todos $a, b, c \in B$:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \qquad \text{y} \qquad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

4. Todo elemento $a \in B$ tiene un complemento, $a^* \in B$, definido por $a \vee a^* = 1$ y $a \wedge a^* = 0$.

Decimos que el álgebra booleana es *completa* si además existen ínfimos y supremos de subconjuntos arbitrarios, para los que se usan los símbolos $\bigwedge$ y $\bigvee$, respectivamente.

Observar que los items 1 y 2 de la definición implican que $(B, \leq)$ es un retículo acotado, o equivalentemente que tiene todos los supremos e ínfimos de conjuntos finitos (la existencia de 0 y 1 es importante porque $\bigwedge \varnothing = 1$ y $\bigvee \varnothing = 0$). La distributividad permite demostrar que los complementos son únicos. Dados b, b' complementos de a,

tenemos que $b = b \wedge (b' \vee a) = (b \wedge b') \vee (b \wedge a) = b \wedge b'$. Concluimos que $b = b \wedge b'$, lo cual significa que b es el ínfimo del conjunto $\{b, b'\}$ y por lo tanto $b \leq b'$. Realizando el razonamiento simétrico tenemos que $b' \leq b$ y por lo tanto son iguales.

Dados $a, b \in B$ se definen las siguientes dos operaciones:

$$a \to b \ := \ a^* \vee b \qquad a \leftrightarrow b \ := \ (a \to b) \wedge (b \to a)$$

Cuando no genere ambigüedad, diremos que B es un álgebra booleana, sin hacer referencia al orden, el cual usualmente será denotado $\leq$. La precedencia es la siguiente: primero los operadores unarios ($\_^*$ antes que $\bigwedge$ y $\bigvee$), luego las conjunciones ($\wedge$), luego las disyunciones ($\vee$) y finalmente las implicaciones y equivalencias ($\to$ y $\leftrightarrow$).

Ejemplos.

1. El álgebra booleana degenerada, $1 = \{0\}$, conformada por un único elemento que es a su vez mínimo y máximo. Esta álgebra booleana representa una lógica inconsistente.

2. El álgebra booleana trivial, $2 = \{0, 1\}$, con $0 \neq 1$. Esta álgebra booleana representa la lógica clásica usual, en la que los dos valores de verdad son «falso» y «verdadero».

3. Dado A un conjunto, $(\mathcal{P}(A), \subseteq)$ es un álgebra booleana completa, donde

$$\begin{array}{lll} a \wedge b = a \cap b & \bigwedge B = \bigcap B & a^* = a^C \\ a \vee b = a \cup b & \bigvee B = \bigcup B & \end{array}$$

4. Si $(B_i, \leq_i)_{i \in I}$ es una familia de álgebras boolenas, el producto $(\Pi_{i \in I} B_i, \leq)$ también es una álgebra booleana con el orden definido por:

$$f \leq g \ \Leftrightarrow \ \forall i \in I \ f(i) \leq_i g(i)$$

   Observar que el álgebra degenerada es el producto de la familia vacía y el álgebra $(\mathcal{P}(A), \leq)$ es isomorfa (como conjunto ordenado) a 2^A.

En la sección 1,2 se presentan otro tipo de álgebras booleanas completas, las inducidas por espacios de probabilidad, que serán un concepto central en el capítulo 4.

Probaremos ahora algunas propiedades de las álgebras booleanas que serán utilizadas extensivamente en el resto del trabajo.

Lema 1.1.2. *Dada un álgebra booleana B y tres elementos $a, b, c \in B$:*

1. $c \leq a \to b$ *sii* $c \wedge a \leq b$

2. $a \leq b$ *sii* $a \to b = 1$
   sii $a \wedge b = a$
   sii $a \vee b = b$

3. $a = b$ *sii* $a \leftrightarrow b = 1$

4. $a \leq b$ *sii* $b^* \leq a^*$

Demostración. 1. ($\Rightarrow$) Por definición de $\to$ tenemos $c \leq a^* \vee b$. Se deduce $c \wedge a \leq (a^* \vee b) \wedge a$. Luego se concluye usando distributividad como sigue.

$$\begin{aligned} c \wedge a &\leq (a^* \vee b) \wedge a \\ &= (a^* \wedge a) \vee (b \wedge a) \\ &= 0 \vee (b \wedge a) \\ &= b \wedge a \leq b \end{aligned}$$

($\Leftarrow$) Es el razonamiento dual. Aplicando $\vee a^*$ a ambos lados y usando distributiva, tenemos $c \vee a^* \leq b \vee a^*$. Por lo tanto, $c \leq c \vee a^* \leq b \vee a^* = a \to b$.

2. La primera equivalencia se deduce del ítem anterior en el caso en que $c = 1$. Por otra parte, de las definiciones de $\wedge$ y $\vee$ se deduce que $a \leq b$ es equivalente a que $a = a \wedge b$ y a que $a \vee b = b$.

3. Es consecuencia del anterior y la antisimetría de $\leq$.

4. Usando el item 2 y que todo elementos es igual a su doble complementos, tenemos que $a \leq b$ si y solo si $a \to b = 1$, si y solo si $a^* \vee b = 1$, si y solo si $(b^*)^* \vee a^* = 1$, si y solo si $b^* \to a^* = 1$, si y solo si $b^* \leq a^*$. La operación $\vee$ es conmutativa por definición. □

Lema 1.1.3. *Sea B un álgebra booleana.*

1. *Dados $a_1, a_2, b \in B$, si $a_1 \leq a_2$ entonces $\quad a_1 \wedge b \leq a_2 \wedge b \quad$ y $\quad a_1 \vee b \leq a_2 \vee b$.*

2. *Dados un elemento $a \in B$ y una familia $(b_i)_{i \in I}$ de elementos de B con supremo e ínfimo, se cumplen:*

   a) $\bigwedge_{i \in I} b_i \wedge a = \bigwedge_{i \in I} (b_i \wedge a)$
   b) $\bigwedge_{i \in I} b_i \vee a = \bigwedge_{i \in I} (b_i \vee a)$
   c) $\bigvee_{i \in I} b_i \wedge a = \bigvee_{i \in I} (b_i \wedge a)$
   d) $\bigvee_{i \in I} b_i \vee a = \bigvee_{i \in I} (b_i \vee a)$

3. *Dada una familia $(b_i)_{i \in I}$ de elementos de B con supremo e ínfimo y tal que $(b_i^*)_{i \in I}$ también tiene supremo e ínfimo, se cumplen las leyes de De Morgan:*

$$\left(\bigvee_{i \in I} b_i \right)^* = \bigwedge_{i \in I} b_i^* \qquad \left(\bigwedge_{i \in I} b_i \right)^* = \bigvee_{i \in I} b_i^*$$

Demostración. 1. $a_1 \wedge b$ es cota inferior de $\{a_2, b\}$, por lo tanto es menor o igual al ínfimo. Por otra parte, $a_2 \vee b$ es cota superior de $\{a_1, b\}$ y por lo tanto es mayor o igual al supremo.

2. Probaremos a) y b), ya que las otras dos son duales. Para probar a), alcanza demostrar que $\{\bigwedge_{i \in I} b_i, a\}$ y $\{b_i \wedge a\}_{i \in I}$ tienen las mismas cotas inferiores. Esto se deduce de que $c \leq \bigwedge_{i \in I} b_i$ si y solo si $c \leq b_i$ para todo $i \in I$, y que $c \leq b_i \wedge a$ si y solo si $c \leq b_i$ y $c \leq a$. Veamos ahora que se cumple b).

Dado $j \in I$, tenemos que $\bigwedge_{i \in I} b_i \vee a \leq b_j \vee a$, por lo que $\bigwedge_{i \in I} b_i \vee a$ es una cota inferior. Sea c cota inferior de $\{b_i \vee a\}_{i \in I}$. Queremos probar $c \leq \bigwedge_{i \in I} b_i \vee a$. Dado $i \in I$, tenemos que $c \leq a^* \to b_i$, lo cual equivale a que $c \wedge a^* \leq b_i$. Por lo tanto, $c \wedge a^* \leq \bigwedge_{i \in I} b_i$ lo cual equivale a $c \leq a^* \to \bigwedge_{i \in I} b_i = \bigwedge_{i \in I} b_i \vee a$.

3. Observar que si probamos al primera igualdad, aplicándola a la familia $(b_i^*)_{i\in I}$ obtenemos la segunda. Vamos a probar que $\bigwedge_{i\in I} b_i^*$ es el complemento de $\bigvee_{i\in I} b_i$. Primero veamos que la disyunción vale 1.

$$\bigvee_{j\in I} b_j \vee \bigwedge_{i\in I} b_i^* \;=\; \bigwedge_{i\in I}\left(\bigvee_{j\in I} b_j \vee b_i^*\right) \;\geq\; \bigwedge_{i\in I}(b_i \vee b_i^*) \;=\; 1$$

Veamos ahora que la conjunción vale 0.

$$\bigvee_{i\in I} b_i \wedge \bigwedge_{j\in I} b_j^* \;=\; \bigvee_{i\in I}\left(b_i \wedge \bigwedge_{j\in I} b_j^*\right) \;\leq\; \bigvee_{i\in I}(b_i \wedge b_i^*) \;=\; 0 \qquad \square$$

Una propiedad de las álgebras booleanas que aporta intuición es que satisfacen todas las tautologías de la lógica clásica proposicional (sin cuantificadores). No entraremos ahora en detalles respecto a cómo enunciarlo precisamente ni cómo demostrarlo (en el teorema 3.3.10 probaremos algo más general). A modo ilustrativo, así como en lógica proposicional se puede derivar $\neg(\phi \wedge \psi) \Leftrightarrow \neg\phi \vee \neg\psi$, en cualquier álgebra booleana B, para todos $a, b \in B$ se cumple $(a\wedge b)^* \leftrightarrow a^* \vee b^* = 1$, o equivalentemente, $(a\wedge b)^* = a^* \vee b^*$.

Pasamos ahora a definir anticadenas, particiones de la unidad y la condición de cadenas numerables, conceptos comúnmente presentes al analizar cardinalidad en modelos booleanos.

Definición 1.1.4 (Anticadenas y particiones de la unidad)**.** Una *anticadena* de B es un subconjunto $A \subseteq B$ cuyos elementos son incompatibles dos a dos, es decir que para todos $a_1, a_2 \in A$ tales que $a_1 \neq a_2$, se cumple $a_1 \wedge a_2 = 0$. Una *partición de la unidad* es una anticadena $C \subseteq B$ tal que $\bigvee C = 1$.

Definición 1.1.5 (Condición de cadenas numerables)**.** Sea B un álgebra booleana. Decimos que B cumple la *condición de cadenas numerables* (o *ccc*) si todas las anticadenas de B son de cardinal a lo sumo numerable.

Con respecto a la «condición de cadenas numerables», una explicación de la nomenclatura utilizada se encuentra en [6] (capítulo 7, página 84). El siguiente lema será de utilidad en la sección 1.2.

Lema 1.1.6. *Si B es un álgebra booleana que cumple la c.c.c. y en que toda familia numerable tiene supremo, entonces B es completa. Además, cada supremo o ínfimo de una familia infinita es igual al de una subfamilia numerable.*

Demostración. Por propiedad de álgebras booleanas, para la completitud alcanza probar que existen todos los supremos (el ínfimo de un conjunto es igual al supremo del conjunto de sus cotas inferiores). Sin pérdida de generalidad se puede trabajar con familias indizadas por ordinales. Vamos a demostrar por inducción en ρ que toda familia $(b_\alpha)_{\alpha<\rho}$ de elementos de B indizada por el ordinal ρ tiene supremo y es igual al de un subconjunto numerable.

Definimos otra familia $(e_\alpha)_{\alpha<\rho}$ indizada en ρ:

$$e_\alpha = b_\alpha - \bigvee_{\beta<\alpha} b_\beta = b_\alpha \wedge \bigwedge_{\beta<\alpha} b_\beta^*$$

Donde los supremos existen por hipótesis inductiva. Por como está definido, $\{e_\alpha \,/\, \alpha < \rho\}$ es una anticadena, lo cual por la ccc implica que es numerable. Tenemos entonces que la imagen de la familia $(e_\alpha)_{\alpha<\rho}$ es numerable. Como para todos $\alpha \neq \beta$ tenemos que $e_\alpha \wedge e_\beta = 0$, el único elemento que puede repetirse es 0 (no pueden haber $\alpha \neq \beta$ tales que $e_\alpha = e_\beta \neq 0$). Esto implica que existe $(\alpha_n)_{n\in\omega}$ tal que para todos los otros α, tenemos que $e_\alpha = 0$ (es decir, los únicos α para los que e_α puede ser no nulo son los α_n).

Observamos que si $e_\alpha = 0$, entonces $b_\alpha \leq \bigvee_{\beta<\alpha} b_\beta$, por la definición de e_α. Veamos por que para todo $\alpha < \rho$:

$$b_\alpha \leq \bigvee_{n\in\omega} b_{\alpha_n}$$

donde sabemos que existe el supremo por ser de un conjunto numerable (hipótesis). Lo probamos por inducción transfinita en α (debemos probarlo para cada ordinal $\alpha < \rho$ teniendo como hipótesis que se cumple para todos los $\beta < \alpha$). El caso en que $\alpha = \alpha_n$ para algún n es directo. Si α no es ningún α_n, tenemos que $e_\alpha = 0$ y por lo tanto $b_\alpha \leq \bigvee_{\beta<\alpha} b_\beta$, por lo que se deduce de la hipótesis inductiva.

Acabamos de probar que que $\bigvee_{n\in\omega} b_{\alpha_n}$ es cota superior de $\{b_\alpha\}_{\alpha<\rho}$. Como $\{\alpha_n\}_{n\in\omega} \subseteq \rho$ tenemos que es la menor. Por lo tanto, $\bigvee_{\alpha<\rho} b_\alpha = \bigvee_{n\in\omega} b_{\alpha_n}$. Probamos que el supremo existe y es igual al de un subconjunto numerable, como queríamos.

Como mencionamos, la existencia de todos los supremos implica la existencia de todos los ínfimos y además por las leyes de De Morgan, también se cumple que los ínfimos de familias arbitrarias son iguales a los de una subfamilia numerable.

$$\bigwedge_{\alpha<\rho} b_\alpha = \left(\bigvee_{\alpha<\rho} b_\alpha^*\right)^* = \left(\bigvee_{n\in\omega} b_{\alpha_n}^*\right)^* = \bigwedge_{n\in\omega} b_{\alpha_n} \qquad \square$$

1.1.1. Ideales, filtros y cocientes

En la sección 1.2, construiremos un álgebra booleana completa cocientando otra respecto a un ideal. En esta subsección presentamos las definiciones y resultados necesarios.

Definición 1.1.7 (Ideales y filtros)**.** Un *ideal* de B es un subconjunto $I \subseteq B$ no vacío, cerrado hacia abajo y por disyunciones. Equivalentemente:

1. $0 \in I$.
2. Para todos $a, b \in B$, si $a \leq b$ y $b \in I$, entonces $a \in I$.
3. Para todos $a, b \in I$, se cumple $a \vee b \in I$.

Por otra parte, un *filtro* de B es un subconjunto $F \subseteq B$ no vacío, cerrado hacia arriba y por conjunciones. Equivalentemente:

1. $1 \in F$.
2. Para todos $a, b \in B$, si $a \leq b$ y $a \in F$, entonces $b \in F$.
3. Para todos $a, b \in F$, se cumple $a \wedge b \in F$.

Observar que en ambos conceptos, considerando el punto 2, el 1 es equivalente a que el subconjunto sea no vacío. Por otra parte, además de ser intuitivamente conceptos duales, están en correspondencia uno a uno mediante la siguiente biyección:

$$I \ \mapsto \ F = I^* = \{a^* \ / \ a \in I\}$$

En palabras, dado un ideal, el conjunto de los complementos de sus elementos (que no tiene por qué coincidir con el complemento del ideal) es un filtro y dado un filtro, el conjunto de los complementos de sus elementos es un ideal.

Lema 1.1.8 (álgebra booleana cociente)**.** *Dada un álgebra booleana $(B, \leq)$ y un ideal $\mathcal{I}$, la siguiente es una relación de equivalencia sobre B compatible con conjunciones disyunciones y complementos:*

$$a \sim b \ \Leftrightarrow \ a \triangle b \in \mathcal{I} \ \Leftrightarrow \ (a \wedge b^*) \vee (a^* \wedge b) \in \mathcal{I}$$

Además, el conjunto cociente $B/\mathcal{I}$ hereda estructura de álgebra booleana con el orden dado por $[a] \leq [b]$ si y solo si $[a \wedge b] = [a]$. Además, las operaciones booleanas finitas bajan al cociente, en el sentido de que:

1. *Para todos $a, b \in B$, $\quad [a] \wedge [b] = [a \wedge b]$.*
2. *Para todos $a, b \in B$, $\quad [a] \vee [b] = [a \vee b]$.*
3. *Para todo $a \in B$, $\quad [a]^* = [a^*]$*

Demostración. Que $\sim$ es reflexiva y simétrica es directo. Veamos la transitividad. Sean $a, b, c \in B$ tales que $a \sim b$ y $b \sim c$. Queremos probar que $(a \wedge c^*) \vee (a^* \wedge c) \in \mathcal{I}$. Como es un ideal, alcanza probar que $a \wedge c^* \in \mathcal{I}$ y que $a^* \wedge c \in \mathcal{I}$. Veamos uno de los dos, ya que son simétricos. Observamos que $a \wedge c^* = a \wedge c^* \wedge b \vee a \wedge c^* \wedge b^*$ (usamos que $b \vee b^* = 1$ y la distributividad; en toda la prueba la intuición proviene del álgebra booleana $(\mathcal{P}(X), \subseteq)$). Como $a \wedge c^* \wedge b \leq b \wedge c^* \in \mathcal{I}$, tenemos que también está en $\mathcal{I}$. Lo mismo se cumple para $a \wedge c^* \wedge b^*$ con $a \wedge b^*$, por lo que también está en $\mathcal{I}$ y concluimos que la disyunción entre los dos también está.

Veamos ahora que la relación es compatible con conjunciones, disyunciones y complementos. Sean $a_1, a_2, b_2, b_2 \in B$ tales que $a_1 \sim a_2$ y $b_1 \sim b_2$. Queremos probar que $a_1 \wedge b_1 \sim a_2 \wedge b_2$, que $a_1 \vee b_1 \sim a_2 \vee b_2$ y $a_1^* \sim a_2^*$. Para probar que $a_1 \wedge b_1 \sim a_2 \wedge b_2$ debemos ver que $(a_1 \wedge b_1) \triangle (a_2 \wedge b_2) \in \mathcal{I}$. Como $\mathcal{I}$ es ideal, alcanza $(a_1 \wedge b_1) \wedge (a_2 \wedge b_2)^* \in \mathcal{I}$ y $(a_1 \wedge b_1)^* \wedge (a_2 \wedge b_2) \in \mathcal{I}$. Veamos el primero, pues el otro es análogo.

$$(a_1 \wedge b_1) \wedge (a_2 \wedge b_2)^* = (a_1 \wedge b_1) \wedge (a_2^* \vee b_2^*) = (a_1 \wedge b_1 \wedge a_2^*) \vee (a_1 \wedge b_1 \wedge b_2^*)$$

Tenemos que $a_1 \wedge b_1 \wedge a_2^* \in \mathcal{I}$ porque $a_1 \wedge a_2^* \in \mathcal{I}$ y que $a_1 \wedge b_1 \wedge b_2^* \in \mathcal{I}$ porque $b_1 \wedge b_2^* \in \mathcal{I}$. Para probar que $a_1 \vee b_1 \sim a_2 \vee b_2$ se razona de la misma forma. Alcanza probar $(a_1 \vee b_1) \wedge (a_2 \vee b_2)^* \in \mathcal{I}$. La cuenta es muy similar a la anterior.

$$(a_1 \vee b_1) \wedge (a_2 \vee b_2)^* = (a_1 \vee b_1) \wedge (a_2^* \wedge b_2^*) = (a_1 \wedge a_2^* \wedge b_2^*) \vee (b_1 \wedge a_2^* \wedge b_2^*)$$

La conclusión es análoga. Para probar que $a_1^* \sim a_2^*$ hay que probar que $a_1^* \wedge a_2 \in \mathcal{I}$ y $a_1^{\wedge} a_2^* \in \mathcal{I}$, las cuales se deducen directamente de que $a_1 \sim a_2$.

Sabiendo que $\sim$ es una relación de equivalencia compatible con conjunciones disyunciones y complementos, podemos definir en $B/\mathcal{I}$ la relación $[a] \leq [b] \Leftrightarrow [a \wedge b] = [a]$. Probaremos ahora que es un orden y luego que las conjunciones, disyunciones y complementos bajan al cociente. Luego se deducirá que es una álgebra booleana usando que B lo es y que las operaciones bajan al cociente.

Veamos que la relación definida es un orden. Dado $a \in B$, es claro que $[a] \leq [a]$. Dados $a, b \in B$, si $[a] \leq [b]$ y $[b] \leq [a]$, usando la conmutatividad de $\wedge$ tenemos que $[a] = [b]$. Finalmente, sean $a, b, c \in B$ tales que $[a] \leq [b]$ y $[b] \leq [c]$. Como $[b \wedge c] = [b]$, tenemos que $b \wedge c \sim b$ y por la compatibilidad de $\wedge$ deducimos que $a \wedge (b \wedge c) \sim a \wedge b$. Por lo tanto, $[a \wedge (b \wedge c)] = [a \wedge b] = [a]$ (acabamos de usar también que $[a] \leq [b]$). Por otra parte, tenemos que $a \wedge b \sim a$, por lo tanto $(a \wedge b) \wedge c \sim a \wedge c$ y finalmente $[(a \wedge b) \wedge c] = [a \wedge c]$. Concluimos usando que $\wedge$ es asociativo.

Nos encaminamos a demostrar que las conjunciones, disyunciones y complementos bajan al cociente. En el caso de las conjunciones por ejemplo, esto quiere decir que para todos $a, b \in B$, existe $[a] \wedge [b]$ (el ínfimo del conjunto $\{[a], [b]\}$) y es igual a $[a \wedge b]$. Notar que no se deducen directamente de que la relación de equivalencia sea compatible con las operaciones.

Vamos a utilizar que $[a] \leq [b]$ es equivalente a que exista $a' \sim a$ tal que $a' \leq b$ y también a que exista $b' \sim b$ tal que $a \leq b'$. Comenzamos con la primera equivalencia. El recíproco se deduce de que la relación $\sim$ es compatible con $\wedge$, pues $[a \wedge b] = [a' \wedge b] = [a'] = [a]$. Para el directo, dados $a, b \in B$ tales que $[a] \leq [b]$, podemos usar $a' := a \wedge b$. Por hipótesis tenemos que $a' \sim a$ y por definición tenemos que $a' \leq b$. Para la otra equivalencia también se utiliza la compatibilidad en una dirección y en la otra se utiliza $b' = b \vee a$.

Sean $a, b \in B$. Queremos probar que $[a] \wedge [b] = [a \wedge b]$. Sea $c \in B$ tal que $[c] \leq [a]$ y $[c] \leq [b]$. Podemos asumir que existen c_1, c_2 tales que $c_1 \leq a$, $c_2 \leq b$ y $c \sim c_1 \sim c_2$. Consideramos $\hat{c} := c_1 \wedge c_2$. Veamos que $c \sim \hat{c}$.

$$\hat{c} \wedge c^* = c_1 \wedge (c_2 \wedge c^*) \quad c \wedge \hat{c}^* = (c \wedge c_1^*) \vee (c \wedge c_2^*)$$

Como $c \sim c_1 \sim c_2$, tenemos que $c_2 \wedge c^*$, $c \wedge c_1^*$ y $c \wedge c_2^*$ pertenecen a $\mathcal{I}$. Usando que el ideal es cerrado hacia abajo y por supremos de a dos, concluimos que $c \sim \hat{c}$. Por lo tanto, las cotas inferiores de $\{[a], [b]\}$ son $[\hat{c}]$ con $\hat{c}$ cota inferior de $\{a, b\}$. Veamos que esto implica que $[a] \wedge [b] = [a \wedge b]$. Tenemos que $[a \wedge b]$ es una cota inferior de $\{[a], [b]\}$ (es claro que si $d \leq e$, entonces $[d] \leq [e]$). Veamos que es la mayor cota inferior. Sea $[c]$ cualquier cota inferior. Por lo que vimos, existe $\hat{c}$ cota inferior de $\{a, b\}$ tal que $[\hat{c}] = [c]$. Que $\hat{c}$ sea cota inferior de $\{a, b\}$ implica que $\hat{c} < a \wedge b$, lo cual implica que $[\hat{c}] \leq [a \wedge b]$.

Que la disyunción baja al cociente se prueba de la misma forma, utilizando $\hat{c} = c_1 \vee c_2$.

Veamos que el complemento baja al cociente. Para esto notamos primero que hay mínimo, [0], y máximo, [1]. Vamos a usar que conjunciones y disyunciones bajan al cociente. Sea $a \in B$.

$$[a] \wedge [a^*] = [a \wedge a^*] = [0] \qquad [a] \vee [a^*] = [a \vee a^*] = [1]$$

Deducimos entonces que $[a]^* = [a^*]$. Veamos finalmente que $(B/\mathcal{I}, \leq)$ es una álgebra booleana (verificando los ítems de la definición 1.1.1).

1. El mínimo es [0] y el máximo [1].

2. Probamos que $[a] \wedge [b] = [a \wedge b]$ y que $[a] \vee [b] = [a \vee b]$. En particular probamos que esos ínfimos y supremos existen.

3. Dados $a, b, c \in B$, las propiedades distributivas se deducen de las de B y que bajan al cociente. Por ejemplo:

$$[a] \wedge ([b] \vee [c]]) = [a \wedge (b \vee c)] = [(a \wedge b) \vee (a \wedge c)] = ([a] \wedge [b]) \vee ([a] \wedge [c])$$

4. Probamos que para todo $a \in B$, el complemento de $[a]$ existe y es $[a^*]$. □

Cabe destacar que los supremos e ínfimos arbitrarios no tienen por qué bajar al cociente de la forma que lo hacen los finitos. Es decir, por ejemplo, que puede haber una familia $(a_i)_{i\in I}$ de elementos de B tal que $\bigvee_{i\in I}[a_i]$ exista pero sea distinto de $[\bigvee_{i\in I} a_i]$. Al final de la sección 1.2 veremos un ejemplo de esto. Por otra parte, probaremos que en ciertas condiciones los ínfimos y supremos numerables sí bajan al cociente.

Lema 1.1.9. *En el contexto del lema 1.1.8, si asumimos también que:*

1. *B tiene todos los ínfimos y supremos de subconjuntos numerables.*

2. *El ideal $\mathcal{I}$ es cerrado además por supremos numerables.*

entonces los supremos e ínfimos numerables en B bajan al cociente, en el sentido de que para toda familia numerable $(a_n)_{n\in\mathbb{N}}$ de elementos de B se cumplen:

$$\bigwedge_{n\in\mathbb{N}} [a_n] = \left[\bigwedge_{n\in\mathbb{N}} a_n\right] \qquad \bigvee_{n\in\mathbb{N}} [a_n] = \left[\bigvee_{n\in\mathbb{N}} a_n\right]$$

En particular, $B/\mathcal{I}$ tiene todos los supremos e ínfimos numerables.

Demostración. El razonamiento es análogo al realizado en la demostración del lema 1.1.8 para probar que las conjunciones y disyunciones bajan al cociente. Para los supremos, dada una familia de cardinal numerable $(a_n)_{n\in\mathbb{N}}$ de elementos de B, y $[c]$ cota superior de $\{[a_n] \,/\, n \in \mathbb{N}\}$, tomamos $(c_n)_{n\in\mathbb{N}}$ tal que para cada n se cumple $a_n \leq c_n$ y $c \sim c_n$ (aquí usamos que $[a] \leq [b]$ si y solo si existe $b' \sim b$ tal que $a \leq b'$). Luego definimos $\hat{c} = \bigvee_{n\in\mathbb{N}} c_n$.

Veamos que $c \sim \hat{c}$. Primero, $c \wedge \hat{c}^* = c \wedge \bigwedge_{n\in\mathbb{N}} c_n^*$, lo cual está en $\mathcal{I}$ ($c \wedge c_0^*$ ya está en $\mathcal{I}$ y los ideales son cerrados hacia abajo). Por otra parte, $c^* \wedge \hat{c} = \bigvee_{n\in\mathbb{N}}(c^* \wedge c_n)$, lo cual pertenece a $\mathcal{I}$ porque este es un ideal cerrado por supremos numerables. Finalmente, $[c] = [\hat{c}]$ siendo $\hat{c}$ una cota superior de $\{a_n \,/\, n \in \mathbb{N}\}$. Deducimos que las cotas superiores de $\{[a_n] \,/\, n \in \mathbb{N}\}$ son exactamente $\{[\hat{c}] \,/\, \bigvee_{n\in\mathbb{N}} a_n \leq \hat{c}\}$ y por lo tanto el supremo es $[\bigvee_{n\in\mathbb{N}} a_n]$ (esta conclusión es análoga a la que fue explicada al terminar de probar que las conjunciones bajan al cociente en el lema 1.1.8). Para los ínfimos numerables el razonamiento es análogo, utilizando $\hat{c} = \bigwedge_{n\in\mathbb{N}} c_n$. □

1.2. Álgebra booleana completa inducida por un espacio de probabilidad

Se considera un espacio de probabilidad $(\Omega, \mathcal{A}, \mu)$, formado por un conjunto Ω no vacío, una σ-álgebra $\mathcal{A}$ sobre Ω (es decir $\mathcal{A} \subseteq \mathcal{P}(\Omega)$ con $\varnothing \in \mathcal{A}$, cerrada por complementos,

uniones numerables y consecuentemente también por intersecciones numerables), y una medida de probabilidad μ en $\mathcal{A}$, es decir: un mapa $\mu : \mathcal{A} \to [0,1]$ tal que:

1. $\mu(\Omega) = 1$
2. Para toda familia numerable $(A_n)_{n\in\mathbb{N}} \in \mathcal{A}^{\mathbb{N}}$ tal que para cada $i \neq j \in \mathbb{N}$ se cumple $A_i \cap A_j = \varnothing$, tenemos $\mu(\bigcup_{i\in\mathbb{N}} A_i) = \sum_{i\in\mathbb{N}} \mu(A_i)$.

Observamos primero que la condición 2 con la familia constante vacía (notar que $\varnothing$ es el único conjunto disjunto con sigo mismo) implica que $\mu(\varnothing) = 0$. Por lo anterior, tenemos que la condición 2 se extiende a familias finitas (completando con el conjunto vacío). Esto a su vez implica que si $A, B \in \mathcal{A}$ son tales que $A \subseteq B$, entonces $\mu(A) \leq \mu(B)$.

Por otra parte, tenemos que $\mu(\bigcup_{i\in\mathbb{N}} A_i) \leq \sum_{i\in\mathbb{N}} \mu(A_i)$ para cualquier familia numerable $(A_n)_{n\in\mathbb{N}} \in \mathcal{A}^{\mathbb{N}}$, con elementos no necesariamente disjuntos dos a dos. Esto es porque podemos definir otra familia $E_n := A_n - \bigcup_{m<n} A_m$, la cual:

- Tiene elementos disjuntos dos a dos, lo cual por la condición 2 nos permite afirmar que $\mu(\bigcup_{n\in\mathbb{N}} E_n) = \sum_{n\in\mathbb{N}} \mu(E_n)$.
- Cumple $\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} E_n$.
- Cumple que para todo $n \in \mathbb{N}$, $\mu(E_n) \leq \mu(A_n)$.

En base a estas tres propiedades, concluimos $\mu(\bigcup_{n\in\mathbb{N}} A_n) \leq \sum_{n\in\mathbb{N}} \mu(A_n)$. También se cumple para familias finitas. Esto se deduce completando con el conjunto vacío y usando que $\mu(\varnothing) = 0$.

Al ser una σ-álgebra, el conjunto $\mathcal{A}$ equipado con el orden de inclusión es un álgebra booleana. En general esta álgebra booleana no es completa, pero para interpretar las cuantificaciones necesitaremos álgebras booleanas completas. Para solucionar esto cocientamos respecto al ideal de los conjuntos de medida nula, valiéndonos del lema 1.1.8.

El ideal de los conjuntos de medida nula es $[\mu = 0] = \{A \in \mathcal{A} \ / \ \mu(A) = 0\}$. Es un ideal porque:

- $\mu(\varnothing) = 0$.
- Para todos $A, B \in \mathcal{A}$ tales que $A \subseteq B$ se cumple que $\mu(A) \leq \mu(B)$.
- Dados $A, B \in \mathcal{A}$ tales que $\mu(A) = \mu(B) = 0$, tenemos $\mu(A \cup B) \leq \mu(A) + \mu(B) = 0$.

Usando que $\mu(\bigcup_{i\in\mathbb{N}} A_i) \leq \sum_{i\in\mathbb{N}} \mu(A_i)$ para cualquier familia numerable $(A_n)_{n\in\mathbb{N}} \in \mathcal{A}^{\mathbb{N}}$, tenemos que es un ideal cerrado por supremos numerables. Esto nos permitirá utilizar el lema 1.1.9, lo cual será relevante.

Definición 1.2.1. Dado un espacio de probabilidad $(\Omega, \mathcal{A}, \mu)$ el álgebra booleana completa inducida es $B = \mathcal{A}/[\mu = 0]$, siendo $[\mu = 0] = \{A \in \mathcal{A} \ / \ \mu(A) = 0\}$.

Al cocientar respecto al ideal de los conjuntos de medida nula tenemos las dos siguientes consecuencias que nos serán útiles:

1. Si $[A] = [B]$ entonces $\mu(A) = \mu(B)$. Tenemos que $A \cup (B - A) = B \cup (A - B)$ es una igualdad de uniones disjuntas, por lo que $\mu(A) + \mu(B - A) = \mu(B) + \mu(A - B)$. Por otra parte, $[A] = [B]$ nos dice que $A \triangle B \in [\mu = 0]$, o sea $\mu(A \triangle B) = 0$. Concluimos observando que $A \triangle B = (A - B) \cup (B - A)$ lo cual implica que en particular $\mu(B - A) = \mu(A - B) = 0$.

2. $\mu(A) = 0$ si y solo si $[A] = 0$. Esto es porque todos los conjuntos de medida nula son equivalentes al vacíon (bajo la relación de tener diferencia simétrica de medida nula).

Veamos que siempre es un álgebra booleana completa. Será un corolario de lo demostrado previamente en este capítulo y de que cumple la c.c.c.

Lema 1.2.2. *Para todo espacio de probabilidad $(\Omega, \mathcal{A}, \mu)$, tenemos que el álgebra booleana $B = \mathcal{A}/[\mu = 0]$ cumple la ccc.*

Demostración. Sea $\{[A_\alpha]\}_{\alpha<\rho} \subseteq B$ una anticadena. Tenemos que para todo $\alpha \neq \beta$ se cumple $[A_\alpha] \wedge [A_\beta] = 0$. Esto significa que $[A_\alpha \cap A_\beta] = 0$ y por lo tanto $\mu(A_\alpha \cap A_\beta) = 0$. A partir de esto deduciremos que para cualquier subconjunto numerable $\{A_{\alpha_n}\}_{n\in\omega}$ se cumple que $\mu(\bigcup_{n\in\omega} A_{\alpha_n}) = \sum_{n\in\omega} \mu(A_{\alpha_n})$.

Definimos $E_n := A_{\alpha_n} - \bigcup_{m<n} A_{\alpha_m} = A_{\alpha_n} - \bigcup_{m<n}(A_{\alpha_n} \cap A_{\alpha_m})$. Tenemos las siguientes tres propiedades de las cuales se deduce lo que queremos probar.

- Tiene elementos disjuntos dos a dos, por lo que $\mu(\bigcup_{n\in\mathbb{N}} E_n) = \sum_{n\in\mathbb{N}} \mu(E_n)$.
- Cumple $\bigcup_{n\in\mathbb{N}} A_{\alpha_n} = \bigcup_{n\in\mathbb{N}} E_n$.
- Para todo $n \in \mathbb{N}$, $\mu(E_n) = \mu(A_{\alpha_n})$. Esto es porque $E_n := A_{\alpha_n} - \bigcup_{m<n}(A_{\alpha_n} \cap A_{\alpha_m})$, de donde $E_n \cup \bigcup_{m<n}(A_{\alpha_n} \cap A_{\alpha_m}) = A_{\alpha_n}$, la cual es una unión disjunta y además $\mu(\bigcup_{m<n}(A_{\alpha_n} \cap A_{\alpha_m})) = 0$. De esto deducimos que $\mu(E_n) = \mu(A_{\alpha_n})$.

Supongo por absurdo que $\{[A_\alpha]\}_{\alpha<\rho}$ es no numerable. Tenemos que $\mu(A) = 0$ si y solo si $[A] = 0$, por lo que hay no numerables con medida positiva. Esto implica que para algún n hay infinitos A_α con medida mayor a $1/n$ (sino $\{A_\alpha\}_{\alpha<\rho}$ sería unión numerable de conjuntos finitos y por lo tanto numerable), lo cual es absurdo porque tendría un subconjunto numerable $\{A_{\alpha_i}\}_{i\in\mathbb{N}}$ tal que para todo i, $\mu(A_{\alpha_i}) \geq 1/n$. Con esto tendríamos $\mu(\bigcup_{i\in\omega} A_{\alpha_i}) = \sum_{i\in\omega} \mu(A_{\alpha_i}) = \infty$, pero $\mu(\Omega) = 1$. □

Corolario 1.2.3. *El álgebra booleana $B = \mathcal{A}/[\mu = 0]$ es completa, los ínfimos y supremos numerables en $\mathcal{A}$ bajan al cociente y todos los supremos e ínfimos de familias infinitas son iguales a los de subconjuntos numerables.*

Demostración. Como ya observamos, el ideal $[\mu = 0]$ es cerrado por supremos numerables. Esto nos permite aplicar el lema 1.1.9 para tener que los ínfimos y supremos numerables de $\mathcal{A}$ bajan al cociente y en particular que B tiene ínfimos y supremos numerables. Como probamos además que cumple la c.c.c, por el lema 1.1.6 tenemos que B es completa y que el supremo o ínfimo de cada familia es igual al de una subfamilia numerable. □

En general, dado $A \in \mathcal{A}$, para referirnos a su clase de equivalencia dentro de B, en lugar de utilizar la notación $[A]$ escribiremos $A/[\mu = 0]$. Observamos que si bien ínfimos y supremos numerables bajan al cociente, no se cumple en general. A modo de ejemplo, consideramos $\Omega = [0, 1]$ con la medida usual y la familia $(a_i)_{i\in\Omega}$ de elementos de $\mathcal{A}$ indizada por $I = \Omega$ definida por $a_i = \{i\}$. En este caso:

$$\left(\bigvee_{i\in\Omega} a_i\right)/[\mu = 0] = \left(\bigvee_{i\in\Omega} \{i\}\right)/[\mu = 0] = \Omega/[\mu = 0] = 1$$

Pero por otra parte:

$$\bigvee_{i\in\Omega} a_i/[\mu = 0] = \bigvee_{i\in\Omega} \{i\}/[\mu = 0] = \bigvee_{i\in\Omega} 0 = 0$$

Aquí usamos que como $\mu(\{i\}) = 0$, entonces $\{i\}/[\mu = 0] = \varnothing/[\mu = 0] = 0$.

Capítulo 2

Conjuntos con equivalencias booleanas

En este capítulo se presentan los B-conjuntos, una categoría de conjuntos con estructura booleana que permite construir modelos de teorías de orden superior. Es una generalización del modelo de reales aleatorios introducido por Scott en [4].

2.1. Un modelo de la negación de la hipótesis del continuo

El trabajo presentado en esta monografía está basado en un artículo de D. Scott de 1967 [4], en que introduce una prueba elemental de la consistencia relativa de la negación de la hipótesis del continuo. Por lo tanto, comenzamos presentando a grandes rasgos los contenidos de ese artículo de Scott.

Recordamos antes que la independencia de la hipótesis del continuo consiste en dos resultados: la consistencia relativa de la hipótesis del continuo y la consistencia relativa de su negación. Cuando hablamos de consistencia relativa aquí, hablamos de consistencia relativa a una teoría de base (usualmente la teoría de conjuntos de ZF, pero puede ser otra que sea suficientemente expresiva), lo cual significa que se puede agregar la fórmula como otro axioma sin riesgo de generar inconsistencias. La consistencia relativa de la hipótesis del continuo respecto a ZF fue demostrada por primera vez por Gödel en 1938 [1] y la de su negación por Cohen en 1963 [2].

2.1.1. El formalismo de Scott

Se trata de una teoría que distingue tres tipos de objetos, cada uno con sus propias variables:

1. Números reales, $\mathbb{R}$, con variables como x, y, z.
2. Funciones de tipo $\mathbb{R} \to \mathbb{R}$, con variables como f, g, h.
3. Funcionales de tipo $(\mathbb{R} \to \mathbb{R}) \to \mathbb{R}$, con variables como F, G, H.

Al decir que las funcionales son de tipo $(\mathbb{R} \to \mathbb{R}) \to \mathbb{R}$, nos referimos a que tienen a las funciones de tipo $\mathbb{R} \to \mathbb{R}$ como dominio y a los reales como codominio. Para cada tipo de variables tenemos cuantificaciones universales y existenciales. Para todas las

cuantificaciones universales usamos el símbolo $\forall$ y para todas las existenciales usamos $\exists$. El dominio de cuantificación queda determinado por la variable. Por ejemplo, $\forall x$ es una cuantificación universal sobre reales, $\exists f$ es una cuantificación existencial sobre funciones y $\forall F$ es una cuantificación universal sobre funcionales. En total, el lenguaje se compone de los siguientes elementos:

1. Las siguientes conectivas lógicas: $\neg$, $\wedge$, $\vee$, $\Rightarrow$ y $\Leftrightarrow$.
2. Variables x, y, z de reales, con sus cuantificadores $\forall x$ y $\exists x$.
3. Variables f, g, h de funciones, con sus cuantificadores $\forall f$ y $\exists f$.
4. Variables F, G, H de funcionales, con sus cuantificadores $\forall F$ y $\exists F$.
5. Símbolos del lenguaje de cuerpo ordenado para los reales: 0, 1, $+$, $\times$ y $\leq$.
6. Símbolo de igualdad $=$, el cual se usa para reales, funciones y funcionales. Es decir, podemos por ejemplo escribir $x = y$, $1 + y = z \times x$, $f = g$ y $F = G$.
7. Aplicación de funciones a reales y de funcionales a funciones. Por ejemplo, podemos escribir $f(x)$, $f(0)$ y $F(f)$.

A modo de ejemplo, las siguientes son fórmulas del lenguaje.

$$\forall f \forall x \forall y \ (x = y \Rightarrow f(x) = f(y)) \qquad \forall F \forall f \forall g \ (f = g \Rightarrow F(f) = F(g))$$

Dentro de este lenguaje podemos expresar dos axiomas de elección (esquemas de axiomas de elección, precisamente), uno para funciones y otro para funcionales. Son los siguientes:

$$\forall x \exists y A(x, y) \Rightarrow \exists f \forall x A(x, f(x)) \qquad \forall f \exists y B(f, y) \Rightarrow \exists F \forall f B(f, F(f))$$

donde $A(x, y)$ es una fórmula que depende posiblemente de las variables x, y y $B(f, y)$ es otra fórmula que depende posiblemente de las variables f e y (en ambos casos pueden haber otras variables, las cuales implícitamente se cuantifican universalmente y juegan el rol de parámetros).

En este formalismo podemos representar conjuntos de reales utilizando funciones características (y conjuntos de conjuntos de reales usando funcionales características). Se usa la convención de que el conjunto definido por f es el de los x tales que $f(x) = 0$. De esta forma, si f representa un conjunto, la cuantificación universal en ese conjunto es $\forall x(f(x) = 0 \Rightarrow \dots)$ y la existencial es $\exists x(f(x) = 0 \wedge \dots)$. De esta forma, podemos hablar de cotas superiores, supremos y axioma de completitud:

$$\begin{aligned} \text{cota\_sup}(f, a) &:\equiv \forall x(f(x) = 0 \Rightarrow x \leq a) \\ \text{supremo}(f, b) &:\equiv \forall x(\text{cota\_sup}(f, x) \Leftrightarrow b \leq x) \\ AC &:\equiv \forall f, \ \exists x \ f(x) = 0 \ \wedge \ \exists a \ \text{cota\_sup}(f, a) \ \Rightarrow \ \exists b \ \text{supremo}(f, b) \end{aligned}$$

Por último, podemos hablar de números naturales y dar un enunciado de la hipótesis del continuo. Los números naturales se definen con la siguiente fórmula.

$$N(y) :\equiv \forall f, \ f(0) = 0 \wedge \forall x(f(x) = 0 \Rightarrow f(x + 1) = 0) \ \Rightarrow \ f(y) = 0$$

El enunciado de la hipótesis del continuo en este formalismo es el siguiente.

$$HC :\equiv \forall h,\ \exists f \forall y (h(y) = 0 \Rightarrow \exists x (N(x) \wedge f(x) = y)) \ \vee \ \exists g \forall y \exists x (h(x) = 0 \wedge y = g(x))$$

En este enunciado, h representa cualquier subconjunto de $\mathbb{R}$ y la disyunción afirma que existe una sobreyección de $\mathbb{N}$ a ese subconjunto (la cual sería f) o existe una sobreyección de ese subconjunto a todo $\mathbb{R}$ (la cual sería g).

2.1.2. El modelo de los reales aleatorios

Luego de haber introducido la sintaxis, Scott presenta un modelo booleano de su formalismo, basado en el álgebra booleana completa inducida por un espacio de probabilidad $(\Omega, \mathcal{A}, \mu)$, es decir $B = \mathcal{A}/[\mu = 0]$ (como fue presentada en la sección 1.2). En este modelo, las proposiciones son interpretadas por los elementos del álgebra booleana B, mientras que las conectivas son interpretadas por las correspondientes operaciones en B. Más precisamente, a cada fórmula cerrada ϕ se asocia su valor de verdad $[\![\phi]\!] \in B$ de forma recursiva, utilizando las operaciones de B para las conectivas de la siguiente forma:

$$[\![\phi \wedge \psi]\!] = [\![\phi]\!] \wedge [\![\psi]\!] \qquad [\![\phi \to \psi]\!] = [\![\phi]\!] \Rightarrow [\![\psi]\!] \qquad [\![\neg\phi]\!] = [\![\phi]\!]^*$$
$$[\![\phi \vee \psi]\!] = [\![\phi]\!] \vee [\![\psi]\!] \qquad [\![\phi \leftrightarrow \psi]\!] = [\![\phi]\!] \Leftrightarrow [\![\psi]\!]$$

Hasta ahora viene siendo la forma usual de interpretar fórmulas con álgebras booleanas. Lo que diferencia a este modelo (o esta clase de modelos, ya que depende de un espacio de probabilidad) es la forma como se interpretan los reales, las funciones y las funcionales.

Los números reales son interpretados por reales aleatorios, definidos como funciones medibles de Ω en $\mathbb{R}$.

$$\mathcal{R} = \{\xi : \Omega \to \mathbb{R} \ / \ \xi \text{ es medible}\}$$

Precisamente, ξ debe cumplir que $\xi^{-1}((-\infty, a)) \in \mathcal{A}$ para todo $a \in \mathbb{R}$. Utilizando terminología de probabilidad, los reales aleatorios son exactamente las variables aleatorias reales. Las constantes 0 y 1 se interpretan con las variables aleatorias constantes correspondientes y las operaciones se interpretan punto a punto, en el sentido de que dados $\xi, \eta \in \mathcal{R}$, tenemos $\xi + \eta, \xi\eta \in \mathcal{R}$ definidos por:

$$(\xi + \eta)(\omega) = \xi(\omega) + \eta(\omega) \qquad (\xi\eta)(\omega) = \xi(\omega)\eta(\omega)$$

Por otra parte, la igualdad se interpreta de modo que dados $\xi, \eta \in \mathcal{R}$, tenemos $[\![\xi = \eta]\!] \in B$ definido por:

$$[\![\xi = \eta]\!] = \{\omega \in \Omega \ / \ \xi(\omega) = \eta(\omega)\}/[\mu = 0]$$

y análogamente, el orden se interpreta con:

$$[\![\xi \leq \eta]\!] = \{\omega \in \Omega \ / \ \xi(\omega) \leq \eta(\omega)\}/[\mu = 0]$$

Como ξ y η son medibles, $\{\omega \in \Omega \ / \ \xi(\omega) = \eta(\omega)\}, \{\omega \in \Omega \ / \ \xi(\omega) \leq \eta(\omega)\} \in \mathcal{A}$.

Veamos ahora cómo se interpretan las funciones de tipo $\mathbb{R} \to \mathbb{R}$. Una primera idea ingenua sería considerar cualquier función $f : \mathcal{R} \to \mathcal{R}$. Sin embargo, en seguida observamos que pueden haber $\xi, \eta \in \mathcal{R}$ tales que $[\![\xi = \eta]\!] = 1$ pero $\xi \neq \eta$ y por lo tanto

podría pasar que $[\![f(\xi) = f(\eta)]\!] = 0$. Esto es inaceptable porque (intuitivamente por ahora, hasta que definamos cómo se interpretan los cuantificadores) contradice la tautología $\forall x, y,\ x = y \Rightarrow f(x) = f(y)$, ya que en este caso $[\![\xi = \eta]\!] \to [\![f(\xi) = f(\eta)]\!] = 0$. Exigiremos a las funciones que verifiquen esa tautología y de hecho esa será la única condición que impondremos. Precisamente, definimos el conjunto $\mathcal{R}^{\mathcal{R}}$ de las funciones aleatorias como:

$$\mathcal{R}^{\mathcal{R}} = \{f : \mathcal{R} \to \mathcal{R} \ / \ \forall \xi, \eta \in \mathcal{R},\ [\![\xi = \eta]\!] \leq [\![f(\xi) = f(\eta)]\!]\}$$

Notar que la condición es más fuerte que simplemente exigir que si $[\![\xi = \eta]\!] = 1$ también se cumpla $[\![f(\xi) = f(\eta)]\!] = 1$. La igualdad entre funciones aleatorias se interpreta de la siguiente forma.

$$[\![f = g]\!] = \bigwedge_{\xi \in \mathcal{R}} [\![f(\xi) = g(\xi)]\!]$$

Las funcionales de tipo $(\mathbb{R} \to \mathbb{R}) \to \mathbb{R}$ se interpretan análogamente con funcionales aleatorias.

$$\mathcal{R}^{\mathcal{R}^{\mathcal{R}}} = \{F : \mathcal{R}^{\mathcal{R}} \to \mathcal{R} \ / \ \forall f, g \in \mathcal{R}^{\mathcal{R}},\ [\![f = g]\!] \leq [\![F(f) = F(g)]\!]\}$$
$$[\![F = G]\!] = \bigwedge_{f \in \mathcal{R}^{\mathcal{R}}} [\![F(f) = G(f)]\!]$$

Notar que en la definición $[\![f = g]\!]$ es igualdad entre funciones aleatorias y $[\![F(f) = F(g)]\!]$ es entre reales aleatorios.

Para interpretar las cuantificaciones se utilizan ínfimos y supremos arbitrarios.

$$[\![\forall x A(x)]\!] = \bigwedge_{\xi \in \mathcal{R}} [\![A(\xi)]\!] \qquad [\![\exists x A(x)]\!] = \bigvee_{\xi \in \mathcal{R}} [\![A(\xi)]\!]$$
$$[\![\forall f B(f)]\!] = \bigwedge_{f \in \mathcal{R}^{\mathcal{R}}} [\![B(f)]\!] \qquad [\![\exists f B(f)]\!] = \bigvee_{f \in \mathcal{R}^{\mathcal{R}}} [\![B(f)]\!]$$
$$[\![\forall F\ C(F)]\!] = \bigwedge_{F \in \mathcal{R}^{\mathcal{R}^{\mathcal{R}}}} [\![C(F)]\!] \qquad [\![\exists F\ C(F)]\!] = \bigvee_{F \in \mathcal{R}^{\mathcal{R}^{\mathcal{R}}}} [\![C(F)]\!]$$

Por último, ya que las funciones aleatorias son en particular funciones de $\mathcal{R}$ en $\mathcal{R}$ y las funcionales aleatorios funciones de $\mathcal{R}^{\mathcal{R}}$ en $\mathcal{R}$, podemos interpretar las aplicaciones de la sintaxis como aplicaciones en el modelo.

Con esto terminamos de definir cómo se interpreta cualquier fórmula ϕ de la sintaxis (presentada en la sección 2.1.1) con un valor de verdad $[\![\phi]\!] \in B$. A modo de ejemplo, la fórmula $\forall f \forall x \forall y (x = y \Rightarrow f(x) = f(y))$ se interpreta como:

$$[\![\forall f \forall x \forall y (x = y \Rightarrow f(x) = f(y))]\!] = \bigwedge_{f \in \mathcal{R}^{\mathcal{R}}} \bigwedge_{\xi \in \mathcal{R}} \bigwedge_{\eta \in \mathcal{R}} ([\![\xi = \eta]\!] \to [\![f(\xi) = f(\eta)]\!])$$

lo cual vale 1 por la definición de $\mathcal{R}^{\mathcal{R}}$.

Decimos que una fórmula ϕ se cumple o es válida en un modelo de reales aleatorios si $[\![\phi]\!] = 1$ en ese modelo (depende del modelo porque hay fórmulas que según el espacio de probabilidad de base $(\Omega, \mathcal{A}, \mu)$, pueden cumplirse o no).

Luego de definir todo lo anterior, Scott demuestra que estos modelos (para cualquier espacio de probabilidad) cumplen los axiomas de elección presentados en la sección 2.1.1

y los axiomas de los números reales, es decir los de cuerpo ordenado y el de completitud. Finalmente, prueba que con un espacio de probabilidad bastante grande (de tipo $[0,1]^I$ con I de cardinal mayor al de $\mathbb{R}$) la hipótesis del continuo (con el enunciado presentado en la sección 2.1.1) no se cumple. De hecho, prueba que $[\![HC]\!] = 0$.

Durante el resto de este trabajo, vamos a extender esta construcción a una teoría de orden superior (lo cual significa en particular que además de funciones y funcionales, se podrá hablar de funcionales de cualquier orden, es decir $((\mathbb{R} \to \mathbb{R}) \to \mathbb{R}) \to \mathbb{R}$, $(((\mathbb{R} \to \mathbb{R}) \to \mathbb{R}) \to \mathbb{R}) \to \mathbb{R}$, etc) y adaptar la prueba de Scott, con el fin que la negación de la hipótesis del continuo se deduzca de conceptos intuitivos de probabilidad, aprovechando el carácter aleatorio de estos modelos.

2.2. Los B-conjuntos

Vamos a algebrizar los elementos subyacentes de la construcción de Scott presentada en la sección 2.1. Para esto, dada un álgebra booleana completa B cualquiera, introducimos la categoría de los B-conjuntos. Si bien al final utilizaremos solamente álgebras booleanas provenientes de espacios de probabilidad, esta generalización permite que B sea cualquier álgebra booleana completa. Por lo tanto, en el resto de la sección B será un álgebra booleana completa cualquiera.

2.2.1. La noción de B-conjunto

Lo primero es definir qué elementos de los objetos usados por Scott abstraer para la generalización. La respuesta es que solamente la existencia de algo para interpretar la igualdad; algo que sea una relación de equivalencia en un sentido booleano. Con eso en mente, definimos los B-conjuntos.

Definición 2.2.1. Sea X un conjunto. Decimos que $\sim$ es una *B-equivalencia* sobre X si es una función $\_ \sim \_ : X \to X \to B$ tal que:

1. $x \sim x = 1$ para todo $x \in X$.
2. $x \sim y = y \sim x$ para todos $x, y \in X$.
3. $x \sim y \wedge y \sim z \leq x \sim z$ para todos $x, y, z \in X$.

En este caso decimos que $(X, \sim)$ es un *B-conjunto*.

Notar que las tres condiciones que se exigen a la B-equivalencia están basadas en las propiedades de reflexividad, simetría y transitividad, expresadas de modo funcional con el álgebra booleana B. Intuitivamente, dados $x, y \in X$ se puede pensar que $x \sim y$ es el valor de verdad de la igualdad entre estos elementos, en el sentido de que si vale 1 son esencialmente el mismo, si vale 0 son distintos y en otro caso son parcialmente iguales.

Notación. Cuando no introduzca ambigüedad, diremos que X es un B-conjunto sin hacer referencia a la B-equivalencia. Al trabajar con distintos B-conjuntos $((X, \sim_X)$, $(Y, \sim_Y)$, etc) en algunos casos usaremos el mismo símbolo $\sim$ para todas las B-equivalencias, dado que usualmente se puede deducir de cual se trata en base a los argumentos.

Como es usual al introducir objetos matemáticos que consisten en conjuntos con estructura adicional, nos interesan las funciones que en cierto sentido respetan esa estructura. Como la estructura adicional hace que distintos elementos puedan ser parcialmente iguales, lo que exigimos a una función es, intuitivamente, que si la aplicamos a elementos parcialmente iguales, los resultados sigan siendo parcialmente iguales. Se lo puede considerar como la propiedad de que el resultado de aplicar una función está completamente determinado por su argumento, en el sentido de que $x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$.

Definición 2.2.2 (Función compatible)**.** Dados dos B-conjuntos $(X, \sim_X)$ y $(Y, \sim_Y)$, decimos que una función $f : X \to Y$ es *compatible* si para todos $x_1, x_2 \in X$:

$$x_1 \sim_X x_2 \leq f(x_1) \sim_Y f(x_2)$$

Denotamos $\mathcal{F}^B(X, Y)$ al conjunto de las funciones compatibles de X a Y.

Notar que $x_1 \sim_X x_2 \leq f(x_1) \sim_Y f(x_2)$ si y solo si $x_1 \sim_X x_2 \to f(x_1) \sim_Y f(x_2) = 1$, lo cual intuitivamente significa que la fórmula $x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$ se cumple en el álgebra B. Observamos que todas las funciones constantes son compatibles, pues por la reflexividad el lado derecho de la desigualdad siempre es 1.

Proposición 2.2.3 (La categoría B-Set)**.** *Los B-conjuntos junto con las funciones compatibles conforman una categoría, denominada B-Set. Específicamente, en esta categoría:*

- *Los objetos son los B-conjuntos.*
- *Las flechas son las funciones compatibles entre B-conjuntos.*
- *Las flechas identidad son las funciones identidad.*
- *La composición de flechas es la composición de funciones.*

Demostración. Se deduce directamente de la definición que la función identidad es compatible. Solo hay que ver que composición de funciones compatibles es compatible. Sean X, Y, Z tres B-conjuntos y sean $f \in \mathcal{F}^B(X, Y)$ y $g \in \mathcal{F}^B(Y, Z)$. Buscamos probar que $g \circ f \in \mathcal{F}^B(X, Z)$. Sean $x_1, x_2 \in X$. Como f es compatible, $x_1 \sim x_2 \leq f(x_1) \sim f(x_2)$, además como g es compatible, tenemos que $f(x_1) \sim f(x_2) \leq g(f(x_1)) \sim g(f(x_2))$. Concluimos por la transitividad del orden. □

Ejemplos. 1. Para cualquier conjunto X, tenemos que $(X, \sim_D)$ es un B-conjunto, con $\sim_D$ definida como

$$x \sim_D y = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{si } x \neq y \end{cases}$$

A $\sim_D$ le llamamos B-equivalencia discreta. Se puede considerar que estos son B-conjuntos triviales, ya que intuitivamente la B-equivalencia no aporta estructura, al no vincular ningún par de elementos distintos.

2. El álgebra booleana con la equivalencia booleana, $(B, \leftrightarrow)$, conforma un B-conjunto. Basta observar que para todos $x, y, z \in B$ se cumplen:

$$x \leftrightarrow x = 1, \qquad x \leftrightarrow y = y \leftrightarrow x, \qquad (x \leftrightarrow y) \wedge (y \leftrightarrow z) \leq x \leftrightarrow z$$

3. Los reales aleatorios (presentados en la sección 2.1) son un ejemplo de B-conjunto (de hecho, a partir del cual se generalizó el concepto), para el caso particular en que $B = \mathcal{A}/[\mu = 0]$ con $(\Omega, \mathcal{A}, \mu)$ espacio de probabilidad. El conjunto X y la B-equivalencia $\sim$ son los siguientes:

$$X = \mathcal{R} = \{\xi : \Omega \to \mathbb{R} \ / \ \xi \text{ medible}\} \quad \xi \sim \eta = \{\omega \in \Omega \ / \ \xi(\omega) = \eta(\omega)\}/[\mu = 0]$$

Las funciones compatibles coinciden con las funciones aleatorias en el sentido de Scott (presentadas en la sección 2.1).

Dados dos B-conjuntos se puede definir un B-conjunto producto de forma natural, el cual resulta ser un producto binario en el sentido categórico.

Proposición 2.2.4 (Producto de B-conjuntos)**.** *Dados un par de B-conjuntos $(X, \sim_X)$ y $(Y, \sim_Y)$, podemos equipar al producto cartesiano con la B-equivalencia $\sim_{X\times Y}$ definida como:*

$$(x_1, y_1) \sim_{X\times Y} (x_2, y_2) = x_1 \sim_X x_2 \ \wedge \ y_1 \sim_Y y_2$$

de modo que $(X \times Y, \sim_{X\times Y})$ es otro B-conjunto. Además, es el objeto producto en sentido categórico.

Demostración. Que la definición del producto da lugar a un B-conjunto se deduce directamente de que X y Y son B-conjuntos. Por ejemplo, la transitividad se verifica de la siguiente forma:

$$\begin{aligned}(x_1, y_1) \sim (x_2, y_2) \ \wedge \ (x_2, y_2) \sim (x_3, y_3) &= (x_1 \sim x_2 \ \wedge \ y_1 \sim y_2) \wedge (x_2 \sim x_3 \ \wedge \ y_2 \sim y_3) \\ &= x_1 \sim x_2 \wedge x_2 \sim x_3 \wedge y_1 \sim y_2 \wedge y_2 \sim y_3 \\ &\leq x_1 \sim x_3 \wedge y_1 \sim y_3 \\ &= (x_1, y_1) \sim (x_3, y_3)\end{aligned}$$

Veamos que se trata del objeto producto. Las proyecciones son las usuales. Debemos ver que son compatibles. Veámoslo con $\pi_1 : X \times Y \to X$. Sean $(x_1, y_1), (x_2, y_2) \in X \times Y$. Debemos ver que $(x_1, y_1) \sim (x_2, y_2) \leq \pi_1(x_1, y_1) \sim \pi_1(x_2, y_2)$. Aplicando las definiciones vemos que se cumple.

Sea Z un objeto y sean f, g flechas de Z a X y de Z a Y, respectivamente. Debemos ver que existe una única flecha (f, g) de Z a $X \times Y$ que hace conmutar los diagramas, o sea que $f = \pi_1 \circ (f, g)$ y $g = \pi_2 \circ (f, g)$. De estas dos ecuaciones concluimos que para todo $z \in Z$, se cumple $(f, g)(z) = (f(z), g(z))$, por lo que tenemos la unicidad y solo resta probar que esa función es compatible. Sean $z_1, z_2 \in Z$.

$$(f(z_1), g(z_1)) \sim (f(z_2), g(z_2)) = f(z_1) \sim f(z_2) \wedge g(z_1) \sim g(z_2) \geq z_1 \sim z_2 \wedge z_1 \sim z_2$$

La última desigualdad se debe a que f y g son funciones compatibles. Por lo tanto, $(f(z_1), g(z_1)) \sim (f(z_2), g(z_2)) \geq z_1 \sim z_2$ y finalmente (f, g) es una flecha. □

Además de los productos finitos, se pueden definir productos arbitrarios. Dada una familia $(X_i, \sim_i)_{i\in I}$ de B-conjuntos, el producto $\Pi_{i\in I} X_i$ resulta otro B-conjunto con la B-equivalencia $f \sim_{\Pi_{i\in I} X_i} g = \bigwedge_{i\in I}(f(i) \sim_i g(i))$, el cual es el objeto producto en sentido categórico. La prueba es análoga a la del caso binario.

Al final de la prueba anterior, como un último paso para probar una desigualdad usamos que $f(z_1) \sim f(z_2) \geq z_1 \sim z_2$, lo cual se cumple porque la función f es compatible. Será muy común que usemos la compatibilidad de esa forma en demostraciones, por lo que usualmente lo haremos sin explicitarlo.

Por otra parte, dados dos B-conjuntos X y Y, se puede equipar al conjunto de la funciones compatibles $\mathcal{F}^B(X,Y)$ con una B-equivalencia de forma natural, resultando en el objeto exponencial en sentido categórico.

Proposición 2.2.5 (Exponencial de B-conjuntos)**.** *Dados dos B-conjuntos $(X, \sim_X)$ y $(Y, \sim_Y)$, podemos equipar al conjunto de funciones compatibles $\mathcal{F}^B(X,Y)$ con la B-equivalencia $\sim_{\mathcal{F}^B(X,Y)}$ definida como:*

$$f \sim_{\mathcal{F}^B(X,Y)} g = \bigwedge_{x \in X} f(x) \sim_Y g(x)$$

de modo que $(\mathcal{F}^B(X,Y), \sim_{\mathcal{F}^B(X,Y)})$ es otro B-conjunto. Además, es el objeto exponencial en sentido categórico.

Demostración. Que el exponencial es un B-conjunto se deduce de que Y lo es. Por ejemplo, la transitividad se verifica de la siguiente forma:

$$\begin{aligned} f \sim g \wedge g \sim h &= \bigwedge_{x \in X} f(x) \sim_Y g(x) \wedge \bigwedge_{x' \in X} g(x') \sim_Y h(x') \\ &= \bigwedge_{x \in X} \left(f(x) \sim_Y g(x) \wedge \bigwedge_{x' \in X} g(x') \sim_Y h(x') \right) \\ &\leq \bigwedge_{x \in X} (f(x) \sim_Y g(x) \wedge g(x) \sim_Y h(x)) \leq \bigwedge_{x \in X} f(x) \sim_Y h(x) = f \sim_{\mathcal{F}^B(X,Y)} h \end{aligned}$$

Notar que usamos la propiedad de transitividad de $\sim_Y$. Será muy común que usemos esa propiedad en cuentas, por lo que usualmente no lo explicitaremos. Probaremos que $\mathcal{F}^B(X,Y)$ es objeto exponencial con $\mathrm{ev} : \mathcal{F}^B(X,Y) \times X \to Y$ definida por $\mathrm{ev}(f,x) = f(x)$. Veamos que ev es una flecha. Sean $(f_1, x_1), (f_2, x_2) \in \mathcal{F}^B(X,Y) \times X$. Nuestro objetivo es probar que $(f_1, x_1) \sim (f_2, x_2) \leq \mathrm{ev}(f_1, x_1) \sim \mathrm{ev}(f_2, x_2)$.

$$\begin{aligned} (f_1, x_1) \sim (f_2, x_2) = f_1 \sim f_2 \wedge x_1 \sim x_2 &= \bigwedge_{x \in X} f_1(x) \sim f_2(x) \wedge x_1 \sim x_2 \\ &\leq \bigwedge_{x \in X} f_1(x) \sim f_2(x) \wedge f_2(x_1) \sim f_2(x_2) \\ &\leq f_1(x_1) \sim f_2(x_1) \wedge f_2(x_1) \sim f_2(x_2) \leq f_1(x_1) \sim f_2(x_2) \end{aligned}$$

En la primera desigualdad usamos que f_2 es compatible.

Veamos que es el objeto exponencial. Sean Z un objeto y $f : Z \times X \to Y$ una flecha. Debemos probar que existe una única flecha $\lambda f : Z \to \mathcal{F}^B(X,Y)$ de modo que $f = \mathrm{ev} \circ (\lambda f, \mathrm{id}_X)$. Que se cumpla la igualdad implica que para todos $(z,x) \in Z \times X$ tenemos $f(z,x) = \lambda f(z)(x)$, lo cual deja un único candidato para λf y por lo tanto prueba la unicidad. Solo resta probar que $\lambda f \in \mathcal{F}^B(Z, \mathcal{F}^B(X,Y))$.

Primero debemos probar que para todo $z \in Z$, $\lambda f(z) \in \mathcal{F}^B(X,Y)$. Para eso fijamos $z \in Z$ y dados $x_1, x_2 \in X$ intentamos probar que $x_1 \sim x_2 \leq \lambda f(z)(x_1) \sim \lambda f(z)(x_2)$.

$$\lambda f(z)(x_1) \sim \lambda f(z)(x_2) = f(z,x_1) \sim f(z,x_2) \geq (z,x_1) \sim (z,x_2) = x_1 \sim x_2$$

Demostremos ahora que dados $z_1, z_2 \in Z$, $z_1 \sim z_2 \leq \lambda f(z_1) \sim \lambda f(z_2)$.

$$\lambda f(z_1) \sim \lambda f(z_2) = \bigwedge_{x \in X} \lambda f(z_1)(x) \sim \lambda f(z_2)(x) = \bigwedge_{x \in X} f(z_1,x) \sim f(z_2,x)$$

Para todo $x \in X$, $f(z_1,x) \sim f(z_2,x) \geq (z_1,x) \sim (z_2,x) = z_1 \sim z_2$, por lo tanto el ínfimo también es mayor o igual a $z_1 \sim z_2$ y terminamos. □

Notar que $f \sim_{\mathcal{F}^B(X,Y)} g = 1$ si y solo si $\forall x \in X,\ f(x) \sim_Y g(x) = 1$. Intuitivamente se corresponde con la igualdad extensional (la extensionalidad funcional se presenta formalmente en la sección 3.3.3).

Volviendo al modelo de reales aleatorios, notar que $(\mathcal{F}^B(\mathcal{R},\mathcal{R}), \sim_{\mathcal{F}^B(\mathcal{R},\mathcal{R})})$ es exactamente el conjunto de las funciones aleatorias con la igualdad que se definió para ellas. Por lo tanto, las funciones aleatorias también conforman un B-conjunto. Del mismo modo, $(\mathcal{F}^B(\mathcal{F}^B(\mathcal{R},\mathcal{R}),\mathcal{R}), \sim_{\mathcal{F}^B(\mathcal{F}^B(\mathcal{R},\mathcal{R}),\mathcal{R})})$ es el conjunto de las funcionales aleatorias con la igualdad definida, el cual resulta ser otro B-conjunto. Notar que podríamos de esta forma seguir definiendo funcionales de mayor orden y todos resultarían ser B-conjuntos.

Veamos ahora que hay objetos terminales.

Proposición 2.2.6. *En B-Set hay objetos terminales.*

Demostración. Consideramos $X = \{*\}$ un conjunto unitario cualquiera, con la única B-equivalencia que puede tener. Entonces es un objeto terminal, pues para cada B-conjunto Y, existe una única función compatible de Y a X, que es la función constante f tal que para todo y, $f(y) = *$. Al ser una función constante es compatible. □

Sabiendo que hay objetos terminales, productos y exponenciales, podemos afirmar que B-Set es una categoría cartesiana cerrada. Finalizamos esta subsección demostrando que hay pullbacks, por lo que tendremos que es una categoría cartesiana cerrada y completa.

Proposición 2.2.7. *En B-Set hay todos los pullbacks.*

Demostración. Sean X, Y, Z objetos y f, g flechas de X a Z y de Y a Z, respectivamente. Queremos un objeto W con flechas a X y Y que hagan conmutar el diagrama resultante. Vamos a usar $W = \{(x,y) \in X \times Y \ /\ f(x) = g(y)\}$ y las proyecciones $\pi_1 : W \to X$ y $\pi_2 : W \to X$. La estructura de B-conjunto de W es la que hereda de $X \times Y$ (cualquier subconjunto de un B-conjunto hereda estructura de B-conjunto).

Veamos que cumple la propiedad del pullback. Sea S un objeto con flechas h_1, h_2 a X e Y respectivamente tales que el diagrama incluyendo a C conmuta. La flecha $m : A \to W$ que factoriza solo puede ser $m = (h_1, h_2)$, la misma construcción que utilizamos en la prueba de que hay productos binarios. Como el diagrama formado por h_1, f, h_2 y g conmuta, tenemos que el codominio de m es efectivamente W. □

Como consecuencia de la existencia de los productos, los objetos terminales, las exponenciales y los pullbacks, tenemos que B-Set es una categoría cartesiana cerrada y completa. Afirmamos que es completa (en lugar de solamente finitamente completa) porque la construcción de productos binarios se extiende a productos arbitrarios, de la forma que se mencionó tras la prueba de la proposición 2.2.4.

Teorema 2.2.8. *B-Set es una categoría cartesiana cerrada y completa.*

2.2.2. Los B-conjuntos reducidos

En un B-conjunto $(X, \sim)$ pueden haber $x_1 \neq x_2$ tales que $x_1 \sim x_2 = 1$. Esto en la mayoría del trabajo no será relevante, pero sí en la proposición 2.2.21, por lo que introducimos el concepto de los B-conjuntos reducidos.

Definición 2.2.9. Un B-conjunto $(X, \sim)$ es *reducido* si $x_1 \sim x_2 = 1$ implica $x_1 = x_2$ para todos $x_1, x_2 \in X$.

Primero que nada, con un cociente sencillo se puede reducir cualquier B-conjunto, llegando a uno prácticamente equivalente.

Proposición 2.2.10. *Sea $(X, \sim)$ un B-conjunto. Sea $\equiv$ la relación sobre X definida por:*

$$x \equiv y \;\Leftrightarrow\; x \sim y = 1$$

Entonces $\equiv$ es una relación de equivalencia y podemos definir $\sim^*$ sobre $X/\equiv$ como $[x] \sim^* [y] = x \sim y$, con lo que $(X/\equiv, \sim^*)$ es un B-conjunto reducido.

Demostración. Sean $x, y \in X$ tales que $x \equiv y$. Sea $z \in X$ cualquiera. Veamos que $x \sim z = y \sim z$. Usamos las propiedades de simetría y transitividad de los B-conjuntos:

$$x \sim z = z \sim x \wedge x \sim y \leq y \sim z$$

De forma simétrica tenemos que $y \sim z \leq x \sim z$, por lo que son iguales. De esto se deduce directamente que $\equiv$ es una relación de equivalencia y que $\sim^*$ está bien definido. Veamos que $(X^*, \sim^*)$ es reducido. Sean $[x], [y] \in X/\equiv$ tales que $[x] \sim^* [y] = 1$. Por definición de $\sim^*$, tenemos que $x \sim y = 1$ y por lo tanto $[x] = [y]$. □

Por último, veamos que los B-conjuntos reducidos son estables por las construcciones presentadas previamente.

Proposición 2.2.11.

1. *Si X, Y son B-conjuntos reducidos, entonces $X \times Y$ es reducido.*
2. *Si X, Y son B-conjuntos y Y es reducido, entonces $\mathcal{F}^B(X, Y)$ es reducido.*
3. *Pullback de B-conjuntos reducidos es reducido.*
4. *El conjunto unitario $\{*\}$ equipado con la única B-equivalencia posible es reducido.*

Demostración. Sean $(x_1, y_1), (x_2, y_2) \in X \times Y$ tales que $(x_1, y_1) \sim (x_2, y_2) = 1$. Por definición, $x_1 \sim x_2 \wedge y_1 \sim y_2 = 1$, de lo que deducimos que $x_1 \sim x_2 = 1$ y $y_1 \sim y_2 = 1$. Como X, Y son reducidos, tenemos que $x_1 = x_2$ y $y_1 = y_2$, como debíamos probar.

Sean $f, g \in \mathcal{F}^B(X, Y)$ tales que $f \sim g = 1$. Por definición, para cada $x \in X$ tenemos que $f(x) \sim g(x) = 1$. Usando que Y es reducido, tenemos que $\forall x \in X\ f(x) = g(x)$, por lo que $f = g$, como debíamos probar.

Que pullback de reducidos es reducido se debe a que producto de reducidos es reducido y subconjunto de reducido es reducido.

Es directo que el conjunto unitario $\{*\}$ equipado con la única B-equivalencia posible es reducido. □

También se cumple que el producto arbitrario de B-conjuntos reducidos es reducido. La prueba es análoga a la del caso binario.

Teorema 2.2.12. *La subcategoría llena B-Set^r conformada por los B-conjuntos reducidos es también cartesiana cerrada y completa.*

2.2.3. Los B-conjuntos mezclables

Hay B-conjuntos en los que se puede mezclar elementos (en el sentido de que existe otro elemento, denominado mezcla, que cumple cierta propiedad). Intuitivamente, se lo puede considerar análogo a la posibilidad de realizar combinaciones lineales en espacios vectoriales. Cuando interpretemos la lógica de orden superior (en el capítulo 3), en general será útil restringirnos a B-conjuntos que cumplan esta propiedad.

Definición 2.2.13 (B-conjunto mezclable)**.** Un B-conjunto $(X, \sim)$ es *mezclable* si para cualquier anticadena $A \subseteq B$ y para cualquier familia $(x_a)_{a \in A}$ de elementos de X, existe $\hat{x} \in X$ tal que para todo $a \in A$ se cumple $\hat{x} \sim x_a \geq a$. Notaremos $\hat{x} = \sum_{a \in A} a \cdot x_a$ o $\hat{x} = a \cdot x_a + b \cdot x_b$, en el caso en que $|A| = 2$.

Usamos la palabra «mezcla» por la intuición de que estamos mezclando la familia $\{x_a\}_{a \in A} \subseteq X$, poniendo cada elemento x_a con proporción al menos a (pues $\hat{x} \sim x_a \geq a$).

Es importante aclarar que en general las mezclas no tienen por qué ser únicas. La notación $\hat{x} = \sum_{a \in A} a \cdot x_a$ es una forma compacta de afirmar que $\hat{x}$ es una mezcla para la anticadena A y la familia $(x_a)_{a \in A}$. Utilizaremos esa notación por comodidad, pero siempre con la precaución de no manipularla como si implicara que la mezcla sea única.

Observamos que para B-conjuntos no vacíos, la existencia de mezclas con anticadenas es equivalente a la existencia de mezclas con particiones de la unidad.

Lema 2.2.14. *Un B-conjunto $(X, \sim)$ es mezclable si y solo si es no vacío y para cada partición de la unidad $C \subseteq B$ y cada familia $(x_c)_{c \in C}$ de elementos de X, existe mezcla.*

Demostración. Para el directo hay que ver que la condición de ser mezclable implica que $X \neq \varnothing$. Esto es porque debe haber mezcla para la anticadena vacía y la familia vacía. Veamos el recíproco. Sea $A \subseteq B$ una anticadena no vacía (la anticadena vacía y la familia vacía tienen cualquier elemento de X como mezcla). Sea $a_0 \in A$. Definimos una partición de la unidad C es la siguiente forma:

$$C = \{a_0 \vee (\bigvee A)^*\} \cup (A \backslash \{a_0\})$$

Sustituimos a_0 por $a_0 \vee (\bigvee A)^*$ y el resto de A se mantiene igual. De esa forma, C está en correspondencia con A. Por hipótesis, tenemos $\hat{x} = \sum_{c\in C} c \cdot x_{a_c}$. Vemos que $\hat{x}$ también es mezcla con respecto a A. Si $a \neq a_0$ entonces $\hat{x} \sim x_a \geq c_a = a$ y en el caso de a_0 se cumple $\hat{x} \sim x_{a_0} \geq c_{a_0} = a_0 \vee (\bigvee A)^* \geq a_0$. □

Continuamos con la unicidad de mezclas con particiones de la unidad salvo equivalencia booleana (y por lo tanto unicidad a secas en B-conjuntos reducidos).

Lema 2.2.15. *En un B-conjunto mezclable las mezclas con particiones de la unidad son únicas salvo equivalencia booleana. Es decir, si $\hat{x}$ y $\hat{y}$ son mezclas para $C \subseteq B$ partición de la unidad y $\{x_c\}_{c\in C} \subseteq X$, entonces $\hat{x} \sim \hat{y} = 1$.*

Demostración. Se deduce en base al siguiente razonamiento, que será recurrente al trabajar con mezclas. Sea $c \in C$.

$$\hat{x} \sim \hat{y} \geq \hat{x} \sim x_c \wedge x_c \sim \hat{y} \geq c \wedge c = c$$

Tomando supremo en c y usando que C es partición de la unidad se deduce $\hat{x} \sim \hat{y} = 1$. □

Veamos que el B-conjunto $(B, \leftrightarrow)$ es mezclable, que producto de mezclables es mezclable, que reducido de mezclable es mezclable y que exponencial con codominio mezclable es mezclable. En el capítulo 4 veremos que los reales aleatorios también son mezclables.

Proposición 2.2.16. *$(B, \leftrightarrow)$ es mezclable con mezcla:*

$$\sum_{c\in C} c \cdot x_c = \bigvee_{c\in C} (c \wedge x_c)$$

Demostración. Sean C una partición de la unidad y $\{x_c\}_{c\in C} \subseteq B$. Sea $\hat{x} = \bigvee_{c\in C}(c \wedge x_c)$. Hay que ver que para cada c, se cumple $c \leq x_c \leftrightarrow \hat{x}$. Es equivalente a $c \wedge x_c \leq \hat{x}$ y $c \wedge \hat{x} \leq x_c$, por el lema 1.1.2. La primera desigualdad es directa porque $c \wedge x_c$ es un elemento del conjunto al que se toma supremo en $\hat{x}$. Veamos la segunda:

$$c \wedge \hat{x} = c \wedge \bigvee_{d\in C} (d \wedge x_d) = \bigvee_{d\in C} (c \wedge d \wedge x_d) = c \wedge x_c \leq x_c$$

En la última igualdad usamos que C es una anticadena, por lo que $c \wedge d = 0$ si $c \neq d$. □

Proposición 2.2.17. *Si X, Y son B-conjuntos mezclables entonces $X \times Y$ es mezclable.*

Demostración. Como X y Y son no vacíos, $X \times Y$ también lo es. Sean C una partición de la unidad y $\{(x_c, y_c)\}_{c\in C} \subseteq X \times Y$. Definimos la mezcla utilizando la de X en la primera coordenada y la de Y en la segunda:

$$\hat{z} = \sum_{c\in C} c \cdot (x_c, y_c) = \left(\sum_{c\in C} c \cdot x_c, \sum_{c\in C} c \cdot y_c \right)$$

Sea $b \in A$. Veamos que $\hat{z} \sim (x_b, y_b) \geq b$.

$$\hat{z} \sim (x_b, y_b) = \sum_{c\in C} c \cdot x_c \sim x_b \wedge \sum_{c\in C} c \cdot y_c \sim y_b \geq b \wedge b = b$$

Utilizamos que $\sum_{c\in C} c \cdot x_c \sim x_b \geq b$ y $\sum_{c\in C} c \cdot y_c \sim x_b \geq b$. □

Análogamente, se prueba que producto arbitrario de B-conjuntos mezclables es mezclable.

Proposición 2.2.18. *Si X es un B-conjunto mezclable, entonces su reducido (2.2.10) también es mezclable.*

Demostración. El reducido de un conjunto no vacío es no vacío. Sean C una partición de la unidad y $\{[x_c]\}_{c\in C} \subseteq X/\equiv$. Definimos la mezcla de la siguiente forma:

$$\sum_{c\in C} c \cdot [x_c] = \left[\sum_{c\in C} c \cdot x_c\right]$$

Para $b \in A$, tenemos que $[\sum_{c\in C} c \cdot x_c] \sim [x_b] = \sum_{c\in C} c \cdot x_c \sim x_b \geq b$. □

Proposición 2.2.19. *Si X, Y son B-conjuntos y Y es mezclable, $\mathcal{F}^B(X,Y)$ es mezclable.*

Demostración. Como Y es no vacío, $\mathcal{F}^B(X,Y)$ también lo es. Sean $C \subseteq B$ una partición de la unidad y $\{f_c\}_{c\in C} \subseteq \mathcal{F}^B(X,Y)$. Nuestro candidato a mezcla es $\hat{f} : X \to Y$, definida usando la mezcla de Y:

$$\hat{f}(x) = \sum_{c\in C} c \cdot f_c(x)$$

Veamos que $\hat{f} \in \mathcal{F}^B(X,Y)$. Sean $x_1, x_2 \in X$. Dado $c \in C$:

$$\hat{f}(x_1) \sim \hat{f}(x_2) \geq \hat{f}(x_1) \sim f_c(x_1) \wedge f_c(x_1) \sim f_c(x_2) \wedge f_c(x_2) \sim \hat{f}(x_2) \geq c \wedge x_1 \sim x_2$$

En el último paso usamos que $\hat{f}(x_i) \sim_\sigma f_c(x_i) \geq c$ por la propiedad de las mezclas y que como $f_c \in \mathcal{F}^B(X,Y)$ entonces $f_c(x_1) \sim f_c(x_2) \geq x_1 \sim x_2$. Por lo tanto tenemos que $\hat{f}(x_1) \sim \hat{f}(x_2) \geq c \wedge x_1 \sim_\tau x_2$ para cualquier $c \in C$. Como C es una partición de la unidad, tomando supremo concluimos la desigualdad buscada. Ahora que sabemos que $\hat{f} \in \mathcal{F}^B(X,Y)$, veamos que cumple la propiedad de la mezcla. Sea $c \in C$:

$$\hat{f} \sim f_c = \bigwedge_{x\in X} \hat{f}(x) \sim f_c(x) \geq \bigwedge_{x\in X} c = c$$

En la última desigualdad usamos la propiedad de la mezcla en Y. □

Como corolario de lo anterior, podemos ver que todo B-conjunto puede extenderse a uno mezclable (aunque no sea algo que vayamos a utilizar).

Corolario 2.2.20. *Sea X un B-conjunto no vacío. Entonces $\mathcal{F}^B(X,B)$ es mezclable y contiene una copia de X, en el sentido de que tiene un subconjunto isomorfo a X como B-conjunto.*

Demostración. Que $\mathcal{F}^B(X,B)$ es mezclable se deduce de las proposiciones anteriores. La copia de X es $\{\varphi_x \,/\, x \in X\} \subseteq \mathcal{F}^B(X,B)$ con $\varphi_x(z) = x \sim z$. Veamos que $\varphi_x \in \mathcal{F}^B(X,B)$. Sean $z_1, z_2 \in X$. Debemos probar que $z_1 \sim z_2 \leq x \sim z_1 \leftrightarrow x \sim z_2$. Es equivalente a probar que $z_1 \sim z_2 \wedge x \sim z_1 \leq x \sim z_2$ y $z_1 \sim z_2 \wedge x \sim z_2 \leq x \sim z_1$, lo cuales se cumplen por la transitividad de B-conjuntos. Veamos que para todos $x, y \in X$, $\varphi_x \sim \varphi_y = x \sim y$, lo cual implica que $\{\varphi_x \,/\, x \in X\}$ y X son isomorfos como B-conjuntos. Tenemos que:

$$\varphi_x \sim \varphi_y = \bigwedge_{z\in X} (x \sim z \leftrightarrow y \sim z)$$

Con $z = y$ tenemos que $\varphi_x \sim \varphi_y \leq x \sim y$. Para probar la otra desigualdad, tomamos un $z \in X$ e intentamos probar que $x \sim y \leq x \sim z \leftrightarrow y \sim z$. Nuevamente, es equivalente a que $x \sim y \wedge x \sim z \leq y \sim z$ y $x \sim y \wedge y \sim z \leq x \sim z$, los cuales se cumplen por transitividad. □

Con lo que probamos hasta ahora, podemos afirmar que la subcategoría llena de los B-conjuntos mezclables es una categoría cartesiana cerrada. Sin embargo, no podemos afirmar que sea completa, porque a priori pueden no haber pullbacks. Para probar que pullback de mezclables es mezclable, debemos asumir también que los B-conjuntos son reducidos.

Proposición 2.2.21. *El pullback de B-conjuntos mezclables reducidos es mezclable.*

Demostración. Volvemos al contexto de la prueba de la proposición 2.2.7. Debemos probar que W es mezclable. Vamos a utilizar que Z es reducido (de hecho, el concepto de B-conjunto reducido fue introducido por ser necesario para esta prueba). Dada una partición de la unidad C y una familia $\{(x_c, y_c)\}_{c \in C} \subseteq S$, debemos probar que la mezcla está en W, o sea que cumple la propiedad que define al subconjunto. Por lo tanto, dado que la mezcla es $(\sum c \cdot x_c, \sum c \cdot y_c)$, hay que probar que $f(\sum c \cdot x_c) = g(\sum c \cdot y_c)$. Vamos a razonar utilizando que C es partición de la unidad. Sea $b \in C$.

$$\begin{aligned} f\left(\sum c \cdot x_c\right) \sim g\left(\sum c \cdot y_c\right) &\geq f\left(\sum c \cdot x_c\right) \sim f(x_b) \wedge f(x_b) \sim g\left(\sum c \cdot y_c\right) \\ &= f\left(\sum c \cdot x_c\right) \sim f(x_b) \wedge g(y_b) \sim g\left(\sum c \cdot y_c\right) \\ &\geq \sum c \cdot x_c \sim x_b \wedge \sum c \cdot y_c \sim y_b \\ &\geq b \wedge b = b \end{aligned}$$

Tomando supremo en $b \in A$ tenemos $f(\sum a \cdot x_a) \sim g(\sum a \cdot y_a) = 1$ y como Z es reducido concluimos que $f(\sum a \cdot x_a) = g(\sum a \cdot y_a)$. □

Teorema 2.2.22. *La subcategoría llena B-Set_m^r conformada por los B-conjuntos reducidos mezclables es cartesiana cerrada y completa.*

Capítulo 3

Lógica de orden superior con equivalencias booleanas

En este capítulo, presentamos la lógica de orden superior y sus interpretaciones en la categoría de los B-conjuntos, introducida en el capítulo 2. Demostraremos propiedades de dichos modelos que justifican la elección de esa categoría en particular. Posteriormente, en el capítulo 4, utilizaremos este marco para realizar la prueba de consistencia de la negación de la hipótesis del continuo. Específicamente, dentro de ZF, que es nuestra metateoría, construiremos un modelo del tipo introducido en este capítulo, en el cual se cumplirá la negación de la hipótesis del continuo.

3.1. Lógica de orden superior

La lógica de orden superior (HOL) es un formalismo que organiza el universo matemático a partir de ciertos tipos de base, y luego permite construir objetos cada vez más complejos mediante tipos de funciones o de predicados. En general, los tipos de base incluyen un tipo de proposiciones (que permite representar los enunciados matemáticos), así como uno o varios tipos para representar los objetos de base de la teoría, como los enteros naturales o los números reales.

A modo de ejemplo, adelantando notación que introduciremos en lo siguiente, supongamos que los tipos de base son `Prop`, para las proposiciones (o equivalentemente, los valores de verdad), y R para los reales. En este caso tendríamos entre otros al tipo $R \to R$ de las funciones reales, el tipo $(R \to R) \to R$ de las funcionales, el tipo $((R \to R) \to R) \to R$ de las funcionales de segundo orden, etc. La principal utilidad del tipo `Prop` es que permite construir tipos de predicados o conjuntos. A modo de ejemplo, el tipo $R \to$ `Prop` representa los predicados sobre reales o equivalentemente los conjuntos de reales. Esto es porque un objeto de tipo $R \to$ `Prop` representa una función que a cada real le asocia un valor de verdad, lo cual además de ser un predicado, codifica un conjunto al ser pensado como función característica (el resultado de aplicar la función a un elemento es el valor de verdad de la pertenencia de ese elemento).

En esta monografía, usaremos una presentación de HOL en el estilo de la teoría de tipos simples de Church, basándonos en el cálculo lambda simplemente tipado extendido con un tipo de proposiciones. Todos estos conceptos se presentan en las siguientes secciones.

3.1.1. El cálculo lambda simplemente tipado

El cálculo lambda simplemente tipado consiste en un conjunto de tipos, que representan distintas clases de objetos, y un conjunto de términos, cada uno de los cuales tiene un tipo asociado y representa un objeto particular de esa clase.

Los tipos se construyen recursivamente a partir de ciertos tipos de base mediante la construcción flecha, que asocia a cada par de tipos τ y σ el tipo $\tau \to \sigma$ de las funciones de τ en σ. Formalmente, el formalismo está parametrizado por un conjunto no vacío de tipos de base, escritos α, β, γ, etc. La definición es la siguiente.

Definición 3.1.1. Dado un conjunto de tipos de base, denotados α, β, γ, etc, definimos el conjunto de los *tipos*, denotados τ, σ, etc, recursivamente con las dos siguientes reglas.

1. Cada tipo de base α es un tipo.
2. Si τ y σ son tipos, entonces $\tau \to \sigma$ es un tipo.

Es decir: un tipo es o bien un tipo de base (α), o bien un tipo flecha $\tau \to \sigma$ construido a partir de dos tipos τ, σ ya definidos.

Usando notación BNF, los tipos se definen con la siguiente gramática:

$$\tau, \sigma \ := \ \alpha \mid \tau \to \sigma$$

Las flechas asocian a la derecha, en el sentido de que $\tau \to \sigma \to \mu$ es $\tau \to (\sigma \to \mu)$. Si bien estrictamente los tipos representan solamente funciones de una variable, mediante currificación se puede trabajar con funciones de varias variables. Si queremos considerar una función que recibe dos argumentos de tipo τ y retorna uno de tipo σ usamos el tipo $\tau \to (\tau \to \sigma)$. A modo de analogía, esto es exactamente lo que se hace en cálculo integral de varias variables al introducir las integrales iteradas y el teorema de Fubini. Se pasa de una función $f(x, y)$ de dos variables a una correspondencia $x \mapsto f_x(y)$, que a cada $x \in \mathbb{R}$ le asocia una función que varía solamente la variable y. Se podría decir que esta correspondencia es justamente de tipo $\mathbb{R} \to (\mathbb{R} \to \mathbb{R})$, ya que a cada real le asocia una función real.

A modo de ejemplo, si los tipos de base son A y B, los siguientes son algunos ejemplos de tipos.

$$A \qquad B \qquad A \to B \qquad A \to A \qquad A \to (A \to B) \to B \qquad ((B \to A) \to A) \to B$$

Los términos, que representan objetos de los distintos tipos, se definen recursivamente con construcciones que permiten hablar de abstracción (definición) y evaluación de funciones. Formalmente, se utilizan los siguientes conjuntos de símbolos.

- Un conjunto de constantes tipadas, denotadas c, d, etc. Esto quiere decir que cada constante c tiene asociado un tipo τ, lo cual denotamos simplemente con $c : \tau$. El conjunto de constantes parametriza el formalismo, en el sentido de que teniendo definidos los tipos, se pueden usar distintos conjuntos de constantes para definir distintos conjuntos de términos.

- Un conjunto de variables tipadas, denotadas x^τ, y^σ, etc. Esto quiere decir que cada variable está asociada a un tipo y de hecho con esta notación, el tipo está presente como supraíndice en la variable. Se supone que para cada tipo tenemos una cantidad numerable de variables de ese tipo.

Usamos una presentación en la que cada término está definido con su tipo, es decir, el tipado está incluido en la definición de los términos.

Definición 3.1.2 (términos)**.** Los términos, denotados M, N, etc en general, están definidos recursivamente mediante las siguientes reglas:

1. Cada variable x^τ de tipo τ es un término de tipo τ.
2. Cada constante c de tipo τ es un término de tipo τ.
3. Si x^τ es una variable de tipo τ y M es un término de tipo σ, entonces $\lambda x^\tau.\, M$ es un término de tipo $\tau \to \sigma$. A estos términos les llamamos *abstracciones*.
4. Si M es un término de tipo $\tau \to \sigma$ y N es un término de tipo τ, entonces MN es un término de tipo σ. A estos términos les llamamos *aplicaciones*.

Usaremos la notación $M : \tau$ para indicar que M es un término de tipo τ. Las aplicaciones asocian a la izquierda, en el sentido de que por ejemplo $MNQ = (MN)Q$. Por otra parte, las aplicaciones tienen mayor precedencia que las abstracciones (términos λ), en el sentido de que por ejemplo $\lambda x^\tau.\, fx$ es $\lambda x^\tau.\, (fx)$.

El término $\lambda x^\tau.\, M$ representa la función que recibe un x de tipo τ y retorna M (término que puede depender de x). Como un primer ejemplo sencillo, $\lambda x^\tau.\, x$ representa la función identidad del tipo τ. Por otra parte, el término MN representa la aplicación del término M (que debe representar una función) al término N (que debe representar un elemento del dominio de dicha función). Por ejemplo, $(\lambda x^\tau.\, x)y^\tau$ representa la función identidad del tipo τ aplicada a la variable y de tipo τ. Notar que realizamos un abuso del lenguaje: cuando el tipo de una variable es claro, omitimos el supraíndice (por ejemplo en la segunda ocurrencia de x en $\lambda x^\tau.\, x$).

Supongamos que tenemos un tipo R y una constante $0 : R$. Los siguientes son ejemplos de términos con sus correspondientes tipos.

$$0 : R \qquad \lambda x^R.\, x : R \to R \qquad \lambda x^R.\, 0 : R \to R \qquad \lambda f^{R\to R} \lambda x^R.\, fx : (R \to R) \to R \to R$$

El primer término representa el elemento 0, el segundo la función identidad de R en R, el tercero la función constante 0 de R en R y el último una función de alto orden que dada una función f y un elemento x, retorna la función f evaluada en el elemento x.

En los términos de la forma $\lambda x^\tau.\, M$ (las abstracciones), decimos que todas las ocurrencias de la variable x dentro de M están ligadas. Decimos que una ocurrencia de una variable en un término es *libre* si no está ligada por ninguna abstracción (se trata de un concepto totalmente análogo al de las variables libres en lógica de primer orden, con las abstracciones jugando el papel de los cuantificadores). Dado un término M, denotamos $\mathrm{FV}(M)$ al conjunto de las variables libres de M. Si un término no tiene variables libres decimos que es *cerrado*.

Nuestro objetivo es poder efectivamente realizar evaluaciones con los términos, de modo que por ejemplo el término $(\lambda x^\tau.\, x)y^\tau$ se pueda evaluar en el término y^τ. Esto se formaliza con la relación de β-equivalencia, para la cual primero debemos introducir la operación de sustitución.

Dados un término M, una variable x^τ y un término N de tipo τ, definimos $M[x := N]$ como el término que se obtiene remplazando en M las ocurrencias *libres* de la variable x por el término N. El resultado es un término del mismo tipo que M. Para que este término esté bien formado, es importante que N sea un término del mismo tipo que la variable x. A modo de ejemplo:

$$(\lambda f^{\tau\to\tau}\lambda x^\tau.\, f^{\tau\to\tau}x^\tau)g^{\tau\to\tau}x^\tau\ [x^\tau := g^{\tau\to\tau}y^\tau]\ \equiv\ (\lambda f^{\tau\to\tau}\lambda x^\tau.\, f^{\tau\to\tau}x^\tau)g^{\tau\to\tau}g^{\tau\to\tau}y^\tau$$

En la operación de sustitución, al igual que en lógica de primer orden, se trabaja a menos de α-equivalencia para evitar problemas de captura de variable. La α-equivalencia nos permite a conveniencia cambiar los nombres de las variables ligadas (las que no están libres), lo cual claramente no cambia el significado del término (todas las construcciones que haremos son independientes de cambio de nombre de variables ligadas). A modo de ejemplo, los términos $\lambda f^{\tau\to\tau}.\, fx^\tau$ y $\lambda g^{\tau\to\tau}.\, gx^\tau$ son equivalentes, pero si remplazáramos la variable x^τ por otra, el término resultante no sería equivalente, porque la variable x^τ está libre. La forma en que utilizaremos esto es que al realizar una sustitución de tipo $\lambda y^\tau.\, M[x^\sigma := N]$, antes remplazaremos la variable y por una fresca, es decir que no aparezca dentro de M ni de N (siempre podemos hacer esto porque los términos solo puede tener finitas variables). Por ejemplo, al realizar la sustitución $\lambda f^{\tau\to\tau}.\, fg^{\tau\to\tau}x^\tau[x := fx]$, como f está libre en fx, antes de realizar la sustitución cambiamos $\lambda f^{\tau\to\tau}.\, fg^{\tau\to\tau}x^\tau$ por $\lambda h^{\tau\to\tau}.\, hg^{\tau\to\tau}x^\tau$ y el resultado es $\lambda h^{\tau\to\tau}.\, hg^{\tau\to\tau}f^{\tau\to\tau}x^\tau$. El único lugar en el que utilizaremos esto de forma explícita es en la demostración del lema 3.3.5.

Para definir la relación de β-equivalencia realizamos las siguientes etapas.

1. Definimos la *β-reducción*, denotada $\to$, como la relación:
$$(\lambda x^\tau.\, M)N \to M[x^\tau := N]$$
2. Definimos la *β-reducción en una etapa*, denotada $\to_\beta$, como la clausura contextual de la β-reducción. Esto significa que la β-reducción se puede realizar adentro del término. A modo de ejemplo:
$$f^{\tau\to\tau}((\lambda x^\tau.\, x)y^\tau) \to_\beta f^{\tau\to\tau}(y^\tau)$$
3. Definimos la *β-equivalencia*, denotada $\equiv_\beta$ como la clausura reflexiva-simétrica-transitiva de la β-reducción en una etapa, es decir la menor relación de equivalencia que incluye a la anterior. Esto implica que, dados dos términos M y N, si existen términos $Q_1, \ldots, Q_n$, $P_1, \ldots, P_m$ y L tales que $M \to_\beta Q_1 \to_\beta \cdots \to_\beta Q_n \to_\beta L$ y por otra parte $N \to_\beta P_1 \to_\beta \cdots \to_\beta P_m \to_\beta L$, entonces $M \equiv_\beta N$.

A modo de ejemplo sencillo, tenemos que $(\lambda x^\tau.\, x)y^\tau \equiv_\beta y^\tau$. Como segundo ejemplo, tenemos que $(\lambda f^{\tau\to\tau}.\, f)g^{\tau\to\tau}y^\tau \equiv_\beta g^{\tau\to\tau}((\lambda x^\tau.\, x)y^\tau)$, no obstante, no será común que usemos la β-equivalencia como en este ejemplo, en el que en particular cambiamos y^τ por $(\lambda x^\tau.\, x)y^\tau$; lo más usual es que procedamos en el otro sentido, como con el remplazo de $(\lambda f^{\tau\to\tau}.\, f)g^{\tau\to\tau}$ por $g^{\tau\to\tau}$. En general, la intuición es que estamos evaluando un término cuando remplazamos fragmentos de la forma $(\lambda x^\tau.\, M)N$ (denominados *redexes*) por $M[x^\tau := N]$.

3.1.2. La lógica de orden superior (HOL)

El cálculo lambda simplemente tipado, con la presentación que utilizamos, está parametrizado por los tipos de base y las constantes. La lógica de orden superior (HOL), se basa en un cálculo lambda simplemente tipado con un tipo de base `Prop`, que representa el tipo de las proposiciones (o valores de verdad) y con constantes para representar las construcciones lógicas de orden superior. Las constantes (con sus tipos correspondientes) son las siguientes.

- Una constante $\Rightarrow : \texttt{Prop} \to \texttt{Prop} \to \texttt{Prop}$ para representar la implicación.
- Para cada tipo τ, una constante $\forall^\tau : (\tau \to \texttt{Prop}) \to \texttt{Prop}$ para representar la cuantificación con dominio τ.

Llamamos proposiciones o fórmulas a los términos de tipo `Prop` y los denotamos con ϕ, ψ, etc. Utilizamos las siguientes notaciones para llevar la escritura al formato usual en matemática:

$$\phi \Rightarrow \psi \ :\equiv \ \Rightarrow \phi\psi \qquad \forall x^\tau.\, \phi \ :\equiv \ \forall^\tau(\lambda x^\tau.\, \phi)$$

Notar que como $\Rightarrow\!: \texttt{Prop} \to \texttt{Prop} \to \texttt{Prop}$, tenemos que $\Rightarrow \phi\psi : \texttt{Prop}$. Es decir, dadas dos proposiciones, ϕ y ψ, tenemos que $\phi \Rightarrow \psi$ es otra proposición, que representa la implicación entre las dos anteriores. Por otra parte, como $\lambda x^\tau.\, \phi : \tau \to \texttt{Prop}$ y además $\forall^\tau : (\tau \to \texttt{Prop}) \to \texttt{Prop}$, tenemos que $\forall^\tau(\lambda x^\tau.\, \phi) : \texttt{Prop}$. Es decir, dadas una una variable x^τ y una proposición ϕ, tenemos que $\forall x^\tau.\, \phi$ es otra proposición, que representa la proposición anterior con la variable x^τ cuantificada universalmente (con el tipo τ como dominio).

Al usar la notación infija, $\Rightarrow$ asocia a la derecha (al igual que $\to$). Por otra parte, las cuantificaciones universales con la notación presentada tienen menor precedencia que las implicaciones. Por ejemplo, $\forall x^\tau.\, \phi \Rightarrow \psi$ es los mismo que $\forall x^\tau.\, (\phi \Rightarrow \psi)$. En algunos casos omitiremos el «.» después de la variable. Cuando hagamos eso consideraremos que la cuantificación tiene la mayor precedencia. A modo de ejemplo, $\forall x^{\texttt{Prop}} x \Rightarrow y^{\texttt{Prop}}$ es $(\forall x^{\texttt{Prop}}.\, x) \Rightarrow y^{\texttt{Prop}}$.

Puede parecer extraño que solamente introduzcamos constantes para la implicación y las cuantificaciones de orden superior. El motivo de este enfoque es que las otras construcciones lógicas son definibles a partir de estas de la siguiente forma.

$$\begin{aligned}
\bot \ &:\equiv \ \forall z^{\texttt{Prop}}.\, z & \qquad \top \ &:\equiv \ \bot \Rightarrow \bot \\
\phi \vee \psi \ &:\equiv \ \forall z^{\texttt{Prop}}.\, (\phi \Rightarrow z) \Rightarrow (\psi \Rightarrow z) \Rightarrow z & \qquad \phi \wedge \psi \ &:\equiv \ \forall z^{\texttt{Prop}}.\, (\phi \Rightarrow \psi \Rightarrow z) \Rightarrow z \\
\neg\phi \ &:\equiv \ \phi \Rightarrow \bot & \qquad \phi \Leftrightarrow \psi \ &:\equiv (\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi) \\
\exists x^\tau.\, \phi \ &:\equiv \ \forall z^{\texttt{Prop}}\, (\forall x^\tau (\phi \Rightarrow z)) \Rightarrow z & \qquad M =_\tau N \ &:\equiv \ \forall z^{\tau \to \texttt{Prop}}.\, zM \Rightarrow zN
\end{aligned}$$

Notar que en general estas codificaciones están inspiradas en las reglas de eliminación usuales de las construcciones lógicas. La definición de $\bot$, por ejemplo, proviene de *ex falso quad libet*, lo cual permite deducir cualquier proposición a partir del absurdo. La definición de $\phi \vee \psi$, por otra parte, nos dice que se cumple cualquier proposición que sea implicada por ϕ e implicada por ψ, lo cual se asemeja a la regla usual de eliminación del $\vee$ en deducción natural. La definición de $M =_\tau N$ nos dice que todo predicado $(z : \tau \to \texttt{Prop})$ que se cumple en M, también se cumple en N.

La sintaxis presentada hasta ahora se denomina Teoría de Tipos Simples de Church. El último elemento de la lógica de orden superior (HOL) es el sistema de deducción, que permite derivar secuentes. Un secuente es un par de la forma $\Gamma \vdash \phi$, donde Γ es una lista finita de proposiciones (términos de tipo `Prop`) y ϕ es una proposición.

Definición 3.1.3 (sistema de deducción)**.** El sistema de deducción de la lógica de orden superior está dado por las siguientes reglas:

$$\frac{}{\Gamma \vdash \phi}\ (\text{si } \phi \in \Gamma) \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash \phi'}\ (\text{si } \phi \equiv_\beta \phi') \qquad \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi} \qquad \frac{\Gamma \vdash \phi \Rightarrow \psi \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \forall x^\tau.\, \phi}\ (\text{si } x^\tau \notin \mathrm{FV}(\Gamma)) \qquad \frac{\Gamma \vdash \forall x^\tau.\, \phi}{\Gamma \vdash \phi[x := M]}\ (M : \tau) \qquad \frac{}{\Gamma \vdash ((\phi \Rightarrow \psi) \Rightarrow \phi) \Rightarrow \phi}$$

Decimos que $\Gamma \vdash \phi$ cuando existe una derivación del secuente.

Tenemos una regla axioma, análoga a la de deducción natural de primer orden. Luego hay una regla que permite trabajar a menos de β-equivalencia. Posteriormente, tenemos las reglas usuales de la implicación y de las cuantificaciones universales (las cuales pueden ser sobre cualquier tipo, pero la lógica de las reglas de introducción y eliminación es la misma que la de primer orden). Finalmente, agregamos la Ley de Peirce que es equivalente al razonamiento por absurdo. Las reglas de deducción usuales de las construcciones lógicas codificadas con implicaciones y cuantificaciones universales son todas derivables.

Una de las características principales de HOL es que para todo tipo τ podemos hablar de conjuntos de objetos de tipo τ mediante el tipo $\tau \to \mathtt{Prop}$. La intuición es que si $A : \tau \to \mathtt{Prop}$, podemos utilizarlo como función característica de un conjunto, de modo que para cada $M : \tau$, el valor de verdad de la pertenencia de M en A es $MA : \mathtt{Prop}$. En este sentido, la construcción $\tau \to \mathtt{Prop}$ en HOL es equivalente a tomar conjunto potencia en la teoría de conjuntos de ZF. Notar que además nada impide que iteremos la construcción anterior. A modo de ejemplo, el tipo $(\tau \to \mathtt{Prop}) \to \mathtt{Prop}$ representa conjuntos de conjuntos de elementos de tipo τ.

3.2. Los modelos booleanos de HOL

El cálculo lambda simplemente tipado se puede interpretar en cualquier categoría cartesiana cerrada. Además, la lógica de alto orden se puede interpretar en cualquier categoría cartesiana cerrada con un objeto que permita representar el tipo de proposiciones.

Cada interpretación de HOL tiene su noción de validez de fórmulas, la cual debe cumplir que todas las fórmulas derivables en HOL sean también fórmulas válidas. No obstante, hay fórmulas que no son derivables en HOL pero que nos pueden interesar como axiomas agregados a HOL. En este trabajo, consideraremos como axiomas extra la extensionalidad funcional, la extensionalidad proposicional, la extensionalidad de predicados, el axioma de elección y la bivalencia, cuyos enunciados se dan a continuación. Cabe aclarar que la extensionalidad funcional, la extensionalidad de predicados y el axioma de elección son en realidad esquemas de axiomas, parametrizados por uno o dos tipos.

- $\texttt{ExtFun}_{\tau,\sigma} :\equiv \forall f, g^{\tau\to\sigma}.\, (\forall x^{\tau}.fx =_{\sigma} gx) \Rightarrow f =_{\tau\to\sigma} g$ para todos tipos τ, σ.
- $\texttt{ExtProp} :\equiv \forall x, y^{\texttt{Prop}}.\, (x \Leftrightarrow y) \Rightarrow x =_{\texttt{Prop}} y$.
- $\texttt{ExtPred}_{\tau} :\equiv \forall P, Q^{\tau\to\texttt{Prop}}.\, (\forall x^{\tau}.Px \Leftrightarrow Qx) \Rightarrow P =_{\tau\to\texttt{Prop}} Q$ para todo tipo τ.
- $\texttt{AC}_{\tau,\sigma} :\equiv \forall S^{\tau\to\sigma\to\texttt{Prop}}.\, \forall x^{\tau}\exists y^{\sigma} Sxy \Rightarrow \exists f^{\tau\to\sigma}\forall x^{\tau} Sx(fx)$ para todos tipos τ, σ.
- $\texttt{Bival} :\equiv \forall x^{\texttt{Prop}}.\, x =_{\texttt{Prop}} \bot \vee x =_{\texttt{Prop}} \top$.

Cabe aclarar que estos axiomas no son independientes. Como veremos en la prueba del teorema 3,3,11, $\texttt{ExtFun}_{\tau,\texttt{Prop}}, \texttt{ExtProp} \vdash \texttt{ExtPred}_{\tau}$ y $\texttt{ExtProp} \vdash \texttt{Bival}$, donde el segundo secuente necesita del tercero excluido para ser demostrado.

Durante lo siguiente vamos a tener en consideración los cinco axiomas, pero desde ya podemos observar que la extensionalidad de predicados es fundamental en nuestro contexto. Como vimos al final de la sección anterior, vamos a usar el tipo $\tau \to \texttt{Prop}$ para representar conjuntos de elementos de tipo τ, considerando cada $A : \tau \to \texttt{Prop}$ como una función característica. Teniendo en cuenta esto, la extensionalidad de predicados resulta exactamente en el axioma de extensionalidad de teoría de conjuntos, el cual nos dice que si dos conjuntos tienen los mismos elementos, entonces son el mismo conjunto. Por lo tanto, al querer usar HOL para trabajar con conjuntos, es indispensable que nuestros modelos cumplan la extensionalidad de predicados.

3.2.1. Interpretación ingenua en la categoría Set

Para entender el interés de trabajar en la categoría B-Set, vale la pena considerar durante un momento lo que pasaría si interpretáramos HOL en la categoría Set en lugar de B-Set. En un marco tan sencillo, los tipos se interpretarían de la siguiente forma (asociando a cada tipo τ un conjunto $[\![\tau]\!]$ por inducción):

- Al tipo $\texttt{Prop}$ se asociaría un álgebra booleana completa B, es decir: $[\![\texttt{Prop}]\!] = B$.
- Para cada otro tipo de base α se fijaría un conjunto no vacío C tal que $[\![\alpha]\!] = C$.
- Para los tipos flecha se usarían espacios de funciones, es decir: $[\![\tau \to \sigma]\!] = [\![\sigma]\!]^{[\![\tau]\!]}$.

Los términos se interpretarían de la siguiente forma, usamos un lenguaje extendido con una constante $\dot{a}$ para cada $a \in [\![\tau]\!]$.

- Para la constante $\Rightarrow$ se utilizaría la implicación de B, es decir $[\![\Rightarrow]\!](a)(b) = a \to b$.
- Para las constantes $\forall^{\tau}$ se utilizarían ínfimos de B, es decir $[\![\forall^{\tau}]\!](f) = \bigwedge_{a\in[\![\tau]\!]} f(a)$, siendo $f \in [\![\tau \to \texttt{Prop}]\!] = B^{[\![\tau]\!]}$.
- Para las constantes $\dot{a}$, tendríamos $[\![\dot{a}]\!] = a$.
- Para cada otra constante c de tipo τ, se fijaría un elemento $c^B \in [\![\tau]\!]$ tal que $[\![c]\!] = c^B$.
- Para $\lambda x^{\tau}.\, M$ definiríamos $[\![\lambda x^{\tau}.\, M]\!](a) = [\![M[x := \dot{a}]]\!]$, con $a \in [\![\tau]\!]$.
- Para MN definiríamos $[\![MN]\!] = [\![M]\!]([\![N]\!])$.

Con lo anterior, podríamos interpretar cada fórmula ϕ : `Prop` en un valor de verdad $[\![\phi]\!] \in B$ y diríamos que ϕ es válida en el modelo si y solo si $[\![\phi]\!] = 1$.

Esta es una forma sencilla de definir modelos de HOL. Sin embargo, en nuestro contexto no nos va a servir, porque, salvo para el caso en que B es el álgebra booleana trivial de dos elementos, la extensionalidad de predicados (el axioma `ExtPred`) no se cumpliría. Recordar que la extensionalidad de predicados es fundamental para trabajar con conjuntos, porque es exactamente el axioma de extensionalidad, que nos dice que dos conjuntos con los mismos elementos son iguales. Como no son los modelos que vamos a utilizar, no entraremos en muchos detalles, pero al final del capítulo haremos una comparación entre las propiedades de estos modelos y las de los que utilizan la categoría B-Set, que son los que sí utilizaremos.

Intuitivamente, el problema parece provenir de que al usar la categoría Set no se aprovecha suficiente el álgebra booleana B. Este problema no va a darse al utilizar la categoría B-Set, que incorpora la estructura del álgebra booleana B en su definición.

3.3. Interpretación de HOL en la categoría B-Set

Presentamos ahora una forma de interpretar HOL en la categoría B-Set, introducida en el capítulo 2. Con esta herramienta, en el capítulo 4 construiremos modelos de la teoría de reales de orden superior, los cuales generalizan los modelos de reales aleatorios presentados por Scott (sección 2.1) y probaremos la consistencia relativa de la negación de la hipótesis del continuo usando un contraejemplo interesante.

3.3.1. Interpretación del cálculo lambda simplemente tipado

Vamos a interpretar el cálculo lambda simplemente tipado en la categoría B-set. Con esto nos referimos a que vamos a asociar a cada tipo τ un B-conjunto $([\![\tau]\!], \sim_\tau)$ y a cada término $M : \tau$ un elemento $[\![M]\!] \in [\![\tau]\!]$.

Comenzamos con la interpretación de los tipos, la cual está parametrizada por las interpretaciones de los tipos de base. Es decir, se debe dar para cada tipo de base α su interpretación $([\![\alpha]\!], \sim_\alpha)$ y luego para los otros tipos se define de forma recursiva (definimos la interpretación del tipo $\tau \to \sigma$ usando las interpretaciones de los subtipos τ y σ).

Definición 3.3.1 (interpretación de tipos)**.** A cada tipo τ se asocia un B-conjunto no vacío $([\![\tau]\!], \sim_\tau)$. Para cada tipo de base se fija la interpretación y luego la interpretación de $\tau \to \sigma$ se define recursivamente como el objeto exponencial $\mathcal{F}^B([\![\tau]\!], [\![\sigma]\!])$, es decir:

$$[\![\tau \to \sigma]\!] := \{f \in [\![\sigma]\!]^{[\![\tau]\!]} \ / \ \forall a, b \in [\![\tau]\!] \ \ a \sim_\tau b \leq f(a) \sim_\sigma f(b)\}$$
$$f \sim_{\tau\to\sigma} g := \bigwedge_{a \in [\![\tau]\!]} f(a) \sim_\sigma g(a)$$

Notar que $[\![\tau \to \sigma]\!]$ es no vacío por las funciones constantes. Lo siguiente es definir interpretación de términos. Vamos a utilizar el enfoque de las valuaciones.

Definición 3.3.2 (Valuación)**.** Una valuación ρ es una función que asocia a cada variable x^τ un elemento $\rho(x) \in [\![\tau]\!]$.

La interpretación de términos está parametrizada por una función $c \mapsto c^{\mathcal{B}}$ que asocia a cada constante $c : \tau$ un elemento $c^{\mathcal{B}} \in [\![\tau]\!]$. En general se define de forma recursiva. Definimos casos de base para las variables y las constantes. Luego, definimos la interpretación de un término $\lambda x^\tau.\, M$ asumiendo que ya sabemos calcular la interpretación de M y definimos la de un término MN asumiendo que ya sabemos calcular la de M y la de N.

Definición 3.3.3 (Interpretación de términos)**.** Para cada término $M : \tau$ y cada valuación ρ se define la interpretación del término bajo la valuación, $[\![M[\rho]]\!] \in [\![\tau]\!]$, por recursión en la estructura del término:

$$\begin{aligned} [\![x^\tau[\rho]]\!] &= \rho(x) \\ [\![c[\rho]]\!] &= c^{\mathcal{B}} \\ [\![\lambda x^\tau.\, M[\rho]]\!](a) &= [\![M[\rho, x \leftarrow a]]\!] \qquad \text{para cada } a \in [\![\tau]\!] \\ [\![MN[\rho]]\!] &= [\![M[\rho]]\!]([\![N[\rho]]\!]) \end{aligned}$$

donde $(\rho, x \leftarrow a)$ es otra valuación que en x vale a y en las otras variables vale lo mismo que ρ.

Hay que demostrar que la definición es correcta. No se deduce directamente por inducción debido al caso de la abstracción. Incluso asumiendo que $[\![M[\rho']]\!] \in [\![\sigma]\!]$ para cualquier valuación ρ', no es claro que $[\![\lambda x^\tau.\, M[\rho]]\!] \in [\![\tau \to \sigma]\!]$, pues esto significa que debe ser una función compatible (por ahora solo estaría claro que es una función de $[\![\tau]\!]$ en $[\![\sigma]\!]$). Lo resolvemos en el siguiente lema, del cual nos interesa solamente el primer ítem, pero la forma de probarlo es por inducción simultanea con el segundo ítem.

Lema 3.3.4. *Para cada término $M : \sigma$ se cumple lo siguiente:*

1. *Para cada valuación ρ, tenemos que $[\![M[\rho]]\!] \in [\![\sigma]\!]$.*
2. *Para cada valuación ρ, para cada variable x^τ y para cada $a, b \in [\![\tau]\!]$, se cumple que:*

$$a \sim_\tau b \leq [\![M[\rho, x \leftarrow a]]\!] \sim_\sigma [\![M[\rho, x \leftarrow b]]\!]$$

Demostración. Se demuestran simultáneamente por inducción en M. Detallaremos un poco lo que esto significa, ya que es la primera prueba por inducción estructural del trabajo. Probamos que para todo término M se ccumple una propiedad $P(M)$ demostrando las siguientes cosas:

- Un primer caso base para las variables. Demostramos que para cada variable x^τ se cumple $P(x^\tau)$.
- Un segundo caso base para las constantes. Demostramos que para cada constante c se cumple $P(c)$.
- Un primer caso inductivo para las abstracciones. Dado un término $\lambda x^\tau.\, M$, asumimos como hipótesis inductiva que se cumple $P(M)$ y probamos que también se cumple $P(\lambda x^\tau.\, M)$.

- Un segundo caso inductivo para las aplicaciones. Dado un término MN, asumimos como hipótesis que se cumplen $P(M)$ y $P(N)$, con lo cual probamos que también se cumple $P(MN)$.

Decir que demostramos las propiedades simultáneamente por inducción significa que nuestra propiedad $P(M)$ consiste de los dos ítems (su conjunción). Por lo tanto, en cada paso debemos probar los dos ítems y las hipótesis inductivas también consisten en los dos ítems.

Caso $M \equiv y^\sigma$**. 1)** $[\![y^\sigma[\rho]]\!] = \rho(y) \in [\![\sigma]\!]$ por definición de valuación.

2) Si $x \not\equiv y$ entonces $[\![y[\rho, x \leftarrow a]]\!] = [\![y[\rho, x \leftarrow b]]\!]$. En este caso la desigualdad se cumple por la reflexividad de $\sim_\sigma$. Si $x \equiv y$ entonces $[\![x[\rho, x \leftarrow a]]\!] = a$ y $[\![x[\rho, x \leftarrow b]]\!] = b$, por lo que la desigualdad queda $a \sim_\tau b \leq a \sim_\tau b$ (notar que en este caso $\tau \equiv \sigma$).

Caso $M \equiv c$**:** El primer ítem se cumple por definición de interpretación de constante y el segundo nuevamente por reflexividad.

Caso $M \equiv \lambda y^\mu.\, N$**. 1)** Primero hay que ver que $[\![\lambda y^\mu.\, N[\rho]]\!] \in [\![\eta]\!]^{[\![\mu]\!]}$, con $N : \eta$. El dominio de $[\![\lambda y^\mu.\, N[\rho]]\!]$ es $[\![\mu]\!]$ por definición y para cada $a \in [\![\mu]\!]$, tenemos que $[\![\lambda y^\mu.\, N[\rho]]\!](a) = [\![N[\rho, y \leftarrow a]]\!]$, el cual está en $[\![\eta]\!]$ por la hipótesis inductiva 1 utilizada con la valuación $(\rho, y \leftarrow a)$. La condición que se pide a las funciones de $[\![\eta]\!]^{[\![\mu]\!]}$ para estar en $[\![\mu \to \eta]\!]$ se deduce de la hipótesis inductiva 2.

2) Hay que probar que $a \sim_\tau b \leq [\![\lambda y^\mu.\, N[\rho, x \leftarrow a]]\!] \sim_{\mu\to\eta} [\![\lambda y^\mu.\, N[\rho, x \leftarrow b]]\!]$. Suponemos $x \not\equiv y$, pues en el caso en que son iguales las interpretaciones dan la misma función y por reflexividad el lado derecho de la desigualdad es 1.

$$
\begin{aligned}
[\![\lambda y^\mu.\, N[\rho, x \leftarrow a]]\!] \sim_{\mu\to\eta} [\![\lambda y^\mu.\, N[\rho, x \leftarrow b]]\!] & \\
&= \bigwedge_{c \in [\![\mu]\!]} [\![N[\rho, x \leftarrow a, y \leftarrow c]]\!] \sim_\eta [\![N[\rho, x \leftarrow b, y \leftarrow c]]\!] \\
&= \bigwedge_{c \in [\![\mu]\!]} [\![N[\rho, y \leftarrow c, x \leftarrow a]]\!] \sim_\eta [\![N[\rho, y \leftarrow c, x \leftarrow b]]\!] \\
&\geq \bigwedge_{c \in [\![\mu]\!]} a \sim_\tau b \quad = a \sim_\tau b
\end{aligned}
$$

donde usamos la hipótesis inductiva 2 con la valuación $(\rho, y \leftarrow c)$.

Caso $M \equiv M'N$**. 1)** Supongamos $M : \mu \to \sigma$ y $N : \mu$. Por hipótesis inductiva 1 tenemos que $[\![M'[\rho]]\!] \in [\![\sigma]\!]^{[\![\mu]\!]}$ y $[\![N[\rho]]\!] \in [\![\mu]\!]$. Usando que $[\![M'N[\rho]]\!] = [\![M'[\rho]]\!]([\![N[\rho]]\!])$ concluimos que $[\![M'N[\rho]]\!] \in [\![\sigma]\!]$.

2) Debemos probar $a \sim_\tau b \leq [\![M'N[\rho, x \leftarrow a]]\!] \sim_\sigma [\![M'N[\rho, x \leftarrow b]]\!]$, siendo el segundo igual a $[\![M'[\rho, x \leftarrow a]]\!]([\![N[\rho, x \leftarrow a]]\!]) \sim_\sigma [\![M'[\rho, x \leftarrow b]]\!]([\![N[\rho, x \leftarrow b]]\!])$. Por una parte, utilizando la hipótesis inductiva 2 de M' y la definición de $\sim_{\mu\to\sigma}$:

$$
\begin{aligned}
a \sim_\tau b &\leq [\![M'[\rho, x \leftarrow a]]\!] \sim_{\mu\to\sigma} [\![M'[\rho, x \leftarrow b]]\!] \\
&\leq [\![M'[\rho, x \leftarrow a]]\!]([\![N[\rho, x \leftarrow a]]\!]) \sim_\sigma [\![M'[\rho, x \leftarrow b]]\!]([\![N[\rho, x \leftarrow a]]\!])
\end{aligned}
$$

Por otra parte, usando la hipótesis inductiva 2 de N y que $[\![M'[\rho, x \leftarrow b]]\!] \in [\![\mu \to \sigma]\!]$:

$$
\begin{aligned}
a \sim_\tau b &\leq [\![N[\rho, x \leftarrow a]]\!] \sim_\mu [\![N[\rho, x \leftarrow b]]\!] \\
&\leq [\![M'[\rho, x \leftarrow b]]\!]([\![N[\rho, x \leftarrow a]]\!]) \sim_\sigma [\![M'[\rho, x \leftarrow b]]\!]([\![N[\rho, x \leftarrow b]]\!])
\end{aligned}
$$

Tomando conjunción y usando transitividad de $\sim_\sigma$, terminamos. □

Se prueba por inducción que dado un término M, si ρ y ρ' son dos valuaciones que coinciden en $\mathrm{FV}(M)$, entonces $[\![M[\rho]]\!] = [\![M[\rho']]\!]$. En particular, si M es un término cerrado, $[\![M[\rho]]\!]$ no depende de la valuación. En base a eso, cuando M sea cerrado a veces escribiremos $[\![M]\!]$ sin especificar una valuación.

Recordamos que definimos la relación de β-equivalencia para poder realizar cálculos (evaluaciones) con los términos. Es importante que los modelos respeten esos cálculos, es decir que si $M \equiv_\beta N$ entonces para toda valuación ρ tengamos que $[\![M[\rho]]\!] = [\![N[\rho]]\!]$. Como en nuestro sistema de deducción tenemos la regla de β-equivalencia, que nos permite intercambiar fórmulas β-equivalentes, es de esperar que si nuestros modelos no respetaran la β-equivalencia, tampoco respetarían las derivaciones. De hecho, en el teorema 3.3.10 probaremos la corrección de los modelos y para eso necesitaremos esta propiedad. Como la relación de β-equivalencia se define como la clausura reflexiva-simétrico-transitiva de la β-reducción en una etapa, alcanza con probar que si dos términos M y M' están relacionados por la β-reducción en una etapa (con la notación que introducimos, $M \to_\beta M'$), entonces para cualquier valuación ρ se cumple $[\![M[\rho]]\!] = [\![M'[\rho]]\!]$. Probaremos eso en el teorema 3.3.6, pero antes vamos a demostrar un lema de sustitutividad que será necesario.

Lema 3.3.5. *Para cada término M, cada variable $x : \tau$, cada término $N : \tau$ y cada valuación ρ, se cumple:*

$$[\![M[x := N][\rho]]\!] = [\![M[\rho, x \leftarrow [\![N[\rho]]\!]]]\!]$$

Demostración. Lo probamos por inducción en M.

Caso $M \equiv y$**:** Si $y \not\equiv x$ entonces ambos dan $\rho(y)$ y si $y \equiv x$ ambos dan $[\![N[\rho]]\!]$.

Caso $M \equiv c$**:** En este caso ambos dan $c^{\mathcal{B}}$.

Caso $M \equiv M_1 M_2$**:**

$$\begin{aligned}
[\![M_1 M_2[\rho, x \leftarrow [\![N[\rho]]\!]]]\!] &= [\![M_1[\rho, x \leftarrow [\![N[\rho]]\!]]]\!]([\![M_2[\rho, x \leftarrow [\![N[\rho]]\!]]]\!]) \\
[\![M_1 M_2[x := N][\rho]]\!] &= [\![(M_1[x := N])(M_2[x := N])[\rho]]\!] \\
&= [\![M_1[x := N][\rho]]\!]([\![M_2[x := N][\rho]]\!])
\end{aligned}$$

Por hipótesis de inducción son iguales.

Caso $M \equiv \lambda y^\sigma.\, M_1$**:** Si $y \equiv x$, entonces:

$$\begin{aligned}
[\![\lambda y^\sigma.\, M_1[\rho, y \leftarrow [\![N[\rho]]\!]]]\!](a) &= [\![M_1[\rho, y \leftarrow a]]\!] \\
[\![\lambda y^\sigma.\, M_1[y := N][\rho]]\!](a) &= [\![\lambda y^\sigma.\, M_1[\rho]]\!](a) = [\![M_1[\rho, y \leftarrow a]]\!]
\end{aligned}$$

Básicamente las sustituciones no tienen efecto y en ambos casos da lo mismo. Supongamos ahora que $y \not\equiv x$. Por la α-equivalencia podemos suponer que $y \notin \mathrm{FV}(N)$ (en otro caso, remplazamos y por una variable que no aparezca en N ni en M_1).

$$\begin{aligned}
[\![\lambda y^\sigma.\, M_1[x := N][\rho]]\!](a) &= [\![M_1[x := N][\rho, y \leftarrow a]]\!] \\
&= [\![M_1[\rho, y \leftarrow a, x \leftarrow [\![N[\rho, y \leftarrow a]]\!]]]\!] \\
&= [\![M_1[\rho, y \leftarrow a, x \leftarrow [\![N[\rho]]\!]]]\!] \\
&= [\![M_1[\rho, x \leftarrow [\![N[\rho]]\!], y \leftarrow a]]\!] \\
&= [\![\lambda y^\sigma.\, M_1[\rho, x \leftarrow [\![N[\rho]]\!]]]\!](a)
\end{aligned}$$

La segunda igualdad es por la hipótesis de inducción con la valuación $(\rho, y \leftarrow a)$ y la tercera es porque $y \notin \mathrm{FV}(N)$. □

Teorema 3.3.6. *Si $M \to_\beta M'$ entonces para cualquier valuación ρ, $[\![M[\rho]]\!] = [\![M'[\rho]]\!]$. Consecuentemente, también se cumple si $M \equiv_\beta M'$.*

Demostración. Definimos la relación de β-reducción en una etapa como la clausura contextual de la β-reducción. De forma precisa, se trata de la siguiente definición recursiva:

1. $(\lambda x^\tau.\, M)N \to_\beta M[x := N]$
2. Si $M \to_\beta M'$ entonces $MN \to_\beta M'N$
3. Si $N \to_\beta N'$ entonces $MN \to_\beta MN'$
4. Si $M \to_\beta M'$ entonces $\lambda x^\tau.\, M \to_\beta \lambda x^\tau.\, M'$

Probamos la tesis por inducción en esta definición recursiva. Los casos 2,3 y 4 se deducen directamente de la hipótesis inductiva. Veamos el caso 1.

Tenemos que $[\![(\lambda x^\tau.\, M)N[\rho]]\!] = [\![\lambda x^\tau.\, M[\rho]]\!]([\![N[\rho]]\!]) = [\![M[\rho, x \leftarrow [\![N[\rho]]\!]]]\!]$, por lo que hay que probar que $[\![M[\rho, x \leftarrow [\![N[\rho]]\!]]]\!] = [\![M[x := N][\rho]]\!]$, pero esto es exactamente lo que acabamos de probar en el lema 3.3.5. □

3.3.2. Interpretación de las construcciones lógicas

Para tener definido un modelo debemos fijar son las interpretaciones de los tipos de base y las constantes. Para el tipo `Prop` y las constantes lógicas se usan siempre las mismias interpretaciones (se deben tomar decisiones al agregar nuevos tipos o constantes). En el caso del tipo `Prop`, usamos el álgebra booleana $(B, \leftrightarrow)$, dada como ejemplo en la sección 2.2, para la constante $\Rightarrow$ usamos la implicación y para las constantes $\forall^\tau$ usamos ínfimos. De forma precisa:

$$[\![\texttt{Prop}]\!] = B \qquad [\![\Rightarrow]\!](a)(b) = a \to b$$
$$a \sim_{\texttt{Prop}} b = a \leftrightarrow b \qquad [\![\forall^\tau]\!](f) = \bigwedge_{a \in [\![\tau]\!]} f(a)$$

Cada vez que se define la interpretación de un tipo de base hay que verificar que la B-equivalencia cumple las propiedades reflexividad, simetría y transitividad. Por otra parte, cuando se define la interpretación de una constante hay que verificar que está en el B-conjunto asociado al tipo correspondiente.

Lema 3.3.7. *Se cumple que $\sim_{\texttt{Prop}}$ es una B-equivalencia, $[\![\Rightarrow]\!] \in [\![\texttt{Prop} \to \texttt{Prop} \to \texttt{Prop}]\!]$ y para cada tipo τ, $[\![\forall^\tau]\!] \in [\![(\tau \to \texttt{Prop}) \to \texttt{Prop}]\!]$.*

Demostración. En el capítulo 2 vimos que $(B, \leftrightarrow)$ es un B-conjunto. En lo siguiente será importante tener presentes los lemas 1.1.2 y 1,1,3.

Dado $a \in B$, $\Rightarrow_a \colon B \to B$ definido como $\Rightarrow_a (b) = a \to b$ está en $[\![\texttt{Prop} \to \texttt{Prop}]\!]$ pues para todos $b_1, b_2 \in B$ tenemos $b_1 \leftrightarrow b_2 \leq (a \to b_1) \leftrightarrow (a \to b_2)$. Lo que debemos probar es que dados $a_1, a_2 \in B$, tenemos $a_1 \leftrightarrow a_2 \leq \Rightarrow_{a_1} \sim_{\texttt{Prop} \to \texttt{Prop}} \Rightarrow_{a_2}$. Esto se cumple porque $\Rightarrow_{a_1} \sim_{\texttt{Prop} \to \texttt{Prop}} \Rightarrow_{a_2} = \bigwedge_{b \in B}((a_1 \to b) \leftrightarrow (a_2 \to b)) \geq \bigwedge_{b \in B}(a_1 \leftrightarrow a_2) = a_1 \leftrightarrow a_2$.

Veamos por último que la interpretación de $\forall^\tau$ es correcta. Hay que probar que dadas $f_1, f_2 \in [\![\tau \to \texttt{Prop}]\!]$, tenemos $f_1 \sim_{\tau \to \texttt{Prop}} f_2 \leq [\![\forall^\tau]\!](f_1) \leftrightarrow [\![\forall^\tau]\!](f_2)$. Esto es equivalente

a probar $f_1 \sim_{\tau\to\texttt{Prop}} f_2 \wedge [\![\forall^\tau]\!](f_1) \leq [\![\forall^\tau]\!](f_2)$ y $f_1 \sim_{\tau\to\texttt{Prop}} f_2 \wedge [\![\forall^\tau]\!](f_2) \leq [\![\forall^\tau]\!](f_1)$. Probaremos solo uno de los dos porque son análogos.

$$f_1 \sim_{\tau\to\texttt{Prop}} f_2 \wedge [\![\forall^\tau]\!](f_1) \leq [\![\forall^\tau]\!](f_2) \Leftrightarrow f_1 \sim_{\tau\to\texttt{Prop}} f_2 \wedge [\![\forall^\tau]\!](f_1) \leq \bigwedge_{b\in[\![\tau]\!]} f_2(b)$$

Fijamos $b \in [\![\tau]\!]$ y debemos probar $f_1 \sim_{\tau\to\texttt{Prop}} f_2 \wedge [\![\forall^\tau]\!](f_1) \leq f_2(b)$. Razonamos así:

$$f_1 \sim_{\tau\to\texttt{Prop}} f_2 \wedge [\![\forall^\tau]\!](f_1) = \bigwedge_{a\in[\![\tau]\!]} (f_1(a) \leftrightarrow f_2(a)) \wedge \bigwedge_{a\in[\![\tau]\!]} f_1(a) \leq (f_1(b) \leftrightarrow f_2(b)) \wedge f_1(b)$$

Finalmente, por propiedades de álgebras booleanas $(f_1(b) \leftrightarrow f_2(b)) \wedge f_1(b) \leq f_2(b)$. Acabamos de probar que $f_1 \sim_{\tau\to\texttt{Prop}} f_2 \wedge [\![\forall^\tau]\!](f_1) \leq f_2(b)$. Como esto es para cualquier $b \in [\![\tau]\!]$, tenemos que $f_1 \sim_{\tau\to\texttt{Prop}} f_2 \wedge [\![\forall^\tau]\!](f_1) \leq \bigwedge_{b\in[\![\tau]\!]} f_2(b)$, como debíamos probar. □

Se demuestra que las otras construcciones lógicas definidas se interpretan de la siguiente forma.

Teorema 3.3.8. *Para todas proposiciones ϕ y ψ y para cualquier valuación ρ se cumple:*

$$\begin{aligned}
[\![\top[\rho]]\!] &= 1 & [\![\bot[\rho]]\!] &= 0\\
[\![\phi \wedge \psi[\rho]]\!] &= [\![\phi[\rho]]\!] \wedge [\![\psi[\rho]]\!] & [\![\phi \vee \psi[\rho]]\!] &= [\![\phi[\rho]]\!] \vee [\![\psi[\rho]]\!]\\
[\![\phi \to \psi[\rho]]\!] &= [\![\phi[\rho]]\!] \to [\![\psi[\rho]]\!] & [\![\neg\phi[\rho]]\!] &= [\![\phi[\rho]]\!]^*\\
[\![\forall x^\tau.\phi[\rho]]\!] &= \bigwedge_{a\in[\![\tau]\!]} [\![\phi[\rho, x \leftarrow a]]\!] & [\![\exists x^\tau.\phi[\rho]]\!] &= \bigvee_{a\in[\![\tau]\!]} [\![\phi[\rho, x \leftarrow a]]\!]
\end{aligned}$$

Por otra parte, si M y N son términos de tipo τ, entonces se cumple:

$$[\![M =_\tau N[\rho]]\!] = [\![M[\rho]]\!] \sim_\tau [\![N[\rho]]\!]$$

Demostración. Probamos la última parte, respecto a la interpretación de la igualdad de Leibnitz. Por definición tenemos:

$$[\![M =_\tau N[\rho]]\!] = \bigwedge_{f\in[\![\tau\to\texttt{Prop}]\!]} (f([\![M[\rho]]\!]) \to f([\![N[\rho]]\!]))$$

Como $f \in [\![\tau \to \texttt{Prop}]\!]$, tenemos que $[\![M[\rho]]\!] \sim_\tau [\![N[\rho]]\!] \leq f([\![M[\rho]]\!]) \sim_{\texttt{Prop}} f([\![N[\rho]]\!])$ y como $\sim_{\texttt{Prop}}$ es la equivalencia lógica, $[\![M[\rho]]\!] \sim_\tau [\![N[\rho]]\!] \leq f([\![M[\rho]]\!]) \to f([\![N[\rho]]\!])$. Esto implica que $[\![M[\rho]]\!] \sim_\tau [\![N[\rho]]\!] \leq [\![M =_\tau N[\rho]]\!]$. La otra desigualdad se deduce de considerar $f \in [\![\tau \to \texttt{Prop}]\!]$ definida como $f(a) = [\![M[\rho]]\!] \sim_\tau a$. Con esta función se cumple $f([\![M[\rho]]\!]) \to f([\![N[\rho]]\!]) = [\![M[\rho]]\!] \sim_\tau [\![N[\rho]]\!]$. Que $f \in [\![\tau \to \texttt{Prop}]\!]$ se verifica viendo que para cualquier $a, b \in [\![\tau]\!]$ se cumple $a \sim_\tau b \leq [\![M[\rho]]\!] \sim_\tau a \leftrightarrow [\![M[\rho]]\!] \sim_\tau b$, lo cual es cierto por transitividad de $\sim_\tau$. □

En ocasiones realizaremos un abuso del lenguaje, mediante el cual dada una fórmula ϕ con variables libres entre $x_1^{\tau_1}, \ldots, x_n^{\tau_n}$ y dados $a_1 \in [\![\tau_1]\!], \ldots, a_n \in [\![\tau_n]\!]$ denotaremos:

$$[\![\phi(a_1, \ldots, a_n)]\!] := [\![\phi[\rho, x_1^{\tau_1} \leftarrow a_1, \ldots, x_n^{\tau_n} \leftarrow a_n]]\!]$$

Con ρ cualquier valuación (la interpretación solamente depende del valor de la valuación en las variables libres). En estos casos escribiremos la fórmula ϕ como $\phi(x_1, \ldots, x_n)$.

Pasamos ahora a tratar la validez de fórmulas y el teorema de corrección, que nos dice que las interpretaciones de fórmulas respetan las derivaciones en HOL. Comenzamos con la definición de fórmula válida, la cual no es sorprendente.

Definición 3.3.9. Dada una interpretación de HOL en la categoría B-Set, decimos que una fórmula cerrada ϕ es válida o que se cumple si $[\![\phi]\!] = 1$.

La corrección está dada por el siguiente teorema. Para cada contexto Γ y cada valuación ρ definimos $[\![\Gamma[\rho]]\!] = \bigwedge_{\phi\in\Gamma}[\![\phi[\rho]]\!]$.

Teorema 3.3.10. *Si $\Gamma \vdash \phi$ entonces para cualquier valuación ρ, $[\![\Gamma[\rho]]\!] \leq [\![\phi[\rho]]\!]$.*

Demostración. Por inducción en la derivación de $\Gamma \vdash \phi$. Recordamos las reglas:

$$\frac{}{\Gamma \vdash \phi}\ (\text{si } \phi \in \Gamma) \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash \phi'}\ (\text{si } \phi \equiv_\beta \phi') \qquad \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi} \qquad \frac{\Gamma \vdash \phi \Rightarrow \psi \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \forall x^\tau.\, \phi}\ (\text{si } x^\tau \notin \mathrm{FV}(\Gamma)) \qquad \frac{\Gamma \vdash \forall x^\tau.\, \phi}{\Gamma \vdash \phi[x := M]}\ (M : \tau) \qquad \frac{}{\Gamma \vdash ((\phi \Rightarrow \psi) \Rightarrow \phi) \Rightarrow \phi}$$

Regla axioma: Si $\phi \in \Gamma$ entonces se cumple la desigualdad por definición.

Regla β: Como consecuencia del teorema 3.3.6, tenemos que $[\![\phi[\rho]]\!] = [\![\phi'[\rho]]\!]$. Por lo tanto se deduce de la hipótesis inductiva.

Regla de introducción de $\Rightarrow$: Tenemos que $[\![\Gamma[\rho]]\!] \wedge [\![\phi[\rho]]\!] \leq [\![\psi[\rho]]\!]$. Por el lema 1.1.2 eso es equivalente a que $[\![\Gamma[\rho]]\!] \leq [\![\phi[\rho]]\!] \to [\![\psi[\rho]]\!]$.

Regla de eliminación de $\Rightarrow$: Tenemos $[\![\Gamma[\rho]]\!] \leq [\![\phi[\rho]]\!] \to [\![\psi[\rho]]\!]$ y $[\![\Gamma[\rho]]\!] \leq [\![\phi[\rho]]\!]$. Por lo tanto, $[\![\Gamma[\rho]]\!] \leq ([\![\phi[\rho]]\!] \to [\![\psi[\rho]]\!]) \wedge [\![\phi[\rho]]\!] \leq [\![\psi[\rho]]\!]$.

Regla de introducción de $\forall$: Que se cumpla $[\![\Gamma[\rho]]\!] \leq [\![\forall x^\tau.\, \phi[\rho]]\!]$ es equivalente a que para todo $a \in [\![\tau]\!]$ tengamos que $[\![\Gamma[\rho]]\!] \leq [\![\phi[\rho, x \leftarrow a]]\!]$, por el teorema 3.3.8. Por hipótesis inductiva, $[\![\Gamma[\rho']]\!] \leq [\![\phi[\rho']]\!]$ para cualquier valuación ρ', por lo que en particular se cumple para $(\rho, x \leftarrow a)$. Finalmente, como $x \notin \mathrm{FV}(\Gamma)$, tenemos que $[\![\Gamma[\rho]]\!] = [\![\Gamma[\rho, x \leftarrow a]]\!]$, con lo que concluimos $[\![\Gamma[\rho]]\!] \leq [\![\phi[\rho, x \leftarrow a]]\!]$.

Regla de eliminación de $\forall$: Por hipótesis tenemos que para todo $a \in [\![\tau]\!]$ se cumple que $[\![\Gamma[\rho]]\!] \leq [\![\phi[\rho, x \leftarrow a]]\!]$. En particular, $[\![\Gamma[\rho]]\!] \leq [\![\phi[\rho, x \leftarrow [\![M[\rho]]\!]]]\!]$. Finalmente usamos que $[\![\phi[x := M][\rho]]\!] = [\![\phi[\rho, x \leftarrow [\![M[\rho]]\!]]]\!]$, lo cual se probó en el lema 3.3.5.

Ley de Peirce: Se cumple en cualquier álgebra Booleana (la interpretación de la tesis del secuente siempre es 1). □

3.3.3. Propiedades

Debido al teorema 3.3.10, sabemos que toda fórmula ϕ derivable en HOL es válida en cualquier modelo booleano de HOL. Sin embargo, en la sección 3.2 vimos fórmulas que no son derivables en HOL pero que queremos agregar como axiomas. Se trata de las siguientes.

- $\mathtt{ExtFun}_{\tau,\sigma} :\equiv \forall f, g^{\tau\to\sigma}.\, (\forall x^\tau.\, fx =_\sigma gx) \Rightarrow f =_{\tau\to\sigma} g$ para todos tipos τ, σ.
- $\mathtt{ExtProp} :\equiv \forall x, y^{\mathtt{Prop}}.\, (x \Leftrightarrow y) \Rightarrow x =_{\mathtt{Prop}} y$.
- $\mathtt{ExtPred}_\tau :\equiv \forall P, Q^{\tau\to\mathtt{Prop}}.\, (\forall x^\tau.\, Px \Leftrightarrow Qx) \Rightarrow P =_{\tau\to\mathtt{Prop}} Q$ para todo tipo τ.
- $\mathtt{AC}_{\tau,\sigma} :\equiv \forall S^{\tau\to\sigma\to\mathtt{Prop}}.\, \forall x^\tau \exists y^\sigma Sxy \Rightarrow \exists f^{\tau\to\sigma} \forall x^\tau Sx(fx)$ para todos tipos τ, σ.
- $\mathtt{Bival} :\equiv \forall x^{\mathtt{Prop}}.\, x =_{\mathtt{Prop}} \bot \vee x =_{\mathtt{Prop}} \top$.

Recordamos que en particular la extensionalidad de predicados es crucial en nuestro contexto, ya que queremos usar el tipo $\tau \to \texttt{Prop}$ para trabajar con conjuntos de elementos de tipo τ. Mencionamos que en la categoría Set esta propiedad no es válida, motivo por el cual descartamos esos modelos. Veamos ahora que en B-Set todas estas propiedades, salvo por ahora el axioma de elección, son válidas.

Teorema 3.3.11. *En los modelos de HOL sobre la categoría B-Set son válidas:*

- $\texttt{ExtFun}_{\tau,\sigma}$ *para todo par de tipos* τ, σ.
- $\texttt{ExtProp}$.
- $\texttt{ExtPred}_\tau$ *para todo tipo* τ.
- $\texttt{Bival}$.

Demostración. Comencemos con la extensionalidad funcional. Tenemos que demostrar que $[\![\forall f, g^{\tau\to\sigma}. \forall x^\tau (fx =_\sigma gx) \Rightarrow f =_{\tau\to\sigma} g]\!] = 1$. Por el teorema 3.3.8, la interpretación vale:

$$\bigwedge_{f,g\in[\![\tau\to\sigma]\!]} \left(\bigwedge_{a\in[\![\tau]\!]} f(a) \sim_\sigma g(a) \;\to\; f \sim_{\tau\to\sigma} g \right)$$

Por definición, $f \sim_{\tau\to\sigma} g = \bigwedge_{a\in[\![\tau]\!]} f(a) \sim_\sigma g(a)$, por lo que para todas $f, g \in [\![\tau \to \sigma]\!]$ se cumple $\bigwedge_{a\in[\![\tau]\!]} f(a) \sim_\sigma g(a) \;\to\; f \sim_{\tau\to\sigma} g = 1$. De esto deducimos que la interpretación de la extensionalidad funcional vale 1.

Veamos ahora que $[\![\forall x, y^{\texttt{Prop}}. (x \Leftrightarrow y) \Rightarrow x =_{\texttt{Prop}} y]\!] = 1$ ($\texttt{ExtProp}$). La interpretación vale:

$$\bigwedge_{a,b\in B} ((a \leftrightarrow b) \to a \sim_{\texttt{Prop}} b)$$

Tenemos que $a \sim_{\texttt{Prop}} b = a \leftrightarrow b$, lo cual análogamente a en el caso anterior implica que el resultado es 1.

Para $\texttt{ExtPred}_\tau$ y $\texttt{Bival}$ probaremos que en HOL son derivables a partir de las que ya vimos que son válidas. Por la corrección (teorema 3.3.10) esto implica que también son válidas. Específicamente, veremos lo siguiente:

$$\texttt{ExtFun}_{\tau,\texttt{Prop}}, \texttt{ExtProp} \vdash \texttt{ExtPred}_\tau \qquad \texttt{ExtProp} \vdash \texttt{Bival}$$

Veamos el primero. Sean $P, Q; \tau \to \texttt{Prop}$ tales que para todo $x : \tau$ se cumple $Px \Leftrightarrow Qx$. Por la extensionalidad proposicional tenemos que para todo $x : \tau$ se cumple $Px =_{\texttt{Prop}} Qx$. Aplicando la extensionalidad funcional con $f \equiv P$ y $g \equiv Q$ concluimos $P =_{\tau\to\texttt{Prop}} Q$.

Veamos el segundo. Sea $x : \texttt{Prop}$. Debemos probar $x =_{\texttt{Prop}} \bot \vee x =_{\texttt{Prop}} \top$. Razonamos utilizando el tercero excluido con x (podemos hacerlo porque tenemos la Ley de Peirce, que es equivalente). Tenemos que se cumple $x \vee \neg x$. Separamos en casos. Si se cumple x, tenemos que se cumple $x \Leftrightarrow \top$. Por extensionalidad proposicional concluimos $x =_{\texttt{Prop}} \top$. Por otra parte, si se cumple $\neg x$ tenemos que se cumple $x \Leftrightarrow \bot$. Por extensionalidad proposicional concluimos $x =_{\texttt{Prop}} \bot$. □

Algunos comentarios respecto al interés de que estas proposiciones sean válidas. Tener la extensionalidad funcional y la de predicados nos permite trabajar con funciones y conjuntos como lo hacemos usualmente. Por otra parte, a priori la bivalencia puede resultar extraña. Parece afirmar que el álgebra booleana sobre la que estamos trabajando es la trivial, en la que solamente tenemos 0 y 1. El hecho de que sea una fórmula válida con cualquier álgebra booleana B, intuitivamente nos dice que aunque en el modelo hayan muchos valores de verdad, la sintaxis "piensa" que solamente hay dos. Esto significa que las proposiciones que podamos demostrar en HOL asumiendo que los únicos valores de verdad son $\bot$ y $\top$, se van a cumplir para cualquier álgebra booleana.

Pasamos ahora a considerar el axioma de elección. Con este axioma lo que ocurre es que para que se cumpla necesitamos que las interpretaciones de los tipos sean B-conjuntos mezclables (noción introducida en la sección 2.2.3). Resultan haber otras propiedades útiles que se cumplen cuando los tipos son mezclables. Debido a esto, en lo que queda del capítulo nos concentraremos en aspectos vinculados a tipos con interpretaciones mezclables, concluyendo con el axioma de elección.

Caso de tipos con interpretaciones mezclables

Comenzamos con un corolario de las proposiciones de la sección 2.2.3, que nos asegura que en lógica de orden superior y sistemas extendidos con tipos de base con interpretaciones mezclables, todos los tipos se interpretan de forma mezclable.

Corolario 3.3.12. *Si todos los tipos de base tienen interpretación mezclable, entonces todos los tipos tienen interpretación mezclable. En particular, en HOL con único tipo de base* `Prop`*, todos los tipos son mezclables.*

Demostración. Se prueba por inducción usando la proposición 2.2.19. La segunda parte se deduce de la proposición 2.2.16. □

Veamos ahora las propiedades que obtenemos de que las interpretaciones de los tipos sean mezclables. Estas propiedades son justamente el motivo de haber introducido las mezclas en este trabajo. Comenzamos con un teorema que nos afirma que los supremos sobre predicados siempre son máximos (se alcanzan en un elemento).

Teorema 3.3.13 (Principio del máximo)**.** *Sea τ un tipo con interpretación mezclable y $\varphi \in [\![\tau \to \texttt{Prop}]\!]$. Entonces:*

$$\exists \hat{a} \in [\![\tau]\!] \quad \varphi(\hat{a}) = \bigvee_{a \in [\![\tau]\!]} \varphi(a)$$

Es decir, los supremos de predicados sobre tipos mezclables se alcanzan.

Demostración. Sea $\{a_\beta\}_{\beta<\rho}$ buen orden de $[\![\tau]\!]$. De este modo, $\bigvee_{a\in[\![\tau]\!]} \varphi(a) = \bigvee_{\alpha<\rho} \varphi(a_\alpha)$. Definimos una familia $(E_\beta)_{\beta<\rho}$ de elementos de B.

$$E_\beta = \varphi(a_\beta) - \bigvee_{\gamma<\beta} \varphi(a_\gamma) = \varphi(a_\beta) \wedge (\bigvee_{\gamma<\beta} \varphi(a_\gamma))^*$$

Veamos que $\{E_\beta \ / \ \beta < \rho\}$ es una anticadena. Si $\alpha < \beta$, entonces $E_\alpha \leq \varphi(a_\alpha)$. Por otra parte, $E_\beta \leq (\bigvee_{\gamma<\beta} \varphi(a_\gamma))^* = \bigwedge_{\gamma<\beta} \varphi(a_\gamma)^* \leq \varphi(a_\alpha)^*$. Por lo tanto, tenemos que

$E_\alpha \wedge E_\beta \leq \varphi(a_\alpha) \wedge \varphi(a_\alpha)^* = 0$. Vamos a usar esta anticadena para hacer una mezcla, pero antes veamos que $\bigvee_{\alpha<\rho} \varphi(a_\alpha) = \bigvee_{\alpha<\rho} E_\alpha$.

Probaremos por inducción en $\alpha < \rho$ que $\bigvee_{\beta\leq\alpha} \varphi(a_\beta) = \bigvee_{\beta\leq\alpha} E_\beta$.

$$\bigvee_{\beta\leq\alpha} E_\beta = \bigvee_{\beta<\alpha} E_\beta \vee E_\alpha = \bigvee_{\beta<\alpha} \bigvee_{\gamma\leq\beta} E_\gamma \vee \left(\varphi(a_\alpha) \wedge (\bigvee_{\beta<\alpha} \varphi(a_\beta))^*\right)$$

Por hipótesis inductiva, para cada $\beta < \alpha$ tenemos $\bigvee_{\gamma\leq\beta} E_\gamma = \bigvee_{\gamma\leq\beta} \varphi(a_\gamma)$. Por lo tanto, $\bigvee_{\beta<\alpha} \bigvee_{\gamma\leq\beta} E_\gamma = \bigvee_{\beta<\alpha} \varphi(a_\beta)$. Concluimos como sigue.

$$\bigvee_{\beta<\alpha} \varphi(a_\beta) \vee \left(\varphi(a_\alpha) \wedge (\bigvee_{\beta<\alpha} \varphi(a_\beta))^*\right) = (\bigvee_{\beta<\alpha} \varphi(a_\beta) \vee \varphi(a_\alpha)) \wedge (\bigvee_{\beta<\alpha} \varphi(a_\beta) \vee (\bigvee_{\beta<\alpha} \varphi(a_\beta))^*)$$

Esto último es igual a $\bigvee_{\beta\leq\alpha} \varphi(a_\beta)$. Terminamos de probar que $\bigvee_{\beta\leq\alpha} \varphi(a_\beta) = \bigvee_{\beta\leq\alpha} E_\beta$. Resta probar que $\bigvee_{\alpha<\rho} \varphi(a_\alpha) = \bigvee_{\alpha<\rho} E_\alpha$. Es por lo siguiente:

$$\bigvee_{\alpha<\rho} E_\alpha = \bigvee_{\alpha<\rho} \bigvee_{\gamma\leq\alpha} E_\gamma = \bigvee_{\alpha<\rho} \bigvee_{\gamma\leq\alpha} \varphi(a_\gamma) = \bigvee_{\alpha<\rho} \varphi(a_\alpha)$$

Sea $\hat{a} = \sum_{\beta<\rho} E_\beta \cdot a_\beta$. Notar que pueden haber distintos β para los que $E_\beta = 0$, no obstante, tomando cualquiera de ellos existe una mezcla y cumple la desigualdad con todos (porque para los otros β tales que $E_\beta = 0$ se cumple trivialmente), es decir para cada $\alpha < \rho$ se cumple $\hat{a} \sim a_\beta \geq E_\beta$. Observemos que dado $\beta < \rho$:

$$\varphi(\hat{a}) \geq \varphi(a_\beta) \wedge a_\beta \sim_\tau \hat{a} \geq \varphi(a_\beta) \wedge E_\beta = E_\beta$$

Tomando supremo en $\beta < \rho$ concluimos $\varphi(\hat{a}) \geq \bigvee_{\beta<\rho} E_\beta = \bigvee_{\beta<\rho} \varphi(a_\beta) = \bigvee_{a\in[\![\tau]\!]} \varphi(a)$. □

Corolario 3.3.14. *Si todos los tipos son mezclables, para cualquier fórmula $\exists x^\tau.\, \phi$ y cualquier valuación ρ, existe $a \in [\![\tau]\!]$ tal que $[\![\phi[\rho, x \leftarrow a]]\!] = [\![\exists x^\tau.\, \phi[\rho]]\!]$.*

Las mezclas también permiten simplificar cálculos de valor de verdad de implicaciones con cuantificaciones universales. La idea central está en el siguiente lema, que será útil para calcular ínfimos de flechas.

Lema 3.3.15. *Sea τ un tipo mezclable y sean $f, g \in [\![\tau \to \texttt{Prop}]\!]$. Supongamos que existe $a_0 \in [\![\tau]\!]$ tal que $f(a_0) = 1$. Entonces para todo $a \in [\![\tau]\!]$ existe $b \in [\![\tau]\!]$ tal que $f(b) = 1$ y $f(a) \to g(a) \geq g(b)$ $(= f(b) \to g(b))$.*

Demostración. Sea $x = f(a)$. Mezclamos a con a_0 utilizando x y x^* como coeficientes, es decir definimos $b := x \cdot a + x^* \cdot a_0$. Veamos que b cumple lo requerido.

Primero veamos que $f(b) = 1$. Por una parte, $f(b) \geq f(a) \wedge a \sim_\tau b \geq f(a) \wedge x = x$. Por otra parte $f(b) \geq f(a_0) \wedge a_0 \sim_\tau b \geq f(a_0) \wedge x^* = x^*$. Por lo tanto, $f(b) \geq x \vee x^* = 1$.

Veamos ahora que $f(a) \to g(a) \geq g(b)$. Esto equivale a $f(a) \wedge g(b) \leq g(a)$. Esto es porque $f(a) \wedge g(b) = x \wedge g(b) \leq a \sim b \wedge g(b) \leq g(a)$. □

Corolario 3.3.16. *Sea τ un tipo mezclable y sean $f, g \in [\![\tau \to \texttt{Prop}]\!]$. Supongamos que existe $a_0 \in [\![\tau]\!]$ tal que $f(a_0) = 1$. Entonces:*

$$\bigwedge_{a \in [\![\tau]\!]} (f(a) \to g(a)) = \bigwedge_{a \in [\![\tau]\!], f(a)=1} g(a)$$

Corolario 3.3.17. *Sean x^τ una variable y $\phi(x^\tau), \psi(x^\tau) : \texttt{Prop}$ dos proposiciones que pueden tener solamente la variable x^τ libre. Supongamos que la interpretación de τ es mezclable y que existe $a_0 \in [\![\tau]\!]$ tal que $[\![\phi(a_0)]\!] = 1$. Entonces $\forall x^\tau.\, \phi(x) \Rightarrow \psi(x)$ es válido si y solo si $[\![\psi(a)]\!] = 1$ para cada $a \in [\![\tau]\!]$ tal que $[\![\phi(a)]\!] = 1$.*

Demostración. Tenemos que $[\![\forall x^\tau.\, \phi(x) \Rightarrow \psi(x)]\!]$ vale:

$$\bigwedge_{a \in [\![\tau]\!]} ([\![\phi(a)]\!] \to [\![\psi(a)]\!]) = \bigwedge_{a \in [\![\tau]\!]} (f(a) \to g(a))$$

Con $f, g : [\![\tau]\!] \to \texttt{Prop}$ definidas con $f(a) = [\![\phi(a)]\!]$ y $f(a) = [\![\psi(a)]\!]$. Tomando como ejemplo $[\![\phi(a)]\!]$, recordamos que esto significa $[\![\phi[\rho, x \leftarrow a]]\!]$ con ρ cualquier valuación (no depende de ρ porque no hay variables libres que no sean x). En base al corolario anterior, alcanza verificar que $f, g \in [\![\tau \to \texttt{Prop}]\!]$. Veámoslo solamente para f, pues para g es análogo. Que $f \in [\![\tau \to \texttt{Prop}]\!]$ se deduce de que $f = [\![\lambda x^\tau.\, \phi(x)]\!]$. Tenemos que $[\![\lambda x^\tau.\, \phi(x)]\!] \in [\![\tau \to \texttt{Prop}]\!]$ porque $\lambda x^\tau.\, \phi(x) : \tau \to \texttt{Prop}$. Veamos que se cumple la igualdad. Sea $a \in [\![\tau]\!]$. Tenemos $[\![\lambda x^\tau.\, \phi(x)]\!](a) = [\![\phi[\rho, x \leftarrow a]]\!] = [\![\phi(a)]\!] = f(a)$, donde ρ es cualquier valuación. □

Este último resultado simplifica mucho varias pruebas de validez de fórmulas. Es más sencillo probar que $[\![\phi(a)]\!] = 1$ para todo a tal que $\phi(a) = 1$ que probar que para todo $a \in [\![\tau]\!]$ se cumple $[\![\phi(a)]\!] \to [\![\psi(a)]\!] = 1$. Vamos a aplicarlo ahora para probar la validez del axioma de elección con tipos con interpretación mezclable y en el capítulo siguiente para probar la validez del axioma de completitud (dos pruebas que tal vez sean las más elaboradas de este trabajo).

Teorema 3.3.18 (Axioma de elección)**.** *Para cualquier par de tipos τ, σ, si $([\![\sigma]\!], \sim_\sigma)$ es mezclable entonces se cumple el axioma de elección de τ a σ:*

$$\forall S^{\tau \to \sigma \to \texttt{Prop}}.\ \forall x^\tau \exists y^\sigma Sxy \Rightarrow \exists f^{\tau \to \sigma} \forall x^\tau Sx(fx)$$

Demostración. El axioma de elección es de la forma $\forall S^{\tau \to \sigma \to \texttt{Prop}}.\phi(S) \Rightarrow \psi(S)$. Notamos que con $f_0 \in [\![\tau \to \sigma \to \texttt{Prop}]\!]$ siendo la función constante 1, se cumple $[\![\phi(f_0)]\!] = 1$. Por lo tanto, por el corolario 3.3.17, podemos asumir que el antecedente de la implicación es válido y demostrar que el consecuente también lo es.

Sea $A \in [\![\tau \to \sigma \to \texttt{Prop}]\!]$ tal que para cualquier $a \in [\![\tau]\!]$:

$$\bigvee_{b \in [\![\sigma]\!]} A(a, b) = 1$$

Esto es equivalente a que $[\![\forall x^\tau \exists y^\sigma Axy]\!] = 1$. Debemos probar $[\![\exists f^{\tau \to \sigma} \forall x^\tau Ax(fx)]\!] = 1$. Por definición esto es:

$$\bigvee_{\psi \in [\![\tau \to \sigma]\!]} \bigwedge_{a \in [\![\tau]\!]} A(a, \psi(a)) = 1$$

Lo probaremos construyendo $\varphi \in [\![\tau \to \sigma]\!]$ tal que para todo $a \in [\![\tau]\!]$, se cumple $A(a, \varphi(a)) = 1$ (es decir, $\bigwedge_{a \in [\![\tau]\!]} A(a, \phi(a)) = 1$).

Consideramos una buena ordenación $\{b_\beta\}_{\beta<\rho} = [\![\sigma]\!]$, con la cual definimos:

$$E^a_\beta = A(a, b_\beta) - \bigvee_{\gamma<\beta} A(a, b_\gamma)$$

Para cada $a \in [\![\tau]\!]$, la familia $\{E^a_\beta\}_{\beta<\rho}$ es una partición de la unidad (es anticadena y tiene el mismo supremo que $A(a, \_)$, que es 1; ver prueba del teorema 3.3.13). Utilizando mezclas definimos $\varphi : [\![\tau]\!] \to [\![\sigma]\!]$:

$$\varphi(a) = \sum_{x \in X} E^a_{\beta_x} \cdot b_{\beta_n}$$

Donde $\{\beta_x\}_{x \in X}$ son los índices para los que $E^a_\beta \neq 0$. Usando la propiedad de las mezclas y que para los otros $E^a_\beta = 0$, tenemos que para todo $\beta < \rho$:

$$E^a_\beta \leq \varphi(a) \sim_\sigma b_\beta$$

Debemos probar que $\varphi \in [\![\tau \to \sigma]\!]$. Antes vamos a probar que para todos $a_1, a_2 \in [\![\tau]\!]$ y para todo $\beta < \rho$ se cumple $a_1 \sim_\tau a_2 \leq E^{a_1}_\beta \leftrightarrow E^{a_2}_\beta$. Como $A \in [\![\tau \to (\sigma \to \texttt{Prop})]\!]$, para todo β se cumple $a_1 \sim_\tau a_2 \leq A(a_1, b_\beta) \leftrightarrow A(a_2, b_\beta)$. Para deducir lo que queremos probar utilizamos las dos siguientes propiedades.

- Para todos $a_1, b_1, a_2, b_2 \in B$ se cumple $(a_1 - b_1) \leftrightarrow (a_2 - b_2) \geq (a_1 \leftrightarrow a_2) \wedge (b_1 \leftrightarrow b_2)$.
- $(\bigvee_{\gamma<\beta} A(a_1, \xi_\gamma)) \leftrightarrow (\bigvee_{\gamma<\beta} A(a_2, \xi_\gamma)) \geq \bigwedge_{\gamma<\beta} (A(a_1, \xi_\gamma) \leftrightarrow A(a_2, \xi_\gamma))$.

Razonamos de la siguiente forma.

$$\begin{aligned}
E^{a_1}_\beta \leftrightarrow E^{a_2}_\beta &= (A(a_1, b_\beta) - \bigvee_{\gamma<\beta} A(a_1, b_\gamma)) \leftrightarrow (A(a_2, b_\beta) - \bigvee_{\gamma<\beta} A(a_2, b_\gamma)) \\
&\geq (A(a_1, b_\beta) \leftrightarrow A(a_2, b_\beta)) \wedge (\bigvee_{\gamma<\beta} A(a_1, b_\gamma) \leftrightarrow \bigvee_{\gamma<\beta} A(a_2, b_\gamma)) \\
&\geq (A(a_1, b_\beta) \leftrightarrow A(a_2, b_\beta)) \wedge (\bigwedge_{\gamma<\beta} (A(a_1, b_\gamma) \leftrightarrow A(a_2, b_\gamma))) \\
&\geq (a_1 \sim_\tau a_2) \wedge (\bigwedge_{\gamma<\beta} (a_1 \sim_\tau a_2)) = a_1 \sim_\tau a_2
\end{aligned}$$

Por lo tanto, para todos $a_1, a_2 \in [\![\tau]\!]$ y para todo $\beta < \rho$ se cumple $a_1 \sim_\tau a_2 \leq E^{a_1}_\beta \leftrightarrow E^{a_2}_\beta$, como queríamos probar. Utilizando eso realizamos el siguiente razonamiento. Sea $\beta < \rho$:

$$a_1 \sim_\tau a_2 \wedge E^{a_1}_\beta \leq E^{a_1}_\beta \wedge E^{a_2}_\beta \leq \varphi(a_1) \sim_\sigma b_\beta \wedge \varphi(a_2) \sim_\sigma b_\beta \leq \varphi(a_1) \sim_\sigma \varphi(a_2)$$

Por lo tanto, para cualquier $\beta < \rho$ tenemos $a_1 \sim_\tau a_2 \wedge E^{a_1}_\beta \leq \varphi(a_1) \sim_\sigma \varphi(a_2)$. Tomando supremo en $\beta < \rho$ y usando que $\{E^{a_1}_\beta\}_{\beta<\rho}$ es una partición de la unidad, concluimos la desigualdad y por ende que $\varphi \in [\![\tau \to \sigma]\!]$. Finalizamos probando que para todo $a \in [\![\tau]\!]$, tenemos $A(a, \varphi(a)) = 1$. Razonamos de forma análoga a lo anterior, tomando $\beta < \rho$:

$$E^a_\beta = E^a_\beta \wedge \varphi(a) \sim_\sigma b_\beta \leq A(a, b_\beta) \wedge \varphi(a) \sim_\sigma b_\beta \leq A(a, \varphi(a))$$

Donde en para la última desigualdad usamos que $A(a, \_) \in [\![\sigma \to \texttt{Prop}]\!]$. Nuevamente, tomando supremo en $\beta < \rho$ y usando que los E^a_β conforman una partición de la unidad, concluimos. □

El axioma de elección es útil para construir funciones desde la sintaxis. En HOL sin axiomas no podemos asegurar la existencia de muchas funciones que con el axioma de elección sí podemos construir.

Concluimos el estudio de las cinco fórmulas presentadas al comienzo de la sección 3.3.3 con una tabla que para cada propiedad indica si se cumple o no en interpretaciones con las categorías Set y B-Set. A los resutlados sobre las interpretaciones en Set los mostramos sin demostrar, mientras que para la categoría B-Set, en este punto ya demostramos todo lo que dice en a tabla. El la siguiente tabla, el «Sí» indica que el correspondiente axioma se cumple para cualquier álgebra booleana completa B y cualquier interpretación de los tipos de base.

	Set	B-Set
ExtFun	Sí	Sí
ExtProp	Solo con $B = 2$	Sí
ExtPred	Solo con $B = 2$	Sí
AC	Sí	Con tipos interpretados mezclables
Bivalencia	Solo con $B = 2$	Sí

Capítulo 4

Teoría de los reales aleatorios de orden superior

El objetivo de este capítulo es introducir un tipo de base R en HOL, e interpretarlo en nuestro modelo de tal modo que cumpla todos los axiomas del cuerpo de los números reales (ahora expresados en HOL). Cabe destacar que en el marco de nuestro modelo de HOL basado en los B-conjuntos, no se puede interpretar el tipo R por el conjunto $\mathbb{R}$ usual. En efecto, veremos más adelante que tal interpretación ingenua (la cual definiremos precisamente) cumple los axiomas de cuerpos ordenados (y más generalmente los axiomas de cuerpos reales cerrados), pero no cumple el axioma de completitud. Al contrario, vamos a usar el modelo de los reales aleatorios introducido por Scott [4](presentado en la sección 2.1), adaptado a nuestro marco de la lógica de orden superior. Veremos finalmente que bajo condiciones adecuadas se cumple la negación de la hipótesis del continuo, con una prueba basada en intuiciones de probabilidad.

4.1. Sintaxis y semántica

A los tipos y constantes de la lógica de orden superior (presentados en el capítulo 3) se agrega un nuevo tipo de base R con símbolos de constante para las operaciones de cuerpo y para la desigualdad.

$$\begin{aligned} 0 &: R & \qquad 1 &: R \\ + &: R \to R \to R & \qquad \times &: R \to R \to R \\ \texttt{opp} &: R \to R & \qquad \texttt{inv} &: R \to R \end{aligned}$$

$$\leq : R \to R \to \texttt{Prop}$$

Usamos la convención de que $0^{-1} = 0$. Esto es por conveniencia, con el fin de poder usar $\texttt{inv} : R \to R$. No tendrá ningún efecto porque el axioma de inverso se aplicará solamente para reales no nulos: $\forall x^R.\, x \neq_R 0 \Rightarrow x \times \texttt{inv}(x) =_R 1$. El agregado de las constantes `opp` y `inv` permite quitar cuantificaciones de los axiomas de números reales, lo cual simplificará las pruebas de validez de estos axiomas.

Nos encaminamos ahora a definir las interpretaciones del nuevo tipo de base y las nuevas constantes (la semántica).

Una interpretación ingenua de R. Antes de introducir la interpretación que usaremos, comentamos la interpretación ingenua en la que R se interpreta con $\mathbb{R}$, la cual dijimos que no nos va a servir. Con interpretar R por $\mathbb{R}$ nos referimos a que $[\![R]\!] = (\mathbb{R}, \sim_D)$, donde $\sim_D$ es la B-equivalencia discreta, es decir:

$$x \sim_D y = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{si } x \neq y \end{cases}$$

Además, se interpretan las constantes de cuerpo con las operaciones correspondientes de $\mathbb{R}$ y la constante de orden con el orden de $\mathbb{R}$. Con esta interpretación son válidas todas las fórmulas que se cumplen en la metateoría que involucren solamente al tipo R y a tipos construidos con flechas a partir solamente de este ($R \to R$, $(R \to R) \to R$, $R \to (R \to R)$, etc). Esto es el caso por ejemplo con los axiomas de cuerpo totalmente ordenado y más aún, de cuerpo real cerrado (introducida en la sección 4.4). Los problemas comienzan a surgir cuando usamos tipos que contienen además al tipo de base `Prop`. Esto es el caso por ejemplo con el axioma de completitud, que para hablar de conjuntos de números reales utiliza el tipo $R \to$ `Prop`. Esta interpretación de R no aprovecha para nada la estructura del álgebra booleana B, de hecho es esencialmente como una interpretación en la categoría Set, ya que la B-equivalencia no relaciona ningún par de elementos distintos. De aquí proviene que surjan problemas al trabajar con fórmulas que contienen a R y a `Prop`, como en particular que no se cumpla el axioma de completitud. En la interpretación que usaremos nos aseguramos de que la estructura del álgebra booleana B se aproveche en las interpretaciones de R y las nuevas constantes. Además, la interpretación del tipo R será mezclable (notar que en esta interpretación ingenua no lo es), lo cual será muy útil para probar la validez del axioma de completitud.

Interpetación por los reales aleatorios. En la sección 1.2 vimos que a partir de un espacio de probabilidad $(\Omega, \mathcal{A}, \mu)$, cocientando $\mathcal{A}$ respecto al ideal de los conjuntos de medida nula obtenemos un álgebra booleana completa, $B = \mathcal{A}/[\mu = 0]$. Posteriormente, en la sección 2.1 presentamos el modelo de reales aleatorios de Scott, dentro del cual definimos el conjunto $\mathcal{R}$ de los reales aleatorios como:

$$\mathcal{R} = \{\xi : \Omega \to \mathbb{R} \ / \ \xi \text{ es medible}\}$$

Recordamos que esto significa que para todo $a \in \mathbb{R}$, se cumple $\xi^{-1}((-\infty, a)) \in \mathcal{A}$. Esta condición (junto con que $\mathcal{A}$ es una σ-álgebra) implica que todos los subconjuntos de Ω que vamos a utilizar en lo siguiente están en $\mathcal{A}$. Recordamos también que en la terminología de probabilidad, $\mathcal{R}$ es el conjunto de las variables aleatorias reales. Utilizando el álgebra booleana completa B y el conjunto de reales aleatorios $\mathcal{R}$, definiremos el modelo de los reales aleatorios de orden superior, el cual es un modelo sobre la categoría B-Set, de los introducidos en la sección 3.3.

Fijamos $(\Omega, \mathcal{A}, \mu)$ un espacio de probabilidad (lo cual a su vez define un conjunto $\mathcal{R}$

de reales aleatorios), fijamos $B = \mathcal{A}/[\mu = 0]$ y definimos las siguientes interpretaciones:

$$\begin{aligned}
[\![R]\!] &= \{\xi : \Omega \to \mathbb{R} \ / \ \xi \text{ es medible}\} \\
\xi \sim_R \eta &= \{\omega \in \Omega \ / \ \xi(\omega) = \eta(\omega)\}/[\mu = 0] \\
[\![0]\!](\omega) &= 0 \\
[\![1]\!](\omega) &= 1 \\
[\![+]\!](\xi)(\eta)(\omega) &= \xi(\omega) + \eta(\omega) \\
[\![\times]\!](\xi)(\eta)(\omega) &= \xi(\omega)\eta(\omega) \\
[\![\mathtt{opp}]\!](\xi)(\omega) &= -\xi(\omega) \\
[\![\mathtt{inv}]\!](\xi)(\omega) &= \xi(\omega)^{-1} \\
[\![\leq]\!](\xi)(\eta) &= \{\omega \in \Omega \ / \ \xi(\omega) \leq \eta(\omega)\}/[\mu = 0]
\end{aligned}$$

En palabras, la interpretación de R es el B-conjunto de los reales aleatorios, las constantes 0 y 1 se interpretan con variables aleatorias constantes, las operaciones binarias de cuerpo se interpretan aplicándolas punto a punto, el opuesto y el inverso también se interpretan aplicándose punto a punto (con la convención de que $0^{-1} = 0$) y el orden se interpreta tomando el conjunto de los $\omega \in \Omega$ para los que se cumple la relación (el cual como ξ y η son medibles está en $\mathcal{A}$) y cocientando para obtener un elemento de B. Veamos que estas interpretaciones son correctas, en el sentido de que $(\mathcal{R}, \sim_R)$ es un B-conjunto y para cada constante $c : \tau$ tenemos que $[\![c]\!] \in [\![\tau]\!]$.

Lema 4.1.1. *La interpretación de R es un B-conjunto y cada $c : \tau$ cumple $[\![c]\!] \in [\![\tau]\!]$.*

Demostración. Comenzamos comentando por qué $\sim_R$ es una B-equivalencia. La reflexividad y la simetría son claras. La transitividad se deduce de que para todos $A_1, A_2 \in \mathcal{A}$ se cumple $A_1/[\mu = 0] \wedge A_2/[\mu = 0] = (A_1 \cap A_2)/[\mu = 0]$.

Que $[\![0]\!] \in [\![R]\!]$ es porque las funciones constantes son medibles. Veamos que $[\![+]\!] \in [\![R \to R \to R]\!]$. Primero que nada, suma punto a punto de funciones medibles es medible. Dado $\xi \in \mathcal{R}$, hay que ver que $+_\xi \in [\![R \to R]\!]$. Sean $\eta_1, \eta_2 \in \mathcal{R}$.

$$\begin{aligned}
\eta_1 \sim_R \eta_2 &= \{\omega \in \Omega \ / \ \eta_1(\omega) = \eta_2(\omega)\}/[\mu = 0] \\
+_\xi(\eta_1) \sim_R +_\xi(\eta_2) &= \{\omega \in \Omega \ / \ \xi(\omega) + \eta_1(\omega) = \xi(\omega) + \eta_2(\omega)\}/[\mu = 0]
\end{aligned}$$

Como $\{\omega \in \Omega \ / \ \eta_1(\omega) = \eta_2(\omega)\} \subseteq \{\omega \in \Omega \ / \ \xi(\omega) + \eta_1(\omega) = \xi(\omega) + \eta_2(\omega)\}$ tenemos que $\eta_1 \sim_R \eta_2 \leq +_\xi(\eta_1) \sim_R +_\xi(\eta_2)$. Resta ver que dados $\xi_1, \xi_2 \in \mathcal{R}$ se cumple que $\xi_1 \sim_R \xi_2 \leq +_{\xi_1} \sim_{R \to R} +_{\xi_2}$.

$$\begin{aligned}
\xi_1 \sim_R \xi_2 &= \{\omega \in \Omega \ / \ \xi_1(\omega) = \xi_2(\omega)\}/[\mu = 0] \\
+_{\xi_1} \sim_{R \to R} +_{\xi_2} &= \bigwedge_{\eta \in \mathcal{R}} +_{\xi_1}(\eta) \sim_R +_{\xi_2}(\eta) \\
&= \bigwedge_{\eta \in \mathcal{R}} \{\omega \in \Omega \ / \ \xi_1(\omega) + \eta(\omega) = \xi_2(\omega) + \eta(\omega)\}/[\mu = 0]
\end{aligned}$$

Observando que para cada $\eta \in \mathcal{R}$ se cumple $\xi_1 \sim_R \xi_2 \leq +_{\xi_1}(\eta) \sim_R +_{\xi_2}(\eta)$ terminamos. Que $[\![\mathtt{opp}]\!]$ y $[\![\mathtt{inv}]\!] \in [\![R \to R]\!]$ es consecuencia de que en general si $f : \mathbb{R} \to \mathbb{R}$ es medible, entonces con $\psi_f : \mathcal{R} \to \mathcal{R}$ definida como $\psi_f(\xi)(\omega) = f(\xi(\omega))$, o equivalentemente

$\psi_f(\xi) = f \circ \xi$, tenemos que $\psi_f \in [\![R \to R]\!]$. Tanto tomar opuesto como tomar inverso son funciones medibles.

Veamos que $[\![\leq]\!] \in [\![R \to R \to \texttt{Prop}]\!]$. Sea $\xi \in \mathcal{R}$. Veamos que $\leq_\xi \in [\![R \to \texttt{Prop}]\!]$.

$$\eta_1 \sim_R \eta_2 = \{\omega \in \Omega \ / \ \eta_1(\omega) = \eta_2(\omega)\}/[\mu = 0]$$
$$\leq_\xi (\eta_1) \sim_{\texttt{Prop}} \leq_\xi (\eta_2) = \{\omega \in \Omega \ / \ \xi(\omega) \leq \eta_1(\omega) \Leftrightarrow \xi(\omega) \leq \eta_2(\omega)\}/[\mu = 0]$$

Nuevamente concluimos en base a la inclusión de los conjuntos. Sean $\xi_1, \xi_2 \in \mathcal{R}$.

$$\begin{aligned} \xi_1 \sim_R \xi_2 &= \{\omega \in \Omega \ / \ \xi_1(\omega) = \xi_2(\omega)\}/[\mu = 0] \\ \leq_{\xi_1} \sim_{R \to \texttt{Prop}} \leq_{\xi_2} &= \bigwedge_{\eta \in \mathcal{R}} \leq_{\xi_1} (\eta) \sim_{\texttt{Prop}} \leq_{\xi_2} (\eta) \\ &= \bigwedge_{\eta \in \mathcal{R}} \{\omega \in \Omega \ / \ \xi_1(\omega) \leq \eta(\omega) \Leftrightarrow \xi_2(\omega) \leq \eta(\omega)\}/[\mu = 0] \end{aligned}$$

Análogamente, para cada $\eta \in \mathcal{R}$ se cumple $\xi_1 \sim_R \xi_2 \leq \leq_{\xi_1} (\eta) \sim_{\texttt{Prop}} \leq_{\xi_2} (\eta)$. □

Notar que esta interpretación adapta el modelo de reales aleatorios de Scott al contexto más amplio de la lógica de orden superior. Usando el marco presentado en la sección 3.3, con definir solamente la interpretación de R y las constantes, tenemos definidas interpretaciones para todos los tipos y términos. En particular, $[\![R \to R]\!]$ coincide con las funciones aleatorias y $[\![(R \to R) \to R]\!]$ coincide con las funcionales aleatorias, las cuales fueron introducidas "a mano" en el modelo de Scott.

4.1.1. Semimétricas y topologías inducidas

En esta subsección realizamos una observación sencilla pero interesante. No profundizamos en esto ya que no fue aplicado en lo siguiente. En las interpretaciones de los tipos se pueden definir semimétricas, con cuyas topología inducida las funciones compatibles son continuas. Para cada tipo τ definimos una semimétrica en $[\![\tau]\!]$ de la siguiente forma:

$$d_\tau(a, b) := 1 - \mu(a \sim_\tau b)$$

teniendo en cuenta que si $A/[\mu = 0] = B/[\mu = 0]$ entonces $\mu(A) = \mu(B)$.

Lema 4.1.2. *Para todo tipo τ, tenemos que d_τ es una semimétrica, en el sentido de que cumple los axiomas de espacio métrico con la excepción de que pueden haber $a \neq b$ con distancia nula.*

Demostración. Es claro que para todos $a, b \in [\![\tau]\!]$, $d_\tau(a, a) = 0$ y $d_\tau(a, b) = d_\tau(b, a)$. Veamos la desigualdad triangular. Sean $a, b, c \in [\![\tau]\!]$. Observamos lo siguiente:

$$\mu(a \sim_\tau b \wedge b \sim_\tau c) = \mu(a \sim_\tau b) + \mu(b \sim_\tau c) - \mu(a \sim_\tau b \vee b \sim_\tau c) \geq \mu(a \sim_\tau b) + \mu(b \sim_\tau c) - 1$$

Razonamos de la siguiente forma.

$$d_\tau(a, c) = 1 - \mu(a \sim_\tau c) \leq 1 - \mu(a \sim_\tau b \wedge b \sim_\tau c) \leq 2 - \mu(a \sim_\tau b) - \mu(b \sim_\tau c)$$

Observamos que el último término es $d_\tau(a, b) + d_\tau(b, c)$. □

En el caso $\tau \equiv \texttt{Prop}$ es una métrica y coincide con tomar la medida de la diferencia simétrica.

Teorema 4.1.3. *Considerando $(\llbracket\tau\rrbracket, d_\tau)$ y $(\llbracket\sigma\rrbracket, d_\sigma)$, todas las funciones de $\llbracket\tau \to \sigma\rrbracket$ son 1-Lipschitz y por lo tanto continuas con las topologías inducidas por las semimétricas.*

Cabe aclarar que no se cumple el recíproco del teorema anterior. Al tomar medida se pierde información que es importante para determinar si una función es compatible. Un contraejemplo es $\Omega = [0,1]$ y $f : B \to B$ tal que $f([X]) = [\{1 - t \ / \ t \in X\}]$.

4.1.2. Mezcla de R

Como a HOL agregamos un único tipo de base R, debido al corolario 3.3.12, si probamos que la interpretación de este tipo es mezclable, tendremos que todos los tipos son mezclables. Eso es exactamente lo que haremos y de hecho que los tipos sean mezclables será un ingrediente muy importante en la prueba de validez del axioma de completitud.

Proposición 4.1.4. *$(\mathcal{R}, \sim_R)$ es mezclable.*

Demostración. Sean $C \subseteq B$ una partición de la unidad y $\{\xi_c\}_{c\in C} \subseteq \mathcal{R}$. Como B cumple la ccc, C es numerable. Esto nos permite para cada $c \in C$ obtener $\Lambda_c \subseteq \Omega$ tal que $c = \Lambda_c/[\mu = 0]$ y tales que Ω es unión disjunta de los Λ_c. Definimos $\hat{\xi} : \Omega \to \mathbb{R}$ de modo que en cada Λ_c es $\hat{\xi}|_{\Lambda_c} = \xi_c$, o sea, en cada Λ_c coincide con ξ_c. Como los Λ_c son medibles y hay numerables de ellos, $\hat{\xi}$ es medible. Finalmente:

$$\xi_c \sim_R \hat{\xi} = \{\omega \in \Omega / \xi_c(\omega) = \hat{\xi}(\omega)\}/[\mu = 0] \geq \Lambda_c/[\mu = 0] = c \qquad \square$$

4.2. Axiomas de los números reales

Veremos que nuestro modelo verifica que $(R, +, \times, 0, 1, \leq)$ es un cuerpo totalmente ordenado completo. Cabe aclarar que esto no significa que $(\mathcal{R}, \llbracket+\rrbracket, \llbracket\times\rrbracket, \llbracket0\rrbracket, \llbracket1\rrbracket, \llbracket\leq\rrbracket)$ sea siquiera un cuerpo en el sentido usual, en su lugar significa que todos los axiomas de cuerpo totalmente ordenado y el de completitud son válidos bajo la interpretación. Nos concentramos primero en los axiomas de cuerpo totalmente ordenado, que son los siguientes.

$\forall x, y, z^R.\ x + (y + z) =_R (x + y) + z$ $\qquad$ $\forall x, y, z^R.\ x \times (y \times z) =_R (x \times y) \times z$

$\forall x, y^R.\ x + y =_R y + x$ $\qquad$ $\forall x, y^R.\ x \times y =_R y \times x$

$\forall x^R.\ x + 0 =_R x$ $\qquad$ $\forall x^R.\ x \times 1 =_R x$

$\forall x^R.\ x + \texttt{opp}(x) =_R 0$ $\qquad$ $\forall x^R.\ x \neq 0 \Rightarrow x \times \texttt{inv}(x) =_R 1$

$\forall x, y, z^R.\ x \times (y + z) =_R x \times y + x \times z$

$\forall x^R.\ x \leq x$ $\qquad$ $\forall x, y^R.\ x \leq y \wedge y \leq x \Rightarrow x = y$

$\forall x, y, z^R.\ x \leq y \wedge y \leq z \Rightarrow x \leq z$ $\qquad$ $\forall x, y^R.\ x \leq y \vee y \leq x$

$\forall x, y, z^R.\ x \leq y \Rightarrow x + z \leq y + z$ $\qquad$ $\forall x, y, z^R.\ x \leq y \wedge 0 \leq z \Rightarrow x \times z \leq y \times z$

No es difícil verificar que cada una de estas fórmulas es válida en el modelo. De hecho si evaluamos sus interpretaciones una por una, veremos que la validez de cada una de ellas se deduce directamente de que la misma propiedad se cumple en $\mathbb{R}$. Vamos a tomar un enfoque que nos permite probar la validez de todas al mismo tiempo. Esto surge de la observación de que todos los axiomas son de la forma $\forall x_1, \dots x_n^R.\, \phi_0$ donde ϕ_0 es una fórmula sin cuantificadores. Vamos a precisar exactamente a lo que nos referimos con esto (no es totalmente directo porque las igualdades y las conectivas lógicas fueron definidas en la sección 3.1.2 usando implicaciones y cuantificadores).

Definición 4.2.1. Los *términos reales de primer orden* se definen recursivamente por la siguiente gramática.

$$t, u := x^R \mid 0 \mid 1 \mid t + u \mid t \times u \mid \texttt{opp}(t) \mid \texttt{inv}(t)$$

donde x^R representa cualquier variable real. La *fórmulas sin cuantificadores* se definen recursivamente por la siguiente gramática.

$$\phi, \psi := t \leq u \mid t =_R u \mid \neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \Rightarrow \psi$$

donde t y u pueden ser cualquier término real de primer orden. Las fórmulas de tipo Π_1^R son de la forma $\forall x_1, \dots, x_n^R.\, \phi$, donde ϕ es una fórmula sin cuantificadores y $n \geq 0$.

Notar que las fórmulas Π_1^R (y en particular también las sin cuantificadores) solamente tienen variables libres de tipo R. Esto permite interpretarlas también como fórmulas de lógica primer orden. Si $\phi(x_1, \dots x_n)$ es una fórmula Π_1^R y tenemos $a_1, \dots a_n \in \mathbb{R}$, la afirmación $\mathbb{R} \models \phi(a_1, \dots, a_n)$ tiene sentido.

Veremos que las fórmulas cerradas Π_1^R válidas en $\mathbb{R}$ también lo son en el modelo de reales aleatorios. Primero probaremos un lema.

Lema 4.2.2. *Sea $\phi(x_1, \dots, x_n)$ una fórmula sin cuantificadores con variables libres entre $x_1, \dots, x_n : R$. Entonces para cada $\xi_1, \dots \xi_n \in \mathcal{R}$:*

$$[\![\phi(\xi_1, \dots \xi_n)]\!] = \{\omega \in \Omega \;/\; \mathbb{R} \models \phi(\xi_1(\omega), \dots, \xi_n(\omega))\}/[\mu = 0]$$

Demostración. Por inducción en la fórmula sin cuantificadores ϕ. Los casos de base ($t \leq u$ y $t =_R u$) son análogos entre sí. Veamos la idea del de $t \leq u$.

$$\begin{aligned}
[\![t \leq u(\xi_1, \dots, \xi_n)]\!] &= \{\omega \in \Omega \;/\; [\![t(\xi_1, \dots, \xi_n)]\!](\omega) \leq [\![u(\xi_1, \dots, \xi_n)]\!](\omega)\}/[\mu = 0] \\
&= \{\omega \in \Omega \;/ t(\xi_1(\omega), \dots, \xi_n(\omega)) \leq u(\xi_1(\omega), \dots, \xi_n(\omega))\}/[\mu = 0] \\
&= \{\omega \in \Omega \;/ \mathbb{R} \models t(\xi_1(\omega), \dots, \xi_n(\omega)) \leq u(\xi_1(\omega), \dots, \xi_n(\omega))\}/[\mu = 0]
\end{aligned}$$

Aquí usamos que para cualquier término real de primer orden $t(x_1, \dots x_n)$, cualesquiera $\xi_1, \dots \xi_n \in \mathcal{R}$ y cualquier $\omega \in \Omega$, se cumple $[\![t(\xi_1, \dots \xi_n)]\!](\omega) = t(\xi_1(\omega), \dots \xi_n(\omega))$. Esto vincula las dos formas de interpretar los términos reales de primer orden: como términos de tipo R en HOL y como términos de lógica de primer orden. La prueba es por inducción en la definición recursiva de los términos reales de primer orden. Los casos inductivos se cumplen de forma directa debido a que las interpretaciones de las operaciones son punto a punto.

Volviendo a lo que debemos probar en este lema, en los casos inductivos, la tesis se deduce de las hipótesis de forma directa. Veamos por ejemplo el de la implicación.

$$\begin{aligned}
[\![\phi((\xi_1,\ldots,\xi_n) \Rightarrow \psi(\xi_1,\ldots,\xi_n))]\!] &= [\![\phi((\xi_1,\ldots,\xi_n)]\!] \to [\![\psi(\xi_1,\ldots,\xi_n))]\!] \\
= \{\omega \in \Omega \;/\; \mathbb{R} \models \phi(\xi_1(\omega),\ldots,\xi_n(\omega))\}/[\mu=0] &\to \{\omega \in \Omega \;/\; \mathbb{R} \models \psi(\xi_1(\omega),\ldots,\xi_n(\omega))\}/[\mu=0] \\
= (\{\omega \in \Omega \;/\; \mathbb{R} \models \phi(\xi_1(\omega),\ldots,\xi_n(\omega))\} &\to \{\omega \in \Omega \;/\; \mathbb{R} \models \psi(\xi_1(\omega),\ldots,\xi_n(\omega))\})/[\mu=0] \\
= (\{\omega \in \Omega \;/\; \mathbb{R} \models \phi(\xi_1(\omega),\ldots,\xi_n(\omega))\}^c &\cup \{\omega \in \Omega \;/\; \mathbb{R} \models \psi(\xi_1(\omega),\ldots,\xi_n(\omega))\})/[\mu=0] \\
= \{\omega \in \Omega \;/\; \mathbb{R} \models \neg\phi(\xi_1(\omega),\ldots,\xi_n(\omega)) &\vee \psi(\xi_1(\omega),\ldots,\xi_n(\omega))\}/[\mu=0] \\
= \{\omega \in \Omega \;/\; \mathbb{R} \models \phi(\xi_1(\omega),\ldots,\xi_n(\omega)) &\Rightarrow \psi(\xi_1(\omega),\ldots,\xi_n(\omega))\}/[\mu=0]
\end{aligned}$$

□

Corolario 4.2.3. *Sea ϕ una fórmula cerrada Π_1^R tal que $\mathbb{R} \models \phi$. Entonces ϕ es válida en el modelo de reales aleatorios.*

Demostración. Tenemos que $\phi \equiv \forall x_1^R \ldots \forall x_n^R \phi_0(x_1,\ldots,x_n)$ donde $\phi_0(x_1,\ldots,x_n)$ es una fórmula sin cuantificadores.

$$[\![\phi]\!] = \bigwedge_{\xi_1,\ldots\xi_n \in \mathcal{R}} [\![\phi_0(\xi_1,\ldots\xi_n)]\!]$$

Sean $\xi_1,\ldots\xi_n \in \mathcal{R}$. Vamos a probar que $[\![\phi_0(\xi_1,\ldots\xi_n)]\!] = 1$. Por el lema anterior:

$$[\![\phi_0(\xi_1,\ldots\xi_n)]\!] = \{\omega \in \Omega \;/\; \mathbb{R} \models \phi_0(\xi_1(\omega),\ldots,\xi_n(\omega))\}/[\mu=0]$$

Como $\mathbb{R} \models \phi$, tenemos que para todos $x_1,\ldots x_n \in \mathbb{R}$ se cumple que $\mathbb{R} \models \phi_0(x_1,\ldots,x_n)$. Por lo tanto, $\{\omega \in \Omega \;/\; \mathbb{R} \models \phi_0(\xi_1(\omega),\ldots,\xi_n(\omega))\} = \Omega$. □

Teorema 4.2.4. *En el modelo de reales aleatorios, $(R,+,\times,0,1,\leq)$ es un cuerpo totalmente ordenado, en el sentido de que todos los axiomas de cuerpos totalmente ordenados son válidos.*

Demostración. Con la presentación que usamos, todos los axiomas de cuerpo ordenado son de tipo Π_1^R. Por lo tanto, se deduce del corolario anterior. □

Solamente resta probar la validez del axioma de completitud, lo cual como es de esperarse requerirá más trabajo.

4.2.1. Axioma de completitud

Recordamos que en HOL los subconjuntos de R son representados por predicados de tipo $R \to \texttt{Prop}$. En este marco, el axioma de completitud de formula así:

$$\forall S^{R\to\texttt{Prop}}.\; \exists x^R Sx \wedge \exists y^R \forall x^R (Sx \Rightarrow x \leq y) \Rightarrow \exists z^R \forall y^R (z \leq y \Leftrightarrow \forall x^R (Sx \Rightarrow x \leq y))$$

Notaremos `Compl` a la proposición anterior. Comenzamos con un lema que será utilizado más de una vez en la prueba.

Lema 4.2.5. *1. Para cada $\xi, \eta \in \mathcal{R}$, se cumple:*

$$[\![\xi \leq \eta]\!] = \bigwedge_{q \in \mathbb{Q}} ([\![\eta \leq q]\!] \to [\![\xi \leq q]\!])$$

2. Para cada $\xi \in \mathcal{R}$ y cada $q \in \mathbb{Q}$, se cumple que:

$$[\![\xi \leq q]\!] = \bigwedge_{r>q} [\![\xi \leq r]\!]$$

Donde identificamos $q \in \mathbb{Q}$ con la función constante $q \in \mathcal{R}$.

Demostración. Probaremos solo la primera, pues la segunda se deduce de un razonamiento análogo más sencillo. La demostración consiste en escribir las definiciones y utilizar que el cociente conmuta con las operaciones booleanas binarias y numerables (por el corolario 1.2.3).

$$\begin{aligned}
\bigwedge_{q\in\mathbb{Q}} ([\![\eta \leq q]\!] \to [\![\xi \leq q]\!]) &= \bigwedge_{q\in\mathbb{Q}} (\{\omega \in \Omega / \eta(\omega) \leq q\}/[\mu = 0] \to \{\omega \in \Omega / \xi(\omega) \leq q\}/[\mu = 0]) \\
&= \bigwedge_{q\in\mathbb{Q}} \{\omega \in \Omega \ / \ \eta(\omega) \leq q \Rightarrow \xi(\omega) \leq q\}/[\mu = 0] \\
&= \left(\bigcap_{q\in\mathbb{Q}} \{\omega \in \Omega \ / \ \eta(\omega) \leq q \Rightarrow \xi(\omega) \leq q\} \right) /[\mu = 0] \\
&= \{\omega \in \Omega \ / \ \forall q \in \mathbb{Q} \ \eta(\omega) \leq q \Rightarrow \xi(\omega) \leq q\}/[\mu = 0] \\
&= \{\omega \in \Omega \ / \ \xi(\omega) \leq \eta(\omega)\}/[\mu = 0] \\
&= [\![\xi \leq \eta]\!]
\end{aligned}$$

□

Teorema 4.2.6. *El axioma de completitud es válido en el modelo de reales aleatorios*

Demostración. Por el corolario 3.3.17, si hay un elemento de $[\![R \to \texttt{Prop}]\!]$ que verifica el antecedente, alcanza probar que todos los que lo hacen también verifican el consecuente. Un elemento que verifica el antecedente es:

$$\varphi_0 \in [\![R \to \texttt{Prop}]\!] \qquad \varphi_0(\xi) = [\![\xi = 0]\!]$$

Sea $\varphi \in [\![R \to \texttt{Prop}]\!]$ tal que $[\![\exists x^R \varphi x \wedge \exists y^R \forall x^R (\varphi x \Rightarrow x \leq y)]\!] = 1$. Debemos probar que $[\![\exists z^R \forall y^R (z \leq y \Leftrightarrow \forall x^R (\varphi x \Rightarrow x \leq y))]\!] = 1$. Usando el principio del máximo (teorema 3.3.13), de la hipótesis sobre φ podemos deducir lo siguiente:

1. Existe $\xi_0 \in \mathcal{R}$ tal que $\varphi(\xi_0) = 1$.
2. Existe $\eta_0 \in \mathcal{R}$ tal que $\forall \xi \in \mathcal{R}$, $\varphi(\xi) \leq [\![\xi \leq \eta_0]\!]$.

Buscamos $\chi \in \mathcal{R}$ tal que $\forall \eta \in \mathcal{R}$, $[\![\chi \leq \eta]\!] = \bigwedge_{\xi\in\mathcal{R}} (\varphi(\xi) \to [\![\xi \leq \eta]\!])$. Para facilitar la notación definimos $\psi \in [\![R \to \texttt{Prop}]\!]$ como $\psi(\eta) = \bigwedge_{\xi\in\mathcal{R}} (\varphi(\xi) \to [\![\xi \leq \eta]\!])$. Este predicado básicamente afirma que η es una cota superior de φ. Efectivamente $\psi \in [\![R \to \texttt{Prop}]\!]$ por ser la interpretación de un término de ese tipo ($\psi = [\![\lambda y^R. \forall x^R. \varphi x \Rightarrow x \leq y]\!]$). Por lo tanto, buscamos $\chi \in \mathcal{R}$ tal que $\forall \eta \in \mathcal{R}$, $[\![\chi \leq \eta]\!] = \psi(\eta)$. Las siguientes son propiedades útiles:

1. $[\![\eta_1 \leq \eta_2]\!] \leq \psi(\eta_1) \to \psi(\eta_2)$.
2. $\psi(\xi_0 - 1) = 0$.

3. $\psi(\eta_0) = 1$.

La primera se cumple porque $[\![\eta_1 \leq \eta_2]\!] \to \psi(\eta_1) \to \psi(\eta_2)$ es la interpretación de una fórmula derivable en base a los axiomas de orden, la cual afirma que si $\eta_1 \leq \eta_2$ y η_1 es una cota superior de φ, entonces η_2 también lo es. Aquí estamos usando el teorema 3.3.10. Vamos a construir χ mediante un razonamiento análogo a las cortaduras de Dedekind, trabajando con $\psi(q)$ para $q \in \mathbb{Q}$. Comenzamos viendo las siguientes tres propiedades:

$$\bigwedge_{q\in\mathbb{Q}} \psi(q) = 0 \qquad \bigvee_{q\in\mathbb{Q}} \psi(q) = 1 \qquad \forall q \in \mathbb{Q},\ \psi(q) = \bigwedge_{r>q} \psi(r)$$

Por 1 tenemos que $[\![q \leq \xi_0 - 1]\!] \wedge \psi(q) = 0$. Por lo tanto $\psi(q) \leq [\![q > \xi_0 - 1]\!]$. Tomando ínfimo en $q \in \mathbb{Q}$ concluimos $\bigwedge \psi(q) = 0$. Análogamente, $[\![\eta_0 \leq q]\!] \wedge \psi(\eta_0) \leq \psi(q)$, por lo que $[\![\eta_0 \leq q]\!] \leq \psi(q)$. Tomando supremo en $q \in \mathbb{Q}$ tenemos $\bigvee \psi(q) = 1$. Para ver la tercera propiedad, dado $q \in \mathbb{Q}$ hacemos lo siguiente (valiéndonos del lema 4.2.5):

$$\begin{aligned}
\psi(q) &= \bigwedge_{\xi\in\mathcal{R}} (\varphi(\xi) \to [\![\xi \leq q]\!]) \\
&= \bigwedge_{\xi\in\mathcal{R}} \left(\varphi(\xi) \to \bigwedge_{r>q} [\![\xi \leq r]\!]\right) \\
&= \bigwedge_{\xi\in\mathcal{R}} \bigwedge_{r>q} (\varphi(\xi) \to [\![\xi \leq r]\!]) \\
&= \bigwedge_{r>q} \bigwedge_{\xi\in\mathcal{R}} (\varphi(\xi) \to [\![\xi \leq r]\!]) \\
&= \bigwedge_{r>q} \psi(r)
\end{aligned}$$

Tomamos (justificado en el siguiente párrafo) una familia $\{\Lambda_q\}_{q\in\mathbb{Q}} \subseteq \Omega$ de representantes que cumple las mismas propiedades que los $\psi(q)$:

1. $\forall q \in \mathbb{Q},\ \psi(q) = \Lambda_q/[\mu = 0]$
2. $\bigcap_{q\in\mathbb{Q}} \Lambda_q = \varnothing$
3. $\bigcup_{q\in\mathbb{Q}} \Lambda_q = \Omega$
4. $\forall q \in \mathbb{Q},\ \Lambda_q = \bigcap_{r>q} \Lambda_r$

Comenzamos con $\{A_q^0\}_{q\in\mathbb{Q}}$ un conjunto de representantes cualquiera, que por lo tanto cumple 1. Definimos $A_q^1 = \bigcap_{r>q} A_r^0$, de modo que ahora tenemos 1 y monotonía (respecto al orden de $\mathbb{Q}$ y la inclusión). Ahora definimos $A_q^2 = A_q^1 - \bigcap_{r\in\mathbb{Q}} A_r^1$, de modo que tenemos 1, 2 y monotonía. Para el siguiente paso consideramos $C = \Omega - \bigcup_{q\in\mathbb{Q}} A_q^2$.

$$A_q^3 = \begin{cases} A_q & \text{si } q < 0 \\ A_q \cup C & \text{si } q \geq 0 \end{cases}$$

Ahora tenemos 1, 2, 3 y monotonía. Finalmente definimos $\Lambda_q = \bigcap_{r>q} A_r^3$ y cumple 1, 2, 3 y 4 (la monotonía es necesaria para ver que cumple 3).

Esta familia nos permite construir $\chi \in \mathcal{R}$ como:

$$\chi(\omega) := \inf\{q \in \mathbb{Q} \ / \ \omega \in \Lambda_q\}$$

el cual tiene la propiedad de que $\forall q \in \mathbb{Q}$, $[\![\chi \leq q]\!] = \psi(q)$. Esto se debe a que:

$$\{\omega \in \Omega \ / \ \chi(\omega) \leq q\} = \{\omega \in \Omega \ / \ q \in \{r \in \mathbb{Q} \ / \ \omega \in \Lambda_r\}\} = \Lambda_q$$

Notar que eso también justifica que χ es medible. Que $\chi(\omega) \leq q$ sea equivalente a que $q \in \{r \in \mathbb{Q} \ / \ \omega \in \Lambda_r\}$ es porque Λ_q cumple la propiedad 4. De esta deducimos que $\{r \in \mathbb{Q} \ / \ \omega \in \Lambda_r\}$ es cerrado hacia arriba y que si el ínfimo es racional, es mínimo.

Resta probar que $\forall \eta \in \mathcal{R}$, $[\![\chi \leq \eta]\!] = \psi(\eta)$. Comenzamos viendo que $\psi(\chi) = 1$, lo cual implicará fácilmente una de las desigualdades. Sea $\xi \in \mathcal{R}$ tal que $\varphi(\xi) = 1$ (usamos el corolario 3.3.17), queremos probar que $[\![\xi \leq \chi]\!] = 1$. Usamos el lema 4.2.5 y dado $q \in \mathbb{Q}$ debemos probar que $[\![\chi \leq q]\!] \leq [\![\xi \leq q]\!]$. Por la propiedad de χ, esto es que $\psi(q) \leq [\![\xi \leq q]\!]$. Concluimos usando que $\varphi(\xi) = 1$:

$$\psi(q) = \psi(q) \wedge \varphi(\xi) \leq (\varphi(\xi) \to [\![\xi \leq q]\!]) \wedge \varphi(\xi) \leq [\![\xi \leq q]\!]$$

Utilizando esto, dado $\eta \in \mathcal{R}$ tenemos que $[\![\chi \leq \eta]\!] = [\![\chi \leq \eta]\!] \wedge \psi(\chi) \leq \psi(\eta)$.

Solo resta dado $\eta \in \mathcal{R}$ probar que $\psi(\eta) \leq [\![\chi \leq \eta]\!]$. Vamos a utilizar nuevamente el lema 4.2.5. Sea $q \in \mathbb{Q}$. Tenemos que $[\![\eta \leq q]\!] \wedge \psi(\eta) \leq \psi(q) = [\![\chi \leq q]\!]$, por lo que $\psi(\eta) \leq [\![\eta \leq q]\!] \to [\![\chi \leq q]\!]$. Tomando supremo en $q \in \mathbb{Q}$ concluimos $\psi(\eta) \leq [\![\chi \leq \eta]\!]$. □

4.3. Hipótesis del continuo

Recordamos nuevamente que en lógica de orden superior se representan los subconjuntos de R como predicados sobre el tipo R, es decir: como funciones de tipo $R \to \texttt{Prop}$. En particular, el subconjunto N de los enteros naturales se puede definir (siguiendo Dedekind) como el subconjunto de R más pequeño que contiene 0 y es estable por sucesor:

$$N := \lambda x^R.\, \forall S^{R \to \texttt{Prop}}.\, S0 \wedge \forall y^R (Sy \Rightarrow S(y+1)) \Rightarrow Sx$$

Con el predicado de los números naturales podemos dar un enunciado elemental de la hipótesis del continuo (análogo al dado al final de la sección 2.1.1):

$$\forall S^{R \to \texttt{Prop}}.\, \exists f^{R \to R} \forall x^R (Sx \Rightarrow \exists y^R (Ny \wedge fy = x)) \vee \exists g^{R \to R} \forall z^R \exists x^R (Sx \wedge gx = z)$$

Lo que afirma literalmente este enunciado es que todo subconjunto de R (representado por $S^{R \to \texttt{Prop}}$) es o bien de cardinal menor o igual al de N (debido a f, que es una función sobreyectiva de N a S) o bien del cardinal de R (debido a g, que es una función sobreyectiva de S a R). Esto excluye la existencia de un conjunto con cardinal estrictamente contenido entre el de N y el de R.

Nuestro objetivo es encontrar un modelo de reales aleatorios (eligiendo el espacio de probabilidad) en el que la hipótesis del continuo no sea válida y que idealmente el contraejemplo $\psi \in [\![R \to \texttt{Prop}]\!]$ (que represente un subconjunto con cardinal estrictamente entre el de N y el de R) tenga alguna interpretación intuitiva, aprovechando el carácter probabilístico de estos modelos. Para poder hacer eso, antes necesitamos entender mejor cómo es la interpretación de N y tener una forma de construir elementos de $[\![R \to \texttt{Prop}]\!]$. Con esos dos fines, probamos los siguientes lemas.

Lema 4.3.1. *Para todo $X \subseteq \mathcal{R}$, definiendo $\varphi : \mathcal{R} \to B$ como*

$$\varphi(\xi) = \bigvee_{x \in X} [\![\xi = x]\!]$$

tenemos que $\varphi \in [\![R \to \texttt{Prop}]\!]$.

Demostración. Sean $\xi, \eta \in \mathcal{R}$. Debemos probar que $[\![\xi = \eta]\!] \leq \varphi(\xi) \leftrightarrow \varphi(\eta)$. Probamos que $[\![\xi = \eta]\!] \wedge \varphi(\xi) \leq \varphi(\eta)$; la otra desigualdad es análoga.

$$[\![\xi = \eta]\!] \wedge \varphi(\xi) = \bigwedge_{x \in X} ([\![\xi = \eta]\!] \wedge [\![\xi = x]\!]) \leq \bigwedge_{x \in X} [\![\eta = x]\!] = \varphi(\eta)$$

□

Veamos que el predicado de los naturales se interpreta como uno de los ejemplos del lema anterior, con $X = \mathbb{N}$.

Lema 4.3.2 (Interpretación de los naturales)**.** *Para cada $\xi \in \mathcal{R}$ tenemos que:*

$$[\![N(\xi)]\!] = \bigvee_{n \in \mathbb{N}} [\![\xi = n]\!]$$

Donde identificamos $n \in \mathbb{N}$ con el real aleatorio constante.

Demostración. Por el corolario 3.3.16 tenemos que:

$$[\![N(\xi)]\!] = \bigwedge_{\varphi \in \mathcal{A}} \varphi(\xi)$$

donde $\mathcal{A} = \{\varphi \in [\![R \to \texttt{Prop}]\!] \ / \ \varphi(0) \wedge \bigwedge_{\eta \in \mathcal{R}} (\varphi(\eta) \to \varphi(\eta + 1)) = 1\}$. Probaremos las dos desigualdades.

Para probar el $\leq$ consideramos $\varphi \in [\![R \to \texttt{Prop}]\!]$ definido con $\varphi(\xi) = \bigvee_{n \in \mathbb{N}} [\![\xi = n]\!]$. La desigualdad se deduce de que $\varphi \in \mathcal{A}$.

Para la otra desigualdad debemos probar que para cualquier $\psi \in \mathcal{A}$ se cumple que $\varphi(\xi) \leq \psi(\xi)$. Como $\psi(0) = 1$ y $\forall \eta \in \mathcal{R},\ \psi(\eta) \leq \psi(\eta + 1)$, tenemos que para todo $n \in \mathbb{N}$ se cumple que $\psi(n) = 1$. Hacemos la siguiente cuenta:

$$[\![\xi = n]\!] = [\![\xi = n]\!] \wedge \psi(n) \leq \psi(\xi)$$

Tomando supremo en n tenemos $\varphi(\xi) \leq \psi(\xi)$. □

El contraejemplo que utilizaremos para la hipótesis del continuo es el conjunto de las variables aleatorias constantes. La intuición es que tenemos por una parte las variables aleatorias naturales, por otra parte todas las variables aleatorias y en el medio las variables aleatorias constantes, es decir que valen el mismo real r para todo $\omega \in \Omega$. Sin embargo, si definimos $\psi : \mathcal{R} \to B$ tal que vale 1 en los $r \in \mathbb{R}$ (reales aleatorios constantes) y 0 en todos los otros, tendremos que $\psi \notin [\![R \to \texttt{Prop}]\!]$. Por ejemplo, supongamos que el espacio de probabilidad es $\Omega = [0, 1]$ y consideremos $\xi \in \mathcal{R}$ tal que $\xi(x) = 0$ si $x < 1/2$ y $\xi(x) = 1$ en otro caso. Tenemos que $0 \sim_R \xi = [0, 1/2]/[\mu = 0] \neq 0$ pero $\psi(\xi) = 0$, $\psi(0) = 1$ y por

lo tanto $\psi(\xi) \sim_{\texttt{Prop}} \psi(0) = 0$ lo cual contradice que ψ sea compatible. Lo que vamos a hacer por lo tanto, es considerar el predicado $R_0 \in [\![R \to \texttt{Prop}]\!]$ definido como:

$$R_0(\xi) = \bigvee_{r \in \mathbb{R}} [\![\xi = r]\!]$$

el cual está en $[\![R \to \texttt{Prop}]\!]$ por el lema 4.3.1. Este predicado R_0, que representa al conjunto de los reales aleatorios constantes, será el contraejemplo de la hipótesis del continuo. Notar que en el ejemplo dado antes con $\Omega = [0,1]$ y $\xi \in \mathcal{R}$ tal que $\xi(x) = 0$ si $x < 1/2$ y $\xi(x) = 1$, con este predicado tenemos que $R_0(\xi) = 1$. En la siguiente y última sección estudiaremos propiedades de este predicado, en particular para justificar que tiene sentido llamarlo el conjunto de los reales aleatorios constantes (veremos en particular que es el menor predicado que vale 1 en todos los $r \in \mathbb{R}$).

Como es usual en construcción de modelos para romper la hipótesis del continuo, si bien cualquier espacio de probabilidad da lugar a un modelo de reales aleatorios, debemos elegir uno específico para asegurar que la hipótesis del continuo sea falsa. Vamos a utilizar $\Omega = [0,1]^I$ con $I = \mathcal{P}(\mathbb{R})$ y la medida producto. La elección de I es para que $|I| > |\mathbb{R}|$. Usamos el espacio de probabilidad producto porque hace que las proyecciones sean totalmente distintas entre sí. Es decir, si para cada $i \in I$ definimos $\xi_i \in \mathcal{R}$ como la proyección en la coordenada i, es decir, $\xi_i(\omega) = \omega(i)$, entonces que para cada $i \neq j$:

$$[\![\xi_i = \xi_j]\!] = \{\omega \in \Omega \ / \ \omega(i) = \omega(j)\}_{[\mu=0]} = 0$$

Vale 0 porque considerando el cuadrado de las coordenadas i y j, este conjunto solo toma valores en la diagonal, la cual tiene medida nula.

Probemos que efectivamente con este espacio de probabilidad, el predicado de los reales aleatorios constantes es un contraejemplo de la hipótesis del continuo.

Teorema 4.3.3. *En el modelo de reales aleatorios con espacio de probabilidad $\Omega = [0,1]^I$ con $I = \mathcal{P}(\mathbb{R})$ y la medida producto, la hipótesis del continuo tiene valor de verdad 0. Más aún, el predicado $R_0 \in [\![R \to \texttt{Prop}]\!]$ definido como:*

$$R_0(\xi) = \bigvee_{r \in \mathbb{R}} [\![\xi = r]\!]$$

funciona como contraejemplo.

Demostración. Debemos probar que $[\![\exists f^{R \to R} \forall x^R (R_0 x \Rightarrow \exists y^R (Ny \wedge fy = x))]\!] = 0$ y que $[\![\exists g^{R \to R} \forall z^R \exists x^R (R_0 x \wedge gx = z)]\!] = 0$. Los argumentos serán muy similares entre sí. Comenzaremos viendo que R_0 no es de cardinal menor o igual al de N, o sea, con la primera igualdad.

Sea $f \in [\![R \to R]\!]$. Supongamos por absurdo $[\![\forall x^R (R_0 x \Rightarrow \exists y^R (Ny \wedge fy = x))]\!] > 0$. Esto implica que para todo $\xi \in \mathcal{R}$ se cumple $[\![R_0 \xi \Rightarrow \exists y^R (Ny \wedge fy = \xi)]\!] > 0$. Sea $r \in \mathbb{R}$. Utilizamos $\xi = r$, el real aleatorio constante.

$$\begin{aligned} 0 &< [\![R_0 r \Rightarrow \exists y^R (Ny \wedge fy = r)]\!] \\ &= R_0(r) \to \bigvee_{\xi \in \mathcal{R}} \bigvee_{n \in \mathbb{N}} ([\![\xi = n]\!] \wedge [\![f(\xi) = r]\!]) \\ &\leq \bigvee_{\xi \in \mathcal{R}} \bigvee_{n \in \mathbb{N}} [\![f(n) = r]\!] = \bigvee_{n \in \mathbb{N}} [\![f(n) = r]\!] \end{aligned}$$

Concluimos que para cada $r \in \mathbb{R}$ existe $n_r \in \mathbb{N}$ tal que $[\![f(n_r) = r]\!] > 0$. Por cardinalidad, existe $k \in \mathbb{N}$ tal que $X := \{r \in \mathbb{R} \ / \ n_r = k\}$ es infinito no numerable. Llegamos a una contradicción porque $A := \{[\![f(k) = r]\!] \ / \ r \in X\} \subseteq B$ es una anticadena infinita no numerable, pues para todo $r \in X$ tenemos que $[\![f(k) = r]\!] > 0$ y dados $r_1, r_2 \in X$:

$$[\![f(k) = r_1]\!] \wedge [\![f(k) = r_2]\!] \leq [\![r_1 = r_2]\!] = 0$$

Esto es una contradicción porque por el lema 1.2.2, el álgebra booleana cumple la ccc y no hay anticadenas infinitas no numerables. Veamos ahora que R_0 tampoco tiene el cardinal de R.

Sea $g \in [\![R \to R]\!]$. Supongamos por absurdo $[\![\forall z^R \exists x^R (R_0 x \wedge gx = z)]\!] > 0$. Esto implica que para todo $\xi \in \mathcal{R}$ se cumple $[\![\exists x^R (R_0 x \wedge gx = \xi)]\!] > 0$. Sea $i \in I$. Utilizaremos $\xi = \xi_i \in \mathcal{R}$, la proyección en la i-ésima coordinada en Ω.

$$\begin{aligned} 0 &< [\![\exists x^R (R_0 x \wedge gx = \xi_i)]\!] \\ &= \bigvee_{\xi \in \mathcal{R}} \bigvee_{r \in \mathbb{R}} ([\![\xi = r]\!] \wedge [\![g(\xi) = \xi_i]\!]) \\ &\leq \bigvee_{\xi \in \mathcal{R}} \bigvee_{r \in \mathbb{R}} [\![g(r) = \xi_i]\!] = \bigvee_{r \in \mathbb{R}} [\![g(r) = \xi_i]\!] \end{aligned}$$

Concluimos que para cada $i \in I$ existe $r_i \in \mathbb{R}$ tal que $[\![g(r_i) = \xi_i]\!] > 0$. Como $|I| > |\mathbb{R}|$ hay un $r \in \mathbb{R}$ tal que $r_i = r$ para infinitos no numerables $i \in I$ y se construye una anticadena infinita no numerable de la misma forma que se hicimos antes, llegando a la misma contradicción. □

4.4. Reales aleatorios constantes

En la prueba de negación de la hipótesis del continuo usamos el predicado de los reales aleatorios constantes, $R_0 \in [\![R \to \texttt{Prop}]\!]$, definido por:

$$R_0(\xi) = \bigvee_{r \in \mathbb{R}} [\![\xi = r]\!]$$

En el siguiente lema daremos una caracterización de este predicado, la cual justifica considerarlo como el que representa al conjunto de los reales aleatorios constantes. Posteriormente, concluimos viendo que este conjunto es un subcuerpo de $\mathcal{R}$ con propiedades interesantes. Aclaramos que con real aleatorio constante nos referimos a $\xi \in \mathcal{R}$ tal que existe $r \in \mathbb{R}$ tal que para todo $\omega \in \Omega$, se cumple $\xi(\omega) = r$. En estos casos, a efectos de notación identificaremos $\xi = r$, como ya hemos hecho.

Lema 4.4.1. *1. Para todo $\xi \in \mathcal{R}$, tenemos que $R_0(\xi) = 1$ si y solo si ξ es equivalente a una mezcla de reales constantes usando una partición de la unidad.*

2. Para toda $\phi \in [\![R \to \texttt{Prop}]\!]$, si $\forall r \in \mathbb{R}\ \phi(r) = 1$ entonces $\forall \xi \in \mathcal{R}\ R_0(\xi) \leq \phi(\xi)$. Esto nos dice que R_0 es el menor conjunto que contiene a los reales aleatorios constantes.

Demostración. 1. Comenzamos con el recípromo. Supongamos que A es una partición de la unidad y $\xi = \sum_{a\in A} a \cdot r_a$. Veamos que $R_0(a) = 1$. Sea $a \in A$.

$$R_0(\xi) \geq R_0(r_a) \wedge \xi \sim r_a = \xi \sim r_a \geq a$$

Tomando supremo en a y usando que A es una partición de la unidad concluimos. Para el directo, sea $\xi \in \mathcal{R}$ tal que $R_0(\xi) = 1$, o sea:

$$\bigvee_{r\in\mathbb{R}} \xi \sim r = 1$$

Sea $A = \{\xi \sim r \ / \ r \in \mathbb{R},\ \xi \sim r \neq 0\}$. Dados $\xi \sim r_1, \xi \sim r_2 \in A$ tenemos que $\xi \sim r_1 \wedge \xi \sim r_2 \leq r_1 \sim r_2$. Por lo tanto, A es una anticadena. Como $R_0(\xi) = 1$, es una partición de la unidad. Definimos la familia $\{r_a\}_{a\in A} \subseteq \mathcal{R}$ con r_a el único real constante tal que $a = \xi \sim r_a$. Afirmamos que $\xi \sim \sum_{a\in A} a \cdot r_a = 1$. Sea $b \in A$.

$$b = \xi \sim r_b \wedge b \leq \xi \sim r_b \wedge \sum_{a\in A} a \cdot r_a \sim r_b \leq \xi \sim \sum_{a\in A} a \cdot r_a$$

En el primer paso usamos que $\xi \sim r_b = b$. Deducimos $b \leq \xi \sim \sum_{a\in A} a \cdot r_a$. Tomando supremo en b, tenemos que $\xi \sim \sum_{a\in A} a \cdot r_a = 1$.

2. Vamos a usar 3,3,16, pues lo que debemos probar es equivalente a que:

$$\bigwedge_{\xi\in\mathcal{R}} (R_0(\xi) \to \phi(\xi)) = 1$$

Por lo tanto, alcanza probar que $\phi(\xi) = 1$ para todo $\xi \in \mathcal{R}$ tal que $R_0(\xi) = 1$. Por el ítem anterior, alcanza entonces probar que $\phi(\xi) = 1$ para todo ξ mezcla de reales constantes con una partición de la unidad. Sea A una partición de la unidad, sea $\{r_a\}_{a\in A} \subseteq \mathcal{R}$ una familia de reales constantes y sea $\xi = \sum_{a\in A} a \cdot r_a$. Probaremos $\phi(a) = 1$. Sea $b \in A$.

$$b = \phi(r_b) \wedge b \leq \phi(r_b) \wedge \xi \sim r_b \leq \phi(\xi)$$

En el primer paso usamos que $\phi(r) = 1$ para todo r real constante. Tomando supremo en b tenemos que $\phi(\xi) = 1$. □

Veamos finalmente que R_0 es de hecho un subcuerpo con propiedades interesantes. Más aún, veremos que cumple los axiomas de cuerpo real cerrado, los cuales recordamos a continuación.

Definición 4.4.2. La teoría de cuerpo real cerrado tiene el lenguaje de la teoría de cuerpo ordenado (símbolos para las operaciones de cuerpo y para el orden) y los siguientes axiomas, formulados en el lenguaje de la lógica de primer orden, con cuantificaciones en R.

1. Los axiomas de cuerpo totalmente ordenado.
2. Existencia de raíces cuadradas: $\forall x,\ x \geq 0 \Rightarrow \exists y\ x = y^2$.
3. Existencia de raíces para los polinomios de grado impar. Es un esquema de axiomas. Para cada n impar tenemos: $\forall a_n, \ldots, \forall a_0,\ a_n > 0 \Rightarrow \exists x\ a_n x^n + \cdots + a_1 x + a_0 = 0$.

Es un resultado de Tarski [7] que la teoría de cuerpo real cerrado es completa, es decir, para cada fórmula cerrada del lenguaje, a partir de los axiomas se la puede demostrar o demostrar su negación. Esto en particular implica que todos los cuerpos reales cerrados son elementalmente equivalentes (cumplen exactamente las mismas fórmulas).

El siguiente lema nos permite deducir que R_0 es un cuerpo real cerrado. En la definición 4.2.1 definimos las fórmulas Π_1^R como las que tienen la forma $\forall x_1, \dots x_n^R.\ \phi$ con ϕ fórmula sin cuantificadores. Una fórmula Π_2^R es de la forma $\forall x_1, \dots x_n^R \exists y_1, \dots y_m^R.\ \phi$ con ϕ fórmula sin cuantificadores y $n, m \geq 0$. Para facilitar los enunciados de lo siguiente extendemos la sintaxis con una constante $R_0 : R \to \texttt{Prop}$ que se interpreta justamente con el predicado R_0.

Lema 4.4.3. *Las fórmulas de tipo Π_2^R que se cumplen en $\mathbb{R}$ son válidas en R_0.*

Demostración. Sea $\forall x_1, \dots \forall x_n \exists y_1, \dots \exists y_m \phi(x_1, \dots, x_n, y_1, \dots y_m)$ una fórmula Π_2^R, o sea con ϕ siendo una fórmula sin cuantificadores, que se cumple en $\mathbb{R}$. Que la fórmula sea válida en R_0 significa que relativizando sus cuantificaciones (o sea remplazando cada $\forall x^R.\ \psi$ por $\forall x^R. R_0 x \Rightarrow \psi$ y cada $\exists y^R.\ \psi$ por $\exists y^R.\ R_0 y \wedge \psi$) llegamos a una fórmula válida en el modelo de reales aleatorios.

Debido al teorema 3.3.13 y al corolario 3.3.16, que $\exists y(R_0 y \wedge \chi(y))$ sea válido es equivalente a que exista $\eta \in \mathcal{R}$ tal que $R_0(\eta) = 1$ y $\chi(\eta)$ sea válido, y que $\forall x(R_0 x \Rightarrow \chi(x))$ sea válido es equivalente a que para todo $\xi \in \mathcal{R}$ tal que $R_0(\xi) = 1$, se cumpla $\chi(\xi)$. Por lo tanto, dados $\xi_1, \dots, \xi_n \in \mathcal{R}$ tales que $R_0(\xi_i) = 1$, vamos a probar que existen $\eta_1, \dots \eta_m \in \mathcal{R}$ tales que $R_0(\eta_j) = 1$ y $\phi(\xi_1, \dots \xi_n, \eta_1, \dots, \eta_m)$ es válido.

Por el lema 4.4.1, podemos asumir que cada ξ_i es mezcla de reales constantes con una partición de la unidad. Digamos que $\xi_i = \sum_{a_i \in A_i} a_i \cdot r_{a_i}$. En principio tenemos una anticadena para cada ξ_i, pero se puede hacer que todos usen la misma anticadena de una forma análoga a como se refinan particiones en análisis. Definimos la siguiente anticadena:

$$A := \{a_1 \wedge \dots \wedge a_n \ /\ a_1 \in A_1, \dots, a_n \in A_n,\ a_1 \wedge \dots \wedge a_n \neq 0\}$$

Es claro que sigue siendo una anticadena. Que sigue siendo una partición de la unidad se deduce del segundo item del lema 1.1.3. Cambiamos cada ξ_i por lo siguiente:

$$\xi_i := \sum_{a \in A, a_i \in A_i, a \wedge a_i \neq 0} a \cdot r_{a_i}$$

Para cada $a_i \in A_i$ y cada $a \in A$ tales que $a \wedge a_i \neq 0$, tenemos que $\xi \sim r_{a_i} \geq a$. Por lo tanto, $\xi \sim r_{a_i} \geq \bigvee_{a \wedge a_i \neq 0} a \geq \bigvee_{a \in A}(a \wedge a_i) = a_i$. Con esto deducimos que ξ_i sigue siendo mezcla con anticadena A_i y elementos $\{r_{a_i}\}_{a_i \in A_i}$. Usando el lema 2.2.15 deducimos que el nuevo ξ_i es equivalente al anterior.

A partir de ahora, asumimos que los ξ_i son todos mezclas con la misma anticadena A. Denotamos $\xi_i = \sum_{a \in A} a \cdot r_a^i$. Para cada $a \in A$ y $i = 1, \dots, n$, $\xi_i \sim r_a^i \geq a$. Dado $a \in A$, como $\forall x_1, \dots \forall x_n \exists y_1, \dots \exists y_m \phi(x_1, \dots, x_n, y_1, \dots y_m)$ se cumple en $\mathbb{R}$, existen $s_a^1, \dots, s_a^m \in \mathbb{R}$ tales que $\phi(r_a^1, \dots, r_a^n, s_a^1, \dots s_a^m)$ se cumple en $\mathbb{R}$. Por el lema 4.2.2, si consideramos a $r_a^1, \dots, r_a^n, s_a^1, \dots s_a^m$ como reales aleatorios constantes en $\mathcal{R}$, tenemos que $[\![\phi(r_a^1, \dots, r_a^n, s_a^1, \dots s_a^m)]\!] = 1$. Usaremos las familias $\{s_a^i\}_{a \in A}$ para definir los η_i, de forma análoga a como los ξ_i se vinculan con los $\{r_a^i\}_{a \in A}$. Definimos los η_i mediante mezclas: $\eta_i := \sum_{a \in A} a \cdot s_a^i$

Como son mezclas de reales aleatorios constantes con una partición de la unidad, cumplen $R_0(\eta_i) = 1$, por el lema 4.4.1. Solo resta ver que $[\![\phi(\xi_1, \ldots, \xi_n, \eta_1, \ldots \eta_m)]\!] = 1$. Sea $a \in A$.

$$\begin{aligned} a &= [\![\phi(r_a^1, \ldots, r_a^n, s_a^1, \ldots s_a^m)]\!] \wedge a \\ &\leq [\![\phi(r_a^1, \ldots, r_a^n, s_a^1, \ldots s_a^m)]\!] \wedge \xi_1 \sim r_a^1 \wedge \cdots \wedge \xi_n \sim r_a^n \wedge \eta_1 \sim s_a^1 \wedge \cdots \wedge \eta_m \sim s_a^m \\ &\leq [\![\phi(\xi_1, \ldots, \xi_n, \eta_1, \ldots \eta_m)]\!] \end{aligned}$$

Tomando supremo en $a \in A$ tenemos $[\![\phi(\xi_1, \ldots, \xi_n, \eta_1, \ldots \eta_m)]\!] = 1$. □

Corolario 4.4.4. *El subconjunto R_0 es un subcuerpo de R y además un cuerpo real cerrado.*

Demostración. Se deduce del lema anterior y de que los axiomas de cuerpo real cerrado son de tipo Π_2^R. □

Veamos finalmente que con el espacio de probabilidad usado en el teorema 4.3.3, R_0 es un cuerpo real cerrado incompleto con cardinal estrictamente entre el de los naturales y el de los reales.

Teorema 4.4.5. *Consideramos el modelo de reales aleatorios inducido por el espacio de probabilidad $\Omega = [0,1]^I$ con $I = \mathcal{P}(\mathbb{R})$ y la medida producto, al igual que en el teorema 4.3.3. En este modelo se cumple que R_0 es un subcuerpo real cerrado de R incompleto con cardinal estrictamente entre el de los naturales y el de los reales.*

Demostración. Solo falta demostrar que R_0 es incompleto. Esto significa encontrar un subconjunto de R_0 que tenga supremo que no esté en R_0. Un subconjunto de R_0 es un predicado $\psi \in [\![R \to \texttt{Prop}]\!]$ tal que para todo $\xi \in \mathcal{R}$, $\psi(\xi) \leq R_0(\xi)$, o equivalentemente, por el corolario 3.3.16, que para todos los $\xi \in \mathcal{R}$ tales que $\psi(\xi) = 1$, tengamos $R_0(\xi) = 1$.

Como $\mathcal{R}$ cumple el axioma de completitud, es válida la propiedad arquimediana y por lo tanto todo elemento es el supremo del conjunto de los racionales menores. El predicado que dice que un real aleatorio ξ es racional es $Q(\xi) \equiv \exists n, m(N(n) \wedge N(m) \wedge m \neq 0 \wedge \xi = \frac{n}{m})$. Llamamos χ a la interpretación de ese predicado. Veamos que χ es un subconjunto de $\mathcal{R}_0$.

Sea $\xi \in \mathcal{R}$ tal que $\chi(\xi) = 1$. Por el principio del máximo 3,3,13, existen $\xi_1, \xi_2 \in \mathcal{R}$ tales que $[\![N(\xi_1)]\!], [\![N(\xi_2)]\!] = 1$, $\forall \omega \in \Omega\ \xi_2(\omega) \neq 0$ y $[\![\xi = \frac{\xi_1}{\xi_2}]\!] = 1$. Alcanza probar que $R_0(\frac{\xi_1}{\xi_2}) = 1$. Como $[\![N(\xi_1)]\!], [\![N(\xi_2)]\!] = 1$, por el lema 4.3.2 tenemos que ambos son mezclas de naturales con particiones de la unidad y como $\forall \omega \in \Omega\ \xi_2(\omega) \neq 0$, la mezcla de ξ_2 es con naturales no nulos. Por el argumento usado en la prueba del lema 4.4.3, podemos asumir que las mezclas son con la misma partición de la unidad. Como las mezclas son con partición de la unidad, son únicas salvo equivalencia booleana. Por lo tanto, podemos asumir que ξ_1 y ξ_2 son como las mezclas usadas en la proposición 4.1.4, es decir que tenemos una partición de Ω tal que en cada parte ξ_1 y ξ_2 son constantes. Concluimos que en cada parte de dicha partición $\frac{\xi_1}{\xi_2}$ es constante y por lo tanto $R_0(\frac{\xi_1}{\xi_2}) = 1$.

Dado $\xi \in \mathcal{R}$ consideramos $\psi \in [\![R \to \texttt{Prop}]\!]$ tal que $\psi(\eta) = \chi(\xi) \wedge [\![\eta \leq \xi]\!]$. Por lo mencionado anteriormente, el supremo de ψ es ξ y como para todo $\eta \in \mathcal{R}$, $\chi(\eta) \leq \psi(\eta)$, tenemos que ψ es un subconjunto de $\mathcal{R}_0$. Por lo tanto, si encontramos un $\xi \in \mathcal{R}$ tal que $R_0(\xi) = 0$ terminamos la prueba. Para esto alcanza fijar $i_0 \in I$ y definir ξ como la proyección en esa coordenada, pues para cada $r \in \mathbb{R}$ la preimagen de r por ξ tiene medida nula y por lo tanto $\xi \sim r = 0$. Tomando supremo en r tenemos $R_0(\xi) = 0$. □

Bibliografía

[1] Kurt Gödel. The consistency of the axiom of choice and of the generalized continuum-hypothesis. *Proceedings of the National Academy of Sciences of the United States of America*, 24(12):556, 1938.

[2] Paul Cohen. The independence of the continuum hypothesis. *Proc. Nat. Acad. Sci. USA*, 50(6):1143–1148, 1963.

[3] Paul J Cohen. The independence of the continuum hypothesis, ii. *Proceedings of the National Academy of Sciences*, 51(1):105–110, 1964.

[4] Dana Scott. A proof of the independence of the continuum hypothesis. *Mathematical systems theory*, 1(2):89–111, 1967.

[5] Alonzo Church. A formulation of the simple theory of types. *The journal of symbolic logic*, 5(2):56–68, 1940.

[6] Thomas Jech. *Set theory. The Third Millenium Edition, revised and expanded.* Springer, 2002.

[7] Alfred Tarski. A decision method for elementary algebra and geometry. In *Quantifier elimination and cylindrical algebraic decomposition*, pages 24–84. Springer, 1998.