Notas de Lógica Matemática

Hector Luis Gramaglia

1 Introducción

En este breve apunte vamos a abordar algunos tópicos importantes de Lógica Matemática, la cual se ocupa del estudio del lenguaje y los métodos de razonamiento de la matemática utilizando como herramienta la misma matemática. Nos vamos a concentrar en una formalización de la noción de demostración conocida como *deducción natural de Gentzen-Prawitz*. Existen numerosas formalizaciones de esta noción que poseen todas ellas virtudes diferentes. Algunas tienen como objetivo modelar la actividad del matemático, y permiten emprender de manera sencilla la construcción formal del edificio matemático. Las formalizaciones de este tipo suelen ser bastante extensas ya que tartan de incorporar en forma de "reglas" todos los recursos de los cuales dispone un matemático en su trabajo cotidiano. La deducción natural de Gentzen-Prawitz no se encuentra dentro de este grupo. De hecho una prueba tiene forma de "árbol", en el cual el número de hojas depende exponencialmente de la altura, de manera que la prueba de los resultados más elementales de la aritmética requerirían de un ancho de hoja difícil de encontrar. La virtud de este sistema es sin duda su simpleza, que permite abordar el estudio de ciertas propiedades sintácticas (eliminación de cortes, normalización, etc.) de una manera adecuada. Por otro lado este sistema nos permite "llevar en paralelo" el estudio de cuestiones relativas a las lógicas clásica e intuicionista, debido a que la incorporación de una una sola regla, la reducción al absurdo, permite extender la noción de prueba intuicionista al contexto clásico.

El "hilo conductor" del apunte es la secuencia: "noción de prueba - semántica - corrección y completitud". Esta secuencia será respetada para las lógicas proposicionales clásica e intuicionista. Para el caso intuicionista se introduce la semántica de Kripke, que extiende la semántica clásica dada por las tablas de verdad. Se posterga para el final del apunte la extensión del sistema a los cuantificadores. Se remite al lector a los apéndices para abordar algunas cuestiones de interés, de manera de no distraer el desarrollo de los tópicos fundamentales. Los temas de mayor complejidad son sin duda las nociones de estructuras algebraicas (Sección 7) que nos permiten obtener las pruebas de completitud.

El único prerequisito para la lectura de este material es un curso básico de álgebra, en el cual asumimos que el lector tomo contacto con las nociones de fórmula proposicional y tablas de verdad. Por cuestiones de espacio, no pondremos demasiado enfásis en las definiciones formales de los lenguajes de las respectivas lógicas. Todos los temas, inclusive este último, son acompañado con referencias bibliográficas para que el lector interesado pueda ampliar los contenidos aquívertidos.

2 Contenidos

3 Deducción Natural de Gentzen-Prawitz

En esta sección vamos a introducir el sistema de deducción natural propuesto por Gentzen, cuyo estudio sistemático fue realizado por Prawitz en [10]. Este sistema, originalmente pensado para la lógica intuicionista, se extiende también a la lógica clásica, perdiendo en esta extensión su simpleza original.

La lógica intuicionista es un fragmento de la lógica clásica, y como consecuencia las tautologías intuicionistas son una parte de las tautologías[1] clásicas. Si utilizamos el sistema de deducción natural de Gentzen-Prawist, las tautologías intuicionistas son exactamente las tautologías clásicas que se pueden probar sin utilizar la regla de reducción al absurdo (Sección 5). Una buena manera de entender el significado de los conectivos intuicionista es a través de la interpretación de Brower, Heyting y Kolmogorov, que se describe en el apéndice 2.

En este sistema, una prueba tiene una estructura similar a un árbol, con una sola conclusión situada en la raiz, y con una cantidad finita de hipótesis que se disponen en las hojas. Esta similitud es una ilusión grafica más que una realidad matemática, como veremos a continuación. Usaremos la notación

$$\begin{array}{c} \vdots \\ A \end{array}$$

para designar una *deducción* de A, es decir, una deducción que posee como conclusión la fórmula A. Tal deducción posee en el lugar de las "hojas" fórmulas que pueden tener dos estados: *activas* o *canceladas*. A las activas se las llama *hipótesis* de la deducción de A. Si uno posee una deducción de A que tiene la fórmula B como hipótesis, situación que denotaremos

$$\begin{array}{c} B \\ \vdots \\ A \end{array}$$

entonces mediante la aplicación ciertas *reglas* podemos obtener nuevas deducciones que eventualmente cancelan una o más ocurrencias de B de la deducción primitiva. El caso típico de cancelación se puede observar en la regla de introducción del $\Rightarrow$:

$$\dfrac{\begin{array}{c}[B] \\ \vdots \\ A\end{array}}{B \Rightarrow A}$$

Según esta regla, partiendo de la deducción de A podemos elegir una cantidad arbitraria (que puede ser 0) de ocurrencias de B como hipótesis y generar una nueva dedución que tiene como conclusión a $B \Rightarrow A$ en la cual las ocurrencias escogidas de B son canceladas. Podría no existir ninguna ocurrencia activa de B con lo cual no hay nada por cancelar. Se suele utilizar un índice natural para vincular las hipótesis descartadas con el "nodo" en el cual se las canceló:

$$\dfrac{\begin{array}{c}[B]^1 \\ \vdots \\ A\end{array}}{B \Rightarrow A}{\scriptstyle (1)}$$

Note que puede utilizarse el mismo índice para cancelar hipótesis distintas, ya que tal aparente ambiguedad queda resuelta observando los antecedentes de las implicaciones involucradas.

La deducción más elemental es la de la forma:

[1] En la lógica proposicional clásica una *tautología* es una fórmula cuya tabla de verdad dá en todos los casos *verdadero*.

HIPOTESIS: A

Esta consiste en una conclusión A que a la vez es su hipótesis. Para cada conectivo tenemos reglas de *introducción* y de *eliminación* para construir nuevas deducciones a partir de otras ya existentes. Estas son:

REGLAS DE INTRODUCCION

$$\frac{\begin{array}{cc}\vdots & \vdots \\ A & B\end{array}}{A \wedge B}\,\wedge I \qquad \frac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \Rightarrow B}\,\Rightarrow I$$

$$\frac{\begin{array}{c}\vdots \\ A\end{array}}{A \vee B}\,\vee I1 \qquad \frac{\begin{array}{c}\vdots \\ B\end{array}}{A \vee B}\,\vee I2$$

REGLAS DE ELIMINACION

$$\frac{\begin{array}{c}\vdots \\ A \wedge B\end{array}}{A}\,\wedge E \qquad \frac{\begin{array}{c}\vdots \\ A \wedge B\end{array}}{B}\,\wedge E \qquad \frac{\begin{array}{cc}\vdots & \vdots \\ A \Rightarrow B & A\end{array}}{B}\,\Rightarrow E$$

$$\frac{\begin{array}{ccc} & [A] & [B] \\ \vdots & \vdots & \vdots \\ A \vee B & C & C\end{array}}{C}\,\vee E$$

Finalmente tenmos una regla más:

REGLA DE ELIMINACION DEL $\perp$

$$\frac{\begin{array}{c}\vdots \\ \perp\end{array}}{B}\,\perp E$$

Note que al igual que en la introducción del $\Rightarrow$, en la aplicación de $\vee E$ se descartan tantas ocurrencias como se quiera de la hipótesis A en la deducción subordinada

$$\begin{array}{c} A \\ \vdots \\ C \end{array}$$

Lo mismo con la hipótesis B. En el sistema de deducción natural no hay reglas para la negación $\neg$, puesto que se considera $\neg A$ como otra forma de escribir $A \Rightarrow \perp$.

La lógica intuicionista rompe con la dualidad $\vee - \wedge$ existente en la lógica clásica, y que se expresa a través de las denominadas leyes de De Morgan. En efecto, la sentencia

$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$$

puede ser probada, mientras que para la sentencia dual sólo vale un implica:

$$\neg A \vee \neg B \Rightarrow \neg(A \wedge B).$$

Como ejemplo damos una deducción de esta última proposición, que envuelve una aplicación de la regla de eliminación del $\vee$. Esta regla posee una característica particular: la fórmula C no guarda ninguna relación con la fórmula principal que contiene al conectivo en cuestión.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg A]^3 \quad \dfrac{[A \wedge B]^2}{A}\wedge E1}{\bot} \quad \dfrac{[\neg B]^3 \quad \dfrac{[A \wedge B]^2}{B}\wedge E2}{\bot}}{\bot}}{\dfrac{\neg(A \wedge B)}{\neg A \vee \neg B \Rightarrow \neg(A \wedge B)}\,(1)\Rightarrow I}\,(2)\Rightarrow I}{[\neg A \vee \neg B]^1}\,(3)\vee E$$

Una exposición clara y de muy amena lectura del sistema de deduccion natural que describimos en este apunte puede encontrarse en [5] y [6]. El mismo libro de Prawits puede ser también consultado [10].

Exercise 1 *Pruebe que existe una deducción utilizando el fragmento* $(\Rightarrow, \wedge, \bot)$ *para las siguientes sentencias:*

1. $A \Rightarrow A$
2. $\bot \Rightarrow A$
3. $A \wedge \neg A \Rightarrow \bot$
4. $A \Rightarrow (B \Rightarrow A)$
5. $A \Rightarrow \neg\neg A$
6. $A \Rightarrow (\neg A \Rightarrow B)$

Exercise 2 *Pruebe que existe una deducción para las siguientes sentencias:*

1. $(A \Rightarrow (B \Rightarrow C)) \Longleftrightarrow (A \wedge B \Rightarrow C)$[2]
2. $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$
3. $\neg A \vee \neg B \Rightarrow \neg(A \wedge B)$
4. $\neg A \vee B \Rightarrow (A \Rightarrow B)$
5. $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$
6. $A \wedge \neg B \Rightarrow \neg(A \Rightarrow B)$

4 Algunas propiedades sintácticas relevantes

En esta sección nos restringiremos al fragmento del sistema de deducción natural dado por las reglas de introducción y eliminación de $\Rightarrow$ y $\wedge$. Aunque las propiedades que vamos a estudiar son válidas en el sistema completo, en este fragmento las bondades de la sintaxis las revelan de una forma sencilla.

Las propiedades que aquínos interesan son de relevancia en el desarrollo de métodos automáticos de pruebas, y no se limitan de ninguna manera al sitema de deducción natural ni a la lógica intuicionista.

Cualquiera que adquiera suficiente experiencia en hacer deducciones naturales puede llegar a observar que evitando casos de "introducción" seguida de "eliminación" de un conectivo puede

[2] $A \Leftrightarrow B$ es una abreviación para $(A \Rightarrow B) \wedge (B \Rightarrow A)$

"achicar" pruebas. Tal es el caso de la deducción:

$$\dfrac{\dfrac{\dfrac{\dfrac{[A \wedge B]^1}{A}\wedge E1}{B \Rightarrow A}\Rightarrow I \qquad \dfrac{[A \wedge B]^1}{B}\wedge E2}{\dfrac{A}{C \Rightarrow A}\Rightarrow I}\Rightarrow E}{(A \wedge B) \Rightarrow (C \Rightarrow A)}(1)\Rightarrow I$$

que puede reducirse a:

$$\dfrac{\dfrac{\dfrac{[A \wedge B]^1}{A}\wedge E1}{C \Rightarrow A}\Rightarrow I}{(A \wedge B) \Rightarrow (C \Rightarrow A)}(1)\Rightarrow I$$

Esta noción de reducción puede formalizarse de la siguiente manera. Una ocurrencia de una fórmula A en una deducción natural se dice un *corte* si ella es la conclusión de una regla de introducción, y a su vez la premisa principal de una regla de eliminación. Las *premisas* son las fórmulas que estan inmediatamente arriba de la linea horizontal que define una regla, y por *premisa principal* de una regla de eliminación entendemos aquella premisa que tiene como conectivo principal el que se elimina. Por ejemplo en la derivación de arriba (la primera) la única ocurrencia de $B \Rightarrow A$ es un corte. La noción de corte nos permite definir una noción de *conversión* de pruebas que consiste en eliminar la secuencia introducción-eliminación:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ A\end{array}}{B \Rightarrow A}\Rightarrow I \qquad \begin{array}{c}\vdots\\ B\end{array}}{\begin{array}{c}A\\ \vdots\end{array}}\Rightarrow E \qquad \text{convierte a} \qquad \begin{array}{c}\vdots\\ A\\ \vdots\end{array}$$

$$\dfrac{\dfrac{\begin{array}{cc}\vdots & \vdots\\ A & B\end{array}}{A \wedge B}\wedge I1}{\begin{array}{c}A\\ \vdots\end{array}}\Rightarrow E \qquad \text{convierte a} \qquad \begin{array}{c}\vdots\\ A\\ \vdots\end{array}$$

Decimos que una deducción de A es *normal* si no posee cortes. Decimos que una deducción $\mathcal{D}$ *reduce* a otra deducción $\mathcal{D}'$ si $\mathcal{D}'$ se obtiene desde $\mathcal{D}$ a través de un número finito de pasos de conversión. La siguiente propiedad se denomina *propiedad de normalización débil:*

Theorem 3 *Toda deducción puede ser "normalizada" mediante una reducción.*

Las deducciones normales poseen una propiedad asombrosa, llamada *propiedad de la subfórmula*:

Theorem 4 *Toda fórmula que ocurre en una deduión normal de A es una subfórmula de A o de alguna hipótesis.*

Una consecuencia notable de esta propiedad es la *decidibilidad* de este fragmento del sistema de deducción natural, o sea podemos dar un "algoritmo" que dada una fórmula A permite determinar si existe o no una deducción de A. En efecto, si existe una deducción de A entonces existe también una deducción normal de A. Pero por la propiedad de la súbformula existe sólo una cantidad

finita de fórmulas que pueden eventualmente formar parte de tal deducción. Claro que una misma fórmula puede ocurrir varias veces, en efecto consideremos el caso de la siguiente prueba normal:

$$\dfrac{\dfrac{\dfrac{[A]^2 \quad [A \Rightarrow A]^1}{A}\wedge E1}{A \Rightarrow A}(2)\ \Rightarrow I}{(A \Rightarrow A) \Rightarrow (A \Rightarrow A)}(1)\ \Rightarrow I \qquad (1)$$

Más aún, por encima de la ocurrencia de $[A]^2$ se puede reproducir la aplicación de $\wedge E1$ tantas veces como se quiera. Esto dá una pista de como solucionar el problema: podemos "achicar" una prueba de manera que en una misma rama (desde la raiz hasta una hoja) no ocurra dos veces la misma fórmula. La deducción de arriba puede ser "achicada" de la siguiente manera:

$$\dfrac{\dfrac{\dfrac{[A]^2}{A \Rightarrow A}(2)\ \Rightarrow I}{(A \Rightarrow A) \Rightarrow (A \Rightarrow A)}(1)\ \Rightarrow I \qquad (0)$$

Luego dada una cantidad finita de fórmulas tenemos sólo una cantidad finita de "árboles" que no repiten fórmulas en una misma rama. En consecuencia basta con generar todos esos "candidatos" a deducción y testear si alguno efectivamente lo es.

La noción de prueba normal en este fragmento del cálculo puede considerarse como una formalización de la noción genérica de semántica constructivista propuesta por Brower, Heyting y Kolmogorov, y que brevemente se introduce en el apéndice 2. Allítambién estudiamos un asombroso significado operacional que queda oculto en la noción de normalización, y que se revela a través del isomorfismo de Curry-Howard, que conecta la noción de demostración con los términos del Cálculo Lambda Tipado.

Al extender los conceptos vertidos en esta sección al resto del cálculo nos enfrentamos a ciertas deficiencias en la sintaxis que originan la llamadas *conmuting conversions*. Tal patología se presenta en la regla de eliminación del existe. Por ejemplo, la derivación de la sección anterior puede reescribirse:

$$\dfrac{\dfrac{[\neg A \vee \neg B]^1 \qquad \dfrac{\dfrac{[\neg A]^3 \quad \dfrac{[A \wedge B]^2}{A}\wedge E1}{\bot}(2)\ \Rightarrow I}{\neg(A \wedge B)} \qquad \dfrac{\dfrac{[\neg B]^3 \quad \dfrac{[A \wedge B]^2}{B}\wedge E2}{\bot}(2)\ \Rightarrow I}{\neg(A \wedge B)}}{\neg(A \wedge B)}(3)\ \vee E}{\neg A \vee \neg B \Rightarrow \neg(A \wedge B)}(1)\ \Rightarrow I$$

Luego se deben considerar clases de equivalencia de pruebas "modulo" las conmuting conversions.

Un exposición detellada de los temas tratados en esta sección se puede encontrar en los textos [12] y [5].

Exercise 5 *Para cada deducción realizada en la sección anterior analice cuales son normales y normalice las que no lo sean.*

5 Deducción Natural para la lógica clásica

Para extender el sistema a la lógica clásica agregamos una regla que "fortelece" le eliminación del $\bot$ (ver $\bot E$ en la sección anterior), permitiendo que en su aplicación se descarten ocurrencias de

$\neg B$. Esta nueva regla se denomina *reducción al absurdo (reductio ad absurdum)*:

$$\dfrac{\begin{array}{c}[\neg B]\\ \vdots\\ \bot\end{array}}{B}\ RAA$$

Esta regla nos permite obtener pruebas para algunas sentencias no aceptadas por la lógica intuicionista como por ejemplo $\neg\neg A \Rightarrow A$:

$$\dfrac{\dfrac{\dfrac{[\neg A]^1 \qquad [\neg\neg A]^2}{\bot}\Rightarrow E}{A}(1)\ RAA}{\neg\neg A \Rightarrow A}(2)\ \Rightarrow I$$

Como se demustra en los ejercicios, la sóla inclusión de esta regla recupera la dualidad $\vee - \wedge$ manifestada por las leyes de De Morgan.

Una exposición clara del sistema clásico de Deducción natural puede encontrarse en [12]. Otros sistemas de demostración para la lógica proposicional clásica que revisten mucho interés desde el punto de vista de la prueba automática de teoremas pueden encontrarse en [4]. En los libros clásicos de lógica suele utilizarse un estilo de prueba denominado *estilo Hilbert*, y que consisten en formular axiomas proposicionales y luego utilizar solamente la regla de eliminación del implica ($\Rightarrow E$), usualmente llamada *Modus Ponens* [9], [3].

Exercise 6 *Utilice RAA para obtener deducciones de:*

1. $\neg(A \wedge B) \Rightarrow \neg A \vee \neg B$
2. $(A \Rightarrow B) \Rightarrow \neg A \vee B$
3. $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$
4. $\neg(A \Rightarrow B) \Rightarrow A \wedge \neg B$

Exercise 7 *Supongamos que tenemos una deducción de* $\vdash \neg A \wedge \bigwedge \Gamma \Rightarrow \bot$[3]*, donde* Γ *es un conjunto finito de fórmulas. Encuentre una deducción para* $\Gamma \vdash A$.

6 Semántica de Kripke

En esta sección vamos a describir una formalización del significado de los conectivos intuicionistas que fue propuesta por Kripke. De manera informal, un modelo de Kripke es un conjunto K de "estados posibles de conocimiento" que son vinculados por el tiempo: $k \leq k'$ significa "k' es un tiempo posterior a k". Por otro lado se cuenta con la relación $k \Vdash X$ que significa "X es establecido (probado, conocido, etc.) en el estado k". Por supuesto, si una sentencia es conocida en un tiempo, lo es en todo tiempo futuro. En símbolos,

$$k \Vdash X \text{ y } k' \geq k \text{ entonces } k' \Vdash X. \qquad (*)$$

Formalmente, un *modelo de Kripke* será un triple $(K, \leq, \Vdash)$ donde K es un conjunto cuyos elementos son llamados *nodos*, $\leq$ es un orden parcial[4], y $\Vdash$ es una relación binaria que vincula elementos de K con variables proposicionales, y que satisface $(*)$.

La relación $\Vdash$ se extiende a las fórmulas: definiremos que significa $k \Vdash A$. De esta manera damos significado formal a los conectivos intuicionistas, y tenemos por añadidura las nociones de "validez" y "tautología", a saber:

[3] $\bigwedge \Gamma = \bigwedge_{\gamma \in \Gamma} \gamma$

[4] = relación binaria reflexiva, antisimétrica y transitiva.

- A es válida en el modelo $(K, \leq, \Vdash)$ si para todo $k \in K$ se tiene $k \Vdash A$,
- A es tautología si es válida en todo modelo de Kripke.

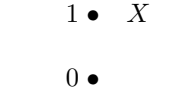
La definición de $k \Vdash A$ se efectua sobre la estructura de las fórmulas. Si A es una variable proposicional, su definición está dada por la relación $\Vdash$ del modelo. Los casos $\wedge$ y $\vee$ no presentan dificultades:

$k \Vdash B \wedge C$ si y sólo si $k \Vdash B$ y $k \Vdash B$,
$k \Vdash B \vee C$ si y sólo si $k \Vdash B$ ó $k \Vdash B$.

El caso $\Rightarrow$ introduce una interpretación original:

$k \Vdash B \Rightarrow C$ si y sólo si para todo $k' \geq k$, si $k' \Vdash B$ entonces $k' \Vdash C$.

En particular, $k \Vdash \neg A$ si y sólo si A no se establece en ningún futuro, ni por supuesto en el estado presente k. Note de que manera esta definición descarta la sentencia $\neg\neg A \Rightarrow A$. Consideremos el modelo $(\{0, 1\}, \leq, \Vdash)$, donde $0 \leq 1$ y $\Vdash$ relaciona únicamente al par $(1, X)$:



Veremos que $\neg\neg X \Rightarrow X$ no es válida en este modelo. En particular, veremos que $0 \nVdash \neg\neg X \Rightarrow X$. En efecto, en 0 se establece $\neg\neg X$ pero no se establece X. Ver que en 0 se establece $\neg\neg X$ requiere que para todo $k \geq 0$ no se establezca $\neg X$. Pero como X se establece en 1, entonces en todo nodo menor o igual a 1 no se establece $\neg X$.

Note que las valuaciones pueden verse como modelos de Kripke con un solo nodo 0, en donde se asigna valor 1 a las variables X que satisfacen $0 \Vdash X$. Más aún, en este caso la noción de validez en el modelo de Kripke coincide con la noción de validez de las tablas de verdad. Luego podemos decir que la semántica intuicionista dada por los modelos de Kripke se obtiene "incorporando" nuevos modelos a la semántica clásica.

Una exposición de la semántica de Kripke para la lógica de primer orden intuicionista se detalla en [12]. Por otro lado en [7] se estudian muchas lógicas de interés en las Ciencias de la Computación (modales, temporales, etc.) para las que se define una semántica de este estilo, usualmente denominada *semántica de los mundos posibles.*

Exercise 8 *Para cada una de las siguientes fórmulas encuentre modelos de Kripke que no las satisfagan.*

1. $\neg(A \wedge B) \Rightarrow \neg A \vee \neg B$
2. $(A \Rightarrow B) \Rightarrow \neg A \vee B$
3. $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$
4. $\neg(A \Rightarrow B) \Rightarrow A \wedge \neg B$

Exercise 9 *Pruebe que la relación extendida $\Vdash$ es monótona, o sea que si $k \Vdash A$ y $k \leq l$ entonces $l \Vdash A$.*

7 Corrección y completitud

Si Γ es un conjunto de fórmulas, utilizaremos la notación $\Gamma \vdash A$ para denotar que existe una deducción de A con hipótesis en Γ (según el contexto sabremos si se trata de una deducción en la lógica clásica o intuicionista). Si Γ es vacío escribimos simplemente $\vdash A$.

Para referirnos a la semántica utilizaremos simplemente el término *modelo,* y su significado dependerá del contexto. En la lógica clásica será una valuación (o sea un modelo de Kripke de

un solo nodo), y en la intuicionista será un modelo de Kripke arbitrario. Al final de la sección el lector encontrará un glosario que indica el significado en cada lógica de cada vocablo o notación utilizados.

$\Gamma \models A$ denota que para todo modelo, si cada fórmula de Γ es cierta, entonces A es cierta[5].

En esta sección Probaremos los siguientes Teoremas:

Theorem 10 ***(Corrección)*** *Si* $\Gamma \vdash A$ *entonces* $\Gamma \models A$.

Theorem 11 ***(Completitud)*** *Si* $\Gamma \models A$ *entonces* $\Gamma \vdash A$.

La prueba del Teorema de Corrección se realiza mediante una inducción sobre la estructura de las pruebas[6]. Por supuesto, la prueba es más dificultosa en el caso intuicionista, al que nos referiremos brebemente. Probaremos que para todo modelo $\mathcal{K} = (K, \leq, \Vdash)$ y para todo $k \in K$, si $k \Vdash B$ para todo $B \in \Gamma$ entonces $k \Vdash A$. (Note que ésta es una hipótesis inductiva un poco más fuerte que la alternativa obvia: si B es cierto en $\mathcal{K}$ para todo $B \in \Gamma$, entonces A es cierto en $\mathcal{K}$.) Vamos a efectuar el caso paradigmático $\Rightarrow I$. Supongamos que A es $C \Rightarrow D$, y que la prueba es de la forma:

$$\begin{array}{c} [C] \\ \vdots \\ \dfrac{D}{C \Rightarrow D} \end{array}$$

Sea $\mathcal{K} = (K, \leq, \Vdash)$ un modelo de Kripke y sea $k \in K$ tal que $k \Vdash B$ para todo $B \in \Gamma$, probaremos que $k \Vdash C \Rightarrow D$, o sea que para todo $l \geq k$, si $l \Vdash C$ entonces $l \Vdash D$. Tomemos $l \geq k$ tal que $l \Vdash C$. Como la relación extendida $\Vdash$ es monótona (Ejercicio 9), tenemos que en l se satisfacen todas las hipótesis de la deducción subordinada

$$\begin{array}{c} C \\ \vdots \\ D \end{array}$$

Luego, por hipótesis inductiva, $l \Vdash D$. $\square$

El Teorema de completitud exige un poco más de trabajo, tanto el "clásico" como el "intuicionista". Ambos se efectuan de acuerdo al mismo esquema sencillo: se supone $\Gamma \nvdash A$ y luego se define un modelo que satisfaga Γ y no satisfaga A (o sea se prueba el contrarecíproco[7]). El resto de la sección será utilizada para construir tal modelo para ambas lógicas. Para ésto debemos introducir algunas nociones relativas a las estructuras algebraicas que surgen de la Lógica. En cada lógica subyace un álgebra, denominada álgebra de Lindembaun, que es en realidad un reticulado distributivo con otras operaciones, dependiendo éstas de la lógica en cuestión. Encontraremos el modelo deseado a partir del álgebra de Lindembaun, mediante la aplicación de un teorema fundamental de la teoría de los reticulados distributivos llamado *Teorema del Filtro Primo.*

Sea L un conjunto no vació, y sea $\leq$ un orden parcial en L (o sea una relación binaria reflexiva antisimétrica y transitiva). Diremos que $(L, \leq)$ es un *reticulado* si existen ambos, el supremo[8] y

[5] En la lógica intuicionista suele usarse el símbolo $\Vdash$.

[6] Este tipo de inducción, llamada estructural, es muy común cuando se manipulan lenguajes formales de cualquier índole.

[7] Pero $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$ no es una tautología intuicionista! Esto no implica que adoptemos una posición filosófica inconsistente. Nuestra adhesión a la lógica clásica es completa y sólo estudiamos la lógica intuicionista como un objeto matemático interesante.

[8] = mínima cota superiror.

el infimo[9], de todo par de elementos. La estructura de reticulado tiene un existencia dual, como conjunto ordenado y como estructura algebraica. En efecto, un reticulado podría ser definido como una estructura $(L, \wedge, \vee)$ tal que L es un conjunto no vacío y $\wedge, \vee$ son dos operaciones binarias que satisfacen las siguientes ecuaciones:

$$\begin{array}{cc} (x \vee y) \vee z = x \vee (y \vee z) & (x \wedge y) \wedge z = x \wedge (y \wedge z) \\ x \vee y = y \vee x & x \wedge y = y \wedge x \\ x \vee x = x & x \wedge x = x \\ x \vee (x \wedge y) = x & x \wedge (x \vee y) = x \end{array}$$

Estas leyes son denominadas *asociatividad, conmutatividad, idempotencia* y *absorción*, en ese orden. La equivalencia de estas dos definiciones queda como ejercicio. Para probar que en toda estructura $(L, \wedge, \vee)$ que satisface los axiomas subyace un reticulado debemos definir

$$x \leq y \Leftrightarrow x \vee y = y.$$

Un reticulado se dice *distributivo* si además satisface las leyes:

$$\begin{array}{c} (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) \\ (x \wedge y) \vee z = (x \vee z) \wedge (y \vee z) \end{array}$$

Un subconjunto no vacío $F \subseteq L$ se dice *filtro* si es creciente y cerrado para el $\wedge$, o sea:
- $x \in F$, $x \leq y$ implica $y \in F$
- $x \in F$, $y \in F$ implican $x \wedge y \in F$.

Un filtro P se dice *propio* si está contenido estrictamente en L. Por último, un filtro propio P se dice *primo* si cada vez que $x \vee y \in P$ se tiene que $x \in P$ o $y \in P$.

Theorem 12 ***(Filtro Primo)*** *Si Γ es un subcunjunto del reticulado distributivo L, y x es un elemento tal que para todo $x_1, ..., x_n \in \Gamma$ se tiene*

$$x_1 \wedge ... \wedge x_n \not\leq x,$$

entonces existe un filtro primo P tal que $\Gamma \subseteq P$ y $x \notin P$.

Para la algebrización de las lógicas clásica e intuicionista debemos considerar expansiones de reticulados distributivos. Ante todo son *reticulados distributivos con* 0, o sea son estructuras de la forma $(L, \vee, \wedge, 0)$ donde 0 es el mínimo de L ($false$ o $\bot$).

La algebrización de la lógica clásica se completa considerando la expansión $(L, \vee, \wedge, 0, 1, ^c)$, donde 1 representa al máximo elemento de L, mientras que x^c representa al complemento de x, o sea se satisfacen los axiomas

$$x \vee x^c = 1 \qquad x \wedge x^c = 0.$$

Por otro lado en la lógica intuicionista tenemos el $\Rightarrow$ (recordemos que $\neg A$ no es otra cosa que $A \Rightarrow \bot$). Desde el punto de vista algebraico, el implica se introduce como una operación binaria $\rightarrow$ denominada *complemento relativo*. Definamos esto de manera precisa. Sea L un reticulado distributivo con 0 y sea $x, y \in L$. Si existe un mayor elemento z satisfaciendo la propiedad $x \wedge z \leq y$, decimos que tal elemento es el complemento relativo de x respecto de y, y lo denotamos $x \rightarrow y$. Una estructura $(L, \vee, \wedge, 0 \rightarrow)$ se dice un álgebra de *Heyting* si $(L, \vee, \wedge, 0)$ es un reticulado distributivo con 0 y $x \rightarrow y$ es el complemento relativo de x respecto de y, para todo $x, y \in L$.

El Álgebra de Lindembaun está formada por clases de fórmulas que se prueban equivalentes (según la noción de prueba en cuestión). Para el caso clásico será un álgebra de Boole, mientras

[9]= máxima cota inferior

que en el intuicionista será un álgebra de Heyting . Vamos a definir en detalle esta álgebra. Utilizamos la notación

$$A \sim B$$

para denotar

$$\vdash (A \Rightarrow B) \wedge (B \Rightarrow A).$$

Queda como ejercicio para el lector demostrar que $\sim$ es una relación de equivalencia, tanto para la deducción clásica como para la intuicionista. Sea $\mathcal{L}$ el conjunto tales clases de equivalencia (es decir el cociente del conjunto de fórmulas por la relación $\sim$). Mediante $[A]$ denotamos a la clase de equivalencia de A según $\sim$. Si consideramos la noción de deducción intuicionista podemos dar a $\mathcal{L}$ una estructura de álgebra de Heyting definiendo:

$$\begin{array}{ccc} 0 & =_{def} & [\bot] \\ [A] \wedge [B] & =_{def} & [A \wedge B] \\ [A] \vee [B] & =_{def} & [A \vee B] \\ [A] \rightarrow [B] & =_{def} & [A \Rightarrow B] \end{array}$$

Similarmente, si consideramos la noción de prueba clásica y definimos

$$\begin{array}{ccc} 1 & =_{def} & [A \vee \neg A] \\ [A]^c & =_{def} & [\neg A] \end{array}$$

tenemos una estructura de álgebra de Boole. Ambas cosas quedan como ejercicio.

Nuestro modelo se construye de una forma sencilla a partir de los filtros primos de $\mathcal{L}$. *Cada filtro primo P define una valuación*: en efecto a cada variable proposicional X le damos el valor de verdad "$[X] \in P$" (o sea vale 1 si y sólo si $[X] \in P$) . En el contexto de la lógica clásica utilizamos la notación $Q \Vdash A$ para denotar que A es cierto en la valuación asociada al filtro primo Q.

Por otro lado, *cada filtro primo P define un modelo de Kripke*: el modelo $(K, \subseteq, \Vdash)$ donde

$$\begin{array}{ccc} K & =_{def} & \{Q : Q \text{ es filtro primo y } P \subseteq Q\} \\ Q \Vdash X & \Leftrightarrow_{def} & [X] \in Q \end{array}$$

En el contexto de la lógica intuicionista $Q \Vdash A$ tiene su significado que surge del hecho que Q es un nodo de K.

El modelo buscado en la prueba de completitud surge del siguiente lema:

Lemma 13 *Para todo filtro primo P de $\mathcal{L}$ se tiene: $P \Vdash A$ si y sólo si $[A] \in P$.*

La prueba de este lema se efectua en el Apéndice 2.

Ahora si estamos en condiciones de terminar la prueba del Teorema de Completitud. Si $\Gamma \nvdash A$ entonces $[A_1 \wedge ... \wedge A_n] \nleq [A]$ para todo $A_1, ..., A_n \in \Gamma$, pues en otro caso tendríamos por definición de $\sim$ una deducción de $\vdash A_1 \wedge ... \wedge A_n \Rightarrow A$ (ver ejercicio 23), lo que nos permitiría completar una prueba de $\Gamma \vdash A$:

$$\dfrac{\begin{array}{cc} & \Gamma \\ \vdots & \vdots \\ A_1 \wedge ... \wedge A_n \Rightarrow A & A_1 \wedge ... \wedge A_n \end{array}}{A}$$

En consecuencia, por el Teorema del Filtro Primo existe un filtro primo P tal que $[B] \in P$ para todo $B \in \Gamma$ y $[A] \notin P$. Luego por el lema se tiene que $P \Vdash B$, para todo $B \in \Gamma$, y que $P \nVdash A$. Por lo tanto el modelo inducido por P en cada una de las respectivas lógicas es el modelo buscado.

Es bastante usual que las pruebas de completitud sean dadas ocultando las estructuras algebraicas subyacentes, como por ejemplo en [12], [4]. Buenos textos de teoría de reticulados son [1], [2], [8].

RESUMEN DE NOTACIÓN:

LÓGICA CLÁSICA:
modelo: valuación o lo que es lo mismo, modelo de Kripke de un sólo nodo.
$\Gamma \vdash A$: deducción utilizando eventualmente RAA.
$\mathcal{L}$: Álgebra de Boole formada por las clases de equivalencia según $\sim$.
$P \Vdash A$: la proposición A es verdadera en la valuación inducida por P.

LÓGICA INTUICIONISTA:
modelo: modelo de Kripke arbitrario.
$\Gamma \vdash A$: deducción sin utilizar RAA.
$\mathcal{L}$: Álgebra de Heyting formada por las clases de equivalencia según $\sim$.
$P \Vdash A$: la proposición A es verdadera en el nodo P del modelo de kripke inducido por P.

Exercise 14 *Complete la prueba de corrección para la deducción intuicionista.*

Exercise 15 *Pruebe la corrección para la deducción clásica.*

Exercise 16 *En un álgebra de Heyting todo elemento es complementado?*

Exercise 17 *En un reticulado distributivo $(L, \wedge, \vee, 0)$ el pseudocomplemento de x es el máximo elemento z (si existe) que satisface $x \wedge z = 0$. Pruebe que:*
a. en las álgebras de Boole el pseudocomplemento es exactamente el complemento,
b. en las álgebras de Heyting siembre existe el pseudocomplemento.

Exercise 18 *Pruebe el Teorema del Filtro Primo utilizando el Lema de Zorn.*

Exercise 19 *Pruebe que si L es un álgebra de Boole y P un filtro primo entonces para todo x se tiene $x \in P$ o $x^c \in P$.*

Exercise 20 *Pruebe que en un álgebra de Heyting la operación $\rightarrow$ queda determinada por los axiomas:*

$$x \wedge (x \rightarrow y) = x \wedge y$$
$$x \wedge (y \rightarrow z) = x \wedge (x \wedge y \rightarrow x \wedge z)$$
$$z \wedge (x \wedge y \rightarrow x) = z$$

Exercise 21 *Pruebe que $\sim$ es una relación de equivalencia.*

Exercise 22 *Pruebe que $\mathcal{L}$ con las operaciones definidas arriba tiene estructura de álgebra de Heyting o de Boole, según el caso.*

Exercise 23 *Pruebe que si $A_1, ..., A_n \vdash A$ entonces en $\mathcal{L}$ se tiene $[A_1 \wedge ... \wedge A_n] \leq [A]$.*

8 Los cuantificadores

Las reglas de introducción y eliminación de $\forall$ y $\exists$ exigen un cuidado especial por los fenómenos de captura de variables que son típicos en la manipulación de cuantificadores. Una ocurrencia de x en una fórmula A se dice *acotada* si se encuentra bajo el alcance de un cuantificador. Por ejemplo si A es la fórmula

$$\forall y\ (\forall x\ x = y) \Rightarrow (x + z > y)$$

entonces la primera ocurrencia de x después de $\forall x$ es acotada mientras la segunda no lo es. A una ocurrencia no acotada se le llama *libre*. En todo razonamiento matemático es típico que se efectuen *sustituciones* de variables por términos. Por ejemplo, si se conoce la sentencia sobre números enteros $\forall x\ A(x)$, se pueden utilizar las fómulas $A(0)$, $A(y)$, $A(2 * x + 1)$, etc. Estas

sustituciones deben ser hechas con cuidado para no llegar a distorciones absurdas. Por ejemplo si $A(x)$ es

$$(\forall y\ x = y) \Rightarrow (0 = 1)$$

y se sustituye x por y entonces obtenemos la afirmación

$$(\forall y\ y = y) \Rightarrow (0 = 1)$$

con lo cual hemos probado que $0 = 1$. Lo que aquíocurre es que la variable y del término que se "introduce" (que en este caso es el mismo y) queda *capturada* por un cuantificador $\forall$. Para prevenir este fenómeno cada vez que se efectua una sustitución de x por t se requiere que x *sea libre para* t en A, o sea que toda ocurrencia libre de x en A no se encuentre afectada por cuantificaciones sobre variables que aparecen en t.

Vamos ahora a dar las reglas del cuantificador $\forall$.

REGLA DE INTRODUCCIÓN DE $\forall$:

$$\dfrac{\begin{array}{c}\vdots\\ A\end{array}}{\forall x\ A}\forall I$$

con la restricción de que x no debe ocurrir libre en ningúna hipótesis de la deducción subordinada de A.

REGLA DE ELIMINACIÓN DE $\forall$:

$$\dfrac{\begin{array}{c}\vdots\\ \forall x\ A\end{array}}{A[t/x]}\forall E$$

Aquí$A[t/x]$ denota la sustitución de x por t y para esto x debe ser libre para t en A.

La restricción de la regla de introducción es necesaria, como lo muestra el siguiente ejemplo, en el cual se la ignora:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x = 0]^1}{\forall x\ x = 0}\forall I}{x = 0 \Rightarrow \forall x\ (x = 0)}(1)\Rightarrow I}{\forall x\ (x = 0 \Rightarrow \forall x\ (x = 0))}\forall I}{0 = 0 \Rightarrow \forall x\ (x = 0)}\forall E$$

Las reglas del conectivo $\exists$ reproducen un fenómeno similar al del $\vee$ debido a que requiere la incorporación de una fórmula que no tiene ninguna relación que la fórmula que contiene al conectivo que se elimina.

REGLA DE INTRODUCCIÓN DE $\exists$:

$$\dfrac{\begin{array}{c}\vdots\\ A[t/x]\end{array}}{\exists x\ A}\exists I$$

Aquíx debe ser libre para t en A.

REGLA DE ELIMINACIÓN DE $\exists$:

$$\dfrac{\exists x\ A \qquad \begin{array}{c}[A]\\ \vdots\\ B\end{array}}{B}\ \exists E$$

Aquíse exige que x no sea libre en B ni en ninguna hipótesis de la deducción subordinada de B, excepto A.

La restricción de la regla de eliminación del $\exists$ es necesaria, como lo muestra el siguiente ejemplo en el cual se la ignora:

$$\dfrac{\dfrac{\exists x\ x=0 \qquad [x=0]^1}{x=0}\ (1)\ \exists E}{\forall x\ x=0}\ \forall I$$

En [12], [5], [6] se exponen las reglas de la manera en que fueron dadas aquí. Existen muchos otro excelentes libros de lógica en los cuales se brindan nociones de demostración más complejas pero que modelan de manera más adecuada la actividad del matemático, como por ejemplo [3], [9]. En [4] se estudian varios métedos de demostración para la lógica de primer orden ligados a la prueba automática de teoremas.

Exercise 24 *Determine cuando x es libre para t en A :*
1. $t = z + x * y,\ A = (\forall y \forall x\ x = y) \Rightarrow (x + z > y)$
2. $t = z + x,\ A = \forall z\ (\forall x\ x = y) \Rightarrow (y + z > y)$
3. $t = x,\ A$ *cualquiera.*

Exercise 25 *Pruebe las siguiente fórmulas intuicionistas:*
1. $\exists x(A \vee B) \Leftrightarrow (\exists xA) \vee (\exists xB)$
2. $\forall x(A \wedge B) \Leftrightarrow (\forall xA) \wedge (\forall xB)$
3. $\neg\exists xA \Leftrightarrow \forall x\neg A$
4. $\exists x\neg A \Rightarrow \neg\forall xA$
5. $\forall x(A \Rightarrow B) \Leftrightarrow (A \Rightarrow \forall xB)$, *donde x no es libre en A.*
6. $\exists x(A \Rightarrow B) \Rightarrow (A \Rightarrow \exists xB)$, *donde x no es libre en A.*

Exercise 26 *Pruebe usando RAA:*
1. $\neg\forall xA \Rightarrow \exists x\neg A$
2. $(A \Rightarrow \exists xB) \Rightarrow \exists x(A \Rightarrow B)$, *donde x no es libre en A.*

References

[1] R. Balbes y P. Dwinger, "Distributive Lattices", University of Missoury Press, 1974.

[2] B. Davey y H. Priestley, "Introduction to Lattices and Orders", Cambridge University Press, 1990.

[3] H. Ebbhingahus, J. Flum, W. Thomas, "Mathematical Logic", Springer Verlag, 1991.

[4] M. Fitting, "First-Order Logic and Automated Theorem Proving", Springer Verlag, 1996.

[5] J. I. Girard, "Proofs and Types", Cambridge Tracts in Theoretical Computer Science, 1989.

[6] J. I. Girard, "Proof Theory and Logical Complexity", Bibliopolis, Elsevier 1987.

[7] R. Goldblatt, "Logic of Time and Computation", CSLI Lecture Notes N7, 1992.

[8] G. Grätzer, "General Lattice Theory", Birkhäuser Verlag, 1998.

[9] E. Mendelson, "Introduction to Mathematical Logic", Wadsworth & Brooks, Monterrey, 1987.

[10] D. Prawitz, "Natural Deduction", Acta Universitati stockholmiensis, 1965.

[11] J. Reynolds, "Theories of Programming Lenguages", Cambridge University Press, 1998.

[12] D. Van Dalen, "Logic and Structure", Springer Verlag, 1997.

APÉNDICE 1: Cálculo lambda tipado y el isomorfismo de Curry-Howard.

1. **Interpretación de Brower-Heyting-Kolmogorov.**

Una interptretación heurística de los conectivos de la lógica intuicionista surge de una propuesta de Heyting, con la cual intenta llegar al verdadero significado de la noción de *prueba matemática.* La interpretación es conocida como interpretación BHK (Brower-Heyting-Kolmogorov). Según Heyting, una prueba escrita en algún sistema formal no es más que un reflejo borroso de lo que la prueba es en realidad. Una prueba de A es una *construcción matemática* (que lleva implícita un *proceso, cómputo, programa, etc.)* que establece A. Por ejemplo, una prueba de $2 + 4 = 6$ es concretamente el proceso de cómputo que permite establecer 6 como resultado de la suma de 2 y 4. Por otro lado:

La prueba de $A \wedge B$ es un par (a, b) de *construcciones* tales que a permite establecer A y b establece B.

La prueba de $A \vee B$ es un par (i, c) tal que i es 1 o 2 y si $i = 1$ entonces c es una *construcción* que permite establecer A, mientras que si $i = 2$ entonces c es una *construcción* que establece B.

La prueba de $A \Rightarrow B$ es una *construcción* que permite transformar una prueba de A en una prueba de B.

La noción de prueba normal puede considerarse una buena aproximación formal a la idea de prueba propuesta por Heyting, sobre todo cuando se la conecta a través del isomorfismo de Curry-Howard con los términos del cálculo lambda tipado, que son una adecuada representación matemática de la noción de *programa*. De hecho distintas extensiones del cálculo lambda constituyen el soporte teórico de los lenguajes de programación funcionales [11].

2. **El cálculo lambda tipado.**

Este es escencialmente un cálculo en el que se modela de manera abstracta dos nociones elementales relativas a la manipulación de funciones: el formar una función a través de una "regla", y el de "aplicar" una función a un elemento. De manera informal, si t es una regla que permite calcular un elemento del conjunto B a partir de un elemento α de A (por ejemplo, $A = \mathbf{N}$, $B = \mathbf{R}$ y $t = \sqrt{a} + 1$), entonces $\lambda\alpha.t$ será la función de A en B que dado $\alpha \in A$ devuelve el elemento de B calculado según t. Por otro lado, $(\lambda\alpha.t)\ u$ denota la aplicación de la función $(\lambda\alpha.t)$ al elemento u de A.

El lenguaje del cálculo lambda posee variables de *tipo* $T_1, T_2, ...$ y variables de *función*, que describiremos a continuación. Los típos se definen de la siguiente manera:

1. T_i es un tipo, para $i = 1, 2, ...$.
2. si U, V son tipos entonces $U \times V$ y V^U son tipos (intuitivamente, el producto cartesiano de U y V, y el conjunto de fuciones de U en V). Una notación alternativa para el tipo V^U es $U \to V$.
3. Los únicos tipos son los que se construyen mediante 1 y 2.

Para cada tipo T disponemos de un conjunto infinito de *variables de función de tipo* T, a saber $\alpha_1^T, \alpha_2^T, ...$. Los términos lambda con sus respectivos tipos se construyen de la siguiente manera:

1. α_i^T es un término de tipo T, para todo i.
2. Si t es un término de tipo T y u es un término de tipo U entonces $\langle t, u\rangle$ es un término de tipo $T \times U$.
3. Si t es un término de tipo $T \times U$ entonces $\pi_1\ t$ es un término de tipo T, y $\pi_2\ t$ es un término de tipo U.
4. Si t es un término de tipo T entonces $\lambda\alpha_i^U.t$ es un término de tipo T^U, para todo i.

5. Si t es un término de tipo T^U y u es un término de tipo U entonces $t\ u$ es un término de tipo T.

Frecuentemente para abreviar la notación utilizamos metavariables de función, de la misma manera que se utilizan $U, T, ...$ como metavariables de tipo. Por ejemplo al término

$$\lambda\alpha_1^T.\lambda\alpha_5^{T\to U}.\ \alpha_5^{T\to U}\ \alpha_1^T$$

de tipo $T \to (T \to U) \to U$ se lo suele abreviar escribiendo $\lambda x.\lambda f.\ f\ x$, y aclarando que x, f son variables de tipo T y $T \to U$ resp. Esta convención es consistente porque en realidad los términos lambda se definen "módulo" *conversiones* α. Vamos a explicar este punto. Consideremos el término $\lambda\alpha_i^T.t$ y supongamos que α_j^T no ocurre en t. Si t' se obtiene de t reemplazando cada ocurrencia de α_i^T por α_j^T, entonces decimos que $\lambda\alpha_j^T.t'$ es una conversión α de $\lambda\alpha_i^T.t$. Luego cuando se utiliza la notación $u = t$ se está diciendo en realidad que t se obtiene de u a través de conversiones α. Por ejemplo, si x, z son variables de tipo T y y es una variable de tipo $T \to (T \to T)$, escribimos

$$\lambda x.\lambda z.\ (y\ z)\ x) = \lambda z.\lambda w.\ (y\ w)\ z$$

En efecto, $\lambda x.\lambda z.\ y\ (z\ x)$ convierte a $\lambda x.\lambda w.\ y\ (w\ x)$ que a su vez convierte a $\lambda z.\lambda w.\ y\ (w\ z)$.

El cálculo Lambda posee una componente operacional notable dada por la noción de *normalización*. Un término t se dice *normal* si no tiene subtérminos de la forma

$$\pi_1\ \langle u, v\rangle \qquad \pi_2\ \langle u, v\rangle \qquad (\lambda\alpha^T.v)\ u$$

Un término t *convierte* a un término t_1 si uno de los siguientes caso ocurre:

$t = \pi_1\ \langle u, v\rangle$	$t = \pi_2\ \langle u, v\rangle$	$t = (\lambda\alpha^T.v)\ u$
$t_1 = u$	$t_1 = v$	$t_1 = v[u/\alpha^T]$

En estos tres casos llamamos a t *red* y a t_1 su *contracción*. En el último caso $v[u/\alpha^T]$ denota el reemplazo de cada ocurrencia libre de α^T por u. Las nociones de *ocurrencia libre* y *reemplazo* respecto del cuantificador λ son análogas a las dadas para el cuantificador $\forall$, en particular deben ser atendidos los fenómenos de captura de variables a la hora de efectuar el reemplazo. Por ejemplo, si $t = (\lambda x.\lambda f.\ f\ x)\ (f\ z)$, donde x, z, f son variables de tipo T, T y $T \to T$ resp., entonces al reemplazar en $\lambda f.\ f\ x$ la variable x por $f\ z$ se produce una captura de la variable f. Luego antes de efectuar la sustitución renombramos $t = (\lambda x.\lambda g.\ g\ x)\ (f\ z)$, lo que arroja la contracción $t_1 = \lambda g.\ g\ (f\ z)$.

Un término t *reduce* a un término n (en símbolos $t \rightsquigarrow^* n$) cuando existe una secuencia finita

$$t = t_0, t_1, ...t_k = n$$

tal que para $i = 1, ..., k$ el término t_i se obtiene de t_{i-1} reemplazando una red por su contracción (se suele utilizar $t_{i-1} \rightsquigarrow t_i$ para denotar esta operación). Una forma *normal* para t es un término normal n tal que t reduce a n.

Notemos que la noción de reducción pone al descubierto un costado operacional (*sentido*) que queda oculto si nos remitimos simplemente a la denotación de los términos, según la cual claramente un término t y su normalización n denotan la misma función.

Algunos ejemplos.

(1) Sea $BOOL$ el tipo $T_1 \to (T_1 \to T_1)$, y sean x, y variables de tipo T_1. Definimos

$$\begin{aligned} TRUE &= \lambda x.\lambda y.x \\ FALSE &= \lambda x.\lambda y.y \end{aligned}$$

Es fácil probar que ambos son términos lambda de tipo $BOOL$ (ejercicio). Definamos además los términos

$$\begin{aligned} NOT &= \lambda b.\lambda x.\lambda y.\ b\ y\ x \\ AND &= \lambda b.\lambda c.\lambda x.\lambda y.\ b\ (c\ x\ y)\ y \end{aligned}$$

Veremos ahora que el término $NOT\ TRUE$ reduce a la forma normal $FALSE$. En efecto:

$NOT\ TRUE$
$=$
$(\lambda b.\lambda x.\lambda y.\ b\ y\ x)\ (\lambda x.\lambda y.x)$
$=$ (renombre para evitar las capturas de x e y)
$(\lambda b.\lambda z.\lambda w.\ b\ w\ z)\ (\lambda x.\lambda y.x)$
$\rightsquigarrow$
$\lambda z.\lambda w.\ (\lambda x.\lambda y.x)\ w\ z$
$\rightsquigarrow$
$\lambda z.\lambda w.\ (\lambda y.w)\ z$
$\rightsquigarrow$
$\lambda z.\lambda w.\ z$
$=$
$FALSE$

De la misma manera se prueba

$NOT\ FALSE \rightsquigarrow^* TRUE$
$AND\ TRUE\ TRUE \rightsquigarrow^* TRUE$
$AND\ TRUE\ FALSE \rightsquigarrow^* TRUE$
$\vdots$

(2) Sean x, f variables de tipo T_1 y $T_1 \to T_1$ resp. Definimos los términos $f^n\ x$, para $n \geq 0$, de la siguiente manera:

$$\begin{aligned} f^0\ x &= x \\ f^{n+1}x &= f\ (f^n\ x) \end{aligned}$$

Los numerales de Church se definen:

$$NUM_n = \lambda f.\lambda x.\ f^n\ x$$

En el ejemplo anterior demostramos que se puede reproducir el álgebra Booleana en el cálculo lambda. De la misma manera, en el ejecicio 27 se muestra como reproducir la aritmética básica. Note que $TRUE$ y $FALSE$ son términos de tipo $T_1 \to (T_1 \to T_1)$ y los numerales de Church son de tipo $(T_1 \to T_1) \to (T_1 \to T_1)$. Esto se corresponde con el hecho de que los booleanos se construyen mediante dos constantes ($true$, $false$) y los enteros positivos mediante una constante (el 0) y la función sucesor. (Ejercicio: busque la correlación.)

Exercise 27 *Defina:*
$SUCC = \lambda n.\lambda f.\lambda x.\ f\ (n\ (f\ x))$
$SUM = \lambda m.\lambda n.\lambda f.\lambda x.\ m\ f\ (n\ (f\ x))$
$MULT = \lambda m.\lambda n.\lambda f.\ m\ (n\ f)$
Pruebe que:
$SUCC\ NUM_n \rightsquigarrow NUM_{n+1}$,
$SUM\ NUM_n\ NUM_m \rightsquigarrow NUM_{n+m}$,
$MULT\ NUM_n\ NUM_m \rightsquigarrow NUM_{nm}$.

3. **Isomorfismo de Curry-Howard.**

Vamos a introducir una leve modificación en la noción de prueba. Asumimos que las ocurrencias de una misma hipótesis están reunidas en grupos identificados con labels naturales, y que cuando se aplica un regla que admite cancelar ocurrencias de A, entonces se escoge un grupo de ocurrencias de A, y se cancelan todas las ocurrencias pertenecientes a ese grupo. Por supuesto, utilizamos el label natural que identifica al grupo para señalar el nodo en el cual se aplica dicha regla. Por ejemplo, la prueba

$$\dfrac{\dfrac{\dfrac{[A]^1 \quad A \Rightarrow A}{A}\wedge E1 \qquad A \Rightarrow A}{A}\wedge E1}{A \Rightarrow A}(1)\ \Rightarrow I \tag{2}$$

puede considerarse como una prueba que posee las dos ocurrencias de la hipótesis $A \Rightarrow A$ en el mismo grupo, labelado por ejemplo con 1, o puede considerarse que posee dos grupos, labelados con 1 y 2:

$$\dfrac{\dfrac{\dfrac{[A]^1 \quad A \Rightarrow A^1}{A} \qquad A \Rightarrow A^1}{A}}{A \Rightarrow A} \tag{3}$$

$$\dfrac{\dfrac{\dfrac{[A]^1 \quad A \Rightarrow A^1}{A} \qquad A \Rightarrow A^2}{A}}{A \Rightarrow A} \tag{4}$$

El isomorfismo de Curry-Howard conecta pruebas con términos lambda:

1. A la deducción A (con A en el grupo i) le hacemos corresponder el término α_i^A.
2. A la deducción

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ A & B\end{array}}{A \wedge B}\wedge I$$

le corresponde el término $\langle a, b\rangle$, donde a es el término de la deducción subordinada de A, y b es el término correspondiente a la deducción de B.

3. A la deducción

$$\dfrac{A \wedge B}{A}\wedge E$$

le corresponde $\pi_1\ t$ donde t es el término de la deducción subordinada de $A \wedge B$. Similar para la otra regla de eliminación.

4. A la deducción

$$\dfrac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \Rightarrow B}\Rightarrow I$$

le corresponde $\lambda\alpha_i^A.b$, donde b es el término de la deducción subordinada de B, y las hipótesis canceladas formaban parte del grupo i.

5. A la deducción

$$\dfrac{A \Rightarrow B \qquad A}{B}\Rightarrow E$$

le corresponde $t\ a$, donde t es el término de la deducción subordinada de $A \Rightarrow B$ y a es el término de la deducción subordinada de A.

Ejemplos:

1. A la deducción (3) le corresponde el término

$$\lambda\alpha_1^{A\to A}.\ \lambda\alpha_1^{A}.\ \alpha_1^{A\to A}\ (\alpha_1^{A\to A}\ \alpha_1^{A}),$$

mientras que a la deducción (4) le corresponde:

$$\lambda\alpha_1^{A\to A}.\ \lambda\alpha_1^{A}.\ \alpha_2^{A\to A}\ (\alpha_1^{A\to A}\ \alpha_1^{A}).$$

2. A la deducción (1) de la sección 4 le corresponde el numeral de Church NUM_1, mientras que a la deducción (0) le correponde el NUM_0. Si por encima de la ocurrencia cancelada de $[A]^2$ se reproducen aplicaciones de $\wedge E1$, se obtienen todos los numerales de Church.

La identificación descripta arriba es en realidad una biyección más que un isomorfismo, puesto que no hemos dicho explicítamente qué estructura se preserva a través de esa identificación. Se le llama isomorfismo porque las nociones de reducción y forma normal, que independientemente fueron establecidas en distintas épocas para las pruebas y para el cálculo lambda, se corresponden.

La relevancia de un isomorfismo está dada por la disparidad de los objetos que identifica. Cuando, como en este caso, la naturaleza de los objetos involucrados es tan distinta, el isomorfismo cobra importancia. El costado funcional revela una componente computacional en las pruebas, de la misma manera que las demostraciones descubren la lógica que envuelve a un algoritmo.

APÉNDICE 2: Prueba del lema 13.

La prueba para ambos casos es por inducción en la estructtura de la fórmula A. Haremos los únicos dos casos que requieren algún cuidado: el caso $A = \neg B$ de la lógica clásica, y el caso $A = B \Rightarrow C$ de la intuicionista.

CASO clásico $A = \neg B$.

Por el ejercicio 18, si $\mathcal{L}$ es un álgebra de Boole y P es un filtro primo de $\mathcal{L}$ entonces $[A] \in P$ o $[\neg A] \in P$ (ejecicio 19). En efecto,

$$P \Vdash A \Leftrightarrow P \nVdash B \Leftrightarrow [B] \notin P \Leftrightarrow [A] \in P.$$

El segundo $\Leftrightarrow$ corresponde a la aplicación de la hipótesis inductiva.

CASO intuicionista $A = B \Rightarrow C$.

($\Leftarrow$) Sea $P' \supseteq P$ tal que $P' \Vdash B$. Por hipótesis inductiva $[B] \in P'$, luego

$$[C] \geq ([B] \to [C]) \wedge [B] \in P'.$$

Nuevamente por hipótesis inductiva, $P' \Vdash C$.

($\Rightarrow$) Tenemos que si $P' \supseteq P$ y $P' \Vdash B$, entonces $P' \Vdash C$. Supongamos que para todo $D \in P$ se tiene $[D] \wedge [B] \not\leq [C]$. Por el teorema del filtro primo existe $P' \supseteq P$ tal que $[C] \notin P'$ y, para todo $D \in P \cup \{B\}$, se tiene $[D] \in P'$. Luego por la hipótesis inductiva se tiene que $P' \Vdash B$ y $P' \nVdash C$, lo que es una contradicción. En consecuencia, existe $D \in P$ tal que $[D] \wedge [B] = 0$. Como $[D] \wedge [B] = 0 \leq [C]$, por definición de complemento relativo se tiene $[D] \leq [B \Rightarrow C]$, luego $[B \Rightarrow C] \in P$ pués P es creciente.

APÉNDICE 3: Cálculo de Secuentes de Gentzen.

Este cálculo es de importancia fundamental en los estudios téoricos relativos a los lenguajes lógicos y la prueba automática de teoremas. El lector interesado puede consultar [5], [6], [4]. Un *secuente* es una expresión de la forma

$$\mathbf{A} \vdash \mathbf{B}$$

donde $\mathbf{A}$ y $\mathbf{B}$ son secuencias de fórmulas,

$$\begin{aligned} \mathbf{A} &= A_1, ..., A_n \\ \mathbf{B} &= B_1, ..., B_m. \end{aligned}$$

La interpretación intuitiva de un secuente es que la conjunción de $\mathbf{A}$ implica la disjunción de $\mathbf{B}$. Así, si $\mathbf{B}$ es la secuencia vacía, entonces el secuente afirma

$$\neg(A_1 \wedge ... \wedge A_n).$$

El cálculo posee un axioma esquema, el **axioma identidad**:

$$C \vdash C$$

El conjunto de reglas que define éste cálculo se divide en dos grupos, las reglas *estructurales* y las *lógicas*. A estas se le suma una última regla llamada **regla de corte:**

$$\frac{\mathbf{A} \vdash C, \mathbf{B} \qquad \mathbf{A}', C \vdash \mathbf{B}'}{\mathbf{A}, \mathbf{A}' \vdash \mathbf{B}, \mathbf{B}'} \; CUT$$

El Teorema de Eliminación de Cortes de Gentzen (Hauptzatz), uno de los más importantes de la Teoría de la Demostración, establece que el cálculo puede prescindir de esta regla. Más aún, dá un algoritmo de eliminación de cortes que es el equivalente en este paradigma al proceso de normalización de una deducción natural (o un término lambda tipado, según Curry-Howard). Esta teoría constituye la base fundacional de los lenguages de programación Lógicos.

REGLAS ESTRUCTURALES.

Reglas de intercambio:

$$\frac{\mathbf{A}, C, D, \mathbf{A}' \vdash \mathbf{B}}{\mathbf{A}, C, D, \mathbf{A}' \vdash \mathbf{B}} \; (LX) \qquad \frac{\mathbf{A} \vdash \mathbf{B}, C, D, \mathbf{B}'}{\mathbf{A} \vdash \mathbf{B}, D, C, \mathbf{B}'} \; (RX)$$

Reglas de debilitamiento:

$$\frac{\mathbf{A} \vdash \mathbf{B}}{\mathbf{A}, C \vdash \mathbf{B}} \; (LW) \qquad \frac{\mathbf{A} \vdash \mathbf{B}}{\mathbf{A} \vdash C, \mathbf{B}} \; (RW)$$

Reglas de contracción:

$$\frac{\mathbf{A}, C, C \vdash \mathbf{B}}{\mathbf{A}, C \vdash \mathbf{B}} \; (LC) \qquad \frac{\mathbf{A} \vdash C, C, \mathbf{B}}{\mathbf{A} \vdash C, \mathbf{B}} \; (RC)$$

REGLAS LÓGICAS.

Negación:

$$\frac{\mathbf{A} \vdash C, \mathbf{B}}{\mathbf{A}, \neg C \vdash \mathbf{B}} \; (L\neg) \qquad \frac{\mathbf{A}, C \vdash \mathbf{B}}{\mathbf{A} \vdash \neg C, \mathbf{B}} \; (R\neg)$$

Conjunción:

$$\frac{\mathbf{A}, C \vdash \mathbf{B}}{\mathbf{A}, C \wedge D \vdash \mathbf{B}}\ (L \wedge 1) \qquad \frac{\mathbf{A}, D \vdash \mathbf{B}}{\mathbf{A}, C \wedge D \vdash \mathbf{B}}\ (L \wedge 2)$$

$$\frac{\mathbf{A} \vdash C, \mathbf{B} \qquad \mathbf{A}' \vdash D, \mathbf{B}'}{\mathbf{A}, \mathbf{A}' \vdash C \wedge D, \mathbf{B}, \mathbf{B}'}\ (R\wedge)$$

Disjunción:

$$\frac{\mathbf{A}, C \vdash \mathbf{B} \qquad \mathbf{A}', D \vdash \mathbf{B}'}{\mathbf{A}, \mathbf{A}', C \vee D \vdash \mathbf{B}, \mathbf{B}'}\ (L\vee)$$

$$\frac{\mathbf{A} \vdash C, \mathbf{B}}{\mathbf{A} \vdash C \vee D, \mathbf{B}}\ (R \vee 1) \qquad \frac{\mathbf{A} \vdash D, \mathbf{B}}{\mathbf{A} \vdash C \vee D, \mathbf{B}}\ (R \vee 2)$$

Implicación:

$$\frac{\mathbf{A} \vdash C, \mathbf{B} \qquad \mathbf{A}', D \vdash \mathbf{B}'}{\mathbf{A}, \mathbf{A}', C \Rightarrow D \vdash \mathbf{B}, \mathbf{B}'}\ (L \Rightarrow) \qquad \frac{\mathbf{A}, C \vdash D, \mathbf{B}}{\mathbf{A} \vdash C \Rightarrow D, \mathbf{B}}\ (R \Rightarrow)$$

El caso intuicionista.

El cálculo de secuentes intuicionista se obtiene básicamente restringiendo el sistema a los *secuentes intuicionistas*, es decir los secuentes $\mathbf{A} \vdash \mathbf{B}$ donde $\mathbf{B}$ es una secuencia formada por *a lo sumo* una fórmula. De esta manera, la única regla estructural sobre la derecha que queda es RW, debido a que las restantes asumen la existencia de al menos dos fórmulas del lado derecho. El verdadero sentido de esta restricción se observa en la prueba (no intuicionista) de la sentencia clásica $\neg A \vee A$. La última regla no puede de ninguna manera ser una regla lógica (la única candidata posible es $R\vee$), puesto que en tal caso el secuente previo sería $\vdash A$ ó $\vdash \neg A$, secuentes que obviamente nunca pueden ser probados. Luego sólo puede ocurrir como última regla una estructural, y de ellas la única posible es RC :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{\vdash \neg A, A}R\neg}{\vdash \neg A \vee A, A}R\wedge 1}{\vdash A, \neg A \vee A}RE}{\vdash \neg A \vee A, \neg A \vee A}R\wedge 2}{\vdash \neg A \vee A}RC$$

Las reglas lógicas preservan su forma original (restringida a los secuentes intuicionistas) con una excepción: la regla $L\vee$ intuicionista es

$$\frac{\mathbf{A}, C \vdash \mathbf{B} \qquad \mathbf{A}', D \vdash \mathbf{B}}{\mathbf{A}, \mathbf{A}', C \vee D \vdash \mathbf{B}}\ (L\vee)$$

A diferencia de la restricción de la regla $(L\vee)$ clásica, aquíexigimos que $\mathbf{B}$ sea exactamente $\mathbf{B}'$.

Estas restricciones arrojan una propiedad fundamental. Supongamos que tenemos una prueba de $\vdash A$ sin cortes. Un breve recorrido por las reglas nos muestra que la última regla aplicada es necesariamente una regla *logica derecha*. Luego, si A es la fórmula $C \vee D$, entonces la última regla es $R\vee 1$ o $R\vee 2$, y por lo tanto tenemos una prueba de $\vdash C$ o de $\vdash D$! Esta propiedad se denomina *propiedad de la disjunción*.