BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS
LICENCIATURA EN MATEMÁTICAS

ESTUDIO EN LOS FUNDAMENTOS DE LAS MATEMÁTICAS COMPARANDO ALGUNAS DE SUS AXIOMATIZACIONES

TESIS

PRESENTADA PARA OBTENER EL TÍTULO DE
LICENCIADO EN MATEMÁTICAS

PRESENTA: JONATHAN JULIÁN HUERTA Y MUNIVE

DIRECTOR DE TESIS: IVÁN MARTÍNEZ RUIZ

PUEBLA, PUE. ABRIL DE 2016

A ti, mi querido lector.

Agradecimientos

Esta tesis es el producto de mi convivencia con distintas personas a lo largo de cuatro años y medio de licenciatura. Son vastos los nombres de aquellos individuos e instituciones que tuvieron influencia en mi crecimiento matemático. Empezando por los más lejanos y abstractos se encuentran sitios web como Wikipedia y StackExchange que ayudaron a saciar mi curiosidad en diversas noches de desvelo.

Posteriormente, deseo agradecerle a matemáticos en todo el mundo que, a veces sin saberlo, me han enseñado más sobre la vida matemática de lo que podría haber aprendido en mi pequeña comunidad, todo gracias a que han plasmado sus ideas en ese increíble lugar llamado internet. Entre las maravillosas personas que puedo recordar se encuentran Ali Enayat, Andrej Bauer, Andres Caicedo, Asaf Karagila, Carlos Ivorra Castillo, Colin McLarty, Freek Wiedijk, Harvey Friedman, Joel David Hamkins, Jeremy Avigad, Lawrence Paulson, Michael Lee Finney, Mike Shulman, Quiaochu Yuan, Steve Awodey, Terrence Tao, Timothy Gowers, Victoria Gitman y Vladimir Voevodsky.

También deseo agradecer a la única institución en Puebla que me permitió estudiar la licenciatura que estaba destinado a cursar, la Benemérita Universidad Autónoma del Estado de Puebla (BUAP), y con ella, agradezco también a todos mis profesores que se tomaron el tiempo para compartir sus conocimientos conmigo. Como mención especial agradezco también a la Vicerrectoría de Investigación y Estudios de Posgrado (VIEP) de la BUAP, pues por medio de sus programas de Jóvenes Investigadores fui capaz de adquirir los conocimientos suficientes para presentar esta tesis. Con esto también expreso mi más profundo agradecimiento a Verónica Borja Macías, Alejandro Ramírez Páramo, Oleg Okunev y Ángel Contreras Pérez, quienes se interesaron personalmente en mi investigación y me instruyeron con referencias, sesiones de estudio, asesorías, tiempo y dedicación.

Agradezco también a mi novia, amigos y familiares por su invaluable apoyo moral, paciencia y comprensión al cursar una carrera tan demandante como lo es la licenciatura en matemáticas. Ustedes son una inspiración para seguir trabajando arduamente y mejorarme cada día.

Finalmente pero no menos importante, agradezco a mi asesor, Iván Martínez Ruiz porque su apoyo ha estado presente desde mis primeros semestres de licenciatura. Sus enseñanzas, observaciones, intervenciones y consideraciones han sido de los regalos más apreciados que obtengo tras estos cuatro años y medio de estudios universitarios. No cabe duda que él es una grandiosa persona a la cual le deseo las más grandes bendiciones en este mundo.

Introducción

La lógica, a lo largo de los últimos doscientos años, se ha diversificado en su alcance. En la actualidad, para llevar a cabo su investigación, un lógico puede requerir conocimientos de teoría de conjuntos, teoría de prueba, teoría de modelos, computabilidad, aritmética, teoría de categorías, topología, lenguajes de programación, teorías de tipos y/o álgebra. Esta diversidad se dio principalmente por las contribuciones de las matemáticas en la lógica y viceversa.

En el presente trabajo el interés recae en la interrelación entre la lógica y los fundamentos de las matemáticas. Particularmente, en la *formalización* de los teoremas matemáticos dentro de un *sistema lógico*. Es sabido que esto se puede hacer de diversas maneras, siendo la predilecta en los cursos de licenciatura, la formalización de las matemáticas en la teoría de conjuntos ZFC (Zermelo-Fraenkel-Choice). No obstante, otras aproximaciones al problema menos conocidas tienen ventajas y desventajas en comparación con ésta.

Con el motivo de mostrar la variedad de sistemas en los cuales se pueden axiomatizar las matemáticas, el presente trabajo exhibe la formalización estándar de las matemáticas en el sistema ZFC así como una implementación moderna en la denominada *teoría de tipos homotopía*, HoTT. A la par se efectúa una comparación conceptual entre ambos enfoques, actuando lo más detalladamente posible para vislumbrar las sutilezas que conlleva cada implementación.

En esencia, el trabajo de tesis fue motivado por tres razones fundamentales:

1. Presentar una introducción a la lógica con un enfoque contemporáneo para estudiantes de la licenciatura hispano-hablantes. Dicha motivante surgió debido a que el autor, al interactuar con matemáticos de distintos países, encontró diversas conversaciones informales que en relación a la lógica hablaban frecuentemente del concepto “sistema formal”. No obstante, al revisar material bibliográfico clásico respecto a lógica matemática, el autor se percató de que el término no aparecía definido explícitamente e incluso, en presentaciones más modernas, el término no era adoptado por los libros de texto. Sin embargo, como ya se mencionó, el concepto es recurrente en conversaciones informales del mundo académico. Por dicha razón, el autor se dio a la tarea de recopilar información respecto a la noción de “sistema formal” y presentarla como marco central para el desarrollo de la lógica y el estudio de los fundamentos de las matemáticas. Esta forma de presentar ambas áreas conlleva el entendimiento de un panorama general de lo que se busca al desarrollar y/o estudiar una lógica.

2. Obtener una mayor comprensión de los fundamentos de las matemáticas

y las diversas ópticas con las cuales se entienden éstos: Cada formalización de las matemáticas en alguna teoría conlleva consigo una estructura de pensamiento característica y estrategias distintas para resolver los mismos problemas. Un ejemplo claro de ésto es el concepto de *conjunto potencia*: Mientras que en una teoría de conjuntos *material* como ZFC, el conjunto potencia se comporta de acuerdo a la intuición, i.e. codifica la relación "ser subconjunto de" por medio de la relación de pertenencia, en una teoría de conjuntos *estructural* como ETCS (Elementary Theory of the Category of Sets) el conjunto potencia es codificado por medio de una propiedad universal, ya sea con un classificador de subobjetos o como un objeto de una categoría cartesiana. Ambos enfoques inducen las propiedades conocidas de un conjunto potencia pero es claro que la manera de concebir a dicho ente varía entre una y otra teoría de conjuntos. Con base en esto, el autor quiso estudiar algunos sistemas formales lo suficientemente "ricos" como para implementar al resto de las matemáticas y aprender las estructuras de pensamiento requeridas para cada uno.

3. Presentación de la *Teoría de Tipos-Homotopía* (*Homotopy Type Theory* -HoTT-) a la comunidad mexicana: Al momento de plantear el trabajo de tesis, las publicaciones en idioma español respecto a HoTT eran nulas de acuerdo a las búsquedas realizadas por el autor. Actualmente hay por lo menos dos tesis respecto a dicho sistema con nombres como "teoría homotópica de tipos" y/o "teoría de homotopía de tipos". Con base en la falta de referencias en español, el autor decidió estudiar dicho sistema formal y utilizar su tesis como un medio para compartir con la comunidad matemática mexicana diversas propiedades del mismo.

Por todo lo dicho anteriormente, la primera mitad de la tesis se enfoca en dar una presentación detallada de lo más básico de lógica matemática, i.e. el concepto de sistema formal, la lógica proposicional y la lógica predicativa. Una vez que se tiene un sistema formal donde desarrollar teorías, se implementa la teoría de conjuntos ZFC paulatinamente, agregando axioma tras axioma y analizando las consecuencias formales que cada uno tiene sobre el universo de todos los conjuntos V. Finalmente, se presenta la teoría tipos homotopía, haciendo énfasis en las diversas interpretaciones que se pueden atribuir a su sistema formal y especificando las diferencias principales entre ésta y otras teorías de tipos.

Así, en el Capítulo 1, los Preliminares, se empieza con el concepto más básico en lógica: los símbolos. A partir de colecciones de éstos, i.e. alfabetos, y métodos recursivos se definen y dan ejemplos de lenguajes, teorías y sistemas formales y lógicos. Finalmente se definen las propiedades más populares deseables en dichos sistemas y se prevee su utilización en capítulos siguientes.

En el Capítulo 2 se presentan las Lógicas Proposicional y Predicativa. Al estudiar la sintaxis de la lógica proposicional se enuncian los teoremas de buena construcción de su lenguaje, i.e. el principio de inducción sobre la complejidad de la fórmula, el teorema de legibilidad única y el teorema de la definición por recursión. Posteriormente, en la subsección de semántica para la lógica proposicional se definen las valuaciones y se verifica su buen comportamiento bajo sustituciones a la vez que se enlistan algunas tautologías de lógica clásica. Finalmente se enuncia un sistema formal para la lógica proposicional y se estudia la robustez y completez de dicho sistema respecto a las valuaciones. La parte de lógica predicativa refleja el comportamiento de su predecesora con la diferencia de que se presta especial atención a la sustitución y los teoremas que la acompañan. En esta sección también se analizan las diversas formas en que libros clásicos de lógica presentan a la semántica de la lógica predicativa. Por último, se enuncia y prueba el teoremas de completez de Kurt Gödel.

El Capítulo 3 expone inicialmente la filosofía de la teoría de conjuntos mediante una presentación informal. Se deducen a partir de ésta dos paradojas que sirven como motivo para estudiar la teoría de conjuntos formalizada en lógica predicativa. A lo largo del capítulo se van exponiendo los axiomas de la teoría de conjuntos: extensionalidad, especificación, par, unión, potencia, infinito, reemplazo, regularidad y elección, a la vez que se van comentando las implicaciones filosóficas, matemáticas e históricas que cada uno de ellos conlleva. Finalmente, se da una presentación de la notación convencional al momento de manejar las distintas subteorías y suprateorías de ZFC.

En última instancia, el Capítulo 4 comienza con una introducción histórica de la teoría de tipos. Posteriormente se presenta la interpretación original que Per Martin-Löf dio a su teoría de tipos analizando cada constructo de la misma: tipos de funciones dependientes, parejas dependientes, coproductos, números naturales, vacío y unidad. A continuación se enuncia la correspondencia Curry-Howard y se especifica esta para cada uno de los tipos presentados. Se aprovecha dicha correspondencia para introducir a los tipos igualdad proposicional y se explica la diferencia entre ésta y su contraparte sintáctica. De aquí se da una presentación formal del sistema HoTT construyendo nuevamente el lenguaje formal del mismo y enunciando sus reglas de inferencia. Finalmente, se explica a grandes rasgos la interpretación homotópica de la teoría de tipos intuicionista y se justifica la necesidad de añadir el axioma de univalencia y el de extensionalidad de funciones.

Índice general

Agradecimientos I

Introducción III

1. Preliminares **1**
I. Lógica y lenguajes 1
II. Sistemas Formales 4
III. Semánticas y sistemas lógicos 8

2. Lógicas Proposicional y Predicativa **13**
I. Lógica Proposicional 13
I. Sintaxis de la Lógica Proposicional 14
II. Semántica para la Lógica Proposicional 23
III. Sistema Formal para la Lógica Proposicional 29
II. Lógica Predicativa 39
I. Sintaxis de la Lógica Predicativa 43
II. Semántica para la Lógica Predicativa 51
III. Sistema formal para la Lógica Predicativa 65

3. Fundamentos en la Teoría de Conjuntos **75**
I. Teoría Informal de Conjuntos 76
II. Teoría Formal de Conjuntos 79
III. Implementación de las Matemáticas en Teoría de Conjuntos 89

4. Teoría de Tipos-Homotopías **105**
I. Introducción Histórica y Motivación Práctica 105
II. Interpretación Original y Motivación Filosófica 107
I. Tipo de Funciones Dependientes 110
II. Tipo de Parejas Dependientes 111
III. Tipo Coproducto 112
IV. Tipo de Números Naturales 112
V. Tipo Vacío o Tipo Nulo 113
VI. Tipo Unidad 113
III. Correspondencia Curry-Howard y Motivación en Lógica 113
I. Cuantificador Universal 114

II. Implicación . . . 115
III. Cuantificador Existencial . . . 116
IV. Conjunción . . . 117
V. Disyunción . . . 119
VI. Inducción en Números Naturales . . . 120
VII. Contradicción y negación . . . 121
VIII. Tautología . . . 122
IX. Igualdad Proposicional . . . 123
IV. Desarrollo formal de HoTT y motivación en los fundamentos . . . 126
V. Interpretación Homotópica y Motivación en Matemáticas . . . 132
I. Estructura ω-grupoide de los tipos igualdad proposicional . . . 133
II. Extensionalidad de funciones . . . 137
III. Univalencia . . . 140

Conclusión **142**

Referencias **144**

Estudio en los Fundamentos de las Matemáticas comparando algunas de sus Axiomatizaciones

Jonathan Julián Huerta y Munive

14 de abril de 2016

Capítulo 1

Preliminares

I. Lógica y lenguajes

La lógica como "área del conocimiento humano que estudia los razonamientos válidos" se ha practicado desde tiempos antiguos; no obstante, hasta el siglo XV la inovación en ésta fue esporádica y escasa en comparación con los avances que se han dado desde el siglo XVIII. Gracias a los métodos de formalización estudiados por individuos como George Boole y Gottlob Frege, la lógica ha evolucionado rápidamente y se ha diversificado en su alcance. Se distinguen dos ramas principales de la lógica: la informal y la formal. La primera de éstas es el tipo de lógica que se estudió en antiguedad en escritos como los Diálogos de Platón, mientras que la última es la que más se estudia contemporáneamente en sus presentaciones de lógica simbólica y lógica matemática.

Históricamente la lógica matemática se ha entendido de tres distintas maneras:

I Lógica Matemática como lógica simbólica, es decir, el estudio de la lógica por medio de abstracciones simbólicas que proveen la esencia del razonamiento válido. Son ejemplos de ésta las lógicas proposicionales, predicativas, lineales, modales, temporales, paraconsistentes, deónticas y doxásticas.

II Lógica Matemática como rama de las matemáticas que provee herramientas y métodos para estudiar las mismas matemáticas. Esta acepción es la que normalmente se clasifica en Teoría de Modelos, Teoría de Prueba, Teoría de Conjuntos y Teoría de la Recursión.

III Lógica Matemática como el estudio de los fundamentos o filosofía de las matemáticas.

Sin importar cuál de todas estas acepciones se desee estudiar, la herramienta básica para estudiar lógica formal es el concepto de "sistema lógico"$\mathscr{L}$, el cual tiene tres constituyentes: un lenguaje $\mathcal{L}$, un aparato deductivo $\mathfrak{D}$ y una semántica $\mathcal{S}$. El primero de estos usualmente se concibe como un conjunto de "expresiones (concatenaciones de símbolos) bien formadas". Es común que la construcción de los lenguajes formales se desarrolle recursivamente indicando primero un alfabeto (conjunto de símbolos) Σ y, posteriormente, qué concatenaciones de ellos son las que están "bien formadas". Dicho enfoque es el que se adopta en el presente trabajo:

Definición I.1 (Cadena)
Una cadena, expresión, palabra o fórmula φ sobre el alfabeto Σ es una concatenación finita $\varphi = s_1 s_2 \cdots s_n$ de algunos de sus símbolos $s_1, s_2, \ldots, s_n \in \Sigma$.

Antes de continuar, el lector debe percatarse de que utilizar símbolos para representar alfabetos y/o cadenas de símbolos puede ser problemático. Un ejemplo de esto sería trabajar con el alfabeto griego $\Sigma = \{A, B, \Gamma, \Delta, \ldots, \Sigma, \ldots, \Omega\}$. Al utilizar posteriormente la letra "Σ" es muy probable que haya confusión respecto a si se está haciendo referencia al alfabeto o únicamente al símbolo dentro de éste. Por esta razón, a lo largo del trabajo se utilizarán las letras griegas como símbolos (metasímbolos) del metalenguaje, es decir, el lenguaje que se está utilizando para trabajar y estudiar los lenguajes formales (lenguajes objeto), siendo excepciones a esta regla los casos en los que el contexto sea suficiente para evitar confusiones.

Además de esto, se convienen las siguientes reglas:

- Dado un alfabeto Σ, la expresión Σ^* denotará al *lenguaje universal*, i.e. el conjunto de todas las posibles cadenas sobre Σ.
- Las letras minúsculas griegas serán usadas como metasímbolos para representar cadenas.
- Para expresar que una palabra, por ejemplo "$\mathfrak{J}\Xi$♫", es representada por el metasímbolo φ la notación será: $\varphi := \mathfrak{J}\Xi$♫.
- Si $\varphi := s_1 s_2 \cdots s_n$ es una fórmula, entonces $|\varphi|$ representa la longitud de ésta, es decir, el número de símbolos (incluyendo repeticiones) en ella: $|\varphi| = n$.
- Dos expresiones $\varphi := s_1 s_2 \cdots s_n$ y $\psi := r_1 r_2 \cdots r_n$ son iguales -denotado por $\varphi = \psi$- si coinciden en el orden de aparición de sus símbolos componente a componente, i.e. si son exactamente la misma cadena. Simbólicamente: $\varphi = \psi$ si y sólo si $s_i = r_i$ para cada $i \in \{1, \ldots, n\}$.
- Si $\varphi := s_1 s_2 \cdots s_n$ y $\psi := r_1 r_2 \cdots r_n$ son cadenas, la nueva cadena formada por la concatenación de éstas será denotada en el metalenguaje por $\varphi\psi$. Es decir $\varphi\psi := s_1 s_2 \cdots s_n r_1 r_2 \cdots r_n$.
- Si $\varphi := s_1 s_2 \cdots s_n$ es una cadena de símbolos de Σ y $s \in \Sigma$, entonces a todo s_i con $i \in \{1, \ldots, n\}$ tal que $s_i = s$ se le llama instancia del símbolo s en φ.
- Si $s_{i_1}, s_{i_2}, \ldots, s_{i_m}$ son todas las instancias de $s \in \Sigma$ en $\varphi := s_1 s_2 \cdots s_n$ y si para todos los $j, k \in \{1, \ldots, m\}$ con $j < k$ se cumple que $i_j < i_k$, entonces s_{i_j} es la j-ésima instancia de s en φ.

- Existe la "cadena vacía" y es usual denotarla por la letra griega lambda: λ.
- La longitud de la cadena vacía es 0, i.e. $|\lambda| = 0$.
- La fórmula λ cumple la propiedad de que concatenarla con cualquier otra cadena (por izquierda o por derecha) siempre da como resultado la otra cadena. O sea que si φ es una cadena entonces $\lambda\varphi = \varphi\lambda = \varphi$.
- Por convención la cadena vacía λ siempre está presente en cualquier lenguaje universal Σ^*.

Nótese que un lenguaje universal siempre es infinito pues incluso un alfabeto de un símbolo como $\Sigma = \{a\}$ genera el lenguaje universal:

$$\Sigma^* = \{\lambda, a, aa, aaa, aaaa, \dots\}$$

Definición I.2 (Lenguaje Formal y Expresiones Bien Formadas)
Una vez generado un espacio infinito de cadenas con las cuales trabajar se presenta un concepto para utilizar sólo con aquellas que tengan sentido sintáctico:

- Se llamará léxico o *lenguaje formal*[1] $\mathcal{L}$ a todo subconjunto de algún lenguaje universal Σ^* derivado de un alfabeto Σ.
- A las cadenas de un lenguaje formal $\varphi \in \mathcal{L}$ se les denomina expresiones o *fórmulas bien formadas*[2] o *wffs* por sus siglas en inglés (well-formed-formulas).

Cuando se estudian o seleccionan ciertos lenguajes es mayor el interés en generar palabras con ciertos patrones a escogerlas arbitrariamente, por esta razón se desarrollaron varias herramientas para seleccionar o identificar cadenas que sí pertenecen a un determinado lenguaje. Algunos de los mecanismos implementados para dicho objetivo son las *expresiones regulares*, los *sistemas de patrones* y las *gramáticas formales*. El estudio de estos mecanismos es un área (de las ciencias computacionales) en sí misma (c.f. [JLRR00]) e incursionar en ella desviaría el objetivo del trabajo, razón por la cual únicamente se utilizará el término genérico de gramática para hacer referencia a una descripción precisa de un lenguaje formal, es decir, un cuerpo de reglas sistemáticas que sirven para generar un lenguaje o para determinar si una cadena pertenece a un lenguaje dado.

Ejemplo I.1 Dado el alfabeto $\Sigma = \{0, 1\}$ es posible calcular el lenguaje universal $\Sigma^* = \{\lambda, 0, 1, 00, 01, 10, 11, 100, \dots\}$. Un lenguaje formal podría ser simplemente el subconjunto finito de éste $\mathcal{L}_1 = \{1, 10, 100, 1000\}$ pero de igual manera se puede construir otro recursivamente mediante las reglas:

[1] A pesar de que el nombre de léxico resulte más apropiado debido a la derivación de este concepto a partir de un alfabeto, en la literatura, por razones históricas, es más común leer el nombre de Lenguaje Formal.

[2] La razón por la cual se utiliza el nombre de "fórmulas bien formadas" es para distinguir a éstas de cualquier otra fórmula/cadena que pudiese estar en el Lenguaje Universal mas no en el que se está estudiando.

(I) 1 es una *wff* de $\mathcal{L}_2$.

(II) Si $\varphi \in \mathcal{L}_2$ (φ es una *wff* de $\mathcal{L}_2$), entonces $\varphi 0$ también es una *wff* de $\mathcal{L}_2$.

(III) Ninguna otra cosa es una *wff* de $\mathcal{L}_2$.

Generando así $\mathcal{L}_2 = \{1, 10, 100, 1000, 10000, 100000, \ldots\}$

II. Sistemas Formales

Definición II.1 (Teoría y Aparato Deductivo)
El siguiente paso para construir un sistema lógico es distinguir algunas *wffs* de otras con el objetivo de establecer cuáles son "verdaderas" y cuáles no:

- Se llama *teoría* (formal) τ a cualquier subconjunto de un lenguaje formal $\mathcal{L}$.
- Un sistema deductivo o *aparato deductivo* $\mathfrak{D}$ sobre un lenguaje $\mathcal{L}$ es un mecanismo que sirve para generar una teoría $\tau \subseteq \mathcal{L}$. Generalmente consisten de una teoría $\mathcal{A} \subseteq \mathcal{L}$, cuyos elementos son llamados *axiomas*, y un conjunto de reglas $\mathcal{R}$, denominadas *de inferencia*, que indican cómo obtener *wffs* de $\mathcal{L}$ a partir de otras *wffs*.

Obsérvese que una teoría τ es también un lenguaje formal ya que $\tau \subseteq \mathcal{L} \subseteq \Sigma^*$ para algún alfabeto Σ y lenguaje $\mathcal{L}$ sobre dicho alfabeto. Ésto significa que se pueden omitir varias definiciones e introducir las teorías directamente desde el lenguaje universal; no obstante, la presentación adoptada aquí es la convencional en lógica, además de que da un sentido de construcción gradual de los objetos que se van a estudiar el resto del presente trabajo.

Ejemplo II.1 Trabájese con el alfabeto $\Sigma = \{u, 4, \Box, \heartsuit, \bigcirc, i\}$ y considérese al lenguaje $\mathcal{L}$ inducido por las siguentes reglas:

- Si $\varphi \in \Sigma^*$ y $\varphi \neq \lambda$, entonces $i\heartsuit\varphi$ es una *wff* de $\mathcal{L}$.
- Ninguna otra cosa es una *wff* de $\mathcal{L}$

Supóngase que el conjunto de axiomas es $\mathcal{A} := \{i\heartsuit u, i\heartsuit\Box, i\heartsuit\bigcirc, i\heartsuit\heartsuit\}$ y la única regla de inferencia en $\mathcal{R}$ es:

$$\frac{i\heartsuit u \qquad i\heartsuit\varphi \qquad |\varphi| = 1}{i\heartsuit u4\varphi}\text{4-Intro}$$

Es decir, de $i\heartsuit u$ y $i\heartsuit\varphi$ siendo φ una cadena de longitud 1, se infiere $i\heartsuit u4\varphi$. Así, la teoría τ generada por el aparato deductivo $\mathfrak{D} = \langle\mathcal{A}, \mathcal{R}\rangle$ es:

$$\tau = \{i\heartsuit u, i\heartsuit\Box, i\heartsuit\bigcirc, i\heartsuit\heartsuit, i\heartsuit u4u, i\heartsuit u4\Box, i\heartsuit u4\bigcirc, i\heartsuit u4\heartsuit\}$$

Como se dijo al inicio del capítulo, una vez generados un lenguaje formal $\mathcal{L}$ y un aparato deductivo $\mathfrak{D}$, el último requisito para construir un sistema lógico es el de una semántica $\mathcal{S}$. No obstante, hay varios sistemas lógicos cuyas semánticas aun no se han definido formalmente, es decir, se tiene una semántica tácita para ellos más no expresa. Más aun, en ciencias computacionales es más común trabajar únicamente con lenguajes formales y aparatos deductivos pues son lo único que se requiere para desarrollar lenguajes de programación. Por todo esto, es más común encontrar en la literatura el concepto de "sistema formal" que el de sistema lógico. El primero de éstos se emplea cuando no hay un consenso respecto a la semántica adecuada para el sistema o cuando la semántica no está presente formalmente hablando:

Definición II.2 (Sistema Formal)
Un *sistema formal* $\mathscr{F}$ es una pareja $\langle\mathcal{L},\mathfrak{D}\rangle$ donde $\mathcal{L}$ es un lenguaje formal y $\mathfrak{D}$ es un aparato deductivo con reglas de inferencia y axiomas definidos sobre $\mathcal{L}$.[3].

Obsérvese que en cualquier sistema formal $\mathscr{F}$, el aparato dedúctivo forma una especie de gramática para las *wffs* del lenguaje pues las separa en dos categorías "aquellas que sí son consecuencia de los axiomas" y las que no. Las siguientes definiciones exploran más a fondo dicha idea:

Definición II.3 (Prueba Formal)
Dados un lenguaje formal $\mathcal{L}$ sobre un alfabeto Σ y un aparato deductivo $\mathfrak{D}$ con axiomas en $\mathcal{A}\subseteq\mathcal{L}$ y reglas de inferencia en $\mathcal{R}$, se dice que una *prueba formal* o deducción Δ de una *wff* φ en el sistema formal $\mathscr{F}=\langle\mathcal{L},\mathfrak{D}\rangle$ a partir de un conjunto de premisas $\Gamma\subseteq\mathcal{L}$ es un conjunto <u>finito y ordenado</u> de *wffs* $\Delta=\langle\varphi_1,\varphi_2,\ldots,\varphi_n\rangle$ cuyo último elemento es φ ($\varphi_n=\varphi$) y además cumple que cada *wff* en la prueba ($\varphi_i\in\Delta$ con $1\leq i\leq n$) es un axioma ($\varphi_i\in\mathcal{A}$), o una premisa ($\varphi_i\in\Gamma$) o resultado de aplicar una regla de inferencia de $\mathcal{R}$ a *wffs* anteriores en la prueba.

Ejemplo II.2 Sea $\mathcal{L}=\{\ldots,-100,-11,-10,-1,0,1,10,11,100,\ldots\}$ y $\mathfrak{D}$, un aparato deductivo sin axiomas y cuyas reglas de inferencia dictan: (i) a partir de -1 y φ se sigue la concatenación $-1\varphi^*$, donde φ^* representa a la cadena original φ sin el símbolo "$-$" antecediéndola, y (ii) de φ se obtiene la *wff* $\varphi0$ solo si φ comienza con $-$ ó con 1. Para cada uno de los siguientes casos supóngase que $\Gamma=\{-1,0\}$ es el conjunto de premisas:

- $\Delta_1=\langle-1,-11,-111\rangle$ es una prueba de -111 a partir de Γ en $\mathscr{F}=\langle\mathcal{L},\mathfrak{D}\rangle$ donde sólo se utilizó la regla (i) y la premisa -1.

- $\Delta_2=\langle-1,-10,-100,-1000\rangle$ es una prueba de -1000 a partir de Γ en $\mathscr{F}=\langle\mathcal{L},\mathfrak{D}\rangle$ donde sólo se usó la regla (ii) y la premisa -1.

[3]Nótese que la representación de $\mathscr{F}$ en términos de parejas es intercambiable por $\langle\Sigma,G,\mathcal{A},\mathcal{R}\rangle$ en caso de que Σ sea el alfabeto de $\mathcal{L}$; G, su gramática; $\mathcal{A}$ los axiomas de $\mathfrak{D}$, y $\mathcal{R}$, sus reglas de inferencia.

- $\Delta_3 = \langle -1, -10, -110, -1100 \rangle$ es una prueba de -1100 a partir de Γ en $\mathscr{F} = \langle \mathcal{L}, \mathfrak{D} \rangle$ donde se usaron alternadamente las reglas (i) y (ii) y sólo la premisa -1.[4]

Definición II.4 (Consecuencia Sintáctica)
Se dice que una *wff* φ es *consecuencia (sintáctica)* de Γ en el sistema formal $\mathscr{F}$, denotado por $\Gamma \vdash_{\mathscr{F}} \varphi$, si existe una prueba formal Δ de φ a partir de Γ en $\mathscr{F}$. Se suele leer también la expresión $\Gamma \vdash_{\mathscr{F}} \varphi$ como Γ deduce a φ en $\mathscr{F}$.

En el caso del ejemplo anterior, al exhibir las tres pruebas, Δ_1, Δ_2 y Δ_3, se puede afirmar respectivamente que $\Gamma \vdash_{\mathscr{F}} -111$, $\Gamma \vdash_{\mathscr{F}} -1000$ y $\Gamma \vdash_{\mathscr{F}} -1100$. Si se prefiere, es posible intercambiar la letra Γ por el conjunto que representa, por ejemplo: $0, -1 \vdash_{\mathscr{F}} -1100$.

Definición II.5 (Teorema y Teoría matemática)
Se dice que una *wff* φ es un *teorema* del sistema formal $\mathscr{F} = \langle \mathcal{L}, \mathfrak{D} \rangle$ si es consecuencia del vacío. En otras palabras, la prueba para obtener φ no requiere de alguna premisa (sólo se usan axiomas y teoremas obtenidos previamente en la deducción). La notación en este caso se simplifica a $\vdash_{\mathscr{F}} \varphi$ en vez de $\emptyset \vdash_{\mathscr{F}} \varphi$. Además se llamará *teoría matemática* a una teoría $\tau \subseteq \mathcal{L}$ que sea el conjunto de todos los teoremas de algún sistema formal $\mathscr{F}$.

Propiedades II.1
Las siguientes son propiedades de la noción de consecuencia sintáctica en un sistema formal $\mathscr{F}$:

1. Si Γ y Δ son teorías tales que $\Gamma \subseteq \Delta$ y $\Gamma \vdash_{\mathscr{F}} \varphi$, entonces $\Delta \vdash_{\mathscr{F}} \varphi$
2. Si $\Gamma \vdash_{\mathscr{F}} \varphi$ entonces existe un un subconjunto finito Δ de Γ tal que $\Delta \vdash_{\mathscr{F}} \varphi$.
3. Si $\Gamma \vdash_{\mathscr{F}} \varphi$ y cada *wff* de Γ es consecuencia de Δ entonces $\Delta \vdash_{\mathscr{F}} \varphi$.

Demostración. En los tres casos se tiene que $\Gamma \vdash_{\mathscr{F}} \varphi$, esto significa que existe una prueba formal E de φ a partir de Γ en $\mathscr{F}$. Por definición la prueba formal es un sucesión finita de *wffs*, $E = \langle \varphi_1, \varphi_2, \ldots, \varphi_n \rangle$ cuya última *wff* es φ y todas las *wffs* en E son axiomas, elementos de Γ o consecuencia de otras *wffs* previas en E.

1. Ya que $\Gamma \subseteq \Delta$, toda *wff* de Γ está en Δ. Particularmente esto se cumple para las *wffs* de Γ en la prueba E. Por ende, E es una prueba de φ a partir de Δ en $\mathscr{F}$. Esto es $\Delta \vdash_{\mathscr{F}} \varphi$.
2. Defínase Δ como el conjunto de todas las *wffs* de Γ que aparecen en E, i.e. $\Delta = \Gamma \cap E$. Como E es finita y el número de *wffs* en Δ está acotado por el de *wffs* en E, Δ es finito. Por otro lado también se tiene que cada *wff* en E o

[4] Nótese la importancia de que la prueba formal (de una *wff* a partir de un conjunto de premisas Γ en un sistema formal $\mathscr{F}$) sea finita. Si la prueba Δ fuese infinita, no se sabría qué *wff* es su conclusión pues para determinarla necesitaríamos identificar la última *wff* en ella.

es axioma, o está en $\Delta \subseteq \Gamma$ o es consecuencia de otras previas en E. Por lo cual podemos concluir que E es una prueba de φ a partir de Δ en $\mathscr{F}$ y así $\Delta \vdash_{\mathscr{F}} \varphi$.

3. Ya que E es finita podemos enumerar las *wffs* de Γ en E: $\Gamma' = \{\gamma_1, \gamma_2, \ldots, \gamma_k\}$. Debido a que, por hipótesis, Δ demuestra a cada una de las *wffs* de Γ', existen correspondientemente las pruebas $E_1, E_2, \ldots, E_k$ a partir de Δ en $\mathscr{F}$. En otras palabras, $\Delta \vdash_{\mathscr{F}} \gamma_i$ para cada i entre 1 y k. Sea Υ la sucesión $E_1 \cup E_2 \cup \cdots \cup E_k \cup E$, entonces Υ es una prueba de φ a partir de Δ en $\mathscr{F}$. Por ende, $\Delta \vdash_{\mathscr{F}} \varphi$.

■

A continuación se presenta un ejemplo que involucra los conceptos desarrollados hasta el momento:

Ejemplo II.3 Tómese al alfabeto $\Sigma = \{a, e, *, ^{-1}, =, (,)\}$ y constrúyase el lenguaje $\mathcal{L}$ mediante las siguientes reglas:

- Los símbolos a y e son términos.[5]
- Si t es un término, entonces (t^{-1}) es un término.
- Si t_1 y t_2 son términos, entonces $(t_1 * t_2)$ es un término también.
- Ninguna otra cosa es un término.
- Si t_1 y t_2 son términos, entonces la expresión $t_1 = t_2$ es una *wff*.
- Ninguna otra cosa es una *wff*.[6]

Intuitivamente hablando puede decirse que el lenguaje $\mathcal{L}$ sólo acepta igualdades como *wffs*. El sistema axiomático, $\mathcal{A}$, se define por medio de esquemas:

A1 Si t_1, t_2 y t_3 son términos, entonces la *wff* $(t_1 * (t_2 * t_3)) = ((t_1 * t_2) * t_3)$ es un axioma.

A2 Si t es un término entonces la *wff* de la forma $(e * t) = t$ es un axioma.

A3 Si t es un término, entonces $((t^{-1}) * t) = e$ es un axioma.

A4 St t es un término, entonces la *wff* $t = t$ siempre es un axioma.

Por su parte, las reglas de inferencia, $\mathcal{R}$, indican que:

R1 Si t_1 y t_2 son términos, entonces de $t_1 = t_2$ se deduce $t_2 = t_1$.

R2 Si t_1, t_2 y t_3 son términos, entonces de $t_1 = t_2$ y $t_2 = t_3$, se deduce $t_1 = t_3$

[5]En este ejemplo los términos son elementos auxiliares para definir *wffs*. Es decir, son cadenas de símbolos cuyo orden permite definir más términos o cadenas especiales y que finalmente serán parte importante de las *wffs*.

[6]Obsérvese la importancia de los paréntesis en la construcción de términos y *wffs*.

R3 Si t_1, t_2 y t_3 son términos, entonces de la *wff* $t_2 = t_3$, se puede deducir tanto $(t_1 * t_2) = (t_1 * t_3)$ como $(t_2 * t_1) = (t_3 * t_1)$.

Nótese que en la siguiente prueba formal, todas las *wffs* son teoremas del sistema formal $\mathscr{F} = \langle \mathcal{L}, \mathfrak{D} \rangle$ donde $\mathfrak{D} = \langle \mathcal{A}, \mathcal{R} \rangle$:

1. $((a^{-1}) * a) = e$ A3
2. $e = ((a^{-1}) * a)$ R1(1)
3. $(((a^{-1})^{-1}) * e) = (((a^{-1})^{-1}) * ((a^{-1}) * a))$ R3(2)
4. $(((a^{-1})^{-1}) * ((a^{-1}) * a)) = ((((a^{-1})^{-1}) * (a^{-1})) * a)$ A1
5. $(((a^{-1})^{-1}) * e) = ((((a^{-1})^{-1}) * (a^{-1})) * a)$ R2(3,4)
6. $(((a^{-1})^{-1}) * (a^{-1})) = e$ A3
7. $((((a^{-1})^{-1}) * (a^{-1})) * a) = (e * a)$ R3(6)
8. $(((a^{-1})^{-1}) * e) = (e * a)$ R2(5,7)
9. $(e * a) = a$ A2
10. $(((a^{-1})^{-1}) * e) = a$ R2(8,9)
11. $(((a^{-1})^{-1}) * e) = ((a^{-1})^{-1})$ A2
12. $((a^{-1})^{-1}) = (((a^{-1})^{-1}) * e)$ R1(11)
13. $((a^{-1})^{-1}) = a$ R2(12,10)

Así, se asevera que el sistema formal $\mathscr{F}$ demuestra la treceava *wff* (y todas las *wffs* de la prueba también), i.e. $\vdash_{\mathscr{F}} ((a^{-1})^{-1}) = a$.

El lector observador habrá notado que los axiomas y reglas de inferencia establecidos en el ejemplo anterior son los axiomas de grupos (de dos elementos). De igual manera, puede verse que la última *wff* de la prueba corresponde al enunciado “el inverso del inverso de algún elemento del grupo es el mismo elemento”, lo cual se cumple en particular para el objeto representado por el símbolo “a”.

III. Semánticas y sistemas lógicos

Existen diferentes formas de definir semánticas de manera formal, por ejemplo, las aproximaciones por secuentes propuestas por Gerhard Gentzen y utilizadas ampliamente en teoría de prueba; las semánticas basadas en teoría de juegos, las probabilísticas, las inducidas por valores de verdad, y las utilizadas en teoría de modelos propuestas por Alfred Tarski: una función -llamada *de interpretación*- que mande a cada símbolo a un ente matemático es la idea básica detras de este último tipo de semánticas.

El estudio de las distintas semánticas es más fácil de realizar por medio de sus respectivas clases de sistemas formales. Por esta razón las semánticas estudiadas en este trabajo se analizarán en las secciones correspondientes a su sistema formal, i.e. lógica proposicional, lógica predicativa y teoría de tipos. Aún así, es posible convenir informalmente que:

Definición III.1
Una *semántica* $\mathcal{S}$ para el lenguaje formal $\mathcal{L}$ es un mecanismo que separa las *wffs* en dos conjuntos: las $\mathcal{S}$-satisfactibles y las $\mathcal{S}$-no-satisfactibles.

Es común que la partición creada por la semántica $\mathcal{S}$ se genere por una colección de entes matemáticos similares entre sí (funciones, juegos, estructuras, medidas) y una relación de *satisfactibilidad* ($\models$) entre éstos y las *wffs* de $\mathcal{L}$. Más precisamente, si $\mathcal{S} := \{S_i \mid i \in \mathcal{I}\}$, se dice que $\varphi \in \mathcal{L}$ es satisfactible bajo $\mathcal{S}$ si y sólo si alguna relación específica (por definir en las siguientes secciones) se satisface entre uno de estos entes S_i y φ, la cual será expresada en la metateoría por la notación $\models_{S_i} \varphi$.

En lógica las semánticas sirven para dar nociones de "validez" y/o "veracidad" siempre relativa a la semántica utilizada. Así, tal y como se dieron definiciones para "consecuencia sintáctica", "teoría matemática" y "teorema" las semánticas proporcionan tres conceptos análogos:

Definición III.2 (Consecuencia Semántica)
En un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$, la *wff* $\varphi \in \mathcal{L}$ es consecuencia semántica de un conjunto $\Gamma \subseteq \mathcal{L}$ de premisas, representado por $\Gamma \models \varphi$, si cada objeto ς de la semántica $\mathcal{S}$ que satisfaga a las *wffs* de Γ también satisface a φ. En términos más formales, $\Gamma \models \varphi$ sii para cada $\varsigma \in \{S_i \mid i \in \mathcal{I}\}$, si a todo $\psi \in \Gamma$, $\models_\varsigma \psi$, entonces también $\models_\varsigma \varphi$.

Definición III.3 (Satisfactibilidad de una teoría)
Dada una teoría $\tau \subseteq \mathcal{L}$ en un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$ y ς, un objeto de la semántica $\mathcal{S}$, se dice que ς satisface a τ, denotado por $\models_\varsigma \tau$, si $\models_\varsigma \varphi$ para cada $\varphi \in \tau$.

Definición III.4 (Validez Lógica)
Si se tiene un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$, se dice que una *wff* $\varphi \in \mathcal{L}$ es lógicamente válida, expresado por $\models \varphi$, si todo objeto de la semántica la satisface, i.e. $\models_\varsigma \varphi$ para cada $\varsigma \in \{S_i \mid i \in \mathcal{I}\}$.

Una vez definidos un aparato deductivo $\mathfrak{D}$ y una semántica $\mathcal{S}$ para un lenguaje $\mathcal{L}$, se busca que el sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$ satisfaga una serie de propiedades respecto a ambos objetos. Por ejemplo, es deseable que el conjunto de *wffs* lógicamente válidas bajo $\mathcal{S}$ sea el mismo que la teoría matemática generada por $\mathfrak{D}$.

Definición III.5
A continuación se da una lista de algunas propiedades esperadas de un sistema lógico y las teorías que genera:

(a) *(Consistencia)* Se dice que una teoría $\tau \subseteq \mathcal{L}$ de un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$, es consistente si y sólo si "carece de contradicciones". En caso contrario se dice que la teoría es inconsistente. Existen dos formas de que ésto ocurra:

- *(Consistencia Semántica)* Una teoría τ es semánticamente consistente si existe un objeto ς de la semántica $\mathcal{S}$ que cumpla $\models_{\varsigma} \tau$.
- *(Consistencia Sintáctica)* Suponiendo que para cada *wff* $\varphi \in \mathcal{L}$ existe otra llamada "su negación" $\varphi^{-} \in \mathcal{L}$, se dice que una teoría τ es sintácticamente consistente si ninguna de sus *wff*s cumple que ella y su negación son miembros de la teoría al mismo tiempo. Es decir si $\varphi \in \tau$, entonces $\varphi^{-} \notin \tau$ y si $\varphi^{-} \in \tau$, entonces $\varphi^{-} \notin \tau$.

(b) *(Robustez)* Un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$ es robusto si todos sus teoremas son lógicamente válidos. Simbólicamente, si $\varphi \in \mathcal{L}$ es tal que $\vdash \varphi$, entonces $\models \varphi$. Cuando se compara con otros tipos de robustez, a ésta se le suele denominar robustez débil:

- *(Robustez Fuerte)* Un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$ es fuertemente robusto si toda *wff* φ derivable a partir de una lista de premisas Γ, también es consecuencia semántica de dicha lista. Formalmente, el sistema es fuertemente robusto si para cada $\varphi \in \mathcal{L}$ que cumple $\Gamma \vdash_{\mathfrak{D}} \varphi$, también cumple $\Gamma \models_{\mathcal{S}} \varphi$.

(c) *(Completez)* Se dice que un sistema formal es completo respecto a alguna propiedad, si toda *wff* que tenga la propiedad también es un teorema de dicho sistema. En caso contrario se dice que éste es incompleto:

- *(Completez Semántica)* El recíproco a la robustez, un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$ es semánticamente completo si toda *wff* φ que sea lógicamente válida, $\models \varphi$, también es un teorema $\vdash \varphi$. A este tipo de completez también se le suele decir completez débil.
- *(Completez Fuerte)* Un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$ es fuertemente completo si toda *wff* φ que sea consecuencia semántica de una lista de premisas Γ es también sintácticamente derivable a partir de Γ. Es decir si $\Gamma \models_{\mathcal{S}} \varphi$, entonces $\Gamma \vdash_{\mathfrak{D}} \varphi$.
- *(Completez Sintáctica)* Suponiendo que para cada *wff* $\varphi \in \mathcal{L}$ existe otra llamada "su negación" $\varphi^{-} \in \mathcal{L}$, se dice que una teoría τ es sintácticamente completa si y sólo si toda *wff* φ cumple que o ella o su negación son teoremas de τ (son *wff*s elementos de τ).[7]

[7] Ya que un sistema formal $\mathscr{F} = \langle \mathcal{L}, \mathfrak{D} \rangle$ induce una teoría, la propiedad de completez sintáctica también puede ser atribuida a $\mathscr{F}$ en vez de a la teoría.

(d) *(Decidibilidad)* Una teoría es decidible si existe un procedimiento efectivo para determinar si una fórmula es teorema o no de la teoría. Es decir, si hay un algoritmo que en una cantidad finita de pasos puede afirmar o negar la pertenencia de la fórmula a la teoría.

Nótese de las definiciones anteriores que si un sistema lógico $\mathscr{L} = \langle \mathcal{L}, \mathfrak{D}, \mathcal{S} \rangle$ es fuertemente robusto o fuertemente completo, entonces también lo es débilmente.

El siguiente capítulo presenta dos sistemas muy conocidos en lógica matemática para los cuales también se demuestran algunas de las propiedades enunciadas recientemente. Todo esto con el fin de que los conceptos sean concretados para su uso posterior en las principales axiomatizaciones de las matemáticas.

Capítulo 2

Lógicas Proposicional y Predicativa

I. Lógica Proposicional

La forma más sencilla y popular de "estudiar los razonamientos válidos" es por medio de la lógica proposicional. La mecánica de ésta consiste en utilizar literales para representar *proposiciones*. Las proposiciones son el equivalente a enunciados declarativos o sentencias en el lenguaje natural (español, inglés, alemán u otro que usen cotidianamente los humanos) y son fácilmente reconocibles porque, en principio, es posible asignarles un *valor de verdad*: verdadero o falso. Un ejemplo de una proposición sería el enunciado "las guitarras son un instrumento musical" mientras que un ejemplo de una oración que no es una proposición sería "¿quién se comió las galletas de avena?". Obsérvese que en el primer caso es posible afirmar que la oración "las guitarras son un instrumento musical" es verdadera mientras que intentar hacer un juicio similar para una interrogante no parece adecuado. Una vez que se han representado las proposiciones con letras, lo único que queda para realizar un estudio, en el marco de la lógica proposicional, es ligarlas por medio de *conectivos* y, finalmente, analizar las inferencias y razonamientos válidos a través de las <u>relaciones extensionales</u> entre los valores de verdad de las proposiciones y dichos conectivos. Esto quiere decir que en el caso de proposiciones más complejas como "si las guitarras son instrumentos musicales, entonces los gorriones son peces voladores", el valor de verdad de éstas dependerá de los valores asignados a las proposiciones simples que las conforman que en el caso del ejemplo son las dos oraciones: "las guitarras son instrumentos musicales" y "los gorriones son peces voladores".

En la presente sección, se desarrolla un lenguaje formal para la lógica proposicional, se extiende éste a un sistema formal que emula el comportamiento descrito en el párrafo anterior y se le da una semántica por medio de "valores de verdad".

I. Sintaxis de la Lógica Proposicional

Es común en el estudio de sistemas formales separar a los símbolos de los alfabetos por su *aridad*. La aridad es un número no negativo asignado a cada símbolo que da información respecto al modo de leerlo en el contexto de un lenguaje formal. La información que ésta provee contesta a la pregunta "¿con cuántos argumentos opera dicho símbolo?" Como ejemplo considérese al símbolo comúnmente utilizado para representar la igualdad en matemáticas: "$=$". Es claro que para que el símbolo "$=$" adquiera un sentido en dicho contexto se requieren de otros dos símbolos (o colecciones de símbolos) en ambos lados de éste como en la expresión "$x = y$". En este caso, la aridad del símbolo "$=$" es dos, que es el número de argumentos con los cuales "trabaja". En el caso de la lógica proposicional, el alfabeto de ésta suele denotarse por la letra griega mayúscula omega: "Ω" y la aridad se señala separándolo en subconjuntos Ω_n donde n representa la aridad de los símbolos que Ω_n contiene.

Definición I.1 (Lenguaje Formal Proposicional)
A continuación se presenta un lenguaje que sirve para representar la lógica proposicional el cual será denotado por $PROP$:

- El alfabeto Ω está dividido en:
  - Los símbolos de aridad cero $\Omega_0 = \{(,), p_0, p_1, p_2, p_3, \ldots\}$. A su vez, estos símbolos se clasifican en símbolos de agrupación: $(,)$, y en letras proposicionales o átomos: $At = \{p_0, p_1, p_2, p_3, \ldots\}$
  - Los conectivos de aridad uno $\Omega_1 = \{\neg\}$
  - Los conectivos de aridad dos $\Omega_2 = \{\Rightarrow, \vee, \wedge, \Leftrightarrow\}$
- Las siguientes reglas describen recursivamente cómo construir *wffs* de $PROP$ que suelen ser llamadas también proposiciones:
  - (I) Si $p \in At$, entonces p es una proposición i.e. $p \in PROP$.
  - (II) Si φ es una proposición, entonces $\neg\varphi$ es una proposición.
  - (III) Si φ, ψ son proposiciones y $\circ \in \Omega_2$,[1] entonces $(\varphi \circ \psi)$ es una proposición.[2]
  - (IV) Ninguna otra cosa es una *wff* de $PROP$.

Es importante resaltar que el lenguaje $PROP$ no es el único que se puede construir para estudiar la lógica proposicional. Hay versiones alternativas en las que la lista de conectivos de aridad dos únicamente posee un elemento, ya sea $\Rightarrow$, $\wedge$ ó $\vee$, y los demás son expresados como metasímbolos abreviando *wffs*, por ejemplo, $(\varphi \vee \psi)$ puede ser la abreviación de $(\neg\varphi \Rightarrow \psi)$; hay otras en las que no existen varias clases de conectivos sino que únicamente se utiliza uno, ya sea $\uparrow$ ó $\downarrow$, e incluso existen lenguajes proposicionales en los que no es necesario tener símbolos de agrupación ya que la misma aridad permite la formación de proposiciones,

[1] En este caso $\circ$ es un metasímbolo para representar a todos los conectivos.
[2] Préstese especial importancia al uso de los paréntesis en la construcción de las *wffs* de $PROP$.

por ejemplo: $\Rightarrow\varphi\psi$ y $\wedge\varphi\psi$ pueden reemplazar a $(\varphi \Rightarrow \psi)$ y $(\varphi \wedge \psi)$ respectivamente, notación conocida como *forma polaca de la fórmula*. De esta manera, en la construcción de la gramática del lenguaje anterior, se pudieron haber reescrito los puntos (I), (II) y (III) en uno solo como a continuación:

- Si $\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_n$ son proposiciones y $\circ$ es un conectivo lógico de aridad "n" i.e. $\circ \in \Omega_n$, entonces $\circ\varphi_0\varphi_1 \ldots \varphi_n$ es una proposición.[3]

Por la naturaleza de la construcción del lenguaje $PROP$ es posible concebir el concepto de "demostración por inducción" el cual permitirá saber si determinada propiedad es satisfecha por todas las *wffs* de $PROP$ haciendo uso precisamente de la manera recursiva en cómo se definieron éstas:

Teorema I.1 (Principio de Inducción sobre la Complejidad de la Fórmula)
Una propiedad se cumple para toda *wff* del lenguaje $PROP$ si y sólo si se satisfacen las siguientes tres condiciones:

(1) Todas las letras proposicionales $p \in At$ cumplen la propiedad.

(2) Si la proposición φ cumple la propiedad, entonces $\neg\varphi$ cumple la propiedad.

(3) Si cualesquiera dos proposiciones φ y ψ cumplen la propiedad entonces también la cumplen las de la forma $(\varphi \circ \psi)$.

Demostración.
$(\Rightarrow)$ Supongamos que todas las proposiciones cumplen la propiedad. Por la gramática de $PROP$, esto significa que (1) todas las letras proposicionales cumplen la propiedad. Supóngase que las *wffs* φ y ψ cumplen la propiedad, entonces sabemos que la expresión $\neg\varphi$ y las de la forma $(\varphi\circ\psi)$ son proposiciones. Por lo tanto (2) $\neg\varphi$ cumple la propiedad y (3) $(\varphi \circ \psi)$ también.
$(\Leftarrow)$ Supongamos que las reglas $(1), (2)$ y (3) son satisfechas. La demostración se hará por inducción (de números naturales) sobre la longitud de la *wff*: $|\varphi|$. Si $|\varphi| = 1$ entonces $\varphi \in At$. Por la regla (1), φ cumple la propiedad. Supóngase que toda proposición de longitud menor a k cumple la propiedad y sea $\varphi \in PROP$ tal que $|\varphi| = k$. Por cómo se definió el lenguaje $PROP$, ó $\varphi = \neg\psi$ ó $\varphi = (\psi \circ \gamma)$ con $\psi, \gamma \in PROP$ y $\circ \in \Omega_2$. En ambos casos, ψ y γ tienen longitud menor a k y por hipótesis inductiva cumplen la propiedad. Aplicando la regla (2) ó (3), se tiene que φ cumple la propiedad. Por ende, dado cualquier número natural n, si $|\varphi| = n$, entonces la proposición φ cumple la propiedad. Dado que toda proposición es de longitud finita (por ser una cadena), toda proposición cumple la propiedad. ■

Con el principio de inducción sobre la complejidad de la fórmula se pueden comprobar diversas propiedades, un ejemplo sencillo es el siguiente:

[3] A partir de este punto se usará el símbolo "$\circ$" para representar a todos los conectivos lógicos clásicos de aridad dos i.e. $\wedge, \vee, \Rightarrow, \Leftrightarrow$.

Lema I.2
Todas las *wffs* del lenguaje $PROP$ tienen tantos paréntesis izquierdos "(" como paréntesis derechos ")".

Demostración. Si se establece que $A(\varphi)$ se lee como "φ tiene tantos paréntesis izquierdos como derechos", entonces se debe probar que A satisface las reglas $(1), (2)$ y (3) del principio de inducción sobre la complejidad de la fórmula:

(I) Las letras proposicionales $p_0, p_1, p_2, \ldots$ tienen 0 paréntesis izquierdos y 0 paréntesis derechos. Por lo tanto, $A(p)$ para cada $p \in At$.

(II) Asúmase como hipótesis de inducción que $A(\varphi)$ con $\varphi \in PROP$. Entonces $\neg\varphi$ tiene los mismos paréntesis que φ, de aquí que $A(\neg\varphi)$.

(III) Supóngase que $\varphi, \psi \in PROP$ y que $A(\varphi)$ y $A(\psi)$. Esto implica que $(\varphi \circ \psi)$ tiene los paréntesis de φ, los paréntesis de ψ, un izquierdo más y un derecho más. Así se tiene que $A((\varphi \circ \psi))$.

Por el principio de inducción sobre la complejidad de la fórmula, todas las proposiciones cumplen la propiedad A, es decir, todas las proposiciones tienen la misma cantidad de paréntesis izquierdos y derechos. ∎

Definición I.2 (Segmento inicial de una cadena)
Dada una cadena $\varphi := s_1 s_2 \ldots s_n \in \Omega^*$, un segmento inicial de φ es una cadena $\psi := s_1 s_2 \ldots s_m$ donde $0 \leq m \leq n$. Cuando $m < n$, se dice que ψ es segmento inicial *propio* de φ.

Lema I.3
Todo segmento inicial propio de una proposición ó es la cadena vacía λ ó es una sucesión de $\neg$'s ó tiene más paréntesis izquierdos "(" que derechos ")".

Demostración. Sea $B(\varphi)$ entendido por "todo segmento inicial propio de φ ó es la cadena vacía o es una sucesión de $\neg$'s ó tiene más paréntesis izquierdos que derechos", entonces:

(I) El único segmento inicial propio de las letras proposicionales $p_0, p_1, p_2, \ldots$ es la cadena vacía λ y, por ende, $B(p)$ para cada $p \in At$.

(II) Supóngase como hipótesis de inducción que $B(\varphi)$ con $\varphi \in PROP$, entonces todo segmento inicial propio de $\neg\varphi$ sólo agrega el símbolo $\neg$ a un segmento inicial propio de φ ó es λ ó es exactamente $\neg$ y, por lo tanto, $B(\neg\varphi)$.

(III) Asúmase que $\varphi, \psi \in PROP$ y que $B(\varphi)$ y $B(\psi)$. Esto implica que todo segmento inicial propio de $(\varphi \circ \psi)$ ó es λ ó agrega un paréntesis izquierdo, es decir, $B((\varphi \circ \psi))$.

Por el principio de inducción sobre la complejidad de la fórmula $B(\varphi)$ para cada $\varphi \in PROP$. ∎

Corolario I.4
Si $\varphi \in PROP$, ningún segmento inicial propio de φ puede ser una proposición.

Idea de Prueba. La demostración requiere de dos pequeñas inducciones probando que ni λ ni ninguna cadena de $\neg$'s es una proposición aunado a los resultados de los dos lemas anteriores. ■

Definición I.3 (Sucesiones Formativas)
Una sucesión formativa de la cadena $\varphi \in \Omega^*$ es una sucesión finita de fórmulas $\langle \varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_n \rangle \in \Omega^{*n}$ que cumplen dos condiciones:

1. La última cadena de la lista es φ, i.e. $\varphi_n = \varphi$.

2. Cada fórmula en la sucesión φ_i ó es un átomo o tiene alguna de las dos formas $\neg\varphi_j$ ó $(\varphi_j \circ \varphi_k)$ con $j, k < i$ y $\circ \in \Omega_2$.

Ejemplo I.1 Se ejemplifican los entes descritos por la definición anterior:

- $\langle p_0, p_1, (p_1 \wedge p_0) \rangle$ es una sucesión formativa de $(p_1 \wedge p_0)$.

- $\langle p_0, p_1, p_2, p_3, \neg p_2, \neg p_3, (\neg p_2 \Rightarrow \neg p_3), (p_1 \vee (\neg p_2 \Rightarrow \neg p_3)) \rangle$ es una sucesión formativa de $(p_1 \vee (\neg p_2 \Rightarrow \neg p_3))$.

- $\langle p_{25}, p_8, (p_8 \Rightarrow p_8), (p_{25} \Rightarrow p_{25}), \neg p_{25} \rangle$ es una sucesión formativa de $\neg p_{25}$ pero no de $(p_8 \Rightarrow p_8)$ porque ésta no es la última fórmula de la sucesión en cuestión.

- $\langle p_7, p_8, (p_8 \Rightarrow p_8), (p_7 \Rightarrow p_{25}), \neg p_7 \rangle$ <u>no</u> es una sucesión formativa de $\neg p_7$ porque la cuarta fórmula tiene una letra proposicional que no había sido escrita antes.

- $\langle p_0, p_1, \neg p_1, (p_0 \Rightarrow p_1), (p_1 \wedge p_0), (\neg p_0 \Rightarrow p_1) \rangle$ <u>no</u> es una sucesión formativa de $(\neg p_0 \Rightarrow p_1)$ porque la expresión $\neg p_0$ no aparece previamente en la sucesión.

Lema I.5
Toda proposición tiene una sucesión formativa.

Demostración. Sea C la propiedad "tiene una sucesión formativa". Entonces:

(I) Fácilmente se verifica que todas las letras proposicionales cumplen la propiedad C.

(II) Sea $\langle \varphi_0, \ldots, \varphi_n \rangle$ la sucesión formativa de φ. Agregando a esta la fórmula $\neg\varphi_n$ se obtiene la sucesión $\langle \varphi_0, \ldots, \varphi_n, \neg\varphi_n \rangle$, que es formativa de $\neg\varphi$. De aquí que $C(\neg\varphi)$.

(III) Supóngase como hipótesis de inducción que $C(\varphi)$ y $C(\psi)$. Enlistando una después de la otra las sucesiones formativas de φ y ψ, y agregando la expresión $(\varphi \circ \psi)$ se obtiene una sucesión formativa de $(\varphi \circ \psi)$. Por lo tanto $C((\varphi \circ \psi))$.

■

Teorema I.6
Las fórmulas con sucesiones formativas son exactamente las proposiciones.

Demostración. Reescribiendo el teorema: la expresión φ tiene sucesión formativa si y sólo si es una *fórmula bien formada* del lenguaje $PROP$:
($\Leftarrow$) El hecho de que una *wff* de $PROP$ tenga una sucesión formativa se resolvió en la demostración pasada.
($\Rightarrow$) Sea φ una fórmula con sucesión formativa $\langle\varphi_0, \varphi_1, \ldots, \varphi_n\rangle$, se demostrará lo requerido por inducción sobre "n":
Caso base: Si $n = 0$, la sucesión formativa de φ es únicamente $\langle\varphi_0\rangle$. La única forma de que ésto ocurra es que φ_0 sea un átomo lo cual implica que φ es una proposición.
Caso inductivo: Supóngase como hipótesis de inducción que cualquier fórmula ψ que tenga una sucesión formativa $\langle\psi_0, \ldots, \psi_n\rangle$ de tamaño $n < k$ es una proposición. Sea φ una fórmula con sucesión formativa $\langle\varphi_0, \varphi_1, \ldots, \varphi_k\rangle$ Por definición de sucesión formativa se tienen tres casos:

1. Si $\varphi = \varphi_k$ es atómica, por la gramática de $PROP$, la expresión φ es una proposición.
2. Si φ_k es de la forma $\neg\varphi_i$ con φ_i siendo una expresión anterior en la sucesión formativa, i.e. $i < k$, entonces la misma sucesión formativa hasta el punto $i < k$ es sucesión formativa de φ_i. Por la hipótesis de inducción φ_i es una proposición. De aquí que $\neg\varphi_i = \varphi_k = \varphi \in PROP$.
3. Si φ_k es de la forma $(\varphi_i \circ \varphi_j)$, la prueba es análoga al caso anterior.

Por lo tanto, la expresión φ tiene sucesión formativa si y sólo si es una proposición.
■

El resultado anterior está diciendo que otra forma de definir al lenguaje $PROP$ es por medio de sucesiones formativas. Es decir, en vez de dar la gramática inductivamente como se hizo al inicio de la sección, se pudo haber dicho que φ es una proposición si y sólo si es la última expresión de una sucesión formativa.

Para este momento el lector posiblemente ya ha notado que una proposición puede tener varias sucesiones formativas. Algunos ejemplos de esto para la proposición $(p_0 \to \neg p_1)$ son los siguientes:

- $\langle p_0, p_1, \neg p_1, (p_0 \to \neg p_1)\rangle$.
- $\langle p_1, p_0, \neg p_1, (p_0 \to \neg p_1)\rangle$.
- $\langle p_1, \neg p_1, p_0, (p_0 \to \neg p_1)\rangle$.
- $\langle p_{25}, p_3, \neg p_3, p_1, \neg p_1, p_0, (p_0 \to \neg p_1)\rangle$.

A pesar de que existen varias sucesiones para la misma proposición, existe un teorema asegurando que toda *wff* de $PROP$ va a ser "leída" de la misma manera sin importar las diferencias en orden y tamaño de sus sucesiones formativas. En otras palabras el siguiente teorema establece que no importa qué sucesión formativa se escoga para cierta proposición φ, siempre estará presente una misma "segmentación" mínima de φ en los elementos de la sucesión.

Teorema I.7 (Teorema de Legibilidad Única para $PROP$)
Toda *wff* de $PROP$ está exactamente en una de las siguientes formas:[4]

a. p_n con n, un número natural, i.e. es una letra proposicional o átomo.

b. $\neg\varphi$ siendo φ una proposición únicamente determinada, es decir, ya se ha identificado en qué caso de los tres φ está ubicada.

c. $(\varphi \circ \psi)$ siendo tanto φ como ψ proposiciones únicamente determinadas.

Demostración. En esta prueba se requieren demostrar tres cosas:

1. Que toda *wff* de $PROP$ está en alguna de las formas.
2. Que esa forma sólo es una, es decir, que no tiene dos o tres formas a la vez.
3. Que dentro de la misma forma para una *wff* no existen varios casos.

Para la primera parte, nuevamente y por ser una propiedad deseada para toda proposición, el método de elección es el de *inducción por complejidad de la fórmula*. Lo deseado se verifica rápidamente.

En cuanto a la segunda parte de la prueba, ya que el caso a. para cualquier *wff* es algún símbolo "p_i", el caso b. empieza con el símbolo "$\neg$" y el caso c, con el símbolo "(", no hay forma de que una misma proposición esté al mismo tiempo en dos o más de las formas en las que una *wff* puede estar ya que todos estos símbolos son distintos.

En el tercer punto, se debe corroborar que expresiones como $\neg p_0$ y $\neg p_1$ no podrían ser "leídas" o "interpretadas" de la misma manera:

a. Nótese que dadas dos letras proposicionales p_n y p_m, si $n \neq m$, entonces los átomos son diferentes. Esto está diciendo que si una proposición está en la forma a. entonces sólo puede ser representada por una <u>única</u> letra proposicional $p_i \in At$.

---

[4]En [End01], el enunciado de este teorema (equivalente al aquí expuesto) es: *las (cinco) operaciones de construcción de* wffs *restringidas a $PROP$ son inyectivas y tienen rangos ajenos a At y entre ellas, es decir, $PROP$ es libremente generado por Ω y las cinco operaciones (reglas) de construcción de* wffs.

b. Supongamos que γ está en la segunda forma y que $\gamma = \neg\varphi$ y $\gamma = \neg\psi$. Sabemos entonces que $\neg\varphi = \neg\psi$. Quitando al símbolo "$\neg$" se implica que $\varphi = \psi$. Por ende, toda proposición en la segunda forma está únicamente determinada.

c. Finalmente, se debe probar que si $(\varphi \circ \psi) = (\gamma * \chi)$ está en la tercera forma con $\circ, * \in \Omega_2$ y $\varphi, \psi, \gamma, \chi \in PROP$ únicamente determinadas, entonces $\varphi = \gamma$, $\circ = *$ y $\psi = \chi$. Eliminando el primer paréntesis se tiene que $\varphi\circ\psi) = \gamma*\chi)$. Por la hipótesis ó φ es segmento inicial de γ ó viceversa. Ya que ambas son proposiciones, por el corolario anterior no pueden ser segmentos iniciales propios. De aquí que $\varphi = \gamma$ y $\circ\psi) = *\chi)$. Con argumentos similares se concluye que $\circ = *$ y $\psi = \chi$.

■

La importancia del *Teorema de Legibilidad Única* radica en que es una condición necesaria para poder construir definiciones recursivas sobre $PROP$:

Teorema I.8 (Teorema de la Definición por Recursión en $PROP$)
Sea X cualquier conjunto y supóngase que se tienen cinco funciones $H_{At} : At \to X$, $H_\neg : X \to X$ y $H_\circ : X^2 \to X$ con $\circ \in \Omega_2$. Entonces existe una única función $F : PROP \to X$ tal que:

$$F(\varphi) = \begin{cases} H_{At}(\varphi) & \text{si } \varphi \in At \\ H_\neg(F(\psi)) & \text{si } \varphi = \neg\psi \\ H_\circ(F(\psi), F(\gamma)) & \text{si } \varphi = (\psi \circ \gamma) \end{cases}$$

Idea de Prueba. Por inducción sobre los naturales demuéstrese que para cada número natural n, si $|\varphi| = n$ entonces (1) existe una (2) única función F_n que va del conjunto de proposiciones de longitud n al conjunto X. Demuéstrese posteriormente que las funciones F_n son compatibles y finalmente revísese que $F := \bigcup_{n\in\mathbb{N}} F_n$ es la función deseada. Para una versión más extensa revísese [Cu14]. ■

Algebraicamente el teorema anterior está diciendo que cualquier función de At a X puede ser extendida a un "homomorfismo" de $PROP$ en X, pero en la práctica, como su nombre lo dice, el teorema permite realizar diversas definiciones de conceptos que dependen de la estructura gramatical de $PROP$.

Ejemplo I.2 Los siguientes son ejemplos de conceptos definidos recursivamente:

1. La *Longitud de una proposición* $L : PROP \to \mathbb{N}$ se define mediante:

$$L(p) = 1$$
$$L(\neg\varphi) = L(\varphi) + 1$$
$$L((\varphi \circ \psi)) = L(\varphi) + L(\psi) + 1$$

Se verifica que para cada $\varphi \in PROP$, $L(\varphi) = |\varphi|$.

2. El *Número de conectivos de una proposición* $C : PROP \to \mathbb{N}$ corresponde a:

$$C(p) = 0$$
$$C(\neg\varphi) = C(\varphi) + 1$$
$$C((\varphi \circ \psi)) = C(\varphi) + C(\psi) + 1$$

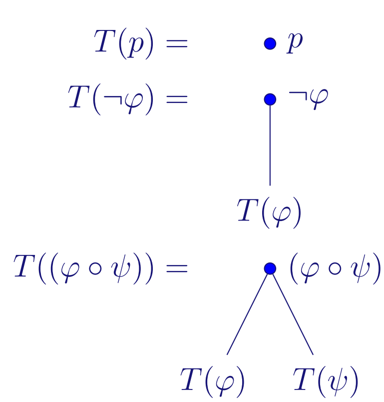
3. Más aun, para $\psi, \gamma \in PROP$ podemos definir la *Sustitución de* ψ *por* γ *en* φ, $[\psi/\gamma](\varphi) : PROP \to PROP$, de la siguiente manera:

$$[\psi/\gamma](p) = \begin{cases} \gamma & \text{si } \psi = p \\ p & \text{si } \psi \neq p \end{cases}$$
$$[\psi/\gamma](\neg\varphi) = \neg[\psi/\gamma](\varphi)$$
$$[\psi/\gamma]((\varphi \circ \chi)) = ([\psi/\gamma](\varphi) \circ [\psi/\gamma](\chi))$$

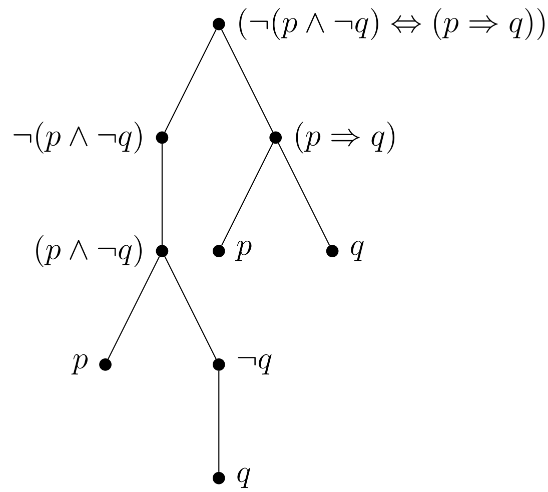
4. El *rango* de una proposición φ se calcula con:

$$r(p) = 0$$
$$r(\neg\varphi) = r(\varphi) + 1$$
$$r((\varphi \circ \psi)) = \max\{r(\varphi), r(\psi)\} + 1$$

5. Finalmente, el *Árbol de análisis gramático de una proposición* se obtiene por:



Considérese la proposición $(\neg(p \wedge \neg q) \Leftrightarrow (p \Rightarrow q))$ y obsérvese su árbol de análisis gramático:



Nótese que las proposiciones en dicho árbol pueden colocarse en una sucesión formativa: $\langle q, p, \neg q, (p \wedge \neg q), \neg(p \wedge \neg q), (p \Rightarrow q), (\neg(p \wedge \neg q) \Leftrightarrow (p \Rightarrow q))\rangle$. Esto es un indicador de que estos árboles pueden contener en sus nodos la "parte común" de todas las sucesiones formativas. Los elementos de ésta parte común son las llamadas *subfórmulas*:

Definición I.4 (Subfórmula y partes de una proposición)
Para emplear el principio de extensionalidad para las proposiciones es necesario saber qué es una subfórmula, por lo cual se procede a definir a continuación dicho concepto junto con otros relacionados:

a. *(Conjunto de subfórmulas)* El conjunto de subfórmulas de una proposición φ se obtiene mediante:

$$\begin{aligned} Sub(p) &= \{p\} \\ Sub(\neg\varphi) &= Sub(\varphi) \cup \{\neg\varphi\} \\ Sub((\varphi \circ \psi)) &= Sub(\varphi) \cup Sub(\psi) \cup \{(\varphi \circ \psi)\} \end{aligned}$$

b. *(Subfórmula o Parte Bien Formada)* Dada $\varphi \in PROP$, se dirá que una proposición ψ es una subfórmula o una parte bien formada de φ si $\psi \in Sub(\varphi)$.

c. *(Alcance de un conectivo)* Si φ es una *wff* de $PROP$ en la que aparece una instancia de un conectivo $\circ \in \Omega_1$ ó $\circ \in \Omega_2$, se le llama alcance del conectivo a la parte bien formada más pequeña que contenga dicha instancia.

d. *(Conectivo Principal)* Dada una proposición φ, se dice que $\circ \in \Omega_i$ con $i = 1$ ó $i = 2$ es el conectivo principal de φ si y sólo si el alcance de una instancia de éste es toda φ.

Ejemplo I.3 En la proposición:

$$(((\neg p_0 \Rightarrow \neg p_1) \Rightarrow (p_1 \Rightarrow p_0)) \Leftrightarrow (\neg(p_0 \wedge p_1) \Leftrightarrow (\neg p_0 \vee \neg p_1)))$$

- Algunas de sus subfórmulas son: la proposición en su totalidad y otras más sencillas como $\neg p_0$, p_1, $\neg p_1$,$(\neg p_0 \Rightarrow \neg p_1)$, $(\neg p_0 \vee \neg p_1)$ y $((\neg p_0 \Rightarrow \neg p_1) \Rightarrow (p_1 \Rightarrow p_0))$.

- Por otro lado la subfórmula $(\neg(p_0 \wedge p_1) \Leftrightarrow (\neg p_0 \vee \neg p_1))$ es una parte bien formada de la proposición mientras que la expresión "$\neg p_1) \Rightarrow (p_1 \Rightarrow p_0)) \Leftrightarrow (\neg$" no lo es.

- El alcance del primer "$\Rightarrow$" que aparece en la proposición en questión es la subfórmula $(\neg p_0 \Rightarrow \neg p_1)$ y el alcance del único "$\vee$" es $(\neg p_0 \vee \neg p_1)$.

- El conectivo principal de toda la *wff* es el primer "$\Leftrightarrow$".

Como comentario final respecto a los objetos definidos al final de esta subsección, es posible hacer pruebas por inducción respecto al rango de una proposición, longitud de una expresión, el número de posiciones en la cadena en las que hay conectivos y similares conceptos. Dichos métodos son necesarios a veces para probar propiedades del lenguaje $PROP$ y se pueden mostrar equivalentes al *principio de inducción por complejidad de la fórmula* demostrado aquí. Para ver un ejemplo de ésto revísese [VD04].

II. Semántica para la Lógica Proposicional

Un principio central para el estudio de la lógica proposicional -mencionado al inicio de la sección- es el de *extensionalidad de las proposiciones*, el cual dicta que el valor de verdad de una proposición depende del de sus subfórmulas. Esto motiva todo el análisis sintáctico efectuado en la subsección previa pues para definir funciones de valores de verdad que se extiendan a todo $PROP$ es necesario que sea válido el teorema de la recursión para dicho lenguaje. A continuación emplearemos los resultados anteriores para definir una semántica formal de la lógica proposicional:

Definición I.5 (Valuación)
Una valuación o *asignación de valores de verdad atómica* consiste en una función $v : At \to \{0, 1\}$ que asigna a cada letra proposicional un "valor de verdad".

Nótese que, por el teorema de la recursión, toda valución atómica $v : At \to \{0, 1\}$ puede ser extendida recursivamente a una única *asignación de valores de verdad proposicional* $[\![\cdot]\!]_v : PROP \to \{0, 1\}$ a través de:

$$
\begin{aligned}
[\![p]\!]_v &= v(p) \\
[\![\neg\varphi]\!]_v &= 1 - [\![\varphi]\!]_v \\
[\![(\varphi \wedge \psi)]\!]_v &= \text{mín}\{[\![\varphi]\!]_v, [\![\psi]\!]_v\} \\
[\![(\varphi \vee \psi)]\!]_v &= \text{máx}\{[\![\varphi]\!]_v, [\![\psi]\!]_v\} \\
[\![(\varphi \Rightarrow \psi)]\!]_v &= \begin{cases} 1 & \textbf{si } [\![\varphi]\!]_v \leq [\![\psi]\!]_v \\ 0 & \textbf{si } [\![\varphi]\!]_v > [\![\psi]\!]_v \end{cases} \\
[\![(\varphi \Leftrightarrow \psi)]\!]_v &= \begin{cases} 1 & \textbf{si } [\![\varphi]\!]_v = [\![\psi]\!]_v \\ 0 & \textbf{si } [\![\varphi]\!]_v \neq [\![\psi]\!]_v \end{cases}
\end{aligned}
$$

El lector puede verificar que esta forma de definir valuaciones corresponde a las ya conocidas tablas de verdad para las proposiciones:

φ	ψ	$\neg\varphi$	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \Rightarrow \psi$	$\varphi \Leftrightarrow \psi$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Obsérvese que no es necesario realmente definir a las valuaciones como funciones con destino en $\{0, 1\}$. Un conjunto de cualesquiera dos elementos $\{V, F\}$ es suficiente, aunque la definición recursiva debe modificarse para no incluir operaciones aritméticas como las usadas aquí.

Continuando con el objetivo de probar el principio de extensionalidad se da la siguiente definición:

Definición I.6 (Soporte de una proposición)
Recursivamente se define el soporte o conjunto de átomos de una proposición por:

$$
\begin{aligned}
\text{Sop}(p) &= \{p\} \\
\text{Sop}(\neg\varphi) &= \text{Sop}(\varphi) \\
\text{Sop}((\varphi \circ \psi)) &= \text{Sop}(\varphi) \cup \text{Sop}(\psi)
\end{aligned}
$$

Así, se verifica lo siguiente:

Teorema I.9 (Principio de extensionalidad)
Sean $\varphi \in PROP$ y $v, \mu : At \to \{0, 1\}$ dos valuaciones atómicas tales que para cada $p \in \text{Sop}(\varphi)$ se cumple que $v(p) = \mu(p)$, entonces $[\![\varphi]\!]_v = [\![\varphi]\!]_\mu$.

Demostración. Se demostrará por inducción sobre la complejidad de la fórmula:

a. Si φ es un átomo, por hipótesis ya se tiene que $[\![\varphi]\!]_v = v(\varphi) = \mu(\varphi) = [\![\varphi]\!]_\mu$.

b. Supóngase que es cierto que para cada $p \in \mathrm{Sop}(\varphi)$ si se cumple $v(p) = \mu(p)$, entonces $[\![\varphi]\!]_v = [\![\varphi]\!]_\mu$. Se computa lo deseado: $[\![\neg\varphi]\!]_v = 1 - [\![\varphi]\!]_v = 1 - [\![\varphi]\!]_\mu = [\![\neg\varphi]\!]_\mu$.

c. Un cálculo similar al anterior para cada uno de los conectivos demuestra lo deseado en el resto de los casos.

■

Con lo hecho recientemente el lector ya debería sospechar que la semántica que se está construyendo está constituida por las valuaciones proposicionales. Lo único que resta por hacer es definir la relación de satisfactibilidad entre una proposición y una valuación para así derivar todos los conceptos vistos al final del capítulo previo:

Definición I.7 (Satisfactibilidad)
Dadas una proposición $\varphi \in PROP$ y una valuación $v : At \to \{0,1\}$, se dice que v satisface a φ, i.e. $\models_v \varphi$ si y sólo si $[\![\varphi]\!]_v = 1$. La negación de esta relación se denota por $\not\models_v \varphi$. Se dice que una proposición φ es *satisfactible* si existe una valuación que la satisfaga, en caso contrario se dice que φ es *insatisfactible* o *contradictoria*.

Es un ejercicio rutinario verificar las siguientes propiedades:

$$\begin{gathered}
\models_v \neg\varphi \text{ sii } \not\models_v \varphi \\
\models_v (\varphi \wedge \psi) \text{ sii } \models_v \varphi \text{ y } \models_v \psi \\
\models_v (\varphi \vee \psi) \text{ sii } \models_v \varphi \text{ o } \models_v \psi \\
\models_v (\varphi \Rightarrow \psi) \text{ sii } \not\models_v \varphi \text{ o } \models_v \psi \\
\models_v (\varphi \Leftrightarrow \psi) \text{ sii } (\models_v \varphi \text{ y } \models_v \psi) \text{ o } (\not\models_v \varphi \text{ y } \not\models_v \psi)
\end{gathered}$$

De la definición anterior surgen las nociones expresadas en general al final del capítulo anterior: “consecuencia semántica” y “*wff* lógicamente válida” que en el caso de la lógica proposicional adquieren los nombres particulares de “consecuencia lógica” y “tautología” respectivamente[5]:

Definición I.8 (Consecuencia Lógica)
Una proposición $\varphi \in PROP$ es consecuencia lógica de un conjunto $\Gamma \subseteq PROP$ de premisas, lo cual se denota por $\Gamma \models \varphi$, si y sólo si toda valuación $v : At \to \{0,1\}$ que satisface a las *wffs* de Γ, también satisface a φ. Equivalentemente, se escribe $\Gamma \models \varphi$ sii para toda $v : At \to \{0,1\}$, si $\models_v \psi$ para cada $\psi \in \Gamma$, entonces $\models_v \varphi$.

Definición I.9 (Tautología)
Una proposición $\varphi \in PROP$ es una tautología, expresado por $\models \varphi$, si toda valuación $v : At \to \{0,1\}$ la satisface[6], i.e. $\models_v \varphi$.

[5]Lo mismo ocurre para conjuntos de proposiciones, es decir la relacion de que una valuación $v : At \to \{0,1\}$ satisfaga a la teoría $\Gamma \subseteq PROP$: $\models_v \Gamma$. En dicho caso recuérdese que Γ es llamada *consistente*.

[6]Equivalentemente, si es consecuencia lógica del conjunto vacío.

Es posible definir en $PROP$ una relación de equivalencia por medio de la consecuencia lógica. Primero nótese que si $\varphi, \psi \in PROP$ son proposiciones entonces $\{\varphi\} \models \psi$ y $\{\psi\} \models \varphi$ si y sólo si $\models \varphi \Leftrightarrow \psi$. Así, definimos la relación "$\equiv$" por medio de: $\varphi \equiv \psi$ si y sólo si $\models \varphi \Leftrightarrow \psi$. Es fácil verificar que ésta es reflexiva, simétrica y transitiva.

La importancia de la relación "$\equiv$" recae en que, junto con el siguiente teorema y algunas otras propiedades, permite manipular las proposiciones como entes algebraicos, es decir, permite hablar de un *cálculo proposicional*. Para ello recuérdese la definición recursiva de sustitución de una *wff* de $PROP$ ψ por otra γ en una tercera φ denotada por $[\psi/\gamma](\varphi) : PROP \to PROP$ y definida mediante:

$$[\psi/\gamma](p) = \begin{cases} \gamma & \text{si } \psi = p \\ p & \text{si } \psi \neq p \end{cases}$$
$$[\psi/\gamma](\neg\varphi) = \neg[\psi/\gamma](\varphi)$$
$$[\psi/\gamma]((\varphi \circ \chi)) = ([\psi/\gamma](\varphi) \circ [\psi/\gamma](\chi))$$

Lema I.10
Dadas tres proposiciones φ_1, φ_2 y ψ; una letra proposicional $p \in At$, y una valuación atómica $v : At \to \{0, 1\}$, se cumple que:

- $[\![(\varphi_1 \Leftrightarrow \varphi_2)]\!]_v \leq [\![([p/\varphi_1](\psi) \Leftrightarrow [p/\varphi_2](\psi))]\!]_v$
- $\models ((\varphi_1 \Leftrightarrow \varphi_2) \Rightarrow ([p/\varphi_1](\psi) \Leftrightarrow [p/\varphi_2](\psi)))$

Demostración. Para la primera parte es suficiente considerar sólo las valuaciones en las que $[\![(\varphi_1 \Leftrightarrow \varphi_2)]\!]_v = 1$ porque si su valor fuese 0 ya se tendría el resultado. Procediendo por inducción sobre la complejidad de ψ:

a. Se tienen dos casos:
   - Si $\psi = p$, entonces $[p/\varphi_i](\psi) = \varphi_i$ con $i \in \{0, 1\}$. De aquí se obtiene el cómputo $[\![([p/\varphi_1](\psi) \Leftrightarrow [p/\varphi_2](\psi))]\!]_v = [\![(\varphi_1 \Leftrightarrow \varphi_2)]\!]_v = 1$.
   - Si $\psi \neq p$, entonces $[p/\varphi_i](\psi) = \psi$ con $i \in \{1, 2\}$. Así, efectuando los cálculos adecuados $[\![([p/\varphi_1](\psi) \Leftrightarrow [p/\varphi_2](\psi))]\!]_v = [\![(\psi \Leftrightarrow \psi)]\!]_v = 1$.

b. Por hipótesis inductiva se tiene que $[\![([p/\varphi_1]([p/\varphi_1](\psi) \Leftrightarrow [p/\varphi_2](\psi))]\!]_v = 1$, lo cual implica que $[\![[p/\varphi_1](\psi)]\!]_v = [\![[p/\varphi_2](\psi)]\!]_v$. Así $1 - [\![[p/\varphi_1](\psi)]\!]_v = 1 - [\![[p/\varphi_2](\psi)]\!]_v$, de donde finalmente se tiene $[\![([p/\varphi_1](\neg\psi) \Leftrightarrow [p/\varphi_2](\neg\psi))]\!]_v = 1$.

c. Cómputos similares al caso anterior sirven para el resto de los casos ya que $[\![[p/\varphi_i]((\psi_1 \circ \psi_2))]\!]_v = [\![([p/\varphi_i](\psi_1) \circ [p/\varphi_i](\psi_2))]\!]_v$ está únicamente determinado por sus partes $[\![[p/\varphi_i](\psi_j)]\!]_v$ con $i, j \in \{1, 2\}$.

Para la segunda parte, verificando rápidamente que $\models \varphi \Rightarrow \psi$ sii $[\![\varphi]\!]_v \leq [\![\psi]\!]_v$, se demuestra que $\models ((\varphi_1 \Leftrightarrow \varphi_2) \Rightarrow ([p/\varphi_1](\psi) \Leftrightarrow [p/\varphi_2](\psi)))$ si y sólo si es válido el resultado recientemente probado. ∎

Teorema I.11 (Teorema de la Substitución)
Sean $\varphi_1, \varphi_2, \psi \in PROP$ tres proposiciones, $p \in At$ y $v : At \to \{0,1\}$ una valuación, entonces si $\models (\varphi_1 \Leftrightarrow \varphi_2)$, también $\models ([p/\varphi_1](\psi) \Leftrightarrow [p/\varphi_2](\psi))$.

Demostración. Inmediato usando el lema anterior. ■

Tras haber usado suficientemente el Teorema de Legibilidad Única es posible aceptar las siguientes convenciones para evitar el uso excesivo de paréntesis y facilitar la lectura al ojo humano:

- Se eliminan paréntesis externos, i.e. en lugar de $(\varphi \circ \psi)$ simplemente se escribirá $\varphi \circ \psi$.

- (0) Lo que está entre paréntesis equivale a un solo objeto para la aridad de cualquier conectivo. (1) El alcance de $\neg$ es tan corto como sea posible de acuerdo a (0). (2) El alcance de $\wedge, \vee$ es tan corto como es posible respetando (0) y (1). El alcance de $\Rightarrow, \Leftrightarrow$ es tan corto como sea posible respetando $(0), (1)$ y (2). De manera resumida, estas reglas se expresan en la siguiente tabla:

Jerarquía	Conectivo
0	( )
1	$\neg$
2	$\vee, \wedge$
3	$\Rightarrow, \Leftrightarrow$

  Por ejemplo, la cadena $\neg(p_0 \vee p_1) \Leftrightarrow \neg p_0 \wedge \neg p_1$ realmente representa la proposición $(\neg(p_0 \vee p_1) \Leftrightarrow (\neg p_0 \wedge \neg p_1))$.

- Cuando un solo conectivo de aridad dos $\circ \in \Omega_2$ se usa consecutivamente $\varphi_1 \circ \varphi_2 \circ ... \circ \varphi_n$ la convención es agrupar a la derecha $(\varphi_1 \circ (\varphi_2 \circ (... \circ \varphi_n)...))$.

- Si un conectivo binario es asociativo, i.e. si $((\varphi \circ \psi) \circ \gamma) \equiv (\varphi \circ (\psi \circ \gamma))$, se podrán eliminar paréntesis internos: $(\varphi \circ \psi \circ \gamma)$.

- En lugar de $\{\psi_1, \psi_2, ..., \psi_n\} \vdash \psi$ ó $\{\psi_1, \psi_2, ..., \psi_n\} \models \psi$ se podrán eliminar las llaves externas del conjunto, i.e. $\psi_1, \psi_2, ..., \psi_n \vdash \psi$ y $\psi_1, \psi_2, ..., \psi_n \models \psi$ respectivamente.

Propiedades I.12
A continuación se da una lista de algunas propiedades computables en el cálculo de proposiciones asumiendo $\varphi, \psi, \gamma \in PROP$:

1. *Leyes Conmutativas*
   - $\models \varphi \vee \psi \Leftrightarrow \psi \vee \varphi$
   - $\models \varphi \wedge \psi \Leftrightarrow \psi \wedge \varphi$
   - $\models (\varphi \Leftrightarrow \psi) \Leftrightarrow (\psi \Leftrightarrow \varphi)$

2. *Leyes Asociativas*
   - $((\varphi \vee \psi) \vee \gamma) \equiv (\varphi \vee (\psi \vee \gamma))$
   - $((\varphi \wedge \psi) \wedge \gamma) \equiv (\varphi \wedge (\psi \wedge \gamma))$
   - $((\varphi \Leftrightarrow \psi) \Leftrightarrow \gamma) \equiv (\varphi \Leftrightarrow (\psi \Leftrightarrow \gamma))$

3. *Leyes Distributivas*
   - $\models \varphi \vee (\psi \wedge \gamma) \Leftrightarrow (\varphi \vee \psi) \wedge (\varphi \vee \gamma)$
   - $\models \varphi \wedge (\psi \vee \gamma) \Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \gamma)$
4. *Leyes de De Morgan*
   - $\models \neg(\varphi \vee \psi) \Leftrightarrow (\neg\varphi \wedge \neg\psi)$
   - $\models \neg(\varphi \wedge \psi) \Leftrightarrow (\neg\varphi \vee \neg\psi)$
5. *Leyes de Idempotencia*
   - $\models \varphi \vee \varphi \Leftrightarrow \varphi$
   - $\models \varphi \wedge \varphi \Leftrightarrow \varphi$
6. *Ley de la doble negación*
   - $\models \neg\neg\varphi \Leftrightarrow \varphi$
7. *Ley del Tercio Excluso*
   - $\models \varphi \vee \neg\varphi$
8. *Contrapositiva o contrarrecíproca*
   - $\models (\varphi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\varphi)$
9. *Exportación*
   - $\models (\varphi \wedge \psi \Rightarrow \gamma) \Leftrightarrow (\varphi \Rightarrow \psi \Rightarrow \gamma)$
10. Cuatro tautologías "arbitrarias" entre la implicación y la negación:
    - $\models \varphi \Rightarrow \psi \Rightarrow \varphi$
    - $\models (\varphi \Rightarrow \psi \Rightarrow \gamma) \Rightarrow (\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \gamma)$
    - $\models (\neg\psi \Rightarrow \neg\varphi) \Rightarrow ((\neg\psi \Rightarrow \varphi) \Rightarrow \psi)$
    - $\models (\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$
11. *Equivalencias a la Implicación*
    - $\models (\varphi \Rightarrow \psi) \Leftrightarrow \neg(\varphi \wedge \neg\psi)$
    - $\models (\varphi \Rightarrow \psi) \Leftrightarrow \neg\varphi \vee \psi$
    - $\models (\varphi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\varphi)$
12. *Equivalencias a la Conjunción*
    - $\models (\varphi \wedge \psi) \Leftrightarrow \neg(\varphi \Rightarrow \neg\psi)$
    - $\models (\varphi \wedge \psi) \Leftrightarrow \neg(\neg\varphi \vee \neg\psi)$
13. *Equivalencias a la Disyunción*
    - $\models (\varphi \vee \psi) \Leftrightarrow \neg\varphi \Rightarrow \psi$
    - $\models (\varphi \vee \psi) \Leftrightarrow \neg(\neg\varphi \wedge \neg\psi)$
14. *Equivalencia a la Bicondicional*
    - $\models (\varphi \Leftrightarrow \psi) \Leftrightarrow (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$
15. *Modus Ponendo Ponens* abreviado como *Modus Ponens* MP es una regla de deducción lógica que dicta:
    - $\varphi, \varphi \Rightarrow \psi \models \psi$
16. *Modus Tollendo Tollens* abreviado como *modus tollens* MT es una regla de deducción lógica que dicta:
    - $\neg\psi, \varphi \Rightarrow \psi \models \neg\varphi$
17. *Contradicciones* destacadas en el cálculo proposcional, es decir, *wffs* de $PROP$ cuya asignación de valores de verdad $[\![\cdot]\!]_v$ siempres es 0:
    - $\varphi \wedge \neg\varphi$
    - $\neg(\neg\varphi \vee \varphi)$
    - $\neg(\varphi \Rightarrow \varphi)$

Como último comentario para la subsección, otra modificación común al lenguaje $PROP$ consiste en agregar uno o dos conectivos de aridad cero $\bot, \top \in \Omega_0$. En la construcción de *wffs* se manejan como letras proposicionales y su objetivo es representar el concepto de *contradicción* y *tautología* dentro del mismo lenguaje. Esto implica que toda valuación $v : At \to \{0, 1\}$ cumple que $[\![\bot]\!]_v = 0$ y que $[\![\top]\!]_v = 1$. En consecuencia, en dichos sistemas, se agregan algunas propiedades a la lista anterior:

- $\models \bot \vee \varphi \Leftrightarrow \varphi$
- $\models \bot \Leftrightarrow \varphi \wedge \neg\varphi$
- $\models \top \wedge \varphi \Leftrightarrow \varphi$
- $\models \neg\varphi \Leftrightarrow (\varphi \Rightarrow \bot)$
- $\models \top \Leftrightarrow (\bot \Rightarrow \bot)$

III. Sistema Formal para la Lógica Proposicional

Una vez hecha explícita la semántica se debe definir un aparato deductivo para la lógica proposicional. No obstante, por motivos de brevedad será conveniente adoptar otro lenguaje distinto a $PROP$ tal que:

I. Si $p \in At$, entonces p es una proposición.

II. Si φ es una proposición, entonces $\neg\varphi$ es una proposición.

III. Si φ, ψ son proposiciones, entonces $(\varphi \Rightarrow \psi)$ es una proposición

IV. Ninguna otra cosa es una proposición.

Es mero trabajo formal revisar que todo lo demostrado para $PROP$ es válido para este lenguaje. Por ende las mismas convenciones sobre notación son asimilables y, con base en las propiedades presentadas al final de la subsección anterior, se adoptan las siguientes. Si φ, ψ son proposiciones, entonces:

- $(\varphi \wedge \psi)$ es una meta-abreviación para $\neg(\varphi \Rightarrow \neg\psi)$.
- $(\varphi \vee \psi)$ es una meta-abreviación para $(\neg\varphi \Rightarrow \psi)$.
- $(\varphi \Leftrightarrow \psi)$ es una meta-abreviación para $((\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi))$.

Los axiomas del aparato deductivo que se utilizará son atribuidos a Jan Łukasiewicz y corresponden a todas las *wffs* de la forma:

A1. $\varphi \Rightarrow (\psi \Rightarrow \varphi)$

A2. $(\varphi \Rightarrow (\psi \Rightarrow \gamma)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \gamma))$

A3. $(\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$

siendo φ, ψ, γ proposiciones. Informalmente los axiomas están aseverando respectivamente que (A1) "una proposición implica que cualquier cosa la implica", (A2) "la implicación entre proposiciones es distributiva por izquierda" y (A3) "la ley de la contrarrecíproca es un axioma". Finalmente, la única regla de inferencia es *Modus Ponens*, la cual dicta que si se sabe que φ y también que $\varphi \Rightarrow \psi$, entonces podemos deducir a ψ, i.e. $\varphi, \varphi \Rightarrow \psi \vdash \psi$ ó:

$$\frac{\varphi \quad \varphi \Rightarrow \psi}{\psi} MP$$

En resúmen, se tiene lo siguiente:

Definición I.10 (Sistema Formal de Łukasiewicz)
Dado un lenguaje proposicional generado por las reglas I., II., III. y IV., el sistema formal Ł sobre este lenguaje con axiomas A1, A2 y A3, y única regla de inferencia MP será llamado sistema formal de Łukasiewicz.

A partir de este punto se abusará de la notación y se utilizará el nombre $PROP$ para el conjunto de *wffs* del nuevo lenguaje y el símbolo Ł para hacer referencia tanto al aparato deductivo como al conjunto de axiomas, el de reglas de inferencia, el sistema formal y la teoría matemática generada por éstos.

Como dato histórico cabe señalar que el conjunto de 6 esquemas de axiomas originales del sistema formal Ł era:

- $\star\ \varphi \Rightarrow (\psi \Rightarrow \varphi)$
- $\star\ \varphi \Rightarrow (\psi \Rightarrow \gamma)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \gamma)$
- $\star\ (\varphi \Rightarrow (\psi \Rightarrow \gamma)) \Rightarrow (\psi \Rightarrow (\varphi \Rightarrow \gamma))$
- $\star\ (\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$
- $\star\ \varphi \Rightarrow \neg\neg\varphi$
- $\star\ \neg\neg\varphi \Rightarrow \varphi$

con φ, ψ y γ en $PROP$. Éstos, fueron publicados por Gottlob Frege y, posteriormente, el trabajo conjunto de Alfred Tarski y Jan Łukasiewicz mostró que el tercero era redundante pues se podía deducir a partir de los primeros dos y *Modus Ponens*. Finalmente, Łukasiewicz probó que los últimos tres podían ser reemplazados por A3.

El siguiente es un pequeño meta-lema respecto al sistema formal de Łukasiewicz. Éste establece que para toda proposición φ, la expresión $\varphi \Rightarrow \varphi$ es un teorema en Ł. Para demostrarlo se requiere exhibir una prueba formal de la instancia de teorema, es decir, una sucesión finita de *wffs* tales que cada una o es axioma de Ł o es resultado de aplicar *Modus Ponens* a dos anteriores. La justificacion de cada fórmula expuesta en la prueba se da a la derecha de la misma.

Lema I.13 (Ley de Identidad - ID)
Para $\varphi \in PROP$, se cumple que $\vdash_{Ł} \varphi \Rightarrow \varphi$

Demostración. Se exhibe una prueba formal de la proposición objetivo:

1.	$\varphi \Rightarrow ((\psi \Rightarrow \varphi) \Rightarrow \varphi)$	A1
2.	$(\varphi \Rightarrow ((\psi \Rightarrow \varphi) \Rightarrow \varphi)) \Rightarrow ((\varphi \Rightarrow (\psi \Rightarrow \varphi)) \Rightarrow (\varphi \Rightarrow \varphi))$	A2
3.	$(\varphi \Rightarrow (\psi \Rightarrow \varphi)) \Rightarrow (\varphi \Rightarrow \varphi)$	MP(1,2)
4.	$\varphi \Rightarrow (\psi \Rightarrow \varphi)$	A1
5.	$\varphi \Rightarrow \varphi$	MP(3,4)
$\therefore$	$\vdash_{Ł} \varphi \Rightarrow \varphi$	

$\blacksquare$

A continuación se demuestra uno de los teoremas más importantes de lógica proposicional, *el teorema de la deducción* o *regla de la prueba condicional*. Su uso es tan frecuente en lógica que en ocasiones se agrega directamente como una regla de inferencia en el aparato deductivo con la forma:

$$\frac{\Gamma, \varphi \vdash_{Ł} \psi}{\Gamma \vdash_{Ł} \varphi \Rightarrow \psi} CP$$

Su importancia recae en que permite el cálculo de demostraciones formales en menos pasos de los que se escribirían si se hiciese la prueba completa:

Teorema I.14 (Teorema de la Deducción - CP)
Si $\varphi \in PROP$ es una premisa en una prueba Δ de ψ a partir de Γ, i.e. $\Gamma, \varphi \vdash_{Ł} \psi$, entonces existe una prueba Δ' de $\varphi \Rightarrow \psi$ a partir de Γ que no usa a φ como premisa, es decir $\Gamma \vdash_{Ł} \varphi \Rightarrow \psi$.

Demostración. La demostración es por inducción sobre la longitud de la prueba $\Delta = \langle \psi_1, \psi_2, \ldots \psi_n \rangle$: Si $\Gamma \subseteq PROP$ y φ, ψ son proposiciones tales que $\Gamma \cup \{\varphi\} \vdash_{Ł} \psi$ con una prueba de longitud $n = 1$, entonces la prueba de ψ, Δ, realmente es $\Delta = \langle \psi_1 \rangle = \langle \psi \rangle$. De aquí que, como ψ no puede ser deducida con MP a partir de dos proposiciones anteriores en la prueba, o ψ es un axioma o $\psi \in \Gamma$ o $\psi = \varphi$. Así:

(I) Si ψ es un axioma, entonces $\vdash_{Ł} \psi \Rightarrow (\varphi \Rightarrow \psi)$ (A1) y $\vdash_{Ł} \psi$. Aplicando *Modus Ponens* se obtiene que $\vdash_{Ł} \varphi \Rightarrow \psi$. Ya que $\emptyset \subseteq \Gamma$, se concluye que $\Gamma \vdash_{Ł} \varphi \Rightarrow \psi$.

(II) Si $\psi \in \Gamma$, procediendo de la misma forma que en el inciso anterior se tiene que $\Gamma \vdash_{Ł} \psi \Rightarrow (\varphi \Rightarrow \psi)$ y $\Gamma \vdash_{Ł} \psi$, así, por *Modus Ponens*, $\Gamma \vdash_{Ł} \varphi \Rightarrow \psi$.

(III) Si $\psi = \varphi$, por el lema anterior sabemos que $\vdash_{Ł} \varphi \Rightarrow \varphi$. Substituyendo metavariables: $\vdash_{Ł} \varphi \Rightarrow \psi$. Procediendo igual que en el primer caso, $\Gamma \vdash_{Ł} \varphi \Rightarrow \psi$.

Como hipóstesis de inducción asúmase que para toda fórmula ψ, si existe una prueba de longitud $n < k$ de ψ a partir de $\Gamma \cup \{\varphi\}$, entonces existe una prueba de $\varphi \Rightarrow \psi$ a partir de Γ. Supóngase que existe una prueba $\Delta = \langle \psi_1, \psi_2, \ldots, \psi_k \rangle$ de longitud k de una proposición ψ a partir de $\Gamma \cup \{\varphi\}$, entonces:

(I) Si $\psi = \psi_k$ es un axioma, $\psi_k \in \Gamma$ ó $\psi_k = \varphi$, el argumento es similar a (I), (II) y (III) anteriores.

(II) Si existen $l, m < k$ tales que $\psi = \psi_k$ es consecuncia de aplicar MP a ψ_l, ψ_m en Δ y además $\psi_l = (\psi_m \Rightarrow \psi_k)$, entonces obsérvese que tanto $\langle \psi_i \rangle_{i=1}^{m}$ como $\langle \psi_i \rangle_{i=1}^{l}$ son pruebas de longitud menor a k, a partir de $\Gamma \cup \varphi$, de ψ_m y $\psi_m \Rightarrow \psi_k$ respectivamente. Aplicándose la hipótesis de inducción se tiene entonces que $\Gamma \vdash_{Ł} \varphi \Rightarrow \psi_m$ y $\Gamma \vdash_{Ł} \varphi \Rightarrow (\psi_m \Rightarrow \psi_k)$. Además, por A2, es axioma que $\Gamma \vdash_{Ł} (\varphi \Rightarrow (\psi_m \Rightarrow \psi_k)) \Rightarrow ((\varphi \Rightarrow \psi_m) \Rightarrow (\varphi \Rightarrow \psi_k))$. Usando *Modus Ponens* dos veces se concluye $\Gamma \vdash_{Ł} \varphi \Rightarrow \psi$.

■

Como extra, también es válido el recíproco al teorema anterior, i.e.

$$\frac{\Gamma \vdash_{Ł} \varphi \Rightarrow \psi}{\Gamma, \varphi \vdash_{Ł} \psi}$$

lo cual se demuestra rápidamente con una aplicación de MP. Nótese también que en la prueba anterior, únicamente se usaron A1, A2, *Modus Ponens* y la *ley de identidad* que también sólo requirió de esos mismos dos axiomas para su prueba. Así, se puede decir que el *teorema de la deducción* es válido en todo sistema formal proposicional que tenga a esas dos proposiciones, ya sea como axiomas o como teoremas, y a *Modus Ponens* como regla de inferencia.

Una vez demostrado CP, se puede aplicar en las pruebas de otras proposiciones:

Lema I.15 (Silogismo hipotético - HS)
Dadas $\varphi, \psi \in PROP$, es válida el enunciado $\varphi \Rightarrow \psi, \psi \Rightarrow \gamma \vdash_{Ł} \varphi \Rightarrow \gamma$.

Demostración. Si φ, ψ y γ son proposiciones, entonces se tiene que:

1.	$\varphi \Rightarrow \psi$	Premisa
2.	$\psi \Rightarrow \gamma$	Premisa
3.	φ	Premisa
4.	ψ	MP(1,3)
5.	γ	MP(2,4)
6.	$\varphi \Rightarrow \psi, \psi \Rightarrow \gamma, \varphi \vdash_{Ł} \gamma$	Resumen(1-5)
$\therefore$	$\varphi \Rightarrow \psi, \psi \Rightarrow \gamma \vdash_{Ł} \varphi \Rightarrow \gamma$	CP(6)

■

Lema I.16
En Ł se verifica que $\varphi \Rightarrow (\psi \Rightarrow \gamma) \vdash_{Ł} \psi \Rightarrow (\varphi \Rightarrow \gamma)$

Demostración. Sean $\varphi, \psi, \gamma \in PROP$, se exhibe una prueba del resultado deseado:

1.	$\varphi \Rightarrow (\psi \Rightarrow \gamma)$	Premisa
2.	$(\varphi \Rightarrow (\psi \Rightarrow \gamma)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \gamma))$	A2
3.	$(\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \gamma)$	MP(1,2)
4.	$\psi \Rightarrow (\varphi \Rightarrow \psi)$	A1
5.	$\psi \Rightarrow (\varphi \Rightarrow \gamma)$	HS(3,4)
$\therefore$	$\varphi \Rightarrow (\psi \Rightarrow \gamma) \vdash_{Ł} \psi \Rightarrow (\varphi \Rightarrow \gamma)$	Resumen(1-5)

■

Hasta ahora sólo se ha trabajado con los primeros dos axiomas de Ł. A continuación se demuestran algunos teoremas en el sistema formal de Łukasiewicz y que en su prueba requieren de A3.

Teorema I.17 (Algunas instancias de teoremas en lógica proposicional)
Son teoremas del sistema formal Ł las siguientes proposiciones:

(a) $\neg\varphi \Rightarrow (\varphi \Rightarrow \psi)$

(b) $\neg\neg\varphi \Rightarrow \varphi$ (Eliminación de la doble Negación)

(c) $\varphi \Rightarrow \neg\neg\varphi$ (Introducción de la doble Negación)

(d) $(\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$ (Transposición)

(e) $\varphi \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$

(f) $(\varphi \Rightarrow \psi) \Rightarrow ((\neg\varphi \Rightarrow \psi) \Rightarrow \psi)$

(g) $(\neg\varphi \Rightarrow \neg\psi) \Rightarrow ((\neg\varphi \Rightarrow \psi) \Rightarrow \varphi)$ (Axioma 3 de Mendelson c.f. [Men97, Cu14])

Demostración. Sean φ y ψ proposiciones, se presentan a continuación las prueba formales necesarias para demostrar el (meta)teorema:

Prueba de (a):

1.	$\neg\varphi$	Premisa
2.	$\neg\varphi \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$	A1
3.	$\neg\psi \Rightarrow \neg\varphi$	MP(1,2)
4.	$(\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$	A3
5.	$\varphi \Rightarrow \psi$	MP(3,4)
6.	$\neg\varphi \vdash_{\text{Ł}} \varphi \Rightarrow \psi$	[1-5]
$\therefore$	$\vdash_{\text{Ł}} \neg\varphi \Rightarrow (\varphi \Rightarrow \psi)$	CP(6)

Prueba de (b):

1.	$\neg\neg\varphi$	Premisa
2.	$\neg\neg\varphi \Rightarrow (\neg\varphi \Rightarrow \neg\neg\neg\varphi)$	(a)
3.	$\neg\varphi \Rightarrow \neg\neg\neg\varphi$	MP(1,2)
4.	$(\neg\varphi \Rightarrow \neg\neg\neg\varphi) \Rightarrow (\neg\neg\varphi \Rightarrow \varphi)$	A3
5.	$\neg\neg\varphi \Rightarrow \varphi$	MP(3,4)
6.	φ	MP(1,5)
7.	$\neg\neg\varphi \vdash_{\text{Ł}} \varphi$	[1-6]
$\therefore$	$\vdash_{\text{Ł}} \neg\neg\varphi \Rightarrow \varphi$	CP(7)

Prueba de (c):

1.	$\neg\neg\neg\varphi \Rightarrow \neg\varphi$	(b)
2.	$(\neg\neg\neg\varphi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \neg\neg\varphi)$	(a)
$\therefore$	$\vdash_{\text{Ł}} \varphi \Rightarrow \neg\neg\varphi$	MP(1,2)

Prueba de (d):

1.	$\varphi \Rightarrow \psi$	Premisa
2.	$\neg\neg\varphi \Rightarrow \varphi$	(b)
3.	$\neg\neg\varphi \Rightarrow \psi$	HS(2,1)
4.	$\psi \Rightarrow \neg\neg\psi$	(c)
5.	$\neg\neg\varphi \Rightarrow \neg\neg\psi$	HS(3,4)
6.	$(\neg\neg\varphi \Rightarrow \neg\neg\psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$	A3
7.	$\neg\psi \Rightarrow \neg\varphi$	MP(5,6)
8.	$\varphi \Rightarrow \psi \vdash_{\text{Ł}} \neg\psi \Rightarrow \neg\varphi$	[1-7]
$\therefore$	$\vdash_{\text{Ł}} (\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$	CP(8)

Prueba de (e):

1.	φ	Premisa
2.	$\varphi \Rightarrow \psi$	Premisa
3.	ψ	MP(1,2)
4.	$\varphi, \varphi \Rightarrow \psi \vdash_{\text{Ł}} \psi$	[1-3]
5.	$\varphi \vdash_{\text{Ł}} (\varphi \Rightarrow \psi) \Rightarrow \psi$	CP(4)
6.	$\varphi \vdash_{\text{Ł}} ((\varphi \Rightarrow \psi) \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$	(d)
7.	$\varphi \vdash_{\text{Ł}} \neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi)$	MP(5,6)
$\therefore$	$\vdash_{\text{Ł}} \varphi \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$	CP(7)

Prueba de (f):

1.	$\varphi \Rightarrow \psi$	Premisa
2.	$(\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$	(d)
3.	$\neg\psi \Rightarrow \neg\varphi$	MP(1,2)
4.	$\neg\varphi \Rightarrow \psi$	Premisa
5.	$\neg\psi \Rightarrow \psi$	HS(3,4)
6.	$\neg\psi \Rightarrow (\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$	(a)
7.	$(\neg\psi \Rightarrow (\psi \Rightarrow \neg(\varphi \Rightarrow \psi))) \Rightarrow ((\neg\psi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi)))$	A2
8.	$(\neg\psi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$	MP(6,7)
9.	$\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi)$	MP(5,8)
10.	$(\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow \psi)$	A3
11.	$(\varphi \Rightarrow \psi) \Rightarrow \psi$	MP(9,10)
12.	ψ	MP(1,11)
13.	$\varphi \Rightarrow \psi, \neg\varphi \Rightarrow \psi \vdash_{Ł} \psi$	[1-12]
$\therefore$	$\vdash_{Ł} (\varphi \Rightarrow \psi) \Rightarrow ((\neg\varphi \Rightarrow \psi) \Rightarrow \psi)$	2xCP(13)

Prueba de (g):

1.	$\neg\varphi \Rightarrow \neg\psi$	Premisa
2.	$\neg\varphi \Rightarrow \psi$	Premisa
3.	$(\neg\varphi \Rightarrow \neg\psi) \Rightarrow (\psi \Rightarrow \varphi)$	A3
4.	$\psi \Rightarrow \varphi$	MP(1,3)
5.	$\neg\varphi \Rightarrow \varphi$	HS(3,4)
6.	$\varphi \Rightarrow \varphi$	ID
7.	$(\varphi \Rightarrow \varphi) \Rightarrow ((\neg\varphi \Rightarrow \varphi) \Rightarrow \varphi)$	(f)
8.	$(\neg\varphi \Rightarrow \varphi) \Rightarrow \varphi$	MP(6,7)
9.	φ	MP(5,8)
10.	$\neg\varphi \Rightarrow \neg\psi, \neg\varphi \Rightarrow \psi \vdash_{Ł} \varphi$	[1-9]
$\therefore$	$\vdash_{Ł} (\neg\varphi \Rightarrow \neg\psi) \Rightarrow ((\neg\varphi \Rightarrow \psi) \Rightarrow \varphi)$	2xCP(11)

■

Se puede verificar, por medio de valuaciones, que todos los teoremas de Ł obtenidos hasta ahora son lógicamente válidos, i.e. tautologías. De igual manera uno podría intentar derivar en Ł todas las tautologías enunciadas al final de la subsección anterior. Esto es exactamente lo que motiva las definiciones de *robustez* y *completez de un sistema lógico* presentadas al final de los preliminares, propiedades que se probarán, en sus versiones fuertes, para la lógica proposicional. De manera más precisa, se demostrará que para cada $\varphi \in PROP$ y $\Gamma \subseteq PROP$:

$$\Gamma \vdash \varphi \text{ si y sólo si } \Gamma \models \varphi$$

La primera implicación de éstas es fácil de probar pues ya se tiene gran parte de lo requerido. Únicamente es necesario observar que la construcción de la teoría generada por Ł, es un proceso inductivo y como tal, si deseamos demostrar alguna propiedad de las consecuencias sintácticas de un conjunto $\Gamma \subseteq PROP$, entonces hay que verificar los casos base:

- Todos los axiomas cumplen la propiedad.

- Todos los elementos de Γ cumplen la propiedad.

y el caso inductivo: "Si $\varphi, (\varphi \Rightarrow \psi) \in PROP$ cumplen la propiedad, entonces ψ cumple la propiedad. De esta manera se prueba el siguiente teorema:

Teorema I.18 (Robustez fuerte de la lógica proposicional)
Para $\varphi \in PROP$ y $\Gamma \subseteq PROP$, si $\Gamma \vdash \varphi$, entonces $\Gamma \models \varphi$.

Demostración. Sea $v : At \to \{0, 1\}$ una valuación atómica tal que $\models_v \Gamma$. Esto implica que ya se tiene uno de los casos bases, a decir, que para cada $\varphi \in \Gamma$ se cumple que $[\![\varphi]\!]_v = 1$. Más aún, de las proposiciones lógicamente válidas en la subsección pasada se sabe que los axiomas A1, A2 y A3 son lógicamente válidos y en consecuencia:

- $\models_v \varphi \Rightarrow (\psi \Rightarrow \varphi)$
- $\models_v (\varphi \Rightarrow (\psi \Rightarrow \gamma)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \gamma))$
- $\models_v (\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$

Y también se ha visto que las valuaciones respetan MP por lo que:

- Si $\models_v \varphi$ y $\models_v \varphi \Rightarrow \psi$, entonces $\models_v \psi$.

Por *inducción sobre las pruebas a partir de* Γ es cierto que $\models_v \varphi$ para cada φ tal que $\Gamma \vdash \varphi$. En resumen, se ha probado que toda consecuencia sintáctica de Γ es también consecuencia semántica de Γ. ∎

Por otro lado, la prueba de la completez de la lógica proposicional requiere de una serie de resultados más, para ello recuérdese de los preliminares que una teoría $\Gamma \subseteq PROP$ es sintácticamente (o formalmente) inconsistente si existe una proposición $\varphi \in PROP$ tal que $\Gamma \vdash_Ł \varphi$ y $\Gamma \vdash_Ł \neg\varphi$. Correspondientemente, la teoría $\Gamma \subseteq PROP$ se dirá consistente si no es inconsistente. Con dicha definición en mente se obtiene la siguiente propiedad:

Propiedades I.19 (Contradicción y Contrapositiva)
Dadas una teoría $\Gamma \subseteq PROP$ y una proposición $\varphi \in PROP$:

- Si $\Gamma \cup \{\varphi\}$ es sintácticamente inconsistente, entonces $\Gamma \vdash_Ł \neg\varphi$ (*Prueba por contradicción*).
- Si $\Gamma \cup \{\varphi\} \vdash_Ł \neg\psi$, entonces $\Gamma \cup \{\psi\} \vdash_Ł \neg\varphi$ (*Prueba por contrapositiva*).

Demostración. Se presentan las demostraciones a manera de pruebas formales. Primero, si $\Gamma \cup \{\varphi\}$ es inconsistente, entonces existe $\gamma \in PROP$ tal que:

1.	$\Gamma, \varphi \vdash_Ł \gamma$ y $\Gamma, \varphi \vdash_Ł \neg\gamma$	Hip.
2.	$\Gamma \vdash_Ł \varphi \Rightarrow \gamma$	CP(1)
3.	$\Gamma \vdash_Ł \varphi \Rightarrow \neg\gamma$	CP(1)
4.	$\Gamma \vdash_Ł \neg\neg\varphi \Rightarrow \varphi$	$\neg\neg$-Elim
5.	$\Gamma \vdash_Ł \neg\neg\varphi \Rightarrow \neg\gamma$	HS(4,3)
6.	$\Gamma \vdash_Ł (\neg\neg\varphi \Rightarrow \neg\gamma) \Rightarrow (\gamma \Rightarrow \neg\varphi)$	A3
7.	$\Gamma \vdash_Ł \gamma \Rightarrow \neg\varphi$	MP(5,6)
8.	$\Gamma \vdash_Ł \neg\neg\varphi \Rightarrow \gamma$	HS(4,2)
9.	$\Gamma \vdash_Ł (\neg\neg\varphi \Rightarrow \neg\gamma) \Rightarrow ((\neg\neg\varphi \Rightarrow \gamma) \Rightarrow \neg\varphi)$	A3(Mendl.)
10.	$\Gamma \vdash_Ł (\neg\neg\varphi \Rightarrow \gamma) \Rightarrow \neg\varphi$	MP(5,9)
$\therefore$	$\Gamma \vdash_Ł \neg\varphi$	MP(8,10)

Por otro lado:

1.	$\Gamma, \varphi \vdash_Ł \neg\psi$	Hip.
2.	$\Gamma \vdash_Ł \varphi \Rightarrow \neg\psi$	CP(1)
3.	$\Gamma, \psi \vdash_Ł \varphi \Rightarrow \neg\psi$	Prps.I.1(2)
4.	$\Gamma, \psi \vdash_Ł \psi$	Def. Prba.
5.	$\Gamma, \psi \vdash_Ł (\varphi \Rightarrow \neg\psi) \Rightarrow (\neg\neg\psi \Rightarrow \neg\varphi)$	A3
6.	$\Gamma, \psi \vdash_Ł \psi \Rightarrow \neg\neg\psi$	$\neg\neg$-Intro
7.	$\Gamma, \psi \vdash_Ł \neg\neg\psi \Rightarrow \neg\varphi$	MP(3,5)
8.	$\Gamma, \psi \vdash_Ł \psi \Rightarrow \neg\varphi$	HS(6,7)
$\therefore$	$\Gamma, \psi \vdash_Ł \neg\varphi$	MP(4,8)

■

Ahora recuérdese que una teoría $\Gamma \subseteq PROP$ es sintácticamente (o formalmente) completa si y sólo si, para cada $\varphi \in PROP$, $\varphi \in \Gamma$ ó $(\neg\varphi) \in \Gamma$. De aquí se derivan los siguientes dos lemas:

Lema I.20 (de Lindembaum-Tarski)
Dada una teoría $\Gamma \subseteq PROP$ sintácticamente consistente, existe una extensión de ésta $\Gamma' \supseteq \Gamma$ que es sintácticamente completa y consistente.

Demostración. Sabiendo que $PROP$ es numerable, es posible dar una sucesión que numere cada proposición, i.e. $PROP = \{\varphi_0, \varphi_1, \varphi_2, \dots\}$. A partir de esto, constrúyase una sucesión de teorías de la siguiente manera: $\Gamma_0 := \Gamma$ y para $n \in \mathbb{Z}^+ \cup \{0\}$:

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\varphi_{n+1}\} & \text{si } \Gamma_n \cup \{\varphi_{n+1}\} \text{ es consistente} \\ \Gamma_n \cup \{\neg\varphi_{n+1}\} & \text{si } \Gamma_n \cup \{\varphi_{n+1}\} \text{ es inconsistente} \end{cases}$$

Por inducción se verifica que Γ_n es sintácticamente consistente para $n \in \mathbb{Z}^+ \cup \{0\}$, pues $\Gamma_0 = \Gamma$ ya lo es por hipótesis y, suponiendo que Γ_n es consistente, si Γ_{n+1} fuese inconsistente, entonces $\Gamma_n \cup \{\varphi_{n+1}\}$ y $\Gamma_n \cup \{\neg\varphi_{n+1}\}$ serían inconsistentes. Por *prueba por contradicción* del lema anterior, $\Gamma_n \vdash_Ł \neg\varphi_{n+1}$ y $\Gamma_n \vdash_Ł \neg\neg\varphi_{n+1}$; pero esto estaría diciendo que Γ_n es inconsistente, lo cual contradice la hipótesis inductiva. Así, sea $\Gamma' = \bigcup_{n \in \mathbb{Z}^+ \cup \{0\}} \Gamma_n$, entonces $\Gamma = \Gamma_0 \subseteq \Gamma'$.

Además, dada una proposición $\varphi \in PROP$, existe $n \in \mathbb{Z}^+ \cup \{0\}$ tal que $\varphi = \varphi_n$, por lo cual $\varphi \in \Gamma_n$ ó $\neg\varphi \in \Gamma_n$, y como $\Gamma_n \subseteq \Gamma'$, la teoría Γ' es sintácticamente completa. Finalmente, si Γ' no fuese sintácticamente consistente, existiría un entero no negativo n tal que $\Gamma' \vdash_{Ł} \varphi_n$ y $\Gamma' \vdash_{Ł} \neg\varphi_n$. Sabemos entonces por las propiedades de pruebas demostradas en los preliminares que existe un conjunto finito $\Gamma^* \subseteq \Gamma'$ que derivaría también sintácticamente a φ_n y $\neg\varphi_n$. Así, para un natural $m \in \mathbb{N}$ suficientemente grande, $\Gamma^* \subseteq \Gamma_m$, y con ello $\Gamma_m \vdash_{Ł} \varphi_n$ y $\Gamma_m \vdash_{Ł} \neg\varphi_n$, lo cual no puede ocurrir. Por ende, Γ' es sintácticamente consistente. ■

Lema I.21 (Completez y consistencia corresponde a valuación proposicional)
Dada una teoría $\Gamma \subseteq PROP$ sintácticamente completa y consistente, si se define una valuación atómica $v : At \to \{0, 1\}$ de tal modo que:

$$v(p) = \begin{cases} 1 & \text{si } p \in \Gamma \\ 0 & \text{si } \neg p \in \Gamma \end{cases}$$

Entonces para cada $\varphi \in PROP$, $[\![\varphi]\!]_v = 1$ si y sólo si $\varphi \in \Gamma$.

Demostración. Por inducción sobre la complejidad de la fórmula:

(a) Por definición de v ya se tiene que $[\![p]\!]_v = 1$ si y sólo si $p \in \Gamma$.

(b) Suponiendo que $[\![\psi]\!]_v = 1$ si y sólo si $\psi \in \Gamma$, entonces $[\![\neg\psi]\!]_v = 1$ si y sólo si $1 - [\![\psi]\!]_v = 1$, lo cual es equivalente a $[\![\psi]\!]_v = 0$, que por hipótesis inductiva es suficiente y necesario para que $\psi \in \Gamma$, y por completez y consistencia sintáctica, eso equivale a $\neg\psi \in \Gamma$.

(c) Si $[\![\psi]\!]_v = 1$ sii $\psi \in \Gamma$, y $[\![\gamma]\!]_v = 1$ sii $\gamma \in \Gamma$, entonces:

($\Rightarrow$) Supóngase por contradicción que $[\![\psi \Rightarrow \gamma]\!]_v = 1$ y que $(\psi \Rightarrow \gamma) \notin \Gamma$. Por completez $\neg(\psi \Rightarrow \gamma) \in \Gamma$, lo cual implica que $\Gamma \vdash_{Ł} \neg(\psi \Rightarrow \gamma)$. Se tienen dos casos:

i. Si $[\![\psi]\!]_v = 0$, entonces, por hipótesis inductiva, $\psi \notin \Gamma$. Con esto se deduce que $\Gamma \vdash_{Ł} \neg\psi$. Sabiendo que la proposición $\neg\psi \Rightarrow (\psi \Rightarrow \gamma)$ es un teorema y aplicando *Modus Ponens* se obtiene $\Gamma \vdash_{Ł} (\psi \Rightarrow \gamma)$, lo cual no puede ocurrir por la consistencia de Γ.

ii. Si $[\![\gamma]\!]_v = 1$, entonces $\Gamma \vdash_{Ł} \gamma$. Por A1 y MP se concluye que $\Gamma \vdash_{Ł} (\psi \Rightarrow \gamma)$, contradicción.

($\Leftarrow$) Si $(\psi \Rightarrow \gamma) \in \Gamma$ y $[\![\psi \Rightarrow \gamma]\!]_v = 0$, entonces $[\![\psi]\!]_v = 1$ y $[\![\gamma]\!]_v = 0$, con lo que $\psi, \neg\gamma \in \Gamma$. En resumen, $\Gamma \vdash_{Ł} \psi \Rightarrow \gamma$, $\Gamma \vdash_{Ł} \psi$ y $\Gamma \vdash_{Ł} \neg\gamma$. Por MP, $\Gamma \vdash_{Ł} \gamma$ y $\Gamma \vdash_{Ł} \neg\gamma$ lo cual contradice las hipótesis.

■

Corolario I.22 (Consistencia sintáctica implica satisfactibilidad)
Si $\Gamma \subseteq PROP$ es sintácticamente consistente, entonces es satisfactible, es decir, existe $v : At \to \{0, 1\}$ valuación atómica tal que $[\![\varphi]\!]_v = 1$ para cada $\varphi \in \Gamma$.

Demostración. Sea Γ, sintácticamente consistente, por el lema de Lindembaum-Tarski ésta puede extenderse a una teoría $\Gamma' \supseteq \Gamma$ formalmente completa y consistente. A su vez, por el lema anterior sabemos que existe una valuación v tal que $[\![\varphi]\!]_v = 1$ si y sólo si $\varphi \in \Gamma'$ para cada $\varphi \in PROP$. En particular esto se cumple para las proposiciones en Γ, con lo cual podemos concluir que Γ es satisfactible, siendo el testigo de esto la valuación v inducida por Γ'. ■

Finalmente, se presenta la demostración de la completez del sistema formal de Łukasiewicz:

Teorema I.23 (Completez semántica fuerte de la lógica proposicional)
Para $\varphi \in PROP$ y $\Gamma \subseteq PROP$, si $\Gamma \models \varphi$, entonces $\Gamma \vdash \varphi$.

Demostración. Argumentando con la contrarrecíproca del corolario anterior, como $\Gamma \cup \{\neg\varphi\}$ es insatisfactible por hipótesis, también es inconsistente. Haciendo una prueba por contradicción dentro de Ł se obtiene que $\Gamma \vdash_{Ł} \neg\neg\varphi$. Ya que es teorema que $\neg\neg\varphi \Rightarrow \varphi$, por *modus ponens* se concluye que $\Gamma \vdash_{Ł} \varphi$. ■

En resumen, los dos resultados principales expuestos en esta sección establecen que tanto el uso de valuaciones proposicionales como de derivaciones en Ł son métodos equivalentes para decidir si una proposición es consecuencia de un conjunto de premisas. Si el conjunto de premisas es vacío,entonces se afirma que todo teorema de Ł es una tautología y viceversa, i.e. $\models \varphi$ sii $\vdash \varphi$. En otras palabras, ambos métodos determinan el mismo conjunto de proposiciones, el cual cumple:

Corolario I.24 (Consistencia sintáctica de la lógica proposicional)
La teoría matemática $\tau \subseteq PROP$ generada por Ł es sintácticamente consistente.

Demostración. Por robustez toda $\varphi \in \tau$ es una tautología. De aquí que $\neg\varphi$ no es tautología (de hecho es una contradicción), se concluye que $\nvdash_{Ł} \neg\varphi$, es decir $\neg\varphi \notin \tau$. ■

Obsérvese que del corolario anterior y el lema de Lindembaum-Tarski, la teoría matemática de Ł puede "extenderse" a una sintácticamente completa y consistente de acuerdo a alguna enumeración de $PROP$. Más aún, en un sistema formal sin átomos más que $\bot$ y, tal vez, $\top$, la teoría matemática resultante sí es sintácticamente completa y consistente. Las proposiciones que incluyen a los conectivos $\wedge, \vee, \Leftrightarrow$ también son parte de ésta teoría gracias a la relación de equivalencia "$\equiv$"; pero si se desea se pueden agregar axiomas a Ł, como $\varphi \wedge \psi \Rightarrow \varphi$, que reflejen el comportamiento completo de la lógica proposicional (véase [Men97, p. 45] para más detalles). Además, aunque no se demuestra formalmente en este trabajo, la lógica proposicional es decidible, es decir, existe un procedimiento efectivo (las tablas de verdad) para determinar si una proposición es tautología o no.

Sería deseable que todo sistema formal satisfaciese las propiedades que cumple la lógica proposicional, sin embargo, mayor expresividad en el lenguaje sacrifica algunas de éstas. Un ejemplo de esto es la lógica analizada en la siguiente sección.

II. Lógica Predicativa

En matemáticas, es común el uso de enunciados con la forma “todos los x (objetos de cierto tipo), satisfacen que φ (una propiedad)” o “existe un x (objeto de cierto tipo) tal que φ (propiedad)”. A pesar de las propiedades metalógicas de la lógica proposicional, ésta no contiene suficiente expresividad como para transmitir cuantificaciones, es decir, no puede hablar de *todos* o *algunos* de los objetos de un cierto tipo, sean números naturales, enteros, racionales, reales, complejos, matrices, polinomios, vectores u otros objetos matemáticos. De igual forma, la lógica proposicional carece de expresividad para transmitir predicados, es decir, las propiedades que satisfacen estos objetos. Por esta razón se generaron nuevos sistemas formales, llamados *lógicas predicativas*, que eliminan las carencias de la lógica proposicional al ampliar las subcolecciones de su alfabeto e incluir una representación de éstos conceptos en su sintaxis. La forma más común de definir semánticas formales para este tipo de sistemas es por medio de *estructuras matemáticas* y, ya que éstas permiten comprender la dinámica detrás de las lógicas predicativas de manera más clara, se presentarán antes que la sintaxis del sistema. Se empieza con el concepto que liga los alfabetos de los lenguajes formales predicativos con tales estructuras:

Definición II.1 (Signatura)
Una signatura Σ es una colección de símbolos tales que para cada uno de ellos existe un correspondiente entero no negativo α llamado aridad que señala el número de argumentos con los cuales opera dicho símbolo.

Nótese que una signatura realmente es un alfabeto con un poco más de información para construir lenguajes formales. En la práctica es común separar a la signatura Σ en varias entidades y escribir $\Sigma = \langle \mathcal{F}, \mathcal{P}, \alpha \rangle$, donde $\mathcal{F}$ y $\mathcal{P}$ son conjuntos de símbolos y $\alpha : \mathcal{F} \cup \mathcal{P} \to \mathbb{Z}^+ \cup \{0\}$ es una correspondencia que asigna a cada uno de esos símbolos su respectiva aridad. Es común llamar a los entes del primer conjunto $\mathcal{F}$ símbolos funcionales, mientras que a los del otro conjunto $\mathcal{P}$ se les suele denominar símbolos predicativos o relacionales. Más aun, frecuentemente es útil hablar del conjunto de todos los símbolos funcionales de aridad “i” con $i \in \mathbb{Z}^+ \cup \{0\}$, el cual se representa mediante $\mathcal{F}_i$. Análogamente, el conjunto de todos los símbolos predicativos de aridad “i” es denotado por $\mathcal{P}_i$. Con esta idea en mente es posible dividir aún más la signatura y reexpresarla como $\Sigma = \langle \mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2, \dots \rangle$. Expandiendo un poco más la notación, si f_i^k representa el i-ésimo símbolo funcional de aridad k y P_j^l es el j-ésimo símbolo predicativo de aridad l, entonces la signatura se puede expresar mediante:

$$\Sigma = \langle f_0^0, f_1^0, \dots, f_0^1, f_1^1, \dots, f_0^2, f_1^2, \dots; P_0^0, P_1^0, \dots, P_0^1, P_1^1, \dots, P_0^2, P_1^2, \dots \rangle$$

Se puede pensar en los símbolos funcionales $f \in \mathcal{F}$ como aquellos que combinados con variables carecen de valor de verdad como serían “$+$” y “$-$”, por ejemplo, cuando se habla de números, a las expresiones “$x+y$” y “$-x$” no se les puede asignar un valor de verdadero o falso. Por otro lado, los símbolos relacionales o predicativos $P \in \mathcal{P}$ son aquellos que sí adquieren valores de verdad con las variables como serían "$\leq$" ó "$=$". Nótese que en el caso de "$\leq$" (tomando su interpretación estándar de menor-o-igual-que y hablando de números), la expresión "$x \leq y$" sí podría tomar un valor de verdad dependiendo de los valores que tomasen "x" y "y". Finalmente, α asigna a cada símbolo su "aridad", es decir, con cuántos argumentos (otros símbolos o cadenas de símbolos) "trabaja". Por ejemplo, para decir que algo es igual a otro algo normalmente se usa el símbolo relacional "$=$" y otros dos más como en la expresión "$x = y$". En este caso, la aridad del símbolo "$=$" es dos. Hay notaciones alternativas para marcar la aridad de un símbolo, por ejemplo, para el símbolo de aridad dos "$+$", en vez de escribir "$x + y$" se puede escribir "$+(x, y)$" ó "$+^2xy$".

Con base en cómo se definió la signatura, es común que en lugar de símbolos funcionales de aridad cero se hable de *constantes* y, en vez de símbolos predicativos de aridad cero, se hable de letras o *símbolos proposicionales*. La explicación de esto se dará una vez se defina el concepto de estructura.

Definición II.2 (Estructura)
Una estructura $\mathfrak{A}$ es la agrupación de uno o varios conjuntos, junto con relaciones y funciones definidas entre ellos.

Las estructuras suelen ser denotadas mediante sus signaturas $\mathfrak{A} = \langle \mathcal{T}, \mathcal{F}, \mathcal{P}, \alpha \rangle$ aumentadas con $\mathcal{T}$, es decir, símbolos de aridad cero, llamados *sorts* o *tipos*, que representen los conjuntos de la estructura, mientras que los símbolos en $\mathcal{F}$ representan las funciones entre los conjuntos y aquellos en $\mathcal{P}$, las relaciones definidas en dichos conjuntos. Por dicha razón es común que los lógicos definan a las estructuras $\mathfrak{A}$ (con un sólo conjunto) como ternas $\langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ donde $\mathcal{D}$ es el *dominio de discurso*, *conjunto subyacente* o *portador de* $\mathfrak{A}$; Σ es la signatura correspondiente, e $\mathcal{I}$ es una *función de interpretación* o, simplemente, una *interpretación*, es decir, una correspondencia entre los símbolos de la signatura Σ y los conjuntos, funciones y/o relaciones definibles en los conjuntos de $\mathfrak{A}$. Más aun, si s es un símbolo en la signatura Σ, la interpretación del símbolo bajo $\mathcal{I}$ se suele denotar por $s^{\mathfrak{A}}$ o por $s_{\mathfrak{A}}$. Así, si $\mathcal{T} = \{s\}$ y $\mathfrak{A}$ sólo tiene un conjunto $\mathcal{D}$, entonces $s^{\mathfrak{A}} = \mathcal{D}$. Por otro lado a cada símbolo funcional de aridad "n", $f \in \mathcal{F}_n$, la interpretación $\mathcal{I}$ le asigna una función $f^{\mathfrak{A}} : \mathcal{D}^n \to \mathcal{D}$ que toma "n" objetos del dominio $\langle a_1, a_2, \ldots, a_n \rangle$ y devuelve otro objeto $a \in \mathcal{D}$. Análogamente, a cada símbolo predicativo de aridad "n", $P \in \mathcal{P}_n$, la correspondencia $\mathcal{I}$ le asigna una relación/predicado $P^{\mathfrak{A}}$ definida entre "n" objetos de $\mathcal{D}$, i.e. $P^{\mathfrak{A}} \subseteq \mathcal{D}^n$. Como ejemplo de ésto, supóngase que $\mathfrak{A}$ es una estructura con posible signatura $\Sigma = \langle A; f, g; R \rangle$ con $A \in \mathcal{T}$, $f, g \in \mathcal{F}_2$ y $R \in \mathcal{P}_2$, entonces $\mathfrak{A}$ realmente es la agrupación $\langle A^{\mathfrak{A}}; f^{\mathfrak{A}}, g^{\mathfrak{A}}; R^{\mathfrak{A}} \rangle$ donde $f^{\mathfrak{A}}$ y $g^{\mathfrak{A}}$ son operaciones binarias en $A^{\mathfrak{A}}$ y $R^{\mathfrak{A}}$, una relación binaria en $A^{\mathfrak{A}}$.

Puede decirse que si p es un símbolo predicativo de aridad cero i.e. $p \in \mathcal{P}_0$, entonces $p^{\mathfrak{A}}$ es una relación entre "cero" objetos. Razonando por medio de analogías, si la característica esencial de las relaciones es que adquieren valores de verdad cuando se especifican los entes que relacionan, entonces $p^{\mathfrak{A}}$ adquiere un valor de verdad constante (dado por la interpretación) inmediatamente y sin argumento alguno, razón por la cual "p" representa una proposición y es posible llamarlo, igual que en la sección anterior, "símbolo proposicional". Similarmente, si a los símbolos funcionales de aridad n se les interpreta como correspondencias que toman n-adas, $\langle a_1, a_2, a_3, \ldots, a_n \rangle \in \mathcal{D}^n$ y devuelven otro objeto del mismo dominio, $a \in \mathcal{D}$, entonces un funcional de aridad cero $c \in \mathcal{F}_0$ es interpretado como una correspondencia que toma al vacío, $\langle\rangle \in \mathcal{D}^0 = \{\emptyset\}$, y le asigna un elemento del dominio $c^{\mathfrak{A}}(\emptyset) = a \in \mathcal{D}$. Así, el símbolo c siempre representará al mismo elemento a del dominio de discurso, razón suficiente para llamar a los funcionales de aridad cero "constantes".

Ejemplo II.1 Se construirá una estructura $\mathfrak{A}$ para el campo finito y ordenado de dos elementos: Así $\mathbb{F}_2$ es el *sort* que denota el "dominio de discurso de únicamente dos objetos". Las constantes utilizadas son $\mathcal{F}_0 = \{0, 1\}$; los funcionales de aridad uno son $\mathcal{F}_1 = \{-, ^{-1}\}$; los de aridad dos, $\mathcal{F}_2 = \{+, \cdot\}$; el único símbolo predicativo de aridad dos es $\mathcal{P}_2 = \{<\}$. La interpretación $\mathcal{I}$ que daremos a estos símbolos será la convencional en matemáticas, es decir:

- Al símbolo "1" se le asigna el neutro bajo la multiplicación.
- Al símbolo "0" se le asigna el neutro bajo la suma.
- Al símbolo funcional "$-$" se le asigna la operación "inverso respecto a la suma". Formalmente: si x es un objeto de $\mathbb{F}_2$, entonces $-x$ es el ente en $\mathbb{F}_2$ tal que sumado con x da 0.[7]
- Al símbolo funcional "$^{-1}$" se le asigna la función "inverso respecto a la multiplicación". Formalmente: si x es un objeto de $\mathbb{F}_2$ y x es distinto de 0, entonces x^{-1} es el ente en $\mathbb{F}_2$ tal que multiplicado con x da 1.
- El símbolo "$+$" es interpretado como la suma en $\mathbb{F}_2$. Esto es, si x y y son objetos de $\mathbb{F}_2$, entonces $x + y$ representa la adición de x y y.
- El símbolo "$\cdot$" se interpreta como la multiplicación en $\mathbb{F}_2$. Así, si x y y son objetos en $\mathbb{F}_2$, entonces $x \cdot y$ representa el producto de x y y.
- Finalmente, la relación "menor que" es asignada al símbolo "$<$". En otras palabras, si x y y son objetos en $\mathbb{F}_2$, entonces al escribir $x < y$ se está afirmando que el objeto x es estrictamente menor que y. Obsérvese que sólo hay una forma de que esto sea verdadero, con x siendo el neutro aditivo y y, el neutro multiplicativo.

Algunos autores combinan el concepto de estructura y signatura en uno mismo, bajo cualquiera de los dos nombres. La razón es que una forma alterna, práctica y cómoda para especificarlas al mismo tiempo -cuando la función de interpretación es clara por el contexto- es enlistar al dominio de discurso junto con

[7] Obsérvese que la variable x es un metasímbolo para explicar la interpretación.

todos los símbolos de la signatura acompañados de un supra-índice que denote su aridad. El orden utilizado en esta notación es importante para tener claras las aridades y distinguir símbolos funcionales de símbolos predicativos. También es común enfatizar esto mediante el uso de puntos y coma ";". Así, en general se suele denotar a la estructura/signatura de la siguiente forma:

$$\mathfrak{A} = \langle \mathcal{D}; f_0^0, f_1^0, \ldots, f_0^1, f_1^1, \ldots, f_0^2, f_1^2, \ldots; P_0^0, P_1^0, \ldots, P_0^1, P_1^1, \ldots, P_0^2, P_1^2, \ldots \rangle$$

Por ejemplo, los números reales usualmente tienen una estructura como la siguiente:

$$\mathfrak{A} = \langle \mathbb{R}; 0^0, 1^0, -^1, (^{-1})^1, +^2, \cdot^2; <^2, =^2 \rangle$$

Es claro lo que cada uno de los símbolos significa:

- El dominio de discurso $\mathcal{D}$ es el conjunto de los números reales, denotado por el *sort* $\mathbb{R}$.
- Las constantes son $\mathcal{F}_0 = \{0, 1\}$, las cuales por el contexto se entiende que representan a los números cero y uno respectivamente.
- Los funcionales de aridad uno son $\mathcal{F}_1 = \{-, ^{-1}\}$ interpretados equivalentemente al ejemplo anterior.
- Los de aridad dos son $\mathcal{F}_2 = \{+, \cdot\}$, que representan las operaciones suma y multiplicación respectivamente.
- Los símbolos predicativos de aridad dos son $\mathcal{P}_2 = \{<, =\}$ a los que se les asignan las relaciones "menor que" e "igual a" respectivamente.

Una variación de esta notación consiste en escribir a la sucesión finita del dominio y los símbolos separada de la de sus aridades correspondientes; esta última además estará ordenada correspondientemente a la primera. Dicha notación se frecuenta cuando no sólo la interpretación es clara por el contexto sino también las aridades. en cuyo caso la sucesión de estas últimas es mera formalidad y se puede omitir. Así, en el caso de los números reales esto se haría de la siguiente manera:

$$\langle \mathbb{R}; 0, 1, -, ^{-1}, +, \cdot; <, = \rangle$$

$$\langle 0, 0, 1, 1, 2, 2; 2, 2 \rangle$$

Es importante resaltar que aunque las estructuras vistas hasta ahora sólo tienen un sort (son uno-sorteadas), también es posible definir otras que tengan dos o más, llamadas estructuras multi-sorteadas.[8] Un ejemplo de estas común en matemáticas se genera al estudiar la topología de los reales pues para hacerlo se necesitan los tres conjuntos $\mathbb{R}, \mathcal{P}(\mathbb{R})$ y $\mathcal{P}(\mathcal{P}(\mathbb{R}))$ junto con las operaciones $\cup$ y $\cap$, y las relaciones $\in$ y $\subseteq$, de tal forma que la signatura/estructura queda expresada por:

$$\langle \mathbb{R}, \mathcal{P}(\mathbb{R}), \mathcal{P}(\mathcal{P}(\mathbb{R})); \emptyset^0, \cup^1, \cap^2; \in^2, \subseteq^2, =^2 \rangle$$

[8] Para mayor información véase [STB] y [CG].

Para finalizar la introducción a la lógica predicativa, obsérvese que la signatura ya incluye una colección $\mathcal{P}$ de símbolos que serán interpretados como predicados en los lenguajes de la lógica predicativa. Resta ver aquéllos que serán utilizados para las cuantificaciones, lo cual requiere que se estudie la sintaxis de este tipo de sistemas formales.

I. Sintaxis de la Lógica Predicativa

Ya que se extenderá la lógica proposicional a un sistema formal más expresivo, es necesario ampliar la cantidad de grupos de símbolos que se utilizarán. De esta manera, los alfabetos a usar en la presente sección se dividen en dos clases cada una de las cuales presenta también sus respectivas subclases ajenas entre sí:

⋆ Símbolos Lógicos:

- Variables (VAR): $x_0, x_1, x_2, x_3, \dots$
- Conectivos Lógicos (Ω):
  - De aridad 1 (Ω_1): $\neg$
  - De aridad 2 (Ω_2): $\wedge, \vee, \Rightarrow, \Leftrightarrow$
- Cuantificadores: $\forall, \exists$
- Símbolos de Agrupación: Paréntesis izquierdo, paréntesis derecho, corchete izquierdo, corchete derecho y coma, i.e. $(,), [,], ,$

⋆ Símbolos no-lógicos (signatura) Σ:

- Símbolos Funcionales ($\mathcal{F}$) cuyas subclases pueden ser vacías o finitas:
  - De aridad 0 ó constantes ($\mathcal{F}_0$): $c_0, c_1, \dots$
  - De aridad 1 ($\mathcal{F}_1$): $f_0^1, f_1^1, f_2^1, \dots$

    $\vdots$
  - De aridad n ($\mathcal{F}_n$): $f_0^n, f_1^n, f_2^n, \dots$

    $\vdots$
- Símbolos Predicativos o relacionales ($\mathcal{P}$) con subclases tal vez vacías/finitas:
  - De aridad 0 ó letras proposicionales ($\mathcal{P}_0$): $p_0, p_1, \dots$
  - De aridad 1 ($\mathcal{P}_1$): $P_0^1, P_1^1, P_2^1, \dots$

    $\vdots$
  - De aridad n ($\mathcal{P}_n$): $P_0^n, P_1^n, P_2^n, \dots$

    $\vdots$

Obsérvese que la parte “modificable” de un alfabeto para una lógica de predicados es la de los símbolos no-lógicos (la signatura), por lo que si éstos se hacen explícitos, uno no requiere más información para determinar completamente la lógica predicativa subyacente. Por dicha razón, muchos autores abusan de la notación y usan expresiones de la forma "sea $\mathcal{L} = \langle c_0, \ldots, f_0^1, \ldots; p_0, \ldots, P_0^1, \ldots \rangle$ un lenguaje predicativo", "sea $\mathcal{L} = \mathcal{F} \cup \mathcal{P}$ un lenguaje predicativo" o "sea $\mathcal{L} = \bigcup_{n\geq 0} \mathcal{F}_n \cup \bigcup_{n\geq 0} \mathcal{P}_n$ un lenguaje predicativo" a pesar de que, como se vio previamente, dichas agrupaciones únicamente representan signaturas y no precisamente un lenguaje formal.

Más aún, es común incluir a la igualdad como parte de la estructura de la lógica predicativa, por lo cual el símbolo "$=$" de $\mathcal{P}_2$ es considerado a veces un símbolo lógico e incluso no es mencionado en la signatura de las estructuras.

Igual que en secciones previas, una vez que se ha dado una lista de símbolos con los cuales trabajar, se dan reglas para la construcción de expresiones bien formadas. En este caso, para dicho fin se empleará una definición auxiliar:

Definición II.3 (Términos)
Recursivamente, el conjunto de términos (bien formados) $TERM$ de un lenguaje predicativo se da por las reglas:

a. Todas las variables son términos, i.e. si $x \in VAR$, entonces $x \in TERM$.

b. Todas las constantes son términos, i.e. si $c \in \mathcal{F}_0$, entonces $c \in TERM$.

c. Si $t_1, t_2, \ldots, t_n \in TERM$ y $f \in \mathcal{F}_n$, entonces $f(t_1, t_2, \ldots, t_n) \in TERM$ siendo n un entero positivo.[9]

d. Ninguna otra cosa es un término.

Ejemplo II.2 Los siguientes ejemplifican la definición recientemente dada:

- x_{1235} es un término pues es una variable (regla a.).
- Aplicando la regla c. la cadena $f_1^5(x_1, x_2, x_3, x_4, x_5)$ es un término.
- Un término más "complejo" sería $f_4^3(f_2^2(x_4, x_{25}), f_1^2(x_4, x_{25}), f_0^1(f_1^1(x_3)))$.
- Obsérvese también que por la regla b. una constante c_{29} es un término.

Nótese que las reglas dadas pudieron haber sido distintas, por ejemplo, es posible ahorrarse el uso de paréntesis y comas si se combinan las reglas b. y c. en su forma polaca:

- Si $t_1, \ldots, t_n \in TERM$ y $f \in \mathcal{F}_n$, entonces $ft_1 \ldots t_n$ es un término.

Además, procediendo de manera análoga a la sección previa es posible probar los siguientes tres teoremas:

Teorema II.1 (Principio de Inducción sobre la Complejidad del Término)
Una propiedad se cumple para todo término si y sólo si se valida que:

[9]En general se usarán las letras x, y, z como metasímbolos para variables; a, b, c como metasímbolos para constantes y r, s, t para los términos.

(1) Todas las variables satisfacen la propiedad.

(2) Todas las constantes satisfacen la propiedad.

(3) Si $t_1, \ldots, t_n$ son términos que satisfacen la propiedad y $f \in \mathcal{F}_n$, entonces también la satisface $f(t_1, t_2, t_3, \ldots, t_n)$, siendo n un entero positivo.

Teorema II.2 (Teorema de Legibilidad Única para Términos)
Todo término t está exactamente en una y sólo una de las siguientes formas:

(a) x_i con i un entero no negativo, es decir, es una variable.

(b) c_j con j un entero no negativo, i.e. es una constante.

(c) $f(t_1, t_2, t_3, \ldots, t_n)$ donde $t_1, t_2, t_3, \ldots, t_n$ son n términos únicamente determinados y f es un símbolo funcional de aridad n, siendo n un entero positivo.

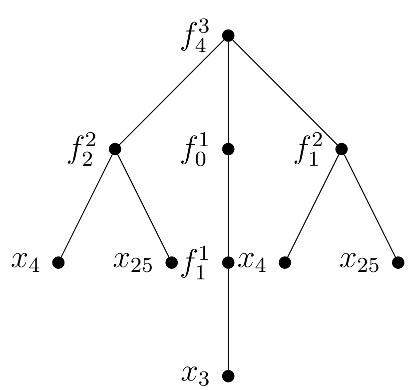
Teorema II.3 (Teorema de la Definición por Recursión en Términos)
Dados un conjunto X, función en variables $H_{VAR} : VAR \to X$, función en constantes $H_{\mathcal{F}_0} : \mathcal{F}_0 \to X$ y funciones $H_n : X^n \to X$ para cada n entero positivo, es posible construir una función única $F : TERM \to X$ tal que:

$$F(t) = \begin{cases} H_{VAR}(t) & \text{si } t \in VAR \\ H_{\mathcal{F}_0}(t) & \text{si } t \in \mathcal{F}_0 \\ H_n(F(t_1), \ldots, F(t_n)) & \text{si } t = f(t_1, \ldots, t_n) \text{ y } f \in \mathcal{F}_n \end{cases}$$

Gracias a estos tres teoremas sintácticos es posible definir las sucesiones formativas de términos y, recursivamente, la longitud de un término y su árbol de análisis gramático. Así, una sucesión formativa de $f_4^3(f_2^2(x_4, x_{25}), f_0^1(f_1^1(x_3)), f_1^2(x_4, x_{25}))$ podría ser:

$$\langle x_3, x_4, x_{25}, f_1^1(x_3), f_1^2(x_4, x_{25}), f_2^2(x_4, x_{25}), f_0^1(f_1^1(x_3)), f_4^3(f_2^2(x_4, x_{25}), f_0^1(f_1^1(x_3)), f_1^2(x_4, x_{25}))\rangle$$

Mientras que la longitud de dicho término es 24 y su árbol está dado por:



Un ejemplo de una definición recursiva en los términos que será de utilidad más adelante es la siguiente:

Definición II.4 (Conjunto de variables de un término)
El conjunto de variables de un término $V : TERM \to \mathcal{P}(VAR)$ se define mediante:

$$V(c) = \emptyset$$
$$V(x) = \{x\}$$
$$V(f(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} V(t_i)$$

Como se dijo previamente, los términos son agrupaciones auxiliares de símbolos para definir los lenguajes formales de las lógicas predicativas:

Definición II.5 (Lenguaje Formal Predicativo)
Se presentan recursivamente las reglas que permiten construir *wffs* de lenguajes predicativos, $\mathcal{L}$:

I. Toda letra proposicional es una fórmula bien formada de un lenguaje predicativo $\mathcal{L}$, i.e. si $p \in \mathcal{P}_0$, entonces $p \in \mathcal{L}$.

II. Si $t_1, t_2, t_3, \ldots, t_n \in TERM$ y $P \in \mathcal{P}_n$, entonces $P(t_1, t_2, t_3, \ldots, t_n) \in \mathcal{L}$ siendo n un entero positvo. Particularmente, este tipo de *wffs* junto con $\mathcal{P}_0$ son los átomos de los lenguajes predicativos y, nuevamente, el conjunto de átomos será denotado por At.

III. Si $\varphi \in \mathcal{L}$, entonces $\neg\varphi$ también es una *wff*.

IV. Si φ, ψ son *wffs* y $\circ \in \Omega_2$, entonces $(\varphi \circ \psi)$ es una *wff*.

V. Si $\varphi \in \mathcal{L}, x \in VAR$ y $\dashv \in \{\forall, \exists\}$, entonces $\dashv x[\varphi]$ es una *wff*.

VI. Ninguna otra cosa es una *wff*.

Ejemplo II.3 Los siguientes ejemplifican la definición recientemente dada:

- Por I. los átomos p_0, p_{25}, p_{1325} y p_{17} son *wffs*.
- Aplicando II. $P_1^5(x_1, x_2, c_0, c_4, x_5)$ es un átomo y, por ende, una *wff*.
- Un átomo más "complejo" sería $P_4^3(f_2^2(x_4, x_{25}), f_1^2(x_4, x_{25}), f_0^1(f_1^1(x_3)))$.
- Por III. y IV. $\neg p_0, (P_1^1(x_2) \Rightarrow P_1^1(x_3))$ y $(P_1^2(x_0, c_0) \wedge P_4^1(c_{10}))$ son *wffs*.
- $\forall x_3[P_0^2(x_3, x_1)], \exists x_5[(p_1 \wedge P_2^1(c_1, x_6))]$ y $\forall x_0[(P_1^2(x_0, c_0) \Rightarrow \exists x_1[(P_1^2(x_1, c_0) \wedge P_2^2(x_0, x_1))])]$ son fórmulas bien formadas de acuerdo a la regla V.

Nuevamente se puede evitar el uso de paréntesis y comas si se enuncian las reglas en su forma polaca:

- Si $t_1, \ldots, t_n \in TERM$ y $P \in \mathcal{P}_n$, entonces $Pt_1 \cdots t_n$ es una *wff*.

- Si $\varphi_1, \ldots, \varphi_n \in \mathcal{L}$ y $\circ \in \Omega_n$, entonces $\circ\varphi_1 \cdots \varphi_n \in \mathcal{L}$.
- Si $\varphi \in \mathcal{L}, x \in VAR$ y $\daleth \in \{\forall, \exists\}$, entonces $\daleth x\varphi \in \mathcal{L}$.

Además, al igual que con los términos, se tienen tres teoremas de sintaxis correspondientes para los lenguajes predicativos:

Teorema II.4 (Principio de Inducción sobre la Complejidad de la Fórmula)
Una propiedad se cumple para toda *wff* si y sólo si se validan las condiciones:

(1) Todos los átomos satisfacen la propiedad.

(2) Si la *wff* φ cumple la propiedad, entonces $\neg\varphi$ cumple la propiedad.

(3) Si las *wffs* φ, ψ validan la propiedad, entonces también lo hacen las de la forma $(\varphi \circ \psi)$ con $\circ \in \Omega_2$.

(4) Si la *wff* φ satisface la propiedad, $x \in VAR$ y $\daleth \in \{\forall, \exists\}$, entonces $\daleth x[\varphi]$ cumple la propiedad también.

Teorema II.5 (Teorema de Legibilidad Única para los Lenguajes Predicativos)
Toda *wff* φ de un lenguaje predicativo está exactamente en una y sólo una de las siguientes formas:

a. $\varphi \in At$, es decir, $\varphi = p_k$ con k un entero no negativo ó $\varphi = P(t_1, \ldots, t_n)$ con $t_1, \ldots, t_n \in TERM$, $P \in \mathcal{P}_n$ siendo n un entero positivo.

b. $\neg\varphi$, siendo φ una *wff* únicamente determinada.

c. $(\varphi \circ \psi)$, siendo tanto φ como ψ *wffs* únicamente determinadas.

d. $\daleth x[\varphi]$, siendo x una variable y φ una *wff* únicamente determinada.

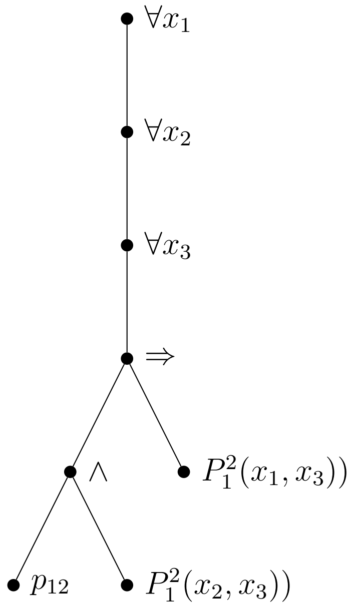
Teorema II.6 (Teorema de la Definición por Recursión en los Lenguajes Predicativos)
Dado un conjunto X y ocho funciones $H_{At} : At \to X$, $H_\neg : X \to X$, $H_\circ : X \times X \to X$ con $\circ \in \Omega_2$ y $H_\daleth : X \times VAR \to X$ con $\daleth \in \{\forall, \exists\}$, es posible construir una función única $F : \mathcal{L} \to X$ tal que:

$$F(\varphi) = \begin{cases} H_{At}(\varphi) & \text{si } \varphi \in At \\ H_\neg(F(\psi)) & \text{si } \varphi = \neg\psi \\ H_\circ(F(\psi), F(\gamma)) & \text{si } \varphi = (\psi \circ \gamma) \\ H_\daleth(F(\psi), x) & \text{si } \varphi = \daleth x\psi \text{ con } x \in VAR \end{cases}$$

Y de manera análoga a cómo se trabajó con las proposiciones y los términos, se pueden definir sucesiones formativas al igual que, recursivamente, árboles de análisis gramático y otros similares. Por ejemplo, una sucesión formativa de la fórmula bien formada, $\forall x_1[\forall x_2[\forall x_3[((p_{12} \wedge P_1^2(x_2, x_3)) \Rightarrow P_1^2(x_1, x_3))]]]$ sería:

$\langle p_{12}, P_1^2(x_2,x_3), P_1^2(x_1,x_3), (p_{12} \wedge P_1^2(x_2,x_3)), ((p_{12} \wedge P_1^2(x_2,x_3)) \Rightarrow P_1^2(x_1,x_3)), \forall x_3[((p_{12} \wedge P_1^2(x_2,x_3)) \Rightarrow P_1^2(x_1,x_3))], \forall x_2[\forall x_3[((p_{12} \wedge P_1^2(x_2,x_3)) \Rightarrow P_1^2(x_1,x_3))]], \forall x_1[\forall x_2[\forall x_3[((p_{12} \wedge P_1^2(x_2,x_3)) \Rightarrow P_1^2(x_1,x_3))]]]\rangle$.

Dicha *wff* tiene una longitud de 31 mientras que su árbol de análisis gramático es:



Definición II.6 (Subfórmula y partes de una proposición)
Igual que en la sección anterior, se tienen los conceptos de subfórmulas, alcance de un conectivo/cuantificador y conectivo/cuantificador principal:

a. *(Conjunto de subfórmulas)* Recursivamente se define el conjunto de subfórmulas de una *wff* φ mediante:

$$\begin{gathered} Sub(\varphi) = \{\varphi\} \text{ para } \varphi \in At \\ Sub(\neg\varphi) = Sub(\varphi) \cup \{\neg\varphi\} \\ Sub((\varphi \circ \psi)) = Sub(\varphi) \cup Sub(\psi) \cup \{(\varphi \circ \psi)\} \\ Sub(\exists x[\varphi]) = Sub(\varphi) \cup \{\exists x[\varphi]\} \end{gathered}$$

b. *(Subfórmula o parte bien formada)* Dada $\varphi \in \mathcal{L}$, una cadena ψ es una subfórmula o parte bien formada de φ si $\psi \in Sub(\varphi)$.[10]

c. *(Alcance de un conectivo)* Si en $\varphi \in \mathcal{L}$ aparece una instancia de un conectivo $\circ \in \Omega_i$ con $i \in \{1,2\}$, entonces se llama *alcance del conectivo* a la parte bien formada más pequeña que contenga dicha instancia.[11]

[10] Por inducción sobre la complejidad de φ se puede probar que cada $\psi \in Sub(\varphi)$ es una *wff* de $\mathcal{L}$.
[11] Esta minimalidad se puede obtener tanto por longitud de cadenas como por el orden inducido por la relación "ser subfórmula de" en $Sub(\varphi)$, la cual puede ser claramente representada como diagrama de Hasse por el árbol de análisis gramático de φ.

d. *(Alcance de un cuantificador)* Si en $\varphi \in \mathcal{L}$ aparece una instancia de un cuantificador $\daleth \in \{\forall, \exists\}$, entonces se llama *alcance del cuantificador* a la parte bien formada más pequeña que la contenga.

e. *(Conectivo/cuantificador principal)* Dada $\varphi \in \mathcal{L}$, se dice que una instancia de $\circ \in \Omega_i$ con $i = 1$ ó $i = 2$ ($\circ \in \{\forall, \exists\}$) en φ es el conectivo (cuantificador) principal de φ si y sólo si el alcance de $\circ$ es toda φ.

Ya que las variables tienen una importancia central en la interpretación de los lenguajes recientemente descritos, será importante distinguir aquellas que estén dentro del alcance de un cuantificador de aquellas que no. Para esto se introducen los conceptos de variable libre y variable acotada:

Definición II.7 (Conjunto de variables libres de una fórmula y sentencias)
Se define recursivamente el conjunto de variables libres para una fórmula de la siguiente manera:

$$\begin{aligned} FV(p_i) &= \emptyset \\ FV(P(t_1, \ldots, t_n)) &= \bigcup_{i=1}^{n} V(t_i) \\ FV((\varphi \circ \psi)) &= FV(\varphi) \cup FV(\psi) \\ FV(\neg\varphi) &= FV(\varphi) \\ FV(\daleth x[\varphi]) &= FV(\varphi) \setminus \{x\} \end{aligned}$$

Decimos que una variable $x \in VAR$ es libre en una *wff* φ si y sólo si $x \in FV(\varphi)$. Si el conjunto de variables libres es vacío, i.e. $FV(\varphi) = \emptyset$, decimos que φ es una sentencia.

Definición II.8 (Conjunto de variables acotadas de una fórmula)
Se define recursivamente el conjunto de variables acotadas para una fórmula de la siguiente manera:

$$\begin{aligned} BV(p_i) &= \emptyset \\ BV(P(t_1, \ldots, t_n)) &= \emptyset \\ BV((\varphi \circ \psi)) &= BV(\varphi) \cup BV(\psi) \\ BV(\neg\varphi) &= BV(\varphi) \\ BV(\daleth x[\varphi]) &= BV(\varphi) \cup \{x\} \end{aligned}$$

Decimos que una variable $x \in VAR$ es acotada (ligada) en una *wff* φ si y sólo si $x \in BV(\varphi)$.

Ejemplo II.4 El conjunto de variables libres para la *wff* de algún lenguaje $\mathcal{L}$: $\exists x_3[((P_0^1(x_1) \vee P_1^2(x_1, x_2)) \Rightarrow P_1^2(x_1, x_3))]$, es $\{x_1, x_2\}$ mientras que el de variables acotadas es $\{x_3\}$.

Nótese también que una variable puede estar libre y acotada para una misma fórmula, por ejemplo, en $\forall x_2[((P_1^2(x_1, x_2) \wedge P_1^2(x_2, x_3)) \Rightarrow \forall x_1[P_1^2(x_1, x_3)]])]$ la variable x_1 está libre y acotada al mismo tiempo. Por dicha razón será más importante el hecho de que una variable x cumpla que $\underline{x \notin FV(\varphi)}$ lo cual significará que: o la variable x no está presente en φ o todas las instancias de x están acotadas en la *wff* φ. De manera similar expresar que $x \notin BV(\varphi)$ significa que o la variable x no aparece en φ o todas las instancias de x en φ son libres, i.e. no están dentro del alcance de algún cuantificador que las acote.

A diferencia de la sección anterior en la que se terminó el estudio sintáctico del lenguaje con la definición de subfórmulas y en donde además las sustituciones sólo fueron mencionadas transitoriamente, en las lógicas predicativas diversos tipos de sustituciones cobrarán mayor importancia y serán necesarias para la implementación de un sistema formal. No obstante, antes de proceder a dar dichas definiciones se adoptarán convenciones de notación similares a las de lógica proposicional respecto a jerarquía de conectivos, eliminación de paréntesis y asociación de conectivos:

- Se eliminan paréntesis externos para los conectivos, es decir, en lugar de $(\varphi \circ \psi)$ simplemente se escribirá $\varphi \circ \psi$ o si se tiene $\exists x[(\varphi \circ \psi)]$ se escribirá $\exists x[\varphi \circ \psi]$.

- Ya que los elementos de $\mathcal{P}_2$ representarán relaciones binarias, éstos se utilizarán como convencionalmente en matemáticas. Por ejemplo, si "$<$" es un símbolo predicativo de aridad dos, entonces se escribirá "$s < t$" en vez de "$<(s,t)$" para términos s y t.

- De igual manera, cuando se empleen algunos símbolos funcionales estándar de aridad dos como $+$ y $\times$, se escribirá tfs en vez de $f(t,s)$ para $t, s \in TERM$ y $f \in \mathcal{F}_2$.

- El alcance de las relaciones binarias es más corto que el del resto de los conectivos, seguido del de las negaciones, las disyunciones y conjunciones y, finalmente, las implicaciones y bicondicionales:

Jerarquía	Conectivo
0	$R \in \mathcal{P}_2$
1	$\neg$
2	$\vee, \wedge$
3	$\Rightarrow, \Leftrightarrow$

- Cuando un solo conectivo de aridad dos $\circ \in \Omega_2$ se usa consecutivamente $\varphi_1 \circ \varphi_2 \circ ... \circ \varphi_n$ la convención es interpretar dicha concatenación como agrupaciones a la derecha: $(\varphi_1 \circ (\varphi_2 \circ (... \circ \varphi_n)...))$.

- Si $\circ \in \{\vee, \wedge, \Leftrightarrow\}$ entonces en $((\varphi \circ \psi) \circ \gamma)$ o en $(\varphi \circ (\psi \circ \gamma))$ se podrán eliminar paréntesis internos, es decir, se podrá escribir $(\varphi \circ \psi \circ \gamma)$.

- Cuando se ocupan varios cuantificadores de manera seriada, se evitará el uso excesivo de corchetes y se dejarán sólo los más internos. Es decir en vez de "$\daleth_1 x[\daleth_2 y[\ldots \daleth_n x[\varphi]\ldots]]$" se escribirá "$\daleth_1 x \daleth_2 y \ldots \daleth_n z[\varphi]$".

Ejemplo II.5 Con base en las convenciones previas, la fórmula bien formada:

$$\forall x_1[\forall x_2[\forall x_3[((P_1^2(x_1,x_2) \vee P_1^2(x_2,x_3)) \Rightarrow P_1^2(x_1,x_3))]]]$$

Se transforma en la expresión no bien formada:

$$\forall x_1 \forall x_2 \forall x_3[x_1 P_1^2 x_2 \vee x_2 P_1^2 x_3 \Rightarrow x_1 P_1^2 x_3]$$

Por otra parte, la fórmula bien formada:

$$\forall x_0[(P_1^2(x_0,c_0) \Rightarrow \exists x_1[\neg((P_1^2(x_1,c_0) \wedge P_2^2(x_0,x_1)) \wedge P_3^2(x_1,c_2))])]$$

Toma la forma abreviada de:

$$\forall x_0[x_0 P_1^2 c_0 \Rightarrow \exists x_1[\neg(x_1 P_1^2 c_0 \wedge x_0 P_2^2 x_1 \wedge x_1 P_3^2 c_2)]]$$

II. Semántica para la Lógica Predicativa

Recuérdese de los preliminares que el objetivo de esta sección es definir una colección de objetos $\{S_i \mid i \in \mathcal{I}\}$ que permitan definir la relación de satisfactibilidad $\models_{S_i}$ entre los objetos de dicha colección y las *wffs*. Tras definir dicha relación, las demás nociones de consecuencia semántica, validez lógica y otras similares se aunarán automáticamente. Como se pudo observar en la subsección previa, el alfabeto para los lenguajes predicativos incluye símbolos de una signatura, razón por la cual se debería sospechar que los objetos que permitirán definir la relación de satisfactibilidad son las estructuras restringidas a dichas signaturas:

Definición II.9 (Estructura para un Lenguaje Predicativo)
Dado un lenguaje predicativo $\mathcal{L}$, decimos que $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ es una estructura para $\mathcal{L}$ si y sólo si $\mathcal{D}$ es un conjunto no vacío, Σ es la signatura de $\mathcal{L}$ (la colección de símbolos no-lógicos de $\mathcal{L}$), e $\mathcal{I}$ es una función de interpretación, es decir, una función que a cada símbolo predicativo de aridad n, $P \in \mathcal{P}_n$, le asigna una relación n-aria $P^{\mathfrak{A}} \subseteq D^n$ y a cada símbolo funcional de aridad m, $f \in \mathcal{F}_m$, le asigna una función m-valuada $f^{\mathfrak{A}} : D^m \to D$.

Con base en lo que se dijo al inicio de la sección es posible decir que una estructura $\mathfrak{A}$ para un lenguaje predicativo $\mathcal{L}$ es una estructura (agrupación de conjuntos, funciones y relaciones) cuya signatura correspondiente es una subcolección del alfabeto de $\mathcal{L}$. De esta manera, ya dada la colección de objetos candidatos a ser semántica para los lenguajes predicativos, sólo resta definir la relación de satisfactibilidad, para lo cual se introduce el siguiente par de conceptos:

Definición II.10 (Valuación de un término bajo una estructura)
Sea $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ una estructura para un lenguaje $\mathcal{L}$, y considérese una *asignación (de variables) en* $\mathfrak{A}$, i.e. una función $\sigma : VAR \to \mathcal{D}$. Por el teorema de la definición por recursión se induce la valuación para términos $\mathrm{val}(t)[\sigma] : TERM \to \mathcal{D}$ de la siguiente manera:

$$\mathrm{val}_{\mathfrak{A}}(x)[\sigma] = \sigma(x)$$
$$\mathrm{val}_{\mathfrak{A}}(c)[\sigma] = c^{\mathfrak{A}}$$
$$\mathrm{val}_{\mathfrak{A}}(f(t_1, , \ldots, t_n))[\sigma] = f^{\mathfrak{A}}(\mathrm{val}_{\mathfrak{A}}(t_1)[\sigma], \ldots, \mathrm{val}_{\mathfrak{A}}(t_n)[\sigma])$$

Ejemplo II.6 En la estructura de los números enteros $\langle \mathbb{Z}; \bar{0}, \bar{1}, \bar{+}, \bar{\cdot} \rangle$, supóngase que $\sigma : VAR \to \mathbb{Z}$ cumple que $\sigma(x_n) := n$ para cada $n \in \mathbb{Z}^+ \cup \{0\}$. Entonces:

- $\mathrm{val}_{\mathfrak{A}}(x_9)[\sigma] = 9$
- $\mathrm{val}_{\mathfrak{A}}(x_{15})[\sigma] = 15$
- $\mathrm{val}_{\mathfrak{A}}(\bar{0})[\sigma] = 0$
- $\mathrm{val}_{\mathfrak{A}}(\bar{1})[\sigma] = 1$
- $\mathrm{val}_{\mathfrak{A}}(x_1 \bar{+} x_9)[\sigma] = 1 + 9 = 10$
- $\mathrm{val}_{\mathfrak{A}}(x_9 \bar{\cdot} x_9)[\sigma] = 9 \cdot 9 = 81$
- $\mathrm{val}_{\mathfrak{A}}(x_{302} \bar{+} x_{302})[\sigma] = 302 + 302 = 604$
- $\mathrm{val}_{\mathfrak{A}}(x_{12} \bar{\cdot} x_{11})[\sigma] = 12 \cdot 11 = 132$

Con base en esta definición se puede dar una valuación predicativa:

Definición II.11 (Valuación de una *wff* bajo una estructura)
Sea $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ una estructura para un lenguaje $\mathcal{L}$ y considérese una asignación $\sigma : VAR \to \mathcal{D}$. Se define recursivamente la valuación de fórmulas $[\![\cdot]\!]^{\sigma}_{\mathfrak{A}} : \mathcal{L} \to \{0, 1\}$ por medio de:

$$[\![p]\!]^{\sigma}_{\mathfrak{A}} = p^{\mathfrak{A}}$$
$$[\![P(t_1, , \ldots, t_n)]\!]^{\sigma}_{\mathfrak{A}} = \begin{cases} 1 & \text{si } (\mathrm{val}_{\mathfrak{A}}(t_1)[\sigma], \ldots, \mathrm{val}_{\mathfrak{A}}(t_n)) \in P^{\mathfrak{A}} \\ 0 & \text{si } (\mathrm{val}_{\mathfrak{A}}(t_1)[\sigma], \ldots, \mathrm{val}_{\mathfrak{A}}(t_n)) \notin P^{\mathfrak{A}} \end{cases}$$
$$[\![\neg\varphi]\!]^{\sigma}_{\mathfrak{A}} = 1 - [\![\varphi]\!]^{\sigma}_{\mathfrak{A}}$$
$$[\![(\varphi \wedge \psi)]\!]^{\sigma}_{\mathfrak{A}} = \text{mín}\{[\![\varphi]\!]^{\sigma}_{\mathfrak{A}}, [\![\psi]\!]^{\sigma}_{\mathfrak{A}}\}$$
$$[\![(\varphi \vee \psi)]\!]^{\sigma}_{\mathfrak{A}} = \text{máx}\{[\![\varphi]\!]^{\sigma}_{\mathfrak{A}}, [\![\psi]\!]^{\sigma}_{\mathfrak{A}}\}$$
$$[\![(\varphi \Rightarrow \psi)]\!]^{\sigma}_{\mathfrak{A}} = \begin{cases} 1 & \text{si } [\![\varphi]\!]^{\sigma}_{\mathfrak{A}} \leq [\![\psi]\!]^{\sigma}_{\mathfrak{A}} \\ 0 & \text{si } [\![\varphi]\!]^{\sigma}_{\mathfrak{A}} > [\![\psi]\!]^{\sigma}_{\mathfrak{A}} \end{cases}$$
$$[\![(\varphi \Leftrightarrow \psi)]\!]^{\sigma}_{\mathfrak{A}} = \begin{cases} 1 & \text{si } [\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = [\![\psi]\!]^{\sigma}_{\mathfrak{A}} \\ 0 & \text{si } [\![\varphi]\!]^{\sigma}_{\mathfrak{A}} \neq [\![\psi]\!]^{\sigma}_{\mathfrak{A}} \end{cases}$$
$$[\![\exists x[\varphi]]\!]^{\sigma}_{\mathfrak{A}} = \begin{cases} 1 & \text{si existe } d \in \mathcal{D} \text{ tal que } [\![\varphi]\!]^{\sigma^d_x}_{\mathfrak{A}} = 1 \\ 0 & \text{si no existe } d \in \mathcal{D} \text{ tal que } [\![\varphi]\!]^{\sigma^d_x}_{\mathfrak{A}} = 1 \end{cases}$$
$$[\![\forall x[\varphi]]\!]^{\sigma}_{\mathfrak{A}} = \begin{cases} 1 & \text{si todo } d \in \mathcal{D} \text{ cumple que } [\![\varphi]\!]^{\sigma^d_x}_{\mathfrak{A}} = 1 \\ 0 & \text{si no es cierto que todo } d \in \mathcal{D} \text{ cumple que } [\![\varphi]\!]^{\sigma^d_x}_{\mathfrak{A}} = 1 \end{cases}$$

Donde $\sigma_x^d : VAR \to \mathcal{D}$ cumple que $\sigma_x^d(y) = \sigma(y)$ para todo $y \neq x$ y $\sigma_x^d(x) = d$.[12]

Uno no debe perder de vista que lo desarrollado hasta ahora pretende coincidir con la noción intuitiva de lo que es una expresión verdadera. Por ejemplo, al tratar de determinar el valor de verdad de la ecuación $x + 2 = 7$, uno se ve forzado a decir que éste depende de quién sea x. Si x es 5, es claro que la ecuación es verdadera. Por otro lado si x no es 5, la ecuación es falsa. Las asignaciones de variables cumplen la función de decir quién es x, es decir, si $\sigma(x) = 5$, entonces $[\![x + 2 = 7]\!]_{\mathbb{R}}^{\sigma} = 1$ mientras que si $\sigma(x) \neq 5$ entonces $[\![x + 2 = 7]\!]_{\mathbb{R}}^{\sigma} = 0$.

Ejemplo II.7 Considérense las estructuras $\langle \mathbb{R}; 0, 1, -, ^{-1}, +, \cdot; \leq \rangle$ y $\langle \mathbb{Z}; 0, 1, -, +, \cdot; \leq \rangle$. Entonces:

- $[\![x + 0 = x]\!]_{\mathbb{R}}^{\sigma} = 1$ para toda asignación $\sigma : VAR \to \mathbb{R}$.
- $[\![z \cdot 1 = 1]\!]_{\mathbb{Z}}^{\sigma} = 0$ cuando $\sigma : VAR \to \mathbb{Z}$ cumple que $\sigma(z) \neq 1$.
- $[\![0 \leq 1 \wedge 1 + 0 = 1]\!]_{\mathbb{R}}^{\sigma} = 1$ para toda $\sigma : VAR \to \mathbb{R}$.
- $[\![1 \leq 1 \Rightarrow 1 \leq 1]\!]_{\mathbb{R}}^{\sigma} = 1$ para toda $\sigma : VAR \to \mathbb{R}$ e incluso si cambiamos de estructura a otra que tenga una relación binaria y una constante.
- $[\![\forall x[x \cdot x = 1]]\!]_{\mathbb{R}}^{\sigma} = 0$ porque σ_x^2 cumple que $\mathrm{val}_{\mathbb{R}}(x \cdot x)[\sigma_x^2] = 4$, lo cual implica que $[\![x \cdot x = 1]\!]_{\mathbb{R}}^{\sigma_x^2} = 0$. Es decir, no es cierto que todo $d \in \mathbb{R}$ cumple que la valuación de $[\![x \cdot x = 1]\!]_{\mathbb{R}}^{\sigma_x^d}$ es 1.
- $[\![\exists z[z \cdot z = 1 + 1]]\!]_{\mathbb{Z}}^{\sigma} = 0$ para toda $\mathbb{Z}$-asignación de variables $\sigma : VAR \to \mathbb{Z}$ porque sabemos que σ_z^d hará que las variables representen enteros y no hay ningún entero cuyo cuadrado sea 2.

De igual manera que en la sección pasada, se da el concepto de satisfactibilidad de una *wff* $\varphi \in \mathcal{L}$, pero esta vez se da en términos de las parejas $\langle \mathfrak{A}, \sigma \rangle$ siendo $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ una estructura para el lenguaje $\mathcal{L}$ y $\sigma : VAR \to \mathcal{D}$ una asignación de variables de $\mathcal{L}$ en $\mathfrak{A}$.

Definición II.12 (Satisfactibilidad)
Dada una estructura $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ para un lenguaje predicativo $\mathcal{L}$ y una $\mathfrak{A}$-asignación $\sigma : VAR \to \mathcal{D}$, se dice que $\langle \mathfrak{A}, \sigma \rangle$ satisface φ, i.e. $\models_{\langle \mathfrak{A}, \sigma \rangle} \varphi$ si y sólo si $[\![\varphi]\!]_{\mathfrak{A}}^{\sigma} = 1$. También se suele decir que φ es verdadera en $\mathfrak{A}$ bajo la asignación σ. La negación de esta relación se denota por $\not\models_{\langle \mathfrak{A}, \sigma \rangle} \varphi$. Se dice que una *wff* $\varphi \in \mathcal{L}$ es *satisfactible* si existe una pareja $\langle \mathfrak{A}, \sigma \rangle$ que la satisfaga, en caso contrario se dice que φ es *insatisfactible* o *contradictoria*. De igual manera, dada una teoría $\tau \subseteq \mathcal{L}$ de un lenguaje predicativo, se dice que $\langle \mathfrak{A}, \sigma \rangle$ *satisface a* τ, denotado por $\models_{\langle \mathfrak{A}, \sigma \rangle} \tau$, si $\models_{\langle \mathfrak{A}, \sigma \rangle} \varphi$ para cada $\varphi \in \tau$.

[12] Alternativamente: $[\![\exists x[\varphi]]\!]_{\mathfrak{A}}^{\sigma} = \text{máx}\{[\![\varphi]\!]_{\mathfrak{A}}^{\sigma_x^d} \mid d \in \mathcal{D}\}$ y $[\![\forall x[\varphi]]\!]_{\mathfrak{A}}^{\sigma} = \text{mín}\{[\![\varphi]\!]_{\mathfrak{A}}^{\sigma_x^d} \mid d \in \mathcal{D}\}$

Nuevamente directamente de las definiciones se tiene lo siguiente:

$$\begin{gathered}
\models_{\langle \mathfrak{A},\sigma\rangle} \neg\varphi \text{ sii } \not\models_{\langle \mathfrak{A},\sigma\rangle} \varphi \\
\models_{\langle \mathfrak{A},\sigma\rangle} (\varphi \wedge \psi) \text{ sii } \models_{\langle \mathfrak{A},\sigma\rangle} \varphi \text{ y } \models_{\langle \mathfrak{A},\sigma\rangle} \psi \\
\models_{\langle \mathfrak{A},\sigma\rangle} (\varphi \vee \psi) \text{ sii } \models_{\langle \mathfrak{A},\sigma\rangle} \varphi \text{ o } \models_{\langle \mathfrak{A},\sigma\rangle} \psi \\
\models_{\langle \mathfrak{A},\sigma\rangle} (\varphi \Rightarrow \psi) \text{ sii } \not\models_{\langle \mathfrak{A},\sigma\rangle} \varphi \text{ o } \models_{\langle \mathfrak{A},\sigma\rangle} \psi \\
\models_{\langle \mathfrak{A},\sigma\rangle} (\forall x[\varphi]) \text{ sii } \models_{\langle \mathfrak{A},\sigma^d_x\rangle} \varphi \text{ para todo } d \in \mathcal{D} \\
\models_{\langle \mathfrak{A},\sigma\rangle} (\exists x[\varphi]) \text{ sii existe } d \in \mathcal{D} \text{ tal que } \models_{\langle \mathfrak{A},\sigma^d_x\rangle} \varphi \\
\models_{\langle \mathfrak{A},\sigma\rangle} (\varphi \Leftrightarrow \psi) \text{ sii } (\models_{\langle \mathfrak{A},\sigma\rangle} \varphi \text{ y } \models_{\langle \mathfrak{A},\sigma\rangle} \psi) \text{ o } (\not\models_{\langle \mathfrak{A},\sigma\rangle} \varphi \text{ y } \not\models_{\langle \mathfrak{A},\sigma\rangle} \psi)
\end{gathered}$$

Además de la satisfactibilidad, siguiendo a los preliminares también se tienen las nociones de consecuencia semántica y *wff* válida bajo la semántica:

Definición II.13 (Consecuencia Lógica)
Una *wff* $\varphi \in \mathcal{L}$ es consecuencia lógica de un conjunto $\Gamma \subseteq \mathcal{L}$ de premisas, lo cual se denota por $\Gamma \models \varphi$, si y sólo si toda pareja $\langle \mathfrak{A}, \sigma\rangle$ que satisface a las *wffs* de Γ, también satisface a φ. Alternativamete, se escribe $\Gamma \models \varphi$ sii para cada $\mathcal{L}$-estructura $\mathfrak{A}$ y cada asignación de variables $\sigma : VAR \to \mathcal{D}$, si $\models_{\langle \mathfrak{A},\sigma\rangle} \psi$ para toda $\psi \in \Gamma$, entonces $\models_{\langle \mathfrak{A},\sigma\rangle} \varphi$.

Definición II.14 (Fórmula lógicamente válida)
Una *wff* $\varphi \in \mathcal{L}$ es lógicamente válida, expresado por $\models \varphi$, si toda pareja $\langle \mathfrak{A}, \sigma\rangle$ de $\mathcal{L}$-estructura y $\mathfrak{A}$-asignación de variables la satisface. Es decir, $\models \varphi$ sii $\models_{\langle \mathfrak{A},\sigma\rangle} \varphi$ para cada $\langle \mathfrak{A}, \sigma\rangle$.[13]

Siendo esta sección un tratado de lógica, el interés recae en determinar las *wffs* que son *lógicamente válidas* pero para responder a la pregunta de si una *wff* cumple esta propiedad o no es necesario considerar las asignaciones de variables y el cálculo de las valuaciones. Sin embargo, parte de dicho trabajo se puede reducir por medio del siguiente par de teoremas, los cuales permitirán estudiar la validez lógica únicamente con estructuras y sentencias (*wffs* sin variables libres), i.e. ignorando las asignaciones de variables y una gran cantidad de *wffs*:

Teorema II.7 (Asignaciones iguales en $FV(\varphi)$ inducen mismas valuaciones)
Supónganse dados una estructura $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I}\rangle$ para un lenguaje $\mathcal{L}$ y un par de asignaciones $\sigma, \bar{\sigma} : VAR \to \mathcal{D}$, entonces para cada $\varphi \in \mathcal{L}$, si $\sigma \restriction_{FV(\varphi)} = \bar{\sigma} \restriction_{FV(\varphi)}$, se cumple que $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = [\![\varphi]\!]^{\bar{\sigma}}_{\mathfrak{A}}$.

Demostración. La prueba debe ser por inducción sobre la complejidad de φ. Específicamente se probará que si dos asignaciones coinciden en las variables libres de φ, entonces $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = [\![\varphi]\!]^{\bar{\sigma}}_{\mathfrak{A}}$:

1. Si φ es un átomo, entonces φ es una letra proposicional $\varphi = p \in \mathcal{P}_0$ ó $\varphi = P(t_1, \ldots, t_n)$ con $P \in \mathcal{P}_n$ y $t_1, \ldots, t_n \in TERM$. En el primer caso ya se tiene lo

[13] Equivalentemente, $\models \varphi$ sii φ es consecuencia lógica del conjunto vacío.

deseado mientras que en el segundo sólo requerimos verificar, por inducción sobre la complejidad del término, que si las asignaciones coinciden en las variables de $t_i \in TERM$, entonces $\mathrm{val}_{\mathfrak{A}}(t_i)[\sigma] = \mathrm{val}_{\mathfrak{A}}(t_i)[\bar{\sigma}]$ para cada entero i entre 1 y n.

II. Supóngase que $\varphi = \neg\psi$ ó $\varphi = (\psi \circ \gamma)$ y que cualesquiera dos asignaciones $\sigma, \bar{\sigma}$ que coincidan en las variables libres de ψ y γ implicarán tanto que $[\![\psi]\!]^{\sigma}_{\mathfrak{A}} = [\![\psi]\!]^{\bar{\sigma}}_{\mathfrak{A}}$ como que $[\![\gamma]\!]^{\sigma}_{\mathfrak{A}} = [\![\gamma]\!]^{\bar{\sigma}}_{\mathfrak{A}}$. Se verifica que si $\sigma \restriction_{FV(\varphi)} = \bar{\sigma} \restriction_{FV(\varphi)}$, entonces $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = [\![\varphi]\!]^{\bar{\sigma}}_{\mathfrak{A}}$.

III. Finalmente, supóngase que $\varphi = \exists x[\psi]$ y que dadas dos asignaciones $\sigma, \bar{\sigma}$ que coincidan en las variables libres de ψ, se cumple que $[\![\psi]\!]^{\sigma}_{\mathfrak{A}} = [\![\psi]\!]^{\bar{\sigma}}_{\mathfrak{A}}$. Por definición del conjunto de variables libres se satisface $FV(\varphi) = FV(\psi) \setminus \{x\}$. De aquí que si $\sigma, \bar{\sigma}$ coinciden en las variables libres de φ, coinciden en las de ψ salvo por x. Considerando dos asignaciones $\sigma^d_x, \bar{\sigma}^d_x : VAR \to \mathcal{D}$ que satisfacen $\sigma^d_x(y) = \sigma(y)$ y $\bar{\sigma}^d_x(y) = \bar{\sigma}(y)$ para $y \in VAR \setminus \{x\}$ y $\sigma^d_x(x) = d = \bar{\sigma}^d_x(x)$, se cumple que $\sigma^d_x \restriction_{FV(\psi)} = \bar{\sigma}^d_x \restriction_{FV(\psi)}$. Por hipótesis de inducción para todo $d \in \mathcal{D}$ se cumple que $[\![\psi]\!]^{\sigma^d_x}_{\mathfrak{A}} = [\![\psi]\!]^{\bar{\sigma}^d_x}_{\mathfrak{A}}$. Por ende:

$$\min_{d\in\mathcal{D}} [\![\psi]\!]^{\sigma^d_x}_{\mathfrak{A}} = \min_{d\in\mathcal{D}} [\![\psi]\!]^{\bar{\sigma}^d_x}_{\mathfrak{A}} \text{ y } \max_{d\in\mathcal{D}} [\![\psi]\!]^{\sigma^d_x}_{\mathfrak{A}} = \max_{d\in\mathcal{D}} [\![\psi]\!]^{\bar{\sigma}^d_x}_{\mathfrak{A}}$$

Con lo cual se concluye que $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = [\![\varphi]\!]^{\bar{\sigma}}_{\mathfrak{A}}$.

■

El teorema anterior está diciendo que al computar la valuación $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}}$ de una *wff* $\varphi \in \mathcal{L}$ no se requieren todos los valores de la asignación σ, sino únicamente aquellos en las variables libres de la *wff*, es decir, los que corresponden al conjunto $FV(\varphi)$. Particularmente para las sentencias, la $\mathfrak{A}$-asignación σ es irrelevante para calcular $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}}$. Por esta razón es común que, en vez de definir la satisfactibilidad para todo el lenguaje $\mathcal{L}$, se defina $\models$ específicamente para las sentencias o, en su defecto, se den las siguientes definiciones:

Definición II.15 (Verdad en una estructura y Modelos)
Sea $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ una estructura para $\mathcal{L}$, se dice que $\varphi \in \mathcal{L}$ ***es verdadera en*** $\mathfrak{A}$ o que φ ***es verdadera relativo a*** $\mathfrak{A}$, i.e. $\models_{\mathfrak{A}} \varphi$ si y sólo si toda asignación en $\mathfrak{A}$, $\sigma : VAR \to \mathcal{D}$, cumple que $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = 1$. De igual manera se expresa que φ ***es falsa en*** $\mathfrak{A}$ sii no existe asignación σ en $\mathfrak{A}$ tal que $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = 1$. Además, para una teoría $\tau \subseteq \mathcal{L}$, $\mathfrak{A}$ es modelo de τ, denotado $\models_{\mathfrak{A}} \tau$, sii toda $\varphi \in \tau$ es verdadera en $\mathfrak{A}$.

Para enfatizar aún más lo que se está diciendo, del teorema y definición anteriores se enlistan los siguientes:

Corolario II.8 (Propiedades de sentencias)
Sea $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ una estructura para el lenguaje predicativo $\mathcal{L}$ y sea $\varphi \in \mathcal{L}$, una sentencia, entonces:

- Cualesquiera dos asignaciones de variables $\sigma, \bar{\sigma} : VAR \to \mathcal{D}$ que se escojan inducirán la misma valuación, i.e. $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = [\![\varphi]\!]^{\bar{\sigma}}_{\mathfrak{A}}$.

- En consecuencia: $\models_{\mathfrak{A}} \varphi$ ó $\not\models_{\mathfrak{A}} \varphi$.
- Si $\Gamma \subseteq \mathcal{L}$ es una teoría de sentencias, entonces $\Gamma \models \varphi$ si y sólo si todo modelo $\mathfrak{A}$ de Γ hace verdadera a φ.

Hacer uso de cualquiera de estos dos “trucos” no implica ningún problema respecto a la definición de validez lógica de las *wffs* que no sean sentencias debido a la siguiente definición y el teorema que conlleva:

Definición II.16 (Clausura universal de una fórmula bien formada)
Suponiendo que $FV(\varphi) = \{z_1, z_2, \ldots, z_n\}$, se define a la clausura universal de φ por:

$$\mathrm{Cl}(\varphi) := \forall z_1 \forall z_2 \ldots \forall z_n[\varphi]$$

Teorema II.9 (Equivalencia entre una fórmula y su clausura)
Sea $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ una estructura para $\mathcal{L}$, entonces se cumple que φ es verdadera en $\mathfrak{A}$ si y sólo si su clausura (universal) también lo es. Es decir, $\models_{\mathfrak{A}} \varphi$ sii $\models_{\mathfrak{A}} \mathrm{Cl}(\varphi)$.

Demostración. ($\Leftarrow$) Si $FV(\varphi) = \emptyset$, entonces φ es una sentencia y el resultado se garantiza por el teorema anterior. Supongamos que $FV(\varphi) = \{z_1, \ldots, z_n\}$ y sea $\sigma : VAR \to \mathcal{D}$ una asignación de variables en $\mathfrak{A}$. Por hipótesis tenemos que $1 = [\![\mathrm{Cl}(\varphi)]\!]_{\mathfrak{A}} = [\![\mathrm{Cl}(\varphi)]\!]_{\mathfrak{A}}^{\sigma} = [\![\forall z_1 \ldots \forall z_{n-1} \forall z_n[\varphi]]\!]_{\mathfrak{A}}^{\sigma} = \text{mín}_{d \in \mathcal{D}} [\![\forall z_1 \ldots \forall z_{n-1}[\varphi]]\!]_{\mathfrak{A}}^{\sigma_x^d}$. En particular σ es uno de éstos σ_x^d por lo que $1 \leq [\![\forall z_1 \ldots \forall z_{n-1}[\varphi]]\!]_{\mathfrak{A}}^{\sigma} \leq 1$ y, por ende, $[\![\forall z_1 \ldots \forall z_{n-1}[\varphi]]\!]_{\mathfrak{A}}^{\sigma} = 1$. Repitiendo el argumento $n-1$ veces se tiene que $[\![\varphi]\!]_{\mathfrak{A}}^{\sigma} = 1$.
($\Rightarrow$) Nuevamente, el caso en que φ es una sentencia ya se tiene por el teorema anterior. Por contrarrecíproca supóngase que $\not\models_{\mathfrak{A}} \mathrm{Cl}(\varphi)$. Entonces existe una asignación de variables $\sigma : VAR \to \mathcal{D}$ tal que $0 = [\![\mathrm{Cl}(\varphi)]\!]_{\mathfrak{A}}^{\sigma} = [\![\forall z_1 \ldots \forall z_{n-1} \forall z_n[\varphi]]\!]_{\mathfrak{A}}^{\sigma} = \text{mín}_{d \in \mathcal{D}} [\![\forall z_1 \ldots \forall z_{n-1}[\varphi]]\!]_{\mathfrak{A}}^{\sigma_x^d}$. De aquí que existe $d_n \in \mathcal{D}$ para el cual $[\![\forall z_1 \ldots \forall z_{n-1}[\varphi]]\!]_{\mathfrak{A}}^{\sigma_x^{d_n}} = 0$. Repitiendo el proceso $n-1$ veces, se encontrará una asignación σ^* tal que para cada $i \in \{1, \ldots, n\}$ existe un $d_i \in \mathcal{D}$ tal que $\sigma^*(z_i) = d_i$ y además $[\![\varphi]\!]_{\mathfrak{A}}^{\sigma^*} = 0$. Así se concluye que $\not\models_{\mathfrak{A}} \varphi$. ■

Corolario II.10
$\varphi \in \mathcal{L}$ es lógicamente válida si y sólo si su clausura también lo es. Es decir:

$$\models \varphi \text{ sii } \models \mathrm{Cl}(\varphi)$$

La prueba del corolario anterior es directa e inmediata. Gracias a este resultado es posible estudiar las *wffs* lógicamente válidas restringiéndo el análisis únicamente a las sentencias.

De manera idéntica que en lógica proposicional, en lógica de predicados se define una relación de equivalencia “$\equiv$”: decimos que dos sentencias φ, ψ son ***lógicamente equivalentes***, denotado por $\varphi \equiv \psi$, si y sólo si $\models \varphi \Leftrightarrow \psi$ o, alternativamente, si y sólo si $\varphi \models \psi$ y $\psi \models \varphi$. Una vez hecho esto, algunos de las siguientes propiedades de la lógica predicativa se pueden enunciar como equivalencias lógicas:

Propiedades II.11
Sea $\mathcal{L}$ un lenguaje predicativo, asumiendo que $\varphi, \psi \in \mathcal{L}$ y que $x, y, z \in VAR$, las siguientes son propiedades del cálculo de predicados correspondiente:

1. *Orden de Cuantificadores*
   - $\models \forall x \forall y[\varphi] \Leftrightarrow \forall y \forall x[\varphi]$
   - $\models \exists x \exists y[\varphi] \Leftrightarrow \exists y \exists x[\varphi]$
2. *Negación de Cuantificadores/ Generalización de las Leyes de De Morgan*
   - $\models \neg \forall x[\varphi] \Leftrightarrow \exists x[\neg \varphi]$
   - $\models \neg \exists x[\varphi] \Leftrightarrow \forall x[\neg \varphi]$
3. *Equivalencias de Cuantificadores*
   - $\models \forall x[\varphi] \Leftrightarrow \neg \exists x[\neg \varphi]$
   - $\models \exists x[\varphi] \Leftrightarrow \neg \forall x[\neg \varphi]$
   - Si $x \notin FV(\varphi)$: $\models \forall x[\varphi] \Leftrightarrow \varphi$
   - Si $x \notin FV(\varphi)$: $\models \exists x[\varphi] \Leftrightarrow \varphi$
4. *Distribución de cuantificadores en conectivos*
   - $\models \forall x[\varphi \wedge \psi] \Leftrightarrow \forall x[\varphi] \wedge \forall x[\psi]$
   - $\models \exists x[\varphi \vee \psi] \Leftrightarrow \exists x[\varphi] \vee \exists x[\psi]$
   - $\models \forall x[\varphi \vee \psi] \Leftrightarrow \forall x[\varphi] \vee \forall x[\psi]$ si $x \notin FV(\psi)$
   - $\models \exists x[\varphi \wedge \psi] \Leftrightarrow \exists x[\varphi] \wedge \exists x[\psi]$ si $x \notin FV(\psi)$
   - $\models (\forall x[\varphi] \Rightarrow \psi) \Leftrightarrow \exists x[\varphi \Rightarrow \psi]$ si $x \notin FV(\psi)$
   - $\models (\exists x[\varphi] \Rightarrow \psi) \Leftrightarrow \forall x[\varphi \Rightarrow \psi]$ si $x \notin FV(\psi)$
   - $\models (\varphi \Rightarrow \forall x[\psi]) \Leftrightarrow \forall x[\varphi \Rightarrow \psi]$ si $x \notin FV(\varphi)$
   - $\models (\varphi \Rightarrow \exists x[\psi]) \Leftrightarrow \exists x[\varphi \Rightarrow \psi]$ si $x \notin FV(\varphi)$
5. *Distribuciones no necesariamente válidas*
   - $\not\models \forall x[\varphi \vee \psi] \Rightarrow \forall x[\varphi] \vee \forall x[\psi]$
   - $\not\models \exists x[\varphi] \wedge \exists x[\psi] \Rightarrow \exists x[\varphi \wedge \psi]$
6. *Implicaciones válidas*
   - $\models \forall x[\varphi] \Rightarrow \exists x[\varphi]$
   - $\models \exists x \forall y[\varphi] \Rightarrow \forall y \exists x[\varphi]$
   - $\models \forall x[\varphi \Rightarrow \psi] \Rightarrow \forall x[\varphi] \Rightarrow \forall x[\psi]$
   - $\models (\exists x[\varphi] \Rightarrow \exists x[\psi]) \Rightarrow \exists x[\varphi \Rightarrow \psi]$
   - $\models \forall x[\varphi \Leftrightarrow \psi] \Rightarrow (\forall x[\varphi] \Leftrightarrow \forall x[\psi])$
   - $\models (\forall x[\varphi] \Rightarrow \exists x[\psi]) \Leftrightarrow \exists x[\varphi \Rightarrow \psi]$
   - $\models (\exists x[\varphi] \Rightarrow \forall x[\psi]) \Rightarrow \forall x[\varphi \Rightarrow \psi]$
7. *Implicaciones no necesariamente válidas*
   - $\not\models \forall x \exists y[\varphi] \Rightarrow \exists y \forall x[\varphi]$
   - $\not\models \exists x[\varphi] \Rightarrow \forall x[\varphi]$
8. *Propiedades de la igualdad*
   - $\models x = x$
   - $\models x = y \Rightarrow y = x$
   - $\models x = y \wedge y = z \Rightarrow x = z$
   - $\models (x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$ si $f \in \mathcal{F}_n$
   - $\models (x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \Rightarrow (P(x_1, \ldots, x_n) \Leftrightarrow P(y_1, \ldots, y_n))$ si $P \in \mathcal{F}_n$
9. Reglas de deducción semántica:
   - $\varphi \models \psi$ sii $\models \varphi \Rightarrow \psi$
   - *Modus Ponens*: $\varphi, \varphi \Rightarrow \psi \models \psi$
   - *Generalización*: Si $\models_{\mathfrak{A}} \varphi$, entonces $\models_{\mathfrak{A}} \forall x[\varphi]$
   - Si $\models_{\mathfrak{A}} \varphi$, entonces $\models_{\mathfrak{A}} \exists x[\varphi]$
   - No ocurre que $\models_{\mathfrak{A}} \varphi$ y $\models_{\mathfrak{A}} \neg \varphi$

Para terminar la sección sólo resta enunciar los teoremas de sustituibilidad y sus consecuencias. Sin embargo, en cálculo de predicados la sustitución es un proceso sutil que requiere un manejo formal adecuado. Considérese por ejemplo la *wff* $\varphi := \forall x \exists y [x < y \Rightarrow z = x]$ y analícense algunos tipos de sustitución que podrían hacerse:

- Es de esperarse que el resultado de una sustitución trivial $[y/y](\varphi)$ coincida con la función identidad, i.e. $[y/y](\varphi) = \varphi = \forall x \exists y [x < y \Rightarrow z = x]$.
- La sustitución $[w/z](\varphi)$ no requiere de mucho esfuerzo y el resultado prácticamente queda inafectado: $\forall x \exists y [x < y \Rightarrow w = x]$.
- No obstante, el cómputo de $[w/x](\varphi)$ podría ejecutarse en, al menos, dos maneras: $\forall w \exists y [w < y \Rightarrow z = w]$ ó $\forall x \exists y [x < y \Rightarrow z = x]$.
- Más aún, $[x/z](\varphi)$ determina la *wff* $\forall x \exists y [x < y \Rightarrow x = x]$ que siempre es verdadera en cualquier estructura con un símbolo predicativo de aridad 2 (y una igualdad). Es decir, se ha cambiado algo satisfactible en algo casi lógicamente válido.

La solución a este problema se da observando que el primer y tercer casos, corresponden a una sustitución donde la variable que va a ser afectada no está libre en φ, razón por la cual, en tales casos la sustitución deberá comportarse como una función identidad. La primera opción del tercer caso es lógicamente equivalente a φ por lo que se puede abordar desde el punto de vista semántico y no por la definición de sustitución. El cuarto caso es corregible al definir las sustituciones sólo para términos que no contengan variables que vayan a ser "atrapadas" por el alcance de un cuantificador al ser sustituidos (o agregando una operación extra en tales casos). Finalmente, el segundo caso es procedente debido a que no cumple ninguna de las restricciones consideradas hasta ahora. Sin más preámbulos, se dan las siguientes:

Definición II.17 (Sustitución de una variable por un término en términos)
Sean $t, t_1, \ldots, t_n \in TERM$, $x \neq y \in VAR$, $c \in \mathcal{F}_0$ y $f \in \mathcal{F}_n$, entonces:

$$\begin{aligned}
[t/x](x) &= t \\
[t/x](y) &= y \\
[t/x](c) &= c \\
[t/x](f(t_1, \ldots, t_n)) &= f([t/x](t_1), \ldots, [t/x](t_n))
\end{aligned}$$

Definición II.18 (Sustitución de una variable por un término en fórmulas)
[14]Sean $\varphi, \psi \in \mathcal{L}$; $t, t_1, \ldots, t_n \in TERM$; $\circ \in \Omega_2$; $\exists\!\!\!\!\forall \in \{\forall, \exists\}$; $x, y, z \in VAR$; $p \in \mathcal{P}_0$, y

[14]Algunas notaciones comunes para la sustitución de t por x en φ son: $\varphi^t_x, \varphi[x := t], \varphi[t/x]$ y $[t/x](\varphi)$.

$P \in \mathcal{P}_n$, entonces:

$$\begin{gathered}
[t/x](p) = p \\
[t/x](P(t_1, \ldots, t_n)) = P([t/x](t_1), \ldots, [t/x](t_n)) \\
[t/x](\neg\varphi) = \neg[t/x](\varphi) \\
[t/x](\varphi \circ \psi) = [t/x](\varphi) \circ [t/x](\psi) \\
[t/x](\exists y[\varphi]) = \begin{cases} \exists y[\varphi] & \text{si } x = y \\ \exists y[\varphi] & \text{si } x \neq y \text{ y } x \notin FV(\varphi) \\ \exists y[[t/x](\varphi)] & \text{si } x \neq y \text{ y } x \in FV(\varphi) \text{ y } y \notin V(t) \\ \exists z[[t/x]([z/y](\varphi))] & \text{si } x \neq y \text{ y } x \in FV(\varphi) \text{ y } y \in V(t) \\ & \text{con } z \notin FV(\varphi) \cup BV(\varphi) \cup V(t) \end{cases}
\end{gathered}$$

[15]Obsérvese que en la definición anterior, los primeros dos casos de $[t/x](\exists y[\varphi])$ se pudieron convertir en uno, mientras que el último se pudo haber omitido si en vez de hacerlo explícito se pide que *al realizar la sustitución, las variables del término no queden "atrapadas" en el alcance de un cuantificador que las afecte.* Esto se formaliza dando la siguiente definición:

Definición II.19 (Término sustituible por una variable en una fórmula)
[16] Sean $\varphi, \psi \in \mathcal{L}$; $t, t_1, \ldots, t_n \in TERM$; $\circ \in \Omega_2$; $\exists \in \{\forall, \exists\}$; $x, y \in VAR$; $p \in \mathcal{P}_0$, y $P \in \mathcal{P}_n$, entonces:

t siempre es *sustituible por* x *en* p

t siempre es *sustituible por* x *en* $P(t_1, \ldots, t_n)$

t *es sustituible por* x *en* $\neg\varphi$ sii t es sustituible por x en φ

t *es sustituible por* x *en* $(\varphi \circ \psi)$ sii t es sustituible por x en φ y en ψ

t *es sustituible por* x *en* $\exists y[\varphi]$ sii $x \notin FV(\exists y[\varphi])$ o $(y \notin V(t)$ y t es sustituible por x en $\varphi)$

De esta manera, se pudo haber dado la definición de $[t/x](\exists y[\varphi])$ como a continuación:

$$[t/x](\exists y[\varphi]) = \begin{cases} \exists y[\varphi] & \text{si } x \notin FV(\exists y[\varphi]) \\ \exists y[[t/x](\varphi)] & \text{si } x \in FV(\exists y[\varphi]) \text{ y } t \text{ es sustituible por } x \text{ en } (\exists y[\varphi] \end{cases}$$

Tomar esta opción significa considerar a $[t/x](\exists y[\varphi])$ indefinida en el caso en que t no es sustituible por x en φ. Esto no afecta el cómputo de la sustitución ya que, en teoría siempre es posible hacer la sustitución sugerida originalmente

[15]Es muy importante recordar que $x \notin FV(\varphi)$ debe leerse como "o x no ocurre en φ o todas las instancias de x están acotadas en φ". Además, se verifica que la condición $z \notin FV(\varphi) \cup BV(\varphi)$ es equivalente a "z no es una variable que ocurre en φ".
[16]También se suele hallar este concepto como *término libre para una variable en una fórmula.*

$[z/y](\varphi)$, siendo z una variable que no ocurra ni en φ ni en t, y después efectuar la sustitución $[t/x]$ sobre esta última. No obstánte, se está asumiendo que siempre existe una variable nueva con la cual se puede llevar a cabo "este truco". Esto es un problema si $\mathcal{L}$ tiene una cantidad finita de variables y la sustitución se trata de efectuar sobre una *wff* que tenga instancias de todas ellas. En dicho caso sólo queda dejar indefinida la sustitución o tener en cuenta que en la práctica siempre se trabaja con una cantidad finita de *wffs* por lo que el número de variables requeridas sólo debe ser suficientemente mayor a eso.

Una vez que la definición de sustitución de un término por una fórmula está dada, se enuncia y demuestra el teorema de su "buen comportamiento" bajo valuaciones predicativas:

Teorema II.12 (Sustituciones respetan valuaciones)
Sean $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ una $\mathcal{L}$-estructura, $\sigma : VAR \to \mathcal{D}$ una $\mathfrak{A}$-asignación, $t, s \in TERM$, $x \in VAR$ y $\varphi \in \mathcal{L}$, entonces:

a) $\mathrm{val}_{\mathfrak{A}}([t/x](s))[\sigma] = \mathrm{val}_{\mathfrak{A}}(s)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}]$

b) $[\![[t/x](\varphi)]\!]_{\mathfrak{A}}^{\sigma} = [\![\varphi]\!]_{\mathfrak{A}}^{\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}}$

Demostración. La prueba en ambos casos se hace por inducción sobre la complejidad de s y φ respectivamente:

- Suponiendo que $s \in VAR$ se tienen dos casos:
  - Si $s \neq x$, entonces $[t/x](s) = s$. Por lo que $\mathrm{val}_{\mathfrak{A}}([t/x](s))[\sigma] = \mathrm{val}_{\mathfrak{A}}(s)[\sigma] = \sigma(s) = \sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}(s) = \mathrm{val}_{\mathfrak{A}}(s)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}]$.
  - Si $s = x$, entonces $\mathrm{val}_{\mathfrak{A}}([t/x](s))[\sigma] = \mathrm{val}_{\mathfrak{A}}(t)[\sigma] = \sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}(x) = \sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}(s) = \mathrm{val}_{\mathfrak{A}}(s)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}]$.
- Si $s \in \mathcal{F}_0$, entonces $\mathrm{val}_{\mathfrak{A}}([t/x](s))[\sigma] = \mathrm{val}_{\mathfrak{A}}(s)[\sigma] = s^{\mathfrak{A}} = \mathrm{val}_{\mathfrak{A}}(s)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}]$.
- Supóngase que $t_1, \ldots, t_n \in TERM$ cumplen la propiedad en cuestión y también que $f \in \mathcal{F}_n$, entonces si $s = f(t_1, \ldots, t_n)$, se sigue que

$$\begin{aligned}
\mathrm{val}_{\mathfrak{A}}([t/x](s))[\sigma] &= \mathrm{val}_{\mathfrak{A}}(f([t/x](t_1), \ldots, [t/x](t_n)))[\sigma] \\
&= f^{\mathfrak{A}}(\mathrm{val}_{\mathfrak{A}}([t/x](t_1))[\sigma], \ldots, \mathrm{val}_{\mathfrak{A}}([t/x](t_n))[\sigma]) \\
&= f^{\mathfrak{A}}(\mathrm{val}_{\mathfrak{A}}(t_1)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}], \ldots, \mathrm{val}_{\mathfrak{A}}(t_n)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}]) \\
&= \mathrm{val}_{\mathfrak{A}}(f(t_1, \ldots, t_n))[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}] \\
&= \mathrm{val}_{\mathfrak{A}}(s)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t)[\sigma]}]
\end{aligned}$$

  Con lo cual culmina la prueba para los términos. El caso base en que φ es una letra proposicional es análogo al de $s \in \mathcal{F}_0$, arriba. De igual manera hay un argumento similar al de los símbolos funcionales con n términos cuando φ es un símbolo predicativo seguido de n términos. El caso en que φ es la concatenación de conectivos y *wffs*, la prueba es una aplicación directa de la hipótesis inductiva. Sólo resta revisar el caso en que $\varphi = \exists y[\psi]$ con ψ cumpliendo la propiedad en cuestión. Éste se divide en tres:

- Suponiendo que $x \notin FV(\exists y[\psi])$, entonces $[\![[t/x](\varphi)]\!]_{\mathfrak{A}}^{\sigma} = [\![[t/x](\exists y[\psi])]\!]_{\mathfrak{A}}^{\sigma} = [\![\exists y[\psi]]\!]_{\mathfrak{A}}^{\sigma}$, lo cual es igual a un límite lím, i.e. un mínimo o un máximo dependiendo del cuatificador que $\exists$ representa. Asi $[\![[t/x](\varphi)]\!]_{\mathfrak{A}}^{\sigma} = \text{lím}\{[\![\psi]\!]_{\mathfrak{A}}^{\sigma_y^d} \mid d \in \mathcal{D}\}$. Como $x \notin FV(\exists y[\psi])$, toda instancia de x en $\exists y[\psi]$ está acotada o x no aparece en $\exists y[\psi]$. En cualquiera de los dos casos, como las valuaciones sólo dependen de los valores de las asignaciones en las variables libres, se verifica que:

$$\text{lím}\{[\![\psi]\!]_{\mathfrak{A}}^{\sigma_y^d} \mid d \in \mathcal{D}\} = \text{lím}\{[\![\psi]\!]_{\mathfrak{A}}^{(\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]})_y^d} \mid d \in \mathcal{D}\}$$

  De esto se concluye que:

$$[\![[t/x](\varphi)]\!]_{\mathfrak{A}}^{\sigma} = \text{lím}\{[\![\psi]\!]_{\mathfrak{A}}^{(\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]})_y^d} \mid d \in \mathcal{D}\} = [\![\exists y[\psi]]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}} = [\![\varphi]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}}$$

- Si $x \in FV(\exists y[\psi])$ pero t es sustituible por x en $\exists y[\psi]$, entonces nótese que $x \neq y$ pues $y \notin FV(\exists y[\psi])$. Así:

$$[\![[t/x](\varphi)]\!]_{\mathfrak{A}}^{\sigma} = [\![\exists y[[t/x](\psi)]]\!]_{\mathfrak{A}}^{\sigma} = \text{lím}\{[\![[t/x]\psi]\!]_{\mathfrak{A}}^{\sigma_y^d} \mid d \in \mathcal{D}\} = \text{lím}\{[\![\psi]\!]_{\mathfrak{A}}^{(\sigma_y^d)_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}} \mid d \in \mathcal{D}\}$$

$$= [\![\exists y[\psi]]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}} = [\![\varphi]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}}.$$

- Obsérvese que hasta ahora lo demostrado es que las sustituciones si preservan valuaciones cuando "es posible efectuarlas". También nótese que t sí es sustituible por x en $\exists z[[z/y]\psi]$. Así, si t no es sustituible por x en $\exists y[\psi]$:

$$[\![[t/x](\exists z[[z/y](\psi)])]\!]_{\mathfrak{A}}^{\sigma} = [\![\exists z[[z/y](\psi)]]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}} \text{ y } [t/x](\exists z[[z/y](\psi)]) = \exists z[[t/x]([z/y](\psi))]$$

  A partir de estas dos igualdades se obtiene que:

$$\begin{aligned}\text{lím}\{[\![[t/x]([z/y](\psi))]\!]_{\mathfrak{A}}^{\sigma_z^d} \mid d \in \mathcal{D}\} &= \text{lím}\{[\![[z/y](\psi)]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}{}_z^d} \mid d \in \mathcal{D}\}\\ &= \text{lím}\{[\![\psi]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}{}_z^d{}_y^d} \mid d \in \mathcal{D}\}\\ &= \text{lím}\{[\![\psi]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}{}_y^d} \mid d \in \mathcal{D}\}\end{aligned}$$

  Donde la segunda línea se da por hipótesis de inducción y la tercera por la independencia entre las valuaciones y las variables que no son libres. Así se concluye que:

$$[\![[t/x](\varphi)]\!]_{\mathfrak{A}}^{\sigma} = [\![[t/x](\exists y[\psi])]\!]_{\mathfrak{A}}^{\sigma} = [\![\exists z[[t/x]([z/y]\psi)]]\!]_{\mathfrak{A}}^{\sigma} = [\![\exists y[\psi]]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}} = [\![\varphi]\!]_{\mathfrak{A}}^{\sigma_x^{\text{val}_{\mathfrak{A}}(t)[\sigma]}}$$

$\blacksquare$

Corolario II.13
Si $\mathcal{L}$ tiene una cantidad no finita de variables, entonces toda $\varphi \in \mathcal{L}$ es lógicamente equivalente a una *wff* en la que ninguna de sus variables ocurre libre y acotada a la vez.

En efecto, lo único que se debe hacer para probar el corolario anterior es hacer una sustitución por cada variable que ocurra libre y acotada en φ.

Las sustituciones de términos por variables no son las únicas que se pueden realizar en un cálculo de predicados, un ejemplo de esto es la siguiente:

Definición II.20 (Sustitución de una *wff* por otra)
Para $\varphi, \psi, \gamma \in \mathcal{L}$, se define la *sustitución de ψ por γ en φ*, $[\psi/\gamma](\varphi) : \mathcal{L} \to \mathcal{L}$, de la siguiente manera:

$$[\psi/\gamma](\varphi) = \begin{cases} \varphi & \text{si } \gamma \neq \varphi \\ \psi & \text{si } \gamma = \varphi \end{cases} \quad \text{si } \varphi \in At$$

$$[\psi/\gamma](\neg\varphi) = \neg[\psi/\gamma](\varphi)$$

$$[\psi/\gamma]((\varphi \circ \chi)) = ([\psi/\gamma](\varphi) \circ [\psi/\gamma](\chi))$$

$$[\psi/\gamma](\exists x[\varphi]) = \begin{cases} \exists x[[\psi/\gamma](\varphi)] & \text{si } x \notin FV(\psi) \\ \exists z[[\psi/\gamma]([z/x](\varphi))] & \text{si } x \in FV(\psi) \text{ con} \\ & z \notin FV(\varphi) \cup BV(\varphi) \cup FV(\psi) \cup BV(\psi) \end{cases}$$

También existe la noción de *wff sustituible por otra en una tercera* y es análoga a su contraparte para términos.

De esta definición se puede enunciar y probar el teorema de la sustitución:

Teorema II.14 (Teorema de la substitución para el cálculo de predicados)
Si $x \in VAR$; $s, t_1, t_2 \in TERM$, y $\varphi, \psi, \gamma, \chi \in \mathcal{L}$, entonces las siguientes son *wffs* verdaderas en toda estructura $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ con igualdad:

(I) $\models_{\mathfrak{A}} t_1 = t_2 \Rightarrow [t_1/x](s) = [t_2/x](s)$

(II) $\models_{\mathfrak{A}} t_1 = t_2 \Rightarrow ([t_1/x](\varphi) \Leftrightarrow [t_2/x](\varphi))$

(III) $\models_{\mathfrak{A}} (\psi \Leftrightarrow \gamma) \Rightarrow ([\psi/\chi](\varphi) \Leftrightarrow [\gamma/\chi](\varphi))$

Demostración. Se desea probar que toda estructura $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ con igualdad hace verdaderas a las implicaciones. Para ello obsérverse que si el antecedente en la implicación es valuado 0, entonces la implicación ya sería verdadera. Por eso se considerarán sólo las estructuras donde éste es valuado 1 y se probará que el consecuente tiene la misma valuación:

(I) Supóngase que $\models_{\mathfrak{A}} t_1 = t_2$ y sea $\sigma : VAR \to \mathcal{D}$ una asignación de variables. Por supuesto se cumple que $[\![t_1 = t_2]\!]^{\sigma}_{\mathfrak{A}} = 1$, lo cual a su vez implica que

$\mathrm{val}_{\mathfrak{A}}(t_1)[\sigma] = \mathrm{val}_{\mathfrak{A}}(t_2)[\sigma]$. Por el teorema anterior sabemos que $\mathrm{val}_{\mathfrak{A}}([t_1/x](s))[\sigma] = \mathrm{val}_{\mathfrak{A}}(s)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t_1)[\sigma]}] = \mathrm{val}_{\mathfrak{A}}(s)[\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t_2)[\sigma]}] = \mathrm{val}_{\mathfrak{A}}([t_2/x](s))[\sigma]$. Por lo cual se tiene que $[\![[t_1/x](s) = [t_2/x](s)]\!]_{\mathfrak{A}}^{\sigma} = 1$. Con esta prueba se concluye lo deseado, a decir, $\models_{\mathfrak{A}} [t_1/x](s) = [t_2/x](s)$.

(II) Utilizando la misma estrategia, si $\models_{\mathfrak{A}} t_1 = t_2$, entonces $[\![[t_1/x](\varphi)]\!]_{\mathfrak{A}}^{\sigma} = [\![\varphi]\!]_{\mathfrak{A}}^{\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t_1)[\sigma]}} = [\![\varphi]\!]_{\mathfrak{A}}^{\sigma_x^{\mathrm{val}_{\mathfrak{A}}(t_2)[\sigma]}} = [\![[t_2/x](\varphi)]\!]_{\mathfrak{A}}^{\sigma}$ para toda $\sigma : VAR \to \mathcal{D}$. De aquí se concluye que $\models_{\mathfrak{A}} [t_1/x](\varphi) \Leftrightarrow [t_2/x](\varphi)$.

(III) Para esta parte supóngase que $\models_{\mathfrak{A}} \psi \Leftrightarrow \gamma$. Como no se tiene un análogo al teorema anterior con la sustitución recientemente definida se procede por inducción sobre la complejidad de φ:

- Si φ es atómica, entonces la valuación de $[\psi/\chi](\varphi)$ es la misma que la de $[\gamma/\chi](\varphi)$ sin importar si ψ ó γ es igual a φ o no.
- Si $\varphi = \neg\psi$ ó $\varphi = \varphi_1 \circ \varphi_2$, se sigue lo deseado con una aplicación directa de la hipótesis de inducción.
- Si $\varphi = \exists x[\xi]$, la prueba debe considerar dos casos:
  - Si ψ y γ son sustituibles por χ en φ, entonces $[\psi/\chi](\exists x[\xi]) = \exists x[[\psi/\chi](\xi)]$ y $[\gamma/\chi](\exists x[\xi]) = \exists x[[\gamma/\chi](\xi)]$. Además por hipótesis inductiva se sabe que $[\![[\psi/\chi](\xi)]\!]_{\mathfrak{A}}^{\sigma} = [\![[\gamma/\chi](\xi)]\!]_{\mathfrak{A}}^{\sigma}$ para toda $\sigma : VAR \to \mathcal{D}$. Así:

    $$[\![\exists x[[\psi/\chi](\xi)]]\!]_{\mathfrak{A}}^{\sigma} = \lim_{d\in\mathcal{D}} [\![[\psi/\chi](\xi)]\!]_{\mathfrak{A}}^{\sigma_x^d} = \lim_{d\in\mathcal{D}} [\![[\gamma/\chi](\xi)]\!]_{\mathfrak{A}}^{\sigma_x^d} = [\![\exists x[[\gamma/\chi](\xi)]]\!]_{\mathfrak{A}}^{\sigma}$$

    Por ende $\models_{\mathfrak{A}} [\psi/\chi](\exists x[\xi]) \Leftrightarrow [\gamma/\chi](\exists x[\xi])$.
  - Si ψ y/o γ no son sustituibles por χ en $\exists x[\xi]$ entonces hay una cantidad finita de variables libres de ψ y/o γ que al ser sustituidas quedarían afectadas por un cuantificador en φ. Efectuando la sustitución definida previamente a la demostración actual, se cambiarían todas estas variables y el presente caso se reduciría al anterior. En otras palabras, la prueba es análoga a la última parte de la demostración del teorema previo a éste.

Por lo tanto $\models_{\mathfrak{A}} [\psi/\chi](\varphi) \Leftrightarrow [\gamma/\chi](\varphi)$.

■

Una vez que se tienen suficientes teoremas para trabajar con las sustituciones, se obtienen las siguientes propiedades y equivalencias lógicas:

Propiedades II.15
Sea $\mathcal{L}$ un lenguaje predicativo, asumiendo que $\varphi, \psi, \gamma \in \mathcal{L}$, $t \in TERM$ y que $x, y, z \in VAR$, las siguientes son propiedades del cálculo de predicados correspondiente a $\mathcal{L}$:

1. *Cambio de variables acotadas*: Si x, y son sustituibles por z en $\exists x[\varphi]$:
   - $\models \forall x[[x/z](\varphi)] \Leftrightarrow \forall y[[y/z](\varphi)]$
   - $\models \exists x[[x/z](\varphi)] \Leftrightarrow \exists y[[y/z](\varphi)]$
2. Es equivalente trabajar con estructuras finitas y lenguajes que tienen una constante por cada elemento de la estructura a trabajar con estructuras finitas y asignaciones. Es decir, si $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ con $\mathcal{D}$ finito y para cada $d \in \mathcal{D}$, existe $c \in \mathcal{F}_0$ tal que $c^{\mathfrak{A}} = d$, entonces toda $\varphi \in \mathcal{L}$ cumple que :
   - Si $x \in FV(\varphi)$ y $c^{\mathfrak{A}} = \sigma(x) = d \in \mathcal{D}$, entonces $\models_{\langle \mathfrak{A}, \sigma \rangle} \varphi \Leftrightarrow [c/x](\varphi)$.
3. Además, en los mismos tipos de lenguajes y estructuras hay una equivalencia entre los cuantificadores y la disyunción y la conjunción. Más precisamente, si $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ con $\mathcal{D} = \{d_1, \dots, d_n\}$ y para cada $i \in \{1, \dots, n\}$, existe $c_i \in \mathcal{F}_0$ tal que $c_i^{\mathfrak{A}} = d_i$, entonces para toda $\varphi \in \mathcal{L}$ con $x \in FV(\varphi)$:
   - $\models \forall x[\varphi] \Leftrightarrow ([c_1/x](\varphi) \wedge \cdots \wedge [c_n/x](\varphi))$.
   - $\models \exists x[\varphi] \Leftrightarrow ([c_1/x](\varphi) \vee \cdots \vee [c_n/x](\varphi))$.
4. Considérese al lenguaje $PROP_{\mathcal{L}}$ inducido al restringir las *wffs* de $\mathcal{L}$ sólo a aquéllas generadas por el alfabeto $\mathcal{P}_0 \cup \Omega$. Entonces las estructuras fungen como valuaciones atómicas para $\mathcal{P}_0$. De aquí que toda instancia de una tautología del cálculo proposicional es lógicamente válida en el cálculo de predicados, es decir:
   - Si $\varphi \in PROP_{\mathcal{L}}$ es una tautología, p es una literal (está en el soporte) de φ y $\psi \in \mathcal{L}$, entonces $\models [\psi/p](\varphi)$.
5. No sólo eso sino que, en general:
   - Si φ es lógicamente válida, entonces $[\psi/\gamma](\varphi)$ también lo es.
6. Finalmente, se enuncian algunas propiedades respecto a sustituciones, igualdades y cuantificadores:
   - $\models \forall x[\varphi] \Rightarrow [t/x](\varphi)$.[17]
   - Si $x \notin FV(\varphi)$, entonces $\models \forall x[\varphi \Rightarrow \psi] \Rightarrow (\varphi \Rightarrow \forall x[\psi])$.
   - Si t es libre para x en φ, entonces $\models [t/x](\varphi) \Rightarrow \exists x[\varphi]$.
   - $\models x = y \Rightarrow (\varphi \Rightarrow \varphi^*)$ donde φ^* surge al reemplazar zero, algunas o todas las instancias libres de x por y.
   - $\models \forall x \exists y[x = y]$.[18]
   - $\models \forall x[x = t \Rightarrow \varphi] \Leftrightarrow [t/x](\varphi)$ siempre que $x \notin V(t)$.

[17] Cuando no se da la definición de sustitución como se dio aquí, se debe pedir que t sea sustituible por x en φ.
[18] Obsérvese que aquí se requiere la condición $\mathcal{D} \neq \emptyset$ dada en la definición de estructuras.

III. Sistema formal para la Lógica Predicativa

En la presente subsección se procede análogamente a su contraparte proposicional, por ende, el alfabeto del lenguaje predicativo $\mathcal{L}$ sólo tendrá como conectivos a $\Omega = \{\neg, \Rightarrow\}$ y su único cuantificador será $\forall$. Similarmente se adoptan las mismas meta-abreviaciones para $\wedge, \vee$ y $\Leftrightarrow$, es decir:

- $(\varphi \wedge \psi)$ es una meta-abreviación para $\neg(\varphi \Rightarrow \neg\psi)$.
- $(\varphi \vee \psi)$ es una meta-abreviación para $(\neg\varphi \Rightarrow \psi)$.
- $(\varphi \Leftrightarrow \psi)$ es una meta-abreviación para $((\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi))$.

A la vez que se agrega la siguiente:

- $\exists x[\varphi]$ es una meta-abreviación para $\neg\forall x[\neg\varphi]$.

Además los axiomas del sistema formal a estudiar $\mathcal{K}$ son todas las *wffs* de la forma:

A1. $\varphi \Rightarrow (\psi \Rightarrow \varphi)$.

A2. $(\varphi \Rightarrow (\psi \Rightarrow \gamma)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \gamma))$.

A3. $(\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$.

A4. $\forall x[\varphi] \Rightarrow [t/x](\varphi)$ siendo t sustituible por x en φ.

A5. $\forall x[\varphi \Rightarrow \psi] \Rightarrow (\varphi \Rightarrow \forall x[\psi])$ con $x \notin FV(\varphi)$.

A6. $\forall x[x = t \Rightarrow \varphi] \Rightarrow [t/x](\varphi)$ con $x \notin V(t)$.

A7. $[t/x](\varphi) \Rightarrow \forall x[x = t \Rightarrow \varphi]$ con $x \notin V(t)$.

Mientras que las reglas de inferencia de $\mathcal{K}$ son *Modus Ponens* y *Generalización*:

$$\frac{\varphi \qquad \varphi \Rightarrow \psi}{\psi}MP \qquad\qquad \frac{\Gamma \vdash \varphi \qquad x \notin FV(\psi) \text{ para cada } \psi \in \Gamma}{\Gamma \vdash \forall x[\varphi]}Gen$$

Algunas aclaraciones respecto a las condiciones dadas recientemente son necesarias:

Los axiomas A1, A2, y A3 fueron agregados de tal manera que todas las tautologías de $PROP$ sean teoremas de este sistema formal también. Es decir, inmediatamente se da el siguiente:

Teorema II.16 (Instancias de tautologías son teoremas)
Sea $\varphi \in PROP_{\mathcal{L}}$ una tautología, si $\{\rho_1, \ldots, \rho_n\} \subseteq \mathcal{P}_0$, entonces para cualesquiera $\psi_1, \ldots, \psi_n \in \mathcal{L}$ se cumple que $\vdash_{\mathcal{K}} [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi)$.

Demostración. Si φ es una tautología, entonces por completez se verifica que $\vdash_{Ł} \varphi$. Esto significa que existe una prueba $\Delta = \langle \varphi_1, \ldots, \varphi_k \rangle$ en Ł de φ. Se demostrará por inducción que para cada $i \in \{1, \ldots, k\}$ se cumple que si $\{\rho_1, \ldots, \rho_n\} \subseteq \mathcal{P}_0$ y $\psi_1, \ldots, \psi_n \in \mathcal{L}$, entonces $\vdash_{\mathcal{K}} [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_i)$:

- Si $i = 1$ entonces $\varphi_i = \varphi_1$ es un axioma de Ł. Así, por inducción sobre n (la cantidad de átomos a sustituir), se prueba que $[\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_i)$ es una instancia de un axioma de $\mathcal{K}$, es decir, $\vdash_{\mathcal{K}} [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_1)$.

- Supóngase que para todo $i < l$, si $\{\rho_1, \ldots, \rho_n\} \subseteq \mathcal{P}_0$, entonces para cualesquiera $\psi_1, \ldots, \psi_n \in \mathcal{L}$ se cumple que $\vdash_{\mathcal{K}} [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_i)$. Veamos que esto también es válido para l. Si φ_l es un axioma de $\mathcal{K}$, la prueba es la misma que para el caso base. Por otro lado, si φ_l es consecuencia de aplicar *modus ponens* a φ_j y $\varphi_k := (\varphi_j \Rightarrow \varphi_l)$ con $j, k < l$, entonces, por hipótesis inductiva, si $\{\rho_1, \ldots, \rho_n\} \subseteq \mathcal{P}_0$, se verifica que $\vdash_{\mathcal{K}} [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_j \Rightarrow \varphi_l)$ y que $\vdash_{\mathcal{K}} [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_j)$. Además sabemos que:

$$[\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_j \Rightarrow \varphi_l) = [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_j) \Rightarrow [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi_l)$$

  Aplicando *modus ponens* se concluye lo deseado.

El resultado recientemente probado es válido particularmente también para $\varphi_k = \varphi$, con lo cual se concluye que $\vdash_{\mathcal{K}} [\psi_1/\rho_1] \cdots [\psi_n/\rho_n](\varphi)$. ■

En A4 la condición dada sólo es necesaria si se está trabajando con la sustitución que no está definida cuando t NO es sustituible por x en φ. En otras palabras, en el presente texto dicha condición sobra por razones discutidas en la subsección anterior. Además el axioma A4 trata de reflejar argumentos estándar en matemáticas, específicamente, cuando se sabe que una propiedad es válida para todo objeto y se quiere utilizarla sólo para uno:

Lema II.17 (Regla de Particularización - Regla A4)
(Si t es sustituible por x en φ, entonces) $\forall x[\varphi] \vdash_{\mathcal{K}} [t/x](\varphi)$.

Demostración. La prueba es una aplicación directa de *modus ponens* a A4. ■

Similarmente, A4 induce una regla para el cuantificador existencial:

Lema II.18 (Regla Existencial - Regla E4)
(Si t es sustituible por x en φ, entonces) $[t/x](\varphi) \vdash_{\mathcal{K}} \exists x[\varphi]$.

Demostración. Por A4 se tiene $\vdash_{\mathcal{K}} \forall x[\neg\varphi] \Rightarrow [t/x](\neg\varphi)$. Ya que $[t/x](\neg\varphi) = \neg[t/x](\varphi)$, por una instancia de una tautología y *modus ponens*, $\vdash_{\mathcal{K}} [t/x](\varphi) \Rightarrow \neg\forall x[\neg\varphi]$. Aplicando *modus ponens* a esta instancia de teorema y al supuesto se concluye lo deseado. ■

En los axiomas A5, A6 y A7 las condiciones están dadas siguiendo la validez lógica de los mismos revisada en la subsección anterior. Es fácil construir una estructura en que una instancia de alguno de ellos es falsa cuando las condiciones no se cumplen. Más aun, A6 y A7 permiten probar las siguientes:

Propiedades II.19 (de la Igualdad)
Para cualesquiera $t_1, t_2, t_3 \in TERM$ y $\varphi \in \mathcal{L}$:

1. $\vdash_{\mathcal{K}} t_1 = t_1$ (Reflexividad).
2. $t_1 = t_2 \vdash_{\mathcal{K}} t_2 = t_1$ (Simetría).
3. $t_1 = t_2, t_2 = t_3 \vdash_{\mathcal{K}} t_1 = t_3$ (Transitividad).
4. $t_1 = t_2 \vdash_{\mathcal{K}} [t_1/x](t_3) = [t_2/x](t_3)$ (S1).
5. $t_1 = t_2, [t_1/x](\varphi) \vdash_{\mathcal{K}} [t_2/x](\varphi)$ (S2).

Demostración. Si $x \notin V(t_1) \cup V(t_2) \cup V(t_3)$ con $t_1, t_2, t_3 \in TERM$, entonces:

Prueba de la reflexividad:

1.	$x = t_1 \Rightarrow x = t_1$	ID
2.	$\forall x[x = t_1 \Rightarrow x = t_1]$	Gen
3.	$\forall x[x = t_1 \Rightarrow x = t] \Rightarrow [t_1/x](x = t_1)$	A6
4.	$[t_1/x](x = t_1)$	MP(2,3)
$\therefore$	$t_1 = t_1$	Def.$[t/x]$

Prueba de la simetría:

1.	$t_2 = t_2$	Refl.
2.	$[t_2/x](t_2 = x)$	Def.$[t_2/x]$
3.	$[t_2/x](t_2 = x) \Rightarrow \forall x[x = t_2 \Rightarrow t_2 = x]$	A7
4.	$\forall x[x = t_2 \Rightarrow t_2 = x]$	MP(2,3)
5.	$[t_1/x](x = t_2 \Rightarrow t_2 = x)$	Regla A4(4)
6.	$t_1 = t_2 \Rightarrow t_2 = t_1$	Def. $[t_1/x]$
7.	$t_1 = t_2$	Hip.
$\therefore$	$t_2 = t_1$	MP(7,6)

Prueba de la transitividad:

1.	$t_2 = t_3$	Hip.
2.	$[t_2/x](x = t_3)$	Def.$[t_2/x]$
3.	$[t_2/x](x = t_3) \Rightarrow \forall x[x = t_2 \Rightarrow x = t_3]$	A7
4.	$\forall x[x = t_2 \Rightarrow x = t_3]$	MP(2,3)
5.	$[t_1/x](x = t_2 \Rightarrow x = t_3)$	Regla A4(4)
6.	$t_1 = t_2 \Rightarrow t_1 = t_3$	Def.$[t_1/x]$
7.	$t_1 = t_2$	Hip.
$\therefore$	$t_1 = t_3$	MP(7,6)

Para las últimas dos obsérvese que si $t \in TERM$ y $\alpha \in TERM \cup \mathcal{L}$ no tienen instancias de $y \in VAR$, entonces $[t/x](\alpha) = [t/y][y/x](\alpha)$. Así, supóngase que φ, t_1, t_2, t_3 no tienen instancias de $y \in VAR$:

1.	$[t_2/x](t_3) = [t_2/x](t_3)$	Refl
2.	$[t_2/y][y/x](t_3) = [t_2/x](t_3)$	Observación
3.	$[t_2/y]([y/x](t_3) = [t_2/x](t_3))$	Def.$[t_2/x]$
4.	$[t_2/y]([y/x](t_3) = [t_2/x](t_3)) \Rightarrow \forall y[y = t_2 \Rightarrow ([y/x](t_3) = [t_2/x](t_3))]$	A7
5.	$\forall y[y = t_2 \Rightarrow ([y/x](t_3) = [t_2/x](t_3))]$	MP(3,4)
6.	$[t_1/y](y = t_2 \Rightarrow ([y/x](t_3) = [t_2/x](t_3)))$	Regla A4(5)
7.	$t_1 = t_2 \Rightarrow [t_1/y]([y/x](t_3) = [t_2/x](t_3))$	Def.$[t_1/y]$
8.	$t_1 = t_2 \Rightarrow [t_1/x](t_3) = [t_2/x](t_3)$	Observacion
9.	$t_1 = t_2$	Hip.
$\therefore$	$[t_1/x](t_3) = [t_2/x](t_3)$	MP(9,8)

1.	$t_1 = t_2$	Hip.
2.	$[t_1/x](\varphi)$	Hip.
3.	$[t_1/y][y/x](\varphi)$	Observación
4.	$[t_1/y][y/x](\varphi) \Rightarrow \forall y[y = t_1 \Rightarrow [y/x](\varphi)]$	A7
5.	$\forall y[y = t_1 \Rightarrow [y/x](\varphi)$	MP(3,4)
6.	$[t_2/y](y = t_1 \Rightarrow [y/x](\varphi))$	Regla A4(5)
7.	$t_2 = t_1 \Rightarrow [t_2/x](\varphi)$	Observacion
8.	$t_2 = t_1$	Simetría(1)
$\therefore$	$[t_2/x](\varphi)$	MP(8,7)

■

Finalmente, la necesidad de la condición dada en la regla de *Generalización* se hace explícita en la demostración del:

Teorema II.20 (de la Deducción - CP)
Si $\varphi \in \mathcal{L}$ es una premisa en una prueba Δ de ψ, i.e. $\Gamma, \varphi \vdash_{\mathcal{K}} \psi$, entonces existe una prueba Δ' de $(\varphi \Rightarrow \psi)$ a partir de Γ que no usa a φ como premisa, es decir $\Gamma \vdash_{Ł} (\varphi \Rightarrow \psi)$. A manera de regla de inferencia:

$$\frac{\Gamma, \varphi \vdash_{\mathcal{K}} \psi}{\Gamma \vdash_{\mathcal{K}} \varphi \Rightarrow \psi} CP$$

Demostración. La estrategia es similar a la demostración inmediata anterior, es decir, si $\Delta = \langle \varphi_1, \ldots, \varphi_n \rangle$, por inducción se debe probar que para cada $i \in \{1, \ldots, n\}$ se cumple que $\Gamma \vdash_{\mathcal{K}} (\varphi \Rightarrow \varphi_i)$. El caso base es muy similar a su análogo proposicional. Por otra parte, el caso inductivo incluye consideraciones al momento de efectuar generalizaciones: Supóngase que $\Gamma \vdash_{\mathcal{K}} (\varphi \Rightarrow \varphi_i)$ para $i < k \leq n$. Si φ_k es φ, un axioma, una premisa en Γ o consecuencia de utilizar *modus ponens* a *wffs* anteriores en Δ, entonces la prueba de que $\Gamma \vdash_{\mathcal{K}} (\varphi \Rightarrow \varphi_k)$ es similar a los análogos proposicionales correspondientes. Si φ_k es consecuencia de aplicar *generalización* a φ_j con $j < k$, entonces $\varphi_k := \forall x[\varphi_j]$ siendo x una variable que no aparece libre en aquellas hipótesis requeridas para derivar a φ_j. De aquí se tienen dos casos:

- Si φ no se utilizó como hipótesis requerida para derivar φ_j, entonces una inducción sobre la longitud de esta derivación muestra que $\Gamma \vdash_{\mathcal{K}} \varphi_j$. Por *ge-*

neralización, $\Gamma \vdash_{\mathcal{K}} \forall x[\varphi_j]$ y, por A1, $\Gamma \vdash_{\mathcal{K}} (\forall x[\varphi_j] \Rightarrow (\varphi \Rightarrow \forall x[\varphi_j]))$. Una aplicación de *modus ponens* permite conlcuir $\Gamma \vdash_{\mathcal{K}} (\varphi \Rightarrow \varphi_k)$.

- Si φ sí se utilizó como hipótesis en la derivación de φ_j, entonces la variable x no aparece libre en φ. Esto permite afirmar una instancia de A5, i.e. $\Gamma \vdash_{\mathcal{K}} \forall x[\varphi \Rightarrow \varphi_j] \Rightarrow (\varphi \Rightarrow \forall x[\varphi_j])$. Además, por hipótesis inductiva se tiene que $\Gamma \vdash_{\mathcal{K}} (\varphi \Rightarrow \varphi_j)$ y, por *generalización*, $\Gamma \vdash_{\mathcal{K}} \forall x[\varphi \Rightarrow \varphi_j]$. Nuevamente, por *modus ponens*, $\Gamma \vdash_{\mathcal{K}} (\varphi \Rightarrow \forall x[\varphi_j])$. Es decir $\Gamma \vdash_{\mathcal{K}} (\varphi \Rightarrow \varphi_k)$.

■

Otros textos no restringen la regla de *generalización* como se hizo en el presente trabajo, sin embargo al momento de enunciar el teorema de la deducción deben agregar las condiciones necesarias para que éste sea válido, c.f. [Men97, End01]. Además, obsérvese que *generalización* trata de formalizar otra "manera cotidiana de razonar del matemático": si un objeto x indeterminado cumple la propiedad φ, entonces es válido concluir que todo objeto tiene la propiedad. Que x sea indeterminado se formaliza precisamente con la condición de que x no aparezca libre en aquellas hipótesis requeridas para deducir a φ. Considérese por ejemplo el siguiente razonamiento:

Ejemplo II.8 Supóngase como hipótesis que $x = c$ con $c \in \mathcal{F}_0$. De aquí, por *generalización* sin restricciones se cumple que $\forall x[x = c]$. Por el teorema de la deducción podría concluirse entonces que $\vdash_{\mathcal{K}} x = c \Rightarrow \forall x[x = c]$. No obstante, recuérdese que la propiedad deseada para $\mathcal{K}$ es que sea robusto y completo respecto a la semántica definida en la subsección anterior. Esto no se cumpliría ya que $\not\models x = c \Rightarrow \forall x[x = c]$ lo cual se verifica rápidamente usando una estructura $\mathfrak{A}$ con más de un elemento. De esta manera, evitar las restricciones en la regla de generalización limitaría las propiedades "deseables" del sistema formal $\mathcal{K}$ que esencialmente corresponden a representar "satisfactoriamente" el razonamiento lógico cotidiano.

Además, heredadas de lógica proposicional, también se tienen las siguientes:

Propiedades II.21 (Contradicción y Contrapositiva)
Dadas una teoría $\Gamma \subseteq \mathcal{L}$ y una *wff* $\varphi \in \mathcal{L}$:

- Si $\Gamma \cup \{\varphi\}$ es sintácticamente inconsistente, entonces $\Gamma \vdash_{\mathcal{K}} \neg\varphi$.
- Si $\Gamma, \varphi \vdash_{\mathcal{K}} \neg\psi$, entonces $\Gamma, \psi \vdash_{\mathcal{K}} \neg\varphi$.

Cuyas pruebas son exactamente las mismas que en lógica proposicional.

Por la manera en que se construyó el sistema formal $\mathcal{K}$ y las observaciones dadas al respecto no debería ser una sorpresa que se tenga el siguiente resultado:

Teorema II.22 (Robustez fuerte de la lógica predicativa)
Para $\varphi \in \mathcal{L}$ y $\Gamma \subseteq \mathcal{L}$:

$$\text{Si } \Gamma \vdash \varphi, \text{ entonces } \Gamma \models \varphi$$

Demostración. Sean $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ una estructura para $\mathcal{L}$, $\sigma : VAR \to \mathcal{D}$ una asignación de variables y supóngase que $\models_{\langle \mathfrak{A}, \sigma \rangle} \Gamma$. Por definición para cada $\varphi \in \Gamma$ se cumple que $[\![\varphi]\!]^{\sigma}_{\mathfrak{A}} = 1$. Más aún, de la subsección pasada sabemos que todas las instancias de axiomas A1, A2, A3, A4, A5, A6 y A7 son lógicamente válidas y en consecuencia se verifica el caso base para esta prueba, es decir:

- $\models_{\langle \mathfrak{A}, \sigma \rangle} \varphi \Rightarrow (\psi \Rightarrow \varphi)$.
- $\models_{\langle \mathfrak{A}, \sigma \rangle} (\varphi \Rightarrow (\psi \Rightarrow \gamma)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \gamma))$.
- $\models_{\langle \mathfrak{A}, \sigma \rangle} (\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$.
- $\models_{\langle \mathfrak{A}, \sigma \rangle} \forall x[\varphi] \Rightarrow [t/x](\varphi)$ (siendo t sustituible por x en φ).
- $\models_{\langle \mathfrak{A}, \sigma \rangle} \forall x[\varphi \Rightarrow \psi] \Rightarrow (\varphi \Rightarrow \forall x[\psi])$ con $x \notin FV(\varphi)$.
- $\models_{\langle \mathfrak{A}, \sigma \rangle} \forall x[x = t \Rightarrow \varphi] \Rightarrow [t/x](\varphi)$ con $x \notin V(t)$.
- $\models_{\langle \mathfrak{A}, \sigma \rangle} [t/x](\varphi) \Rightarrow \forall x[x = t \Rightarrow \varphi]$ con $x \notin V(t)$.

Como caso inductivo se tiene que:

- Si $\models_{\langle \mathfrak{A}, \sigma \rangle} \varphi$ y $\models_{\langle \mathfrak{A}, \sigma \rangle} (\varphi \Rightarrow \psi)$, entonces, ya que las valuaciones respetan *modus ponens*, $\models_{\langle \mathfrak{A}, \sigma \rangle} \psi$.
- Sea x una variable tal que $x \notin FV(\psi)$ para cada $\psi \in \Gamma$ y supóngase que $\Gamma \models \varphi$. Si $d \in \mathcal{D}$, entonces obsérvese que $[\![\psi]\!]^{\sigma^d_x}_{\mathfrak{A}} = [\![\psi]\!]^{\sigma}_{\mathfrak{A}} = 1$. Por hipótesis inductiva se cumple que $[\![\varphi]\!]^{\sigma^d_x}_{\mathfrak{A}} = 1$, lo cual implica que $[\![\forall x[\varphi]]\!]^{\sigma}_{\mathfrak{A}} = \text{mín}_{d \in \mathcal{D}} [\![\varphi]\!]^{\sigma^d_x}_{\mathfrak{A}} = 1$. Por lo tanto $\models_{\langle \mathfrak{A}, \sigma \rangle} \forall x[\varphi]$.

Por *inducción sobre las pruebas a partir de* Γ se cumple que $\models_{\langle \mathfrak{A}, \sigma \rangle} \varphi$ para cada φ tal que $\Gamma \vdash \varphi$. En resumen, se ha probado que toda consecuencia sintáctica de Γ es también consecuencia semántica de Γ. ■

Antes de probar el teorema de completez de $\mathcal{K}$, se recuerdan las siguientes definiciones:

Definición II.21 (Consistencia y completez)
Sea $\Gamma \subseteq \mathcal{L}$ una teoría, entonces:

- Γ es contradictoria (sintácticamente inconsistente) si y sólo si existe $\varphi \in \mathcal{L}$ tal que $\Gamma \vdash_{\mathcal{K}} \varphi$ y $\Gamma \vdash_{\mathcal{K}} \neg\varphi$.
- Γ es (sintácticamente) consistente si y sólo si no es contradictoria.
- Γ es (sintácticamente) completa si y sólo si para toda $\varphi \in \mathcal{L}$ se cumple que ó $\varphi \in \Gamma$ ó $\neg\varphi \in \Gamma$.

Con éstas y con el teorema anterior se obtiene el siguiente:

Corolario II.23 (Consistencia semántica implica consistencia sintáctica)
Si Γ es satisfactible (semánticamente consistente), i.e. si existen una estructura $\mathfrak{A}$ y una asignación σ tales que $\models_{\langle \mathfrak{A},\sigma\rangle} \Gamma$, entonces Γ es (sintácticamente) consistente.

Demostración. El resultado se demostrará probando el contrarrecíproco. Así, supóngase que Γ no es consistente, entonces existe $\varphi \in \mathcal{L}$ tal que $\Gamma \vdash_{\mathcal{K}} \varphi$ y $\Gamma \vdash_{\mathcal{K}} \neg\varphi$. Por robustez esto significa que $\Gamma \models \varphi$ y $\Gamma \models \neg\varphi$. Pero ninguna pareja $\langle \mathfrak{A}, \sigma\rangle$ cumple que $\models_{\langle \mathfrak{A},\sigma\rangle} \varphi$ y $\models_{\langle \mathfrak{A},\sigma\rangle} \neg\varphi$, por lo cual no hay pareja $\langle \mathfrak{A}, \sigma\rangle$ que satisfaga a todas las fórmulas de Γ, es decir, Γ no es satisfactible. ■

A continuación se irán probando lemas, cada uno de los cuales servirá para verificar la completez (semántica) fuerte de la lógica predicativa:

Lema II.24 (de Lindembaum-Tarski)
Dada una teoría de primer orden (sintácticamente) consistente Γ_0 es posible expandirla para obtener una teoría de primer orden $\Gamma \supseteq \Gamma_0$ consistente y (sintácticamente) completa.

La prueba del enunciado anterior es la misma que la de su análogo proposicional. Más aun, el siguiente también es un meta-teorema respecto a $\mathcal{K}$:

Lema II.25 (Generalización sobre constantes)
Dados un lenguaje predicativo $\mathcal{L}$, una teoría $\Gamma \subseteq \mathcal{L}$, una *wff* $\varphi \in \mathcal{L}$, una constante $c \in \mathcal{F}_0$ que no ocurre en ninguna *wff* en Γ, se cumple que si $\Gamma \vdash_{\mathcal{K}} [c/x](\varphi)$, entonces $\Gamma \vdash_{\mathcal{K}} \forall x[\varphi]$.

Demostración. Sea $\Delta = \langle \varphi_1, \ldots, \varphi_k\rangle$ la prueba de $[c/x](\varphi)$ a partir de Γ en $\mathcal{K}$, probaremos que $\Delta' = \langle [y/c](\varphi_1), \ldots, [y/c](\varphi_k)\rangle$[19], con y una variable que no ocurre en alguna *wff* de Δ, es una prueba de $[y/c]([c/x](\varphi)) = [y/x](\varphi)$ a partir de Γ en $\mathcal{K}$:

- Si φ_i es un axioma entonces la sustitución $[y/c](\varphi_1)$ no afectará este hecho.
- Por otro lado, si φ_i es una premisa, entonces c no ocurre en φ_i (por hipótesis) por lo cual $[y/c](\varphi_i) = \varphi_i \in \Gamma$.
- Si φ_i es consecuencia de *modus ponens* aplicado a $\varphi_j \Rightarrow \varphi_i$ y φ_j con $j < i$, entonces $[y/c](\varphi_i)$ es consecuencia de aplicar *modus ponens* a $[y/c](\varphi_j \Rightarrow \varphi_i) = [y/c](\varphi_j) \Rightarrow [y/c](\varphi_i)$ y a $[y/c](\varphi_j)$.
- Si $\varphi_i := \forall z[\varphi_j]$ es resultado de aplicar *generalización* a φ_j con $j < i$ y z, una variable que no está libre en las φ_k tales que $k \leq j$, entonces $[y/c](\forall z[\varphi_j]) = \forall z[[y/c](\varphi_j)]$ quien es consecuencia de una *generalización* sobre $[y/c](\varphi_j)$.

[19] La definición de la substitución de una constante por una variable, aunque no fue dada anteriormente, con la condición dada en la prueba es fácilmente definible y no genera mayores problemas.

De aquí se obtiene que Δ' es una prueba de $[y/x](\varphi)$ a partir de Γ en $\mathcal{K}$. Ya que y no ocurre en las *wffs* de Γ, por generalización se cumple que $\Gamma \vdash \forall y[[y/x](\varphi)]$. Por regla de particularización (regla A4), también es válido que $\Gamma \vdash [x/y]([y/x](\varphi))$, i.e. $\Gamma \vdash \varphi$. Como x fue sustituida por y en Δ', se cumple que $x \notin FV(\psi)$ para ψ en Δ', por lo que se puede aplicar *generalización* nuevamente y concluir que $\Gamma \vdash \forall x[\varphi]$. ■

Estos lemas y la siguiente definición se utilizarán para efectuar la prueba estándar de la completez de $\mathcal{K}$:

Definición II.22 (Teoría Henkin)
Sea $\mathcal{L}$ un lenguaje predicativo, entonces $\Gamma \subseteq \mathcal{L}$ es una teoría Henkin, también llamada teoría-chivo-expiatorio, sii para cada $\varphi \in \mathcal{L}$, existe una constante $c_\varphi \in \mathcal{F}_0$ tal que $(\neg\forall x[\varphi] \Rightarrow \neg[c_\varphi/x](\varphi)) \in \Gamma$. A c_φ se le denomina el Henkin-testigo de φ.

Lema II.26 (de Lindembaum-Tarski para teorías Henkin)
Toda teoría consistente $\Gamma \subseteq \mathcal{L}$ tiene una extensión Henkin $\Gamma''' \supseteq \Gamma$ completa y consistente.

Demostración. De igual manera que en la versión original para teorías no-Henkin, se construye una sucesión de lenguajes predicativos $\mathcal{L}_0 \subseteq \mathcal{L}_1 \subseteq \mathcal{L}_2 \ldots$ y una sucesión de teorías $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \ldots$ tales que $\Gamma_i \subseteq \mathcal{L}_i$ para $i \in \mathbb{Z} \cup \{0\}$. Ya que los lenguajes predicativos, en general sólo cambian en su signatura (parte no lógica), es suficiente con construir una sucesión de signaturas $\Sigma_0 \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \ldots$. Defínase así $\Sigma_0 := \Sigma$ y $\Sigma_{n+1} := \Sigma_n \cup \{c_\varphi \mid \varphi \in \mathcal{L}_n\}$, i.e. $\mathcal{L}_{n+1}$ es el lenguaje predicativo generado al agregar a las constantes de $\mathcal{L}_n$ una nueva (y distinta a todas las demás) c_φ por cada $\varphi \in \mathcal{L}_n$. Se verifica rápidamente que $\mathcal{L}_n \subseteq \mathcal{L}_{n+1}$ para cada $n \in \mathbb{Z} \cup \{0\}$. Por otro lado, se hace fijo que $\Gamma_0 := \Gamma$ y recursivamente se define $\Gamma_{n+1} := \Gamma_n \cup \{(\neg\forall x[\varphi] \Rightarrow \neg[c_\varphi/x](\varphi)) \mid \varphi \in \mathcal{L}_n\}$ para finalmente denotar:

$$\mathcal{L}' := \bigcup_{n \in \mathbb{Z}\cup\{0\}} \mathcal{L}_n \text{ y } \Gamma' := \bigcup_{n \in \mathbb{Z}\cup\{0\}} \Gamma_n$$

Sea $\Gamma'' := \{\varphi \in \mathcal{L}' \mid \Gamma' \vdash \varphi\}$, entonces claramente $\Gamma \subseteq \Gamma' \subseteq \Gamma''$. Veamos que Γ'' es una teoría de Henkin consistente:

- Si $\varphi \in \mathcal{L}'$ entonces existe $n \in \mathbb{Z} \cup \{0\}$ tal que $\varphi \in \mathcal{L}_n$. Por definición de Γ_n sabemos que $(\neg\forall x[\varphi] \Rightarrow \neg[c_\varphi/x](\varphi)) \in \Gamma_n \subseteq \Gamma''$. Por ende Γ'' es una teoría Henkin.

- Para probar la consistencia de Γ'' es suficiente con ver, por inducción, que cada Γ_n es consistente. Por hipótesis Γ_0 es consistente. Supóngase que Γ_n es consistente pero que Γ_{n+1} no lo es. Como las deducciones son finitas existe $\Delta \subseteq \{(\neg\forall x[\varphi] \Rightarrow \neg[c_\varphi/x](\varphi)) \mid \varphi \in \mathcal{L}_n\}$ finito y $\varphi \in \mathcal{L}_{n+1}$ tal que $\Gamma_n \cup \Delta \vdash \varphi$ y $\Gamma_n \cup \Delta \vdash \neg\varphi$. Así, aplicando la regla de contradicción, para $\psi \in \Delta$ se cumple que $\Gamma_n \cup (\Delta \setminus \{\psi\}) \vdash \neg\psi$. Ya que $\neg\psi$ tiene la forma $\neg(\neg\forall x[\varphi] \Rightarrow \neg[c_\varphi/x](\varphi))$, con razonamientos tautológicos se puede probar que $\Gamma_n \cup (\Delta \setminus \{\psi\}) \vdash \neg\forall x[\varphi]$ y que $\Gamma_n \cup (\Delta \setminus \{\psi\}) \vdash [c_\varphi/x](\varphi)$. Por generalización sobre constantes se obtiene de esta última que $\Gamma_n \cup (\Delta \setminus \{\psi\}) \vdash \forall x[\varphi]$. Por ende $\Gamma_n \cup (\Delta \setminus \{\psi\})$ es contradictoria. Aplicando este mismo argumento hasta agotar todas las *wffs* de $\Delta \setminus \{\psi\}$ se concluye que Γ_n es inconsitente, lo cual contradice la hipótesis de inducción. Así Γ' es consistente y, consecuentemente, Γ'' también.

De aquí sólo queda aplicar el lema de Lindembaum-Tarski original para obtener una teoría de Henkin $\Gamma''' \supseteq \Gamma'' \supseteq \Gamma$ completa y consistente. ■

Lema II.27 (de Henkin)
Si Γ es una teoría Henkin completa y consistente, entonces Γ admite un modelo.

Demostración. Considérese la relación sobre términos:

$$t \sim s \text{ sii } (t = s) \in \Gamma$$

Por las propiedades de la igualdad se verifica que $\sim$ es de equivalencia. Considérese ahora a las clases de equivalencia inducidas por ésta:

$$\mathcal{D} := \frac{TERM}{\sim} := \{[t] \mid t \in TERM\}$$

Además para $f \in \mathcal{F}_n$ con $n \in \mathbb{Z}^+$ defínase a la interpretación $\mathcal{I}$ de f bajo $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$ por $f^{\mathfrak{A}}([t_1], \ldots, [t_n]) := [f(t_1, \ldots, t_n)]$ (la clase de equivalencia del término $f(t_1, \ldots, t_n)$). Esto está bien definido porque, gracias a las propiedades de la igualdad (S1), se puede obtener una prueba de $(s_1 = t_1 \wedge \cdots \wedge s_n = t_n) \Rightarrow f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)$ en $\mathcal{K}$. Más aun, particularmente para $c \in \mathcal{F}_0$, definimos $c^{\mathfrak{A}} = [c]$. Finalmente, para $P \in \mathcal{P}_n$ con $n \in \mathbb{Z}^+$ diremos que $\langle [t_1], \ldots, [t_n] \rangle \in \mathcal{P}^{\mathfrak{A}}$ si y sólo si $P(t_1, \ldots, t_n) \in \Gamma$ y, en especial para $p \in \mathcal{P}_0$ definimos $p^{\mathfrak{A}} = 1$ si y sólo si $p \in \Gamma$. Con base en esto, probamos por inducción sobre el número de conectivos y cuantificadores en φ, que $\models_{\mathfrak{A}} \varphi$ si y sólo si $\varphi \in \Gamma$:

- Si φ no tiene cuantificadores ni conectivos, entonces φ es atómica, de donde se desprenden dos casos:
  - Por construcción $\models_{\mathfrak{A}} p$ si y sólo si $p \in \Gamma$.
  - $\models_{\mathfrak{A}} P(t_1, \ldots, t_n)$ sii $\langle t_1^{\mathfrak{A}}, \ldots, t_n^{\mathfrak{A}} \rangle \in \mathcal{P}^{\mathfrak{A}}$ sii $\langle [t_1], \ldots, [t_n] \rangle \in \mathcal{P}^{\mathfrak{A}}$ sii $P(t_1, \ldots, t_n) \in \Gamma$.
- Supóngase que si el número de cuantificadores y conectivos en γ es menor que k, entonces $\models_{\mathfrak{A}} \gamma$ si y sólo si $\gamma \in \Gamma$. Así:
  - Si el número de cuantificadores y conectivos en $\neg\varphi$ es k, entonces φ tiene $k-1$, por lo que $\models_{\mathfrak{A}} \varphi$ si y sólo si $\varphi \in \Gamma$. De aquí que $\models_{\mathfrak{A}} \neg\varphi$ sii $\not\models_{\mathfrak{A}} \varphi$ sii $\varphi \notin \Gamma$ sii $\neg\varphi \in \Gamma$.
  - Si el número de cuantificadores y conectivos en $\varphi \Rightarrow \psi$ es k, entonces φ y ψ tienen menos que k, por lo que la hipótesis de inducción aplica en ellas. De aquí que $\models_{\mathfrak{A}} \varphi \Rightarrow \psi$ sii ($\not\models_{\mathfrak{A}} \varphi$ ó $\models_{\mathfrak{A}} \psi$) sii ($\neg\varphi \in \Gamma$ ó $\psi \in \Gamma$) sii $\varphi \Rightarrow \psi \in \Gamma$ (por A1, el principio de explosión, *modus ponens* y *modus tollens*).

- Si el número de cuantificadores y conectivos en $\forall x[\varphi]$ es k, entonces φ tiene $k-1$ y la hipótesis de inducción le aplica:
  ($\Rightarrow$) Si $\models_{\mathfrak{A}} \forall x[\varphi]$ es fácil ver que $\models_{\mathfrak{A}} [c_\varphi/x](\varphi)$ y, por hipótesis inductiva, $[c_\varphi/x](\varphi) \in \Gamma$. Supongamos para obtener una contradicción que $\forall x[\varphi] \notin \Gamma$. Por completez obtenemos que $\neg\forall x[\varphi] \in \Gamma$. Por ser teoría Henkin, también se cumple que $(\neg\forall x[\varphi] \Rightarrow \neg[c_\varphi/x](\varphi)) \in \Gamma$, lo cual por *modus ponens* implica que $\neg[c_\varphi/x](\varphi) \in \Gamma$, lo cual contradice que Γ sea consistente. Por lo tanto $\forall x[\varphi] \in \Gamma$
  ($\Leftarrow$) Si $\forall x[\varphi] \in \Gamma$, entonces por particularización $[t/x](\varphi) \in \Gamma$. Aplicando la hipótesis inductiva se tiene que $\models_{\mathfrak{A}} [t/x](\varphi)$, de donde fácilmente se obtiene que $\models_{\mathfrak{A}} \varphi$. Por generalización semántica $\models_{\mathfrak{A}} \forall x[\varphi]$.

De aquí que si $\varphi \in \Gamma$, entonces existe $\mathfrak{A} = \langle \mathcal{D}, \Sigma, \mathcal{I} \rangle$, tal que $\models_{\mathfrak{A}} \varphi$, es decir, Γ admite un modelo. ■

El lema de Henkin es parte del argumento estándar contemporáneo para probar la completez de $\mathcal{K}$ y se prefiere porque es más fácil generalizarlo a lenguajes de cualquier cardinalidad. No obstante la completez de la lógica de predicados fue originalmente demostrada por Kurt Gödel en su tesis doctoral de 1930 con un argumento distinto al presentado aquí. La conlusión es la misma en ambos casos:

Teorema II.28 (de completez de Gödel)
Sea $\mathcal{L}$ un lenguaje predicativo, entonces para $\varphi \in \mathcal{L}$ y $\Gamma \subseteq \mathcal{L}$ se cumple que:

$$\text{Si } \Gamma \models \varphi, \text{ entonces } \Gamma \vdash \varphi$$

La prueba de este resultado es análoga a su contraparte proposicional y, similarmente, tanto el uso de parejas de estructuras y asignaciones como la obtención de derivaciones en $\mathcal{K}$ son métodos equivalentes para decidir si una *wff* es consecuencia de un conjunto de premisas o no. Además como consecuencias a todo lo dicho en esta sección se tienen las siguientes:

Propiedades II.29 (Propiedades de la lógica predicativa)
Para un lenguaje predicativo $\mathcal{L}$ y su sistema formal $\mathcal{K}$ correspondiente, se cumple que:

- La teoría matemática de $\mathcal{K}$ coincide con el conjunto de *wffs* lógicamente válidas.
- La teoría matemática generada por $\mathcal{K}$ es sintácticamente consistente.

Con esto concluye la sección de lógica predicativa. Algunos resultados concernientes a modelos serán demostrados en los siguientes capítulos debido a que en los sistemas axiomáticos es donde se ve mayormente las aplicaciones de dichos resultados y todo lo visto hasta ahora.

Capítulo 3

Fundamentos en la Teoría de Conjuntos

Hasta ahora se ha visto que el razonamiento lógico clásico se puede formalizar de manera fidedigna en algún sistema formal $\mathscr{F}$. Con base en esto es posible que se desee ampliar el alcance de dicha formalización. Esto es, si la lógica puede representarse sintácticamente ¿qué impide que pueda hacerse lo mismo con las matemáticas, la física o incluso el lenguaje natural? Cabe señalar que, con ayuda de las computadoras, diversos proyectos han formalizado gran parte de las matemáticas utilizando algún sistema formal específico. Más aun, en 1994 se publicó el *manifiesto QED* que proponía "tener una única base de datos estrictamente formalizada, computarizada y accesible, de todo el conocimiento matemático establecido, con las demostraciones verificadas por computadora" [B$^+$, Mizar]. No obstante, hasta la fecha este objetivo no ha sido alcanzado.

El proceso de formalización de las matemáticas puede efectuarse de distintas maneras. Una de éstas consiste en seleccionar una teoría base "lo suficientemente grande" como para englobar al resto de las teorías matemáticas. Una de las más populares para efectuar dicho proceso es la *Teoría de Conjuntos* que bajo la consigna "todo es un conjunto" y le relación binaria "$\in$" (épsilon)[1] de pertenencia es capaz de definir, virtualmente, todos los conceptos matemáticos y desarrollar el resto de la matemática. En los siguientes capítulos, se presentará evidencia en favor de que la formalización de (una parte considerable de) las matemáticas es posible y además se puede hacer de más de una manera; al mismo tiempo se explicará la motivación detrás de los sistemas elegidos para dicho fin. Particularmente, en la siguiente sección se presentará de manera informal cómo se podría llevar a cabo dicho proceso en la teoría de conjuntos a la vez que se explica la ontología de esta rama de las matemáticas.

[1] Inicialmente Giuseppe Peano presentó esta relación por medio de la letra griega épsilon "ε" para representar el verbo "est" (ser/estar). Por ejemplo $x \varepsilon \mathbb{N}$, significaría "x es un natural". Probablemente por el uso de otra variante de la letra griega épsilon, a decir "ϵ", el símbolo derivó en el hoy más utilizado "$\in$".

I. Teoría Informal de Conjuntos

Históricamente, el primer tratado de teoría de conjuntos fue desarrollado a finales del siglo XIX por Georg Cantor. Sin ahondar mucho en detalles, él estaba estudiando propiedades de la recta real, las cuales lo llevaron a estudiar "colecciones" de números reales y el "tamaño" de estas colecciones. El concepto de *colección* es central para desarrollar una primera intuición respecto a lo que es un conjunto. En términos de Ernst Zermelo, "dada cualquier propiedad *bien definida*, es posible construir el conjunto de todos los objetos que cumplen dicha propiedad." Así, si la propiedad "ser un número par" está bien definida, uno tiene permitido pensar en el conjunto (la colección) de todos los números pares. A esta regla de formación de conjuntos comúnmente se le denomina *principio de comprensión* y es el primer punto que se debe tener en consideración para estudiarlos y usarlos.

Otro atributo importante de los conjuntos es su *extensión* que informalmente uno puede pensar como el "listado" de los objetos que el conjunto contiene. Si dos conjuntos tienen la misma extensión, entonces se puede determinar que son iguales. Por ejemplo, el conjunto de "los primeros cinco enteros no negativos" y el conjunto de "los enteros mayores o iguales que cero y menores o iguales a cuatro" tienen la misma extensión (los números cero, uno, dos, tres y cuatro) y, por lo tanto, son el mismo conjunto.

La notación para construir conjuntos ya es conocida. Se escribe $\{x \mid P(x)\}$ para denotar al conjunto de todos los objetos que cumplen la propiedad P. Si el conjunto es finito éste se puede denotar por medio de su extensión:

$$\{z \mid z \text{ es un entero positivo par menor que } 10\} = \{2, 4, 6, 8\}$$

Se pueden utilizar puntos suspensivos en la extensión si el conjunto es discreto, infinito y el lector puede inferir el resto de los elementos:

$$\{n \mid n \text{ es entero positivo}\} = \{1, 2, 3, 4, 5, \dots\}$$

Por extensionalidad, el orden en que se presenten los objetos que contiene un conjunto será irrelevante para determinar las propiedades del conjunto. Similarmente, también será irrelevante si hay instancias repetidas de un mismo objeto en la extensión. Es decir, el conjunto representado por $\{a, b, c\}$ es el mismo que el denotado por $\{b, a, c\}$ y también es el mismo que $\{c, b, b, b, a\}$.

A los objetos "dentro" de un conjunto se les llama *elementos* y éstos se relacionan con los conjuntos por medio de la relación de *pertenencia* "$\in$". Así, para expresar que "a es un elemento del conjunto $\{a, b, c\}$" o, equivalentemente, que "a pertenece a $\{a, b, c\}$", se escribe $a \in \{a, b, c\}$. La negación de esta relación se denota por "$\notin$".

Además de la relación de pertenencia, se tiene otra relación entre conjuntos, la de contención "$\subseteq$". Se dice que un conjunto A está contenido en otro B, o que A

es subconjunto de B, si todo elemento de A es un elemento de B. Esto es, $A \subseteq B$ si y sólo si $x \in A$, entonces $x \in B$. Similarmente, la negación de esta relación se simboliza por "$\not\subseteq$". Como consecuencia de esto, el principio de extensionalidad de conjuntos se puede reformular de la siguiente manera: "dos conjuntos A y B son iguales, i.e. $A = B$, si $A \subseteq B$ y $B \subseteq A$".

En vez de usar una propiedad P para describir a un conjunto se puede utilizar un funcional f para hacer explícita la forma de los objetos en el conjunto. Esto es, $\{f(x) \mid x \in A\}$ representa a todos los objetos con la forma $f(x)$ siendo x un "índice" que corre sobre todos los elementos de A. Por ejemplo, el conjunto denotado por $\{n+n \mid n \in \{1,2,3\}\}$ es el mismo que $\{2,4,6\}$. También es posible "combinar" ambas formas: $\{f(x) \mid P(x)\}$. Es decir, denotar el conjunto de todos los objetos de la forma $f(x)$ tales que x cumple la propiedad P. No obstante, obsérvese que todas estas formas se derivan del principio de comprensión pues:

$$\{f(x) \mid P(x)\} = \{f(x) \mid x \in \{y \mid P(y)\}\} \quad \text{y} \quad \{f(x) \mid x \in A\} = \{y \mid \exists x[x \in A \wedge y = f(x)]\}$$

Ya que una "propiedad bien definida" P es una aseveración acerca de algún objeto x (x cumple P o x no cumple P), es posible operar con éstas como con las proposiciones. Así, si se tienen dos conjuntos A y B, por el principio de comprensión, uno puede pensar en el conjunto de todos los objetos que o están en A o están en B, i.e. $\{x \mid x \in A \vee x \in B\}$. A este conjunto se le denota por $A \cup B$ y se le llama la *unión de A y B* debido a que tiene a todos los elementos de A y a los de B también. Más aún, obsérvese que si $A = \{x \mid \alpha(x)\}$ y $B = \{y \mid \beta(y)\}$, entonces $A \cup B = \{z \mid \alpha(z) \vee \beta(z)\}$.

Análogamente, uno tiene permitido pensar en el conjunto de todos los objetos que están en A y en B al mismo tiempo, es decir, su *intersección*, la cual es denotada por $A \cap B$. Utilizando las mismas notaciones del párrafo anterior: $A \cap B = \{x \mid x \in A \wedge x \in B\} = \{x \mid \alpha(x) \wedge \beta(x)\}$.

En matemáticas también es importante el uso de "tuplas", "n-adas" o "sucesiones finitas" $\langle x_1, x_2, \ldots, x_n\rangle$; esto es, agrupaciones de objetos en las cuales el orden sí cuenta. Por ejemplo la pareja ordenada de letras $\langle a, b\rangle$ es distinta de la pareja ordenada $\langle b, a\rangle$. Con el principio de comprensión uno puede construir conjuntos cuyos elementos sean estas parejas. Más específicamente si A y B son conjuntos, existe su *producto cartesiano* $A \times B$ y es el conjunto de las parejas $\langle a, b\rangle$ tales que $a \in A$ y $b \in B$, i.e. $A \times B = \{\langle a, b\rangle \mid a \in A \wedge b \in B\}$.

De manera similar es posible "restar" dos conjuntos, A y B, al construir al conjunto de todos los objetos en A que no están en B, i.e. $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$. Además obsérvese que si $A = \{x \mid \alpha(x)\}$ y $B = \{y \mid \beta(y)\}$, entonces la *diferencia de conjuntos* es $A \setminus B = \{x \mid \alpha(x) \wedge \neg\beta(x)\}$. Más aún, suponiendo que U es un *supraconjunto* de A, es decir, que $A \subseteq U$, es factible concebir a U como un "universo" o un "todo" y, en consecuencia, A sería una fracción de ese total. En dichos casos, la *diferencia conjuntista* es también llamada *toma de complementos*, y el conjunto de todos los objetos en U que no están en A se denota A^c y es referido como el *complemento de* A. Más precisamente $A^c = U \setminus A = \{x \mid x \in U \wedge x \notin A\}$.

Directamente del principio de comprensión uno puede construir el *conjunto vacío* $\emptyset$, o sea, el conjunto que no tiene elementos. Para esto uno no necesita dar más que una contradicción "$P(x) \wedge \neg P(x)$" como la propiedad "bien definida" requerida por el principio. Es decir, $\emptyset = \{x \mid P(x) \wedge \neg P(x)\}$, pues no hay ningún objeto existente que cumpla una contradicción de acuerdo a la lógica clásica. Nótese también que se habla del conjunto vacío (y no de "un conjunto vacío") por el principio de extensionalidad, ya que la falta de elementos es una misma extensión sin importar la contradicción utilizada para generar al vacío, i.e. $\emptyset = \{x \mid P(x) \wedge \neg P(x)\} = \{x \mid \neg(Q(x) \Rightarrow Q(x))\} = \{x \mid \bot\}$.

Dualmente, en vez de utilizar contradicciones se pueden emplear tautologías para aplicar el principio de comprensión y formar al *conjunto universal*, es decir, el conjunto $V = \{x \mid \top\} = \{x \mid x = x\} = \{x \mid P(x) \Rightarrow P(x)\}$ que tiene cualquier objeto en su interior, pues todos satisfacen la tautología. Es aquí en donde empiezan a surgir complicaciones en la teoría que se está desarrollando. Por ejemplo, otra propiedad "bien definida" es la relación de "ser subconjunto" $\subseteq$. Así, uno tiene permitido concebir "el conjunto $\mathcal{P}(A)$ de todos los subconjuntos del conjunto A", llamado el *conjunto potencia de* A, i.e. $\mathcal{P}(A) = \{X \mid X \subseteq A\}$. Es un teorema, demostrado por el mismo Cantor, que el conjunto potencia de cualquier conjunto X tiene "mayor tamaño" que el conjunto X original. Aplicando esta observación al conjunto universal, V, su potencia $\mathcal{P}(V)$ debería tener mayor tamaño que el mismo V. Pero ¿cómo es esto posible si V ya contiene a todas las cosas, incluyendo a todos los elementos de $\mathcal{P}(V)$?

Lo dicho en el párrafo anterior se formaliza por medio del concepto de *cardinalidad* de conjuntos. Se le llama cardinalidad al "tamaño" de un conjunto y éstas pueden cumplir una relación de órden "$\leq$". Así, que el conjunto A tenga menor cardinalidad que el conjunto B, se representa simbólicamente por "$|A| < |B|$". Cantor probó que para cualesquiera dos conjuntos, A y B:

- Si $A \subseteq B$, entonces $|A| \leq |B|$.
- $|A| < |\mathcal{P}(A)|$.

De esta manera, se tendría que $|\mathcal{P}(V)| \leq |V| < |\mathcal{P}(V)|$, lo cual, por propiedad de órdenes, implicaría que $|\mathcal{P}(V)| \neq |\mathcal{P}(V)|$, que claremente es una contradicción.

Es bien sabido que si uno llega a una contradicción mediante un razonamiento lógico válido, se debe a que las hipótesis utilizadas son contradictorias. En el presente caso el error estuvo en el *principio de comprensión* pues el concepto de "propiedad bien definida" precisamente no está bien definido. Bertrand Russell hizo explícito ésto al construir también su propia paradoja en la teoría de conjuntos. El argumento que él dio lo hizo para el sistema formal desarrollado por

Gottlob Frege en su *Begriffsschrift* de 1879 (una lógica predicativa de segundo orden)[2] y es rápidamente trasladable a lo desarrollado en esta sección. Considérese al conjunto $R = \{x \mid x \notin x\}$. Como ejemplo de un objeto que no está en R se puede tomar a V, pues $V \in V$. Es válido también preguntarse si $R \in R$. El argumento procede como a continuación:

- Si $R \in R$, entonces R cumple la propiedad especificada por R, es decir, $R \notin R$. De aquí que $(R \in R) \wedge (R \notin R)$, una contradicción.
- Por otro lado, si $R \notin R$, entonces R cumple la propiedad especificada por R. Por el principio de comprensión $R \in R$. Nuevamente se tiene la contradicción $(R \in R) \wedge (R \notin R)$.

Todo esto motivó un programa de formalización de la teoría de conjuntos bajo unos axiomas que la hiciesen consistente. En la siguiente sección se presenta el sistema formal más popular en el cual se lleva a cabo dicho objetivo.

II. Teoría Formal de Conjuntos

Para la formalización se utilizará un lenguaje formal predicativo (de primer orden) $\mathcal{L}$ que en su signatura (los símbolos no-lógicos) sólo tiene un símbolo predicativo de aridad dos distinto de la igualdad, i.e. $\Sigma = \mathcal{P}_2 = \{=, \in\}$.[3] Se adoptarán los mismos axiomas utilizados en el capítulo anterior al igual que las mismas reglas de inferencia. A éstos se les denominará *axiomas lógicos* mientras que los agregados en esta sección serán llamados *axiomas no-lógicos*. El primero de éstos es una formalización del *principio de extensionalidad* mencionado en la sección anterior:

Definición II.1 (Axioma de extensionalidad)
El *axioma de extensionalidad* es la *wff*:

$$\forall x \forall y [\forall z [z \in x \Leftrightarrow z \in y] \Rightarrow x = y]$$

Una vez presentado el lenguaje y dado el primer axioma, algunas aclaraciones pueden ser necesarias. Al momento de formalizar algún conocimiento en un lenguaje predicativo uno debe renunciar a explicar qué significan ciertas cosas dentro de la teoría. Si uno tratase de definir todo lo expuesto, cada concepto requeriría otras nociones que a su vez requerirían de más definiciones, entrando

[2] Una lógica predicativa de segundo órden se genera cuando se separa el conjunto de variables VAR del lenguaje predicativo $\mathcal{L}$ en dos: aquéllas que serán σ-asignadas a los elementos del dominio de discurso $d \in \mathcal{D}$, y aquéllas que serán asignadas a los predicados monádicos (predicados de aridad 1) definibles en $\mathcal{D}$, i.e. $P \subseteq \mathcal{D}$. Así, las lógicas predicativas estudiadas en el capítulo anterior fueron todas lógicas predicativas de primer orden, pues las variables eran todas asignadas sólo a elementos de algún dominio de discurso.

[3] Nótese que, de acuerdo al abuso de lenguaje ocupado en otros textos, al presentar *el lenguaje de la teoría de conjuntos* varios autores expresan lo dicho anteriormente mediante oraciones similares a la siguiente: "llamaremos $\mathcal{L} = \{\in\}$ al lenguaje de la teoría de conjuntos". Pues equiparan lenguaje con signatura y consideran a la igualdad un símbolo lógico.

así en una regresión infinita. Esto se soluciona dejando algunos conceptos, denominados *primitivos*, sin definir, que en el caso de una teoría de conjuntos clásica son dos: las nociones de conjunto y pertenencia. Así, la relación $\in$ y el universo de todos los conjuntos V nunca serán explicitados y, por ende, al momento de presentar modelos para la teoría que se está construyendo diferentes interpretaciones podrán ser dadas a ellos.

En el párrafo anterior se habló de la posibilidad de definir relaciones (como la de pertenencia) dentro de la teoría, no obstante, no se ha dicho cómo podría llevarse a cabo dicho proceso. Considérese por ejemplo la relación de ser subconjunto "$\subseteq$". Su respectivo símbolo no está en la signatura del lenguaje de la teoría de conjuntos por lo que hipotéticamente no podría utilizarse; pero aun así, por lo dicho en la sección pasada, se sabe que $x \subseteq y \equiv \forall z[z \in x \Rightarrow z \in y]$. Para ésto se tienen dos soluciones:

- Añadir un nuevo símbolo predicativo $P \in \mathcal{P}_n$ a la signatura Σ de $\mathcal{L}$ por cada nueva relación n-ádica definida en la teoría. Además habría que agregar un axioma de la forma $P(x_1, \ldots, x_n) \Leftrightarrow \varphi$ al aparato deductivo, siendo φ la *wff* que "define" lo que significa el nuevo símbolo. En el caso de la contención de conjuntos, se debería agregar a $\mathcal{P}_2$ el símbolo "$\subseteq$" al mismo tiempo que se agrega el axioma:
$$x \subseteq y \Leftrightarrow \forall z[z \in x \Rightarrow z \in y]$$
- Pensar en las definiciones de relaciones como *meta-abreviaciones de wffs*, tal y como se hizo con los conectivos "$\wedge, \vee, \Leftrightarrow$" y el cuantificador "$\exists$" en el capítulo anterior.

El segundo enfoque es más sencillo, pues se está trabajando en la meta-teoría y no es necesario demostrar, como en el primreo, que las modificaciones al lenguaje y los axiomas no afectan la teoría matemática resultante. Dicha solución es la que se adoptará momentáneamente mientras no se presentan otro tipo de definiciones dadas comúnmente en matemáticas. Más adelante se enunciará un teorema que justificará el primer enfoque y permitirá formalizar lo que probablemente pueda sentirse como un argumento de fe, es decir, confiar en que siempre se pueden "des-abreviar" las meta-cadenas para tener las *wffs* dadas en $\mathcal{L}$.

Mientras tanto, se puede probar con lo dicho hasta ahora que "la relación de contención de conjuntos es una relación de órden parcial":

Propiedades II.1 (de la contención de conjuntos)
Son teoremas de una teoría de conjuntos con axioma de extensionalidad las siguientes tres "*wffs*":

- $\forall x[x \subseteq x]$.
- $\forall x \forall y \forall z[x \subseteq y \wedge y \subseteq z \Rightarrow x \subseteq z]$.
- $\forall x \forall y[x \subseteq y \wedge y \subseteq x \Rightarrow x = y]$.

Demostración. Las demostraciones se hacen formalmente:

1.	$z \in x \Rightarrow z \in x$	ID
2.	$\forall z[z \in x \Rightarrow z \in x]$	Gen(1)
3.	$x \subseteq x$	Def.$\subseteq$
$\therefore$	$\forall x[x \subseteq x]$	Gen(3)

1.	$x \subseteq y \wedge y \subseteq z$	Hip.
2.	$x \subseteq y$	$\wedge$Elim1(1)
3.	$y \subseteq z$	$\wedge$Elim2(1)
4.	$\forall u[u \in x \Rightarrow u \in y]$	Def.$\subseteq$(2)
5.	$\forall v[v \in y \Rightarrow v \in z]$	Def.$\subseteq$(3)
6.	$w \in x$	Hip.
7.	$w \in x \Rightarrow w \in y$	ReglaA4(4)
8.	$w \in y$	MP(6,7)
9.	$w \in y \Rightarrow w \in z$	ReglaA4(5)
10.	$w \in z$	MP(6,7)
11.	$w \in x \vdash w \in z$	Resumen(6-10)
12.	$\vdash w \in x \Rightarrow w \in z$	CP(11)
13.	$\forall w[w \in x \Rightarrow w \in z]$	Gen(12)
14.	$x \subseteq z$	Def.$\subseteq$(13)
15.	$x \subseteq y \wedge y \subseteq z \vdash x \subseteq z$	Resumen(1-15)
16.	$\vdash x \subseteq y \wedge y \subseteq z \Rightarrow x \subseteq z$	CP(15)
$\therefore$	$\forall x \forall y \forall z[x \subseteq y \wedge y \subseteq z \Rightarrow x \subseteq z]$	Gen(16)x3

1.	$x \subseteq y \wedge y \subseteq x$	Hip.
2.	$x \subseteq y$	$\wedge$Elim1(1)
3.	$y \subseteq x$	$\wedge$Elim2(1)
4.	$\forall u[u \in x \Rightarrow u \in y]$	Def.$\subseteq$(2)
5.	$\forall v[v \in y \Rightarrow v \in x]$	Def.$\subseteq$(3)
6.	$w \in x \Rightarrow w \in y$	ReglaA4(4)
7.	$w \in y \Rightarrow w \in x$	ReglaA4(5)
8.	$w \in x \Leftrightarrow w \in y$	$\Leftrightarrow$Intro(6,7)
9.	$\forall x \forall y[\forall w[w \in x \Leftrightarrow w \in y] \Rightarrow x = y]$	Extensionalidad
10.	$\forall w[w \in x \Leftrightarrow w \in y] \Rightarrow x = y$	ReglaA4(9)x2
11.	$\forall w[w \in x \Leftrightarrow w \in y]$	Gen(8)
12.	$x = y$	MP(11,10)
13.	$x \subseteq y \wedge y \subseteq x \vdash x = y$	Resumen(1-12)
14.	$\vdash x \subseteq y \wedge y \subseteq x \Rightarrow x = y$	CP(13)
$\therefore$	$\forall x \forall y[x \subseteq y \wedge y \subseteq x \Rightarrow x = y]$	Gen(14)x2

■

Ya se ha visto que si se agrega el *principio de comprensión* a la teoría que se está construyendo se generarán paradojas. Para evitarlas sólo se requiere una ligera modificación a dicho principio, la cual consiste en admitir la construcción de "subconjuntos" de conjuntos ya existentes, más no una construcción descontrolada. Es decir, en vez de formar el conjunto de todos los objetos que cumplen la propiedad P; i.e. $\{x \mid P(x)\}$, dado un conjunto X, se podrá formar el conjunto de todos los elementos de X que cumplen la propiedad, i.e. $\{x \in X \mid P(x)\}$. Esto no traslada la paradoja de Russell al "universo alternativo" X, como se puede ver en el siguiente argumento: Sea $R = \{x \in X \mid x \notin x\}$ entonces es válido preguntarse si $R \in R$:

- Si $R \in R$, entonces R cumple lo especificado por R, es decir que $R \in X$ y $R \notin R$. De aquí se desprende la ya conocida contradicción $(R \in R) \wedge (R \notin R)$.

- Si $R \notin R$, entonces R no cumple lo especificado por R, es decir, ó $R \notin X$ ó $R \in R$. Como la segunda no puede ocurrir, porque generaría la contradicción, sólo resta concluir que $R \notin X$. Por lo tanto, $R \notin R$ y además $R \notin X$.

Por cómo se modificó el mecanismo de construcción de conjuntos, esta nueva forma de hacerlos es llamada *principio de comprensión restringida, axioma de subconjuntos, axioma de especificación o axioma de separación.* Para hacerlo estrictamente un axioma, es necesario clarificar qué es una propiedad "bien definida". Como se vio anteriormente, toda *wff* puede sustituirse por un nuevo predicado cuya aridad sea mayor (o igual) a la cantidad de variables libres en la *wff*. Por eso no es sorpresa que se escoja utilizar *wffs* en vez de "propiedades bien definidas". Es decir la formalización del *principio de comprensión restringida* es:

Definición II.2 (Esquema de Axioma de Especificación)
Dada una *wff* $\varphi \in \mathcal{L}$ cuyas variables libres estén entre $x, w_1, \ldots, w_n, z$, siendo n un entero no-negativo, la siguiente *wff* es un axioma de la teoría de conjuntos:

$$\forall w_1 \ldots \forall w_n \forall z \exists y \forall x[x \in y \Leftrightarrow x \in z \wedge \varphi]$$

El enunciado anterior es un *esquema de axioma* porque proporciona un axioma por cada *wff* de $\mathcal{L}$. Ernst Zermelo fue quien introdujo esta modificación al *principio de comprensión* de Frege. Posteriormente se agregará otro esquema que permitirá derivar el recientemente presentado; pero por el momento el esfuerzo será dirigido a ver las consecuencias del recientemente expuesto:

Teorema II.2 (Existe un conjunto que no tiene elementos)
Es teorema de una teoría con esquema de axioma de especificación la *wff*:

$$\exists y \forall x[\neg(x \in y)]$$

Demostración. El argumento procede de la siguiente manera:

1.	Si φ es una sentencia de $\mathcal{L}$, entonces $\psi := (\varphi \wedge \neg\varphi) \in \mathcal{L}$	DefiniciónTemporal
2.	$\gamma := x \in z \wedge \psi$	DefiniciónTemporal
3.	$\forall z \exists y \forall x[x \in y \Leftrightarrow \gamma]$	Especificación(1)
4.	$\exists y \forall x[x \in y \Leftrightarrow \gamma]$	ReglaA4(3)
5.	$\gamma \Leftrightarrow \psi$	Inst.Tautol.
6.	$[\psi/\gamma](\exists y \forall x[x \in y \Leftrightarrow \gamma]) \Leftrightarrow [\psi/\psi](\exists y \forall x[x \in y \Leftrightarrow \gamma])$	Teo.Sust.(4,5)
7.	$\exists y \forall x[x \in y \Leftrightarrow \psi] \Leftrightarrow \exists y \forall x[x \in y \Leftrightarrow \gamma]$	Def.$[\psi/\gamma]$
8.	$\exists y \forall x[x \in y \Leftrightarrow \gamma] \Rightarrow \exists y \forall x[x \in y \Leftrightarrow \psi]$	$\Leftrightarrow$-Elim2
9.	$\xi := (x \in y \Leftrightarrow \psi)$	DefiniciónTemporal
10.	$\exists y \forall x[\xi]$	MP(4,8)
11.	$\xi \Leftrightarrow \neg(x \in y)$	Teorema Lógico
12.	$[\neg(x \in y)/\xi](\exists y \forall x[\xi]) \Leftrightarrow [\xi/\xi](\exists y \forall x[\xi])$	Teo.Sust.(10,11)
13.	$\exists y \forall x[\neg(x \in y)] \Leftrightarrow \exists y \forall x[\xi]$	Def.$[\neg(x \in y)/\xi]$
14.	$\exists y \forall x[\xi] \Rightarrow \exists y \forall x[\neg(x \in y)]$	$\Leftrightarrow$-Elim2
$\therefore$	$\exists y \forall x[\neg(x \in y)]$	MP(10,14)

■

Esto significa que existe al menos *un conjunto vacío*. Para poder hablar del *único conjunto vacío* $\emptyset$, será necesario comprobar su *unicidad*. Es bien sabido que para probar que sólo hay un objeto que cumpla una propiedad, se debe suponer que la propiedad es válida para dos variables y probar, a partir de ésto, que el objeto que designan dichas variables es el mismo. En particular esto será válido para cualquier construcción de la forma $\{x \in z \mid \varphi(x)\}$:

Lema II.3 (El conjunto del que habla especificación es único)
Es teorema de una teoría con axioma de extensionalidad la siguiente *wff*:

$$\forall z \forall y \forall w[\forall x[x \in y \Leftrightarrow x \in z \wedge \varphi] \wedge \forall x[x \in w \Leftrightarrow x \in z \wedge \varphi] \Rightarrow y = w]$$

Siendo φ una *wff* con variables libres entre $x, w_1, \ldots, w_n, z$.

Demostración. Se tiene que:

1.	$\forall x[x \in y \Leftrightarrow x \in z \wedge \varphi] \wedge \forall x[x \in w \Leftrightarrow x \in z \wedge \varphi]$	Hip.
2.	$\forall x[x \in y \Leftrightarrow x \in z \wedge \varphi]$	$\wedge$Elim1(1)
3.	$\forall x[x \in w \Leftrightarrow x \in z \wedge \varphi]$	$\wedge$Elim2(1)
4.	$x \in y \Leftrightarrow x \in z \wedge \varphi$	ReglaA4(2)
5.	$x \in w \Leftrightarrow x \in z \wedge \varphi$	ReglaA4(3)
6.	$x \in y \Leftrightarrow x \in w$	$\Leftrightarrow$Transitiv(4,5)
7.	$\forall y \forall w[\forall x[x \in y \Leftrightarrow x \in w] \Rightarrow y = w]$	Extensionalidad
8.	$\forall x[x \in y \Leftrightarrow x \in w]$	Gen(6)
9.	$\forall x[x \in w \Leftrightarrow x \in y] \Rightarrow y = w$	ReglaA4(7)x2
10.	$y = w$	MP(8,9)
11.	$\forall x[x \in y \Leftrightarrow x \in z \wedge \varphi] \wedge \forall x[x \in w \Leftrightarrow x \in z \wedge \varphi] \vdash y = w$	Resumen(1-10)
12.	$\vdash \forall x[x \in y \Leftrightarrow x \in z \wedge \varphi] \wedge \forall x[x \in w \Leftrightarrow x \in z \wedge \varphi] \Rightarrow y = w$	CP(11)
$\therefore$	$\forall z \forall y \forall w[\forall x[x \in y \Leftrightarrow x \in z \wedge \varphi] \wedge \forall x[x \in w \Leftrightarrow x \in z \wedge \varphi] \Rightarrow y = w]$	Gen(12)x3

■

Son comunes en matemáticas las demostraciones de existencia y unicidad de algún objeto. Por dicha razón frecuentemente se presenta la instancia de fórmula "$\exists! x[\varphi]$" con $x \in FV(\varphi)$ como abreviación de $\exists x[\varphi] \wedge \forall y \forall w[[y/x](\varphi) \wedge [w/x](\varphi) \Rightarrow y = w]$. Este es el enfoque que se utilizará también en el presente texto.

Una vez que se ha probado (1) *la existencia* y (2) *la unicidad* del conjunto vacío, se tiene permitido "definirlo". Es decir, un libro de texto estándar de matemáticas procedería en este caso a decir algo como: "$\emptyset$ denotará al conjunto vacío". Sin embargo, esto requeriría aumentar los símbolos funcionales $\mathcal{F}$ de la signatura Σ de $\mathcal{L}$. Para sortear estos últimos obstáculos formales, se dan las siguientes definiciones y teoremas:

Definición II.3 (Definición de un símbolo en un lenguaje)
Sean $\Sigma \subseteq \Sigma'$ dos signaturas cuyos lenguajes predicativos (de primer orden) correspondientes son $\mathcal{L} \subseteq \mathcal{L}'$ respectivamente.

- Dado $P \in (\Sigma' \setminus \Sigma) \cap \mathcal{P}_n$, se dice que δ_P *es definición de P (en $\mathcal{L}'$)* sii existe $\varphi_P \in \mathcal{L}$ con $FV(\varphi_P) \subseteq \{w_1, \ldots, w_n\}$ tal que:

$$\delta_P := \forall z_1 \ldots \forall z_n [P(z_1, \ldots, z_n) \Leftrightarrow [z_n/w_n] \cdots [z_1/w_1](\varphi_P)]$$

- Dado $f \in (\Sigma' \setminus \Sigma) \cap \mathcal{F}_n$, se dice que δ_f *es definición de f (en $\mathcal{L}'$)* sii existe $\varphi_f \in \mathcal{L}$ con $FV(\varphi_f) \subseteq \{w_1, \ldots, w_n, w_{n+1}\}$ tal que:

$$\delta_f := \forall z_1 \ldots \forall z_n [[f(z_1, \ldots, z_n)/w_{n+1}][z_n/w_n] \cdots [z_1/w_1](\varphi_f)]$$

Definición II.4 (Extensión por definiciones de una teoría)
Sean $\Sigma \subseteq \Sigma'$ dos signaturas cuyos lenguajes predicativos (de primer orden) correspondientes son $\mathcal{L} \subseteq \mathcal{L}'$ respectivamente. Para cada $s \in (\Sigma' \setminus \Sigma)$, denótese δ_s a una definición de s (en $\mathcal{L}'$) siendo testigo de esto la fórmula bien formada de $\mathcal{L}$, φ_s. Dadas dos teorías $\Gamma \subseteq \mathcal{L}$ y $\Gamma' \subseteq \mathcal{L}'$, se dice que Γ' *es extensión por definiciones de* Γ sii:

- $\Gamma' = \Gamma \cup \{\delta_s \mid s \in (\Sigma' \setminus \Sigma)\}$
- Para cada símbolo funcional n-ario $f \in (\Sigma' \setminus \Sigma)$ se cumple que:

$$\Gamma \vdash \forall z_1 \ldots \forall z_n \exists! y [[y/w_{n+1}][z_n/w_n] \cdots [z_1/w_1](\varphi_f)]$$

  Con $FV(\varphi_f) \subseteq \{w_1, \ldots, w_n, w_{n+1}\}$.

El lector no debe confundirse por las sustituciones presentadas en las definiciones anteriores: Se sabe que escribir $\varphi(w_1, \ldots, w_n)$, con la notación usada en la sección de teoría informal de conjuntos, significa que los objetos designados por $w_1, \ldots, w_n$ se comportan de acuerdo a lo que dice φ. Así, la *wff* $[z_n/w_n] \cdots [z_1/w_1](\varphi_P)$ es la notación formal para su análogo informal $\varphi(z_1, \ldots, z_n)$ y así δ_P está diciendo que $P(z_1, \ldots, z_n) \Leftrightarrow \varphi(z_1, \ldots, z_n)$, esto es, que $z_1, \ldots, z_n$ cumplirán que P si y sólo si $\varphi(z_1, \ldots, z_n)$. De igual manera, δ_f afirma que el objeto designado por $f(z_1, \ldots, z_n)$ cumple lo que dice φ (junto con $z_1, \ldots, z_n$), que en notación informal se representaría por $\varphi(z_1, \ldots, z_n, f(z_1, \ldots, z_n))$. Similarmente, la segunda condición en la definición anterior, i.e. $\Gamma \vdash \forall z_1 \ldots \forall z_{n-1} \exists! y[[y/w_{n+1}][z_n/w_n] \cdots [z_1/w_1](\varphi_f)]$ para $f \in (\Sigma' \setminus \Sigma)$, informalmente está diciendo que a partir de Γ debe ser demostrable que exista un único y que cumpla la "propiedad" φ, i.e. $\varphi(z_1, \ldots, z_n, y)$. Dicha unicidad, como ya se mencionó previamente, es un requisito cotidiano en matemáticas. Finalmente, se utilizaron clausuras universales ($\forall z_1 \ldots \forall z_n$) para formar sentencias debido a que se desea que la relación de satisfactibilidad $\models$ dependa sólo de la estructura $\mathfrak{A} = \langle \mathcal{D}, \Sigma', \mathcal{I} \rangle$ y no de la asignación $\sigma : VAR \to \mathcal{D}$.

Ejemplo II.1 Se aclarará lo recientemente dicho con las definiciones de contención de conjuntos $\subseteq$ y el conjunto vacío $\emptyset$. En este caso originalmente la signatura es $\Sigma = \langle \in, = \rangle$, por lo que $\Sigma' := \langle \emptyset; \in, =, \subseteq \rangle$. Defínase $\varphi_{\subseteq} := \forall z[z \in x_1 \Rightarrow z \in x_2]$, entonces la definición de "$\subseteq$" es la sentencia $\delta_{\subseteq} := \forall x \forall y[x \subseteq y \Leftrightarrow \forall z[z \in x \Rightarrow z \in y]]$. Similarmente, se sabe que es teorema de una teoría con extensionalidad y especificación que $\exists! y \forall x[\neg(x \in y)]$. Tomando a $\varphi_\emptyset$ como $\forall x[\neg(x \in y)]$, la sentencia $\delta_\emptyset := \forall x[\neg(x \in \emptyset)]$ es una definición de $\emptyset$. De esta manera, cuando se afirme algo en $\mathcal{L}'$ como $\forall x[x \in \emptyset \Rightarrow x \subseteq \emptyset]$, se espera que esto se pueda reformular en $\mathcal{L}$ mediante $\exists y[\forall x[\neg(x \in y)] \land \forall x[x \in y \Rightarrow \forall z[z \in x \Rightarrow z \in y]]]$.

Ahora sólo se debe verificar que *extender por definiciones* "no afecta" la teoría matemática generada por el conjunto original. Esto quiere decir que no importa qué teorema φ' se obtenga a partir de la extensión por definiciones $\Gamma' \subseteq \mathcal{L}'$ de $\Gamma \subseteq \mathcal{L}$, debe existir un teorema φ a partir de Γ que sea lógicamente equivalente al derivado por Γ'. No obstante, probar este resultado es tedioso ya que los casos a considerar son diversos y no es obvio determinar cómo abordarlos con suficiente generalidad pero con la rigurosidad necesaria para incluirlos a todos. Por dicha razón se da el siguiente par de ejemplos que dan una idea del algoritmo necesario para efectuar la prueba:

Ejemplo II.2 En los siguientes ejemplos Σ' representa una signatura que es resultado de añadir a otra, Σ, nuevos símbolos. En dado caso $\mathcal{L}'$ representará el lenguaje generado por Σ' mientras que $\mathcal{L}$, el generado por Σ:

1. Sean $\Sigma := \langle \in, = \rangle$ y $\Sigma' := \langle \emptyset, \{-\}; \in, =, \leq \rangle$ y supóngase que φ' es una *wff* de $\mathcal{L}'$ tal que $\varphi' := \emptyset \leq \{\emptyset\}$. Para obtener la *wff* correspondiente, $\varphi \in \mathcal{L}$, es recomendable convertir a φ' a su forma polaca, i.e. "$\leq \emptyset\{-\}\emptyset$". Después se debe asignar a cada nuevo símbolo funcional (de derecha a izquierda recorriendo la fórmula en su forma polaca) una nueva variable, en este caso: $\emptyset \mapsto y_1, \{-\} \mapsto y_2, \emptyset \mapsto y_3$. Con esto en mente, únicamente se debe hacer una aseveración existencial de estas variables y usar las definiciones de los símbolos funcionales como a continuación:

$$\exists y_1 \exists y_2 \exists y_3[\forall x[\neg(x \in y_1)] \land \forall x[x \in y_2 \Leftrightarrow x = y_1] \land \forall x[\neg(x \in y_3)] \land y_3 \in y_2]$$

Denótese $\varphi_\emptyset := \forall x[\neg(x \in w_1)], \varphi_{\{-\}} := \forall x[x \in w_2 \Leftrightarrow x = w_1]$ y $\varphi_\leq := w_1 \in w_2$. Con esto en mente, de manera más general se puede representar lo anterior mediante:

$$\exists y_1 \exists y_2 \exists y_3 [\varphi_\emptyset(y_1) \wedge \varphi_{\{-\}}(y_1, y_2) \wedge \varphi_\emptyset(y_3) \wedge \varphi_\leq(y_3, y_2)]$$

Que formalmente no es más que:

$$\varphi := \exists y_1 \exists y_2 \exists y_3 [[y_1/w_1]\varphi_\emptyset \wedge [y_2/w_2][y_1/w_1]\varphi_{\{-\}} \wedge [y_3/w_1]\varphi_\emptyset \wedge [y_2/w_2][y_3/w_1]\varphi_\leq]$$

II. Supóngase que $\Sigma = \langle 0, + \rangle$ y que $\Sigma' = \langle 0, 1, +, \times; \leq \rangle$. Si $\varphi' := (x + 1) \times 0 = 0 + 0$, entonces, de acuerdo a lo dicho en el punto anterior, su equivalente *wff* $\varphi \in \mathcal{L}$ sería:

$$\varphi := \exists y_1 \exists y_2 [[y_1/w_1]\varphi_1 \wedge [y_2/w_3][0/w_2][x + y_1/w_1]\varphi_\times \wedge y_2 = 0 + 0]$$

Teorema II.4 (Invarianza bajo extensiones por definiciones)
Si $\Gamma' \subseteq \mathcal{L}'$ es una extensión por definiciones de $\Gamma \subseteq \mathcal{L}$, entonces para cada $\varphi' \in \mathcal{L}'$ existe $\varphi \in \mathcal{L}$ tal que:

- $\Gamma' \vdash (\varphi \Leftrightarrow \varphi')$
- Si $\Gamma' \vdash \varphi'$, entonces $\Gamma \vdash \varphi$.

Idea de Prueba. Para el primer punto, la demostración se debe desglozar en casos. Si $\varphi' \in \mathcal{L}$, entonces haciendo $\varphi := \varphi'$ se tiene lo deseado. Por otro lado, si $\varphi' \in (\mathcal{L}' \setminus \mathcal{L})$, el argumento procede por inducción sobre la complejidad de φ'. En general ésta es sencilla excepto en el caso base $\varphi' = P(t_1, \ldots, t_n)$ con $P \in \mathcal{P}_n$ y n un entero no negativo. Éste se resuelve formalizando el algoritmo dado en el ejemplo anterior. Para la segunda parte, se puede suponer que $\Gamma' \vdash \varphi'$ pero $\Gamma \nvdash \varphi$. Utilizando la contrarrecíproca al teorema de completez de Gödel, debería existir una estructura $\mathfrak{A}$ para $\mathcal{L}$ que sea modelo de Γ pero no de φ. Siempre es posible expandir esta estructura a otra $\mathfrak{A}'$ de tal modo que para cada $s \in (\Sigma' \setminus \Sigma)$, $s^{\mathfrak{A}'}$ satisfaga lo que dice la definición de s en Γ'. De este modo, $\models_{\mathfrak{A}'} \Gamma'$ pero $\not\models_{\mathfrak{A}'} \varphi'$, contradiciendo el teorema de robustez aplicado a $\Gamma' \vdash \varphi'$. ■

Las demostraciones formales de los últimos teoremas se han tornado considerablemente largas en comparación con las primeras pruebas presentadas en lógica proposicional. Ahora que se ha agregado la posibilidad de dar definiciones, es de esperarse que se alarguen aún más. Por dicha razón, a partir de éste punto, se trabajará como comúnmente en matemáticas, es decir, en vez de proporcionar instancias de pruebas formales, se utilizarán argumentos *rigurosos* para justificar las consecuencias de los axiomas que se revisen. La primera de éstas es la demostración de que no existe el conjunto V:

Teorema II.5 (No existe un conjunto de todos los conjuntos)
Es teorema de una teoría con axioma de extensionalidad y esquema de axioma de especificación que:

$$\neg \exists y \forall x [x \in y]$$

Demostración. Supóngase que existe tal conjunto y denótesele por V. En dicho caso, por el principio de comprensión restringida, se puede construir el conjunto de Russell, $R := \{x \in V \mid x \notin x\}$. Se sabe muy bien que éste lleva a una contradicción. Por lo tanto se tiene lo deseado. ■

A pesar de ésto, es común que varios matemáticos hablen de la clase de todos los conjuntos, definiéndola por $V = \{x \mid x = x\}$. Filosóficamente esto se suele justificar regresando al concepto informal de *colección* y aseverando que una *clase* es únicamente una colección tan grande que no puede considerarse conjunto. Así, todo conjunto es una clase pero no toda clase es un conjunto. Formalmente esta distinción se puede hacer mediante axiomas, lógica de segundo orden o aseverando que al tratar con clases, realmente se está tratando con *wffs*. Es decir, en su mayoría la terminología de clases son abreviaciones de *wffs* más complejas. Como ejemplos de ésto supóngase que A y C son las clases $A = \{x \mid \alpha(x)\}$ y $C = \{x \mid \varphi(x)\}$, entonces:

- Escribir $x \in C$ representa que $\varphi(x)$.
- La expresión $x \in A \cup C$ se debe interpretar como $\alpha(x) \vee \varphi(x)$.
- Igualar A con C, i.e. $A = C$ significa $\forall x[\alpha(x) \Leftrightarrow \varphi(x)]$.
- Las oraciones "la clase C es un conjunto" y "el conjunto C sí existe" son dos maneras de decir $\exists y \forall x[x \in y \Leftrightarrow \varphi(x)]$. En caso de que esto no sea demostrable se dirá que C *es una clase propia*.

Como últimas consecuencias puramente del esquema de axioma de especificación, se hace notar lo siguiente: dados cualesquiera dos conjuntos, A y B, se pueden construir $A \cap B = \{x \in A \mid x \in B\}$ y $A \setminus B = \{x \in A \mid x \notin B\}$. Ésto es viable ya que ambos son subconjuntos de A. Sin embargo, como $A \cup B = \{x \mid x \in A \vee x \in B\}$ en general es un supraconjunto de A y B, no es posible construirlo a partir de los axiomas dados hasta el momento. Ésto es igualmente válido para cualquier conjunto que en sus elementos tenga a A y/o a B, por ejemplo $\{A\} = \{x \mid x = A\}$ y $\{A, B\} = \{x \mid x = A \vee x = B\}$. Es por esta razón que se requieren de más axiomas para desarrollar la teoría de conjuntos de acuerdo a lo que dicta la intuición:

Definición II.5 (Axiomas del par y de la unión)
Ambos axiomas enuncian la existencia de un conjunto, p en el caso del par, y u en el caso de la unión:

- El *axioma del par* establece que dados cualesquiera dos conjuntos x y y, existe otro que tiene a ambos como elementos, i.e. $\forall x \forall y \exists p[x \in p \wedge y \in p]$.
- El *axioma de la unión* dicta que dada una familia de conjuntos z (un conjunto de conjuntos), existe un conjunto que contiene a la unión de todos los y, elementos de z. Formalmente: $\forall z \exists u \forall y \forall x[x \in y \wedge y \in z \Rightarrow x \in u]$.[4]

[4]Uno podría haber dado un axioma que permitiese la construcción de $x \cup y$, sin embargo, la formulación dada aquí tiene la ventaja de que permite unir "infinitos" conjuntos, suponiendo claro que z es infinito.

Nótese que a pesar de que ya se tienen los conjuntos p y u, aún así se requiere del principio de comprensión restringida y el axioma de extensionalidad para definir a los ya conocidos:

$$\{x, y\} := \{z \in p \mid z = x \vee z = y\} \text{ y } \bigcup z := \{x \in u \mid \exists[y \in z \wedge x \in y]\}$$

A partir de éstas sólo se requiere especificación y extensionalidad para definir otros conceptos comunes de teoría de conjuntos:

- $\{x\} := \{x, x\}$.
- $(x, y) := \{\{x\}, \{x, y\}\}$.[5]
- $x \cup y := \bigcup\{x, y\}$.
- $\bigcap z := \{x \in \bigcup z \mid \forall y[y \in z \Rightarrow x \in y]\}$ para $z \neq \emptyset$.
- $\{x, y, z\} := \{x, y\} \cup \{z\}$.
- $\{z_1, \ldots, z_{n+1}\} := \{z_1, \ldots, z_n\} \cup \{z_{n+1}\}$.
- $S(x) := x \cup \{x\}$.
- $0 := \emptyset$.
- $1 := S(0) = \{\emptyset\}$.
- $2 := S(1) = \{\emptyset, \{\emptyset\}\}$.

$\vdots$

Con base en todas estas definiciones uno puede verificar varios resultados de la teoría informal de conjuntos como las leyes de De Morgan para conjuntos, e.g. $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$; la caracterización de la igualdad de *parejas ordenadas*, i.e. $x = y \wedge x' = y' \Leftrightarrow (x, y) = (x', y')$, o la extensionalidad de conjuntos finitos: $\{x, y, z\} = \{x, z, y\}$. No obstante, también se pueden derivar enunciados que podrían considerarse contrarios a la intuición, por ejemplo: $(0, 1) = \{1, 2\}, 1 \in 3$ y $(1, 0) = \{\{1\}, 2\}$. Éstas consecuencias a veces llamadas "patológicas" aparentemente no son características de las teorías de conjuntos, sino que se extienden a todo sistema formal "sencillo" que pretenda fundamentar al resto de las matemáticas. La razón es que formalizarlas bajo una sola teoría requiere *codificar* ciertos objetos estándar como los números naturales, las funciones y las relaciones por medio de otros que, inicialmente, podrían parecerles ajenos.

Con lo obtenido hasta ahora se pueden empezar a formalizar el resto de los conceptos matemáticos. En la siguiente sección se dará un panorama general de cómo podría llevarse a cabo dicho proceso. Si en algún momento algún axioma es requerido, se agregará directamente tal y como se ha ido trabajando hasta el momento. Para concluir la sección se da una última definición y una serie de convenciones para manejar los conceptos presentados de manera más acorde a la praxis:

- La expresión $\forall x \in y[\varphi]$ representará la *wff* $\forall x[x \in y \Rightarrow \varphi]$.
- Se usará $\exists x \in y[\varphi]$ en vez de $\exists x[x \in y \wedge \varphi]$.

[5] La definición convencional es gracias a Kazimier Kuratowski, sin embargo otras son posibles como $\langle x, y\rangle := \{\{\{x\}, \emptyset\}, \{\{y\}\}\}$ dada por Norbert Wiener o $\langle x, y\rangle := \{\{x, 1\}, \{y, 2\}\}$, por Felix Hausdorff.

- En vez de utilizar varios cuantificadores iguales seguidos, $\daleth z_1 \daleth z_2 \ldots \daleth z_n[\varphi]$ con $\daleth \in \{\forall, \exists\}$, se utilizará uno sólo con las variables separadas por comas, esto es $\daleth z_1, \ldots, z_n[\varphi]$.

- A partir de este punto prácticamente no habrá restricciones respecto a las meta-variables utilizadas para denotar conjuntos. Es decir, en vez de minúsculas podrán utilizarse también mayúsculas, letras griegas y otras tipografías para representar conjuntos.

- Se adoptará la notación de la teoría informal de conjuntos, esto es, se escribirá $\varphi(x)$ cuando se desee expresar que x cumple la "propiedad" φ.

Definición II.6 (Teoría de Conjuntos restringida de Zermelo)
Se llamará *teoría (restringida) de Zermelo*, Z^*, a la teoría cuyos axiomas no lógicos son:

- Extensionalidad: $\forall z[(z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y]$.

- Especificación: $\exists Z \forall x[x \in Z \Leftrightarrow (x \in Y \wedge \varphi(x))]$.

- Par: $\exists P[x \in P \wedge y \in P]$.

- Unión: $\exists U \forall Y \forall x[x \in Y \wedge Y \in \mathcal{F} \Rightarrow x \in U]$.

III. Implementación de las Matemáticas en Teoría de Conjuntos

Se empezará definiendo los conceptos más básicos en matemáticas, es decir, las relaciones y funciones. Intuitivamente, las relaciones son objetos que al interactuar con otros expresan "sí" o "no", es decir, dan un valor de verdad. Para implementarlas dentro de una teoría de conjuntos lo común es codificar dichos valores de verdad por medio de la única relación existente en el lenguaje: la de pertenencia. De esta manera que a y b estén relacionados por R se podría expresar mediante $\{a, b\} \in R$. El único inconveniente es que una relación sí distingue el orden en que se presentan los objetos (no es lo mismo "a es padre de b" que "b es padre de a"). Con base en esto la codificación correcta de la expresión aRb (a está R-relacionado con b) es $(a, b) \in R$. Así se genera la siguiente definición:

Definición III.1 (Relación binaria)
La clase R es una relación binaria si y sólo si todos sus elementos son parejas ordenadas:

$$R \text{ es relación} \Leftrightarrow \forall z \in R \exists x, y[z = (x, y)]$$

Además $x \mathrel{R} y := (x, y) \in R$ mientras que $x \not\mathrel{R} y := (x, y) \notin R$.

De aquí uno puede definir conjuntos (clases) comúnmente tratados junto con las relaciones como:

- El *dominio de una relación*: $\mathrm{Dom}(R) := \{x \in \bigcup\bigcup R \mid \exists y[x \mathrel{R} y]\}$.

- El *rango de una relación*: $\mathrm{Ran}(R) := \{y \in \bigcup\bigcup R \mid \exists x[x\ R\ y]\}$.
- La *imagen directa de* A *bajo* R: $R[A] := \{y \in \bigcup\bigcup R \mid \exists x \in A[x\ R\ y]\}$.
- La *imagen inversa de* B *bajo* R: $R^{-1}[B] := \{x \in \bigcup\bigcup R \mid \exists y \in B[x\ R\ y]\}$.
- La *restricción de* R *en* A: $R \restriction A = R\restriction_A := \{(x, y) \in R \mid x \in A\}$.

También es posible dar todos los tipos de relaciones de la misma manera en que se dan en álgebra y áreas afines, por ejemplo:

- R es reflexiva en $A \Leftrightarrow \forall x \in A[x\ R\ x]$.
- R es simétrica en $A \Leftrightarrow \forall x, y \in A[x\ R\ y \Rightarrow y\ R\ x]$.
- R es transitiva en $A \Leftrightarrow \forall x, y, z \in A[x\ R\ y \wedge y\ R\ z \Rightarrow x\ R\ z]$.
- R es antisimétrica en $A \Leftrightarrow \forall x, y \in A[x\ R\ y \wedge y\ R\ x \Rightarrow x = y]$.
- R es asimétrica en $A \Leftrightarrow \forall x, y \in A[x\ R\ y \Rightarrow y \not R\ x]$.
- R es total/linear en $A \Leftrightarrow \forall x, y \in A[x\ R\ y \vee y\ R\ x]$.
- $\sim$ es de equivalencia en A sii $\sim$ es reflexiva, simétrica y transitiva en A.
- $\leq$ es un orden parcial en A sii $\leq$ es reflexiva, transitiva y antisimétrica en A.
- $<$ es un orden estricto en A sii $<$ es transitiva y asimétrica en A.
- $\leq$ es un orden lineal en A sii $\leq$ es transitiva, antisimétrica y total en A.

En el caso de las funciones, es común pensar en ellas como colecciones de reglas de correspondencias $x \mapsto f(x)$ que asignan a cada elemento x de un conjunto, A, un único elemento $f(x)$ de otro, B. Es bien sabido que ésto se puede codificar mediante relaciones al traducir $x \mapsto y$ como $x\ f\ y$ (x está f-relacionado con y). Como ya se conoce la codificación de las relaciones en teoría de conjuntos, sólo resta escribir propiamente la:

Definición III.2 (Funciones)
La clase F es una función si F es una relación y para cada $x \in \mathrm{Dom}(F)$, existe un único y tal que $x\ F\ y$, esto es[6]:

$$F \text{ es función} \Leftrightarrow F \text{ es relación } \wedge \forall x, y, z[(x, y) \in F \wedge (x, z) \in F \Rightarrow y = z]$$

Así, el familiar $F : x \mapsto y$ ("x es mapeado a y bajo F" o "F mapea x en y"), es una representación del enunciado conjuntista $(x, y) \in F$. Por otro lado, al único y tal que $F : x \mapsto y$ se le denota por $F(x)$. Como consecuencia de esta meta-definición, escribir $F(x) = y$ (la imagen de x bajo F es y) es otra manera de decir $(x, y) \in F$.

[6]Nótese que se están dando dos definiciones de función: la primera en términos de su dominio y la segunda en términos de sus elementos. Ambas son formalizables en Z^* y demostrablemente equivalentes.

De esta definición uno puede generar las otras más cercanas a la praxis:

- F *es función en* A si y sólo si F es función y $\mathrm{Dom}(F) = A$.

- F *es función a* B o B *es codominio de* F, denotado por $\mathrm{Cod}(F) = B$, sii F es función y $\mathrm{Ran}(F) \subseteq B$.

∘ F *es función de* A *a* B, denotado por $F : A \to B$, si $\mathrm{Dom}(F) = A$ y $\mathrm{Cod}(F) = B$.

⋆ Se dice que una función, F, *es inyectiva* o que *es uno a uno* cuando se cumple $\forall x, y \in \mathrm{Dom}(F)[F(x) = F(y) \Rightarrow x = y]$.

⋆ Similarmente a una función F a $\mathrm{Cod}(F)$, se le llama *suprayectiva o sobreyectiva* cuando ésta cumple $\forall y \in \mathrm{Cod}(F) \exists x \in \mathrm{Dom}(F)[F : x \mapsto y]$.

∘ F *es función de* A *en* B, comúnmente abreviado por $F : A \xrightarrow{1-1} B$ ó $F : A \rightarrowtail B$, sii $F : A \to B$ y F es inyectiva.

∘ F *es función de* A *sobre* B, representado por $F : A \xrightarrow{onto} B$ ó $F : A \twoheadrightarrow B$, sii $F : A \to B$ y F es sobreyectiva.

⋆ Dada una función F, ésta es *biyectiva* si es inyectiva y sobreyectiva.

∘ Finalmente, se combina todo lo anterior escribiendo $F : A \rightarrowtail\!\!\!\!\twoheadrightarrow B$ ó $F : A \xrightarrow[onto]{1-1} B$ si $F : A \to B$ y F es biyectiva.

También directamente de la definición se tiene la siguiente propiedad de funciones:

Teorema III.1 (Extensionalidad de funciones)
Dadas dos funciones f y g, éstas son iguales, i.e. $f = g$, si y sólo si $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ y $\forall x, y, z[(f : x \mapsto y) \wedge (g : x \mapsto z) \Rightarrow y = z]$.

Demostración. Sean f y g funciones, entonces:
($\Rightarrow$) Si $f = g$, entonces $(x, y) \in f \Leftrightarrow (x, y) \in g$. Veamos que $\mathrm{Dom}(f) = \mathrm{Dom}(g)$:
($\subseteq$) Supóngase que $x \in \mathrm{Dom}(f)$, entonces existe un y tal que $(x, y) \in f$. Como $f = g$, $(x, y) \in g$. Por lo tanto $x \in \mathrm{Dom}(g)$. ($\supseteq$) La prueba es análoga al caso anterior.
Para probar que $\forall x, y, z[(f : x \mapsto y) \wedge (g : x \mapsto z) \Rightarrow y = z]$, supóngase que x, y, z son tales que $f : x \mapsto y$ y $g : x \mapsto z$. Como $f = g$, se sabe que $(x, z) \in f$. Por unicidad de la imagen de x bajo f se concluye que $y = z$.
($\Leftarrow$) Para probar que $f = g$ se deben verificar dos casos:
($\subseteq$) Si $(x, y) \in f$, entonces $x \in \mathrm{Dom}(f)$. Como $\mathrm{Dom}(f) = \mathrm{Dom}(g)$, se puede probar que $x \in \mathrm{Dom}(g)$. Esto quiere decir que existe un z para el cual $(x, z) \in g$. Por la segunda propiedad $y = z$, de donde $(x, y) = (x, z)$ y, por lo tanto, $(x, y) \in g$. La prueba para ($\supseteq$) es análoga a la recientemente hecha. ■

Si uno observa la definición formal de función dada en el presente texto se percatará de que ésta no requirió de otros conceptos más que el de parejas ordenadas y la relación de pertenencia. No obstante, rara vez en matemáticas se da una función sin especificar quiénes son su dominio y su codominio. Ésta es otra característica de las teorías de conjuntos muy criticada, pues de acuerdo a algunas personas, una fundamentación adecuada de las matemáticas debería incorporar en su implementación la manera en la que los matemáticos trabajan diariamente. Todas estas observaciones respecto a las “fallas” de las teorías de conjuntos son importantes porque varias de ellas fueron motivo para el desarrollo de sistemas alternos como los presentados en capítulos siguientes.

Con base en lo dicho anteriormente, se podría tratar de diseñar un sistema formal en el que las funciones sean el concepto fundamental de la teoría; pero para esto, uno debería ser capaz de codificar los conjuntos dentro de las funciones. Esto sí es posible, de hecho, John von Neumann presentó un sistema axiomático en términos de funciones.[7] Hasta ahora sólo se ha visto que las relaciones son conjuntos y que las funciones son relaciones. Para verificar que es posible codificar conjuntos en términos de funciones (y ver que en esencia fundamentar en términos de funciones, conjuntos y/o relaciones es equivalente) sólo resta comprobar que todo conjunto es una función. A pesar de que no se prueba en el presente texto, la idea es bien conocida en matemáticas, pues todo conjunto A tiene asociada una función χ_A llamada su *función característica*, definida por:

$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}$$

De esta manera, una teoría de conjuntos podría considerarse también una teoría de relaciones o una teoría de funciones.

Con lo presentado hasta ahora se podría creer que ya se tiene lo suficiente para hacer matemáticas, pero ni siquiera se tiene lo requerido para hacer todo lo que permite hacer la teoría informal de conjuntos. Por ejemplo, dados dos conjuntos cualesquiera, A y B, el problema de construir su producto cartesiano, $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$, no se puede resolver con los axiomas dados hasta ahora. Para hacer más evidente esto, considérese la definición del producto cartesiano bajo el principio de comprensión: $A \times B := \{z \mid \exists a \in A, b \in B[z = (a, b)]\}$. Para poder definirlo de manera formal, debería utilizarse el principio de comprensión

[7]Posteriormente Paul Bernays convirtió la teoría de funciones de von Neumann en una teoría de clases y conjuntos. Para esto separó a las variables de su lenguaje en dos colecciones, las de la primera eran asignadas a clases mientras que las de la segunda a los conjuntos. Posteriormente, Kurt Gödel adaptaría el trabajo de Bernays y von Neumann en una teoría con un solo tipo de variables al hacer a todo conjunto una clase. Por dicha razón la teoría resultante es conocida hoy en día como la teoría de conjuntos NBG (Neumann-Bernays-Gödel) [BG]. Aunque ésta no es la que se presenta en este trabajo, es bien conocido en la comunidad matemática que todo teorema de NBG se puede probar en la teoría presentada aquí y viceversa.

restringida, sin embargo ésto no es posible en todos los casos porque no siempre se sabe en qué supraconjunto de $A \times B$ "viven" sus elementos (los $z = (a, b)$). Por dicha razón, es necesario agregar otro axioma. Para ello, uno podría considerar un axioma del *producto cartesiano*, pero las soluciones más populares agregan cualquiera de dos axiomas: el del *potencia* o el *esquema de axioma de reemplazo*. La verdadera ventaja de añadir el de reemplazo a Z^* se observa una vez que se combina con el axioma del infinito. Por ende nos enfocaremos primero en el:

Definición III.3 (Axioma del potencia)
El *axioma del potencia* afirma que dado cualquier conjunto X, existe un conjunto P que en sus elementos tiene a todos los subconjuntos de X, esto es:

$$\forall X \exists P \forall Y [Y \subseteq X \Rightarrow Y \in P]$$

Nuevamente, por el esquema de axioma de especificación, uno puede definir ahora al *conjunto potencia* de X:

$$\mathcal{P}(X) := \{Y \in P \mid Y \subseteq X\}$$

Y con esto, la definición del producto cartesiano nada más requiere de analizar los "niveles" en los que se ubican las parejas (a, b). Esto es, a y b son elementos de $A \cup B$. Aplicando la operación potencia a esta unión una vez, se obtendrían los conjuntos $\{a\}$ y $\{a, b\}$. Una segunda aplicación del potencia ya tendría como elementos a las parejas ordenadas $(a, b) = \{\{a\}, \{a, b\}\}$. Por ende:

$$A \times B := \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \exists a \in A, b \in B[z = (a, b)]\}$$

La utilidad del conjunto potencia no sólo se ve reflejada al poder definir el producto cartesiano, sino que otras construcciones comunes también lo requieren. Por ejemplo, una vez que se tiene una relación de equivalencia $\sim$ sobre un conjunto X uno puede definir las *clases de equivalencia* como es usual en matemáticas. Es decir, para cada $x \in X$, la clase de equivalencia de x es el conjunto $[x] := \{y \in X \mid x \sim y\}$. Finalmente, se construye al *conjunto cociente* mediante:

$$\frac{X}{\sim} = X/\sim := \{[x] \in \mathcal{P}(X) \mid x \in X\}$$

Similarmente, para definir la *composición de relaciones* y las *relaciones inversas* se necesita del producto cartesiano (ergo, del conjunto potencia):

$$R \circ S := \{(x, z) \in \mathrm{Dom}(R) \times \mathrm{Ran}(S) \mid \exists y[(x, y) \in R \wedge (y, z) \in S)]\}$$

$$R^{-1} := \{(y, x) \in \mathrm{Ran}(R) \times \mathrm{Dom}(R) \mid (x, y) \in R\}$$

De aquí se pueden demostrar propiedades conocidas de las relaciones y funciones, como que "la imagen directa de un conjunto A bajo la relación inversa R^{-1} coincide con la imagen inversa del conjunto A bajo la relación original $R^{-1}[A]$"; "todo subconjunto de un producto cartesiano es una relación"; "la composición de dos funciones es una función”; “dadas dos funciones, f y g, $\mathrm{Dom}(g \circ f) = \mathrm{Dom}(f) \cap f^{-1}[\mathrm{Dom}(g)]$ y para cada $x \in \mathrm{Dom}(g \circ f)$, $(g \circ f)(x) = g(f(x))$”; “una función es invertible, i.e. f^{-1} es función, si y sólo si es inyectiva”, y “si f es invertible, entonces f^{-1} también lo es y además $(f^{-1})^{-1} = f$”.

Además de lo presentado hasta ahora, también se pueden definir conjuntos de funciones. Dados dos conjuntos A y B, recuérdese que una función f de A a B formalmente no es más que un subconjunto del producto cartesiano $A \times B$. Así que, gracias al axioma del potencia, *el conjunto de funciones de* A *a* B ya se puede construir:

$$B^A := \{f \in \mathcal{P}(A \times B) \mid f : A \to B\}$$

Ahora recuérdese que *una sucesión* no es más que una función con algún conjunto de *índices* I como dominio. Este conjunto de índices realmente puede ser cualquier conjunto pero en general se ocupan conjuntos que tengan una relación de orden en ellos como “los conjuntos” de los números naturales, enteros, racionales y/o reales. En el caso de las sucesiones, al único elemento del codominio de la sucesion que es imagen de $i \in I$ se le denota por una variable con un subíndice, e.g x_i. Con esto en mente, la sucesión de los x_i tales que $i \in I$ se suele representar mediante $\langle x_i \rangle_{i \in I}$ o por $\langle x_i \mid i \in I \rangle$. En el caso de sucesiones indizadas sobre conjuntos finitos, la notación puede variar. Por ejemplo, suponiendo que $I = \{1, 2, \ldots, n\}$ es el conjunto de los primeros n enteros positivos, una sucesión indizada por I puede denotarse por $\langle x_i \rangle_{i=1}^{i=n}$ o por la equivalente $\langle x_1, x_2, \ldots, x_n \rangle$.

Supóngase que $\mathcal{A}$ es una familia de conjuntos (un conjunto de conjuntos). Utilizando sucesiones de elementos de $\mathcal{A}$ indizadas por algún conjunto I, i.e. $S = \langle A_i \in \mathcal{A} \mid i \in I \rangle$, uno puede definir uniones e intersecciones “controladas” de dichos elementos:

$$\bigcup_{i \in I} A_i := \bigcup \{A_i \in \mathcal{A} \mid i \in I\} = \bigcup \mathrm{Ran}(S) \qquad \bigcap_{i \in I} A_i := \bigcap \{A_i \in \mathcal{A} \mid i \in I\} = \bigcap \mathrm{Ran}(S)$$

Y con estos conceptos se puede construir el *producto cartesiano generalizado*:

$$\prod_{i \in I} A_i := \{f \in \Big(\bigcup_{i \in I} A_i\Big)^I \mid f(i) \in A_i\}$$

Obsérvese que si $s \in \prod_{i \in \{1,2,3\}} A_i$, entonces $s(1) \in A_1, s(2) \in A_2$ y $s(3) \in A_3$. Representando a s como sucesión finita, se tiene que $s = \langle s_1, s_2, s_3 \rangle$, lo cual se corresponde con $(s_1, s_2, s_3) \in (A_1 \times A_2) \times A_3$. Se puede generar entonces una biyección entre el producto $\prod_{i \in \{1,2,3\}} A_i$ y el conjunto $(A_1 \times A_2) \times A_3$. Es en este sentido que el conjunto anterior es un producto cartesiano generalizado, pues sus elementos pueden ser sucesiones “infinitas” si el conjunto de índices I es “infinito”.

Por el momento ya es posible construir todos los conjuntos que se definieron en la sección de teoría informal de conjuntos: el vacío, uniones, intersecciones, tuplas, productos cartesianos, diferencias de conjuntos y hasta complementos relativos (porque no existe el conjunto $V = \{x \mid x = x\}$). También se pueden construir los números naturales, pues se tiene al número $0 = \emptyset$ y a la operación sucesor $S(x) = x \cup \{x\}$, cumpliéndose así:

$$0 = \emptyset, \quad 1 = S(0) = \{0\}, \quad 2 = S(1) = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \quad 4 = \{0, 1, 2, 3\}, \ldots$$

[8]Sin embargo, aún no se han desarrollado los conceptos necesarios para expresar dentro de la teoría de Zermelo restringida, junto con el axioma del potencia, el predicado “ser un número natural”. Una vez logrado ésto, se podrá cuantificar sobre el dominio de discurso de todos los números naturales y, en consecuencia, hacer aritmética básica:

Definición III.4 (Ordinal)
De manera amplia uno puede decir que el conjunto α *es un ordinal* (denotado por $\alpha \in ON$) si la relación de pertenencia $\in_\alpha := \{(a, b) \in \alpha \times \alpha \mid a \in b \vee a = b\}$ es un orden lineal y bien fundado (todo subconjunto no vacío de α tiene elemento mínimo) en α. Formalmente se dirá que α es un ordinal si y sólo si:

- α es transitivo: $\forall x, y[x \in y \wedge y \in \alpha \Rightarrow x \in \alpha]$.
- $\in$ es tricotómica en α: $\forall x, y \in \alpha[x \in y \vee y \in x \vee x = y]$.
- α es bien fundado (bajo $\in$): $\forall \beta[\beta \subseteq \alpha \wedge \beta \neq \emptyset \Rightarrow \exists \gamma \in \beta[\gamma \cap \beta = \emptyset]$.

Se verifica que la definición recientemente dada implica lo que informalmente se deseaba expresar:

Propiedades III.2 (de ordinales)
Las siguientes son propiedades de lo recientemente definido:

1. Un conjunto X es transitivo si y sólo si $\forall x \in X[x \subseteq X]$.
2. Si $\in$ es tricotómica en X y $A \subseteq X$, entonces $\in$ es tricotómica en A.
3. Si X es bien fundado y $A \subseteq X$, entonces A es bien fundado.
4. Si X es bien fundado, entonces $X \notin X$.
5. El vacío $\emptyset$ es un ordinal.

[8]La definición dada aquí de los números naturales es atribuida a von Neumann. En la formulación original de sus axiomas y el desarrollo de la teoría consecuente, Zermelo no definió a los números naturales de la misma manera. Sí empezo con $0 := \emptyset$, pero definió $S(x) := \{x\}$. Esto es, los naturales en la construcción de Zermelo son:

$$0 = \emptyset, \quad 1 = S(0) = \{0\}, \quad 2 = S(2) = \{1\}, \quad 3 = \{2\}, \quad 4 = \{3\}, \ldots$$

6. Si X es un ordinal, entonces su sucesor $S(X) = X \cup \{X\}$ es un ordinal.

7. Todo elemento de un ordinal es un ordinal.

8. Si A es un ordinal entonces $\in_A$ es un orden linear bien fundado en A.

Demostración. Las primeras tres propiedades se siguen directo de las definiciones, mientras que la quinta, por vacuidad.
4. Supóngase que $X \in X$, entonces $\{X\} \subseteq X$. De aquí que el único elemento de $\{X\}$, X, cumple que $X \cap \{X\} = \emptyset$. De donde $X \notin X$, lo cual contradice que $X \in X$.
6. Para ver que el sucesor del ordinal X es transitivo obsérvese que si $y \in X \cup \{X\}$, entonces cualquier $x \in y$ cumplirá que $x \in X \cup \{X\}$, ya sea por transitividad o porque $y = X$. En el caso de la tricotomía, si $x, y \in X \cup \{X\}$, la prueba se divide en cuatro casos, todos directos. Finalmente, para revisar que $X \cup \{X\}$ es bien fundado, dado un subconjunto no vacío A de $S(X)$, sabemos que todo elemento de A o es elemento de X o es exactamente X. Por buena fundación, o $A \setminus \{X\}$ tiene un elemento x tal que $x \cap (A \setminus \{X\}) = \emptyset$ o $A \setminus \{X\} = \emptyset$. De aquí que $x \cap A = \emptyset$ o $X \cap A = \emptyset$ pues en ambos casos, en uno por transitividad y en otro por definición, suponer lo contrario lleva a $X \in X$, lo que contradice la cuarta propiedad.
7. Dado un ordinal X y $\alpha \in X$, por transitividad $\alpha \subseteq X$ y por la segunda y tercera propiedad $\in$ es tricotómica en α y éste es bien fundado. Para $y \in \alpha$ y $x \in y$ se cumplirá que $x, y \in X$, de donde $\{x, y, \alpha\} \subseteq X$. Por buena fundación alguno de los tres intersectado con $\{x, y, \alpha\}$ da el vacío. Claramente ni y ni α cumplen esto, así que $x \cap \{x, y, \alpha\} = \emptyset$. Por tricotomía $x \in \alpha$ o $\alpha \in x$ o $x = \alpha$. Los dos últimos casos contradicen que $x \cap \{x, y, \alpha\} = \emptyset$ y, por ende, $x \in \alpha$. Con esto se demuestra la transitividad de α y, por ende, α es un ordinal.
8. Para ver que $\in_A$ es transitiva en A, dados $x, y, z \in A$ tales que $x \in_A y$ y $y \in_A z$, se tiene que $x \in y \vee x = y$ y $y \in z \vee y = z$. Los casos en los que haya igualdades son fáciles de manejar. En el otro caso, por la propiedad anterior, z es un ordinal también, de donde $y \subseteq z$ y, por ende, $x \in z$. Supóngase que $x, y \in A$ son tales que $x \in_A y$ y $y \in_A x$. Como ambos son ordinales, $x \subseteq y$ y $y \subseteq x$. De aquí se deriva la igualdad y, en general que, $\in_A$ es antisimétrica en A. La totalidad de $\in_A$ es equivalente a la tricotomía de $\in$ en A. Finalmente, sea B un subconjunto no vacío de A, por hipótesis existe un elemento C de B tal que $B \cap C = \emptyset$. Veamos que C es elemento mínimo de B respecto a $\in_A$. Sea $D \in B$, por la propiedad de C, se cumple que $D \notin C$. Ahora, por tricotomía $C \in_A D$, i.e. todo elemento de B es "mayor o igual que" C. Con esto concluye la prueba. ■

Más propiedades de los ordinales no demostradas aquí son válidas, por ejemplo, asumiendo la buena fundación de un conjunto X, otras equivalencias a "X es un ordinal" son "X es un conjunto transitivo totalmente ordenado por la contención de conjuntos $\subseteq$", y "X es un conjunto transitivo de conjuntos transitivos". De igual manera uno puede derivar de las definiciones dadas que la intersección de dos ordinales es un ordinal y que la clase ON de los oridinales es una clase "transitiva", "bien fundada" tal que "$\in$ es tricotómica en ON" (todo esto, tomándolo como abreviaciones de fórmulas bien formadas del lenguaje de la teoría de conjuntos $\mathcal{L}$). De aquí se concluye que ON es una clase propia, pues si fuese un conjunto se tendría que $ON \in ON$, lo cual violaría su buena fundación. También, como en los ordinales $\in$ es un orden linear, nada impide tomar la notación $<:=\in$ al momento de hablar de éstos. Es en dichos términos que "$\emptyset$ es el mínimo ordinal", "si $\alpha \in ON$, entonces $S(\alpha)$ es el mínimo ordinal mayor que α" y "todo conjunto de ordinales admite un supremo".

Aunado a todo esto, por cómo se fueron definiendo los números $0, 1, 2, 3, 4, \ldots$ y por las propiedades 5 y 6, anteriores, uno podría aseverar que los ordinales contienen a los naturales. Para demostrar esto, se debe dar una subclase de los ordinales $\omega \subseteq ON$, bien definida (en términos de una *wff* de $\mathcal{L}$) y probar que ésta cumple el comportamiento esperado de los números naturales, que en términos de lógica matemática significa verifica que ω modela los axiomas de Peano:

Definición III.5 (Clase ω o predicado "ser número natural")
Un conjunto n ***es un número natural***, denotado por $n \in \omega$, si todo $\alpha \leq n$ ($\alpha \in n \vee \alpha = n$) es 0 o el sucesor de un ordinal:[9]

$$n \in \omega \Leftrightarrow \forall \alpha \leq n[\alpha = 0 \vee \exists \beta \in ON[\alpha = S(\beta)]]$$

Propiedades III.3 (de la clase ω)
Por cómo se definieron los números naturales se cumple que:

★ $\omega \subseteq ON$.

★ La clase ω "es un ordinal".

★ La clase ω es modelo de los axiomas (originales)[10] de Peano, i.e:

(I) El 0 es un número natural: $0 \in \omega$
(II) El sucesor de un natural es un natural: $\forall n \in \omega[S(n) \in \omega]$
(III) Inyectividad de la función sucesor: $\forall m, n \in \omega[S(m) = S(n) \Rightarrow m = n]$
(IV) El 0 no es sucesor de nadie: $\forall n[\neg(0 = S(n))]$
(V) Axioma de Inducción: $\forall K[(0 \in K \wedge \forall n \in \omega[n \in K \Rightarrow S(n) \in K]) \Rightarrow \omega \subseteq K]$

Demostración. Directamente de la definición se obtiene que $n \in \omega \Rightarrow n \in ON$ (sólo hay que aplicarla a $n \leq n$ y usar las propiedades 5 y 6), esto es $\omega \subseteq ON$. Además, de aquí se obtiene que $\in$ es tricotómica en ω y que ésta es bien fundada. Ahora, si $x \in y$ y $y \in \omega$, entonces y es un ordinal, por lo que $x \subseteq y$. Así, dado cualquier $z \in x$, se cumplirá que $z \in y$, de donde $z = 0 \vee \exists w \in ON[z = S(w)]$. Por lo tanto

[9]Un poco más extendida: $n \in \omega \Leftrightarrow \forall \alpha[(\alpha \in n \vee \alpha = n) \Rightarrow (\alpha = 0 \vee \exists \beta \in ON[\alpha = S(\beta)])]$.

[10]Originalmente Peano postuló sus axiomas utilizando lógica de segundo orden para el de inducción. Con esto, recursivamente se pueden definir la suma, la multiplicación y, en general, la aritmética básica en los naturales. No obstante, para que en lógica de primer orden se obtengan los mismos axiomas, deben agregarse símbolos en la signatura para la suma $+$ y la multiplicación $\cdot$, además de axiomas que definan el comportamiento de éstas en los naturales.

$x \in \omega$, i.e. ω es una clase transitiva. Con esto culmina la prueba de que si ω fuese un conjunto, entonces sería un ordinal. Para los axiomas de Peano, trivialmente se obtiene que (I) $0 \in \omega$, mientras que la prueba de (II) $n \in \omega \Rightarrow S(n) \in \omega$ es directa. Para el tercer postulado si $m \neq n$, entonces $m < n$ ó $n < m$ (por tricotomía). Si $m < n$ entonces $S(m) \leq n < S(n)$, ergo $S(m) \neq S(n)$. El otro caso procede análogamente y, por contrarrecíproca, (III) $S(m) = S(n) \Rightarrow m = n$. Por otro lado si $0 = S(x) = x \cup \{x\}$, entonces $x \in 0 = \emptyset$, lo cual es una contradicción y, por ende, (IV) $\forall n[\neg(0 = S(n))]$. Finalmente, supóngase que K cumple las hipótesis de (V) y que existe un natural n tal que $n \notin K$. Entonces $n \neq 0$, de donde $n = S(m)$ para algún ordinal m. Por transitividad de la clase ω y porque $m < n$, $m \in \omega$. Además, por contrarrecíproca $m \notin K$, lo cual significa que $n \setminus K \neq \emptyset$. No obstante, $n \setminus K \subseteq ON$, y por buena fundación de ésta, existe el mínimo x de $n \setminus K$ respecto a la relación épsilon, de pertenencia en dicho conjunto. Así, por transitividad de ω, x es un natural que no está en K. Repitiendo el argumento existiría $y \in ON$ tal que $x = S(y)$ y $y \notin K$; pero x era el mínimo que cumplía esto, por lo que no debe existir $n \in \omega$ tal que $n \notin K$, i.e. (V) $\forall K[(0 \in K \wedge \forall n \in \omega[n \in K \Rightarrow S(n) \in K]) \Rightarrow \omega \subseteq K]$. ■

Obsérvese que el concepto de número natural fue desarrollado sin necesidad del axioma del potencia, por lo que $x \in \omega$ es perfectamente definible en Z^*. Además, gracias a éste ahora es posible definir formalmente el concepto de "finitud", pues siguiendo a Cantor, la inyectividad, sobreyectividad y biyectividad de las funciones son las que determinan qué conjunto es "más grande" o de "igual tamaño" que otro[11]:

Definición III.6 (Cardinalidad y Finitud)
Para cualesquiera conjuntos X y Y:

- La expresión $X \preceq Y$ ó $|X| \leq |Y|$ leída como "X *tiene menor cardinalidad que* Y" significa que existe f tal que $f : X \rightarrowtail Y$.
- Se dice que "X *es equipotente con* Y" o que "X *tiene la misma cardinalidad que* Y", denotado por $X \approx Y$ ó $|X| = |Y|$,[12] si existe f tal que $f : X \twoheadrightarrow Y$.
- Se escribe $X \prec Y$ siempre que $X \preceq Y$ y $\neg(X \approx Y)$.
- Se define el predicado "X *es finito*" mediante la expresión $\exists n \in \omega[n \approx X]$ y, por ende, "X *es infinito*" si y sólo si X no es finito.

No es difícil ver que la equipotencia $\approx$ "es una relación de equivalencia". Por otro lado, por el teorema de Cantor-Berstein-Schröder ($A \approx B \Leftrightarrow A \preceq B \wedge B \preceq A$), la relación $\preceq$ es una especie de "orden parcial" sobre alguna subclase de V.

[11]No obstante lo dicho al principio del párrafo, para trabajar cómodamente con cardinalidades se requiere de un axioma que derive la existencia de productos cartesianos, pues si $f : A \to B$, entonces $f \subseteq A \times B$.

[12]Esta segunda notación se prefiere cuando, agregando algunos axiomas, se ha probado que "dado cualquier conjunto X, existe un único ordinal que es equipotente con tal conjunto", en cuyo caso a ese único ordinal se le denota por $|X|$.

Con esto se han desarrollado los conceptos más fundamentales en matemáticas, i.e. relaciones, funciones, colecciones (conjuntos) y números naturales. No obstante, imagínese que se desean construir los enteros o los racionales positivos a partir de los naturales. Es bien sabido que el proceso estándar para esto es por medio de clases de equivalencia $[(m,n)]_\sim$ ó $[(m,n)]_\approx$ sobre parejas de naturales respecto a las relaciones "$(a,b) \sim (c,d)$ sii $a+d = b+c$" y "$(a,b) \approx (c,d)$ sii $a \cdot d = b \cdot c$". Como se vio previamente, el "conjunto" cociente de estas clases de equivalencia es un subconjunto del potencia de $\omega \times \omega$, del cual no se sabe si es un conjunto o no, porque ni siquiera se ha probado para la misma clase ω. Uno podría seguir tratando estos conceptos como abreviaciones de fórmulas, pero este enfoque podría considerarse impráctico dado que, en la praxis, no es nada extraño pensar en el conjunto de todos los números naturales. Por todo esto, se introduce el:

Definición III.7 (Axioma del Infinito)
El axioma del infinito establece que existe un conjunto inductivo, i.e. un conjunto I tal que $0 \in I$ y si $n \in I$ entonces $S(n) \in I$:

$$\exists I[\emptyset \in I \wedge \forall x \in I[S(x) \in I]]$$

De éste y el quinto postulado de Peano (el axioma de inducción) se deriva que todo número natural es un elemento de I. Así, por el esquema de especificación se define formalmente:

$$\omega := \{n \in I \mid \forall \alpha[(\alpha \in n \vee \alpha = n) \Rightarrow (\alpha = 0 \vee \exists \beta \in ON[\alpha = S(\beta)])]\}$$

En una presentación tradicional de los axiomas expuestos hasta ahora, se podrían extraer los números naturales directamente del axioma del infinito. La técnica consiste en introducir la definición $I(x) \Leftrightarrow \emptyset \in I \wedge \forall x \in I[S(x) \in I]$, i.e. el predicado "ser conjunto inductivo" y tomar la "intersección de todos los conjuntos inductivos". Por el riesgo de que la clase de todos los conjuntos inductivos sea propia, se afirma primero la existencia de uno de éstos I por el axioma del infinito y, posteriormente, se define:

$$\omega := \{x \in I \mid \forall J[I(J) \Rightarrow x \in J]\}$$

Obsérvese que ω (bajo esta definición) es el "mínimo" conjunto inductivo pues $0 \in J$ para cada inductivo J, ergo también es elemento de ω. Si x es un elemento de ω, entonces x es elemento de todos los conjuntos inductivos y, precisamente por eso, $S(x)$ también lo es. De esto que $S(x) \in \omega$ y, por ende, $I(\omega)$. Fácilmente se verifica que $\omega \subseteq J$, para cualquier J tal que $I(J)$. Esta última presentación del conjunto ω permite probar rápidamente el principio de inducción para los números naturales pues si $J = \{x \in \omega \mid \varphi(x)\}$ es un conjunto inductivo, entonces por lo recientemente probado $\omega \subseteq J$ y, por ende, $\omega = J$.

Ahora que se ha presentado el axioma del infinito, se da otro nombre para la teoría desarrollada hasta el momento:

Definición III.8 (Primera Teoría de Conjuntos de Zermelo)
Se llamará *(primera) teoría de Zermelo*, Z^{**}, a la teoría cuyos axiomas no lógicos son:

- Extensionalidad: $\forall z[(z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y]$.
- Especificación: $\exists Z \forall x[x \in Z \Leftrightarrow (x \in Y \wedge \varphi(x))]$.
- Par: $\exists P[x \in P \wedge y \in P]$.
- Unión: $\exists U \forall Y \forall x[x \in Y \wedge Y \in \mathcal{F} \Rightarrow x \in U]$.
- Potencia: $\exists P \forall Y[Y \subseteq X \Rightarrow Y \in P]$.
- Infinito: $\exists I[\emptyset \in I \wedge \forall x \in I[S(x) \in I]]$.

De las propiedades de los números naturales se obtiene que $\omega \in ON$ y, más aún, que $S(\omega) = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\} \in ON$. Es claro que a partir de Z^{**} se pueden seguir construyendo n sucesores de ω, denotando $\omega + n$ al n-ésimo sucesor de ω, y siendo todos ellos ordinales. De manera más formal: se puede definir una función clase $F : \omega \to V$ tal que $F(0) = \omega$ y $F : S(n) \mapsto F(S(n)) := S(F(n)) = w + S(n)$. Este tipo de funciones clase con dominio el conjunto de los números naturales, i.e. sucesiones, son muy comunes en matemáticas y es común requerir que estas sean conjuntos. En el caso de que las funciones sean subconjuntos del producto cartesiano de dos conjuntos no hay ningún inconveniente, pues comprensión restringida resuelve el problema; no obstante, si el codominio de la función es una clase propia, como en el caso de F, la existencia del conjunto no es posible. Cuando Zermelo presentó sus axiomas, Adolf Fraenkel y Throralf Skolem se percataron de que en Z^{**} no se podía probar la existencia del conjunto de las n-ésimas potencias del conjunto de los naturales de Zermelo, $W := \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots\}$, i.e. no se podía demostrar la existencia de $\{W, \mathcal{P}(W), \mathcal{P}(\mathcal{P}(W)), \ldots\}$. Por esta razón, ambos autores propusieron el siguiente esquema como un posible[13] axioma de la teoría de conjuntos:

Definición III.9 (Esquema de axioma de reemplazo)
Informalmente el *esquema de axioma de reemplazo* establece que si la clase F, definida por $F = \{(x, y) \mid \varphi(x, y)\}$, es una función en el conjunto A, entonces la imagen directa de A bajo F, $F[A]$, es un conjunto.[14] Formalmente, dada una *wff* $\varphi \in \mathcal{L}$ cuyas variables libres estén entre $w_1, \ldots, w_n, A, x, y$, siendo n un entero no-negativo, la siguiente *wff* es un axioma de la teoría de conjuntos:

$$\forall w_1, \ldots, w_n, A[\forall x \in A \exists! y[\varphi(x, y)] \Rightarrow \exists B \forall y[y \in B \Leftrightarrow \exists x \in A[\varphi(x, y)]]$$

[13]Tanto Fraenkel como Skolem parecían estar inciertos respecto a si el axioma de reemplazo debía agregarse como tal a la teoría de conjuntos: Fraenkel opinaba que “reemplazo era un axioma muy fuerte para la teoría general de conjuntos” y Skolem simplemente escribió “podríamos introducir” reemplazo, c.f. [Kan12].

[14]En palabras de Fraenkel: “si M es un conjunto y cada elemento de M es *reemplazado* por “un objeto en el dominio [de discurso]”, entonces M se convierte en un conjunto”.

Obsérvese que el axioma de reemplazo permite, al igual que en teoría informal de conjuntos, construir el conjunto de todos los objetos de la forma $F(x)$ con x un índice corriendo en el conjunto A y F, una función-clase. O sea, reemplazo afirma la existencia de conjuntos de la forma $\{F(x) \mid x \in A\}$. De aquí que en Z^{**} con reemplazo se puede probar la existencia del conjunto $\{\omega+n \mid n \in \omega\}$ y, tomando la unión de éste, el ordinal $\omega + \omega = \{0, 1, 2 \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$. También, gracias al axioma de reemplazo se tiene un método alternativo para construir el producto cartesiano de dos conjuntos:

Teorema III.4 (Reemplazo implica existencia de productos cartesianos) En una teoría restringida de Zermelo, Z^*, con esquema de axioma de reemplazo, dados dos conjuntos A y B, existe su producto cartesiano:

$$A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$$

Demostración. Dados dos conjuntos A, B, considérese la cadena de símbolos $\varphi(x, z) := (z = (x, y))$. Por reemplazo, $\exists(A \times \{y\})\forall z[z \in A \times \{y\} \Leftrightarrow \exists x \in A[z = (x, y)]]$, es decir, existe el conjunto $A \times \{y\} := \{(x, y) \mid x \in A\}$. Ahora denótese por $\psi(y, w)$ a la fórmula recientemente derivada, i.e. $\forall z[z \in w \Leftrightarrow \exists x \in A[z = (x, y)]]$, y aplíquesele el esquema de reemplazo. Se deriva la fórmula:

$$\exists C\forall w[w \in C \Leftrightarrow \exists y \in B\forall z[z \in w \Leftrightarrow \exists x \in A[z = (x, y)]]]$$

Que representa al conjunto $C := \{A\times\{y\} \mid y \in B\}$. Finalmente, por extensionalidad todo conjunto construido con reemplazo es único y particularmente C también. El resultado se obtiene definiendo $A \times B := \bigcup C$. ■

No obstante, reemplazo "trabaja" sobre conjuntos ya dados, de tal forma que construcciones permitidas en Z^* junto con el axioma del potencia, como la del potencia mismo (que es un supraconjunto de mayor cardinalidad), no son garantizadas por el esquema de axioma de reemplazo. A lo más, de lo derivado a partir del conjunto potencia, el axioma recientemente presentado permitiría definir los conjuntos cociente y las relaciones inversas.

Como se dijo al presentar el esquema de axioma de especificación, asumiendo los de extensionalidad, par, unión y la existencia del conjunto vacío se puede probar que:

Teorema III.5 (Reemplazo y existencia del vacío implican especificación) En una teoría axiomática con el esquema de axioma de reemplazo y la sentencia $\exists y\forall x[x \notin y]$, se deriva el esquema de axioma de especificación.

Demostración. Sea $\varphi \in \mathcal{L}$ con variables libres entre $x, w_1, \ldots, w_n, z$, siendo n un entero no-negativo y X un conjunto. Si ningún elemento de X satisface φ, entonces, como el vacío existe, se cumple que $\exists\emptyset\forall y[y \in E \Leftrightarrow y \in X \wedge \varphi(x)]$.[15]

En el caso en que sí hay un elemento $x \in X$ para el cual se satisfaga φ, defínase $\psi(x, y) = \varphi(x) \wedge x = y$. Por reemplazo se cumple:

$$\exists E\forall y[y \in E \Leftrightarrow \exists x \in X[\psi(x, y)]]$$

Es decir, existe el conjunto $E := \{y \mid \exists x \in X[\varphi(x) \wedge x = y]\}$. Es demostrable que $\exists x \in X[\varphi(x) \wedge x = y]$ es equivalente a $y \in X \wedge \varphi(y)$, de donde:

$$\exists E\forall y[y \in E \Leftrightarrow y \in X \wedge \varphi(y)]]$$

Que es el esquema de axioma de especificación. ■

Tanto Adolf Fraenkel como John von Neumann se percataron de que en Z^{**} no se prohibía la existencia de algún conjunto X que satisfaciese $X \in X$. Como se vio al presentar los ordinales, un clase de conjuntos que nunca pertenecen a sí mismos son *los conjuntos bien fundados*. En [Kun80] Kenneth Kunen prueba una serie de teoremas que indican que todas las matemáticas se llevan a cabo dentro de dicha clase. Por lo tanto, con el motivo de facilitar el estudio del universo V, es común que se agregue el axioma de fundación de von Neumann (posteriormente adaptado por Zermelo a su Z^{**}) a las teorías de conjuntos:

Definición III.10 (Axioma de regularidad)
Pensando, como Dmitry Mirimanoff, que un conjunto E es regular/ordinario cuando da lugar sólo a sucesiones finitas descendientes, i.e. $E_n \in \cdots \in E_1 \in E$ c.f. [All16], el axioma de regularidad dicta que sólo existen conjuntos regulares. Alternativamente, se puede afirmar que el axioma de regularidad dice que todos los conjuntos son "bien fundados":

$$\forall x[x \neq \emptyset \Rightarrow \exists y \in x[y \cap x = \emptyset]]$$

A pesar de agregar este enunciado como axioma, se suele afirmar que "regularidad nunca se necesita en el desarrollo de las matemáticas" [Kun09]. Obsérvese entonces que, al menos desde el axioma del potencia, los axiomas por agregar se han tornado más y más controversiales, en el sentido de que adoptarlos implica tomar una postura filosófica respecto al universo de todos los conjuntos V. Por ejemplo, uno podría escoger entre el axioma del potencia y el esquema de reemplazo con el axioma de infinito. Similarmente, hay una corriente filosófica, denominada finitista, que rechaza la existencia de cualquier conjunto infinito y, en consecuencia, hay axiomatizaciones finitistas de la teoría de conjuntos. En general, cada axioma agregado desde el del infinito ha sido para que la teoría de conjuntos se adapte a la manera en la que trabajan los matemáticos. Otros dos ejemplos de enunciados que podrían agregarse como axiomas son:

[15] Esta condición de la existencia del vacío puede ser removida si se considera la siguiente variación al axioma de reemplazo:

$$\forall w_1, \ldots, w_n[\forall x, y, z[\varphi(x, y) \wedge \varphi(x, z) \Rightarrow y = z] \Rightarrow \forall A\exists B\forall y[y \in B \Leftrightarrow \exists x \in A[\varphi(x, y)]]$$

Definición III.11 (Axioma de Elección y la Hipótesis del Continuo)
El axioma de elección, denotado AC por su nombre en inglés (axiom of choice), afirma que dada una familia de conjuntos no vacía F, existe una función de elección f definida en F, es decir, una función tal que para cada $X \in F$, la imagen de X bajo f es un elemento de X, i.e. $f(X) \in X$. Formalmente:

$$\forall F[F \neq \emptyset \Rightarrow \exists f[f : F \to \bigcup F \wedge \forall X \in F[f(x) \in X]]]$$

Por otra parte, sabiendo en Z^{**} que la cardinalidad de un conjunto siempre es menor que la de su potencia, i.e. $|X| < |\mathcal{P}(X)|$ para cada conjunto X, la hipótesis del continuo CH afirma que no hay un conjunto cuya cardinalidad esté estrictamente entre la de ω y su potencia $\mathcal{P}(\omega)$, i.e:

$$\neg\exists X[|\omega| < |X| \wedge |X| < |\mathcal{P}(\omega)|]$$

Se aprovecha esta definición para explicar las notaciones más utilizadas al referirse a diversas teorías de conjuntos:

Definición III.12 (Teoría de Conjuntos Zermelo-Fraenkel-Choice y variantes)
La teoría de conjuntos ZFC, es la teoría cuyos axiomas no lógicos son:

1. Extensionalidad: $\forall z[(z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y]$.
2. Regularidad: $\forall x[x \neq \emptyset \Rightarrow \exists y \in x[y \cap x = \emptyset]]$.
3. Especificación: $\exists Z \forall x[x \in Z \Leftrightarrow (x \in Y \wedge \varphi(x))]$.
4. Par: $\exists P[x \in P \wedge y \in P]$.
5. Unión: $\exists U \forall Y \forall x[x \in Y \wedge Y \in \mathcal{F} \Rightarrow x \in U]$.
6. Reemplazo: $\forall x \in A \exists! y[\varphi(x,y)] \Rightarrow \exists B \forall y[y \in B \Leftrightarrow \exists x \in A[\varphi(x,y)]$.
7. Infinito: $\exists I[\emptyset \in I \wedge \forall x \in I[S(x) \in I]]$.
8. Potencia: $\exists P \forall Y[Y \subseteq X \Rightarrow Y \in P]$.
9. Elección: $\forall F[F \neq \emptyset \Rightarrow \exists f[f : F \to \bigcup F \wedge \forall X \in F[f(x) \in X]]]$.

La teoría de Zermelo-Fraenkel es ZFC sin el axioma de elección. Por otra parte, la teoría de Zermelo, Z, y la de Zermelo-Elección, ZC, son respectivamente ZF y ZFC sin el esquema de reemplazo. Similarmente, $\mathrm{Z}^{-}, \mathrm{ZF}^{-}, \mathrm{ZC}^{-}$ y ZFC^{-} son Z, ZF, ZC y ZFC sin el axioma de regularidad. Si se desea eliminar el axioma del potencia a alguna teoría se escribe el nombre de ésta concatenado con la terminación "$-$P", por ejemplo, ZFC sin el potencia se denota ZFC$-$P. Más aún, si se desea agregar un enunciado a la teoría, como la hipótesis del continuo CH, se añade el nombre de éste junto con el signo "$+$", por ejemplo, ZFC con la negación de la hipótesis del continuo se representa por ZFC$+\neg$CH.

Kurt Gödel construyó un modelo para ZFC+CH, esto es, probó que ZFC+CH es consistente. Por medio de su revolucionaria técnica del *forcing*, Paul Cohen probó que ZF¬C y ZFC+¬CH también son consistentes. Con estas pruebas de consistencia, correspondía a los matemáticos decidir cuál de las tres "teorías de conjuntos" eligirían como fundamento para las matemáticas (o escoger una axiomatización ajena a los conjuntos). Adoptar el axioma de elección fue una decisión fácil pues su utilización tiene consecuencias matemáticas agradables como que "todo espacio vectorial tiene una base" o la caracterización de puntos de acumulación de un subconjunto de reales A por medio de la existencia de una sucesión en A que convergiese al punto o por medio de la intersección no vacía de A con un intervalo abierto de radio un real positivo y centro en el punto. Por otro lado, sigue sin escogerse alguno de los dos enunciados, la hipótesis del continuo o su negación, como parte de la axiomatización de las matemáticas. Inlcuso algunos investigadores de la teoría de conjuntos creen que, ya que familiarizarse con diversas axiomatizaciones de V es fácil, realmente la postura adecuada para adoptarse es la creencia en un *multiverso* de la teoría de conjuntos. [Ham11]

Con lo presentado hasta ahora se ha mostrado evidencia en favor de que las matemáticas son axiomatizables dentro de un sistema formal $\mathscr{F}$. Si en algún momento ZFC se considerase inadecuada o insuficiente para dicha labor, los matemáticos pueden confiar en que su trabajo puede formalizarse en una teoría alterna o que se pueden agregar más axiomas. Un ejemplo de esto es lo que ocurrió cuando la *teoría de categorías* tomó relevancia en diversas áreas de las matemáticas. Como varias categorías requieren considerar clases propias como entes formados, una teoría de conjuntos como NBG que las axiomatiza o una teoría de conjuntos con axiomas enunciados con conceptos categóricos (como la teoría elemental de la categoría de los conjuntos de Lawvere -ETCS-) fue suficiente para que los matemáticos estuviesen seguros de la precisión y el rigor de lo que hacen.

En el siguiente capítulo se presenta un sistema formal para axiomatizar a las matemáticas que no está basado en una teoría de conjuntos. Al igual que en el presente capítulo se presentará inicialmente y de manera informal lo que diversas notaciones representan y posteriormente se presentará el sistema formal y la implementación de las matemáticas en dicha teoría.

Capítulo 4

Teoría de Tipos-Homotopías

En capítulos anteriores se llevó a cabo el proceso de formalización de las matemáticas dentro de una teoría base: la teoría de conjuntos. En el presente capítulo, se efectúa un proceso similar; salvo que se adopta la postura de que los conceptos matemáticos fundamentales ya vienen dados desde el sistema formal. Más concretamente, cada variable y/o constante introducida tendrá inmediatamente un *tipo* asociado. Por ejemplo, se asume que al hablar del número 0, el tipo de éste es el tipo de los *números naturales* $\mathbb{N}$, y se podría derivar en algún momento que si x es una variable del mismo tipo, denotado por $x : \mathbb{N}$, entonces $x + 0 = x$ en dicho tipo. La situación es parecida (y de hecho comparte los mismos fundamentos) a la declaración de variables al escribir el código de programas de computadora, en los cuales, de acuerdo al tipo de variable utilizada, el programa podrá o no implementar el algoritmo descrito por el código.

Con base en lo recientemente dicho, el presente capítulo sirve como evidencia extra para argumentar que la formalización de (una parte de) las matemáticas es posible, además, sirve como ejemplo para determinar que ésta no es única.

I. Introducción Histórica y Motivación Práctica

La *teoría de tipos* comienza aproximadamente al inicio del siglo XX con el descubrimiento de diversas paradojas en algunos sistemas formales. El método usual para "bloquear" varias de ellas consiste en evitar la auto-referencia. Por ejemplo, en el idioma español es fácil construir la expresión paradójica "*esta oración es falsa*" cuyo elemento auto-referente es que la oración está hablando de ella misma. Para evadir estas paradojas dentro de las matemáticas, Bertrand Russell y Alfred North Whitehead propusieron, en sus trabajos *Principia Mathematica*, la creación de una jerarquía de *tipos* o propiedades, la cual cumplía que cada nuevo ente construido sólo podía hacer referencia a objetos en niveles inferiores de la jerarquía; de esta manera, la expresión "*esta oración es falsa*" estaría mal construida en el lenguaje de la teoría de tipos y no existiría ninguna paradoja. La comunidad académica más interesada en los *Principia Mathematica* fue la filosófica, mientras que la comunidad matemática optó por evitar las paradojas por medio del esquema de axioma de especificación presente en la teoría de conjuntos de Ernst Zermelo.

Posteriormente Alonzo Church, como parte de sus investigaciones en los fundamentos de las matemáticas, desarrolló su *Cálculo Lambda*. Las aplicaciones de éste y su éxito en las ciencias computacionales hicieron que varios individuos, como Stephen Kleene, lo estudiaran y encontraran inconsistencias lógicas en forma de paradojas. Motivado por esto Church propuso dos sistemas: el primero fue el λ-cálculo original pero restringido únicamente a la parte relevante para la computación, ahora conocido como *Cálculo Lambda No Tipificado*, y el segundo fue un sistema dónde evadía las paradojas con el mismo método desarrollado por Russell y Whitehead ahora llamado *Cálculo Lambda Simplemente Tipificado*. Más tarde surgieron diversas modificaciones a este sistema que se convirtieron en las primeras teorías de tipos modernas. El desarrollo de éstas se vio incrementado tras el descubrimiento, por parte de Haskell Curry, de una correspondencia entre las deducciones en algunas lógicas y las computaciones efectuadas dentro de algunas teorías de tipos. Posteriormente, William Alvin Howard reenunciaría esto como un isomorfismo entre la deducción natural en lógica intuicionista y los cómputos en la teoría de tipos. Más adelante, a esta correspondencia Joachim Lambek le agregaría una relación con la teoría de categorías, razón por la cual hoy es conocida como la *Correspondencia Curry-Howard-Lambek*. El descubrimiento de esta relación permitió la construcción de más teorías de tipos a partir de ciertas lógicas y viceversa. En las décadas de los 70's y 80's Per Erick Rutger Martin-Löf creó una teoría de tipos que correspondía a la lógica de predicados intuicionista por medio del empleo de "tipos dependientes", por esta razón actualmente es llamada teoría de tipos intuicionista/constructiva/dependiente o, simplemente, *Teoría de Tipos de Martin-Löf* (MLTT). Algunas variantes de esta teoría, por ser consistentes y decidibles, son empleadas en la teoría de lenguajes de programación, y en la programación de *asistentes de prueba*.

Los asistentes de prueba son programas diseñados para formalizar detalladamente los razonamientos matemáticos y para verificar que las deducciones realizadas sean congruentes con los axiomas planteados. De esta manera, se reduce el riesgo de un error humano en alguna demostración de un teorema abstracto y complejo. En la investigación matemática es común que los detalles técnicos y formales de las pruebas no sean verificados minuciosamente sino que son respaldados por la reputación del autor. Esto implica que si algún trabajo de algún matemático reconocido mundialmente tiene un error, otros trabajos que dependen de éste tengan el riesgo de arrastrar el error consigo. Un ejemplo de esto lo dio Vladimir Voevodsky (cf. [Voe14]), ganador de una Medalla Fields y uno de los fundadores de la *Teoría de Tipos-Homotopías* HoTT (Homotopy Type Theory). Voevodsky señala que alrededor de 1993 escribió un artículo titulado "*Cohomological Theory of Presheaves with Transfers*" el cual tenía un defecto muy sutil en la demostración de un lema clave para el argumento del artículo. Sin embargo, este error no fue encontrado sino hasta siete años después por el mismo Voevodsky mientras realizaba una serie de pláticas sobre el tema en el Instituto de Estudios Avanzados de Princeton. Él afirma que varios matemáticos habían estudiado su artículo desde 1993 y ninguno se había dado cuenta del error, lo cual infundió incertidumbre en Voevodsky respecto a las demostraciones complejas que había realizado a lo largo de su vida y las que tendría que hacer en el futuro para llevar a cabo sus investigaciones. Por ello decidió utilizar asistentes de prueba para ayudarlo con sus demostraciones, los cuales habían sido estudiados y desarrollados desde la década de 1960. Cuando empezó a investigar encontró distintos asistentes de prueba basados en diversas teorías: el sistema Mizar, por ejemplo, está basado "bellamente" -según Voevodsky- en los fundamentos actuales de las matemáticas, la teoría de conjuntos ZFC; pero no le satisfizo como un software de verificación de pruebas. El sistema *Automath* por otra parte, escrito por Nicolaas de Bruijin y basado en las teorías de tipos dependientes, "fue capaz de verificar un libro de texto de Análisis Matemático en relativamente poco tiempo" [Voe14].

A pesar de las aplicaciones de los sistemas de tipos dependientes, su carácter sintáctico generó poco interés del lado de la investigación semántica hasta que en 2006, Michael Warren, su asesor Steve Awodey, Voevodsky y otros encontraron modelos basados en teoría de categorías y *teoría de homotopías* (modelos de Quillen) para esta clase de sistemas. Gracias a ello, se prestó más atención a los tipos dependientes, que proveyeron un método sintáctico para demostrar propiedades y teoremas en la teoría de homotopías. Con el estudio de estos modelos surgió la variante de MLTT, denominada *Teoría de Tipos-Homotopías* (HoTT), que incluye el *axioma de univalencia* de Vladimir Voevodsky y la posibilidad de definir tipos de inducción-más-alta. Esta variante es la teoría emblema para el *programa de Fundamentos Univalentes* de Voevodsky el cual -según Awodey- consiste en "hallar un fundamento comprehensivo y computacional para las Matemáticas basado en la interpretación homotópica de la Teoría de Tipos" [Awo14].

En este capítulo se presenta la variante de MLTT oficialmente expuesta en el libro de Teoría de Tipos-Homotopías, HoTT, por el Programa de Fundamentos Univalentes. Antes de presentar la sintaxis del sistema, se expondrán la interpretación original de éste, así como algunas de las razones que motivaron a Per Martin-Löf a construir su teoría de tipos dependientes.

II. Interpretación Original y Motivación Filosófica

Una de las principales observaciones que se deben hacer al hablar de teorías de tipos es recordar la distinción original por Gottlob Frege entre un juicio y una proposición[1]: la segunda es una aseveración dentro de alguna teoría mientras que la primera es una aseveración (metalógica) de la veracidad de alguna proposición. Para ejemplificar esta distinción considérese la expresión "*el león es feroz*": ya que

[1]Estas ideas fueron posteriormente reemplazadas por las "más formales" fórmula bien formada (*wff*) y teorema (de un sistema formal).

ésta puede ser evidenciada y no hace referencia a ningún otro enunciado, es posible llamarla proposición. Por otro lado, la oración "*es verdad que 'el león es feroz'*" corresponde a un juicio pues se está afirmando la veracidad de la proposición anterior. Esto queda brevemente esquematizado por el diagrama siguiente:

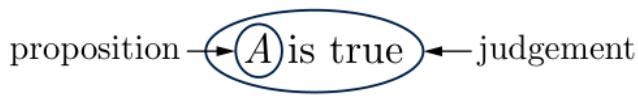


Fig. 1 tomada de [ML84]

Posteriormente es necesario notar que una deducción lógica se hace a partir de juicios, por ejemplo, cuando en deducción natural (en lógica) se usa la regla de introducción de la disyunción (*de A se deduce que A ó B*):

$$\frac{A}{A \vee B} \vee \text{-Intro}$$

realmente se está aseverando (*si A es proposición y B es proposición y A es verdadera, entonces A ó B es una proposición verdadera*), i.e:

$$\frac{A\text{: Prop.} \qquad B\text{: Prop.} \qquad A \text{ is True}}{A \vee B \text{ is True}} \vee \text{-Intro}$$

o con la notación de capítulos previos:

$$\frac{A, B \in \mathcal{L} \qquad \vdash A}{\vdash A \vee B} \vee \text{-Intro}$$

Con base en esto, el objetivo de Per Martin-Löf al desarrollar su teoría de tipos fue crear un sistema formal donde éstos hechos implícitamente tratados en otras teorías fuesen explícitos en la suya. Esta elección logra que MLTT tenga algunas ventajas computacionales y constructivas sobre otras teorías fundamentales y, a la par, hace que MLTT tenga un "único nivel" de deducción, a diferencia de la tradicional lógica de primer orden (FOL por sus siglas en inglés: first order logic) con teoría de conjuntos (FOL+ZFC) que consiste en "dos niveles": el deductivo (lógica) y el axiomático (conjuntos).

En el sistema del libro HoTT existen tres tipos de juicios que corresponden a las <u>expresiones bien formadas</u> de dicho sistema formal:

- El primer juicio es "Γ es un contexto", denotado por Γctx.[2]
- El segundo, "a es un término del tipo A involucrando variables en el contexto Γ", formalmente escrito como $\Gamma \vdash a : A$.[3]

[2]Aquí Γ es un metasímbolo para una sucesión de *wffs* de la forma: $x_1 : A_1, x_2 : A_2, \ldots, x_n : A_n$.
[3]Per Martin-Löf entendía esto como "a es un elemento del conjunto A" y lo denotaba por $a \in A$.

- El tercero y último es "a y b son términos (definicionalmente/juzgadamente) iguales en el tipo A con base en las variables del contexto Γ", formalizado mediante $\Gamma \vdash a = b : A$.[4]

En la construcción de MLTT, Per Martin-Löf considera otros dos juicios: $A\,\mathrm{Set}$ y $A = B$ que significan "A es un tipo (conjunto)" y "A y B son tipos (conjuntos) iguales" respectivamente. No obstante en HoTT los autores decidieron expresar esto mediante una jerarquía de tipos-universo $\mathcal{U}_1, \mathcal{U}_2, \ldots$ donde dichos enunciados son sustituidos por "*A es un tipo en el universo (de acuerdo al contexto* Γ*)*" y "*A y B son tipos iguales en el universo (con base en variables del contexto* Γ*)*, es decir, los juicios $\Gamma \vdash A : \mathcal{U}_i$ y $\Gamma \vdash A = B : \mathcal{U}_i$ (para algún índice i). Más aun, algunos otros consideran que MLTT, por su uso particular de tipos dependientes, tiene otras dos formas de juicios, a decir, $x : A \vdash P(x) : \mathcal{U}_i$ y $x : A \vdash f(x) : P(x)$ que corresponden a los enunciados "$P(x)$ es un tipo (en el universo) para cada $x : A$" y "$f(x)$ es un término en $P(x)$ para cada $x : A$" (cf. [Rij12]). En el caso de HoTT, estos enunciados son derivables a partir de las reglas de inferencia del sistema y representan un caso particular del juicio "$\Gamma \vdash a : A$". La idea de un tipo dependiente como los previamente señalados, puede ser ejemplificada con los tipos $\mathbb{R}^n$, que son tipos cuyos "elementos" son n-tuplas pero cuyas entradas dependen de los términos de otro tipo, i.e. $n : \mathbb{N}$.

Adicionalmente, es necesario destacar que hay diferencias importantes entre las teorías de tipos y las teorías de conjuntos. Por ejemplo, obsérvese que en MLTT a cada término le corresponde un único tipo de manera predeterminada a diferencia de FOL+ZFC donde "ser elemento de" es una relación que puede ocurrir (o no) entre dos objetos cualesquiera. Otra diferencia importante es que en FOL+ZFC las expresiones $a \in A$ y $a = b$ son proposiciones mientras que aquí se han vuelto juicios. Esto lleva a que en la formalización de la teoría, la expresión $a = b$ sea una noción sintáctica. Más adelante se verá que la correspondencia Curry-Howard-Lambek motiva el empleo de otros tipos denominados *tipos identidad* (o igualdades proposicionales) por lo que otra diferencia clave entre FOL+ZFC y MLTT es que en la primera sólo se tiene una igualdad mientras que en la segunda se tienen dos igualdades, la proposicional y la *definicional*. Esta diferencia en cómo tratar las igualdades hace que a MLTT se le llame una teoría *intensional* y a FOL+ZFC, *extensional* (cf. [LP14]). La distinción entre ambos términos consiste en que una teoría extensional, declara iguales dos objetos si sus extensiones son las mismas, es decir, en FOL+ZFC dos distintas descripciones hablan de un mismo conjunto si y sólo si "las colecciones" cuyos objetos cumplen dichas descripciones, son las mismas. Por otra parte, una teoría intensional como MLTT declara iguales dos objetos si sus intensiones son las mismas, lo que simplemente significa que dos distintas descripciones nos darán dos distintos tipos. Un ejemplo burdo para ilustrar esto es considerar las descripciones "animal de cuatro patas que hace 'guau"' y "el mejor amigo del hombre"; aunque las extensiones de ambas

[4] De manera similar, para Martin-Löf esto significaba que "a y b son elementos iguales en el conjunto A", escrito por $a = b \in A$.

descripciones son el mismo ente (el perro), las intensiones no son las mismas.[5]

Antes de proceder a exponer los principales constructos en la teoría de tipos dependientes, se hace hincapié en que, para hacer sencilla la exposición semántica de su lenguaje, se utilizarán expresiones informales (tal y como se hace usualmente en matemáticas). En otras palabras, sólamente en la sección del "desarrollo formal de (el sistema formal) HoTT y motivación en los fundamentos", se utilizarán en su totalidad todos los términos bien formados necesarios para generar una teoría computable.

I. Tipo de Funciones Dependientes

Asumiendo que $A : \mathcal{U}$ (A es un tipo) y que por cada "elemento" $x : A$ (término de tipo A) existe un tipo $B(x) : \mathcal{U}$, siempre se puede construir el *producto* de éstos indizado por $A : \mathcal{U}$, mejor conocido como el *tipo de funciones dependientes*[6]:

$$\prod_{x:A} B(x) : \mathcal{U}$$

Más aun, si para cada $x : A$ se cumple que $f(x) : B(x)$, entonces la función definida por la λ-expresión $\lambda x.f(x)$ es de tipo $\prod_{x:A} B(x)$. Recuérdese aquí que escribir $\lambda x.f(x)$ es equivalente a nombrar a la función con regla de correspondencia $f : x \mapsto f(x)$[7] y, por ende, al evaluarla se obtiene el cómputo $(\lambda x.f(x))(a) = f(a)$[8]. En otras palabras, los únicos "elementos" de un tipo producto son funciones cuyo dominio es $A : \mathcal{U}$ y sus imágenes viven en cada uno de los correspondientes $B(x) : \mathcal{U}$. Por ende, para obtener elementos de alguno de los $B(x) : \mathcal{U}$ lo único que se debe hacer es evaluar a $f : \prod_{x:A} B(x)$ en un valor determinado de $A : \mathcal{U}$. Por ejemplo, si $a : A$ entonces $f(a) : B(a)$. Es importante recordar también que dos funciones son iguales si sus dominios y reglas de correspondencia son las mismas, esta característica de las funciones es explícitamente dada para cada tipo de funciones dependientes; así si para cada $x : A$, se cumple que la expresión $b(x) = b'(x) : B(x)$ entonces $\lambda x.b(x) = \lambda x.b'(x) : \prod_{x:A} B(x)$.

Finalmente, obsérvese que la condición crucial para construir al tipo producto es la existencia de la familia $\{B(x) : \mathcal{U} \mid x : A\}$, por lo que haciéndola constante, $B(x) = B : \mathcal{U}$ para cada $x : A$, se obtiene el caso específico del *tipo de funciones "no-dependientes"*:

$$A \to B = A^B := \prod_{x:A} B : \mathcal{U}$$

[5]La distinción entre ambos conceptos es crucial para que MLTT sea una teoría decidible y adquiera un carácter computable: en la práctica estamos limitados por lo que podemos demostrar (o hemos demostrado hasta el momento) y tiene sentido considerar distintas (o no relacionadas) a dos intensiones, hasta que se demuestre lo contrario.

[6]Nótese que el alcance del símbolo "Π" es interrumpido por los dos puntos ":" junto a la $\mathcal{U}$, i.e. el "operador" principal en la expresión son dichos puntos.

[7]Una regla conocida como η-conversión o η-reducción.

[8]A esta regla se le conoce como β-conversión o β-reducción.

II. Tipo de Parejas Dependientes

Al igual que para las funciones dependientes, un tipo índice $A:\mathcal{U}$ y una familia de tipos $B(x):\mathcal{U}$, con $x:A$, son lo único que se requiere para crear al *tipo de parejas dependientes* denotado como *la suma* de dicha familia:

$$\sum_{x:A} B(x) : \mathcal{U}$$

El objetivo original al concebir este tipo era tener un análogo a la unión disjunta de conjuntos; no obstante, su característica principal es que sus "elementos", i.e. sus variables correspondientes, son parejas ordenadas $\langle a, b\rangle : \sum_{x:A} B(x)$ donde la primera coordenada es una expresión $a : A$ mientras que la segunda varía dependiendo de la primera $b : B(a)$. Para lograr que los únicos elementos de estos tipos sean dichas parejas se enuncia el *principio de inducción para parejas dependientes*, el cual establece que "dada una familia $Q(p):\mathcal{U}$ con $p : \sum_{x:A} B(x)$, construir una función que vaya de la suma a la familia, $f : \prod_{p:\sum_{x:A} B(x)} Q(p)$, sólo requiere tener otra análoga $g : \prod_{a:A}\prod_{b:B(a)} Q(a,b)$ que sea evaluada iteradamente", proceso conocido como *currying*. Es decir, si $a : A$ y $b : B(a)$ entonces realmente $f(a,b) = g(a)(b) : Q(a,b)$. Partiendo de esto, es posible "probar" informalmente el siguiente lema:

Lema II.1 (*Existencia de las proyecciones canónicas*)
En la teoría de tipos intuicionista, para cada tipo $B(x):\mathcal{U}$ dependiente de algún $A:\mathcal{U}$, existen las *proyecciones canónicas*:

- $\pi_1 : \left(\sum_{x:A} B(x)\right) \to A$ tal que $\pi_1(a,b) := a$
- $\pi_2 : \prod_{p:\sum_{x:A} B(x)} B(\pi_1(p))$ tal que $\pi_2(a,b) := b$

Demostración. Supóngase ya dado $p : \sum_{x:A} B(x)$ y considérese a la familia (constante) $Q_1(p) = A:\mathcal{U}$. Es fácil ver que la función que se necesita para aplicar el principio de inducción y construir a π_1 tal como se desea es $g_1 = \lambda a.\lambda b.a : \prod_{a:A}\prod_{b:B(a)} A$. Para la segunda proyección se debe hacer la observación de que $\pi_1(p) : A$ para cada $p : \sum_{x:A} B(x)$, por lo que $Q_2(p) = B(\pi_1(p)) : \mathcal{U}$ es una familia indizada por la suma. Definiendo a $g_2 = \lambda a.\lambda b.b : \prod_{a:A}\prod_{b:B(a)} B(\pi_1(a,b))$ y aplicando el principio de inducción para parejas dependientes se genera a π_2 como se requiere. ■

Finalmente, de forma análoga a la subsección anterior, si la familia de tipos $\{B(x):\mathcal{U} \mid x : A\}$ es constante, i.e. $B(x) = B:\mathcal{U}$ par cada $x : A$, entonces el tipo de parejas dependientes es simplemente el *producto cartesiano*:

$$A \times B := \sum_{x:A} B$$

III. Tipo Coproducto

Los *coproductos*, tal como en teoría de categorías, son el concepto dual al producto cartesiano y para formarlos únicamente se requiere de la existencia de dos tipos. Es decir, si $A, B : \mathcal{U}$ entonces:

$$A + B : \mathcal{U}$$

De igual manera, si las proyecciones canónicas π_1 y π_2 permiten "descomponer" los elementos de los tipos producto, entonces los tipos coproducto requieren de las *inclusiones canónicas* ι_1 y ι_2 para introducir sus elementos; más explícitamente: si $a : A$ y/o $b : B$, entonces $\iota_1(a) : A + B$ y/o $\iota_2(b) : A + B$.

Repitiendo la idea de la subsección anterior, el *principio de inducción para los tipos coproducto* dice que "dada una familia $Q(x)$ con $x : A+B$, para construir una función que vaya de $A+B : \mathcal{U}$ a la familia $f : \prod_{x:A+B} Q(x)$ sólo se requiere tener dos funciones previas $g_1 : \prod_{a:A} Q(\iota_1(a))$ y $g_2 : \prod_{b:B} Q(\iota_2(b))$", de tal modo que:

$$f(\iota_1(a)) = g_1(a) : Q(\iota_1(a))$$

$$f(\iota_2(b)) = g_2(b) : Q(\iota_2(b))$$

Esta manera de construir tipos por medios inductivos es característica de MLTT y será la forma en la que se construirán los restantes tres tipos fundamentales de la teoría.

IV. Tipo de Números Naturales

Hasta ahora sólo se han dicho qué tipos se pueden construir dados otros previamente existentes, el *tipo de números naturales* $\mathbb{N} : \mathcal{U}$ es el primer ejemplo de un tipo que es posible generar en cualquier momento sin necesidad de otros previos.

Los elementos del tipo de los naturales se construyen recursivamente como es estándar en otras teorías axiomáticas que los presentan, es decir, de facto ya se tiene que $0 : \mathbb{N}$ y que si $n : \mathbb{N}$, entonces $S(n) : \mathbb{N}$. Así mismo, el *principio de inducción para el tipo de los naturales* dice que "si $P(n) : \mathcal{U}$ es una familia indizada por los números naturales, i.e. $n : \mathbb{N}$, entonces para construir una función de los naturales a la familia $f : \prod_{n:\mathbb{N}} P(n)$ es suficiente con construir dos funciones que reflejen cómo se comporta ésta en el caso base $c_0 : P(0)$ y en el caso recursivo/inductivo $c_S : \prod_{n:\mathbb{N}} P(n) \to P(S(n))$" de tal modo que:

$$f(0) = c_0$$

$$f(S(n)) = c_S(n, f(n))$$

En la sección siguiente se explicará cómo se relaciona este principio inductivo con la inducción estándar realizada en matemáticas cotidianamente. Mientras tanto, se presenta al tipo vacío o nulo.

V. Tipo Vacío o Tipo Nulo

De igual manera que con los naturales, sin asumir nada más se puede formar al tipo vacío:

$$\emptyset : \mathcal{U}$$

Su utilidad se hace más clara tras analizar la correspondencia Curry-Howard entre teorías de tipos y lógicas intuicionistas pero por el momento sólo se expondrá el *principio de inducción para el tipo vacío* que en pocas palabras establece que $\emptyset : \mathcal{U}$ no tiene elementos y para ello se conviene que en el caso de que se hallase un término $z : \emptyset$, entonces cualquier tipo concebible estará habitado. Más explícitamente, "siempre que se tenga un tipo $Q : \mathcal{U}$, se puede construir una función $f : \prod_{z:\emptyset} Q(z)$" tal que:

$$f(z) : C(z)$$

VI. Tipo Unidad

Finalmente, el *tipo unidad* se puede formar sin ninguna hipótesis previa $\mathbf{1} : \mathcal{U}$ y el único elemento que se puede introducir de él es $\star : \mathbf{1}$. Con base en esto su *principio de inducción para el tipo unidad* reza que "si $Q(x) : \mathcal{U}$ depende de $\mathbf{1} : \mathcal{U}$, una función $f : \prod_{x:\mathbf{1}} Q(x)$ sólo necesita definirse en un elemento, a decir en $c(\star) : Q(\star)$" de tal modo que:

$$f(\star) = c(\star) : Q(\star)$$

III. Correspondencia Curry-Howard y Motivación en Lógica

Recuérdese de la sección pasada que si $a : A$ y $b : B$, entonces $\langle a, b\rangle : A \times B$. Ésto es fácilmente expresable como una regla de deducción en un sistema formal de la siguiente manera:

$$\frac{a : A \qquad\qquad b : B}{\langle a, b\rangle : A \times B} \times\text{-Intro}$$

Nótese el parecido de esta deducción con la introducción de la conjunción en lógica expresada como una deducción natural:

$$\frac{\Gamma \vdash A \qquad\qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-Intro}$$

Esta relación, aunada a otras similares para el resto de los tipos construidos en la sección anterior es lo que se conoce como la correspondencia Curry-Howard entre la lógica intuicionista y la teoría de tipos. Con base en ella cada tipo representa una proposición, es decir, al expresar que $P : \mathcal{U}$, realmente se está aseverando que P puede o no ser verificada. Cuando el tipo está habitado, i.e. $x : P$, se interpreta a dicho elemento x como un testigo de la veracidad de P o una prueba de que P es verdadera. Nótese que ésto marca una diferencia importante entre la lógica clásica y la interpretación intuicionista que se está dando a MLTT, pues en lógica clásica una proposición ya tiene de antemano un valor de verdad (tal vez desconocido), mientras que en teoría de tipos una proposición puede ser vista como "la colección” de todos los testigos de su veracidad y sólo será verdadera hasta que se haya exhibido una prueba de ésta, es decir, en lógica intuicionista se identifica demostrabilidad con veracidad.

Con base en lo previamente dicho, el resto de la sección será dedicado a hacer explícita la correspondencia Curry-Howard y establecer algunas consecuencias de ésta. Para hacer más palpable dicha correspondencia, se exponen reglas lógicas de deducción natural en una columna derecha mientras que sus equivalentes en teoría de tipos son expuestos en la columna izquierda.

I. Cuantificador Universal

En la correspondencia Curry-Howard, el cuantificador universal es identificado con el tipo de funciones dependientes, de tal modo que:[9]

$$(\forall\, x \in X)P(x) \equiv (\prod x : X)P(x)$$

A partir de esta equivalencia se observa el comportamiento “intuicionista” que tienen los tipos producto de MLTT:

$$\frac{X : \mathcal{U} \qquad x : X \vdash P(x) : \mathcal{U}}{\Pi_{x:X} P(x) : \mathcal{U}}\Pi\text{-Form} \qquad \frac{X \text{ Set} \qquad x \in X \vdash P(x) \text{ Prop.}}{\forall_{x \in X} P(x) \text{ Prop.}}\forall\text{-Form}$$

$$\frac{x : X \vdash f(x) : P(x)}{\lambda x.f(x) : \Pi_{x:X} P(x)}\Pi\text{-Intro} \qquad \frac{x \in X \vdash P(x) \text{ True}}{\forall_{x \in X} P(x) \text{ True}}\forall\text{-Intro}$$

$$\frac{a : X \qquad f : \Pi_{x:X} P(x)}{f(a) : P(a)}\Pi\text{-Elim} \qquad \frac{a \in X \quad \forall_{x \in X} P(x) \text{ True}}{P(a) \text{ True}}\forall\text{-Elim}$$

La primera regla dicta algo parecido a la gramática del lenguaje de la lógica, pues está diciendo que si X ya es un objeto bien formado y se verifica que “si x es una variable de tipo X, entonces $P(x)$ es un objeto bien formado del lenguaje”, entonces se puede afirmar que $\prod_{x:X} P(x)$ es una expresión bien formada. La segunda regla está afirmando a grandes rasgos el principio de generalización visto en capítulos previos: si $P(x)$ es verdadera para cada $x \in X$, entonces $(\forall x \in X)P(x)$ es verdadera también. Finalmente, la tercera regla es equivalente al lema de particularización del cuantificador universal $\forall$ (Regla A4) visto en lógica predicativa.

Recordando que la expresión $(\forall\, x \in X)P(x)$ sólo es una abreviación de la fórmula $\forall x[x \in X \Rightarrow P(x)]$, no es sorpresa que al lograr que P no dependa de $x : X$ se obtenga la implicación $X \Rightarrow P$ que es el siguiente conectivo lógico a analizar.

[9]En lo subsiguiente la notación $(\exists x \in X)P(x)$ será un alternante de la más familiar utilizada en capítulos previos $\exists x \in X[P(x)]$. De igual manera, si se escribe “$P(x)$ Prop.”, se estará expresando que $P \in \mathcal{L}$ con $x \in FV(P)$, mientras que $P(x)$ True representará la aseveración de que $[\![P(x)]\!] = 1$.

II. Implicación

Análogo al caso anterior, se identifica al tipo de funciones no-dependientes con la implicación:

$$P \Rightarrow Q \equiv P \to Q \equiv Q^P \equiv (\Pi x : P)Q$$

Esta última equivalencia induce tres reglas, de las cuales la primera establece cuándo es relevante construir una implicación (cuando el antecedente es verdadero); la segunda es el conocido teorema de la deducción, y la tercera corresponde a la regla de deducción *modus ponens* (MP):

$$\frac{P : \mathcal{U} \qquad x : P \vdash Q : \mathcal{U}}{P \to Q : \mathcal{U}} \to \text{-Form} \qquad \frac{P \text{ Prop.} \qquad P \text{ True } \vdash Q \text{ Prop.}}{P \Rightarrow Q \text{ Prop.}} \Rightarrow \text{-Form}$$

$$\frac{x : P \vdash f(x) : Q}{\lambda x.f(x) : P \to Q} \to \text{-Intro} \qquad \frac{P \text{ True } \vdash Q \text{ True}}{P \Rightarrow Q \text{ True}} \Rightarrow \text{-Intro}$$

$$\frac{x : P \qquad f : P \to Q}{f(x) : Q} \to \text{-Elim} \qquad \frac{P \text{ True} \qquad P \Rightarrow Q \text{ True}}{Q \text{ True}} \Rightarrow \text{-Elim}$$

Más aun, las deducciones en la teoría de tipos permiten demostrar propiedades lógicas ya conocidas de la implicación material:

Proposición III.1
En MLTT son verdaderas las fórmulas:

1. $P \Rightarrow P$
2. $P \Rightarrow (Q \Rightarrow P)$
3. $(P \Rightarrow (Q \Rightarrow R)) \Rightarrow ((P \Rightarrow Q) \Rightarrow (P \Rightarrow R))$

Demostración. Como se vio anteriormente, para demostrar un enunciado en teoría de tipos es necesario construir un elemento del tipo. En este caso, se está tratando con tipos de funciones por lo que la enunciación de la regla de correspondencia de una función, será suficiente para probar lo requerido:

1. Sea $P : \mathcal{U}$ una proposición, entonces asumir la veracidad de $P : \mathcal{U}$ proporciona un testigo de ésta, i.e. $x : P$. Esto se puede reenunciar diciendo que para cada $x : P$ se cumple que $x : P$, es decir, $x : P \vdash x : P$. Por introducción de la implicación se puede construir la función $\lambda x.x : P \to P$ y, por ende, la proposición $P \Rightarrow P$ es verdadera.

2. Sean $P, Q : \mathcal{U}$ proposiciones y supóngase que $x : P$ y $y : Q$, entonces la función definida por la regla de corespondencia $\lambda y.x$ cumple $\lambda y.x : Q \to P$. Por lambda abstracción nuevamente se obtiene que $\lambda x.\lambda y.x : P \to (Q \to P)$, esto es, la función que toma a x y lo manda a la función que mapea y en x es un testigo de la veracidad de $P \Rightarrow (Q \Rightarrow P)$.

3. Supónganse que P, Q y R son proposiciones, es decir que $P, Q, R : \mathcal{U}$. Además asúmase que $P, P \Rightarrow Q$ y $P \Rightarrow (Q \Rightarrow R)$ son verdaderas. Entonces se pueden seleccionar testigos de dichas veracidades por ejemplo $x : P, f : P \to Q$ y $g : P \to (Q \to R)$. De aquí que $f(x) : Q$ y $g(x) : Q \to R$. Por ende, al evaluarlos se tiene que $g(x)(f(x)) : R$. De esta manera, por λ-abstracción se pued construir un testigo de la veracidad de la proposición deseada, a decir, $\lambda g.\lambda f.\lambda x.g(x)(f(x)) : (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$.

■

Nótese que los últimos dos resultados son axiomas del sistema lógico de Łukasiewicz, faltando la "contrarrecíproca" o "contrapositiva" para tener el sistema completo. No obstante, ésta última no es demostrable en MLTT pues hacerlo induciría la lógica clásica y, como se ha enfatizado previamente, la teoría de tipos de Martin Löf corresponde a una lógica intuicionista.

III. Cuantificador Existencial

Procediendo de manera similar a las dos subsecciones anteriores, se exhibe la correspondencia Curry-Howard para el cuantificador existencial:

$$(\exists\, x \in X)P(x) \equiv (\Sigma\, x : X)P(x)$$

la cual induce las deducciones siguientes:

$$\frac{X : \mathcal{U} \qquad x : X \vdash P(x) : \mathcal{U}}{\Sigma_{x:X} P(x) : \mathcal{U}}\Sigma\text{-Form} \qquad \frac{X \text{ Set} \qquad x \in X \vdash P(x) \text{ Prop.}}{\exists_{x \in X} P(x) \text{ Prop.}}\exists\text{-Form}$$

$$\frac{x : X \qquad y : P(x)}{\langle x, y\rangle : \Sigma_{x:X} P(x)}\Sigma\text{-Intro} \qquad \frac{x \in X \qquad P(x) \text{ True}}{\exists_{x \in X} P(x) \text{ True}}\exists\text{-Intro}$$

$$\frac{x : X, y : P(x) \vdash g(x)(y) : Q \qquad\qquad p : \Sigma_{x:X} P(x)}{\mathrm{Ind}_{\Sigma}(Q, g, p) : Q}\Sigma\text{-Elim}$$

$$\frac{x \in X, P(x) \text{ True } \vdash Q \text{ True} \qquad \exists_{x \in X} P(x) \text{ True}}{Q \text{ True}}\exists\text{-Elim}$$

Recuérdese que en la sección anterior se construyeron las proyecciones canónicas π_1 y π_2 para los Tipos de Parejas dependientes, las cuales, cumplían que si $\langle a, b\rangle : \sum_{x:A} B(x)$, entonces $\pi_1(a, b) = a : A$ y $\pi_2(a, b) = b : B$. La interpretación que se da a esta demostración en la correspondencia Curry-Howard es, en el caso de la primera proyección, que si $(\exists x \in A)B(x)$ es verdadera, entonces es posible obtener al testigo que satisface la propiedad B, o sea, $a : A$. Por otro lado la segunda proyección permite demostrar precisamente que $B(a)$ True, es decir, por medio de $\pi_2(a, b) = b : B(a)$, el elemento $a : A$ satisface la propiedad B.

IV. Conjunción

A la conjunción le corresponde, bajo Curry-Howard, el producto cartesiano de dos tipos:

$$P \wedge Q \equiv P \times Q \equiv (\Sigma x : P)Q$$

Entonces, las reglas de formación, introducción y eliminación de este conectivo lógico son:

$$\frac{P : \mathcal{U} \qquad x : P \vdash Q : \mathcal{U}}{P \times Q : \mathcal{U}} \times\text{-Form} \qquad\qquad \frac{P \text{ Prop.} \qquad P \text{ True } \vdash Q \text{ Prop.}}{P \wedge Q \text{ Prop.}} \wedge\text{-Form}$$

$$\frac{x : P \qquad y : Q}{\langle x, y\rangle : P \times Q} \times\text{-Intro} \qquad\qquad \frac{P \text{ True} \qquad Q \text{ True}}{P \wedge Q \text{ True}} \wedge\text{-Intro}$$

$$\frac{x : P, y : Q \vdash g(x)(y) : R \qquad\qquad p : P \times Q}{\mathrm{Ind}_\times(R, g, p) : R} \times\text{-Elim}$$

$$\frac{P \text{ True }, Q \text{ True } \vdash R \text{ True} \qquad P \wedge Q \text{ True}}{R \text{ True}} \wedge\text{-Elim}$$

Obsérvese que de la última regla se pueden derivar las más conocidas reglas de eliminación de la conjunción pues siempre se cumple P True $\vdash$ P True y es posible aumentar una hipótesis a esto último sin modificar su validez, i.e. P True $, Q$ True $\vdash$ P True. Suponiendo que $P \wedge Q$ True y aplicando la regla anterior se deriva que P True. Esto es, se he verificado que:

$$\frac{P \wedge Q \text{ True}}{P \text{ True}}$$

El resultado equivalente para Q True se obtiene de manera análoga.

Igual que en la subsección de implicación, se procede a probar un par de resultados de lógica intuicionista:

Proposición III.2
En MLTT son verdaderas las fórmulas:

1. $P \Rightarrow (Q \Rightarrow P \wedge Q)$
2. $(P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \wedge Q \Rightarrow R)$

Demostración.

1. Supongamos que $P : \mathcal{U}$ y $Q : \mathcal{U}$ son verdaderas, i.e. $x : P$ y $y : Q$. Sabemos entonces por la regla de introducción de la conjunción que $\langle x, y\rangle : P \times Q$. Por λ-abstracción podemos concluir que $\lambda x.\lambda y.\langle x, y\rangle : P \to (Q \to P \times Q)$ que es lo que queríamos demostrar.

2. Sean $f : P \to (Q \to R)$ y $p : P \times Q$. Suponiendo $x : P, y : Q$ podemos ver que $f(x)(y) : R$, es decir: $x : P, y : Q \vdash f(x)(y) : R$. Por el principio de inducción para tipos producto $\mathrm{Ind}_\times(R, f, p) : R$. Por lo tanto, utilizando lambda abstracción (teorema de la deducción) $\lambda f.\lambda p.\,\mathrm{Ind}_\times(R, f, p) : (P \to (Q \to R)) \to (P \times Q \to R)$.

■

Además de este par de teoremas de lógica intuicionista, un resultado curioso al trabajar en MLTT y la correspondencia Curry-Howard es una especie de *axioma de elección*:

Teorema III.3 (*Axioma de Elección de la Teoría de Tipos*)
Dados un tipo $A : \mathcal{U}$, una familia $\{B(x) : \mathcal{U} \mid x : A\}$ y una relación binaria (familia) $\{R(a,b) : \mathcal{U} \mid \langle a,b\rangle : \sum_{x:A} B(x)\}$, se cumple que:

$$\mathrm{ac} : \left(\prod_{x:A}\sum_{y:B(x)} R(x,y)\right) \to \left(\sum_{f:\prod_{x:A} B(x)} \prod_{t:A} R(t, f(t))\right)$$

Demostración. Sea $g : \prod_{x:A}\sum_{y:B(x)} R(x,y)$, entonces si $a : A$, su imagen $g(a)$ cumple que $\pi_1(g(a)) : B(a)$ y $\pi_2(g(a)) : R(a, \pi_1(g(a)))$. Deseamos entonces construir una pareja tal que la primera entrada sea una función $f : \prod_{x:A} B(x)$ y la segunda, otra función en $\prod_{t:A} R(t, f(t)) : \mathcal{U}$. Para esto vemos que $f := \lambda x.\pi_1(g(x)) : \prod_{x:A} B(x)$, mientras que $\lambda t.\pi_2(g(t)) : \prod_{t:A} R(t, f(t))$. Por ende, la pareja $\langle \lambda x.\pi_1(g(x)), \lambda t.\pi_2(g(t))\rangle$ es un testigo de la veracidad de $\sum_{f:\prod_{x:A} B(x)} \prod_{t:A} R(t, f(t))$. Finalmente, definimos a la función ac como:

$$\mathrm{ac} = \lambda g.\langle \lambda x.\pi_1(g(x)), \lambda t.\pi_2(g(t))\rangle : \left(\prod_{x:A}\sum_{y:B(x)} R(x,y)\right) \to \left(\sum_{f:\prod_{x:A} B(x)} \prod_{t:A} R(t, f(t))\right)$$

■

Lo anterior puede ser interpretado mediante la correspondencia Curry-Howard como:

$$\forall x \in A \exists y \in B(x)[R(x,y)] \Rightarrow \exists f \in \Pi_{x\in A} B(x) \forall t \in A[R(t, f(t))] \text{ True}$$

Obsérvese que al cambiar $R(x,y)$ por $y \in x$ este enunciado se asemeja al axioma de elección ($\emptyset \notin A \Rightarrow \exists f : A \to \bigcup A \forall t \in A(f(t) \in t)$) y, como recién se ha visto, es demostrable en la Teoría de Tipos. No obstante, es importante resaltar que ac no está llevando a cabo realmente ninguna elección pues ésta ya está dada en la premisa y por ello la prueba fue fácil de realizar: sólo se requirió tomar la función original $g : \prod_{x:A}\sum_{y:B(x)} R(x,y)$ y dividirla en otras dos funciones $\lambda x.\pi_1(g(x)), \lambda t.\pi_2(g(t))$. Éstas, al combinarse en una pareja ordenada, recuperan el testimonio de la "elección".

Además de las interpretaciones dadas al tipo de parejas dependientes, también se le usa frecuentemente para construir entes matemáticos. Por ejemplo, si uno recuerda que el principio de comprensión restringida de ZFC permite construir conjuntos de la forma $\{x \in A \mid B(x)\}$, y además observa que un elemento $a : A$ que satisface $B(a)$, genera una prueba $b : B(a)$, entonces uno puede concluir que el conjunto de los $x : A$ tales que $B(x)$ es realmente el tipo de parejas $\langle a, b\rangle : \sum_{x:A} B(x)$. También es común construir las estructuras algebraicas por medio de los tipos de parejas dependientes. Por ejemplo, recordando que los magmas son vistos como *parejas* donde la primera entrada es un conjunto y la segunda, una operación binaria, se puede definir el tipo

$$\text{Magma} := \sum_{A:\mathcal{U}} (A \to (A \to A))$$

Si además uno desea agregar el axioma de asociatividad a dicha operación binaria para convertir el magma en un semigrupo, los tipos coproducto siguen siendo de utilidad para este fin, pues únicamente se define

$$\text{Semigroup} := \sum_{A:\mathcal{U}} \sum_{*:A\to(A\to A)} \prod_{x,y,z:A} *(*(x,y),z) =_A *(x,*(y,z))$$

V. Disyunción

El coproducto es el tipo que le corresponde a la disyunción bajo el isomorfismo de Curry-Howard:

$$P \vee Q \equiv P + Q$$

Por lo que las reglas de formación, introducción y eliminación de este conectivo lógico quedan de la siguiente manera:

$$\frac{P:\mathcal{U} \qquad Q:\mathcal{U}}{P+Q:\mathcal{U}} + \text{-Form} \qquad\qquad \frac{P \text{ Prop.} \qquad Q \text{ Prop.}}{P \vee Q \text{ Prop.}} \vee \text{-Form}$$

$$\frac{x:P}{\iota_1(x):P+Q} + \text{-Intro1} \qquad\qquad \frac{P \text{ True}}{P \vee Q \text{ True}} \vee \text{-Intro1}$$

$$\frac{y:Q}{\iota_2(x):P+Q} + \text{-Intro2} \qquad\qquad \frac{Q \text{ True}}{P \vee Q \text{ True}} \vee \text{-Intro2}$$

$$\frac{x:P \vdash g_1(x):C \qquad y:Q \vdash g_2(y):C \qquad z:P+Q}{\text{Ind}_+(C, g_1, g_2, z):C} + \text{-Elim}$$

$$\frac{P \text{ True } \vdash C \text{ True} \qquad Q \text{ True } \vdash C \text{ True} \qquad P \vee Q \text{ True}}{C \text{ True}} \vee \text{-Elim}$$

En esta subsección también se presentan algunos resultados de lógica intuicionista:

Proposición III.4

En MLTT son verdaderas las fórmulas:

1. $P \Rightarrow P \vee Q$
2. $Q \Rightarrow P \vee Q$
3. $(P \Rightarrow R) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \vee Q \Rightarrow R)$

Demostración. Suponiendo que $x : P$, sabemos que $\iota_1(x) : P + Q$. Fácilmente tenemos que $\lambda x.\iota_1(x) : P \to P + Q$. La prueba para $Q \Rightarrow P \vee Q$ es análoga con la segunda inclusión.

Sean $f : P \to R$, $g : Q \to R$ y $z : P + Q$, entonces claramente para $x : P$ se tiene que $f(x) : R$, mientras que $g(y) : R$ si $y : Q$. Con esto completamos las hipótesis para aplicar el principio de inducción para el tipo coproducto, por lo que $\mathrm{Ind}_+(R, f, g, z) : R$. Por lambda abstracción tenemos lo requerido:

$$\lambda f.\lambda g.\lambda z.\,\mathrm{Ind}_+(R, f, g, z) : (P \to R) \to ((Q \to R) \to (P + Q \to R)$$

■

VI. Inducción en Números Naturales

En el caso del tipo de números naturales $\mathbb{N} : \mathcal{U}$, gracias a la correspondencia Curry-Howard, el *principio de inducción para el tipo de los naturales* se convierte en el ya utilizado cotidianamente en matemáticas: si $P(n) : \mathcal{U}$ es una propiedad de números naturales, i.e. $n : \mathbb{N}$, para construir un testigo de que ésta se cumple para todos los naturales $f : \prod_{n:\mathbb{N}} P(n)$ es suficiente con definir cómo se comporta éste en el caso base $c_0 : P(0)$ y en el caso inductivo $c_S : \prod_{n:\mathbb{N}} P(n) \to P(S(n))$ de tal modo que:

$$f(0) = c_0$$

$$f(S(n)) = c_S(n, f(n))$$

Semiformalmente esto queda expresado de la siguiente manera:

$$\frac{c_0 : P(0) \qquad x : \mathbb{N}, y : P(x) \vdash c_S(x, y) : P(S(x)) \qquad n : \mathbb{N}}{\mathrm{Ind}_{\mathbb{N}}(P, c_0, c_S, n) : P(n)}\,\mathbb{N}\text{-Elim}$$

$$\frac{c_0 : P(0) \qquad x : \mathbb{N}, y : P(x) \vdash c_S(x, y) : P(S(x))}{\mathrm{Ind}_{\mathbb{N}}(P, c_0, c_S, 0) = c_0 : P(0)}\,\mathbb{N}\text{-Comp1}$$

$$\frac{c_0 : P(0) \qquad x : \mathbb{N}, y : P(x) \vdash c_S(x, y) : P(S(x)) \qquad n : \mathbb{N}}{\mathrm{Ind}_{\mathbb{N}}(P, c_0, c_S, S(n)) = c_S(n, \mathrm{Ind}_{\mathbb{N}}(P, c_0, c_S, n)) : P(S(n))}\,\mathbb{N}\text{-Comp2}$$

Gracias a lo previamente dicho es posible construir en los naturales las operaciones ya familiares como la suma:

Ejemplo III.1 (*Construcción de la suma de naturales en MLTT*) Tradicionalmente se ve a la suma como una función $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Haciendo currying (en el producto) esto equivale a construir una función de la forma $+ : \mathbb{N} \to (\mathbb{N} \to \mathbb{N})$. De esta manera, el caso base para la inducción será una función $c_0 : \mathbb{N} \to \mathbb{N}$ mientras que al caso recursivo le corresponderá otra $c_S : \mathbb{N} \to ((\mathbb{N} \to \mathbb{N}) \to (\mathbb{N} \to \mathbb{N}))$. Obsérvese que para cada $m : \mathbb{N}$, el resultado de $+(m, 0)$ debería ser igual a m, por lo que el candidato para el caso base c_0 es la función identidad, i.e. $\lambda m.m : \mathbb{N} \to \mathbb{N}$. Por otro lado, se desea que si $n \neq 0$, entonces $+(m)(S(n)) = +(m, S(n)) = S(+(m, n)) = S(+(m)(n))$, lo cual da una idea de cómo definir a c_S pues suponiendo ya dados $x : \mathbb{N}$ y $y : \mathbb{N} \to \mathbb{N}$ es posible construir a la función $\lambda m.\lambda y.\lambda x.S(y(x)) : \mathbb{N} \to ((\mathbb{N} \to \mathbb{N}) \to (\mathbb{N} \to \mathbb{N}))$. Por el principio de inducción $\mathrm{Ind}_{\mathbb{N}}(\mathbb{N} \to \mathbb{N}, \lambda m.m, \lambda m.\lambda y.\lambda x.S(y(x)), n) : \mathbb{N} \to \mathbb{N}$ donde $\mathrm{Ind}_{\mathbb{N}}(\mathbb{N} \to \mathbb{N}, c_0, c_S, 0)(m) = (\lambda m.m)(m) = m$ en el caso base, y en el recursivo $\mathrm{Ind}_{\mathbb{N}}(\mathbb{N} \to \mathbb{N}, c_0, c_S, S(n))(m) = (\lambda m.\lambda y.\lambda x.S(y(x)))(n, \mathrm{Ind}_{\mathbb{N}}(\mathbb{N} \to \mathbb{N}, c_0, c_S, n), m) = S(\mathrm{Ind}_{\mathbb{N}}(\mathbb{N} \to \mathbb{N}, c_0, c_S, n)(m))$. De esta forma, se define a la suma mediante:

$$+ := \lambda m.\lambda n.\, \mathrm{Ind}_{\mathbb{N}}(\mathbb{N} \to \mathbb{N}, c_0, c_S, n)(m) : \mathbb{N} \to (\mathbb{N} \to \mathbb{N})$$

El ejemplo recientemente hecho presenta la definición recursiva de manera diferente a como se expone normalmente, pues la función $\mathrm{Ind}_{\mathbb{N}}(P, c_0, c_S, n)$ resulta poco familiar a menos que se compute tal y como se hizo aquí. Para evadir estas dificultades se usa la coincidencia de patrones para realizar definiciones recursivas. De esta manera, en vez de introducir a la función suma por medio del inductor, se puede definir de la siguiente manera[10]:

$$+(m, 0) = m$$

$$+(m, S(n)) = S(+(m, n))$$

VII. Contradicción y negación

Por medio de la correspondencia Curry-Howard se tiene que:

$$\perp \equiv \emptyset$$

Dado que el Tipo Vacío ya es parte del universo, la regla de formación de este tipo sólo establece que "la contradicción" es una proposición:

$$\frac{}{\emptyset : \mathcal{U}}\ \emptyset\text{-Form} \qquad\qquad \frac{}{\perp \text{ Prop.}}\ \perp\text{-Form}$$

Sin embargo, no hay ninguna manera de construir elementos del Tipo Vacío, por lo que no se tienen reglas de introducción de la contradicción. Aun así, sí se tiene una regla de eliminación o inductor, el cual hace explícito *el principio lógico de explosión*:

[10] Obsérvese la semejanza entre la construcción del ejemplo y la coincidencia de patrones para la suma.

$$\frac{x : \emptyset}{\mathrm{Ind}_\emptyset(Q, x) : Q}\emptyset\text{-Elim} \qquad\qquad \frac{\perp \text{ True}}{Q \text{ True}}\perp\text{-Elim}$$

De esto es fácil derivar la tautología $\perp \Rightarrow P$, siendo el testigo de la veracidad de esto la función $\lambda x. \mathrm{Ind}_\emptyset(P, x) : \emptyset \to P$. Además, procediendo igual que en lógica, es posible definir a la negación de la siguiente manera:

$$\neg A \equiv A \Rightarrow \perp \equiv A \to \emptyset$$

A partir de esta equivalencia se pueden probar los teoremas de la negación ya conocidos de lógica intuicionista, como $\neg A \wedge \neg B \Rightarrow \neg(A \vee B)$:

Ejemplo III.2 Supongamos que $p : (A \to \emptyset) \times (B \to \emptyset)$ y que $z : A + B$. Sabemos entonces que $\pi_1(p) : A \to \emptyset$ y que $\pi_2(p) : B \to \emptyset$. Por otro lado, si $x : A$, entonces $\pi_1(p)(x) : \emptyset$ y si $y : B$, $\pi_2(p)(y) : \emptyset$. Por el principio de inducción para el coproducto tenemos que $\mathrm{Ind}_+(\emptyset, \pi_1(p), \pi_2(p), z) : \emptyset$ y por lambda abstracción:

$$\lambda p.\lambda z. \mathrm{Ind}_+(\emptyset, \pi_1(p), \pi_2(p), z) : (A \to \emptyset) \times (B \to \emptyset) \to (A + B \to \emptyset)$$

VIII. Tautología

Si al vacío le correspondía la contradicción no debería sorprender que al tipo unidad le corresponda la partícula tautológica:

$$\top \equiv \mathbf{1}$$

Al igual que en el caso anterior, sin requerir condiciones ya se tiene que $\top$ es una proposición:

$$\frac{}{\mathbf{1} : \mathcal{U}}\mathbf{1}\text{-Form} \qquad\qquad \frac{}{\top \text{ Prop.}}\top\text{-Form}$$

Pero la unidad se distingue del vacío en que sí presenta un elemento, i.e. siempre es verdadera:

$$\frac{}{\star : \mathbf{1}}\mathbf{1}\text{-Intro} \qquad\qquad \frac{}{\top \text{ True}}\top\text{-Intro}$$

Finalmente, si suponiendo una tautología se deriva algo, entonces se sabe que el resultado de dicha deducción también es verdadero:

$$\frac{x : \mathbf{1} \vdash y : Q(x) \quad a : \mathbf{1}}{\mathrm{Ind}_\mathbf{1}(Q, y, a) : Q}\mathbf{1}\text{-Elim} \qquad\qquad \frac{\top \text{ True } \vdash Q \text{ True} \quad \top \text{ True}}{Q \text{ True}}\top\text{-Elim}$$

IX. Igualdad Proposicional

Una vez que se ha hecho explícita la correspondencia Curry-Howard entre los tipos presentados en la sección anterior y algunos conectivos lógicos, es posible motivar la definición de una clase de tipos más: la igualdad proposicional. Ésta se distinguirá de la igualdad que se ha estado utilizando hasta ahora (la juzgamentada o definicional) en cuanto a que la primera representa, como su nombre lo dice, una proposición y, por ende, es susceptible a mostrar testigos de su veracidad, mientras que la segunda es una igualdad meramente sintáctica.

Más aun, la introducción de esta nueva igualdad permite operar con ella tal y como se hace en la práctica, i.e. se puede negar, conjuntar, disyuntar o implicar. Nótese que esto no es posible para la igualdad definicional porque ésta corresponde a un juicio y éstos no pueden operarse o cuantificarse lógicamente. La distinción entre ambas igualdades no es comúnmente explicitada en matemáticas aunque, siendo pedantes, debería hacerse pues afirmar que $2+2=2\times 2$ puede considerarse falso si se lee al signo "$=$" como "*es idéntico a*", mientras que es verdadero cuando el símbolo $=$ representa "[tras computar] *tiene el mismo valor que*". Tomando en cuenta lo dicho anteriormente, se procede a formular las reglas de formación, introducción, eliminación y computación de los tipos igualdad proposicional:

La primera regla dice que dado cualquier tipo $A:\mathcal{U}$ y dos elementos de éste $a,b:A$, se puede plantear el problema de si ámbos términos son iguales, o sea $a=_A b:\mathcal{U}$ ó $\mathrm{Id}_A(a,b):\mathcal{U}$:

$$\frac{A:\mathcal{U}\quad a:A\quad b:A}{\mathrm{Id}_A(a,b):\mathcal{U}} = \text{-Form}$$

La segunda regla establece que todo término de cualquier tipo $a:A$ es proposicionalmente idéntico a sí mismo $r_a:\mathrm{Id}_A(a,a)$ ó $\mathrm{refl}_a : a=_A a$.

$$\frac{a:A}{r_a:\mathrm{Id}_A(a,a)} = \text{-Intro}$$

Finalmente el *principio de inducción para la igualdad proposicional* dice a grandes rasgos que para estudiar la igualdad de cualesquiera dos elementos de un tipo dado, es suficiente con estudiar cómo se comporta la igualdad en la reflexividad (pues una vez que se tiene ésta, si los elementos son <u>sintácticamente</u> iguales, por medio de sustituciones se puede llegar a la igualdad <u>proposicional</u> de éstos). Expresar estas ideas en términos similares a la sección anterior se traduce en afirmar que dada una familia $Q(x,y,r)$ con $x,y:A$ y $r:\mathrm{Id}_A(x,y)$, construir una función $f:\prod_{x,y:A}\prod_{r:\mathrm{Id}_A(x,y)}Q(x,y,r)$ requiere tener otra únicamente definida en la reflexividad $g:\prod_{x:A}Q(x,x,r_x)$ de tal modo que $f(x,x,r_x)=g(x)$. En forma de reglas de deducción esto se puede escribir de la siguienta manera:

$$\frac{x:A\vdash g(x):Q(x,x,r_x)\qquad a:A\qquad b:A\qquad p:\mathrm{Id}_A(a,b)}{\mathrm{Ind}_{=_A}(Q,g,a,b,p):Q(a,b,p)} = \text{-Elim}$$

$$\frac{x : A \vdash g(x) : Q(x, x, r_x) \qquad a : A}{\mathrm{Ind}_{=_A}(Q, g, a, a, r_a) = g(a) : Q(a, a, r_a)} = \text{-Comp}$$

Gracias a la correspondencia Curry-Howard en MLTT y a la introducción de los tipos igualdad propocional con las reglas de formación, introducción, eliminación y computación dadas recientemente, es posible probar el recíproco al principio ontológico de Leibniz, la identidad de los indescirnibles, i.e. *la indiscernibilidad de los idénticos*: si dos objetos son iguales, entonces satisfacerán los mismos predicados.

Teorema III.5 (*Indiscernibilidad de los Idénticos*)
Para cualquier predicado P respecto a elementos de $A : \mathcal{U}$, i.e. $x : A \vdash P(x) : \mathcal{U}$, se cumple que:

$$f : \prod_{x,y:A} \prod_{p:\mathrm{Id}_A(x,y)} P(x) \to P(y) \quad \text{donde } f = \lambda(t : P(x)).t$$

Demostración. Si $x : A$, sabemos que $P(x) : \mathcal{U}$, y por una proposición anterior tenemos que $\lambda(t : P(x)).t : Q(x, x, r_x) := P(x) \to P(x)$. En otras palabras, se satisface la primera hipótesis de la regla de eliminación para la igualdad proposicional $x : A \vdash g(x) : Q(x, x, r_x)$, siendo $g(x) = \lambda(t : P(x)).t$. Más aun, para cualesquiera $x : A$ y $y : A$ tales que $p : \mathrm{Id}_A(x, y)$, la inducción asevera que:

$$f := \mathrm{Ind}_{=_A}(Q, g, x, y, p) : Q(x, y, p)$$

Con lo que concluimos que:

$$f = \lambda x.\lambda y.\lambda p.\, \mathrm{Ind}_{=_A}(Q, g, x, y, p) = g(x) = \lambda(t : P(x)).t : \prod_{x,y:A} \prod_{p:\mathrm{Id}_A(x,y)} P(x) \to P(y)$$

■

La igualdad proposicional es la que permitirá demostrar diversas propiedades ya familiares en matemáticas, por ejemplo, la clásica propiedad de que toda función manda preimágenes iguales a imágenes iguales $x = y \Rightarrow f(x) = f(y)$:

Lema III.6 (*Las funciones se comportan functorialmente sobre caminos*)
Sean $A, B : \mathcal{U}$ y $f : A \to B$ entonces:

$$\mathrm{ap}_f : \prod_{x,y:A} x =_A y \to f(x) =_B f(y) \quad \text{con } \mathrm{ap}_f(x, x, r_x) = r_{f(x)}$$

Demostración. Queremos construir una función a partir de una igualdad, lo cual inmediatamente implica la utilización del principio de inducción para la igualdad proposicional. Así, sea $x : A$, sabemos que $f(x) : B$ y, por introducción de la igualdad, $r_{f(x)} : f(x) =_B f(x) := Q(x, x, r_x)$. De aquí que $g := \lambda x.r_{f(x)} : \prod_{x:A} Q(x, x, r_x)$, es decir, la primera premisa de la inducción $x : A \vdash g(x) : Q(x, x, r_x)$. Además si $x, y : A$ son proposicionalmente iguales $p : x =_A y$, la eliminación de la igualdad hace el resto y sólo requerimos definir $\mathrm{ap}_f := g$ con lo cual se concluye la prueba. ■

Teorema III.7 (*La suma en los naturales es asociativa*)

$$\mathrm{assoc} : \prod_{k,m,n:\mathbb{N}} k + (m+n) =_{\mathbb{N}} (k+m)+n$$

Demostración. Para aplicar el principio de inducción para los números naturales, requerimos primero probar el enunciado para el caso base. Esto es fácilmente demostrable ya que si $n : \mathbb{N}$, entonces $n + 0 = n : \mathbb{N}$, de donde $0 + (m+n) = m+n = (0+m)+n$. Por introducción de la igualdad, podemos construir un testigo $r_{m+n} : 0+(m+n) =_{\mathbb{N}} (0+m)+n$. Definiendo $assoc_0 := \lambda m.\lambda n.r_{m+n}$ completamos el caso base. Supóngase que $k : \mathbb{N}$ y que además $h : \prod_{m,n:\mathbb{N}} k + (m+n) =_{\mathbb{N}} (k+m)+n$. Recordando el comportamiento de la suma de naturales se tiene que $S(k)+(m+n) = S(k+(m+n))$ y $(S(k)+m)+n = S(k+m)+n = S((k+m)+n)$. Además, utilizando el lema anterior sabemos que $\mathrm{ap}_S : \prod_{x,y:\mathbb{N}} x =_{\mathbb{N}} y \to S(x) =_{\mathbb{N}} S(y)$. Por ende $\mathrm{ap}_S(m,n,h(m,n)) : S(k+(m+n)) =_{\mathbb{N}} S((k+m)+n)$. De esta manera, definiendo a $assoc_S$ como $\lambda k.\lambda h.\lambda m.\lambda n.\,\mathrm{ap}_S(m,n,h(m,n))$, tenemos que:

$$asoc_S : \prod_{k:\mathbb{N}} \Big(\prod_{m,n:\mathbb{N}} k+(m+n) =_{\mathbb{N}} (k+m)+n \Big) \to \prod_{m,n:\mathbb{N}} S(k+(m+n)) =_{\mathbb{N}} S((k+m)+n)$$

Aplicando $\mathrm{Ind}_{\mathbb{N}}$ apropiadamente se obtiene lo deseado. ■

Además, a diferencia de la teoría de conjuntos ZFC donde se define a un producto cartesiano $A \times B$ como el conjunto de parejas $\langle a,b\rangle$ donde $a \in A$ y $b \in B$; en MLTT este hecho es demostrable. Aquí se mostrará el caso general para los tipos suma:

Teorema III.8 (*Principio de Unicidad Proposicional para los Tipos de Parejas Dependientes*)

$$\mathrm{uppt} : \prod_{p:\sum_{a:A} B(a)} \langle \pi_1(p), \pi_2(p)\rangle =_{\Sigma} p$$

Demostración. Sea $x : A$ y $y : B(x)$, por introducción de la suma sabemos que $\langle x,y\rangle : \sum_{a:A} B(a)$ y por introducción de la igualdad, $r_{\langle x,y\rangle} : \langle x,y\rangle =_{\Sigma} \langle x,y\rangle$. Con las proyecciones canónicas obtenemos que $\pi_1(x,y) = x : A$ y $\pi_2(x,y) = y : B(a)$. Por ser estas dos últimas igualdades de juicio, podemos sustituir en el tipo identidad y obtener que $r_{\langle x,y\rangle} : \langle \pi_1(x,y), \pi_2(x,y)\rangle =_{\Sigma} \langle x,y\rangle$. Por lambda abstracción construimos la función $g := \lambda x.\lambda y.r_{\langle x,y\rangle} : \prod_{a:A}\prod_{b:B(a)} \langle \pi_1(x,y), \pi_2(x,y)\rangle =_{\Sigma} \langle x,y\rangle$. En conclusión y resumiendo, hemos probado $x : A, y : B(x) \vdash g(x)(y) : \langle \pi_1(x,y), \pi_2(x,y)\rangle =_{\Sigma} \langle x,y\rangle$. Sea $p : \sum_{a:A} B(a)$, por la inducción sobre la suma y lambda abstracción tenemos que:

$$\mathrm{uppt} := \lambda p.\,\mathrm{Ind}_{\Sigma}(Q,g,p) = \lambda p.r_p : \prod_{p:\sum_{a:A} B(a)} \langle \pi_1(p), \pi_2(p)\rangle =_{\Sigma} p$$

■

Por último, es común que en HoTT, además del principio de inducción para la igualdad proposicional, se utilice el siguiente principio equivalente:

Definición III.1 (*Inducción de caminos basada*)
Sea $a : A$ fijo. Dada una familia $Q(x, r_x)$ indizada por $x : A$ y $r_x : a =_A x$, si $c : Q(a, r_a)$, entonces es posible obtener una función $f : \prod_{x:A} \prod_{p:a=_A x} Q(x, p)$ tal que $f(a, r_a) = c$.

Algunas observaciones finales antes de concluir la sección:

- La equivalencia entre esta inducción y la inicialmente dada se puede efectuar de diversas maneras, para más información véase [Pro13].
- No es difícil probar que la igualdad proposicional es una "relación" de equivalencia, es decir, es reflexiva, simétrica y transitiva.
- Finalmente, con base en la Correspondencia Curry-Howard y en cómo se definió a la negación, claramente se tiene que:

$$x \neq_A y \equiv \neg(x =_A y) \equiv x =_A y \to \emptyset$$

IV. Desarrollo formal de HoTT y motivación en los fundamentos

En este punto el lector ya debe estar familiarizado con la notación utilizada en teoría de tipos y su manejo informal. Con esta idea en mente se procede a presentar la sintaxis del lenguaje formal de dicha teoría así como el sistema formal con el cual se trabajará el resto del capítulo.

Al igual que todos los lenguajes y sistemas formales, la presentación de una teoría de tipos varía por autor. No obstante esta consideración, en el presente trabajo se adopta una presentación similar a la del Programa de Fundamentos Univalentes en el libro *Homotopyy Type Theory: Univalent Foundations of Mathematics* [Pro13]. De esta forma, se asume que el alfabeto Σ de símbolos del lenguaje a construir consta de:

- Variables: $x, x', x'', \ldots$
- Constantes: $c, c', c'', \ldots$
- Punto, paréntesis y dos puntos: $., (,), :$
- Acotador de variables lambda: λ

Definición IV.1 (Lambda términos)
El conjunto Λ de λ-términos bien formados se construye recursivamente por:

$\lambda 1.$ Todas las variables son λ-términos.

$\lambda 2$. Todas las constantes son λ-términos.

$\lambda 3$. Si $s, t \in \Lambda$, entonces $s(t) \in \Lambda$.

$\lambda 4$. Si $f, t \in \Lambda$ y x es una varibale, entonces $(\lambda(x{:}t).f) \in \Lambda$.

$\lambda 5$. Nada más es un λ-término.

Las expresiones bien formadas de una teoría de tipos tienen la forma "$\alpha : \beta$" donde $\alpha, \beta \in \Lambda$. Esto representa la idea "el término α es de tipo β". Comúnmente se utiliza la expresión *well typed* (bien tipificado) para expresar que un tipo fue construido apropiadamente a partir de las reglas de inferencia de la teoría, esto a su vez implica que la expresión en cuestión es una fórmula bien formada. También es común formalizar en estas teorías los juicios, i.e. los enunciados metalógicos. Por dicha razón se presentan a continuación los juicios básicos de la teoría HoTT:

- La expresión "$\Gamma \vdash$" simboliza "Γ es un contexto bien formado".[11]
- Otro juicio es "$\Gamma \vdash a : A$" que significa "a es un término de tipo A involucrando variables en el contexto Γ".
- Finalmente, "$\Gamma \vdash a_i = a_j : A$" también es un juicio y representa "a_i y a_j son términos (definicionalmente/juzgadamente) iguales en el tipo A con base en los términos del contexto Γ".

Posteriormente se procede a presentar las diferentes reglas de inferencia para obtener dichos juicios. Éstas dicen cómo operar con los contextos formados hasta determinado momento en cualquier prueba formal. La primera regla adquiere su nombre, ctx-Emp, por las palabras en inglés *context* (contexto) y *empty* (vacío), y especifica que la "nada" es un contexto bien formado. La segunda dice que todo contexto contiene hipótesis, y lo enuncia afirmando que si se tiene un contexto bien formado Γ, entonces cualesquiera de sus expresiones bien formadas puede pasarse del lado derecho del símbolo "$\vdash$" para expresar que dicha buena tipificación involucra variables en el contexto Γ. Finalmente, la tercera regla dice que "si en el contexto de las variables $x_1, \ldots, x_{n-1}$, la expresión A_n es de tipo $\mathcal{U}_i$, i.e. A_n es un tipo, entonces el *contexto extendido* $(x_1 : A_1, \ldots, x_n : A_n)$ está bien formado:

$$\frac{}{\cdot \vdash}\text{ctx-Emp} \qquad \frac{(x_1 : A_1, \ldots, x_n : A_n) \vdash}{x_1 : A_1, \ldots, x_n : A_n \vdash x_i : A_i}\text{Vble} \qquad \frac{x_1 : A_1, \ldots, x_{n-1} : A_{n-1} \vdash A_n : \mathcal{U}_i}{(x_1 : A_1, \ldots, x_n : A_n) \vdash}\text{ctx-Ext}$$

En la tercera regla anterior se utilizó una constante: $\mathcal{U}_i$. Como se dijo anteriormente, en HoTT existen "universos" con los cuales se hace explícito qué expresiones están bien tipificadas. Gracias a éstos es posible expresar la noción "A es un tipo" mediante la expresión $A : \mathcal{U}_i$ para algún i. Su comportamiento se formaliza en la teoría por medio de una sucesión de constantes $\mathcal{U}_0, \mathcal{U}_1, \mathcal{U}_2, \ldots$ y las reglas:

[11] Un contexto es una sucesión finita de fórmulas $x_1 : A_1, x_2 : A_2, \ldots, x_n : A_n$ tales que $x_i \neq x_j$ para $j \neq i$, indicando que las expresiones $x_1, \ldots, x_n$ (distintas una de la otra) son de tipo $A_1, \ldots, A_n$ respectivamente. Las reglas que definen formalmente qué es un contexto están enunciadas más abajo.

$$\frac{\Gamma \vdash}{\Gamma \vdash \mathcal{U}_i : \mathcal{U}_{i+1}}\mathcal{U}\text{-Intro} \qquad \frac{\Gamma \vdash A : \mathcal{U}_i}{\Gamma \vdash A : \mathcal{U}_{i+1}}\mathcal{U}\text{-Cumul}$$

Que en resumen dicen que los universos forman una jerarquía acumulativa pues cada universo es de tipo el siguiente universo y si un tipo está en algún universo, está también en los que le siguen. Además se establece que la igualdad definicional es una relación de equivalencia respetada por la tipificación:

$$\frac{\Gamma \vdash a : A}{\Gamma \vdash a = a : A} \quad \frac{\Gamma \vdash a = b : A}{\Gamma \vdash b = a : A} \quad \frac{\Gamma \vdash a = b : A \quad \Gamma \vdash b = c : A}{\Gamma \vdash a = c : A} \quad \frac{\Gamma \vdash a = b : A \quad \Gamma \vdash A = B : \mathcal{U}_i}{\Gamma \vdash a = b : B} \quad \frac{\Gamma \vdash a : A \quad \Gamma \vdash A = B : \mathcal{U}_i}{\Gamma \vdash a : B}$$

Con esto se ha formalizado gran parte de lo que no se había tratado en secciones previas. Lo que resta de la sección consiste básicamente en repetir lo dicho en secciones previas pero con la notación y especificaciones formales adoptadas en esta. Así, el siguiente paso para formalizar la teoría de tipos es presentar las reglas de *formadores de tipos* clasificadas en cinco:

- **Reglas de Formación** que establecen cuándo es posible aplicar el *formador de tipos* o construir un tipo. Son el equivalente en teoría de conjuntos a decir cuándo existe un conjunto.
- **Reglas de Introducción** que indican cómo invocar términos del tipo, i.e. cuándo existen los "elementos" del tipo.
- **Reglas de Eliminación** que muestran cuándo será posible operar con los elementos del tipo formado (posiblemente usando eliminadores).
- **Reglas de Computación** que explican lo que sucede con los términos de un tipo al aplicarles los eliminadores.
- **Principios de Unicidad** que señalan de qué manera cada elemento del tipo formado está únicamente determinado por la aplicación de los eliminadores.

La primera clase de tipos vista en las secciones pasadas son los *tipos de funciones dependientes* $\prod_{x:A} B(x)$ obtenidos a partir de un tipo $A : \mathcal{U}$ y una familia indizada por éste, i.e. $B(x) : \mathcal{U}_i$ con $x : A$. Originalmente se planeaba que fuesen el equivalente al producto cartesiano arbitrario de una familia de objetos en teoría de conjuntos. Por esta misma razón sus elementos son funciones únicamente determinadas como λ-expresiones. Esto se expresa en el sistema formal codificando la expresión $\prod_{x:A} B(x)$ con el λ-término $c_\Pi((\lambda(x : A).B))$ y empleando las reglas:

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma, x : A \vdash B : \mathcal{U}_i}{\Gamma \vdash \Pi_{x:A} B : \mathcal{U}_i}\Pi\text{-Form} \quad \frac{\Gamma, x : A \vdash b : B}{\Gamma \vdash (\lambda(x{:}A).b) : \Pi_{x:A} B}\Pi\text{-Intro} \quad \frac{\Gamma \vdash a : A \quad \Gamma \vdash f : \Pi_{x:A} B}{\Gamma \vdash f(a) : B[a/x]}\Pi\text{-Elim}$$

$$\frac{\Gamma \vdash a : A \qquad \Gamma, x : A \vdash b : B}{\Gamma \vdash (\lambda(x{:}A).b)(a) = b[a/x] : B[a/x]}\Pi\text{-Comp} \qquad \frac{\Gamma \vdash f : \Pi_{x:A}B}{\Gamma \vdash f = (\lambda(x{:}A).f(x)) : \Pi_{x:A}B}\Pi\text{-Uniq}$$

Donde una expresión de la forma $\Phi[\alpha/\beta]$ representa la expresión Φ con toda instancia no acotada (por el acotador λ) de β sustituida por α.[12] Cuando $B(x)$ no depende de $x : A$, se tiene el clásico tipo de funciones de A en B, es decir, $A \to B$. Además de éstas cinco reglas, cada formador de tipos incluye una regla expresando que su respectivo constructor preserva la igualdad definicional, por ejemplo:

$$\frac{\Gamma \vdash A = A' : \mathcal{U}_i \qquad \Gamma, x : A \vdash B = B' : \mathcal{U}_i \qquad \Gamma, x : A \vdash b = b' : B}{\Gamma \vdash (\lambda(x{:}A).b) = (\lambda(x{:}A).b') : \Pi_{x:A}B}\Pi\text{-Intro-Eq}$$

Este último tipo de reglas se dejará tácito en esta presentación. Más aún, de ahora en adelante se omitirán los nombres de las reglas respetando el orden proporcionado anteriormente (salvo ocasiones en las que deba variar la presentación) y, dado que los principios de unicidad restantes son derivables en la teoría (como el que se derivó para el tipo de parejas dependientes), tampoco serán explícitamente escritos en lo sucesivo.

La segunda clase de tipos vistos con anterioridad son los *tipos de parejas dependientes* $\sum_{x:A} B(x)$, los cuales se forman de la misma manera que los de la clase anterior. El eliminador para éstos o *principio de inducción para parejas dependientes* ind_Σ establece el enunciado ya conocido: "dada una familia $Q(p) : \mathcal{U}_i$ con $p : \sum_{x:A} B(x)$, construir una función que vaya de la suma a la familia $f : \prod_{p:\sum_{x:A} B(x)} Q(p)$ sólo requiere tener otra análoga $g : \prod_{a:A} \prod_{b:B(a)} Q(a, b)$ que sea evaluada iteradamente, proceso conocido como *currying*, es decir, si $a : A$ y $b : B(a)$ entonces realmente $f(a, b) = g(a)(b) : Q(a, b)$". Formalmente:

$$\frac{\begin{array}{l}\Gamma \vdash A : \mathcal{U}_i \\ \Gamma, x : A \vdash B : \mathcal{U}_i\end{array}}{\Gamma \vdash \Sigma_{x:A}B : \mathcal{U}_i} \qquad \frac{\begin{array}{l}\Gamma, x : A \vdash B : \mathcal{U}_i \\ \Gamma \vdash a : A \\ \Gamma \vdash b : B[a/x]\end{array}}{\Gamma \vdash \langle a, b\rangle : \Sigma_{x:A}B} \qquad \frac{\begin{array}{l}\Gamma, z : \Sigma_{x:A}B \vdash Q : \mathcal{U}_i \\ \Gamma, x : A, y : B \vdash g : Q[\langle x, y\rangle/z] \\ \Gamma \vdash p : \Sigma_{x:A}B\end{array}}{\Gamma \vdash \mathrm{ind}_\Sigma(z.Q, x.y.g, p) : Q[p/z]}$$

$$\frac{\Gamma, z : \Sigma_{x:A}B \vdash Q : \mathcal{U}_i \qquad \Gamma, x : A, y : B \vdash g : Q[\langle x, y\rangle/z] \qquad \Gamma \vdash a' : A \qquad \Gamma \vdash b' : B[a'/x]}{\Gamma \vdash \mathrm{ind}_\Sigma(z.Q, x.y.g, \langle a', b'\rangle) = g[a', b'/x, y] : Q[\langle a', b'\rangle/z]}$$

Donde $\sum_{x:A} B(x)$ es codificado mediante el término $c_\Sigma((\lambda(x : A).B))$ que acota todas las instancias libres de x en B. Además, las cadenas $x.y.g$ y $z.Q$ representan la acotación de x, y y z en g y Q respectivamente para el término $c_{\mathrm{ind}_{\Sigma_{x:A}B}}(z.Q)(x.y.g)(p)$

[12]Aunque esta definición no se ve en este capítulo, es prácticamente la misma que la definida para la semántica de la lógica predicativa con las diferencias involucradas por el lenguaje como que el símbolo acotador es λ en vez de $\forall$ o $\exists$.

quien codifica al inductor ind_Σ. Más aún, siempre que $B(x)$ no dependa de $x : A$, el tipo de parejas dependientes $\sum_{x:A} B$ se abrevia con la notación de producto cartesiano $A \times B$.

Las reglas de los *tipos coproducto* $A + B$ en HoTT, siguiendo las mismas convenciones de acotación y uso de constantes del párrafo anterior para los tipos de parejas dependientes, se formalizan por:[13]

$$\frac{\begin{array}{c}\Gamma \vdash A : \mathcal{U}_i \\ \Gamma \vdash B : \mathcal{U}_i\end{array}}{\Gamma \vdash A + B : \mathcal{U}_i} + \text{-Form} \qquad \frac{\begin{array}{c}\Gamma \vdash A : \mathcal{U}_i \\ \Gamma \vdash B : \mathcal{U}_i \\ \Gamma \vdash a : A\end{array}}{\Gamma \vdash \iota_1(a) : A + B} + \text{-Intro1} \qquad \frac{\begin{array}{c}\Gamma \vdash A : \mathcal{U}_i \\ \Gamma \vdash B : \mathcal{U}_i \\ \Gamma \vdash b : B\end{array}}{\Gamma \vdash \iota_2(b) : A + B} + \text{-Intro2}$$

$$\frac{\Gamma, z : A + B \vdash Q : \mathcal{U}_i \quad \Gamma, x : A \vdash g_1 : Q[\iota_1(x)/z] \quad \Gamma, y : B \vdash g_2 : Q[\iota_2(y)/z] \quad \Gamma \vdash w : A + B}{\Gamma \vdash \mathrm{ind}_{A+B}(z.Q, x.g_1, y.g_2, w) : Q[w/z]} + \text{-Elim}$$

$$\frac{\Gamma, z : A + B \vdash Q : \mathcal{U}_i \quad \Gamma, x : A \vdash g_1 : Q[\iota_1(x)/z] \quad \Gamma, y : B \vdash g_2 : Q[\iota_2(y)/z] \quad \Gamma \vdash a : A}{\Gamma \vdash \mathrm{ind}_{A+B}(z.Q, x.g_1, y.g_2, \iota_1(a)) = g_1[a/x] : Q[\iota_1(a)/z]} + \text{-Comp1}$$

$$\frac{\Gamma, z : A + B \vdash Q : \mathcal{U}_i \quad \Gamma, x : A \vdash g_1 : Q[\iota_1(x)/z] \quad \Gamma, y : B \vdash g_2 : Q[\iota_2(y)/z] \quad \Gamma \vdash b : B}{\Gamma \vdash \mathrm{ind}_{A+B}(z.Q, x.g_1, y.g_2, \iota_2(b)) = g_2[b/y] : Q[\iota_2(b)/z]} + \text{-Comp2}$$

En secciones anteriores también se vio que el *tipo vacío* $\mathbf{0} : \mathcal{U}_i$ y el *tipo unidad* $\mathbf{1} : \mathcal{U}_i$ pueden ser construidos a partir de cualquier contexto. Se pretende que el primero no tenga elementos, por lo cual no tiene reglas de introducción ni computación y se conviene que en el caso de que se hallase un término $z : \mathbf{0}$, entonces cualquier tipo concebible estará habitado (siguiendo el principio lógico *ex falso quodlibet*). Por otro lado, el tipo unidad siempre está habitado y únicamente tiene un "elemento". Formalmente:

$$\frac{\Gamma \vdash}{\Gamma \vdash \mathbf{0} : \mathcal{U}_i} \mathbf{0}\text{-Form} \qquad \frac{\Gamma, x : \mathbf{0} \vdash Q : \mathcal{U}_i \quad \Gamma \vdash z : \mathbf{0}}{\Gamma \vdash \mathrm{ind}_{\mathbf{0}}(x.Q, z) : Q[z/x]} \mathbf{0}\text{-Elim}$$

$$\frac{\Gamma \vdash}{\Gamma \vdash \mathbf{1} : \mathcal{U}_i} \qquad \frac{\Gamma \vdash}{\Gamma \vdash \star : \mathbf{1}} \qquad \frac{\begin{array}{c}\Gamma, x : \mathbf{1} \vdash Q : \mathcal{U}_i \\ \Gamma, y : \mathbf{1} \vdash g : Q[y/x] \\ \Gamma \vdash a : \mathbf{1}\end{array}}{\Gamma \vdash \mathrm{ind}_{\mathbf{1}}(x.Q, y.g, a) : Q[a/x]} \qquad \frac{\begin{array}{c}\Gamma, x : \mathbf{1} \vdash Q : \mathcal{U}_i \\ \Gamma, y : \mathbf{1} \vdash g : Q[y/x]\end{array}}{\Gamma \vdash \mathrm{ind}_{\mathbf{1}}(x.Q, y.g, \star) = g[\star/y] : Q[\star/x]}$$

[13]Las reglas se presentan de manera extendida para que el lector pueda apreciar las ligeras diferencias entre las de eliminación y las de computación.

Al igual que el vacío y la unidad, el *tipo de números naturales* $\mathbb{N} : \mathcal{U}_i$ se puede construir bajo cualquier contexto. La construcción de los elementos de este tipo como ya se vio antes es recursiva y, por ende, requere de más de una regla de introducción. Así mismo, su principio de inducción para el tipo de los naturales o eliminador es equivalente bajo Curry-Howard al principio de inducción de los números naturales en matemáticas y se formaliza por:

$$\frac{\Gamma \vdash}{\Gamma \vdash \mathbb{N} : \mathcal{U}_i}\mathbb{N}\text{-Form} \qquad \frac{\Gamma \vdash}{\Gamma \vdash 0 : \mathbb{N}}\mathbb{N}\text{-Intro1} \qquad \frac{\Gamma \vdash n : \mathbb{N}}{\Gamma \vdash S(n) : \mathbb{N}}\mathbb{N}\text{-Intro2}$$

$$\frac{\Gamma, x : \mathbb{N} \vdash P : \mathcal{U}_i \quad \Gamma \vdash c_0 : P[0/x] \quad \Gamma, x : \mathbb{N}, y : P \vdash c_S : P[S(x)/x] \quad \Gamma \vdash n : \mathbb{N}}{\Gamma \vdash \mathrm{ind}_{\mathbb{N}}(x.P, c_0, x.y.c_S, n) : P[n/x]}\mathbb{N}\text{-Elim}$$

$$\frac{\Gamma, x : \mathbb{N} \vdash P : \mathcal{U}_i \quad \Gamma \vdash c_0 : P[0/x] \quad \Gamma, x : \mathbb{N}, y : P \vdash c_S : P[S(x)/x]}{\Gamma \vdash \mathrm{ind}_{\mathbb{N}}(x.P, c_0, x.y.c_S, 0) = c_0 : P[0/x]}\mathbb{N}\text{-Comp1}$$

$$\frac{\Gamma, x : \mathbb{N} \vdash P : \mathcal{U}_i \quad \Gamma \vdash c_0 : P[0/x] \quad \Gamma, x : \mathbb{N}, y : P \vdash c_S : P[S(x)/x] \quad \Gamma \vdash n : \mathbb{N}}{\Gamma \vdash \mathrm{ind}_{\mathbb{N}}(x.P, c_0, x.y.c_S, S(n)) = c_S[n, \mathrm{ind}_{\mathbb{N}}(x.P, c_0, x.y.c_S, n))/x, y] : P[S(n)/x]}\mathbb{N}\text{-Comp2}$$

Finalmente, los últimos tipos de la teoría son los *tipos igualdades proposicionales*. Las reglas de éstos prácticamente ya fueron dadas pero se modifican en la presente sección de tal manera que no falten hipótesis omitidas previamente por motivos de claridad al explicar su función:

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash a : A \quad \Gamma \vdash b : A}{\Gamma \vdash \mathrm{Id}_A(a, b) : \mathcal{U}_i} = \text{-Form} \qquad \frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash a : A}{\Gamma \vdash r_a : \mathrm{Id}_A(a, a)} = \text{-Intro}$$

$$\frac{\begin{array}{c}\Gamma, x : A, y : A, p : \mathrm{Id}_A(x, y) \vdash Q : \mathcal{U}_i \\ \Gamma, z : A \vdash g : Q[z, z, r_z/x, y, p] \quad \Gamma \vdash a : A \quad \Gamma \vdash b : A \quad \Gamma \vdash p' : \mathrm{Id}_A(a, b)\end{array}}{\Gamma \vdash \mathrm{ind}_{=_A}(x.y.p.Q, z.g, a, b, p') : Q[a, b, p'/x, y, p]} = \text{-Elim}$$

$$\frac{\Gamma, x : A, y : A, p : \mathrm{Id}_A(x, y) \vdash Q : \mathcal{U}_i \quad \Gamma, z : A \vdash g : Q[z, z, r_z/x, y, p] \quad \Gamma \vdash a : A}{\Gamma \vdash \mathrm{ind}_{=_A}(x.y.p.Q, z.g, a, a, r_a) = g[a/z] : Q[a, a, r_a/x, y, p]} = \text{-Comp}$$

La teoría desarrollada hasta ahora corresponde a MLTT, es decir, la teoría intuicionista de tipos. Para obtener al sistema formal HoTT de la teoría de tipos-homotopías es necesario agregar algunos "axiomas" más: *extensionalidad de funciones*, *univalencia* y aquellos para los *tipos de inducción superior*. Extensionalidad de funciones se sigue de univalencia, mientras que los tipos de inducción superior (HIT's por sus siglas en inglés: *Higher Inductive Types*) se van agregando conforme se necesitan en la teoría y, al conocimiento del autor, es un problema abierto la determinación de una única regla (esquema de regla) que determine a todos los HIT's permisibles. A continuación se presentan los primeros dos "axiomas", i.e. extensionalidad de funciones y univalencia, reservando su explicación detallada a la siguiente sección:

$$\frac{\Gamma \vdash f : \Pi_{x:A} B \qquad \Gamma \vdash g : \Pi_{x:A} B}{\Gamma \vdash \mathrm{funExt}(f,g) : \mathrm{isEquiv}(\mathrm{hApply}_{f,g})} = \Pi\text{-Ext}$$

Como su nombre lo indica, el principio de extensionalidad de funciones está dictando que dos funciones $f, g : \Pi_{x:A} B$ son iguales, si coinciden en las imágenes de cada uno de sus puntos. Esto se puede expresar como una *equivalencia* entre el tipo $\mathrm{Id}_{\Pi_{x:A} B(x)}(f,b)$ y $\prod_{x:A} \mathrm{Id}_{B(x)}(f(x), g(x))$ (con base en la correspondencia Curry-Howard). De esta manera, la regla Π-Ext afirma la veracidad de dicha equivalencia.

Por otro lado, el axioma de univalencia intuitivamente expresa la oración "siempre que dos tipos sean equivalentes, afirmarlo es equivalente a decir que son iguales." De manera informal esto se suele representar mediante $(A \simeq B) \simeq (A = B)$ y formalmente se escribe especificando quién es el testigo de dicha equivalencia:

$$\frac{\Gamma \vdash A : \mathcal{U}_i \qquad \Gamma \vdash B : \mathcal{U}_i}{\Gamma \vdash \mathrm{univ}(A,B) : \mathrm{isEquiv}(\mathrm{idToEquiv}_{A,B})} = \mathcal{U}\text{-Univ}$$

V. Interpretación Homotópica y Motivación en Matemáticas

No obstante la interpretación dada originalmente por Per Martin-Löf o la correspondencia Curry-Howard-Lambek, la idea central de la *teoría de tipos homotopías* es que los tipos pueden ser vistos como espacios de la *teoría de homotopías* o *grupoides de dimensión superior* de la teoría de categorías:

Cuando se habla de espacios en la teoría de homotopías clásicamente se hace referencia a un conjunto de puntos X equipado con una topología τ. Comúnmente se puede hablar de trayectorias o caminos entre dos puntos x, y del espacio, las cuales son representadas por una función continua $p : [0,1] \to X$ donde $p(0) = x$ y $p(1) = y$. Estos caminos se pueden concatenar de tal manera que la concatenación de un camino p, de x a y, y otro q, de y a z, es un camino $p \centerdot q$ de x a z. Se tiene también la existencia de un camino identidad que es constante todo el tiempo en un mismo punto. Más aun, dado un camino p de x a y, hay otro camino inverso p^{-1} tales que concatenados nos dan un ciclo/lazo/bucle $p \cdot p^{-1}$ de x a x. Estas propiedades se asemejan a los axiomas de grupos, salvo que en grupos no existen "varias identidades", i.e. ciclos, ni "varios inversos", i.e. caminos del final de un camino al inicio de éste. Además, el lazo $p \centerdot p^{-1}$ con p de x a y no es exactamente igual al camino "estático"-identidad ni es necesariamente igual al ciclo $p \centerdot q$ con q de y a x. No obstante, una generalización natural al concepto de trayectoria consiste en ver a las mismas trayectorias como puntos y pensar en trayectorias entre trayectorias. Así, si se tienen dos trayectorias $p, q : [0,1] \to X$ de x a y, a una trayectoria entre éstas se le llama homotopía de p a q que formalmente se concibe como una función continua $H : [0,1] \times [0,1] \to X$, la cual satisface que $H(s,0) = p(s)$, $H(s,1) = q(s)$ para cada $s \in [0,1]$ y $H(0,t) = x$, $H(1,t) = y$ para cada $t \in [0,1]$. Esta generalización puede continuar y engendrar una jerarquía donde los caminos son homotopías de dimensión 1, las homotopías tradicionales tienen dimensión 2 y hay más homotopías n-dimensionales, cada una de las cuales es respetada por las operaciones de $n-1$-concatenación y $n-1$-inversos. La estructura algebraica descrita por esta jerarquía infinita es comúnmente denominada ∞-grupoide (débil), la cual es un tipo especial de categoría de dimensión superior.

Ahora obsérvese que los tipos, gracias a la igualdad proposicional, se comportan bajo esta estructura de ∞-grupoide (débil), pues la regla de introducción de los tipos igualdad proposicional puede aplicarse a ellos mismos. Es decir, si $p : \mathrm{Id}_A(x,y)$ y $q : \mathrm{Id}_A(x,y)$ es posible construir el tipo $\mathrm{Id}_{\mathrm{Id}_A(x,y)}(p,q) : \mathcal{U}_i$. Así, suponiendo que todo tipo $A : \mathcal{U}_i$ representa un espacio, dados dos puntos de éste $x, y : A$, si $p : \mathrm{Id}_A(x,y)$, entonces p puede verse como una trayectoria que conecta x con y en A. En otras palabras, el tipo $\mathrm{Id}_A(x,y)$ se interpreta como el espacio de caminos de x a y. Por consecuencia si H es un elemento de $\mathrm{Id}_{\mathrm{Id}_A(x,y)}(p,q)$, i.e. $H : \mathrm{Id}_{\mathrm{Id}_A(a,b)}(p,q)$, entonces H representa una homotopía entre p y q. Siguiendo con la interpretación dada, se pueden definir homotopías de dimensión más alta, sólo hay que considerar el tipo igualdad proposicional para cualesquier dos homotopías. Por todo esto, en la presente sección se adoptará la notación $x \rightsquigarrow_A y$ para el tipo $\mathrm{Id}_A(x,y)$ y se omitirá el subíndice cuando sea claro de quién se está hablando.

Nótese que bajo la interpretación homotópica de los tipos, el *principio de inducción de tipos igualdad proposicional* se convierte en el siguiente enunciado: "para demostrar una propiedad de todos los caminos de $a : A$ a $b : A$ es suficiente con probar que los lazos (bucles/ciclos) la satisfacen, i.e. dada una familia $Q(x,y,r)$ con $x, y : A$ y $r : x \rightsquigarrow y$, construir una función $f : \prod_{x,y:A} \prod_{r:x \rightsquigarrow y} Q(x,y,r)$ requiere tener otra únicamente definida en los lazos $g : \prod_{x:A} Q(x,x,r_x)$ de tal modo que $f(x,x,r_x) = g(x)$." De la misma manera en que se cambió de notación de $\mathrm{Id}_A(x,y)$ a $x \rightsquigarrow_A y$, se renombra este principio como *principio de inducción de caminos*.

I. Estructura ω-grupoide de los tipos igualdad proposicional

En lo subsiguiente se enuncian una serie de propiedades que validan la interpretación recientemente descrita. El lector habrá observado que las pruebas formales en teoría de tipos requieren de cadenas largas de símbolos y es de esperarse que la longitud de éstas solo incremente. Por ello, de la misma manera que en el capítulo de teoría de conjuntos donde se pasó de pruebas formales a argumentos rigurosos, aquí la prueba para la primera de las demostraciones se realiza de la manera más apegada posible a la semi-formalidad de secciones previas, mientras que las pruebas sucesivas serán similares a las demostraciones estándar en la literatura:

Lema V.1 (Existencia de un camino inverso)
Dado un tipo $A : \mathcal{U}$ y dos términos suyos $a, b : A$, si hay un camino de a a b, entonces hay un camino de b a a. Esto es, existe una función $-^{-1} : (a \rightsquigarrow b) \to (b \rightsquigarrow a)$ tal que para $x : A$, si $r : x \rightsquigarrow x$, entonces $(r)^{-1} = r$.

Demostración. Recordando la correspondencia Curry-Howard, el enunciado del lema es equivalente a $\prod_{a,b:A}(a \rightsquigarrow b) \to (b \rightsquigarrow a)$ que en notación de tipos dependientes se vuelve:

$$\prod_{a,b:A} \prod_{r:a \rightsquigarrow b} (b \rightsquigarrow a)$$

Por ende, se desea construir un testigo de tal tipo, i.e. la función $-^{-1}$. Para resolver dicho problema se usará inducción de caminos. Así, por la regla de introducción de los tipos igualdad proposicional, se sabe que si $a : A$, entonces se puede implicar la existencia de un testigo de la reflexividad de la igualdad en a, i.e. $r_a : a \rightsquigarrow a$. Por Π-Intro, $\lambda a.r_a : \prod_{a:A} a \rightsquigarrow a$. Aplicando inducción de caminos se tiene que para cada $r : a \rightsquigarrow b$, el término $\mathrm{ind}_{=_A}(b \rightsquigarrow a, \lambda a.r_a, a, b, r) : b \rightsquigarrow a$ y además satisface que $\mathrm{ind}_{=_A}(b \rightsquigarrow a, \lambda x.r_x, a, b, r) = r_a$. Nuevamente por Π-Intro se concluye que:

$$r^{-1} := \lambda a.\lambda b.\lambda r.\,\mathrm{ind}_{=_A}(b \rightsquigarrow a, \lambda a.r_a, a, b, r) : \prod_{a,b:A} \prod_{r:a \rightsquigarrow b} (b \rightsquigarrow a)$$

■

Lema V.2 (Concatenación de caminos)
Es posible concatenar caminos, esto es, dado un tipo $A : \mathcal{U}$ y términos $a, b, c : A$ existe una función $- \centerdot - : (a \rightsquigarrow b) \to (b \rightsquigarrow c) \to (a \rightsquigarrow c)$ tal que para cada $x : A$, el testigo de la reflexividad de la igualdad de x, r_x, cumple que $r_x \centerdot r_x = r_x$.

Demostración. Se debe construir un testigo de $a \rightsquigarrow c$, suponiendo que $p : a \rightsquigarrow b$ y $q : b \rightsquigarrow c$ con $a, b, c : A$. Se probará esto por inducción de caminos sobre $p : a \rightsquigarrow b$ seguida de otra sobre $q : b \rightsquigarrow c$. La primera hipótesis de inducción es que $b = a$ y $p = r_a$ por lo que $q : a \rightsquigarrow c$. La segunda consiste en asumir que $c = a$ y, en consecuencia, que $q = r_a$. De esta forma $r_a : a \rightsquigarrow a = a \rightsquigarrow c$ y, siempre que $a = b = c$, se cumplirá $r_a \centerdot r_a = r_a$. Por inducción de caminos se concluye lo deseado. ■

Nótese que las pruebas anteriores corresponden a la simetría y transitividad de la igualdad proposicional, es decir que $(-)^{-1} : (a =_A b) \to (b =_A a)$ y que $(-\centerdot-) : (a =_A b) \to (b =_A c) \to (a =_A c)$. No obstante, para validar la interpretación homotópica, estas propiedades no son suficientes pues además también se debe demostrar el comportamiento como neutro de los lazos $r_a : p \rightsquigarrow p$, la asociatividad de $\centerdot$ y que los caminos inversos realmente se comportan como inversos bajo $\centerdot$:

Teorema V.3 (Estructura ω-grupoide de los tipos igualdad proposicional)
Si $a, b, c, d : A$, $p : a \rightsquigarrow b$, $q : b \rightsquigarrow c$, y $r : c \rightsquigarrow d$, entonces:[14]

[14]Nótese que las igualdades enunciadas en el lema son igualdades proposicionales y que, por motivos de claridad, son presentadas con el tipo al que hacen referencia encima del símbolo "=".

I. Los lazos son "neutros": $p \overset{a\rightsquigarrow b}{=\!=} p \blacksquare r_b$ y $p \overset{a\rightsquigarrow b}{=\!=} r_a \blacksquare p$.

II. Inversos operados con su original son lazos: $p^{-1} \blacksquare p \overset{b\rightsquigarrow b}{=\!=} r_b$ y $p \blacksquare p^{-1} \overset{a\rightsquigarrow a}{=\!=} r_a$.

III. Inverso del inverso es el original: $(p^{-1})^{-1} \overset{a\rightsquigarrow b}{=\!=} p$.

IV. La concatenación es asociativa: $p \blacksquare (q \blacksquare r) \overset{a\rightsquigarrow d}{=\!=} (p \blacksquare q) \blacksquare r$.

Demostración. Cada prueba requiere de la inducción sobre caminos:

I. La hipótesis de inducción dice que $r_a = p = r_b$. En este caso, de la prueba anterior sabemos que $p = r_a = r_a \blacksquare r_a = r_a \blacksquare p$. Por ser definicionalmente iguales $r_p : (p \rightsquigarrow p) = (p \rightsquigarrow r_a \blacksquare p) = (p \overset{a\rightsquigarrow b}{=\!=} r_a \blacksquare p)$.

II. Por hipótesis inductiva $r_a = p = r_b$. Así, $p^{-1} = r_a^{-1} = r_a$. Por ende $p \blacksquare p^{-1} = r_a$. Invóquese el correspondiente testigo proposicional por $=$-Intro.

III. Sabiendo que $r_a = p$ compútese $(p^{-1})^{-1}$.

IV. La primera inducción asume que $r = r_a$, la segunda que $q = r_a$ y la tercera, $p = r_a$. Computando lo requerido se obtiene que $r_{r_a} : r_a \rightsquigarrow r_a = r_a \blacksquare (r_a \blacksquare r_a) \rightsquigarrow (r_a \blacksquare r_a) \blacksquare r_a = p \blacksquare (q \blacksquare r) \rightsquigarrow (p \blacksquare q) \blacksquare r$.

■

Otra propiedad, en términos de la correspondencia Curry-Howard, es que toda función respeta las igualdades proposicionales. Topológicamente esto significa que todas las funciones en HoTT preserven caminos, es decir, son continuas:

Teorema V.4 (Funciones no dependientes se comporten functorialmente)
Dada una función $f : A \to B$, para cualesquiera $x, y : A$ se cumple que:

$$\mathrm{ap}_f : (x \rightsquigarrow y) \to (f(x) \rightsquigarrow f(y)) \text{ donde } \mathrm{ap}_f(r_x) = r_{f(x)}$$

Aquí ap_f puede leerse como "la aplicación de f a un camino" o "la acción sobre caminos de f". Además, suponiendo que $f : A \to B, g : B \to C, p : x \rightsquigarrow_A y$ y que $q : y \rightsquigarrow_A z$, son válidas las igualdades proposicionales:

I. $\mathrm{ap}_f(p \blacksquare q) = \mathrm{ap}_f(p) \blacksquare \mathrm{ap}_f(q)$.

II. $\mathrm{ap}_f(p^{-1}) = \mathrm{ap}_f(p)^{-1}$.

III. $\mathrm{ap}_g(\mathrm{ap}_f(p)) = \mathrm{ap}_{g\circ f}(p)$.

IV. $\mathrm{ap}_{\lambda x.x}(p) = p$.

Demostración. Para la primera parte (la construcción de ap_f) se asume, por hipótesis inductiva que $x = y$, de la cual se deriva un testigo $p : x = y$ que realmente es $r_x : x = x$. Además se sabe que existe un téstigo de la reflexividad de la igualdad en $f(x)$, i.e. $r_{f(x)} : f(x) = f(x)$. Así se define ap_f como la función que al testigo de $x = y$ lo manda al testigo de la reflexividad de la igualdad en $f(x)$, i.e. $\mathrm{ap}_f(p) := r_{f(x)} : (f(x) \rightsquigarrow f(x)) = (f(x) \rightsquigarrow f(y))$. Para las restantes cuatro propiedades:

I. Por una primera hipótesis inductiva, $p = r_x$, i.e. $p : x =_A y$. De aquí se obtiene que $q : x =_A z$. Por una segunda hipótesis inductiva, $q = r_x$. Con esto se obtiene que $\mathrm{ap}_f(p \centerdot q) = \mathrm{ap}_f(r_x \centerdot r_x) = \mathrm{ap}_f(r_x) = \mathrm{ap}_f(r_x) \centerdot \mathrm{ap}_f(r_x) = \mathrm{ap}_f(p) \centerdot \mathrm{ap}_f(q)$. Por inducción de caminos dos veces se obtiene lo deseado.

II. Por hipótesis inductiva $p = r_x$, de aquí que:
$\mathrm{ap}_f(p^{-1}) = \mathrm{ap}_f(r_x^{-1}) = \mathrm{ap}_f(r_x) = r_{f(x)} = r_{f(x)}^{-1} = (\mathrm{ap}_f(r_x))^{-1} = \mathrm{ap}_f(p)^{-1}$.

III. Nuevamente por la hipótesis inductiva se obtendrá que:
$\mathrm{ap}_g(\mathrm{ap}_f(p)) = r_{g(f(x))} = r_{g\circ f(x)} = \mathrm{ap}_{g\circ f}(p)$.

IV. La prueba es una aplicación directa de una inducción de caminos.

■

Es común que en vez de $\mathrm{ap}_f(p)$ se abuse de la notación y se escriba $f(p)$. Con esta notación se hace más clara la “functorialidad” de las funciones:

I. $f(p \centerdot q) = f(p) \centerdot f(q)$.

II. $f(p^{-1}) = (f(p))^{-1}$.

III. $g(f(p)) = g \circ f(p)$.

IV. $(\lambda x.x)(p) = p$.

Sería deseable tener el mismo resultado para las funciones dependientes, sin embargo, esto no es posible directamente en teoría de tipos ya que si $f : \prod_{a:A} B(a)$ y $p : x \rightsquigarrow_A y$, entonces $f(x) : B(x)$ mientras que $f(y) : B(y)$. La conclusión se sigue de que no se pueden igualar dos términos de distintos tipos. No obstante, el problema se puede sortear mediante el uso del siguente lema que, por Curry-Howard, es básicamente la indiscernibilidad de los idénticos:

Teorema V.5 (Transporte)
Suponiendo que $x : A \vdash P(x) : \mathcal{U}_i$ y que $p : \mathrm{Id}_A(x, y)$, se puede construir una función $p_* : P(x) \to P(y)$.

Demostración. Por inducción $x = y$ y $p = r_x$. Así $\lambda(t : P(x)).t : P(x) \to P(x)$. Definiendo la función $r_{x*} = p_* := \lambda(t : P(x)).t$ se cumple lo deseado.[15] ■

[15]Cuando el tipo dependiente requiera ser expresado en vez de la notación p_* se suele usar $\mathrm{transport}^P(p, -)$.

Lema V.6 (Del mapeo dependiente)
Para $f : \prod_{a:A} P(a)$ se tiene:

$$\mathrm{apd}_f : \prod_{p:x \rightsquigarrow_A y} p_*(f(x)) \rightsquigarrow_{P(y)} f(y)$$

Demostración. Asúmase que $x = y$ y que $r_x = p$. Por ende, $p_*(f(x)) = r_{x*}(f(x)) = f(x) = f(y)$ y $r_{f(x)} : f(x) \rightsquigarrow f(x)$. Definiendo $\mathrm{apd}_f := \lambda f.r_{f(x)}$ se concluye lo deseado. ■

Propiedades similares a la "functorialidad" de las funciones no-dependientes se pueden derivar involucrando al transporte y al apd. Para más información consúltese el libro oficial HoTT ([Pro13]) capítulo 2, sección 3.

II. Extensionalidad de funciones

Con base en la interpretación homotópica y la correspondencia Curry-Howard, sólo resta afirmar lo siguiente "que dos funciones $f, g : \prod_{a:A} B(a)$ sean iguales, i.e. $H : \mathrm{Id}(f, g)$, es equivalente a que coincidan en sus imágenes: $H' : \prod_{x:A} \mathrm{Id}(f(x), g(x))$". Ya que $\mathrm{Id}(f, g)$ representa los caminos entre f y g, sus elementos pueden ser considerdos homotopías, y como se espera que este tipo sea equivalente al tipo $\prod_{x:A} \mathrm{Id}(f(x), g(x))$, se llamará a este último el *tipo de homotopías* y se denotará por:

$$f \sim g := \prod_{x:A} \mathrm{Id}(f(x), g(x))$$

Topológicamente puede parecer erróneo definir al tipo de homotopías como las elecciones de caminos $f(x) \rightsquigarrow g(x)$ para $x : A$, pues esto es insuficiente en la teoría de homotopías clásica. Pero como las funciones en HoTT "son continuas", esto sí es posible en teoría de tipos-homotopías. Más aun, existen varios modelos para las homotopías, como los conjuntos simpliciales y modelos de Quillen de teoría de categorías, donde la definición recientemente dada es apropiada [Rij12, p. 27].

Con base en esto se puede probar que, en cada tipo de funciones no dependientes $A \to B$, la homotopía es una relación de equivalencia. Las pruebas para cada una de las propiedades de la relación $\sim$: reflexividad, simetría y transitividad, se especifican como sus respectivos "elementos":

$$\lambda f.\lambda x.r_{f(x)} : \prod_{f:A\to B} f \sim f$$

$$\lambda f.\lambda g.\lambda(H{:}f \sim g).\lambda x.(H(x))^{-1} : \prod_{f,g:A\to B} (f \sim g) \to (g \sim f)$$

$$\lambda f.\lambda g.\lambda h.\lambda(H_1{:}f \sim g).\lambda(H_2{:}g \sim h).\lambda x.H_1(x) \centerdot H_2(x) : \prod_{f,g,h:A\to B} (f \sim g) \to (g \sim h) \to (f \sim h)$$

Más aún, si las funciones en HoTT actúan functorialmente, se demuestra entonces que las homotopías actúan como *transformaciones naturales* de teoría de categorías:

Lema V.7 (Naturalidad de las homotopías)
Si $H : f \sim g$ es una homotopía entre $f, g : A \to B$ y $p : x \rightsquigarrow_A y$ es un camino de $x : A$ a $y : A$, entonces $H(x) \centerdot \mathrm{ap}_g(p) =_{\mathrm{Id}(f(x),g(x))} \mathrm{ap}_f(p) \centerdot H(y)$. Por abuso de notación esta igualdad proposicional se vuelve $H(x) \centerdot g(p) = f(p) \centerdot H(y)$ y en términos de diagramas se puede reescribir como:

$$\begin{tikzcd} g(x) \arrow[r, equal, "H(x)"] \arrow[d, equal, "g(p)"'] & f(x) \arrow[d, equal, "f(p)"] \\ g(y) \arrow[r, equal, "H(y)"'] & f(y) \end{tikzcd}$$

Demostración. Por hipótesis de inducción, definicionalmente se tiene que $x = y$ y $p = r_x$. De esta manera $H(x) \centerdot \mathrm{ap}_g(p) = H(x) \centerdot \mathrm{ap}_g(r_x) = H(x) \centerdot r_{g(x)} = H(x) = r_{f(x)} \centerdot H(x) = \mathrm{ap}_f(r_x) \centerdot H(x) = \mathrm{ap}_f(p) \centerdot H(y)$. La conclusión se sigue al aplicar $=$-Intro a esta igualdad. ■

Corolario V.8
Sea $H : f \sim \mathrm{Id}_A$ una homotopía con $f : A \to A$ e $1_A :\equiv \lambda(x : A).x$, entonces para cada $x : A$ se tiene que:

$$H(f(x)) = \mathrm{ap}_f(H(x))$$

Demostración. Por naturalidad de H, el siguiente diagrama conmuta:

$$\begin{tikzcd} 1_A(f(x)) \arrow[r, equal, "H(f(x))"] \arrow[d, equal, "H(x)"'] & f(f(x)) \arrow[d, equal, "\mathrm{ap}_f(H(x))"] \\ 1_A(x) \arrow[r, equal, "H(x)"'] & f(x) \end{tikzcd}$$

Lo cual quiere decir que $H(f(x)) \centerdot H(x) = \mathrm{ap}_f(H(x)) \centerdot H(x)$. Aplicando $(H(x))^{-1}$ de ambos lados se tiene lo deseado. ■

Pueden derivarse más propiedades de buen comportamiento bajo "$\centerdot$" similares a las obtenidas previamente para caminos pero esta vez para las homotopías; no obstante se regresará al problema de la equivalencia entre los dos tipos $\mathrm{Id}(f, g)$ y $\prod_{x:A} \mathrm{Id}(f(x), g(x))$. Por Curry-Howard, para generar un bicondicional (equivalencia lógica), uno nada más debería probar dos implicaciones, esto es, $\mathrm{Id}(f, g) \to (f \sim g)$ y $(f \sim g) \to \mathrm{Id}(f, g)$. No obstante, para preservar la estructura homotópica deseada, se definen las *equivalencias homotópicas* que, bajo Curry-Howard, corresponderían al tipo:

$$\sum_{g:B\to A} (f \circ g \sim (\lambda(y{:}B).y)) \times (g \circ f \sim (\lambda(x{:}A).x))$$

Para cada función no dependiente $f : A \to B$. Obsérvese que esta definición también casi coincide con la versión categórica de *isomorfismo*, pues se sabe que en una categoría $\mathcal{C}$, $f : A \to_{\mathcal{C}} B$ es un $\mathcal{C}$-isomorfismo si existe un $\mathcal{C}$-morfismo $g : B \to_{\mathcal{C}} A$ tal que $f \circ g = 1_B$ y $g \circ f = 1_A$, donde $1_X : X \to_{\mathcal{C}} X$ representa el morfismo identidad asociado al $\mathcal{C}$-objeto X. Pero por la naturaleza constructiva de HoTT y el enfoque filosófico de éste que dicta que "las pruebas previamente realizadas son relevantes para el trabajo en matemáticas", se opta por una definición alternativa, derogando al tipo anteror como el *tipo de las casi-inversas*, i.e.

$$\mathrm{qInv}(f) := \sum_{g:B\to A} (f \circ g \sim 1_B) \times (g \circ f \sim 1_A)$$

Así, el tipo que en HoTT sí vaya a ser la definición de "equivalencia homotópica", debe satisfacer las siguientes condiciones:

1. Para cada $f : A \to B$, son lógicamente equivalentes $\mathrm{qInv}(f)$ e $\mathrm{isEquiv}(f)$. Es decir, si $f : A \to B$, entonces $\mathrm{qInv}(f) \to \mathrm{isEquiv}(f)$ e $\mathrm{isEquiv}(f) \to \mathrm{qInv}(f)$ son válidas.

2. Para cualesquiera $e_1, e_2 : \mathrm{isEquiv}(f)$ se tiene que $\mathrm{Id}(e_1, e_2)$ es satisfecha.

Se verifica por inducción de caminos que el tipo:

$$\mathrm{isEquiv}(f) := \left(\sum_{g:B\to A} (f \circ g \sim 1_B) \right) \times \left(\sum_{h:B\to A} (h \circ f \sim 1_A) \right)$$

satisface la primera propiedad. Mientras que la segunda propiedad requiere de unos pocos resultados técnicos más para ser verificada. Con base en todo esto, se define al predicado "A y B son *homotópicamente equivalentes*" por:

$$A \simeq B := \sum_{f:A\to B} \mathrm{isEquiv}(f)$$

Obsérvese que esta sí es la definición de isomorfismo categórico pues primero se pide la existencia de inversos (izquierdo y derecho) y después se verifica que éstos coinciden (único inverso). Es fácil verificar que la relación de ser homotópicamente equivalentes es de equivalencia. Con todo esto en mente, se esperaría que, para $f, g : \prod_{x:A} B(x)$, hubiese un testigo de la veracidad de:

$$\mathrm{Id}(f, g) \simeq \prod_{x:A} \mathrm{Id}_{B(x)}(f(x), g(x))$$

Esto casi es demostrable en MLTT, pues se verifica por inducción de caminos la existencia de la función hApply de tipo:

$$\mathrm{hApply} : \mathrm{Id}(f, g) \to (f \sim g)$$

Pero para la equivalencia se requiere que hApply sea una equivalencia. Esto es precisamente lo que enuncia el *axioma de extensionalidad de funciones*:

$$\frac{\Gamma \vdash f : \Pi_{x:A}B \qquad \Gamma \vdash g : \Pi_{x:A}B}{\Gamma \vdash \mathrm{funExt}(f, g) : \mathrm{isEquiv}(\mathrm{hApply}_{f,g})} = \Pi\text{-Ext}$$

Es decir, que para $A, B(x) : \mathcal{U}_i$ con $x : A$ y $f, g : \prod_{x:A} B(x)$, la función $\mathrm{hApply}_{f,g}$ es una equivalencia. De aquí directamente se obtiene que:

$$(f =_\Pi g) \simeq (f \sim g)$$

Así, que dos funciones $f, g : \prod_{x:A} B(x)$ sean iguales equivale a afirmar que para cada $x : A$, se cumple que $f(x) =_{B(x)} g(x)$. No obstante, es deseable tener un resultado más fuerte. Uno que incluso haga a esta última equivalencia casi una igualdad proposicional. Para ello se agrega a MLTT el axioma de univalencia.

III. Univalencia

Es común en matemáticas tener dos mismos conjuntos para un mismo objeto. Por ejemplo, el plano cartesiano se puede representar por medio de los conjuntos/tipos $\mathbb{R}\times\mathbb{R}$, $2 \to \mathbb{R}$ e incluso $\{\langle x, y, z\rangle \in \mathbb{R}^3 \mid z = 0\}$. No obstante, los matemáticos denotan $\mathbb{R}^2$ a todos estos conjuntos/tipos sin preocuparse de cuál de ellos en específico se está hablando. Esto es posible gracias a la noción de isomorfismo de estructuras y a la *categoricidad* de éstas. Así, no importa cómo se hayan construido los números reales $\mathbb{R}$, ya sea por cortaduras de Dedekind, completación del espacio métrico de los racionales, como subconjunto del espacio de Baire o subconjunto de cualquier otra clase más grande como los surreales o los hyperreales, es posible dar una axiomatización (en lógica de segundo orden) de los números reales que permita probar que todas estas construcciones son instancias isomorfas del mismo objeto. En la práctica, el lógico desearía que el sistema formal que fundamente el trabajo del matemático garantice esta categoricidad y le permita deslindarse de cualquier trabajo extra que involucre probar que una u otra construcción de los números reales es equivalente al modelo estándar. Esta es precisamente la más importante consecuencia de agregar el axioma de univalencia de Voevodsky a la teoría de tipos de Martin-Löf. Es decir, si en MLTT se agrega univalencia, entonces se garantiza que dadas dos estructuras (tipos) isomorfas (homotópicamente equivalentes), éstas podrán considerarse en esencia (proposicionalmente) iguales, i.e:

$$(A =_{\mathcal{U}_i} B) \simeq (A \simeq B)$$

En primera instancia, de igual manera que con la extensionalidad de funciones, es posible demostrar en MLTT que:

$$\mathrm{idToEquiv} : \mathrm{Id}_{\mathcal{U}_i}(A, B) \to A \simeq B$$

No obstante que idToEquiv sea una equivalencia se escapa del alcance de MLTT, por lo que se enuncia el axioma de univalencia:

$$\frac{\Gamma \vdash A : \mathcal{U}_i \qquad \Gamma \vdash B : \mathcal{U}_i}{\Gamma \vdash \mathrm{univ}(A, B) : \mathrm{isEquiv}(\mathrm{idToEquiv}_{A,B})} = \mathcal{U}\text{-Univ}$$

Con el cual se garantiza, ya en HoTT, que idToEquiv es una equivalencia y, por lo tanto se concluye que:

$$(A =_{\mathcal{U}_i} B) \simeq (A \simeq B)$$

Con lo dicho hasta ahora se puede afirmar que, ya que desde la creación del sistema formal se tienen los números naturales, las funciones y sus respectivos comportamientos matemáticos característicos, es de esperarse que la implementación de las matemáticas sea posible. De hecho en "el libro HoTT" (HoTT book) [Pro13, Cap. 11] se implementan varias construcciones de los números reales en HoTT. Con esta última oración como referencia, es claro que lo presentado en esta tesis no es todo lo que la comunidad académica sabe del sistema HoTT, simplemente se ha hecho una presentación del sistema formal y algunas de sus consecuencias básicas. Particularmente, en el Instituto de Estudios Avanzados de Princeton se dedicó casi un año entero (9 meses del año académico 2012-2013) a la redacción del *HoTT book*, el cual es un compendio más extenso y detallado de cómo operan estos nuevos fundamentos de las matemáticas. En sí, la teoría de tipos homotopías es un área recientemente descubierta (2006) y con mucho potencial en diversos ámbitos. Las aplicaciones se reflejan en teoría de la computación donde se buscan semánticas para las *cubical type theories* (teorías de tipos cúbicas) que implican el axioma de univalencia y, por ende, la extensionalidad de funciones; en matemáticas donde el lenguaje formal de HoTT permite desarrollar pruebas en teoría de homotopías de manera sintáctica, i.e. sin hacer referencia a la analiticidad (continuidad) de las funciones, los caminos y las n-homotopías; en lógica, donde la estructura de ω-grupoide para los tipos forma una jerarquía que permite analizar las proposiciones en contraste con los conjuntos y otros tipos más complejos, o donde la simple correspondencia Curry-Howard permite el estudio fino de la lógica engendrada por HoTT, y en la filosofía de las matemáticas, donde nuevos fundamentos siempre son interesantes y aportan una mayor perspectiva respecto a lo que es y cómo se comporta el complejo ente denominado matemáticas.

Conclusión

A lo largo de este trabajo se ha llevado a cabo, en el marco de sistemas lógicos, la formalización de cuatro entes abstractos: la lógica proposicional, la lógica predicativa, la teoría de conjuntos y la teoría de tipos homotopía. En el caso de las lógicas se ha dado un argumento riguroso verificando que éstas coinciden con el comportamiento esperado de las mismas. En el caso de la teoría de conjuntos y la teoría de tipos homotopía, a manera de un argumento heurístico, se ha presentado evidencia en favor de que toda construcción matemática es realizable dentro de dichos sistemas. A continuación se realiza una enunciación detallada de los teoremas probados y objetos definidos en cada capítulo.

En los Preliminares se dio un marco de referencia sobre el cual se desarrollarían las siguientes secciones. Los conceptos importantes presentados en dicho capítulo son el de sistema formal, sistema lógico y sus constituyentes (lenguaje formal, aparato deductivo, teoría y semántica) así como las diversas propiedades que pueden o no llegar a tener; es decir, consistencia, robustez, completez y decidibilidad.

En el segundo capítulo, en la sección de lógica proposicional, se construyó un lenguaje formal cuyas fórmulas bien formadas servirían para representar proposiciones. Se enunciaron tres propiedades importantes de ese lenguaje en dicha sección: el principio de inducción sobre la complejidad de la fórmula, el teorema de legibilidad única y el teorema de la definición por recursión. El primero provee de un método para verificar qué propiedades son satisfechas por todas las fórmulas del lenguaje, el segundo asegura que una misma fórmula no sea interpretada de distintas maneras, y el tercero permite extender funciones definidas en los átomos del lenguaje a funciones en todo el lenguaje. Posteriormente se dio una semántica a dicho lenguaje por medio de valuaciones proposicionales y se probó el principio de extensionalidad para las proposiciones, el cual dice que el valor de verdad de una proposición depende del de sus subfórmulas atómicas. Para culminar la sección, se describió un sistema formal para la lógica proposicional, se describieron esquemas de teoremas para dicho sistema y se probó que éste era robusto y completo respecto a la semántica de valuaciones proposicionales.

Por otra parte, en la sección de Lógica Predicativa del mismo capítulo, se efectuó un proceso análogo al de su contraparte proposicional con algunas diferencias considerables. Inicialmente se describieron los constituyentes de la semántica (para la lógica predicativa): las estructuras (matemáticas), y también se presentaron sus correspondientes entes simbólicos: las signaturas. Posteriormente se introdujo la sintaxis de los lenguajes predicativos para los cuales se enunciaron sus respectivos teoremas de buen comportamiento, es decir, su principio de inducción, teorema de legibilidad única y teorema de definición por recursión. Además se aprovechó el capítulo para contrastar, justificar y/o advertir sobre las distintas notaciones y concepciones dadas a las estructuras, signaturas y lenguajes formales predicativos en diversos libros de texto. Más aún, se hicieron explícitos hechos poco o nada resaltados en otras referencias como que al definir el conjunto de variables libres de una fórmula ($FV(\varphi)$), la aseveración que da más información (o al menos la que es más utilizada) no es “la variable pertenece al conjunto” ($x \in FV(\varphi)$), sino la afirmación “la variable no pertenece al conjunto” ($x \notin FV(\varphi)$). Con todos estos entes presentados se hizo explícita la semántica formal de la lógica predicativa y se probaron propiedades relacionando a ésta y los lenguajes predicativos. Particularmente se prestó especial atención a la definición de dos tipos de sustitución en las fórmulas de dichos lenguajes. Finalmente, se presentó un sistema formal para la lógica predicativa y se demostró el teorema de completez de Gödel.

Ya con el manejo simbólico de la lógica bien fundamentado, en el capítulo 3 se procedió a desarrollar sobre ésta la teoría de conjuntos axiomática. Como introducción al tema se presentó dicha teoría en su versión informal y se analizaron las paradojas que ésta generaba. Esto se utilizó para motivar el desarrollo axiomático previamente referido. Por ende, la presentación cambió a un esquema de análisis en el cual, por cada axioma presentado, se estudiaban las consecuencias que éste tenía dentro de la teoría. A la par se dieron definiciones formales de distintos conceptos matemáticos dentro del sistema formal y se guió al lector para que apreciara el argumento heurístico que versaba la formalización de las matemáticas en una lógica de primer orden con los axiomas de Zermelo-Fraenkel-Choice (FOL+ZFC). Además se aprovechó el trabajo de tesis para proveer de contexto histórico a los axiomas y conceptos desarrollados a lo largo del capítulo 3.

En el cuarto y último capítulo se dio una introducción histórica de la teoría de tipos homotopía, en particular se menciona uno de los objetivos prácticos por los cuáles surgió: la verificación automática de argumentos matemáticos. Posteriormente se enunciaron algunas nociones filosóficas bajo las cuales surgió la teoría de tipos constructiva y se dio una primera explicación de los tipos existentes y las construcciones permisibles dentro de la teoría. Además se hizo explícita la correspondencia Curry-Howard entre lógica intuicionista y la teoría de tipos de Martin-Löf lo cual sirvió como motivación para presentar los tipos igualdad proposicional. Finalmente se presentó un sistema formal que englobara a la teoría de tipos homotopía (HoTT) y se presentaron dos de las reglas de inferencia características de la misma: el axioma de extensionalidad de funciones y el axioma de univalencia.

Bibliografía

[ACD] Andreas Abel, Thierry Coquand, and Peter Dybjer. Normalization by evaluation for martin-löf type theory with typed equality judgements. Göteborg.

[ACP] Andreas Abel, Thierry Coquand, and Miguel Pagano. A modular type-checking algorithm for type theory with singleton types and proof irrelevance. Göteborg.

[All16] Mauro Allegranza. Mathstackexchange: Why do we call “comprehension” and “regularity” to the axiom schemas in set theory?, Febrero 2016.

[Awo14] Steve Awodey. Homotopy type theory and the univalent foundations for mathematics, December 2014.

[B$^+$] Bencerek et al. Mizar home page.

[BG] Andreas Blass and Yuri Gurevich. Why sets? *Bulletin of the European Association for Theoretical Computer Science*, (84):20, October.

[CG] Carlos Caleiro and Ricardo Gonçalves. On the algebraization of many-sorted logics*.

[Cu14] Andres Caicedo and user92805. Mathstackexchange: Definition by recursion, 2014.

[End01] Herbert B. Enderton. *A Mathematical Introduction to Logic*. Harcourt/Academic Press, California, Los Angeles, 2 edition, 2001.

[Ham11] Joel David Hamkins. The set-theoretic multiverse. *arXiv*, 1:35, Aug 2011.

[HJ99] Karel Hrbacek and Thomas Jech. *Introduction to Set Theory*. 3. Marcel Dekker Inc., 3 edition, 1999.

[Hun71] Geoffrey Hunter. *Metalogic, An Introduction to the Metatheory of Standar First Order Logic*. University of California Press, United States, 1971.

[IC11] Carlos Ivorra Castillo. Lógica y teoría de conjuntos, 2011.

[IC15] Carlos Ivorra Castillo. *Lógica Matemática*. 2 edition, 2015.

[JLRR00] Tao Jang, Ming Li, Bala Ravikumar, and Kenneth W. Regan. Formal grammars and languages, 2000.

[Kan12] Akihiro Kanamori. In praise of replacement. *The Bulletin of Symbolic Logic*, 18(1):90, March 2012.

[Kun80] Kenneth Kunen. *Set Theory, An Introduction to Independence Proofs*. Elsevier Science, The Netherlands, 1 edition, 1980.

[Kun09] Kenneth Kunen. *The Foundations of Mathematics*. College Publications, 2009.

[LP14] James Ladyman and Stuart Presnell. A primer on homotopy type theory part i: The formal type theory, November 2014.

[Men97] Elliott Mendelson. *Introduction to Mathematical Logic*. Chapman and Hall, 4 edition, 1997.

[ML84] Per Erick Rutger Martin-Löf. *Intuitionistic Type Theory: Notes by Giovanni Sambin of a series of lectures given in Padua, June 1980*. Bibliopolis, Napoli, 1 edition, 1984.

[Pro13] The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. Institute for Advanced Study, 2013.

[Rij12] Egbert Rijke. Homotopy type theory. Master's thesis, Utrecht University, Ljubljana, Slovenia, July 2012.

[Shu13] Michael A. Shulman. The n-category café: From set theory to type theory, January 2013.

[SKSC08] Alexander S. Kechris, Michael A. Shulman, and Andrés E. Caicedo. Ma/cs 6c notes, 2008.

[Som00] Giovanni Sommaruga. *History and Philosophy of Constructive Type Theory*. Springer Science+Business Media, Dordrecht, 1 edition, 2000.

[STB] Urs Schreiber, Todd Trimble, and Toby Bartels. nlab: signature (in logic).

[VD04] Dirk Van Dalen. *Logic and Structure*. Springer, United States, 5 edition, 2004.

[Voe14] Vladimir Voevodsky. The origins and motivations of univalent foundations. *The Institute Letter*, Summer 2014:7–9, 2014.

[Zar06] Calogero G. Zarba. Lecture notes on decision procedures, 2006.

Índice alfabético

β-conversión, 110
η-conversión, 110
∞-grupoide, 133
índices, 94
árbol de análisis gramático, 21
átomos, 14
Łukasiewicz, 30

alcance del conectivo, 22
alfabeto, 2
antisimétrica, 90
aparato deductivo, 4
argumentos rigurosos, 86
aridad, 14
asignación de variables, 52
asimétrica, 90
asistentes de prueba, 106
Automath, 107
axioma de elección, 103
axioma de extensionalidad, 79
axioma de extensionalidad de funciones, 131
axioma de la unión, 87
axioma de regularidad, 102
axioma de univalencia, 131
axioma del infinito, 99
axioma del par, 87
axioma del potencia, 93
axiomas, 4
axiomas de Peano, 97
axiomas lógicos, 79
axiomas no-lógicos, 79

bien tipificado, 127
bucle, 133

cálculo lambda, 106
cálculo lambda no tipificado, 106
cálculo lambda simplemente tipificado, 106
cadena, 2
cadena vacía, 3
caminos, 132
cardinalidad, 78
clase, 87
clausura universal, 56
codificar, 88
colección, 76
complemento, 78
completez, 10
completez fuerte, 10
completez semántica, 10
completez sintáctica, 10
conceptos primitivos, 80
conectivo principal, 22
conectivos, 14
conjunto bien fundado, 95
conjunto inductivo, 99
conjunto potencia, 78
conjunto transitivo, 95
conjunto universal, 78
conjunto vacío, 78
consecuencia lógica, 25
consecuencia semántica, 9
consecuencia sintáctica, 6
consistencia, 10
consistencia semántica, 10
consistencia sintáctica, 10
constantes, 40
contexto, 108
correspondencia

Curry-Howard-Lambek, 106
cuantificadores, 43

decidibilidad, 11
definición de un símbolo en un lenguaje, 84
diferencia de conjuntos, 77
dominio de discurso, 40
dominio de una relación, 89

equipotencia, 98
esquema de axioma, 82
esquema de axioma de especificación, 82
esquema de axioma de reemplazo, 100
estructura, 40
estructura para un lenguaje predicativo, 51
expresión, 2
extensión, 76
extensión por definiciones, 84
extensionalidad, 76

fórmula, 2
fórmulas bien formadas, 3
forcing, 104
función, 90
funcionales, 39

gramática, 3
grupoide, 132

identidad de los indescirnibles, 124
igualdad definicional, 109
igualdad proposicional, 123
imagen directa de un conjunto bajo una relación, 90
imagen inversa de un conjunto bajo una relación, 90
inclusión canónica, 112
indisceernibilidad de los idénticos, 124
inducción sobre la complejidad de la fórmula, 15
instancia, 2
interpretación, 40
intersección, 77

juicio, 107

lógica, 1
lógica de segundo orden, 79
lógica matemática, 1
lógica predicativa, 39
lógica proposicional, 13
lógica simbólica, 1
lógicamente válida, 9
lambda-expresión, 110
lazo, 133
legibilidad única, 20
lenguaje formal, 3
lenguaje proposicional, 14
lenguaje universal, 2
letras proposicionales, 14
longitud de una fórmula, 2

metalenguaje, 2
metasímbolo, 2
Mizar, 107
modelo, 55
modus ponens, 28
modus tollens, 28
multiverso, 104

número natural, 97

orden estricto, 90
orden lineal, 90
orden parcial, 90
ordianl, 95

palabra, 2
parejas ordenadas, 88
parte bien formada, 22
Particularización, 66
predicativos, 39
primera teoría de Zermelo, 100
principio de comprensión, 76
principio de comprensión restringida, 82
principio de inducción de caminos, 133
principios de unicidad, 128

producto cartesiano, 77
producto cartesiano generalizado, 94
programa de Fundamentos Univalentes, 107
proposiciones, 13
proyección canónica, 111
prueba formal, 5

rango de una proposición, 21
rango de una relación, 90
recursión, 20
reflexiva, 90
reglas de computación, 128
reglas de eliminación, 128
reglas de formación, 128
reglas de inferencia, 4
reglas de introducción, 128
relación binaria, 89
relación de equivalencia, 90
relación linear, 90
relación total, 90
relación tricotómica, 95
restricción de una relación a un conjunto, 90
robustez, 10
robustez fuerte, 10

satisfactibilidad, 9
segmento inicial, 16
segmento inicial propio, 16
semántica, 9
sentencia, 49
signatura, 39
simétrica, 90
sistema formal, 5
sistema lógico, 1
soporte, 24
sorts, 40
subfórmula, 22
sucesión, 94
sucesión formativa, 17
sustitución de una fórmula por otra, 62
sustitución de una proposición por otra, 21
sustitución de una variable por un término en fórmulas, 59
sustitución de una variable por un término en términos, 58

término, 44
término sustituible por una variable en una fórmula, 59
tautología, 25
teoría, 4
Teoría de Conjuntos, 75
teoría de homotopías, 107
teoría de tipos, 105
teoría de tipos de Martin-Löf, 106
teoría de tipos-homotopías, 106
teoría extensional, 109
teoría Henkin, 72
teoría intensional, 109
teoría matemática, 6
teoría restringida de Zermelo, 89
teorema, 6
testigo de veracidad, 113
tipo coproducto, 112
tipo de funciones dependientes, 110
tipo de parejas dependientes, 111
tipo unidad, 113
tipo vacío, 113
topología, 132
transitiva, 90
tuplas, 77

unión, 77
unicidad, 83

valuación atómica, 23
valuación predicativa, 52
valuación proposicional, 23
variable acotada, 49
variable libre, 49
variables, 43
verdad en una estructura, 55

wffs, 3