Universidad de Sevilla

Facultad de Matemáticas

La lógica de la demostrabilidad

Autor:
Samuel Ortiz Morales

Tutor:
Francisco Félix Lara Martín

Trabajo Fin de Grado

Grado en Matemáticas

Departamento de Ciencias de la Computación e Inteligencia Artificial

Sevilla, 2021

Abstract

Our main goal in this work is the study of the arithmetical completeness theorem for **GL** (presented for first time by Solovay in [Sol76]), based on the book The logic of provability by G. Boolos. To reach our goal, we will introduce the formal language of arithmetic toghether with the Peano Arithmetic system, in order to study the provability formula $Prov(x)$ along with Löb's derivability conditions. Moreover we will do a brief study on modal logic, focusing on the main system used in provability logic, **GL** (for Gödel-Löb) with the purpose of linking **GL** and Peano Arithmetic. This relationship between these two systems will be achieved by interpreting the box $\Box$ as $Prov$, and then we will be able to prove the arithmetical completeness theorem for **GL**. In the last chapter, the fixed point theorem for **GL** will be presented along with a proper algorithm for calculating them.

Resumen

Nuestro objetivo en esta memoria es el estudio del teorema de completitud aritmética para **GL** demostrado por primera vez por Solovay en [Sol76], basándonos en el libro *The logic of provability* de G. Boolos. Para alcanzar dicho objetivo, introduciremos el lenguaje de la aritmética y haremos un estudio sobre el sistema de la Aritmética de Peano, usando funciones recursivas y codificación de la sintaxis de la aritmética para definir el predicado Prov junto a las condiciones de derivabilidad de Löb. A continuación haremos un breve estudio de lógica modal, centrándonos en el sistema por excelencia de la lógica de la demostrabilidad, **GL** (por Gödel-Löb), con el propósito de crear una relación entre la Aritmética de Peano y **GL**. Esta correspondencia la conseguiremos interpretando la caja $\Box$ como el predicado $Prov$, y de esta forma poder demostrar el teorema objetivo. Para concluir, demostraremos el teorema de punto fijo para **GL**, unos de los resultados modales más importantes, junto con un algoritmo para calcularlos.

Índice

Introducción

La lógica modal estudia los razonamientos que involucran la introducción de las expresiones "es necesario que" y "es posible que", simbolizadas por los operadores $\Box$ y $\Diamond$ respectivamente. Aunque el término va más allá pues sería incorrecto hablar de una sola lógica modal ya que podemos encontrar una familia de lógicas, en las que se encuentran entre otras, la lógica deóntica, donde $\Box$ cambia por O y se lee "es obligatorio que" y $\Diamond$ cambia por P y se lee "se permite que", o la lógica temporal, donde tenemos los operadores G "siempre será el caso de que" y H "siempre fue el caso de que". Es por esto que en ocasiones se acuña el término de Lógicas Modales.

Nosotros nos restringiremos al uso de lógica modal para hablar de aquella que añaden los operadores $\Box$ y $\Diamond$ a la lógica proposicional. Dentro de la lógica modal, a su vez, podemos encontrar distintos sistemas modales con distintos axiomas y reglas de inferencia. Uno de los sistemas modales más débiles y que se suele usar habitualmente como sistema base es el llamado **K** por Saul Kripke. Los símbolos de **K** son $\bot, \to$ de la lógica proposicional, y el operador modal $\Box$ que leeremos como "es necesario que". El operador "es posible que" se define a partir de $\Box$ de la siguiente forma $\Diamond = \neg\Box\neg$.
K va a heredar todos los axiomas lógicos de la lógica proposicional, pero además se le añaden todas las instancias del axioma de distribución y la regla de inferencia, a la que llamaremos necesidad:

- Axioma de distribución: $\Box(A \to B) \to (\Box A \to \Box B)$
- Necesidad: Si se tiene $\mathbf{K} \vdash A$, inferimos $\mathbf{K} \vdash \Box A$.

La regla de necesidad nos describe que todo teorema de **K** es necesario. Es fácil observar, y lo veremos con más detalle en el capítulo 2, que **K** es un sistema demasiado débil para hablar de necesidad en profundidad, tal es el caso que **K** no puede por ejemplo demostrar

$$\Box A \to A$$

que nos dice que, cualquier cosa que es necesaria, ocurre. Debido a esta debilidad, los lógicos empezaron a creas distintos sistemas con distintos axiomas donde destacan $\mathbf{K4}, \mathbf{T}, \mathbf{B}, \mathbf{S4}$ entre otros, y que estudiaremos a lo largo de este trabajo.

Este desarrollo en los comienzos de la lógica modal a principios del siglo XX (ver [Bal21])se lleva a cabo en su mayoría por filósofos, donde se destaca la labor pionera del filósofo americano C.I. Lewis en [Lew12]. Lewis muestra su preocupación con dos teoremas encontrados en el Principia Mathematica de Russell y Whitehead:

$$\neg p \to (p \to q) \tag{1}$$

$$p \to (q \to p) \tag{2}$$

(1) significa que una proposición falsa *implica* cualquier proposición y (2) que una proposición verdadera está *implicada* por cualquier otra proposición. Lewis no tiene un problema con estos teoremas, sino con el significado que toma *implicar*. El filósofo americano apuesta por una *implicación* $\to$ que cumpla lo siguiente: una proposición *implica* otra si la segunda proposición puede ser deducida lógicamente de la primera. Con esta interpretación, (1) y (2) no deberían ser teoremas, por lo que la lógica proposicional no sería correcta en relación con el significado de $\to$ como operador lógico. Esto conllevó a consideraciones similares en otros operadores lógicos como $\vee$, aunque dichas consideraciones no eran nuevas en la época de Lewis, ya en 1880, Hugh MacColl en [Mac80] hace esta distinción entre la lectura extensional o intencional de operadores lógicos, en particular presenta como $(p \to q)$ y $(\neg p \vee q)$ no son equivalentes. MacColl argumenta que $(\neg p \vee q)$ se sigue de $(p \to p)$ pero no viceversa.

Todas estas consideraciones filosóficas son las que incitan el estudio de la lógica modal moderna, y a la creación de los sistemas de Lewis a partir de 1918, donde destacamos **S4** que trataremos en el capítulo 2. Con este nuevo campo de estudio floreciendo, muchos matemáticos veían a esta rama de la lógica con cierta distancia, como podemos observar en la reseña de Rusell al libro *Symbolic Logic and its Aplication* de MacCollin, ver [Mar16], donde Russell se muestra crítico ante este punto de vista sobre los operadores lógicos.

Gödel fue primordial en la entrada de matemáticos a esta rama de la lógica con su artículo "An Interpretation of the Intuitionistic Propositional Calculus" y su primera aproximación a axiomatizar **S4** separando la base de la lógica proposicional del sistema de los axiomas modales y las reglas de inferencia propias. Esto trajo a muchos matemáticos al estudio de la lógica modal donde hoy en día tiene un papel importante tanto en matemáticas como en ciencias de la computación.

En el capítulo 2 presentaremos resultados para distintos sistemas de la lógica modal pero nuestra prioridad se tornará a las lógicas de la demostrabilidad, usadas en el estudio sobre lo que las teorías aritméticas pueden expresar sobre sus predicados de demostrabilidad. En esta memoria la teoría aritmética que vamos a tratar es la Aritmética de Peano **PA**. En las lógicas de la demostrabilidad, $\Box$ significará "es demostrable que" en la aritmética, es decir, $\Box p$ significará que aquello que denote p será demostrable, en nuestro caso, en **PA**. Usando este convenio, las fórmulas de estas lógicas podrán expresar verdades sobre la demostrabilidad, por ejemplo:

$$\neg\Box\bot$$

dice que **PA** es consistente,

$$\Box A \to A$$

afirma que **PA** es correcta, en el sentido de que si **PA** demuestra A entonces A es verdadera,

$$\neg\Box\bot \to \neg\Box\neg\Box\bot$$

manifiesta que si **PA** es consistente entonces **PA** no puede demostrar su propia consistencia.

En este trabajo, nos centraremos en el estudio del sistema **GL** (nombrado así por por Gödel y M.H. Löb), basándonos en el libro *The logic of provability* de George Boolos y con el objetivo de demostrar el teorema de completitud aritmética presentado por primera vez por Robert M. Solovay en [Sol76].

GL es el sistema que resulta de **K** al añadirle el axioma **G**:

$$\Box(\Box A \to A) \to \Box A$$

Es importante destacar que en **GL** el operador $\Box$ que indica demostrabilidad, no lo podemos tratar como un tipo de necesidad, ya que **GL** $\nvdash \Box A \to A$, aunque no supone ningún problema ya que no buscamos estudiar necesidad en **GL**. El axioma **G** captura el Teorema de Löb, un resultado importante en aritmética que estudiaremos más adelante. Recordemos que $\Box A \to A$ afirma que si **PA** es capaz de demostrar A entonces A es verdadera, esto es **PA** es correcta para A, pero **G** encierra un importante significado, si **PA** pudiera probar la fórmula que afirma que **PA** es correcta para A entonces **PA** demuestra a A. El teorema de Löb remarca la modestia, en palabras de Boolos, de **PA**.

En esta memoria trataremos el siguiente contenido:

En el capítulo 1 estudiaremos la aritmética necesaria para el objetivo de este trabajo. Introduciremos el lenguaje de la aritmética junto a la teoría de la Aritmética de Peano. Presentaremos las clases de fórmulas Δ, Σ, Π y demostraremos un importante resultado sobre estas, la Σ Completitud de **PA**. A continuación indagaremos en una clase importante de funciones, las funciones recursivas, que serán una base fundamental en nuestro estudio de la aritmética. Para finalizar el capítulo, trataremos la aritmetización de la sintaxis, donde presentamos una codificación de sucesiones finitas partiendo de una enumeración de Gödel y el predicado de demostrabilidad $Prov(\ulcorner S \urcorner)$, el cual afirma que la fórmula cerrada con número de Gödel $\ulcorner S \urcorner$ es demostrable en **PA**. Concluimos con los teoremas de incompletitud para **PA**, el teorema de Löb

En el Capítulo 2 introduciremos el lenguaje de la lógica modal juntos a los distintos sistemas **K**, **K4**, **B**, **T**, **S4** y **GL** con sus respectivos teoremas de completitud, haciendo un estudio más profundo de **GL** como sistema principal a tratar en este trabajo.

En el capítulo 3 examinaremos la relación entre la lógica modal y la Aritmética de Peano mediante la interpretación de $\Box$ como la fórmula $Prov(x)$ de **PA**. Definiremos las realizaciones como funciones que toman fórmulas modales y las *traducen* a fórmulas cerradas de la aritmética. Además estudiaremos una implicación del teorema de la completitud aritmética para **GL** así como la introducción de un nuevo sistema modal, **GLS**.

En el capítulo 4 encontramos finalmente el resultado objetivo de esta memoria, el teorema de la completitud aritmética demostrado para **GL**, el sistema anteriormente introducido **GLS** y el teorema de completitud aritmética uniforme para **GL**.

Para finalizar, en el capítulo 5 presentamos un resultado modal central en la lógica de la demostrabilidad: el teorema del punto fijo. Aunque está formulado en términos modales, tiene un gran significado aritmético, declara que la auto referencia no es necesaria en el sentido expuesto a continuación:
Sea p una variable modal y $A(p)$ una fórmula modal donde p aparece en el rango de $\Box$. El teorema afirma que existe otra fórmula modal B donde p no ocurre, y cualquier otra variable modal que ocurre en B también lo hace en A cumpliendo:

$$\mathbf{GL} \vdash B \leftrightarrow A(B)$$

La fórmula B será el punto fijo de A. Tanto las condiciones para probar la existencia y unicidad de un punto fijo para una fórmula modal A, como un algoritmo para calcularlo serán el objeto de estudio de este capítulo.

Capítulo 1

La Aritmética de Peano

1.1 El lenguaje de la aritmética

Definición 1.1.1. Una sucesión finita de longitud k es un objeto s tal que para todo i con $0 \leq i \leq n$ existe un objeto s_i que es la entrada i-ésima de s.

Denotaremos a la sucesión s como $\langle s_0, ..., s_i, ..., s_{k-1} \rangle$.

Definición 1.1.2. Definimos la sucesión vacía como la única sucesión de longitud 0 que denotaremos $\langle \rangle$.

Sean s y t dos sucesiones finitas, denotaremos $s \equiv t$ para indicar que son la misma sucesión de símbolos, esto es, si $s = \langle s_0, ..., s_n \rangle$ y $t = \langle t_0, ..., t_k \rangle$ entonces $n = k$ y para todo i tal que $0 \leq i \leq n$ se tiene que $s_i = t_i$.

Definición 1.1.3. Sean $s = \langle s_0, ..., s_n \rangle$ y $t = \langle t_0, ..., t_k \rangle$ dos sucesiones. Definimos la concatenación de sucesiones como la sucesión $s * t = \langle s_0, ..., s_n, t_0, ..., t_k \rangle$.

Definición 1.1.4. El lenguaje de la aritmética que denotaremos por $\mathcal{L}_{\mathrm{A}}$, es un lenguaje de primer orden con igualdad cuyos símbolos no lógicos son $\mathbf{0}, \boldsymbol{'}, +, \times$ donde:

- $\mathbf{0}$ es una constante.
- $\boldsymbol{'}$ es una función de aridad 1.
- $+, \times$ son funciones binarias.

Denotaremos al conjunto de variables de $\mathcal{L}_{\mathrm{A}}$ por:

$$\mathrm{VAR}_{\mathcal{L}_{\mathrm{A}}} := \{x, y, z, ..., z_0, y_0, z_0, ...\}$$

Definición 1.1.5. El conjunto de términos de $\mathcal{L}_{\mathrm{A}}$, $\mathrm{TERM}_{\mathcal{L}_{\mathrm{A}}}$ se define recursivamente de la siguiente forma:

- $\mathbf{0} \in \mathrm{TERM}_{\mathcal{L}_{\mathrm{A}}}$
- Si $x \in \mathrm{VAR}_{\mathcal{L}_{\mathrm{A}}}$ entonces $x \in \mathrm{TERM}_{\mathcal{L}_{\mathrm{A}}}$

- Si $\boldsymbol{t} \in \mathrm{TERM}_{\mathcal{L}_\mathrm{A}}$ entonces $\boldsymbol{t'} \in \mathrm{TERM}_{\mathcal{L}_\mathrm{A}}$
- Si $\boldsymbol{t}$, $\boldsymbol{s} \in \mathrm{TERM}_{\mathcal{L}_\mathrm{A}}$ entonces $\boldsymbol{t}+\boldsymbol{s}, \boldsymbol{t}\times\boldsymbol{s} \in \mathrm{TERM}_{\mathcal{L}_\mathrm{A}}$.

Definición 1.1.6. El conjunto de fórmulas de $\mathcal{L}_\mathrm{A}$, $\mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ se define recursivamente de la siguiente forma:

- $\bot \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$
- Si $\boldsymbol{t}$, $\boldsymbol{s} \in \mathrm{TERM}_{\mathcal{L}_\mathrm{A}}$ entonces $(\boldsymbol{t} = \boldsymbol{s}) \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$
- $\varphi, \psi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ entonces $\varphi \to \psi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$
- $\varphi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$, $x \in \mathrm{VAR}_{\mathcal{L}_\mathrm{A}}$ entonces $\forall x\varphi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$.

Definición 1.1.7. Dados $s, t \in \mathrm{TERM}_{\mathcal{L}_\mathrm{A}}$ diremos que $\varphi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ es una fórmula atómica si φ es $\bot$ ó φ es $s = t$.

Definición 1.1.8. Para $\varphi, \psi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ haremos las siguientes abreviaturas:

- $\neg\varphi := \varphi \to \bot$
- $\varphi \vee \psi := \neg\varphi \to \psi$
- $\varphi \wedge \psi := \neg(\neg\varphi \vee \neg\psi)$
- $\varphi \leftrightarrow \psi := (\varphi \to \psi) \wedge (\psi \to \varphi)$
- $\exists x\varphi := \neg\forall x(\neg\varphi)$

Definición 1.1.9. El conjunto de fórmulas cerradas (sin variables libres) de $\mathcal{L}_\mathrm{A}$ se denotará por $\mathrm{SENT}_{\mathcal{L}_\mathrm{A}}$.

Es importante destacar que podremos ver los términos y las fórmulas de la aritmética como pares ordenados. Dados $s, t \in \mathrm{TERM}_{\mathcal{L}_\mathrm{A}}$ y $\varphi, \psi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ tendremos que $s + t$, $s \times t$, $s = t$ y s' serán respectivamente $\langle +, \langle s, t\rangle\rangle$, $\langle \times, \langle s, t\rangle\rangle$, $\langle =, \langle s, t\rangle\rangle$ y $\langle ', s\rangle$. A su vez, $\varphi \to \psi$ y $\forall x\varphi$ serán $\langle \to, \langle \varphi, \psi\rangle\rangle$ y $\langle \forall, \langle x, \varphi\rangle\rangle$.

1.2 La aritmética de Peano

Definición 1.2.1. Definimos el numeral $\boldsymbol{n}$ asociado al número natural n como el término de $\mathcal{L}_\mathrm{A}$ dado por:

- $\mathbf{0}$ si $n = 0$.
- $\boldsymbol{k'}$ si $n = k + 1$.

Definición 1.2.2. La teoría $\boldsymbol{\mathcal{Q}}$ de Robinson es la teoría de lenguaje $\mathcal{L}_{\mathrm{A}}$ con los siguientes axiomas:

($\mathcal{Q}_1$) $\forall x \forall y[x' = y' \rightarrow x = y]$

($\mathcal{Q}_2$) $\forall x[\mathbf{0} \neq x']$

($\mathcal{Q}_3$) $\forall x[(x + \mathbf{0}) = x]$

($\mathcal{Q}_4$) $\forall x \forall y[(x + y') = (x + y)']$

($\mathcal{Q}_5$) $\forall x[(x \times \mathbf{0}) = \mathbf{0}]$

($\mathcal{Q}_6$) $\forall x \forall y[(x \times y') = ((x \times y) + x)]$

Definición 1.2.3. Sea $\varphi(x, \vec{v})$ una fórmula. El axioma de inducción relativo a φ y a la variable x, es la fórmula:

$$\boldsymbol{I}_{\varphi,x}(\vec{v}) \equiv \varphi(\mathbf{0}, \vec{v}) \wedge \forall x(\varphi(x, \vec{v}) \rightarrow \varphi(x', \vec{v})) \rightarrow \forall x \varphi(x, \vec{v}).$$

Definición 1.2.4. La Aritmética de Peano **PA** es la teoría de lenguaje $\mathcal{L}_{\mathrm{A}}$ cuyos axiomas son:

$$\boldsymbol{\mathcal{Q}} \cup \{\boldsymbol{I}_{\varphi,x}(\vec{v}) : \varphi(x, \vec{v}) \in \mathrm{FORM}_{\mathcal{L}_{\mathrm{A}}}\}$$

Junto a estos axiomas, **PA** también tiene un conjunto de axiomas lógicos que no haremos explícitos, pero que, junto a las siguientes reglas de inferencia, permiten demostrar todas las fórmulas lógicamente válidas de la lógica de primer orden.

Definición 1.2.5. Las reglas de inferencia para **PA** serán las siguientes:

1. Modus Ponens, MP: $\dfrac{\varphi,\ \varphi \rightarrow \psi}{\psi}$

2. Generalización Universal, GU: $\dfrac{\varphi(v)}{\forall v \varphi(v)}$, con $v \in \mathrm{VAR}_{\mathcal{L}_{\mathrm{A}}}$.

Se dirá que ψ es consecuencia de φ y $(\varphi \rightarrow \psi)$ por MP y que $\forall x \varphi(x)$ es consecuencia de $\varphi(x)$ por GU.

Definición 1.2.6. Una demostración $\mathcal{D}$ en **PA** de $\varphi \in \mathrm{FORM}_{\mathcal{L}_{\mathrm{A}}}$ es una sucesión finita de fórmulas en $\mathcal{L}_A$, $s = \langle s_0, ..., s_n \rangle$, donde $s_n = \varphi$ y para todo $0 \leq i < n$ se cumple que s_i es un axioma lógico, un axioma o una consecuencia de una regla de inferencia, es decir, existen $j, k < i$ tales que s_i es consecuencia de s_j y s_k por MP; o bien, existe $j < i$ tal que s_i es consecuencia de s_j por GU.
Si existe una demostración $\mathcal{D}$ de $\varphi \in \mathrm{FORM}_{\mathcal{L}_{\mathrm{A}}}$ se dirá que φ es demostrable en **PA** o φ es un teorema de **PA** y lo denotaremos por $\mathbf{PA} \vdash \varphi$.

Definición 1.2.7. Introducimos las siguientes abreviaturas:

1) $x < y := \exists u(x + u' = y)$

2) $y > x := x < y$

3) $x \leq y := (x < y \vee x = y)$

4) $y \geq x := x \leq y$

5) $(\forall x < y)\varphi(x) := \forall x[x < y \rightarrow \varphi(x)]$

6) $\exists! y\varphi(\vec{x}, y) := \exists y\big[\varphi(\vec{x}, y) \wedge \forall u\,[\varphi(\vec{x}, u) \rightarrow u = y]\,\big]$

Definición 1.2.8. El modelo estándar de la aritmética es la $\mathcal{L}_{\mathrm{A}}$-estructura $\mathcal{N}$ que se define, para $n, m \in \mathbb{N}$, como:

- El universo de $\mathcal{N}$, $|\mathcal{N}| = \mathbb{N}$
- $\mathbf{0} = 0$
- $'(n) = n + 1$
- $+(n, m) = n + m$
- $\times(n, m) = n \cdot m$

Definición 1.2.9. La teoría de $\mathcal{N}$ se define como el conjunto de fórmulas cerradas $\varphi \in \mathrm{SENT}_{\mathcal{L}_{\mathrm{A}}}$ que son verdaderas en $\mathcal{N}$ y lo denotamos por

$$\mathbf{Th}(\mathcal{N}) = \{\varphi \in \mathrm{SENT}_{\mathcal{L}_{\mathrm{A}}} : \mathcal{N} \vDash \varphi\}$$

En el modelo estándar, cada término cerrado t de $\mathcal{L}_{\mathrm{A}}$ *denotará* a un único número natural de la siguiente forma:

- $\mathbf{0}$ denota a 0.
- Si s y t denotan a los números naturales i y j, entonces s', $s + t$ y $s \times t$ denotan a $i + 1$, $i + j$ y a $i \cdot j$ respectivamente.

1.3 Teoría de números en PA

En esta sección demostraremos varios resultados sobre teoría de números que podemos demostrar razonando en **PA**, introduciremos el concepto de p-término y las clases de fórmulas Δ, Σ, Π. Además demostraremos que **PA** es completa con respecto a Σ fórmulas, un importante resultado que necesitaremos en capítulos posteriores.

Lema 1.1. **PA** $\vdash \forall x[x + \mathbf{0'} = x']$

Demostración.

(1) $\quad$ **PA** $\vdash \forall x[x + \mathbf{0'} = (x + \mathbf{0})']$ $\qquad$ Axioma $\mathcal{Q}_4$

(2) $\quad$ **PA** $\vdash \forall x[x + \mathbf{0'} = x'].$ $\qquad$ Axioma $\mathcal{Q}_3$

■

Los siguientes tres lemas nos dicen que **PA** puede demostrar cosas que creemos fundamentales, como que si la suma de l y m es n entonces en **PA** se tendrá que cumplir que $\vdash \boldsymbol{l} + \boldsymbol{m} = \boldsymbol{n}$, o que si $k = j$ entonces en **PA** se deberá cumplir que $\boldsymbol{k} = \boldsymbol{j}$. Nuestro entendimiento más básico de la aritmética es demostrable en **PA**.

Lema 1.2.

1. *Sean* $n, l, m \in \mathbb{N}$, *si* $l + m = n$ *entonces* **PA** $\vdash \boldsymbol{l} + \boldsymbol{m} = \boldsymbol{n}$.

2. *Sean* $n, l, m \in \mathbb{N}$, *si* $l \cdot m = n$ *entonces* **PA** $\vdash \boldsymbol{l} \times \boldsymbol{m} = \boldsymbol{n}$.

Demostración.

1. Por inducción en j, si $i + j = k$ y $j = 0$ entonces $i = k$ y el numeral $\boldsymbol{j}$ es $\mathbf{0}$, así **PA** $\vdash \boldsymbol{i} + \boldsymbol{j} = \boldsymbol{i} + \mathbf{0} = \boldsymbol{i} = \boldsymbol{k}$, por el axioma $(\mathcal{Q}_3)$.
Supongamos que para todo k, si $i + j = k$ entonces **PA** $\vdash \boldsymbol{i} + \boldsymbol{j} = \boldsymbol{k}$.
En el caso $j + 1$, si $i + (j + 1) = k$ entonces existe un m con $i + j = m$ y $m + 1 = k$ esto implica que el numeral de k es $\boldsymbol{m'}$, así **PA** $\vdash \boldsymbol{i} + \boldsymbol{j} = \boldsymbol{m}$ y por el axioma $(\mathcal{Q}_4)$ **PA** $\vdash \boldsymbol{i} + \boldsymbol{j'} = \boldsymbol{m'} = \boldsymbol{k}$.

2. De nuevo por inducción en j: si $i \cdot j = k$ y $j = 0$ entonces el numeral $\boldsymbol{j}$ es $\mathbf{0}$ y así **PA** $\vdash \boldsymbol{i} \times \boldsymbol{j} = \boldsymbol{i} \times \mathbf{0} = \mathbf{0} = \boldsymbol{k}$, por el axioma $(\mathcal{Q}_5)$.
Supongamos que para todo k, si $i \cdot j = k$ entonces **PA** $\vdash \boldsymbol{i} \times \boldsymbol{j} = \boldsymbol{k}$.
En el caso $j + 1$, si $i \cdot (j + 1) = k$ entonces existe un m con $i \cdot j = m$ y $m + i = k$. Esto implica que el numeral de k es $\boldsymbol{m} + \boldsymbol{i}$, así **PA** $\vdash \boldsymbol{i} \times \boldsymbol{j} = \boldsymbol{m}$ y por el axioma $(\mathcal{Q}_6)$ **PA** $\vdash \boldsymbol{i} \times \boldsymbol{j'} = \boldsymbol{m} + \boldsymbol{i} = \boldsymbol{k}$.

■

Lema 1.3. *Sea* $t \in TERM_{\mathcal{L}_A}$ *un término cerrado que denota a* $n \in \mathbb{N}$, *entonces* **PA** $\vdash t = \boldsymbol{n}$.

Demostración.

Por inducción en t tenemos:
Si $t = \mathbf{0}$ entonces **PA** $\vdash t = \mathbf{0}$ pues **PA** $\vdash \mathbf{0} = \mathbf{0}$.
Si $t = r + s$ con $r, s \in \mathrm{TERM}_{\mathcal{L}_A}$ denotando a $i, j \in \mathbb{N}$ respectivamente, por hipótesis de inducción, **PA** $\vdash r = \boldsymbol{i}$ y **PA** $\vdash s = \boldsymbol{j}$ y además existe un $k \in \mathbb{N}$ con $k = i + j$,

por la proposición anterior tenemos que $\mathbf{PA} \vdash t = \boldsymbol{i} + \boldsymbol{j}$.
De la misma forma se demuestra para $t = r \times s$ y para $t = r'$.

$\blacksquare$

Lema 1.4. *Sean* $s, t \in TERM_{\mathcal{L}_A}$ *los términos cerrados que denotan a* $m, n \in \mathbb{N}$ *respectivamente, entonces* $m = n$ *implica* $\mathbf{PA} \vdash s = t$.

Demostración.

Tenemos por la proposición anterior que $\mathbf{PA} \vdash s = \boldsymbol{m}$ y $\mathbf{PA} \vdash t = \boldsymbol{n}$, y debido a que $m = n$ entonces m y n tienen que tener el mismo numeral, esto es $\boldsymbol{m} = \boldsymbol{n}$, luego $\mathbf{PA} \vdash s = t$.

$\blacksquare$

Lema 1.5. $\mathbf{PA} \vdash \forall x[x = \mathbf{0} \vee \exists y(x = y')]$

Demostración.

Sea $\varphi(x) \equiv x = \mathbf{0} \vee \exists y(x = y')$. Lo demostraremos por inducción, es decir, razonando en **PA** demostraremos $\varphi(\mathbf{0})$ y $\forall x[\varphi(x) \to \varphi(x')]$.

(1)	$\mathbf{0} = \mathbf{0}$	Lógicamente válida
(2)	$(\mathbf{0} = \mathbf{0}) \to \varphi(\mathbf{0})$	Lógicamente válida
(3)	$\varphi(\mathbf{0})$.	Caso base
(4)	$x' = x'$	Lógicamente válida
(5)	$(x' = x') \to \exists y[x' = y']$,	Lógicamente válida
(6)	$\exists y[x' = y']$	Modus ponens; (4), (5)
(7)	$x' = \mathbf{0} \vee \exists y[x' = y']$	Consecuencia lógica; (6)
(8)	$\varphi(x) \to \varphi(x')$	Consecuencia lógica; (7)
(9)	$\forall x[\varphi(x) \to \varphi(x')]$	Generalización universal
(10)	$\varphi(\mathbf{0}) \wedge \forall x[\varphi(x) \to \varphi(x')]$	Consecuencia lógica; (3), (9)
(11)	$\forall x\big[x = \mathbf{0} \vee \exists y[x = y']\big]$	Inducción; (10)

$\blacksquare$

Lema 1.6. $\mathbf{PA} \vdash \forall x[\neg(x < \mathbf{0})]$

Demostración.

Sabemos que $x < 0$ equivale a $\exists u[x + u' = \mathbf{0}]$

(1)	$\mathbf{PA} \vdash \forall x \forall u[x + u' = (x + u)']$	Axioma ($\mathcal{Q}_4$)
(2)	$\mathbf{PA} \vdash \forall x \forall u[(x + u)' \neq \mathbf{0}]$	Axioma ($\mathcal{Q}_2$)
(3)	$\mathbf{PA} \vdash \forall x \forall u[x + u' \neq \mathbf{0}]$	Consecuencia lógica; (1), (2)
(4)	$\mathbf{PA} \vdash \forall x[\neg(\exists u(x + u' = \mathbf{0}))]$	Definición de $\exists$; (3)
(5)	$\mathbf{PA} \vdash \forall x[\neg(x < \mathbf{0})]$	

■

Lema 1.7. $\mathbf{PA} \vdash \forall x \forall y[x < y' \leftrightarrow (x = y \vee x < y)]$

Demostración.

Razonando en **PA** tenemos que $x < y'$ si y sólo si $\exists u[x + \boldsymbol{u'} = y']$ si y sólo si $\exists u[(x + \boldsymbol{u})' = y']$ si y sólo si $\exists u[x + \boldsymbol{u} = y]$ si y sólo si $x + \mathbf{0} = y \vee \exists z[x + z' = y]$ por el Lema 1.5 si y sólo si $x = y \vee x < y$. Por generalización universal se tiene el resultado.

■

Lema 1.8. $\mathbf{PA} \vdash \forall x[x < \boldsymbol{n} \leftrightarrow \bigvee_{i<n} x = \boldsymbol{i}]$

Demostración.

Por inducción en n, asumamos que $n = 0$, entonces $\bigvee_{i<0} x = \boldsymbol{i} \equiv \perp$ y como $\mathbf{PA} \vdash \neg x < \mathbf{0}$ se tiene $\mathbf{PA} \vdash x < \mathbf{0} \leftrightarrow \bigvee_{i<0} x = \boldsymbol{i}$. Supongamos que para $n \in \mathbb{N}$ se tenga $\mathbf{PA} \vdash x < \boldsymbol{n} \leftrightarrow \bigvee_{i<n} x = \boldsymbol{i}$.
Por el Lema 1.7, $\mathbf{PA} \vdash x < \boldsymbol{n'} \leftrightarrow (x = \boldsymbol{n} \vee x < \boldsymbol{n})$ y, por hipótesis de inducción obtenemos $\mathbf{PA} \vdash x < \boldsymbol{n}' \leftrightarrow (x = \boldsymbol{n} \vee \bigvee_{i<n} x = \boldsymbol{i})$, luego

$$\mathbf{PA} \vdash x < \boldsymbol{n}' \leftrightarrow \bigvee_{i<n+1} x = \boldsymbol{i}$$

■

Podemos demostrar usando inducción que la suma y el producto son conmutativos.

Teorema 1.9.

1. $\mathbf{PA} \vdash \forall x[\mathbf{0} + x = x]$
2. $\mathbf{PA} \vdash \forall x[\mathbf{0}' + x = (\mathbf{0} + x)']$
3. $\mathbf{PA} \vdash \forall x \forall y \forall z[x(y + z) = (x + y)z]$
4. $\mathbf{PA} \vdash \forall x \forall y[x' + y = (x + y)']$
5. $\mathbf{PA} \vdash \forall x \forall y[x + y = y + x]$

1.3.1 Σ_1-Completitud de PA

Notación. Denotaremos por:

- $\vec{x}$ a $\langle x_0, \ldots, x_n \rangle$.
- $\forall \vec{x}$ a $\forall x_0 \cdots \forall x_n$.
- $\exists \vec{x}$ a $\exists x_0 \cdots \exists x_n$.

Definición 1.3.1. Sea $\varphi(\vec{x}, y) \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$, diremos que $\varphi(\vec{x}, y)$ es un p-término si $\mathbf{PA} \vdash \forall \vec{x}\, \exists! y \varphi(\vec{x}, y)$.

La motivación del uso de p-términos viene por lo débil que puede parecer **PA**, debido a que sus únicos símbolos no lógicos son la constante $\mathbf{0}$, y las funciones $+$, $\times$ y $'$ puede parecer que **PA** solo puede hablar de una clase muy restringida de funciones, por ejemplo, no podría hablar ni de la función exponencial, ya que mayora a todo polinomio que se pueda construir a base de términos de **PA**. Veremos en las próximas secciones que **PA** va a poder hablar de la exponencial y de otras muchas funciones que a priori, no creamos que se puedan expresar en términos de la aritmética que hemos estado viendo en este capítulo.

Cabe destacar que un p-término $F(\vec{x}, y) \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ define una función f de aridad n de $\mathbb{N}^{n+1}$ en $\mathbb{N}$ ya que $\mathbf{PA} \vdash \forall \vec{x}\, \exists! y F(\vec{x}, y)$. Debido a esta unicidad, podremos referirnos a $F(\vec{x}, y)$ sin mencionar a la variable y. Vamos a denotar a $F(\vec{x}, y)$ por $f(\vec{x}) = y$ y utilizaremos a $f(\vec{x})$ como un término de $\mathcal{L}_\mathrm{A}$.
Además, dada $A(y) \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ escribiremos $A(f(\vec{x}))$ para referirnos a la fórmula $\exists y[F(\vec{x}, y) \wedge A(y)]$. Debido a que $\mathbf{PA} \vdash \forall \vec{x} \exists! y F(\vec{x}, y)$ entonces $\exists y[F(\vec{x}, y) \wedge A(y)]$ es equivalente a $\forall y[F(\vec{x}, y) \to A(y)]$.

Definición 1.3.2 (Cuantificación acotada)**.** Sean x una variable, t un término que no ocurre en x, y $\varphi(x)$ una fórmula. Definimos:

- $(\exists x \leq t)[\varphi(x)] := \exists x[x \leq t \wedge \varphi(x)]$
- $(\forall x \leq t)[\varphi(x)] := \forall x[x \leq t \to \varphi(x)]$.

A continuación vamos a definir tres clases importantes de fórmulas, las fórmulas Δ_0, Σ, Π.

Definición 1.3.3 (Fórmulas Δ_0)**.**

- Si $x, y \in \mathrm{TERM}_{\mathcal{L}_A}$ entonces $x = y$, $x \leq y$ son fórmulas Δ_0.
- Si $\varphi, \psi \in \mathrm{FORM}_{\mathcal{L}_A}$ entonces $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \rightarrow \psi$, $\varphi \leftrightarrow \psi$ son fórmulas Δ_0.
- Si $\varphi \in \mathrm{FORM}_{\mathcal{L}_A}$ es Δ_0 entonces $(\forall x \leq y)\varphi$, $(\exists x \leq y)\varphi$ son fórmulas Δ_0, donde x es libre en φ y y es un numeral o una variable distinta de x.

Definición 1.3.4 (Fórmulas Σ)**.**

- Toda fórmula Δ_0 es una Σ fórmula.
- Si $\varphi, \psi \in \mathrm{FORM}_{\mathcal{L}_A}$ son Σ, entonces $\varphi \wedge \psi$ y $\varphi \vee \psi$ son Σ.
- Si $\varphi \in \mathrm{FORM}_{\mathcal{L}_A}$ es Σ entonces $(\forall x \leq y)\varphi$, $(\exists x \leq y)\varphi$ son fórmulas Σ, donde x es libre en φ e y es un numeral o una variable distinta de x.
- Si φ es Σ entonces $(\exists x)\varphi$ es una Σ fórmula.

Definición 1.3.5 (Fórmulas Π)**.**

- Toda fórmula Δ_0 es una Π fórmula.
- Si $\varphi, \psi \in \mathrm{FORM}_{\mathcal{L}_A}$ son Π, entonces $\varphi \wedge \psi$ y $\varphi \vee \psi$ son Π.
- Si $\varphi \in \mathrm{FORM}_{\mathcal{L}_A}$ es Π entonces $(\forall x \leq y)\varphi$, $(\exists x \leq y)\varphi$ son fórmulas Π, donde x es libre en φ e y es un numeral o una variable distinta de x.
- Si φ es Π entonces $(\forall x)\varphi$ es una Π fórmula.

Definición 1.3.6 (Fórmulas Δ)**.** Sea $\varphi \in \mathrm{FORM}_{\mathcal{L}_A}$ diremos que φ es una Δ fórmula si ambas φ y $\neg\varphi$ son Σ fórmulas

Proposición 1.10. *Si $\varphi(\vec{x}, y) \in FORM_{\mathcal{L}_A}$ es un p-término y además $\varphi(\vec{x}, y) \in \Sigma$ se tiene que $\varphi(\vec{x}, y) \in \Delta$.*

Demostración.

Como φ es un p-término, $\mathbf{PA} \vdash \exists! y \varphi(\vec{x}, y)$, luego

$$\neg\varphi(\vec{x}, y) \equiv \exists u[\neg u = y \wedge \varphi(\vec{x}, u)] \in \Sigma$$

por lo tanto, $\varphi(\vec{x}, y) \in \Delta$.

■

Proposición 1.11. *Si* $F(\vec{x}, y) \in \Sigma$ *es un p-término y* $A(y) \in \Delta$*, entonces* $\exists y[F(\vec{x}, y) \wedge A(y)] \in \Delta$.

Demostración.

Debido a que $F(\vec{x}, y)$ y $A(y)$ son fórmulas Σ tenemos que $\exists y[F(\vec{x}, y) \wedge A(y)]$ es una fórmula Σ y como $F(\vec{x}, y)$ es un p-término, como vimos al principio de la sección, $\exists y[F(\vec{x}, y) \wedge A(y)]$ es equivalente a $\forall y[F(\vec{x}, y) \rightarrow A(y)]$ y así tenemos que $\neg\forall y[F(\vec{x}, y) \rightarrow A(y)]$ es equivalente a $\exists y[F(\vec{x}, y) \wedge \neg A(y)]$ que es una fórmula Σ.

■

En resumidas cuentas, Δ contiene a todas las fórmulas atómicas y del tipo $t < s$ para t, s términos; y es cerrada bajo conectores lógicos, cuantificación acotada y sustitución de Σ p-términos.

Teorema 1.12 (Σ-Completitud de **PA**)**.** $\varphi \in SENT_{\mathcal{L}_A}$ *es una fórmula* Σ *verdadera, es decir,* $\mathcal{N} \vDash \varphi$ *si y sólo si* $\mathbf{PA} \vdash \varphi$.

Demostración.

($\Leftarrow$) Todos los axiomas de **PA** son verdaderos en el modelo estándar, por lo tanto cualquier teorema de **PA** derivado de estos axiomas es verdadero también.

($\Rightarrow$) Haremos la demostración por inducción en el grado de conectivas. Sean $\psi_1, \psi_2 \in \Sigma$ fórmulas cerradas:
Caso base, si φ es de la forma $t = s$ una Δ_0 fórmula, con t y s dos términos y $\mathcal{N} \vDash \varphi$ entonces, por el Lema 1.4, $\mathbf{PA} \vdash \varphi$.
Si φ es de la forma $\psi_1 \wedge \psi_2$ con ψ_1 y ψ_2 cumpliendo el teorema, $\mathcal{N} \vDash \psi_1 \wedge \psi_2$ implica $\mathcal{N} \vDash \psi_1$ y $\mathcal{N} \vDash \psi_2$, luego, por hipótesis de inducción, $\mathbf{PA} \vdash \psi_1$ y $\mathbf{PA} \vdash \psi_2$, lo que conlleva $\mathbf{PA} \vdash \psi_1 \wedge \psi_2$.
Si φ es de la forma $\psi_1 \vee \psi_2$ entonces $\mathcal{N} \vDash \psi_1$ o $\mathcal{N} \vDash \psi_2$, que por hipótesis de inducción $\mathbf{PA} \vdash \psi_1$ o $\mathbf{PA} \vdash \psi_2$ y, de esta forma, $\mathbf{PA} \vdash \psi_1 \vee \psi_2$.
Si φ es de la forma $(\forall x \leq \boldsymbol{n})\psi_1(x)$ entones para todo $m \leq n$ se tiene $\mathcal{N} \vDash \psi_1(\boldsymbol{m})$ y por hipótesis de inducción, para todo $m \leq n$ se cumple $\mathbf{PA} \vdash \psi_1(\boldsymbol{m})$, luego $\mathbf{PA} \vdash x = \boldsymbol{m} \rightarrow \psi_1(x)$. Por el Lema 1.8 $\mathbf{PA} \vdash x \leq \boldsymbol{n} \leftrightarrow \bigvee_{m \leq n} x = \boldsymbol{m}$ y de esta forma $\mathbf{PA} \vdash x \leq \boldsymbol{n} \rightarrow \psi_1(x)$, que es $\mathbf{PA} \vdash (\forall x \leq \boldsymbol{n})\psi_1(x)$. De la misma forma se demuestra si φ es $(\exists x\boldsymbol{n})\psi_1(x)$.
Finalmente si φ es $\exists x\psi_1(x)$, como $\mathcal{N} \vDash \exists x\psi_1(x)$ existe un natural n tal que $\mathbf{PA} \vdash \psi_1(\boldsymbol{n})$, por lo tanto $\mathbf{PA} \vdash \exists x\psi_1(x)$.

■

1.4 Funciones Recursivas

En esta sección demostraremos que las funciones recursivas $\mathcal{P}$, la menor clase de funciones que contiene a las funciones básicas y es cerrada bajo composición, recursión primitiva y μ-recursión, son aritméticamente definibles. Y además estudiaremos una función muy importante para este desarrollo, la función β de Gödel.

1.4.1 Funciones primitivas recursivas

Definición 1.4.1. Las funciones primitivas recursivas (p.r.) básicas son las siguientes:

- La función sucesor:

$$\begin{aligned} &\mathcal{S} : \mathbb{N} \to \mathbb{N} \\ &\mathcal{S}(n) = n + 1 \end{aligned}$$

- La función idénticamente nula:

$$\begin{aligned} &\mathcal{O} : \mathbb{N} \to \mathbb{N} \\ &\mathcal{O}(n) = 0 \end{aligned}$$

- Las funciones proyecciones: $\forall i, n \in \mathbb{N}$ tal que $0 \leq i \leq n$

$$\begin{aligned} &\Pi_i^{n+1} : \mathbb{N}^{n+1} \to \mathbb{N} \\ &\Pi_i^{n+1}(x_0, \ldots, x_n) = x_i \end{aligned}$$

Definición 1.4.2. Sean $g : \mathbb{N}^{n+1} \to \mathbb{N}$ y $h_0, ..., h_n : \mathbb{N}^{m+1} \to \mathbb{N}$, diremos que $f : \mathbb{N}^{n+1} \to \mathbb{N}$ se obtiene por composición de $g, h_0, ..., h_n$ que denotaremos por $f = \mathcal{C}[g; h_0, ..., h_n]$ si

$$f(x_0, ..., x_m) = g(h_0(x_0, ..., x_m), \ldots, h_n(x_0, ..., x_m))$$

Definición 1.4.3. Sean $g : \mathbb{N}^m \to \mathbb{N}$, $h : \mathbb{N}^{m+2} \to \mathbb{N}$. Denotaremos por $\mathcal{R}(g; h)$ a la función $f : \mathbb{N}^{m+1} \to \mathbb{N}$ definida por recursión primitiva a partir de g y h dada por: Para todo $\vec{x} \in \mathbb{N}, y \in \mathbb{N}$

$$\begin{cases} f(\vec{x}, 0) = g(\vec{x}) \\ f(\vec{x}, y + 1) = h(\vec{x}, y, f(\vec{x}, y)) \end{cases}$$

Definición 1.4.4. Las clase de las funciones primitivas recursivas $\mathcal{PR}$ es la menor clase de funciones que contiene a las funciones básicas y es cerrada bajo composición y recursión primitiva.

Veamos algunos ejemplos de funciones primitivas recursivas:

- Suma:

$$\begin{aligned} suma(x,0) &= x = \Pi^1_0(x) \\ suma(x,y+1) &= x+y+1 = 1+suma(x,y) = \mathcal{S}(suma(x,y)) = \\ &= \mathcal{C}[\mathcal{S},\Pi^3_2](x,y,suma(x,y)) \end{aligned}$$

  $suma(x,y) = \mathcal{R}(\Pi^1_0;\mathcal{C}[\mathcal{S};\Pi^3_2])$.

- Producto:

$$\begin{aligned} prod(x,0) &= 0 = \mathcal{O}(x) \\ prod(x,y+1) &= x+prod(x,y) = suma(x,prod(x,y)) = \\ &= suma(\Pi^3_0(x,y,prod(x,y)),\Pi^3_2(x,y,prod(x,y))) = \\ &= \mathcal{C}[suma;\Pi^3_0,\Pi^3_2](x,y,prod(x,y)) \end{aligned}$$

  $prod = \mathcal{R}(\mathcal{O};\mathcal{C}[suma;\Pi^3_0,\Pi^3_2])$.

De la misma forma podemos comprobar que son p.r.:

- Factorial: $fact(0) = 0$, $fact(x+1) = prod(s(x), fact(x))$.
- Diferencia reducida: $x \dot{-} y = 0$ si $x \leq y$, $x \dot{-} y = x - y$ en otro caso.
- Signo: $sg(x) = 0$ si $x = 0$, $sg(x) = 1$ en entro caso.
- Signo contrario: $\overline{sg}(x) = 0$ si $x \neq 0$, $\overline{sg}(x) = 1$ en otro caso.

1.4.2 Funciones Recursivas

Definición 1.4.5. Sea $f : \mathbb{N}^{n+1} \to \mathbb{N}$, la función obtenida de f por $\mu-$recursión es: Para todo $\vec{x} \in \mathbb{N}^n$,

$$(\mu y)f(\vec{x},y) = \begin{cases} y & \text{Si } f(\vec{x},y) = 0 \text{ y para todo } z < y \text{ se tiene que } f(\vec{x},z) \\ & \text{existe y además } f(\vec{x},z) \neq 0. \\ \text{No definido} & \text{En caso contrario.} \end{cases}$$

Definición 1.4.6. La clase de las funciones recursivas $\mathcal{P}$ es la menor clase de funciones que contiene las funciones básicas y es cerrada bajo composición, recursión primitiva y μ-recursión.

Definición 1.4.7. Dada $k \in \mathbb{N}$, sea $R \subseteq \mathbb{N}^k$ una relación. Su función característica $\chi_R : \mathbb{N}^k \to \{0,1\}$ es la función, que dado un $\vec{x} \in \mathbb{N}^k$ se define como:

$$\chi_R(\vec{x}) = \begin{cases} 1 & \text{Si } \vec{x} \in R \\ 0 & \text{En caso contrario} \end{cases}$$

Llamaremos a la relación R (primitiva) recursiva si χ_R es (primitiva) recursiva.

Definición 1.4.8. Diremos que un conjunto $A \subseteq \mathbb{N}^k$ es (primitivo) recursivo si su función característica χ_A es (primitiva) recursiva.

Algunos ejemplos de relaciones primitivas recursivas:

- $<$ con función característica $\chi_< = \overline{sg}(x \dot{-} y)$.
- $=$ con función característica $\chi_= = \overline{sg}(suma(sg(x \dot{-} y), sg(y \dot{-} x))$.
- De la misma forma $\leq, \geq, \neq, >$ tienen funciones características primitivas recursivas.

Proposición 1.13 (Definición por casos)**.**

1. *Sean $g, h : \mathbb{N}^k \to \mathbb{N}$ (primitivas) recursivas y $R \subseteq \mathbb{N}^k$ una relación (primitiva) recursiva, entonces:*

$$\forall \vec{x} \in \mathbb{N}^k, \;\; f(\vec{x}) = \begin{cases} g(\vec{x}) & si \;\; \chi_R(\vec{x}) = 1 \\ h(\vec{x}) & si \;\; \chi_R(\vec{x}) = 0 \end{cases}$$

es una función (primitiva) recursiva.

2. *Sea $\{A_0, \dots, A_k\}$ una partición de $\mathbb{N}^k$ por conjuntos (primitivos) recursivos mutuamente excluyentes y $g_0, \dots, g_m : \mathbb{N}^k \to \mathbb{N}$ funciones (primitivas) recursivas. Entonces:*

$$\forall \vec{x} \in \mathbb{N}^k, \;\; f(\vec{x}) = \begin{cases} g_0(\vec{x}) & si \;\; \chi_{A_0}(\vec{x}) = 1 \\ \vdots & \vdots \\ g_m(\vec{x}) & si \;\; \chi_{A_m}(\vec{x}) = 1 \end{cases}$$

es una función (primitiva) recursiva.

Corolario 1. *Las funciones máximo y mínimo son p.r.*

$$max(x, y) = \begin{cases} y & x < y \\ x & c.c. \end{cases} \qquad min(x, y) = \begin{cases} x & x < y \\ y & c.c. \end{cases}$$

Definición 1.4.9. Sean $f : \mathbb{N}^{k+1} \to \mathbb{N}, \vec{x} \in \mathbb{N}^k, y \in \mathbb{N}$, definimos:

$$\Sigma_f(\vec{x}, y) = \sum_{j \leq y} f(\vec{x}, j) \tag{1.1}$$

$$\Pi_f(\vec{x}, y) = \prod_{j \leq y} f(\vec{x}, j) \tag{1.2}$$

Proposición 1.14. *Si $f : \mathbb{N}^{k+1} \to \mathbb{N}$ es primitiva recursiva, entonces Σ_f y Π_f también lo son.*

Notación. Sea $R \subseteq \mathbb{N}^k$ una relación y $\vec{x} \in \mathbb{N}^k$. Escribiremos $R(\vec{x})$ para indicar $\vec{x} \in R$.

Definición 1.4.10. Sea $f : \mathbb{N}^k \to \mathbb{N}$, definimos el grafo de f como:

$$G(f) = \{(\vec{x}, y) : f(\vec{x}) = y\} \subseteq \mathbb{N}^{k+1}$$

Proposición 1.15. *Si $f : \mathbb{N}^k \to \mathbb{N}$ es (primitiva) recursiva, entonces $G(f)$ es (primitivo) recursivo.*

Demostración.

Si f es (primitiva) recursiva, $\chi_{G(f)}(\vec{x}, y) = \overline{sg}(|f(\vec{x}) - y|)$ y $G(f)$ es un conjunto (primitivo) recursivo.

■

Definición 1.4.11. Una relación $R \subseteq \mathbb{N}^{k+1}$ es aritméticamente definible si y solo si existe una fórmula $\varphi_R(x_0, \ldots, x_k) \in \text{FORM}_{\mathcal{L}_\text{A}}$ tal que para toda sucesión $\langle n_0, \ldots, n_k \rangle \in \mathbb{N}^{k+1}$ se tiene:

$$\langle n_0, \ldots, n_k \rangle \in R \Leftrightarrow \mathcal{N} \vDash \varphi_R(\boldsymbol{n_0}, \ldots, \boldsymbol{n_k})$$

Definición 1.4.12. Una función $f : \mathbb{N}^{k+1} \to \mathbb{N}$ es aritméticamente definible si y solo si existe una fórmula $\varphi_f(x_0, ..., x_k, y) \in \text{FORM}_{\mathcal{L}_\text{A}}$ tal que para toda sucesión $\langle n_0, \ldots, n_k \rangle \in \mathbb{N}^{k+1}$ y $m \in \mathbb{N}$ se tiene:

$$f(n_0, \ldots, n_k) = m \Leftrightarrow \mathcal{N} \vDash \varphi_f(\boldsymbol{n_1}, \ldots, \boldsymbol{n_k}, \boldsymbol{m})$$

Definición 1.4.13. $\text{Resto}(x, d, r)$ es la fórmula

$$(d = \mathbf{0} \wedge r = x) \vee (r < d \wedge \exists q \leq x[x = ((q \times d) + r])$$

Definición 1.4.14. $\text{Div}(x, d, q)$ es la fórmula

$$(d = \mathbf{0} \wedge q = \mathbf{0}) \vee (\exists r < d[x = (q \times d) + r])$$

Ambas fórmulas Resto y Div son Δ_0 (y por lo tanto Σ) p-términos y definen aritméticamente a las funciones resto y divisor respectivamente.

Definición 1.4.15. La función exponencial es primitiva recursiva y se define como:

$$\begin{cases} exp(x, 0) = 1 \\ exp(x, y + 1) = prod(x, exp(x, y)) \end{cases}$$

La abreviaremos por $exp(x, y) = x^y$.

Definición 1.4.16. Definimos la función β de Gödel como:

$$\beta(a, b, i) := resto(a, b(i + 1) + 1)$$

Definición 1.4.17. $B(a, b, i, r)$ definida como $Resto(a, \mathbf{1} + \boldsymbol{(i + 1)} \times b, r)$ es una fórmula Σ que define aritméticamente a la β de Gödel.

Lema 1.16. *Dado $k \in \mathbb{N}$ y una sucesión $\langle a_0, \dots, a_k \rangle \in \mathbb{N}$ existen $s, t \in \mathbb{N}$ tal que para todo $0 \leq i \leq k$ se tiene $a_i = \beta(s, t, i)$.*

Demostración.

La demostración de este lema es un resultado puramente de teoría de números donde se usa el teorema chino del resto y la existencia de infinitos primos, para una demostración detallada ver [Boo95] páginas 31-32.

■

Como corolario inmediato se tiene:

Corolario 2. *Para todo c, d, k, n números naturales, existen a y b naturales tal que $\beta(a, b, k) = n$ y para todo $i < k$ se tiene que $\beta(a, b, i) = \beta(c, d, i)$.*

Definición 1.4.18. El par ordenado $\langle s, t \rangle$ codificará la sucesión $\langle a_0, \dots, a_k \rangle$ si y solo si para todo $0 \leq i \leq k$ se tiene que $a_i = \beta(s, t, i)$.

El siguiente teorema justifica el estudio de las funciones recursivas en este trabajo:

Teorema 1.17. *Si $f(x_0, \dots, x_k)$ es un función recursiva de aridad k, entonces existe una fórmula $\varphi_f(x_0, \dots, x_k, y) \in FORM_{\mathcal{L}_A}$ que define aritméticamente a f.*

Demostración.

Lo demostraremos por inducción en la complejidad de f:

Funciones básicas:
La función idénticamente nula está definida por $\varphi_{\mathcal{O}}(x, y) \equiv y = 0$.
La función sucesor está definida por $\varphi_{\mathcal{S}}(x, y) \equiv y = x'$
La función proyección está definida por $\varphi_{\Pi_i^{n+1}}(x_0, \dots, x_k, y) \equiv y = x_i$.

Composición:
Sea $f(x_0, \dots, x_k) = g(h_0(x_0, \dots, x_k), \dots, h_m(x_0, \dots, x_k))$ con $g, h_0, \dots, h_m$ funciones aritméticamente definidas por $\varphi_g, \varphi_{h_0}, \dots, \varphi_{h_m}$ respectivamente. Sean $n, a_0, \dots, a_m, b_0, \dots, b_m \in \mathbb{N}$ y denotemos $\vec{a} = \langle a_0, \dots, a_m \rangle, \vec{b} = \langle b_0, \dots, b_m \rangle$ con:

$$\begin{aligned} \langle \boldsymbol{a_0}, \dots, \boldsymbol{a_m} \rangle &= \vec{\boldsymbol{a}} \\ \langle \boldsymbol{b_0}, \dots, \boldsymbol{b_m} \rangle &= \vec{\boldsymbol{b}} \\ h_0(a_0, \dots, a_m) &= b_0 \\ &\vdots \\ h_m(a_0, \dots, a_m) &= b_m \end{aligned}$$

$$g(h_0(\vec{a}), \dots, h_m(\vec{a})) = n$$

Se tiene que $\varphi_{h_0}(\vec{\boldsymbol{a}}, \boldsymbol{b_0}), \dots, \varphi_{h_m}(\vec{\boldsymbol{a}}, \boldsymbol{b_m})$ y $\varphi_g(\vec{\boldsymbol{b}}, \boldsymbol{n})$ son verdaderas, por lo tanto

$$\varphi_{h_0}(\boldsymbol{a}, \boldsymbol{b_0}) \wedge \cdots \wedge \varphi_{h_m}(\boldsymbol{a}, \boldsymbol{b_m}) \wedge \varphi_g(\boldsymbol{b_0}, \dots, \boldsymbol{b_m}, \boldsymbol{n})$$

es verdadera. De esta forma:

$$\exists\vec{c}\,[\varphi_{h_0}(\boldsymbol{a_0},\dots,\boldsymbol{a_m},c_0)\wedge\cdots\wedge\varphi_{h_m}(\boldsymbol{a_0},\dots,\boldsymbol{a_m},c_m)\wedge\varphi_g(c_0,\dots,c_m,\boldsymbol{n})]$$

también es verdadera. Ahora, sea $\vec{x}=\langle x_0,\dots,x_m\rangle\in\mathbb{N}^{m+1}$ definimos:

$$\varphi_f(\vec{\boldsymbol{x}},y)=\exists\vec{y}\,[\varphi_{h_0}(\vec{\boldsymbol{x}},y_0)\wedge\cdots\wedge\varphi_{h_m}(\vec{\boldsymbol{x}},y_m)\wedge\varphi_g(y_0,\dots,y_m,y)]$$

Tenemos que demostrar que para toda sucesión $\langle a_0,\dots,a_m\rangle\in\mathbb{N}^{m+1}$ se cumple que:

$$f(a_0,\dots,a_m)=n \text{ si y sólo si } \varphi_f(\boldsymbol{a}_0,\dots,\boldsymbol{a}_m,\boldsymbol{n}) \text{ es verdadera.}$$

($\Rightarrow$) Por construcción.
($\Leftarrow$) Supongamos que $\varphi_f(\boldsymbol{a_0},\dots,\boldsymbol{a_m},\boldsymbol{n})$ es verdadera entonces existen $d_0,\dots,d_m$ números naturales tal que

$$\varphi_{h_0}(\boldsymbol{a_0},\dots,\boldsymbol{a_m},d_0)\wedge\cdots\wedge\varphi_{h_m}(\boldsymbol{a_0},\dots,\boldsymbol{a_m},d_m)\wedge\varphi_g(d_0,\dots,d_m,\boldsymbol{n})$$

es verdadera y además son también verdaderas

$$\varphi_{h_0}(\boldsymbol{a_0},\dots,\boldsymbol{a_m},d_0),\dots,\varphi_{h_m}(\boldsymbol{a_0},\dots,\boldsymbol{a_m},d_m),\varphi_g(d_0,\dots,d_m,\boldsymbol{n})$$

De esta forma tenemos:

$$\begin{aligned} h_0(a_0,\dots,a_m)&=d_0\\ &\vdots\\ h_m(a_0,\dots,a_m)&=d_m\\ g(d_0,\dots,d_m)&=n=f(a_0,\dots,a_m)\end{aligned}$$

Recursión primitiva:
Supongamos que $f:\mathbb{N}^{m+1}\to\mathbb{N}$ está definida por recursión primitiva a partir de $g:\mathbb{N}^m\to\mathbb{N}$ y $h:\mathbb{N}^{m+2}\to\mathbb{N}$, es decir, $f=\mathcal{R}(g;h)$ con g y h funciones aritméticamente definidas por $\varphi_g,\varphi_h\in\mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ respectivamente. Sea $z=f(\vec{x},y)$, entonces existe una sucesión $\langle k_0,\dots,k_p\rangle$ tal que para $u<p$ se cumple que:

$$\begin{aligned} k_0&=g(\vec{x})\\ k_{u+1}&=h(\vec{x},u,f(\vec{x},u))=f(\vec{x},u+1)\\ k_p&=h(\vec{x},y,z)=f(\vec{x},y+1)\end{aligned}$$

A continuación definimos $F(\vec{x},y,z)$ como sigue:

$$\begin{aligned}\exists s\exists t\Big[&\exists u[B(s,t,0,u)\wedge\varphi_g(\vec{x},u)]\wedge\\ (\forall u<y)&\Big[\exists v\exists w[B(s,t,u,v)\wedge B(s,t,u',w)\wedge w=h(\vec{x},u,v)]\Big]\wedge\\ &B(s,t,y,z)\Big]\end{aligned}$$

$F(\vec{x}, y, z)$ define aritméticamente a nuestra función f.

Minimización:

Sea $f : \mathbb{N}^{m+1} \to \mathbb{N}$ una función y sea $(\mu y)f(\vec{x}, y)$ la función definida por μ-recursión a partir de f. Definimos $(\mu y)F(\vec{x}, y)$ de la siguiente forma:

$$\exists s \exists t \Big[B(s, t, y, \mathbf{0}) \wedge$$
$$(\forall z \leq y)\big[z = y \vee \exists u[B(s, t, z, u) \wedge u \neq \mathbf{0}]\big]\Big]$$

$(\mu y)F(\vec{x}, y)$ define aritméticamente a $(\mu y)f(\vec{x}, y)$.

■

Corolario 3. *Toda relación recursiva es aritméticamente definible.*

Corolario 4. *Toda función recursiva es aritméticamente definible por una fórmula* Σ.

1.5 Aritmetización de la sintaxis

En esta sección desarrollaremos la sintaxis de **PA** dentro de **PA** gracias a la idea de Gödel de asociar expresiones de la teoría formal con números naturales.

1.5.1 Numeración de Gödel

Asociaremos a cada símbolo primitivo de **PA** un número natural, al que llamaremos su número de Gödel.

A los símbolos $\perp, \to, =, \forall, \mathbf{0}, ', +, \times$ le asignaremos los números $1, 3, 5, 7, 9, 11, 13, 15$ respectivamente y a la variable x_i le asignaremos $2i+17$. De esta forma cada símbolo primitivo de **PA** tiene un número impar de Gödel asociado.

Sean x, y dos objetos, ya sean símbolos o pares ordenados, con respectivos números de Gödel i, j, entonces el par ordenado $\langle x, y\rangle$ tendrá número de Gödel

$\pi(i, j) = 2((i + j)(i + j) + i + 1)$.

Remarcamos que cada símbolo tiene número de Gödel impar, mientras que para cualesquiera i, j, $\pi(i, j)$ será par y por lo tanto no será el número de Gödel de ningún símbolo primitivo de **PA**.

Con esta codificación, todos los términos y fórmulas de **PA** tienen su correspondiente número de Gödel asignado, ya que estos son una variable, $\mathbf{0}$, $\perp$, o un par ordenado.

Definición 1.5.1. $\mathrm{Par}(x, y, z)$ denota la Σ fórmula $2((x + y)(x + y) + x + 1) = z$.

Esta definición de la función Par se fundamenta en que el número

$(i + j)(i + j) + i + 1$ realmente codifica $\langle i, j\rangle$ de manera única.

Notación. $(x, y) = 2((x + y)(x + y) + x + 1)$

Proposición 1.18. *Si* $(x, y) = (u, v)$ *entonces* $x = u, y = v$.

Demostración.

Supongamos que $(x + y)(x + y) + x + 1 = (u + v)(u + v) + u + 1$.
Si $x + y < u + v$ entonces

$$(x + y)(x + y) + x + 1 \leq (x + y + 1)(x + y + 1) \leq (u + v)(u + v) + u + 1$$

que no puede pasar.
Aplicando el mismo razonamiento cuando $u + v < x + y$ obtenemos $(u, v) < (x, y)$.
Por lo tanto $x + y = u + v, x = u, y = v$.

■

De esta forma nos queda el siguiente resultado:

Proposición 1.19.

1. *Si* $x < u$ *entonces* $(x, y) < (u, y)$
2. *Si* $y < v$ *entonces* $(x, y) < (x, v)$.

Definición 1.5.2. $\mathrm{Fst}(z, w)$ es la fórmula
$(\exists y < z)[(w, y) = z] \vee ((\neg\exists x, y < z)[(x, y) = z] \wedge w = \mathbf{0})$.

Definición 1.5.3. $\mathrm{Snd}(z, w)$ es la fórmula
$(\exists y < z)[(y, w) = z] \vee ((\neg\exists x, y < z)[(y, w) = z] \wedge w = \mathbf{0})$.

Fst y Snd son ambos Σ p-términos que definen aritméticamente funciones de $\mathbb{N}^2$ en $\mathbb{N}$, fst y snd respectivamente, de modo que utilizando nuestra convención dobre p-términos se tiene: $\mathbf{PA} \vdash fst((x, y)) = x$ y $\mathbf{PA} \vdash snd((x, y)) = y$.

De igual forma, para tratar con triples definimos:

Definición 1.5.4. $(x, y, z) = (x, (y, z))$

Definición 1.5.5. Y tenemos:

1. $ft(w) = fst(w)$, $\mathbf{PA} \vdash ft((x, y, z)) = x$
2. $sd(w) = fst(snd(w))$, $\mathbf{PA} \vdash sd((x, y, z)) = y$
3. $td(w) = snd(snd(w))$, $\mathbf{PA} \vdash td((x, y, z)) = z$

1.5.2 Codificación de sucesiones finitas

Una sucesión finita $\varphi_0, \ldots, \varphi_k$ está determinada por su longitud $k + 1$ y sus valores φ_i con $0 \leq i \leq k$. Si dos sucesiones distintas s y t tienen la misma longitud, existe un $0 \leq j \leq k$ tal que $s_j \neq t_j$.

Recordando la Definición 1.2.6, vamos a tratar las demostraciones en **PA** como sucesiones, por lo tanto cada demostración tendrá asignada un número de Gödel, nuestro objetivo ahora es que ese número sea distinto de cada fórmula y cada símbolo de **PA**. Para ello, el número de Gödel para sucesiones de longitud k será de la forma $\pi(\pi(a,b),k+1)$.

De esta forma, definimos una sucesión finita s de longitud $k+1$ como sigue.

Definición 1.5.6. $FinSeq(s)$ es la fórmula

$$(\exists a < s \exists b < s \exists k < s)\Big[s = ((a,b),k) \wedge$$
$$(\forall c < s \forall d < s)\Big[(c,d) < (a,b) \to (\exists i < k)[\beta(c,d,i) \neq \beta(a,b,i)]\Big]\Big]$$

Definición 1.5.7. $long(s) = snd(s)$ da el valor de la longitud de la sucesión codificada por s.

Definición 1.5.8. $valor(s,i) = \beta(fst(fst(s)), snd(fst(s)), i)$ devuelve el valor de la entrada i-ésima de la sucesión.

De la propia definición de $Finseq(s)$ aparecen las siguientes dos obseraciones:

Proposición 1.20.

1. *$FinSeq(s) \in \Delta$.*
2. *$long(s)$ y $valor(s,i)$ son aritméticamente definibles por las fórmulas $Long(s,y)$ y $Val(s,i,z)$ respectivamente.*

Se puede demostrar que las sucesiones solo dependen de sus entradas y su longitud, esto es:

PA $\vdash (FinSeq(s) \wedge FinSeq(t) \wedge long(s) = long(t) \wedge (\forall i < long(s))[s_i = t_i]) \to s = t.$
PA $\vdash \exists! t[FinSeq(s) \wedge long(s) = \mathbf{0}]$.

Proposición 1.21 (Inducción fuerte)**.** *Para toda fórmula $\varphi(x) \in FORM_{\mathcal{L}_A}$ se cumple:*

$$\forall x\big(\forall y[y < x \to \varphi(y)] \to \varphi(x)\big) \to \varphi(x)$$

Demostración.

Sea $G(x)$ la fórmula $\forall y[y < x \to \varphi(y)] \wedge \varphi(x)$. Razonando en **PA**, asumiremos que $\vdash \forall x\big(\forall y[y < x \to \varphi(y)] \to \varphi(x)\big)$ y demostraremos $\forall x G(x)$ por inducción, es decir, veamos que $\vdash G(\mathbf{0})$ y $\vdash \forall x[G(x) \to G(x')]$.

$\vdash G(\mathbf{0})$:

(1)	$\forall x\big[\forall y[y < \mathbf{0} \to \varphi(y)] \to \varphi(\mathbf{0})\big]$	Suposición
(2)	$\forall y[\neg(y < \mathbf{0})]$	Lema 1.6
(3)	$\forall y[y < 0 \to \varphi(y)]$	Consecuencia lógica; (2)
(4)	$\varphi(\mathbf{0})$	Consecuencia lógica; (1), (3)
(5)	$G(\mathbf{0})$	Consecuencia lógica; (4)

$\vdash \forall x[G(x) \to G(x')]$:

(1)	$\forall x\big[\forall y[y < x \to \varphi(y)] \to \varphi(x)\big]$	Suposición
(2)	$G(x)$	Suposición
(3)	$\forall y[y < x \to \varphi(y)]$	Consecuencia lógica; (2)
(4)	$\varphi(x)$	Consecuencia lógica; (2)
(5)	$\forall y[y < x' \to \varphi(y)]$	Lema 1.7
(6)	$\varphi(x')$	Consecuencia lógica; (1), (5)
(7)	$\forall y[y < x' \to \varphi(y)] \wedge \varphi(x')$	Consecuencia lógica; (5), (6)
(8)	$G(x')$	Definición de $G(x)$; (7)

■

Corolario 5 (Principio del menor elemento)**.** *Se tiene que:*

$$\mathbf{PA} \vdash \varphi(x) \to \exists x\big[\varphi(x) \wedge \forall y[y < x \to \neg\varphi(y)]\big]$$

Demostración.

Se demuestra sustituyendo $\neg\varphi(x)$ por $\varphi(x)$ en el principio de inducción fuerte.

■

Proposición 1.22.

$$\mathbf{PA} \vdash \mathit{long}(s) = x \to \exists! t[\mathit{FinSeq}(t) \wedge \mathit{long}(t) = x' \wedge (\forall i < x)[s_i = t_i \wedge t_x = \boldsymbol{n}]]$$

Demostración.

Supongamos que $\mathit{long}(s) = x$, sean $c = fst(fst(s)), d = snd(fst(s))$, como en Corolario 2 sabemos que existen a, b tal que $\beta(a, b, x) = n$ y para toda $i < x$ se tiene que $\beta(a, b, i) = \beta(c, d, i)$. De esta forma, siendo t la sucesión dada por $t = ((a, b), x')$ se tiene que $\mathit{long}(t) = \mathit{long}(s)'$ y para toda $i < x$, $t_i = s_i$ y $t_x = \beta(a, b, x)$. Por el principio del menor elemento obtenemos (a, b) mínimos.

■

Como corolario se obtiene:

Corolario 6. *Para todo p-término $H(i, y)$ se tiene*

$$\mathbf{PA} \vdash \exists! s\big[\mathit{Finseq}(s) \wedge \mathit{long}(s) = x \wedge (\forall i < x)[s_i = h(i)]\big]$$

A continuación vamos a describir de manera formal como podemos truncar y concatenar sucesiones finitas.

$$\begin{aligned}\mathbf{PA} \vdash &(e \leq j < k \wedge long(s) = k) \rightarrow \\ &\exists! t[FinSeq(t) \wedge long(t) = j - e \wedge (\forall i < j - e)[t_i = s_{e+i}]\end{aligned} \tag{1.3}$$

$$\begin{aligned}\mathbf{PA} \vdash &long(s) = k \wedge long(t) = l \wedge j \leq k + l \wedge \\ &(\exists v)[FinSeq(v) \wedge long(v) = j \wedge \\ &(\forall i < j)[i < k \rightarrow v_i = s_i \wedge k \leq i < j \rightarrow v_i = t_{i-k}]\end{aligned} \tag{1.4}$$

$$\begin{aligned}\mathbf{PA} \vdash &long(s) = k \wedge long(t) = l \rightarrow \\ &(\exists v)\big[FinSeq(v) \wedge long(v) = k + l \wedge \\ &(\forall i < k)[v_i = s_i \wedge (\forall i < l)[v_{k+1} = t_i]\big]\end{aligned} \tag{1.5}$$

$(1.3), (1.4)$ se demuestran fácilmente usando la Proposición 1.22 y (1.5) sale como corolario de (1.4).

Definición 1.5.9. $Trunc(s, e, j, t)$ es la fórmula

$$\begin{aligned}&(\neg(e \leq j < long(s)) \wedge t = \langle\rangle) \vee \\ &(e \leq j < long(s) \wedge FinSeq(t) \wedge \\ &long(t) = j - e + 1 \wedge (\forall i < j - e + 1)[t_i = s_{e+i}])\end{aligned}$$

Trunc es un Σ p-término que dada una sucesión $s = \langle s_0, \ldots, s_e, \ldots, s_j, \ldots, s_n\rangle$, define $trunc(s, e, j) = \langle s_e, \ldots, s_j\rangle$.

Notación. $trunc(s, e, j) = s_{[e,j]}$

Definición 1.5.10. $Concat(s, t, v)$ es la fórmula

$$\begin{aligned}&FinSeq(v) \wedge long(v) = long(s) + long(t) \wedge \\ &\forall i < long(s)[v_i = s_i] \wedge \\ &\forall i < long(t)[v_{long(s)+i} = t_i])\end{aligned}$$

Notación. $s * t = concat(s, t)$.

Definición 1.5.11.

$$Seq(n, s) \equiv FinSeq(s) \wedge long(s) = 1 \wedge s_0 = n$$

Notación. $\langle n\rangle = seq(n)$.

Gracias a $(1.3), (1.4), (1.5)$ Trunc, Concat y Seq son Σ p-términos. Además es fácil ver que:

Proposición 1.23.
$\mathbf{PA} \vdash FinSeq(s) \rightarrow \langle\rangle * s = s = s * \langle\rangle$.
$\mathbf{PA} \vdash (FinSeq(s) \wedge FinSeq(t) \wedge FinSeq(v)) \rightarrow s * (t * v) = (s * t) * v$.

1.5.3 Formalización de la codificación de Gödel en PA

Gracias a lo desarrollado anteriormente podemos hablar de términos y fórmulas de **PA** dentro de **PA**.

Definición 1.5.12. $\ulcorner\bot\urcorner, \ulcorner\rightarrow\urcorner, \ulcorner\forall\urcorner, \ulcorner=\urcorner, \ulcorner\mathbf{0}\urcorner, \ulcorner\prime\urcorner, \ulcorner+\urcorner, \ulcorner\times\urcorner$ son los términos $\mathbf{1}, \mathbf{3}, \mathbf{5}, \mathbf{7}, \mathbf{9}, \mathbf{11}, \mathbf{13}, \mathbf{15}$ respectivamente.

Definición 1.5.13. $Var(v)$ es la Δ fórmula $(\exists i < v)[v = \mathbf{2} \times \boldsymbol{i} + \mathbf{17}]$

Definición 1.5.14. $Term(t)$ es la fórmula

$$\exists s \Big[FinSeq(s) \wedge long(s) > \mathbf{0} \wedge s_{long(s)-1} = t \wedge$$
$$\forall i < long(s) \Big[s_i = \ulcorner\mathbf{0}\urcorner \vee Var(s_i) \vee$$
$$(\exists j, k < i) \big[s_i = (\ulcorner\prime\urcorner, s_j) \vee s_i = (\ulcorner+\urcorner, s_j, s_k) \vee s_i = (\ulcorner\times\urcorner, s_j, s_k) \big] \Big] \Big]$$

Es fácil ver que $Term$ es Σ, pero se puede demostrar que es una fórmula Δ (ver [Boo95] pág 42).

Definición 1.5.15. $AtForm(x)$ es la fórmula

$$x = \ulcorner\bot\urcorner \vee (\exists s < x \exists t < x) \left[Term(s) \wedge Term(t) \wedge x = (\ulcorner=\urcorner, s, t) \right]$$

Debido a que $Term$ es Δ, $AtForm$ es también una fórmula Δ.

Definición 1.5.16. $Formula(x) \equiv$

$$\exists s \Big[FinSeq(s) \wedge long(s) > \mathbf{0} \wedge s_{long(s)-1} = x \wedge$$
$$(\forall i < long(s)) \Big[AtForm(s_i) \vee (\exists j, k < i) \big[s_i = (\ulcorner\rightarrow\urcorner, s_j, s_k) \vee$$
$$(\exists j < i \exists v) \big[Var(v) \wedge s_i = (\ulcorner\forall\urcorner, v, s_j) \big] \Big] \Big]$$

$Formula(x)$ vuelve a ser una Δ fórmula y la demostración es similar a la de $Term$.

Gracias a las funciones definidas, podemos demostrar en **PA** fórmulas como la siguiente:

$$(\forall x) \left[Formula(x) \rightarrow Formula((\ulcorner\rightarrow\urcorner, x, \ulcorner\bot\urcorner)) \right]$$

que nos afirma que la negación de cualquier fórmula es también una fórmula de **PA**. Y como esta, **PA** puede demostrar muchas fórmulas que hablen sobre la propia sintaxis de **PA** o de carácter similar.

Supongamos la existencia de $Axioma(x)$ (ver [Mon76] para una prueba), una fórmula Δ que afirma que x es el número de Gödel de un axioma de **PA** o un axioma lógico, supongamos también de la fórmula $sub(t, i, x)$, un Σ p-término que sustituye el término con número de Gödel t en la iésima variable de la fórmula con número de Gödel x.

A continuación definiremos dos fórmulas que son verdaderas cuando la fórmula con número de Gödel x es la conclusión de, respectivamente, aplicar Modus Ponens y Generalización:

Definición 1.5.17. $ConseqMP(x, y, z)$ es la fórmula

$$Formula(x) \wedge Formula(z) \wedge y = \ulcorner z \rightarrow x \urcorner$$

Definición 1.5.18. $ConseqG(x, y)$ es la fórmula

$$(\exists z < x)\,[Formula(y) \wedge Var(z) \wedge x = (\ulcorner \forall \urcorner, z, y)]$$

Definición 1.5.19. $Pf(y, x)$ es la fórmula

$$FinSeq(y) \wedge s_{long(y)-1} = x \wedge (\forall i < long(y) - 1)\Big[Axioma(y_i) \vee$$
$$(\exists j < i \exists k < i)[ConseqMP(y_i, y_j, y_k)] \vee (\exists j < i)[ConseqG(y_i, y_j)]\Big]$$

Definición 1.5.20. Definimos $Prov(x)$ como la fórmula $\exists y Pf(y, x)$.

$Prov$ es la fórmula que expresa la demostrabilidad en **PA**, claramente es una Σ fórmula ya que Pf es Δ.

Lema 1.24. *Sea $\varphi \in SENT_{\mathcal{L}_A}$, si φ es Σ entonces* $\mathbf{PA} \vdash \varphi \rightarrow Prov(\ulcorner \varphi \urcorner)$.

A continuación vamos a introducir las condiciones de derivabilidad introducidas por M.H. Löb $P1 - P3$.

Proposición 1.25.

P1. *Si* $\mathbf{PA} \vdash \varphi$ *entonces* $\mathbf{PA} \vdash Prov(\ulcorner \varphi \urcorner)$

P2. $\mathbf{PA} \vdash Prov(\ulcorner \varphi \rightarrow \psi \urcorner) \rightarrow (Prov(\ulcorner \varphi \urcorner) \rightarrow Prov(\ulcorner \psi \urcorner))$

P3. $\mathbf{PA} \vdash Prov(\ulcorner \varphi \urcorner) \rightarrow Prov(\ulcorner Prov(\ulcorner \varphi \urcorner) \urcorner)$

Demostración.

1. Supongamos que $\mathbf{PA} \vdash \varphi$, entonces $Prov(\ulcorner \varphi \urcorner)$ es una Σ fórmula verdadera y así $\mathbf{PA} \vdash Prov(\ulcorner \varphi \urcorner)$.

2. Supongamos que $\mathbf{PA} \vdash Prov(\ulcorner \varphi \rightarrow \psi \urcorner)$, y supongamos $\mathbf{PA} \vdash Prov(\ulcorner \varphi \urcorner)$, nuestro objetivo es construir una demostración de ψ, para ello sean a, b los números de Gödel de las demostraciones de **PA** de $\varphi \rightarrow \psi$ y φ respectivamente y sea $a * b$ la concatenación de las sucesiones codificadas por a y b, si a continuación concatenamos $(a * b) * \langle \psi \rangle$ obtenemos una demostración de ψ gracias a *modus ponens*, esto implica que $\mathbf{PA} \vdash \exists y[Pf(y, \ulcorner \psi \urcorner)]$ que equivale a $\mathbf{PA} \vdash Prov(\ulcorner \psi \urcorner)$.

3. Como $Prov(\ulcorner\varphi\urcorner)$ es Σ, por el Lema 1.24 tenemos el resultado.

■

Las condiciones de derivabilidad $P1-P3$ y el Teorema de Löb que presentaremos en el capítulo 3, nos ofrecen un análisis completo de $Prov$, que va a ser fundamental en el objetivo de esta memoria.

1.5.4 Teoremas de incompletitud de Gödel

Lema Diagonal Generalizado. *Sean $y_0, ..., y_n, z_1, ..., z_m$ variables distintas y $\varphi_0(y_0, ..., y_n, \vec{z}), ..., \varphi_n(y_0, ..., y_n, \vec{z})$, donde $\vec{z} = (z_1, ..., z_m)$, son fórmulas de* **PA** *donde todas las variables libres están en $y_0, ..., y_n, \vec{z}$.*
Entonces existen formulas $\psi_0(\vec{z}), ..., \psi_n(\vec{z})$ del lenguaje de **PA** *donde todas las variables libres están en $\vec{z}$ tal que:*

$$\mathbf{PA} \vdash \psi_0 \leftrightarrow \varphi_0(\ulcorner\psi_0(\vec{z})\urcorner, ..., \ulcorner\psi_n(\vec{z})\urcorner, \vec{z})$$
$$\vdots$$
$$\mathbf{PA} \vdash \psi_n \leftrightarrow \varphi_n(\ulcorner\psi_0(\vec{z})\urcorner, ..., \ulcorner\psi_n(\vec{z})\urcorner, \vec{z})$$

Demostración.

Sea $sus(\vec{y})$ una función Σ definible de aridad $n+2$ cuyo valor $sus(a, x_o, \ldots, x_n)$ es el número de Gödel que resulta a sustituir $x_0, \ldots, x_n$ por los numerales $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n$ en la fórmula con número de Gödel a.

Dado $0 \leq i \leq n$ sean

$$k_i = \ulcorner\varphi_i\,(sus(x_0, x_0, \ldots, x_n), \ldots, sus(x_n, x_0, \ldots, x_n), \vec{z})\urcorner$$
$$\psi_i(\vec{z}) = \varphi_i\,(sus(\boldsymbol{k}_0, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n), \ldots, sus(\boldsymbol{k}_n, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n), \vec{z})$$

Hay que demostrar que $\mathbf{PA} \vdash sus(\boldsymbol{k}_i, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n) = \ulcorner\psi_i\urcorner$; por definición de sus, $sus(\boldsymbol{k}_i, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n)$ es el número de Gödel de sustituir $x_0, \ldots, x_n$ por $\boldsymbol{k}_0, \ldots, \boldsymbol{k}_n$ en la fórmula con número de Gödel $k_i = \ulcorner\varphi_i\,(sus(x_0, x_0, \ldots, x_n), \ldots, sus(x_n, x_0, \ldots, x_n), \vec{z})\urcorner$, esto es:

$$sus(\boldsymbol{k}_i, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n) = \ulcorner\varphi_i\,(sus(\boldsymbol{k}_0, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n), \ldots, sus(\boldsymbol{k}_n, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n), \vec{z})\urcorner = \ulcorner\psi_i\,(\vec{z})\urcorner$$

Al ser $sus(\boldsymbol{k}_i, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n) = \ulcorner\psi_i\,(\vec{z})\urcorner$ una fórmula Σ y verdadera, se tiene finalmente

$$\mathbf{PA} \vdash sus(\boldsymbol{k}_i, \boldsymbol{k}_0, \ldots, \boldsymbol{k}_n) = \ulcorner\psi_i\,(\vec{z})\urcorner$$

■

Corolario 7. *Sean $P_0(y_0, ..., y_n), ..., P_n(y_0, ..., y_n)$ fórmulas de* **PA***, donde las variables libres están entre $y_0, ..., y_n$. Entonces existen fórmulas cerradas $S_0, ..., S_n$ de* **PA** *tal que:*

$$\mathbf{PA} \vdash S_0 \leftrightarrow P_0(\ulcorner S_0\urcorner, ..., \ulcorner S_n\urcorner),$$
$$\mathbf{PA} \vdash S_n \leftrightarrow P_0(\ulcorner S_0\urcorner, ..., \ulcorner S_n\urcorner).$$

Corolario 8 (Lema Diagonal). *Sea $P(x) \in FORM_{\mathcal{L}_A}$ donde x es la única variable libre, entonces existe $S \in SENT_{\mathcal{L}_A}$ tal que* $\mathbf{PA} \vdash S \leftrightarrow P(\ulcorner S \urcorner)$.

Por el lema diagonal, sabemos que existe una fórmula, llamémosla G, tal que $\mathbf{PA} \vdash G \leftrightarrow \neg Prov(\ulcorner G \urcorner)$.

Lema 1.26. *Si* $\mathbf{PA}$ *es consistente, entonces* $\mathbf{PA} \nvdash G$.

Demostración.

Por reducción al absurdo:

(1)	$\mathbf{PA} \vdash G$	Suposición
(2)	$\mathbf{PA} \vdash Prov(\ulcorner G \urcorner)$	P1; (1)
(3)	$\mathbf{PA} \vdash G \leftrightarrow \neg Prov(\ulcorner G \urcorner)$	Lema diagonal
(4)	$\mathbf{PA} \vdash G \rightarrow \neg Prov(\ulcorner G \urcorner)$	Consecuencia lógica; (3)
(5)	$\mathbf{PA} \vdash \neg G$	Consecuencia lógica; (4)
(6)	$\mathbf{PA} \vdash G \wedge \neg G$	Consecuencia lógica; $(1), (5)$

Y llegamos a la contradicción.

■

Definición 1.5.21. Una teoría $\mathbf{T}$ que extiende a $\boldsymbol{Q}$ es ω-consistente si para toda fórmula $\varphi(x) \in \mathrm{FORM}_{\mathcal{L}_A}$ y si para todo $n \in \mathbb{N}$ se tiene $\mathbf{T} \vdash \neg\varphi(n)$ entonces $\mathbf{T} \nvdash \exists x \varphi(x)$.
$\mathbf{T}$ se dice ω-inconsistente en otro caso.

Proposición 1.27. *Toda teoría ω-consistente también es consistente.*

Demostración.

Si $\mathbf{T}$ es inconsistente, entonces para toda fórmula φ de $\mathbf{T}$, $\mathbf{T}\vdash \varphi$, en particular deriva $\exists x \varphi(x)$ y $\neg\varphi(\mathbf{0})$,$\neg\varphi(\mathbf{1})$,..., y por lo tanto es ω-inconsistente.

■

Lema 1.28. *Si* $\mathbf{PA}$ *es ω-consistente, entonces* $\mathbf{PA} \nvdash \neg G$ *siendo G como en el Lema 1.26.*

Demostración.

Suponemos $\mathbf{PA} \vdash \neg G$, si $\mathbf{PA}$ es inconsistente entonces es ω-inconsistente y ya hemos acabado.
Si $\mathbf{PA}$ es consistente, $\mathbf{PA} \nvdash G$ por el lema 1.26, por lo tanto $\mathbf{PA} \nvdash \exists x[Pf(x, \ulcorner G \urcorner)]$ y como $\mathbf{PA}$ es consistente $\mathbf{PA} \vdash \neg Pf(\mathbf{0}, \ulcorner G \urcorner), ...$ pero como $\neg G \equiv \exists x[Pf(x, \ulcorner G \urcorner)]$ y $\mathbf{PA} \vdash G$ por suposición, tenemos la contradicción buscada. ■

Como corolario de los lemas 1.26 y 1.28 se tiene:

Teorema 1.29 (Primer teorema de Gödel). *Si* **PA** *es ω-consistente entonces no es completa.*

Definición 1.5.22. $Con_{\mathbf{PA}} \equiv \neg Prov(\ulcorner 0 = 1 \urcorner)$

$Con_{\mathbf{PA}}$ afirma que **PA** es consistente.

Teorema 1.30 (Segundo teorema de Gödel)**.** *Si* **PA** *es consistente, entonces:*

$$\mathbf{PA} \nvdash Con_{\mathbf{PA}}$$

Demostración.

La idea de la demostración se basa en que, gracias al lema 1.26 sabemos que si **PA** es consistente entonces no puede derivar G, por lo que tenemos una demostración de $Con_{\mathbf{PA}} \to \neg Prov(\ulcorner G \urcorner)$. Si suponemos que **PA** deriva $Con_{\mathbf{PA}}$, tenemos $\neg Prov(\ulcorner G \urcorner)$ pero $G \leftrightarrow \neg Prov(\ulcorner G \urcorner)$, por lo tanto **PA** deriva G, lo que nos lleva a una contradicción y **PA** no deriva $Con_{\mathbf{PA}}$. Formalizando este argumento:

(1)	$\mathbf{PA} \vdash G \leftrightarrow \neg Prov(\ulcorner G \urcorner)$	Lema diagonal
(2)	$\mathbf{PA} \vdash G \to \neg Prov(\ulcorner G \urcorner)$	Consecuencia lógica; (1)
(3)	$\mathbf{PA} \vdash G \to (Prov(\ulcorner G \urcorner) \to \bot)$	Definición de $\neg$
(4)	$\mathbf{PA} \vdash Prov(\ulcorner G \to (Prov(\ulcorner G \urcorner) \to \bot) \urcorner)$	P1; (3)
(5)	$\mathbf{PA} \vdash Prov(\ulcorner G \urcorner) \to Prov(\ulcorner Prov(\ulcorner G \urcorner) \to \bot \urcorner)$	P2; (4)
(6)	$\mathbf{PA} \vdash Prov(\ulcorner G \urcorner) \to$ $\to (Prov(\ulcorner Prov(\ulcorner G \urcorner) \urcorner) \to Prov(\ulcorner \bot \urcorner))$	P2; (5)
(7)	$\mathbf{PA} \vdash Prov(\ulcorner G \urcorner) \to Prov(\ulcorner Prov(\ulcorner G \urcorner) \urcorner)$	P3
(8)	$\mathbf{PA} \vdash Prov(\ulcorner G \urcorner) \to Prov(\ulcorner \bot \urcorner)$	Consecuencia lógica; (6), (7)
(9)	$\mathbf{PA} \vdash \neg Prov(\ulcorner \bot \urcorner) \to \neg Prov(\ulcorner G \urcorner)$	Consecuencia lógica; (8)
(10)	$\mathbf{PA} \vdash \neg Prov(\ulcorner \mathbf{0} = \mathbf{1} \urcorner) \to \neg Prov(\ulcorner G \urcorner)$	$\bot \equiv \mathbf{0} = \mathbf{1}$
(11)	$\mathbf{PA} \vdash Con_{\mathbf{PA}} \to \neg Prov(\ulcorner G \urcorner)$	
(12)	$\mathbf{PA} \vdash Con_{\mathbf{PA}} \to G$	Consecuencia lógica; (1), (11)

■

Podemos generalizar el teorema a cualquier teoría $\mathbf{T}$ con una fórmula $Prov_T$ que satisfaga las condiciones de derivabilidad de la proposición 1.25 para dicha teoría $\mathbf{T}$ y cambiando G por G_T cumpliendo $\mathbf{T} \vdash G_T \leftrightarrow \neg Prov_T(\ulcorner G_T \urcorner)$.

Capítulo 2

Lógica Modal

2.1 Lenguaje de la lógica modal proposicional

Definición 2.1.1. El lenguaje de la lógica modal proposicional $\mathcal{L}_\Box$ consta de los siguientes símbolos:

- Conjunto infinito numerable de variables proposicionales $p_0, p_1, ...$
- Conectores Booleanos $\{\rightarrow, \bot\}$.
- Operador modal $\Box$.

Definición 2.1.2. Se define el conjunto de proposiciones atómicas $\textsc{At}$ como el menor conjunto que contiene a $\bot$ y todas las variables proposicionales $p_0, p_1, ...$

Definición 2.1.3. Se define el conjunto de fórmulas de $\mathcal{L}_\Box$ como el menor conjunto $\mathrm{FORM}_{\mathcal{L}_\Box}$ como sigue:

- $\bot \in \mathrm{FORM}_{\mathcal{L}_\Box}$.
- $p_0, p_1, ... \in \mathrm{FORM}_{\mathcal{L}_\Box}$.
- $A, B \in \mathrm{FORM}_{\mathcal{L}_\Box} \Rightarrow (A \rightarrow B) \in \mathrm{FORM}_{\mathcal{L}_\Box}$.
- $A \in \mathrm{FORM}_{\mathcal{L}_\Box} \Rightarrow (\Box A) \in \mathrm{FORM}_{\mathcal{L}_\Box}$.

Definición 2.1.4. Sean $A, B \in \mathrm{FORM}_{\mathcal{L}_\Box}$:

- $\neg A := A \rightarrow \bot$
- $A \vee B := \neg A \rightarrow B$
- $A \wedge B := \neg(\neg A \vee \neg B)$
- $A \leftrightarrow B := (A \rightarrow B) \wedge (B \rightarrow A)$
- $\Diamond := \neg\Box\neg$.

2.2 Semántica

En el estudio de la semántica introduciremos dos conceptos imprescindibles, los marcos y los modelos, juntos a las relaciones entre mundos y las evaluaciones de fórmulas modales. También estudiaremos los principales axiomas de la lógica modal así como su validez en los distintos tipos de marcos.

Definición 2.2.1.

- R es una relación en W si para todo w, x, si wRx entonces $w, x \in W$.
- Una relación R en W es reflexiva en W si para todo w en W, wRw.
- Una relación R en W es irreflexiva en W si para todo w en W, no ocurre que wRw.
- R es antisimétrica si para todo w, x; si wRx y xRw entonces $w = x$.
- R es transitiva si para todo w, x, y, si wRx y xRy entonces wRy.
- R es simétrica si para todo w, x; si wRx entonces xRw.
- R es euclídea si para todo w, x, y, si wRx y wRy entonces xRy.
- R es una relación de equivalencia en W si R es reflexiva en W, transitiva y simétrica.

Definición 2.2.2. Un marco es un par ordenado $F = \langle W, R \rangle$ donde W es conjunto no vacío llamado dominio, cuyos elementos se denominan mundos y
$R \subseteq W \times W$ es una relación de W llamada relación de accesibilidad.
Para $w, x \in W$ escribimos xRw si $\langle w, x \rangle \in R$ y lo leemos 'w tiene acceso a x'.

Definición 2.2.3. Una evaluación V en un conjunto W es una relación entre los elementos de W y variables proposicionales, $V \subseteq W \times \text{AT}$.

Definición 2.2.4. Un modelo es una estructura $M = \langle W, R, V \rangle$ donde $\langle W, R \rangle$ es un marco y V es una evaluación en W. Un modelo $\langle W, R, V \rangle$ se dice que está basado en el marco $\langle W, R \rangle$.

Definición 2.2.5. Un modelo es finito, reflexivo, transitivo,..., si y solo si el marco donde se basa es finito, reflexivo, transitivo,...

Definición 2.2.6. Para todo $A \in \text{FORM}_{\mathcal{L}_\Box}$, modelo $M = \langle W, R, V \rangle$ y mundo $w \in W$, definimos la relación $M, w \vDash A$ como:

- $\neg(M, w \vDash \bot)$, que denotaremos $M, w \nvDash \bot$.
- $M, w \vDash p_i \Leftrightarrow wVp_i$.

- $M, w \models (B \to C) \Leftrightarrow (M, w \not\models B \vee M, w \models C)$.
- $M, w \models \Box B \Leftrightarrow$ para todo $x \in W$ tal que wRx tenemos $M, x \models B$.

Definición 2.2.7. Para $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$ y $M = \langle W, R, V \rangle$ decimos que:

- A es verdadera en un mundo w en un modelo M si y solo si $M, w \models A$.
- A es válida en un modelo M si y solo si para todo mundo $w \in W$ se tiene que $M, w \models A$.
- A es válida en marco F si y solo si para todo modelo M basado en F, A es válida en M.
- Diremos que A es satisfacible en M si y solo si existe un mundo $w \in W$ tal que A es verdadera en w.
- Diremos que A es satisfacible en un marco $F = \langle R, V \rangle$ si y solo si existe un modelo basado en F donde A es satisfacible.

Notación. $\boxdot A = \Box A \wedge A$

Definición 2.2.8. Axiomas modales:

- **K**: $\Box(A \to B) \to (\Box A \to \Box B)$.
- **T**: $\Box A \to A$.
- **4**: $\Box A \to \Box\Box A$.
- **B**: $A \to \Box\Diamond A$.
- ***G*** : $\Box(\Box A \to A) \to \Box A$.

Usualmente a **K** se le denomina axioma de distribución.

Proposición 2.1. *El axioma **K** es válido en la clase de todos los marcos.*

Demostración.

Sea $M = \langle W, R, V \rangle$ un modelo, $w \in W$ un mundo y $A, B \in \mathrm{FORM}_{\mathcal{L}_\Box}$ fórmulas válidas en $F = \langle R, V \rangle$. Suponemos $M, w \models \Box(A \to B)$ y $M, w \models \Box A$. Sea $x \in W$ tal que wRx, entonces $M, x \models A \to B$ y $M, x \models A$. Esto es consecuencia de la definición de $M, x \models A \to B$, luego $M, x \models B$. Como x era arbitrario tenemos $M, w \models \Box B$. Al ser M y w arbitrarios, el axioma **K** es válido en F.

$\blacksquare$

Proposición 2.2. *El axioma **T** es válido en la clase de los marcos reflexivos.*

Demostración.

Sea $M = \langle W, R, V\rangle$ un modelo reflexivo basado en un marco reflexivo $F = \langle W, R\rangle$ y sea $w \in W$, como F es reflexivo, wRw. Supongamos que $M, w \vDash \Box A$, entonces $M, w \vDash A$, tenemos así que $\Box A \to A$ es válido en todo marco reflexivo F al ser M y w arbitrarios.

■

Proposición 2.3. *El axioma **4** es válido en la clase de los marcos transitivos.*

Demostración.

Sea $M = \langle W, R, V\rangle$ un modelo basado en un marco $F = \langle W, R\rangle$ transitivo, y $w \in W$. Supongamos que $M, w \vDash \Box A$ y sea $x \in W$ tal que wRx. Como $M, w \vDash \Box A$ si y solo si $\forall v \in M(wRv)[M, v \vDash A]$; tenemos que $\forall y \in M.\ xRy,\ M, y \vDash A$ ya que F es transitivo, y entonces $M, x \vDash \Box A$ y como x era arbitrario, $M, w \vDash \Box\Box A$. Por lo tanto, al ser M y w arbitrarios, el axioma **4** es válido en F.

■

Proposición 2.4. *El axioma **B** es válido en la clase de los marcos simétricos.*

Demostración.

Sea $M = \langle W, R, V\rangle$ un modelo basado en un marco $F = \langle W, R\rangle$ simétrico, y $w \in W$. Suponemos $M, w \vDash A$, y sea $x \in W$ un mundo tal que wRx, esto implica que xRw ya que el marco es simétrico y por lo tanto tenemos $M, x \vDash \Diamond A$. Como el x es arbitrario, entonces $\forall x \in W.wRx$, $M, x \vDash \Diamond A$, obteniendo así $M, w \vDash \Box\Diamond A$. Como w y M son arbitrarios, tenemos que $A \to \Box\Diamond A$. es válido en F.

■

2.3 Sistema axiomático

El sistema de demostración al que nos vamos a restringir para el estudio que llevaremos a cabo sobre la lógica modal proposicional será un sistema axiomático deductivo. Nuestros axiomas básicos van a ser:

1. Todas los axiomas lógicos en $\mathcal{L}_\Box$.

2. Para toda $A, B \in \mathrm{FORM}_{\mathcal{L}_\Box}$ se tiene $\vdash \Box(A \to B) \to (\Box A \to \Box B)$.

Se dirá que $\Box(A \to B) \to (\Box A \to \Box B)$ es una instancia del axioma de distribución.

Además, las reglas de inferencia serán:

1. Modus Ponens.
2. Necesidad: $\dfrac{A}{\Box A}$.

Definición 2.3.1. Sean $A, p, B \in \text{FORM}_{\mathcal{L}_\Box}$, el resultado $A_p(B)$ de sustituir p por B es A se define de la siguiente forma:

1. Si $A = p$ entonces $A_p(B)$ es B.
2. Si A es una variable modal $q \neq p$ entonces $A_p(B)$ es q.
3. Si $A = \bot$ entonces $A_p(B)$ es $\bot$.
4. Si $A = C \to D$ entonces $A_p(B)$ es $(C_p(B) \to D_p(B))$.
5. Si $A = \Box C$ entonces $A_p(B)$ es $\Box C_p(B)$.

Definición 2.3.2. Diremos que un sistema modal es normal si contiene todos los axiomas lógicos, todas las instancias del axioma de distribución y es cerrado bajo modus ponens, necesidad y sustitución.

Sea **L** un sistema modal. Al igual que hicimos con **PA** vamos a definir lo que va a ser una demostración en **L**.

Definición 2.3.3. Una demostración $\mathcal{D}$ en **L** de $A \in \text{FORM}_{\mathcal{L}_\Box}$ es una sucesión finita de fórmulas en $\mathcal{L}_\Box$, $s = \langle s_0, ..., s_n \rangle$, donde $s_n = A$ y para todo $0 \leq i < n$ se cumple que s_i es un axioma lógico, un axioma o una consecuencia de una regla de inferencia aplicada a fórmulas anteriores en D.
Si existe una demostración $\mathcal{D}$ de $A \in \text{FORM}_{\mathcal{L}_\Box}$ se dirá que A es demostrable en **L** o A es un teorema de **L** y lo denotaremos por $\mathbf{L} \vdash A$.

Proposición 2.5. *Las reglas de inferencia de modus ponens y necesidad son correctas, es decir, derivan fórmulas válidas partiendo de fórmulas válidas.*

Demostración.

- *Modus ponens:* Sea $M = \langle W, R, V \rangle$ un modelo, y sean $A, B \in \text{FORM}_{\mathcal{L}_\Box}$ fórmulas tal que A y $A \to B$ son ambas válidas en M. Sea $w \in W$, tenemos $M, w \vDash A \to B$ y $M, w \vDash A$, como $A \to B$ es verdadera en w entonces A es falsa o B es verdadera en w. Dado que A es verdadera B también lo es, luego $M, w \vDash B$.

- *Necesidad*: Sea $M = \langle W, R, V\rangle$ un modelo y $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$ un fórmula válida en M. Sea $w \in W$ un mundo, como A es válida en M entonces, para todo mundo $x \in W$ tal que wRx se tiene que $M, x \vDash A$, y por definición, $M, w \vDash \Box A$.

■

Vamos a definir distintos sistemas de la lógica modal que vamos a estudiar en las siguientes secciones.

Definición 2.3.4.

1. **K** es el sistema modal normal más pequeño que vamos a estudiar. Sus axiomas son todos lo axiomas lógicos y todas las instancias del axioma de distribución (axioma **K**) y es cerrado bajo modus ponens y necesidad.

2. **T** es el sistema modal normal que contiene como axiomas a todas las instancias del axioma **T**.

3. **K4** es el sistema modal normal que contiene como axiomas a todas las instancias del axioma **4**.

4. **B** es el sistema modal normal que contiene como axiomas a todas las instancias de los axiomas **T** y **B**.

5. **S4** es el sistema modal normal que contiene como axiomas a todas las instancias de los axiomas **T** y **4**.

Es fácil ver que los sistemas anteriores son cerrados bajo sustitución (y por lo tanto normales como se afirman).

Lema 2.6. *Dados $A, B \in FORM_{\mathcal{L}_\Box}$, si $\mathbf{L} \vdash A \to B$ entonces $\mathbf{L} \vdash \Box A \to \Box B$.*

Demostración.

(1)	$\mathbf{L} \vdash A \to B$	
(2)	$\mathbf{L} \vdash \Box(A \to B)$	Necesidad; (1)
(3)	$\mathbf{L} \vdash \Box(A \to B) \to (\Box A \to \Box B)$	Axioma de distribución
(4)	$\mathbf{L} \vdash \Box A \to \Box B$	Modus ponens; $(2), (3)$

■

Lema 2.7. *Dados $A, B \in FORM_{\mathcal{L}_\Box}$ si $\mathbf{L} \vdash A \leftrightarrow B$ entonces $\mathbf{L} \vdash \Box A \leftrightarrow \Box B$.*

Demostración.

(1)	$\mathbf{L} \vdash A \leftrightarrow B$	Suposición
(2)	$\mathbf{L} \vdash A \rightarrow B$	Consecuencia lógica; (1)
(3)	$\mathbf{L} \vdash B \rightarrow A$	Consecuencia lógica; (2)
(4)	$\mathbf{L} \vdash \Box A \rightarrow \Box B$	Lema 2.6; (2)
(5)	$\mathbf{L} \vdash \Box B \rightarrow \Box A$	Lema 2.6; (3)
(6)	$\mathbf{L} \vdash \Box A \leftrightarrow \Box B$	Consecuencia lógica; (4), (5)

■

Lema 2.8. *Dados $A, B \in FORM_{\mathcal{L}_\Box}$ se tiene que* $\mathbf{L} \vdash \Box(A \wedge B) \leftrightarrow (\Box A \wedge \Box B)$

Demostración.

(1)	$\mathbf{L} \vdash \Box(A \wedge B)$	Suposición
(2)	$\mathbf{L} \vdash (A \wedge B) \rightarrow A$	Lógicamente válida
(3)	$\mathbf{L} \vdash (A \wedge B) \rightarrow B$	Lógicamente válida
(4)	$\mathbf{L} \vdash \Box(A \wedge B) \rightarrow \Box A$	Lema 2.6; (1)
(5)	$\mathbf{L} \vdash \Box(A \wedge B) \rightarrow \Box B$	Lema 2.6; (2)
(6)	$\mathbf{L} \vdash \Box(A \wedge B) \rightarrow (\Box A \wedge \Box B)$	
(7)	$\mathbf{L} \vdash A \rightarrow (B \rightarrow (A \wedge B))$	Lógicamente válida
(8)	$\mathbf{L} \vdash \Box A \rightarrow \Box(B \rightarrow (A \wedge B))$	Lema 2.6; (5)
(9)	$\mathbf{L} \vdash \Box(B \rightarrow (A \wedge B)) \rightarrow (\Box B \rightarrow \Box(A \wedge B))$	Axioma de distribución
(10)	$\mathbf{L} \vdash p \wedge q \rightarrow p$	Tautología
(11)	$\Box A \wedge \Box B \rightarrow \Box A$	Sustitución; (10)
(12)	$\mathbf{L} \vdash \Box A \wedge \Box B \rightarrow (\Box B \rightarrow \Box(A \wedge B)$	Consecuencia lógica; (8), (11)
(13)	$\Box A \wedge \Box B \rightarrow \Box B$	Análogo (11)
(14)	$\mathbf{L} \vdash \Box A \wedge \Box B \rightarrow \Box(A \wedge B)$	Consecuencia lógica (12), (13)

■

Lema 2.9. *Dados* $A_0, \ldots, A_n \in FORM_{\mathcal{L}_\Box}$, $\mathbf{L} \vdash \Box(A_0 \wedge \cdots \wedge A_n) \leftrightarrow (\Box A_0 \wedge \cdots \wedge \Box A_n)$

Demostración.

El resultado se demuestra por inducción usando los lemas 2.6, 2.7 y 2.8. Para una demostración detallada ver [Boo95] página 6.

■

Teorema 2.10. *Para cualquier fórmula* $A \in FORM_{\mathcal{L}_\Box}$

1. *Si* $\mathbf{K} \vdash A$ *entonces* A *es válida en todos los marcos.*
2. *Si* $\mathbf{T} \vdash A$ *entonces* A *es válida en todos los marcos reflexivos.*
3. *Si* $\mathbf{K4} \vdash A$ *entonces* A *es válida en todos los marcos transitivos.*
4. *Si* $\mathbf{B} \vdash A$ *entonces* A *es válida en todos los marcos simétricos.*
5. *Si* $\mathbf{S4} \vdash A$ *entonces* A *es válida en todos los marcos reflexivos y transitivos.*

Demostración.

Haremos la demostración de 5, las demás son equivalentes.
Sea $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$ con $\mathbf{S4} \vdash A$, sea $F = \langle W, R \rangle$ un marco reflexivo y transitivo, y se $M = \langle W, R, V \rangle$ un modelo basado en F. Como **S4** es **K** con todas las instancias de los axiomas **T** y **4**, entonces todos los axiomas de **S4** son válidos en F ya que, los axiomas de **K** son válidos en todos los marcos, y **T** y **4** son válidos en los marcos reflexivos y transitivos respectivamente. Además, por la Proposición 2.5, sabemos que las reglas de inferencia son correctas, luego A es válida en todo marco reflexivo y transitivo.

■

2.4 Completitud de K, K4, T, B, S4

En esta sección estudiaremos los resultados de completitud para los sistemas modales **K**, **K4**, **T**, **B**, **S4** estos resultados los aplicaremos más específicamente en el sistema modal **GL** en la próxima sección.

Definición 2.4.1. Diremos que un marco $F = \langle W, R \rangle$ es apropiado para

1. **K4** si y sólo si F es transitivo.
2. **T** si y sólo si F es reflexivo.
3. **B** si y sólo si F es simétrico y reflexivo.
4. **S4** si y sólo si F es transitivo y reflexivo.

Sea $\mathbf{L}$ un sistema modal de los citados anteriormente, y sea D una fórmula modal que no sea un teorema de $\mathbf{L}$. Queremos probar que existe un modelo $\mathbf{L}$ donde D no es válida.

Definición 2.4.2. Diremos que A es una D-subfórmula si A ó $\neg A$ es una subfórmula de D.

Definición 2.4.3. Diremos que un conjunto finito $X = \{A_0, \ldots, A_n\}$ de D-subfórmulas es $\mathbf{L}$-consistente si y sólo si no ocurre $\mathbf{L} \vdash \wedge X \to \bot$, donde $\wedge X$ es $A_0 \wedge \cdots \wedge A_n$.

Definición 2.4.4. Un conjunto X de D-subfórmulas se dirá $\mathbf{L}$-consistente maximal si X es $\mathbf{L}$-consistente y, para cada A subfórmula de D, se cumple que $A \in X$ ó $\neg A \in X$.

Proposición 2.11. *Dados A, B subfórmulas de D, X un conjunto $\mathbf{L}$-consistente maximal y $A_0, \ldots, A_n \in X$, se cumple lo siguiente:*

1. *$A \in X$ si y sólo si $(\neg A) \notin X$.*

2. *$\mathbf{L} \vdash A_0 \wedge \cdots \wedge A_n \to B$ entonces $B \in X$.*

Demostración.

1. Tenemos que $\mathbf{L} \vdash \neg(A \wedge \neg A)$, si ambas A y $\neg A$ estuvieran en X entonces $\mathbf{L} \vdash \wedge X \to \bot$.

2. Si B no estuviera en X entonces por 1. se tendría que $\neg B \in X$ por lo tanto $\mathbf{L} \vdash (A_0 \wedge \cdots \wedge A_n \wedge \neg B) \to \bot$ y entonces $\mathbf{L} \vdash \wedge X \to \bot$.

■

A partir de ahora trabajaremos en el modelo $M_{\mathbf{L}} = \langle W_{\mathbf{L}}, R_{\mathbf{L}}, V_{\mathbf{L}} \rangle$ con $W_{\mathbf{L}}$ el conjunto de conjuntos $\mathbf{L}$-consistente maximales, es decir, todo mundo $w \in W_{\mathbf{L}}$ será un conjunto $\mathbf{L}$-consistente maximal. $V_{\mathbf{L}}$ se define como $wV_{\mathbf{L}}p$ si y sólo si $p \in w$ y p ocurre en D. Ahora definimos la relación $R_{\mathbf{L}}$ que debe satisfacer las dos condiciones siguientes:

C1. Para toda subfórmula $\Box A$ de D y todo mundo $w \in W$ se cumple que

$$\Box A \in w \text{ si y sólo si para todo } x \text{ tal que } wRx \text{ se cumple } A \in x.$$

C2. $\langle W, R \rangle$ es apropiado para $\mathbf{L}$.

Proposición 2.12. *Sea $M_{\mathbf{L}} = \langle W_{\mathbf{L}}, R_{\mathbf{L}}, V_{\mathbf{L}} \rangle$ con $W_{\mathbf{L}}$, entonces para toda subfórmula A de D y todo mundo $w \in W$ se cumple que:*

$$A \in w \textit{ si y sólo si } M_{\mathbf{L}}, w \models A$$

Demostración.

Por inducción en la longitud de A:
Si $A \equiv \perp$ entonces $A \notin w$, ya que si $A \in w$ entonces $\mathbf{L} \vdash \neg\perp$ y w no sería $\mathbf{L}$-consistente, por lo tanto $A \notin w$ y w es $\mathbf{L}$-consistente.
Si A es la variable modal p entonces $p \in w$ si y sólo si wVp, si y sólo si $M, w \vDash p$.
Si A es de la forma $B \to C$ con B y C cumpliendo la proposición, como se cumple que $\mathbf{L} \vdash \neg A \to B$, $\mathbf{L} \vdash \neg A \to \neg C$ y $\mathbf{L} \vdash B \to (\neg C \to \neg A)$ entonces $A \notin w$ sii $\neg A \in w$ por consistencia maximal, si y sólo si $B \in w$ y $\neg C \in w$, si y sólo si $B \in w$ y $C \notin w$ de nuevo por consistencia maximal. Por hipótesis de inducción $w \vDash B$ y $w \nvDash C$ si y sólo si $w \nvDash A$, obteniendo así el resultado $A \in w$ si y sólo si $w \vDash A$.
Ahora sea A de la forma $\Box B$ con B cumpliendo la proposición, $A \in w$ si y sólo si por la propiedad $C1$ para todo x con $wR_{\mathbf{L}}x$ se tiene que $B \in x$, pero por la hipótesis de inducción $B \in w$ si y sólo si $M_{\mathbf{L}}, w \vDash B$. De esta forma $A \in w$ si y sólo si para todo mundo x tal que $wR_{\mathbf{L}}$ se cumple $M_{\mathbf{L}}, x \vDash B$ si y sólo si $M_{\mathbf{L}}, w \vDash \Box B$.

■

A continuación describiremos como definir la relación $R_{\mathbf{L}}$ en cada sistema, para no sobrecargar la notación llamaremos R y W a $R_{\mathbf{L}}$ y $W_{\mathbf{L}}$, la relación y conjunto de mundos de cada sistema respectivamente, pero tenemos que tener cuidado porque R y W dependerán del sistema donde trabajemos.

K. Dados $w, x \in W$ se tiene wRx si y sólo si para todo $\Box A \in w$ se cumple que $A \in x$. De esta forma $F = \langle W, R \rangle$ es apropiado para **K** y la condición $C2$ se cumple. Veamos que $C1$ se cumple, una implicación es inmediata ya que si $\Box A \in w$ y wRx se tiene que $A \in x$.
Para la otra, supongamos que $\Box A \notin w$ y veamos que existe un x con wRx tal que $A \notin x$:
Sea $X = \{\neg A\} \cup \{B : \Box B \in w\}$ y supongamos que no es **K**-consistente, entonces

$$\mathbf{K} \vdash \neg(\neg A \land B_0 \land \cdots \land B_n)$$

con $\Box B_0, \ldots, \Box B_n \in w$, pero por consecuencia lógica se tiene que

$$\mathbf{K} \vdash B_0 \land \cdots \land B_n \to A$$

por los lemas 2.6 y 2.9 se tiene

$$\mathbf{K} \vdash \Box B_0 \land \cdots \land \Box B_n \to \Box A$$

y por la Proposición 2.11 se obtiene $\Box A \in w$. Luego como $\Box A \notin w$ entonces X es **K**-consistente y X se puede extender a un conjunto consistente maximal $X \subseteq x$. Además $\neg A \in X$, $A \notin x$, y dado $\Box B \in w$ entonces $B \in X \subseteq x$, finalmente por definición de R tenemos que wRx.

K4. Se cumple wRx si y sólo si para todo $\Box A \in w$ tanto $\Box A$ como A están en x. Evidentemente $C2$ se cumple al ser R transitiva y veamos que se cumple $C1$.

Si $\Box A \in w$ y wRx entonces $A \in w$.
Para la otra inclusión: sea $X = \{\neg A\} \cup \{B, \Box B : \Box B \in w\}$ y $\Box A \notin w$. Si X es **K4**-inconsistente, entonces:

(1)	$\mathbf{K4} \vdash \neg(\neg A \wedge B_0 \wedge \cdots \wedge B_n \wedge \Box B_0 \wedge \cdots \wedge \Box B_n)$	
(2)	$\mathbf{K4} \vdash (B_0 \wedge \cdots \wedge B_n \wedge \Box B_0 \wedge \cdots \wedge \Box B_n) \to A$	Consecuencia lógica; (1)
(3)	$\mathbf{K4} \vdash \Box(B_0 \wedge \cdots \wedge B_n \wedge \Box B_0 \wedge \cdots \wedge \Box B_n) \to \Box A$	Lema 2.6; (2)
(4)	$\mathbf{K4} \vdash \Box B_0 \wedge \cdots \wedge \Box B_n \wedge \Box\Box B_0 \wedge \cdots \wedge \Box\Box B_n \to$ $\to \Box A$	Lema 2.9; (3)
(5)	$\mathbf{K4} \vdash \Box B \to \Box\Box B$	Axioma **4**
(6)	$\mathbf{K4} \vdash \Box B_0 \wedge \cdots \wedge \Box B_n \to \Box A$	Consecuencia lógica; (4), (5)

Como $\Box B_0, \ldots, \Box B_n$ están en w, por la Proposición 2.11 se cumple que $\Box A \in w$, ya que $\Box A \notin w$ se tiene que X es **K4**-consistente y está contenido en un conjunto consistente maximal $X \subseteq x$. Debido a que $\neg A \in X$ entonces $A \notin x$ y si $\Box B \in w$ entonces $\Box B, B \in x$ y wRx.

La forma de demostrar que se cumple $C1$ es muy similar para todos los sistemas modales, por lo tanto para los que nombremos a continuación no vamos a demostrarlo. Para el argumento completo ver [Boo95] páginas 81, 82.

T. Siendo R igual que para **K**, como $\mathbf{T} \vdash \Box A \to A$ entonces si $\Box A \in w$ se cumple $A \in w$ lo que hace que F sea reflexivo y se cumple la propiedad $C2$.

S4. R es el mismo que para **K4**, que ya vimos que R era transitivo, sabemos que $\mathbf{S4} \vdash \Box A \to A$ entonces al igual que con **T**, R es reflexivo.

B. Sea wRx si y sólo si para todo $\Box A \in w$ se tiene $A \in x$ y para todo $\Box B \in x$ se cumple $B \in w$. De esta forma R es simétrica y como $\mathbf{B} \vdash \Box A \to A$ entonces R es también reflexiva y F es apropiado.

Por lo tanto, si **L** es uno de los sistemas anteriores, se tiene el sguiente teorema.

Teorema 2.13. *Sea $A \in FORM_{\mathcal{L}_\Box}$ entonces:*

$$\mathbf{L} \vdash A \text{ si y sólo si } A \text{ es válida en todo modelo finito de } \mathbf{L}$$

Además, la naturaleza de la demostración nos permite probar que **L** es decidible (ver [Boo95] página 83).

2.5 El sistema GL.

Una vez estudiados sistemas modales anteriores, pasaremos a estudiar en profundidad a **GL**, que es el sistema en el que habitualmente se trabaja en lógica de la demostrabilidad.

Definición 2.5.1. Definimos **GL** como el sistema modal normal que contiene como axiomas a todas las instancias del axioma **G**.

Teorema 2.14. *Para toda* $p \in VAR_{\mathcal{L}_\Box}$ *se tiene que* $\mathbf{GL} \nvdash \Box p \to p$.

Demostración.

Por reducción al absurdo, para toda $p \in \mathrm{FORM}_{\mathcal{L}_\Box}$ tenemos que $\mathbf{GL} \vdash \Box p \to p$, por sustitución $\mathbf{GL} \vdash \Box\bot \to \bot$:

(1)	$\mathbf{GL} \vdash \Box\bot \to \bot$	
(2)	$\mathbf{GL} \vdash \Box(\Box\bot \to \bot)$	Necesidad; (1)
(3)	$\mathbf{GL} \vdash \Box(\Box\bot \to \bot) \to \Box\bot$	Axioma **G**
(4)	$\mathbf{GL} \vdash \Box\bot$	Modus Ponens; $(2), (3)$
(5)	$\mathbf{GL} \vdash \bot$	Modus Ponens; $(1), (4)$

■

Teorema 2.15. *Para toda* $A \in FORM_{\mathcal{L}_\Box}$ *se cumple* $\mathbf{GL} \vdash \Box A \to \Box\Box A$.

Demostración.

(1)	$\mathbf{GL} \vdash A \to ((\Box\Box A \wedge \Box A) \to (\Box A \wedge A))$	Lógicamente válida
(2)	$\mathbf{GL} \vdash A \to (\Box(\Box A \wedge A) \to (\Box A \wedge A))$	Lema 2.8
(3)	$\mathbf{GL} \vdash \Box A \to \Box(\Box(\Box A \wedge A) \to (\Box A \wedge A))$	Lema 2.6
(4)	$\mathbf{GL} \vdash \Box(\Box(\Box A \wedge A) \to (\Box A \wedge A)) \to$ $\to \Box(\Box A \wedge A)$	Axioma **G**
(5)	$\mathbf{GL} \vdash \Box A \to \Box(\Box A \wedge A)$	Consecuencia lógica; $(3), (4)$
(6)	$\mathbf{GL} \vdash \Box(\Box A \wedge A) \to \Box\Box A$	Lema 2.8
(7)	$\mathbf{GL} \vdash \Box A \to \Box\Box$	Consecuencia lógica $(5), (6)$

■

Gracias al Teorema 2.15 obtenemos de forma inmediata el siguiente resultado.

Corolario 9. $\mathbf{K4} \subseteq \mathbf{GL}$.

Proposición 2.16. *Dada* $A \in FORM_{\mathcal{L}_\Box}$ *se tiene*

$$\mathbf{GL} \vdash \Box(\Box A \to A) \leftrightarrow \Box A \leftrightarrow \Box(\Box A \wedge A)$$

Demostración.

(1)	$\mathbf{GL} \vdash \Box(\Box A \to A) \to \Box A$	Axioma **G**
(2)	$\mathbf{GL} \vdash A \to (\Box A \to A)$	Lógicamente válida
(3)	$\mathbf{GL} \vdash \Box A \to \Box(\Box A \to A)$	Lema 2.6
(4)	$\mathbf{GL} \vdash \Box(\Box A \to A) \leftrightarrow \Box A$	Consecuencia lógica (1), (3)
(5)	$\mathbf{GL} \vdash \Box A \to \Box\Box A$	Teorema 2.15
(6)	$\mathbf{GL} \vdash \Box(\Box A \wedge A) \leftrightarrow \Box\Box A \wedge \Box A$	Lema 2.8
(7)	$\mathbf{GL} \vdash \Box A \to (\Box\Box A \to (\Box\Box A \wedge \Box A))$	Lógicamente válida
(8)	$\mathbf{GL} \vdash \Box A \to (\Box\Box A \wedge \Box A)$	Consecuencia lógica; (5), (7)
(9)	$\mathbf{GL} \vdash \Box A \to \Box(\Box A \wedge A)$	Consecuencia lógica; (6), (8)
(10)	$\mathbf{GL} \vdash (\Box\Box A \wedge \Box A) \to \Box A$	Lógicamente válida
(11)	$\mathbf{GL} \vdash \Box(\Box A \wedge A) \to \Box A$	Consecuencia lógica; (6), (10)
(12)	$\mathbf{GL} \vdash \Box A \leftrightarrow \Box(\Box A \wedge A)$	Consecuencia lógica; (9), (11)

■

Proposición 2.17. *Dado* $A \in FORM_{\mathcal{L}_\Box}$ *se cumple* $\mathbf{GL} \vdash \Box\bot \leftrightarrow \Box\Diamond A$.

Demostración.

(1)	$(\Rightarrow)$ $\mathbf{GL} \vdash \bot \to \Diamond A$	Lógicamente válida
(2)	$\mathbf{GL} \vdash \Box\bot \to \Box\Diamond A$	Lema 2.6; (1)
(3)	$(\Leftarrow)$ $\mathbf{GL} \vdash \Diamond A \to \Diamond\top$	Lógicamente válida
(4)	$\mathbf{GL} \vdash \Diamond\top \to \neg\Box\neg\top$	Definición de $\Diamond$

(5)	$\mathbf{GL} \vdash \Diamond\top \to \neg\Box\bot$	Consecuencia lógica; (4)
(6)	$\mathbf{GL} \vdash \neg\Box\bot \leftrightarrow (\Box\bot \to \bot)$	$\top$ es $\neg\bot$
(7)	$\mathbf{GL} \vdash \Diamond\top \to (\Box\bot \to \bot)$	Definición de $\Diamond$; (6)
(8)	$\mathbf{GL} \vdash \Diamond A \to (\Box\bot \to \bot)$	Consecuencia lógica; (3), (4)
(9)	$\mathbf{GL} \vdash \Box\Diamond A \to \Box(\Box\bot \to \bot)$	Lema 2.6; (8)
(10)	$\mathbf{GL} \vdash \Box(\Box\bot \to \bot) \to \Box\bot$	Axioma **G**
(11)	$\mathbf{GL} \vdash \Box\Diamond A \to \Box\bot$	Consecuencia lógica; (9), (10)

■

Teorema 2.18. $\mathbf{GL} \vdash \Box(A \leftrightarrow \neg\Box A) \leftrightarrow \Box(A \leftrightarrow \neg\Box\bot)$

Demostración.

La demostración consiste en aplicar los lemas 2.6, 2.7, 2.8, para una demostración detallada ver [Boo95] páginas 13 y 14.

■

Pasemos a demostrar los correspondientes resultados de completitud y corrección para el sistema modal **GL**, para ello empecemos con definir el tipo de marco en el que vamos a trabajar.

Definición 2.5.2.

- Una relación R es bien fundada (R es BF) si en todo conjunto X no vacío, existe al menos un elemento $w \in X$ tal que no existe un $x \in X$ que cumpla xRw, esto significa w no es accesible desde ningún mundo de X.
- Una relación R es inversamente bien fundada (R es IBF) si en todo conjunto X no vacío, existe al menos un elemento $w \in X$ tal que para para todo $x \in X$ no ocurre wRx, esto es w no puede acceder a ningún mundo de X.

Definición 2.5.3. Un marco $F = \langle W, R\rangle$ se dirá bien fundado (resp. inversamente bien fundado) si R es BF (resp. IBF).

Definición 2.5.4. Dados una relación R y un conjunto X de mundos diremos que $x \in X$ es un elemento R-mínimo si no existe otro mundo $y \in X$ que cumpla que yRx

Definición 2.5.5. Dados una relación R y un conjunto X de mundos diremos que $x \in X$ es un elemento R-máximo si no existe otro mundo $y \in X$ que cumpla que xRy

Proposición 2.19. *Si $F = \langle W, R\rangle$ es un marco IBF, entonces F es irreflexivo.*

Demostración.

Suponemos $W = \{w\}$ y F reflexivo, entonces para todo mundo $x \in W$ se tendría que wRx, por lo tanto w podría acceder a todo mundo de W, lo que contradice que F sea IBF.

■

Teorema 2.20 (Inducción en el inverso de R)**.** *Sea P una propiedad de mundos y $F = \langle W, R\rangle$ un marco IBF. Para demostrar que todos los mundos de W tienen la propiedad P, hace falta demostrar que: si para cada $w \in W$ y para cada $x \in W$ tal que wRx se cumple que x tiene la propiedad P, entonces w tiene la propiedad P.*

Demostración.

Supongamos que F es IBF, sea $w \in W$ un mundo para el cual, para todo $x \in W$ con wRx, x cumple la propiedad P. Sea $X = \{w : w \in W \wedge \neg Pw\} \subseteq W$. Supongamos que X es no vacío, esto implica que existe un mundo $y \in X$ para el cual no se cumple P, lo que conlleva a que existe otro mundo $z \in W$ con yRz que tampoco cumple P, luego $z \in X$ por definición de X. Esto muestra todo mundo perteneciente al conjunto X puede acceder a otro mundo de X, contradiciendo así que F sea IBF. Por lo tanto X es vacío y todo mundo $w \in W$ tiene la propiedad P.

■

Teorema 2.21. *Sea $F = \langle W, R\rangle$ un marco finito y transitivo. Entonces F es irreflexivo si y sólo si F es inversamente bien fundado.*

Demostración.

($\Leftarrow$) Por la Proposición 2.19 tenemos que si F es IBF entonces F es irreflexivo.

($\Rightarrow$) Supongamos que F es irreflexivo, por reducción al absurdo supongamos F no es un marco inversamente bien fundado.

Como F no es IBF entonces existe un subconjunto de mundos $X \subseteq W$ tal que $X \neq \emptyset$ y para todo mundo $x \in X$ existe otro mundo $y_x \in X$ tal que xRy_x. Sea $x_0, ..., x_n$ una sucesión de elementos de W tal que $x_0Rx_1R...Rx_n$. Si para $0 \leq i < j \leq n$ ocurriera que $x_i = x_j$ entonces por transitividad de F tendríamos que x_iRx_i, cosa que contradice la suposición de que F es irreflexivo, por lo tanto, para cada cadena $x_0Rx_1R...Rx_n$ de W sabemos que si $0 \leq i < j \leq n$ se va a cumplir que $x_i \neq x_j$.

Ahora, por inducción en n veremos que podemos construir una sucesión de accesibilidad entre mundos todos distintos entre ellos: Sea $X \neq \emptyset$ con $x_0 \in X$, entonces, por F no ser IBF, existe un $x_1 \in X$ tal que x_0Rx_1 y $x_0 \neq x_1$. Supongamos que existe una cadena de longitud $n = k$, $x_0R...Rx_k$ con cada x_i en X todos distintos. Puesto que $x_k \in X$por definición de $x_{k+1} \in X$ tal que x_kRx_{k+1} existe dicho $x_{k+1} \in X$ cumpliendo $x_0R...Rx_kRx_{k+1}$ y así tenemos una cadena de longitud $n = k + 1$ de mundos de X. Como esto lo podemos hacer para todo $n \in \mathbb{N}$, entonces W es infinito, que contradice la premisa que F es finito. ■

Hemos estudiado varias propiedades de los marcos inversamente bien fundados, esto se debe al siguiente resultado.

Teorema 2.22. *Sea $p \in VAR_{\mathcal{L}_\Box}$ se cumple que $\Box(\Box p \to p) \to \Box p$ es válida en el marco $F = \langle W, R\rangle$ si y sólo si R es transitiva e inversamente bien fundada.*

Demostración.

$\Rightarrow$) Supongamos que $\Box(\Box p \to p) \to \Box p$ es válida en F entonces todas las fórmulas $\Box(\Box B \to B) \to \Box B$ son válidas en F y por lo tanto todos los teoremas son válidos en F, pues los teoremas de **K** son válidos en todo marco. Además como $\mathbf{GL} \vdash \Box A \to \Box\Box A$, por la Proposición 2.3 se tiene que F es transitivo.
Para ver que R es inversamente bien fundado, sea X un conjunto de mundos no vacío que no tenga un elemento R-máximo. Sea $w \in X$ y sea V una evaluación en W tal que para todo mundo $a \in W$ se cumpla que aVp si y sólo si $a \notin X$. Veamos que para $M = \langle W, R, V\rangle$ se tiene que $M, w \vDash \Box(\Box p \to p)$ y $M, w \nvDash \Box p$: Sea $x \in X$ con wRx cumpliendo $M, x \nvDash p$, esto es $\neg(xVp)$, como X no tiene un elemento R-máximo, entonces existe un $y \in X$ con xRy y además $M, y \nvDash p$ por lo tanto $M, x \nvDash \Box p$. Esto conlleva que $M, x \vDash \Box p \to p$ y finalmente $M, w \vDash \Box(\Box p \to p)$, contradiciendo la validez de $\Box(\Box A \to A) \to \Box A$.

$\Leftarrow$) Supongamos que F es transitivo e inversamente bien fundado y que para $M = \langle W, R, V\rangle$ se tenga que $M, w \nvDash \Box p$. Sea $X = \{x \in W : wRx \wedge x \nvDash p\}$. Como $M, w \nvDash \Box p$ entonces existe un $y \in W$ tal que $M, y \nvDash p$ y por lo tanto $y \in X$ y X es no vacío. Además, por ser F inversamente bien fundado, se tiene que existe un $z \in X$ tal que no se cumple zRx para todo $x \in X$. Debido a que $z \in X$, por definición, wRz y $M, z \nvDash p$. Si existiera un mundo $v \in W$ cumpliendo zRv implicaría que $v \notin X$, pero como por transitividad wRv, esto conlleva a que $M, v \vDash p$, así $M, z \vDash \Box p$ y $M, z \nvDash \Box p \to p$, y además $M, w \nvDash \Box(\Box p \to p)$, llegando finalmente a la conclusión de que $\Box(\Box p \to p) \to \Box p$ es válido en F.

■

Esto conlleva que los marcos transitivos e inversamente bien fundados sean los apropiados para **GL** y en los que vamos a trabajar a partir de ahora.

Teorema 2.23 (Completitud para GL). *Para toda fórmula $A \in FORM_{\mathcal{L}_\Box}$, si A es* **GL***-válida entonces* $\mathbf{GL} \vdash A$.

Para la demostración de este teorema, desarrollaremos toda una importante batería de resultados que presentamos a continuación.

Teorema 2.24 (Corrección de GL). *Para cualquier $A \in FORM_{\mathcal{L}_\Box}$, si* $\mathbf{GL} \vdash A$ *entonces A es válida en todos los marcos que son transitivos e inversamente bien fundados.*

Demostración.

Supongamos que $A \in \text{FORM}_{\mathcal{L}_\Box}$ y $\mathbf{GL} \vdash A$. Sea $M = \langle W, R, V\rangle$ un modelo basado en $F = \langle W, R\rangle$ un marco transitivo e inversamente bien fundado. **GL** es **K** con todas las instancias del axioma $\boldsymbol{G}$ y por el Teorema 2.10 sabemos todo teorema de **K** es válido en F.
Nos queda demostrar entonces, que el axioma $\boldsymbol{G}$ es válido en M, y para ello vamos a demostrar que $\neg\Box B \to \neg\Box(\Box B \to B)$ es válido en M.

Sea $w \in W$ un mundo con $M, w \vDash \neg\Box B$, es decir, $M, w \nvDash \Box B$, esto implica que existe al menos un mundo $x \in W$ tal que wRx y además $M, x \nvDash B$.
Sea $X = \{v \in W : wRv \wedge M, v \nvDash B\}$, X es no vacío pues $x \in X$.

Como F es IBF y X es un subconjunto no vacío de W, existe un mundo $y \in X$ tal que para todo $z \in X$ se cumple $\neg(yRz)$. Luego, para todo $a \in W$ con yRa se tiene wRa y $a \notin X$, lo que conlleva a $M, a \vDash B$ y $M, y \vDash \Box B$ por definición de $\vDash$.

Como $M, y \vDash \Box B$ y $M, y \nvDash B$, tenemos que $M, y \nvDash \Box B \to B$, $y \in X$ era un mundo arbitrario tal que wRy, entonces $M, w \nvDash \Box(\Box B \to B)$, o lo que es lo mismo $M, w \vDash \neg\Box(\Box B \to B)$ y así $M, w \vDash \neg\Box B \to \neg\Box(\Box B \to B)$.

Como $w \in W$ era arbitrario, tenemos que $\neg\Box B \to \neg\Box(\Box B \to B)$ es válido en M, y como este a su vez era un modelo arbitrario de F, entonces $\neg\Box B \to \neg\Box(\Box B \to B)$ es válido en todo marco transitivo e inversamente bien fundado.

■

Corolario 10. *Para toda $A \in FORM_{\mathcal{L}_\Box}$, si $\mathbf{GL} \vdash A$, entonces A es válida en todo marco finito, transitivo e irreflexivo.*

Proposición 2.25. *Existe una fórmula $A \in FORM_{\mathcal{L}_\Box}$ tal que $\mathbf{GL} \nvdash A$.*

Demostración.

Si $\mathbf{GL} \vdash (p \wedge \neg p)$ entonces $\mathbf{GL} \vdash \bot$, que contradice la corrección de **GL**.

■

Sea $G \in \text{FORM}_{\mathcal{L}_\Box}$ tal que $\mathbf{GL} \nvdash G$. Nos basaremos en esta G para definir y demostrar varios resultados importantes.

Definición 2.5.6. Sea $A \in \text{FORM}_{\mathcal{L}_\Box}$, diremos que A es una G-fórmula si A o $\neg A$ es una subfórmula de G.

Si A es una G-fórmula, también lo es $\neg A$.

Definición 2.5.7. Sea $X = \{A_0, \ldots, A_n\} \subseteq \text{FORM}_{\mathcal{L}_\Box}$ un subconjunto de fórmulas. Diremos que X es un conjunto de fórmulas **GL**-consistente, si $\mathbf{GL} \nvdash \neg(A_0 \wedge \cdots \wedge A_n)$.

Debido a que las G-fórmulas son subfórmulas de G y hay un número finito de subfórmulas de G, las podemos numerar $G_0, \ldots, G_n$. Por lo tanto, definimos el conjunto de G-fórmulas $\mathsf{GFORMS} := \{G_0, \neg G_0, \ldots, G_n, \neg G_n\}$.

Definición 2.5.8. Un conjunto X de G-fórmulas se dirá **GL**-consistente maximal, si X es **GL**-consistente y para toda $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$ subfórmula de G, A o $\neg A$ están en X.

Proposición 2.26. *Sea $A, B_0, \ldots, B_k, C \in FORM_{\mathcal{L}_\Box}$, X un conjunto* **GL**$-$*consistente maximal, se cumple lo siguiente:*

1. *Si A es una subfórmula de G, entonces $A \in X \leftrightarrow \neg A \notin X$.*

2. *Si $B_0, \ldots, B_k \in X$, C es una subfórmula de G, y* $\mathbf{GL} \vdash (B_0 \wedge \cdots \wedge B_k) \to C$*, entonces $C \in X$*

Demostración.

Es similar a la Proposición 2.11.

■

Proposición 2.27. *Todo conjunto* **GL**-*consistente está contenido en un conjunto* **GL**-*consistente maximal.*

Demostración.

Inmediata, ya que todo conjunto **GL**-consistente es finito.

■

Lema 2.28. $\{\neg G\}$ *es* **GL**$-$*consistente.*

Demostración.

Si no lo fuera, entonces $\mathbf{GL} \vdash \neg\neg G$ y por lo tanto$\mathbf{GL} \vdash G$. Que contradice que la elección de G.

■

Supongamos $X_{\neg G}$ es un conjunto **GL**$-$consistente maximal tal que $\{\neg G\} \subseteq X_{\neg G}$, y sea $W_G := \{X \subseteq \mathsf{GFORMS} : X \text{ es } \mathbf{GL}\text{-consistente maximal}\}$.
Se tiene que $X_{\neg G} \in W_G$. Como G tiene un número finito k de subfórmulas, entonces, a lo más habrá 2^k conjuntos **GL**$-$consistentes maximales (debido a que una subfórmula y su negación no pueden estar en el mismo conjunto consistente maximal), y por lo tanto W_G es un conjunto finito.

Nuestro objetivo ha sido buscar herramientas que nos permita demostrar que la fórmula G no es válida, nos queda definir el modelo donde nos vamos a basar.

Sea $M_G = \langle W_G, R_G, V_G \rangle$, con wV_Gp si y sólo si $p \in w$ y p ocurre en G. Ahora definimos:
wR_Gx si y sólo si para todo $\Box A$ en w se tiene que $\Box A$ y A están en x, y para algún $\Box B$ en x se cumple que $\neg\Box B$ está en w.

Tenemos que:

1. R_G es transitiva, pues si wR_Gx, xR_Gz y $\Box A$ está en w entonces $\Box A$ está en x y $\Box A, A$ están en z. Además si $\Box B$ está en x y $\neg\Box B$ en w entonces $\Box B$ está en z y así wR_Gz.

2. R es irreflexiva, ya que si wR_Gw entonces para algún A tanto $\Box A$ como $\neg\Box A$ estarían en w.

Debido a esto, el marco $\langle W_G, R_G\rangle$ es transitivo e inversamente bien fundado, al ser W_G finito, por lo tanto $\langle W_G, R_G\rangle$ es un marco apropiado para **GL**.

Veamos que se cumple $C1$:

Proposición 2.29. *Para toda fórmula $\Box A \in$ GFORMS y para todo mundo $w \in W_G$ tenemos:*

$$\Box A \in w \textit{ si y sólo si para todo } v \in W_G \textit{ tal que } wR_Gv \textit{ se cumple } A \in v.$$

Demostración.

$\Rightarrow$) Por definición de R_G.

$\Leftarrow$) Lo demostraremos por contraposición. Supongamos que $\Box A \notin w$, tenemos que probar que existe un mundo $v \in W_G$ tal que wR_Gv y además $A \notin v$.
Sea $X = \{\neg A, \Box A\} \cup \{B, \Box B : \Box B \in w\}$.
Supongamos que X es **GL**-inconsistente:

(1)	$\mathbf{GL} \vdash \neg(\neg A \wedge \Box A \wedge B_0 \wedge \Box B_0, \wedge \cdots \wedge B_n \wedge \Box B_n)$	
(2)	$\mathbf{GL} \vdash (B_0 \wedge \Box B_0 \wedge \cdots \wedge B_n \wedge \Box B_n) \to (\Box A \to A)$	Consecuencia lógica; (1)
(3)	$\mathbf{GL} \vdash \Box(B_0 \wedge \Box B_0 \wedge \cdots \wedge B_n \wedge \Box B_n) \to \Box(\Box A \to A)$	Lema 2.6; (2)
(4)	$\mathbf{GL} \vdash (\Box B_0 \wedge \Box\Box B_0 \wedge \cdots \wedge \Box B_n \wedge \Box\Box B_n) \to$ $\to \Box(\Box A \to A)$	Lema 2.9; (3)
(5)	$\mathbf{GL} \vdash \Box(\Box A \to A) \to \Box A$	Axioma **G**
(6)	$\mathbf{GL} \vdash \Box B \to \Box\Box B$	Teorema 2.15
(7)	$\mathbf{GL} \vdash \Box B_0 \wedge \cdots \wedge \Box B_n \to \Box A$	Consecuencia lógica; $(4), (5), (6)$

Como $\Box B_0, \ldots, \Box B_n \in w$ entonces por la Proposición 2.26 se tiene $\Box A \in w$, lo cual contradice la suposición y X es **GL**-consistente.

Por la Proposición 2.27 sabemos que X está contenido en un conjunto $X \subseteq v_0$ **GL**-consistente maximal.

Vamos a ver que de hecho, $v_0 \in W_G$ es el mundo que buscamos.

Queremos ver que wRv_0, la primera condición es que para todo $\Box C \in w$ se cumpla que $C, \Box C \in v_0$, que ocurre debido a $X \subseteq v_0$. Para la segunda condición, $\Box A \in v_0$ y $\Box A \notin w$ por suposición, y por Proposición 2.27 tenemos que $\neg\Box A \in w$, por lo que tenemos que $wR_G v_0$.

Finalmente, ya que $\neg A \in X \subseteq v_0$, tenemos que $A \notin v_0$ y v_0 es el mundo de W_G que cumple lo que buscamos.

■

Teorema 2.30. *Para toda $A \in$ GFORMS y para todo mundo $w \in W_G$ tenemos:*

$$M_G, w \vDash_G A \Leftrightarrow A \in w$$

Demostración.

Lo demostraremos por inducción en la complejidad de A:

Sea $A = \bot$, como $\mathbf{GL} \vdash \neg\bot$, tenemos que $\bot \notin w$ y además $M_G, w \nvDash \bot$.

Si $A = p$ una variable proposicional que ocurre en G, por definición $M_G, w \vDash_G p$ si y sólo si $wV_G p$ si y sólo si $p \in w$.

Supongamos que $A = (B \to C)$ con B y C cumpliendo el teorema:

(1)	$M, w \vDash (B \to C)$	Suposición
(2)	$M, w \nvDash B$ o $M, w \vDash C$	Definición 2.26
(3)	$B \notin w$ o $C \in w$	Hipótesis de inducción
(4)	$B \to C \in w$	Consecuencia lógica; (4)
(5)	$A \in w$	Definición de A

Si $A = \neg B$ con B cumpliendo el teorema

(1)	$M, w \vDash \neg B$	Suposición
(2)	$M, w \nvDash B$	Definición
(3)	$B \notin w$	Hipótesis de inducción
(4)	$\neg B \in w$	Proposición 2.26
(5)	$A \in w$	Definición de A

Si $A = \Box B$ con B cumpliendo el teorema

(1)	$M, w \vDash \Box B$	
(2)	Para todo x con wRx se tiene: $M, x \vDash B$	Definición
(3)	$B \in x$	Hipótesis de inducción

(4) $\Box B \in w$ Proposición 2.29

(5) $A \in w$ Definición de A

■

Finalmente, recordemos que $X_G \in W_G$ era un conjunto **GL**-consistente maximal de subfórmulas de G tal que $\neg G \in X_G$. Por el teorema que acabamos de demostrar $M_G, X_G \not\models G$, por lo tanto G no es válida en todo modelo transitivo, finito e inversamente bien fundado como M_G, i.e., G no es **GL**-válida, obteniendo así la demostración del teorema de completitud para **GL**.

Capítulo 3

La caja como Prov

Definición 3.0.1. Una realización es una función * : $\mathrm{VAR}_{\mathcal{L}_\Box} \to \mathrm{SENT}_{\mathcal{L}_\mathrm{A}}$. Dada p variable modal, $A, B \in \mathrm{FORM}_{\mathcal{L}_\Box}$, definimos la extensión de * a $\mathrm{FORM}_{\mathcal{L}_\Box}$ de la siguiente forma:

1. $\bot^* = \bot$.
2. $p^* = {}^*(p)$.
3. $(A \to B)^* = (A^* \to B^*)$
4. $(\neg A)^* = \neg(A)^*$.
5. $(\Box A)^* = Prov(\ulcorner A^* \urcorner)$

Llamaremos a A^* la traducción de la fórmula modal A bajo la realización *.

Definición 3.0.2. Sea $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$, si para toda realización * se cumple que $\mathbf{PA} \vdash A^*$, diremos que A es **siempre demostrable**.

Teorema 3.1. *Si* $\mathbf{K4} \vdash A$ *entonces para toda realización* **,* $\mathbf{PA} \vdash A^*$.

Demostración.

Si A es una composición tautológica de fórmulas modales en **K4**, entonces se cumple que A^* es la misma composición tautológica de fórmulas aritméticas en **PA** y por lo tanto $\mathbf{PA} \vdash A^*$.

Axioma de Distribución: Dadas A, B fórmulas modales, por P2 se tiene que $\mathbf{PA} \vdash Prov(\ulcorner A^* \to B^* \urcorner) \to (Prov(\ulcorner A^* \urcorner) \to Prov(\ulcorner B^* \urcorner))$ y por lo tanto $\mathbf{PA} \vdash (\Box(A \to B) \to (\Box A \to \Box B))^*$ por definición de *, esto implica que la traducción de los axiomas de distribución bajo * para cualquier par de fórmulas modales son teoremas de **PA**.

Axioma **4**. Para toda realización * y toda fórmula modal A se tiene que $\mathbf{PA} \vdash Prov(\ulcorner A^* \urcorner) \to Prov(\ulcorner Prov(\ulcorner A^* \urcorner) \urcorner)$, esto es $\mathbf{PA} \vdash (\Box A \to \Box\Box A)^*$.

Ahora veamos que **PA** es cerrada bajo *modus ponens* y necesidad:

Modus ponens: Si $\mathbf{PA} \vdash (A \to B)^*$ y $\mathbf{PA} \vdash A^*$, se tiene $\mathbf{PA} \vdash (A^* \to B^*)$, y por lo tanto $\mathbf{PA} \vdash B^*$.

Necesidad: Si $\mathbf{PA} \vdash A^*$, por P1 sabemos $\mathbf{PA} \vdash Prov(\ulcorner A^* \urcorner)$ y finalmente $\mathbf{PA} \vdash \Box A^*$.

■

Teorema 3.2 (Teorema de Löb)**.** *Sea* $\varphi \in FORM_{\mathcal{L}_A}$*, si* $\mathbf{PA} \vdash Prov(\ulcorner \varphi \urcorner) \to \varphi$ *entonces* $\mathbf{PA} \vdash \varphi$*.*

Demostración.

Supongamos que para $\varphi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ se tiene que $\mathbf{PA} \vdash Prov(\ulcorner \varphi \urcorner) \to \varphi$, sea $B(y)$ la fórmula $Prov(y) \to \varphi$, por el Lema Diagonal sabemos que existe $\psi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$ tal que $\mathbf{PA} \vdash \psi \leftrightarrow (Prov(\ulcorner \psi \urcorner) \to \varphi)$, por lo tanto:

(1)	$\mathbf{PA} \vdash \psi \leftrightarrow (Prov(\ulcorner \psi \urcorner) \to \varphi)$	
(2)	$\mathbf{PA} \vdash \psi \to (Prov(\ulcorner \psi \urcorner) \to \varphi)$	
(3)	$\mathbf{PA} \vdash Prov(\ulcorner \psi \to (Prov(\ulcorner \psi \urcorner) \to \varphi)\urcorner)$	P1;(2)
(4)	$\mathbf{PA} \vdash Prov(\ulcorner \psi \urcorner) \to Prov(\ulcorner Prov(\ulcorner \varphi \urcorner) \to \varphi \urcorner)$	P2;(3)
(5)	$\mathbf{PA} \vdash Prov(\ulcorner \psi \urcorner) \to$ $\to (Prov(\ulcorner Prov(\ulcorner \psi \urcorner)\urcorner) \to Prov(\ulcorner \varphi \urcorner))$	P2;(4)
(6)	$\mathbf{PA} \vdash (Prov(\ulcorner \psi \urcorner) \to Prov(\ulcorner Prov(\ulcorner \psi \urcorner)\urcorner)) \to$ $\to (Prov(\ulcorner \psi \urcorner) \to Prov(\ulcorner \varphi \urcorner))$	Consecuencia lógica; (5)
(7)	$\mathbf{PA} \vdash Prov(\ulcorner \psi \urcorner) \to Prov(\ulcorner Prov(\ulcorner \psi \urcorner)\urcorner)$	P3
(8)	$\mathbf{PA} \vdash Prov(\ulcorner \psi \urcorner) \to Prov(\ulcorner \varphi \urcorner)$	Modus Ponens; $(6), (7)$
(9)	$\mathbf{PA} \vdash Prov(\ulcorner \varphi \urcorner) \to \varphi$	Suposición
(10)	$\mathbf{PA} \vdash Prov(\ulcorner \psi \urcorner) \to \varphi$	Consecuencia lógica; $(9), (10)$
(11)	$\mathbf{PA} \vdash (Prov(\ulcorner \psi \urcorner) \to \varphi) \to \psi$	Consecuencia lógica; (1)
(12)	$\mathbf{PA} \vdash \psi$	Modus Ponens; $(10), (11)$
(13)	$\mathbf{PA} \vdash Prov(\ulcorner \psi \urcorner)$	P1; (12)
(14)	$\mathbf{PA} \vdash \varphi$	Modus Ponens; $(10), (13)$

■

Fácilmente podemos observar como el Segundo Teorema de Incompletitud se tiene como corolario del Teorema de Löb:

Teorema 3.3. *Si* **PA** *es consistente, entonces* $\mathbf{PA} \nvdash \neg Prov(\ulcorner \bot \urcorner)$.

Demostración.

Si $\mathbf{PA} \vdash Prov(\ulcorner \bot \urcorner) \to \bot$ entonces por el Teorema de Löb se cumple que $\mathbf{PA} \vdash \bot$ y por lo tanto **PA** sería inconsistente. Entonces $\mathbf{PA} \nvdash Prov(\ulcorner \bot \urcorner) \to \bot$, lo que significa que $\mathbf{PA} \nvdash Con_{\mathbf{PA}}$.

■

Definimos una nueva regla de inferencia en la lógica modal:

Regla de Löb. *De* $\vdash (\Box A \to A)$ *inferimos* $\vdash A$.

Ahora definimos **K4LR** como el sistema lógico modal **K4** + Regla de Löb.

Teorema 3.4. *Si* $\mathbf{K4LR} \vdash A$, *entonces para toda realización* * *se cumple* $\mathbf{PA} \vdash A^*$.

Demostración.

Solo tenemos que ver que **PA** es cerrada bajo la Regla de Löb que acabamos de introducir:

(1)	$\mathbf{PA} \vdash (\Box A \to A)^*$	
(2)	$\mathbf{PA} \vdash (Prov(\ulcorner A^* \urcorner) \to A^*)$	Definición de *
(3)	$\mathbf{PA} \vdash A^*$	Teorema de Löb; (2)

■

Teorema 3.5. *Sea* $A \in FORM_{\mathcal{L}_\Box}$, $\mathbf{GL} \vdash A$ *si y sólo si* $\mathbf{K4LR} \vdash A$.

Demostración.

($\Leftarrow$) Como vimos en Teorema 2.15, $\mathbf{GL} \vdash \Box A \to \Box\Box A$. Por lo que nos queda ver que **GL** es cerrada bajo la Regla de Löb:

(1)	$\mathbf{GL} \vdash \Box A \to A$	
(2)	$\mathbf{GL} \vdash \Box(\Box A \to A)$	Necesidad; (1)
(3)	$\mathbf{GL} \vdash \Box(\Box A \to A) \to \Box A$	Axioma G
(4)	$\mathbf{GL} \vdash \Box A$	Modus ponens; (2), (3)
(5)	$\mathbf{GL} \vdash A$	Modus ponens; (1), (4)

($\Rightarrow$) Tenemos que demostrar que **K4LR** puede probar cualquier instancia del axioma **G**: $\Box(\Box A \to A) \to \Box A$.

(1)	$\mathbf{K4LR} \vdash \Box(\Box(\Box A \to A) \to \Box A) \to$ $\to (\Box\Box(\Box A \to A) \to \Box\Box A)$	Axioma **K**
(2)	$\mathbf{K4LR} \vdash \Box(\Box A \to A) \to \Box\Box(\Box A \to A)$	Axioma **4**
(3)	$\mathbf{K4LR} \vdash \Box(\Box(\Box A \to A) \to \Box A) \to$ $\to (\Box(\Box A \to A) \to \Box\Box A)$	Consecuencia lógica; $(1), (2)$
(4)	$\mathbf{K4LR} \vdash \Box(\Box A \to A) \to (\Box\Box A \to \Box A)$	Axioma **K**
(5)	$\mathbf{K4LR} \vdash \Box(\Box(\Box A \to A) \to \Box A) \to$ $\to (\Box(\Box A \to A) \to \Box A)$	Consecuencia lógica; $(3), (4)$
(6)	$\mathbf{K4LR} \vdash \Box(\Box A \to A) \to \Box A$	Regla de Löb; (5)

■

Teorema 3.6. *Si* $\mathbf{GL} \vdash A$, *entonces para toda realización* *, $\mathbf{PA} \vdash A^*$.

Demostración.

GL y **K4LR** tienen los mismos teoremas.

■

Sean $\varphi, \psi \in \mathrm{SENT}_{\mathcal{L}_\mathrm{A}}$, a veces utilizaremos un lenguaje no matemático para expresar afirmaciones del lenguaje matemático. Entre ellas encontraremos afirmaciones como "φ es demostrable" cuya aritmetización sería la fórmula cerrada $Prov(\ulcorner\varphi\urcorner)$, "$\varphi$ es consistente" que corresponde a $\neg Prov(\ulcorner\neg\varphi\urcorner)$ o la aritmetización de "la aritmética es consistente" sería $\neg Prov(\ulcorner\bot\urcorner)$.
Una afirmación será demostrable en **PA** cuando lo sea su aritmetización.

Corolario 11. *El segundo teorema de incompletitud para* **PA** es derivable en **PA**.

Demostración.

(1)	$\mathbf{GL} \vdash \Box(\Box\bot \to \bot) \to \Box\bot$	Axioma **G**
(2)	$\mathbf{GL} \vdash (\Box(\Box\bot \to \bot) \to \Box\bot) \to$ $\to (\neg\Box\bot \to \neg\Box(\Box\bot \to \bot))$	Consecuencia lógica; (1)
(3)	$\mathbf{GL} \vdash \neg\Box\bot \to \neg\Box(\Box\bot \to \bot)$	Modus Ponens; $(1), (2)$

Sea * una realización, por el Teorema 3.6 se tiene $\mathbf{PA} \vdash (\neg\Box\bot \to \neg\Box(\Box\bot \to \bot))^*$, esto es $\mathbf{PA} \vdash \neg Prov(\ulcorner\bot\urcorner) \to \neg Prov(\ulcorner\neg Prov(\ulcorner\bot\urcorner)\urcorner)$.

■

Corolario 12. **PA** puede demostrar que si la inconsistencia de la aritmética no es demostrable en **PA**, entonces la consistencia de la aritmética es indecidible.

Demostración.

(1)	$\mathbf{GL} \vdash \Box\bot \to \Box\Box\bot$	Axioma 4
(2)	$\mathbf{GL} \vdash \neg\Box\Box\bot \to \neg\Box\bot$	Consecuencia lógica; (1)
(3)	$\mathbf{GL} \vdash \neg\Box\bot \to \neg\Box\neg\Box\bot$	Corolario 11
(4)	$\mathbf{GL} \vdash \neg\Box\Box\bot \to \neg\Box\neg\Box\bot$	Consecuencia lógica; (2), (3)
(5)	$\mathbf{GL} \vdash \neg\Box\Box\bot \to (\neg\Box\Box\bot \wedge \neg\Box\neg\Box\bot)$	

Por lo tanto:

$$\mathbf{PA} \vdash \neg Prov(\ulcorner Prov(\ulcorner \bot \urcorner)\urcorner) \to (\neg Prov(\ulcorner Prov(\ulcorner \bot \urcorner)\urcorner) \wedge \neg Prov(\ulcorner \neg Prov(\ulcorner \bot \urcorner)\urcorner))$$

Esto significa que si **PA** no puede demostrar su inconsistencia entonces la consistencia de la aritmética es indecidible.

■

Corolario 13 (Teorema de Löb formalizado).
Sea $\varphi \in SENT_{\mathcal{L}_A}$ *entonces se tiene* $\mathbf{PA} \vdash Prov(\ulcorner Prov(\ulcorner \varphi \urcorner) \to \varphi \urcorner) \to Prov(\ulcorner \varphi \urcorner)$.

Demostración.

Por el axioma **G** tenemos que $\mathbf{GL} \vdash \Box(\Box p \to p) \to \Box p$, para p una variable modal, por el teorema 3.6 para toda realización * y tomando * tal que $p^* = \varphi$ tenemos:

(1) $\mathbf{PA} \vdash (\Box(\Box p \to p) \to \Box p)^*$

(2) $\mathbf{PA} \vdash Prov(\ulcorner Prov(\ulcorner p^* \urcorner) \to p^* \urcorner) \to Prov(\ulcorner p^* \urcorner)$

(3) $\mathbf{PA} \vdash Prov(\ulcorner Prov(\ulcorner \varphi \urcorner) \to \varphi \urcorner) \to Prov(\ulcorner \varphi \urcorner)$

■

Corolario 14 (Löb Fuerte). *Sean* $\varphi, \psi \in SENT_{\mathcal{L}_A}$*, si se cumple que* $\mathbf{PA} \vdash (Prov(\ulcorner \varphi \urcorner) \wedge Prov(\ulcorner \psi \urcorner)) \to \psi$ *entonces* $\mathbf{PA} \vdash Prov(\ulcorner \varphi \urcorner) \to \psi$.

Demostración.

(1)	$\mathbf{PA} \vdash (Prov(\ulcorner\varphi\urcorner) \wedge Prov(\ulcorner\psi\urcorner)) \to \psi$	Suposición
(2)	$\mathbf{PA} \vdash Prov(\ulcorner\varphi\urcorner) \to (Prov(\ulcorner\psi\urcorner) \to \psi)$	Consecuencia lógica; (1)
(3)	$\mathbf{PA} \vdash Prov(\ulcorner Prov(\ulcorner\varphi\urcorner) \to (Prov(\ulcorner\psi\urcorner) \to \psi)\urcorner)$	P1;(2)
(4)	$\mathbf{PA} \vdash Prov(\ulcorner Prov(\ulcorner\varphi\urcorner)\urcorner)$ $\to Prov(\ulcorner Prov(\ulcorner\psi\urcorner) \to \psi\urcorner)$	P2;(3)
(5)	$\mathbf{PA} \vdash Prov(\ulcorner Prov(\ulcorner\psi\urcorner) \to \psi\urcorner) \to Prov(\ulcorner\psi\urcorner)$	Löb formalizado
(6)	$\mathbf{PA} \vdash Prov(\ulcorner Prov(\ulcorner\varphi\urcorner)\urcorner) \to Prov(\ulcorner\psi\urcorner)$	Consecuencia lógica; (4), (5)
(7)	$\mathbf{PA} \vdash Prov(\ulcorner\varphi\urcorner) \to Prov(\ulcorner Prov(\ulcorner\varphi\urcorner)\urcorner)$	P3
(8)	$\mathbf{PA} \vdash Prov(\ulcorner\varphi\urcorner) \to Prov(\ulcorner\psi\urcorner)$	Consecuencia lógica; (6), (7)
(9)	$\mathbf{PA} \vdash Prov(\ulcorner\varphi\urcorner) \to \psi$	Consecuencia lógica; (2), (8)

■

Definición 3.0.3. Sea $\varphi \in \mathrm{FORM}_{\mathcal{L}_\mathrm{A}}$, a la fórmula $Prov(\ulcorner\varphi\urcorner) \to \varphi$ la llamaremos *principio de reflexión* o *reflexión* para φ.

De esta forma, el teorema de Löb nos afirma que para toda fórmula cerrada φ de **PA**, si reflexión para φ es demostrable, φ también lo es. A continuación introduciremos un nuevo sistema de lógica modal proposicional al que llamaremos **GLS**, por Solovay.

Definición 3.0.4. $\mathbf{GLS} = \mathbf{GL} +$ Axioma **T** y su única regla de inferencia es *modus ponens*.

La motivación detrás de **GLS** es la siguiente: debido a que cada teorema de **PA** es verdadero en el modelo estándar, para toda fórmula $\varphi \in \mathrm{SENT}_{\mathcal{L}_\mathrm{A}}$ se tiene que si $Prov(\ulcorner\varphi\urcorner)$ es verdadera (esto es, existe una demostración en **PA** de φ) entonces φ es un teorema de **PA** y así φ es verdadera. Esto conlleva que, para toda realización * y toda fórmula modal $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$ tenemos que $(\Box A \to A)^*$ es verdadera. Si además A es un teorema de **GL** entonces A^* es un teorema de **PA**. Debido a esto, el siguiente teorema surge de forma natural.

Teorema 3.7. *Para* $A \in FORM_{\mathcal{L}_\Box}$*, si* $\mathbf{GLS} \vdash A$ *entonces para toda realización* **,* A^* *es verdadera en el modelo estándar.*

Cabe remarcar, que **GLS** aunque sea cerrada bajo *modus ponens* y sustitución, no lo es bajo necesidad, por lo tanto **GLS** no es un sistema modal normal, lo podemos observar en que $\mathbf{GLS} \vdash \Box\bot \to \bot$ por el axioma **T**, si **GLS** fuera cerrada bajo necesidad tendríamos que $\mathbf{GLS} \vdash \Box(\Box\bot \to \bot)$ y por el teorema anterior $(\Box(\Box\bot \to \bot))^*$ sería verdadera lo que implicaría que $(\Box(\neg\Box\bot))^*$ fuera verdadera y con ella la consistencia de la aritmética sería demostrable, cosa que no ocurre.

Capítulo 4

Completitud aritmética de GL y GLS

4.1 Completitud aritmética de GL

Teorema 4.1. *Para toda fórmula $A \in FORM_{\mathcal{L}_\Box}$, si para toda realización * se cumple que* $\mathbf{PA} \vdash A^*$ *entonces* $\mathbf{GL} \vdash A$.

Demostración.

Sea $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$ tal que $\mathbf{GL} \nvdash A$, entonces existe un modelo $M' = \langle W', R', V' \rangle$ transitivo, finito e IBF en el cual A no es válida. Nuestro objetivo es construir una interpretación * en la que $\mathbf{PA} \nvdash A^*$.

Sin pérdida de generalidad, podemos definir:

- $W' := \{1, ..., n\}$
- $1R'i$ si y sólo si $1 < i \leq n$

y asumimos que $M', 1 \nvDash' A$.

La idea de la demostración consiste en construir $S_0, \ldots, S_n$ fórmulas de **PA** a las que llamaremos *Fórmulas de Solovay* que nos servirán para determinar la interpretación * que buscamos.

Primero, vamos a expandir M' a M, al final de la demostración se comprenderá la motivación de esta expansión:

- $W = W' \cup \{0\}$.
- $R = R' \cup \{\langle 0, i \rangle | 1 \leq i \leq n\}$, R es transitivo, IBF y finito ya que R' lo es.
- Para toda p variable modal y para toda i con $1 \leq i \leq n$ tendremos iVp si y sólo si $iV'p$; y $0Vp$ si y sólo si $1V'p$.

Buscamos definir una función h acotada por un cierto l y que siempre tome valores distintos de l.

Sea $h : \mathbb{N} \to \#(W)$ definida como:

$$\begin{cases} h(0) = 0, \\ \\ h(m+1) = \begin{cases} j \;\; si \;\; h(m) = i \wedge iRj \wedge Pf(\mathbf{m}, \ulcorner l \neq \mathbf{j} \urcorner), \\ \\ i \text{ en caso contrario.} \end{cases} \end{cases}$$

h va a operar de la siguiente forma: dado $h(x) = i$, si se cumple que x es el número de Gödel de la demostración en **PA** de que j no es el límite de h entonces $h(x+1) = j$.

Ahora queremos definir aritméticamente nuestra función h, para ello desarrollaremos lo siguiente. Si $H(a,b)$ es una fórmula de **PA** que define la relación $\{\langle a,b\rangle | h(a) = b\}$, entonces definimos:

$$S_j \equiv \exists c \forall a (a \geq c \to \exists b (b = \mathbf{j} \wedge H(a,b)))$$

Donde S_j va a ser la *Fórmula de Solovay* que afirme que j es el límite de h.
Para conseguir la expresión de $H(a,b)$, tenemos que usar sucesiones de símbolos de **PA** para describir aritméticamente a h, para ello tomamos $h(a) = b$ si y sólo si existe una sucesión finita s con $long(s) = a+1$ tal que $s_0 = 0$, $s_a = b$ y además para todo $x < a$ si $s_x = i$ entonces:

$$\begin{cases} s_{x+1} = j & \text{si } iRj \wedge Pf(\mathbf{x}, \ulcorner \neg \exists c \forall a (a \geq c \to \exists b (b = \mathbf{j} \wedge H(a,b))) \urcorner) \\ s_{x+1} = i & \qquad\qquad\qquad\qquad\qquad c.c. \end{cases}$$

Sea $\text{notlim}(\boldsymbol{m}, \boldsymbol{j}) \equiv \ulcorner \neg \exists c \forall a (a \geq c \to \exists b (b = \boldsymbol{j} \wedge F_{\boldsymbol{m}})) \urcorner$ con F_m la fórmula con número de Gödel m y sea:

$$\begin{aligned} B(y,a,b) \equiv \exists s \Bigg(& \text{FinSeq}(s) \wedge \text{long}(s) = a+1 \wedge s_0 = \mathbf{0} \wedge s_a = \mathbf{b} \\ & \wedge \forall x < a \bigwedge_{0 \leq i \leq n} \Bigg[s_x = \mathbf{i} \to \Big\{ \bigwedge_{j:iRj} [Pf(\mathbf{x}, \ulcorner \text{notlim}(y, \mathbf{j}) \urcorner) \to s_{x+1} = \mathbf{j}] \\ & \wedge \Big[\Big\{ \bigwedge_{j:iRj} \neg Pf(\mathbf{x}, \ulcorner \mathbf{notlim}(y, \mathbf{j}) \urcorner) \Big\} \to s_{x+1} = s_x \Big] \Big\} \Bigg] \Bigg). \end{aligned}$$

Vamos a usar estas dos fórmulas para terminar de definir aritméticamente a h. Usando el lema diagonal generalizado existe una fórmula $H(a,b)$ con a,b sus únicas variables libres tal que $\mathbf{PA} \vdash H(a,b) \leftrightarrow B(\ulcorner H(a,b) \urcorner, a, b)$.
Sea m el número de Gödel de la fórmula $H(a,b)$, esto hace que $F_m = H(a,b)$ y además $\mathbf{PA} \vdash notlim(Prov(\ulcorner H(a,b) \urcorner), \boldsymbol{j}) = notlim(\boldsymbol{m}, \boldsymbol{j}) = \ulcorner \neg S_j \urcorner$ por definición de $notlim(\boldsymbol{m}, \boldsymbol{j})$ y de S_j.

Finalmente, usando todo esto obtenemos:

$$\mathbf{PA} \vdash H(a,b) \leftrightarrow \exists s \Bigg(\text{FinSeq}(s) \wedge \text{long}(s) = a+1 \wedge s_0 = \mathbf{0} \wedge s_a = \mathbf{b}$$
$$\wedge \, \forall x < a \bigwedge_{0 \leq i \leq n} \Bigg[s_x = \mathbf{i} \rightarrow \Bigg\{ \bigwedge_{j:iRj} [Pf(\mathbf{x}, \ulcorner \neg S_j \urcorner) \rightarrow s_{x+1} = \mathbf{j}] \wedge$$
$$\Big[\Big\{ \bigwedge_{j:iRj} \neg Pf(\mathbf{x}, \ulcorner \neg S_j \urcorner) \Big\} \rightarrow s_x + 1 = s_x \Big] \Bigg\} \Bigg] \Bigg).$$

Así, h queda definida aritméticamente por el Σ ptérmino $H(a,b)$.

Una vez encontrada $H(a,b)$ y construidas las *Fórmulas de Solovay*, vamos a demostrar algunas propiedades sobre estas últimas que nos ayudarán a terminar de demostrar el teorema.

Aserto 1. $\mathbf{PA} \vdash \exists! b H(a,b)$.

Demostración.

Lo haremos por inducción en a:
Como $h(0) = 0$, tenemos que $\mathbf{PA} \vdash H(\mathbf{0}, \mathbf{0})$ y como existe una única sucesión que contenga solo al 0, $\langle \mathbf{0} \rangle$, tenemos $\mathbf{PA} \vdash \exists! b H(\mathbf{0}, b)$.

Supongamos que $\mathbf{PA} \vdash \exists! b H(\mathbf{k}, b)$, esto es $h(k) = i$, entonces por definición de h existe una sucesión $s = \langle a_0, ..., a_k \rangle$ tal que $a_0 = \mathbf{0}$ y $a_k = \boldsymbol{i}$, por lo tanto $h(k+1) = i$ ó para iRj $h(k+1) = j$, pudiendo así aumentar la sucesión $s = \langle a_0 \ldots, a_k, a_{k+1} \rangle$ donde $a_{k+1} = \boldsymbol{i}$ ó $a_{k+1} = \boldsymbol{j}$, en cualquier caso $\mathbf{PA} \vdash \exists b H(k+1, b)$.
Para la unicidad, dada cualquier otra sucesión $r = \langle r_0, \ldots, r_{k+1} \rangle$ que cumpla $r_0 = a_0, \ldots, r_k = a_k$ y satisfaga $H(k+1, c)$ necesariamente se tendrá que $r_{k+1} = a_{k+1}$ por definición de h y $b = c$, obteniendo así que $\mathbf{PA} \vdash \exists! b H(a,b)$.

■

Aserto 2 (Unicidad del límite)**.** Para todo i, j tal que $0 \leq i < j \leq n$ se tiene que $\mathbf{PA} \vdash \neg(S_i \wedge S_j)$.

Demostración.

Por reducción al absurdo, sean $0 \leq i < j \leq n$ tal que $\mathbf{PA} \vdash S_i \wedge S_j$, tenemos $\mathbf{PA} \vdash S_i$ y $\mathbf{PA} \vdash S_j$, esto implica la existencia de n_1, n_2 que cumplen:

$$\mathbf{PA} \vdash \forall a [a \geq n_1 \rightarrow H(a, \mathbf{i})]$$
$$\mathbf{PA} \vdash \forall a [a \geq n_2 \rightarrow H(a, \mathbf{j})]$$

Tomando $N = \text{máx}\{n_1, n_2\}$ tenemos $\mathbf{PA} \vdash H(\boldsymbol{N}, \boldsymbol{i})$ y $\mathbf{PA} \vdash H(\boldsymbol{N}, \boldsymbol{j})$ lo que implica por el Aserto 1 que $i = j$ contradiciendo $i < j$.

■

Aserto 3. $\mathbf{PA} \vdash H(a, \mathbf{i}) \to \left(S_i \vee \bigvee_{j:iRj} S_j\right)$.

Demostración.

Lo demostraremos por inducción en el inverso de R. Sea $0 \leq i \leq n$, supongamos que para todo $j \in W$ tal que iRj se tiene :

$$\mathbf{PA} \vdash H(a, \mathbf{j}) \to \left(S_j \vee \bigvee_{k:jRk} S_k\right). \tag{1}$$

Por definición de $H(a, b)$, tenemos:

$$\mathbf{PA} \vdash H(a, \mathbf{i}) \to \forall c \left[c \geq a \to \left(H(c, \mathbf{i}) \vee \bigvee_{j:iRj} H(c, \mathbf{j})\right)\right]$$

Por (1):

$$\mathbf{PA} \vdash H(a, \mathbf{i}) \to \forall c \left[c \geq a \to \left(H(c, \mathbf{i}) \vee \bigvee_{j:iRj} \left(S_j \vee \bigvee_{k:jRk} S_k\right)\right)\right]$$

Simplificando:

$$\mathbf{PA} \vdash H(a, \mathbf{i}) \to \left(\forall c \left[c \geq a \to H(c, \mathbf{i})\right] \vee \bigvee_{j:iRj} \left(S_j \vee \bigvee_{k:jRk} S_k\right)\right)$$

Por definición de S_i:

$$\mathbf{PA} \vdash H(a, \mathbf{i}) \to \left(S_i \vee \bigvee_{j:iRj} \left(S_j \vee \bigvee_{k:jRk} S_k\right)\right)$$

Y finalmente, como R es transitivo:

$$\mathbf{PA} \vdash H(a, \mathbf{i}) \to \left(S_i \vee \bigvee_{j:iRj} S_j\right)$$

■

Aserto 4. $\mathbf{PA} \vdash S_0 \vee S_1 \vee \cdots \vee S_n$.

Demostración.

Ya vimos que $\mathbf{PA} \vdash H(\mathbf{0}, \mathbf{0})$, entonces por el Aserto 3 obtenemos que

$$\mathbf{PA} \vdash \left(S_0 \vee \bigvee_{j:0Rj} S_j \right)$$

y como para todo j con $1 \leq j \leq n$ se tiene que $0Rj$, finalmente:

$$\mathbf{PA} \vdash S_0 \vee S_1 \vee \cdots \vee S_n.$$

■

Aserto 5. Si iRj entonces $\mathbf{PA} \vdash S_i \to \neg Prov(\ulcorner \neg S_j \urcorner)$.

Demostración.

Supongamos que el límite de h es i y sea m tal que para todo $r > m$ se tiene que $h(r) = h(m) = i$. Como cada teorema de **PA** tiene infinitas demostraciones (recordemos que una demostración en **PA** es una sucesión donde podemos introducir tantas tautologías como queramos para obtener infinitas demostraciones de un teorema) existe un $k > m$ tal que k es el número de Gödel de una demostración de $\neg S_j$ en **PA** y entonces $h(k+1) = j \neq i$, lo que nos llevaría a una contradicción, teniendo así el resultado.

■

Aserto 6. Para todo $i \geq 1$ tenemos que $\mathbf{PA} \vdash S_i \to Prov(\ulcorner \neg S_i \urcorner)$.

Demostración.

(1)	$\mathbf{PA} \vdash S_i \to \exists a H(a, \mathbf{i})$,	Definición de S_i
(2)	$\mathbf{PA} \vdash H(a, \mathbf{i}) \to \exists x Pf(\mathbf{x}, \ulcorner \neg S_i \urcorner)$,	Definición de $H(a, i)$
(3)	$\mathbf{PA} \vdash S_i \to Prov(\ulcorner \neg S_i \urcorner)$.	Lógica proposicional; (1), (2)

■

Aserto 7. Para todo $i \geq 1$ se tiene que $\mathbf{PA} \vdash S_i \to Prov(\ulcorner \bigvee_{j:iRj} S_j \urcorner)$.

Demostración.

(1)	$\mathbf{PA} \vdash H(a,\mathbf{i}) \to \left(S_i \vee \bigvee_{j:iRj} S_j\right)$	Aserto 3
(2)	$\mathbf{PA} \vdash \exists a H(a,\mathbf{i}) \to \left(S_i \vee \bigvee_{j:iRj} S_j\right)$	Cálculo lógico
(3)	$\mathbf{PA} \vdash Prov(\ulcorner \exists a H(a,\mathbf{i}) \to \left(S_i \vee \bigvee_{j:iRj} S_j\right)\urcorner)$	P1
(4)	$\mathbf{PA} \vdash Prov(\ulcorner \exists a H(a,\mathbf{i})\urcorner) \to$ $\to Prov(\ulcorner \left(S_i \vee \bigvee_{j:iRj} S_j\right)\urcorner)$	P2
(5)	$\mathbf{PA} \vdash (Prov(\ulcorner \neg S_i \urcorner) \wedge Prov(\ulcorner S_i \vee \bigvee_{j:iRj} S_j \urcorner)) \to$ $\to Prov(\ulcorner \bigvee_{j:iRj} S_j \urcorner)$	Lógicamente válida
(6)	$\mathbf{PA} \vdash H(a,\mathbf{i}) \to Prov(\ulcorner H(a,\mathbf{i})\urcorner)$	H es Σ
(7)	$\mathbf{PA} \vdash S_i \to \exists a H(a,\mathbf{i})$	Aserto 6.
(8)	$\mathbf{PA} \vdash \exists a H(a,\mathbf{i}) \to Prov(\ulcorner \exists a H(a,\mathbf{i}\urcorner))$	Σ-completitud de **PA**
(9)	$\mathbf{PA} \vdash S_i \to Prov(\ulcorner \exists a H(a,\mathbf{i}\urcorner))$	Consecuencia lógica; (7), (8)
(10)	$\mathbf{PA} \vdash S_i \to Prov(\ulcorner S_i \vee \bigvee_{j:iRj} S_j \urcorner)$	Consecuencia lógica; (2), (9)
(11)	$\mathbf{PA} \vdash S_i \to Prov(\ulcorner \neg S_i \urcorner)$	Aserto 6.
(12)	$\mathbf{PA} \vdash S_i \to$ $\to (Prov(\ulcorner \neg S_i \urcorner) \wedge Prov(\ulcorner S_i \vee \bigvee_{j:iRj} S_j \urcorner))$	Consecuencia lógica; (10), (11)
(13)	$\mathbf{PA} \vdash S_i \to Prov(\ulcorner \bigvee_{j:iRj} S_j \urcorner)$.	Consecuencia lógica; (5), (12)

■

Para toda variable proposicional p, definimos nuestra interpretación * como

$$p^* := \bigvee_{i:iVp} S_i$$

Aserto 8. Para todo i tal que $1 \leq i \leq n$ y toda subfórmula B de A, se tiene:
Si $M', i \vDash' B$ entonces $\mathbf{PA} \vdash S_i \rightarrow B^*$.
Si $M', i \nvDash' B$ entonces $\mathbf{PA} \vdash S_i \rightarrow \neg B^*$.

Demostración.

Inducción en la complejidad de B:

Sea $B = p$:
Si $M', i \vDash' B$ entonces $M, i \vDash B$ y por lo tanto $\mathbf{PA} \vdash S_i \rightarrow B^*$.
Si $M', i \nvDash' B$ entonces $M, i \nvDash B$, por lo tanto $p^* = \bigvee_{j:jVp} S_j$ donde S_i es distinto a todo S_j que aparece en p^*, por la unicidad del límite para todo S_j que aparece en p^* se tiene que $\mathbf{PA} \vdash S_i \rightarrow \neg S_j$ y finalmente $\mathbf{PA} \vdash S_i \rightarrow \neg B^*$.

Sea $B = \Box C$ con C cumpliendo el aserto, $B^* = Prov(\ulcorner C \urcorner)$.
Se tiene que $M', i \vDash' B$ si y sólo si para todo mundo j tal que $iR'j$ se tiene $M', j \vDash' C$. Como C cumple el aserto, se tiene que para todo j tal que $iR'j$ que $\mathbf{PA} \vdash S_j \rightarrow C^*$ y así:

(1)	$\mathbf{PA} \vdash S_j \rightarrow C^*$	
(2)	$\mathbf{PA} \vdash \bigvee_{j:iR'j} S_j \rightarrow C^*$	Consecuencia lógica; (1)
(3)	$\mathbf{PA} \vdash Prov(\ulcorner \bigvee_{j:iR'j} S_j \urcorner) \rightarrow B^*$	P1 y P2; (2)
(4)	$\mathbf{PA} \vdash S_i \rightarrow Prov(\ulcorner \bigvee_{j:iR'j} S_j \urcorner)$	Aserto 7
(5)	$\mathbf{PA} \vdash S_i \rightarrow B^*$	Consecuencia lógica; (3), (4)

Si $M', i \nvDash' B$ existe al menos un j tal que $iR'j$ y $M', j \nvDash' C$ entonces $\mathbf{PA} \vdash S_j \rightarrow \neg C^*$.

(1)	$\mathbf{PA} \vdash C^* \rightarrow \neg S_j$	
(2)	$\mathbf{PA} \vdash Prov(\ulcorner C^* \urcorner) \rightarrow Prov(\ulcorner \neg S_j \urcorner)$	P1 y P2;(1)
(3)	$\mathbf{PA} \vdash \neg Prov(\ulcorner \neg S_j \urcorner) \rightarrow \neg Prov(\ulcorner C^* \urcorner)$	Consecuencia lógica; (2)
(4)	$\mathbf{PA} \vdash S_i \rightarrow \neg Prov(\ulcorner \neg S_j \urcorner)$	Aserto 5.
(5)	$\mathbf{PA} \vdash S_i \rightarrow \neg Prov(\ulcorner C^* \urcorner)$	Consecuencia lógica; (3), (4)
(6)	$\mathbf{PA} \vdash S_i \rightarrow \neg B^*$	Inducción en C

Sea $B = C \rightarrow D$. Sabemos que $M', i \vDash' B$ si y sólo si $M', i \nvDash' C$ ó $M, w \vDash D$, entonces, como por hipótesis de inducción C y D cumplen el aserto, tenemos que $\mathbf{PA} \vdash S_i \rightarrow \neg C^*$ ó $\mathbf{PA} \vdash S_i \rightarrow D^*$.

(1)	$\mathbf{PA} \vdash S_i \rightarrow \neg C^*$ o $\mathbf{PA} \vdash S_i \rightarrow D^*$	
(2)	$\mathbf{PA} \vdash S_i \rightarrow (\neg C^* \vee D^*)$	Consecuencia lógica; (1)

(3) $\mathbf{PA} \vdash S_i \to (\neg C \vee D)^*$ Definición de *

(4) $\mathbf{PA} \vdash S_i \to (C \to D)^*$ Consecuencia lógica; (3)

(5) $\mathbf{PA} \vdash S_i \to B^*$ Definición de B

$M', i \not\models' B$ si y sólo si $M', i \not\models' C \to D$ si y sólo si $M', i \models' C \wedge M', i \not\models' D$.

(1) $\mathbf{PA} \vdash S_i \to C^*$ y $\mathbf{PA} \vdash S_i \to \neg D^*$

(2) $\mathbf{PA} \vdash S_i \to (C^* \wedge \neg D^*)$ Consecuencia lógica; (1)

(3) $\mathbf{PA} \vdash S_i \to \neg(C \to D)^*$ Consecuencia lógica; (2)

(4) $\mathbf{PA} \vdash S_i \to \neg B^*$ Definición de B

Sea $B = \neg C$, sabemos que $M', i \models' B$ si y sólo si $M', i \models' \neg C$ si y sólo si $M', i \not\models' C$.

(1) $\mathbf{PA} \vdash S_i \to \neg C^*$

(2) $\mathbf{PA} \vdash S_i \to B^*$ Definición de B

De la misma forma $M', i \not\models' B$ si y sólo si $M', i \models' C$.

(1) $\mathbf{PA} \vdash S_i \to C^*$

(2) $\mathbf{PA} \vdash S_i \to \neg B^*$ Definición de B

■

Aserto 9. $\mathbf{PA} \vdash S_0 \to \neg Prov(\ulcorner A^* \urcorner)$.

Demostración.

Como A es subfórmula de sí misma y $M', 1 \not\models' A$, se tiene:

(1) $\mathbf{PA} \vdash S_1 \to \neg A^*$ Aserto 8

(2) $\mathbf{PA} \vdash A^* \to \neg S_1$ Consecuencia lógica; (1)

(3) $\mathbf{PA} \vdash Prov(\ulcorner A^* \urcorner) \to Prov(\ulcorner \neg S_1 \urcorner)$ P1 y P2;(2)

(4) $\mathbf{PA} \vdash \neg Prov(\ulcorner \neg S_1 \urcorner) \to \neg Prov(\ulcorner A^* \urcorner)$ Consecuencia lógica; (3)

(5) $\mathbf{PA} \vdash S_0 \to \neg Prov(\ulcorner \neg S_1 \urcorner)$ Aserto 5

(6) $\mathbf{PA} \vdash S_0 \to \neg Prov(\ulcorner A^* \urcorner)$ Consecuencia lógica; (4), (5)

■

Como **PA** es correcta, todo teorema de **PA** es verdadero en el modelo estándar. Por el Aserto 6, sabemos que si $i \geq 1$ y S_i es verdadera, entonces $Prov(\ulcorner \neg S_i \urcorner)$ es verdadera, así $\neg S_i$ es demostrable en **PA** y $\neg S_i$ es verdadera, por lo tanto S_i no puede ser verdadera.
Por el Aserto 4 sabemos que **PA** $\vdash S_0 \vee \cdots \vee S_n$ por lo que S_0 es verdadera.
Por el Aserto 9 **PA** $\vdash S_0 \to \neg Prov(\ulcorner A^* \urcorner)$ y $\neg Prov(\ulcorner A^* \urcorner)$ son verdaderas y A^* no es un teorema de **PA** .

■

4.2 Completitud aritmética de GLS

Definición 4.2.1. Sea $A \in \text{FORM}_{\mathcal{L}_\Box}$, definimos

$$A^s := \bigwedge \{(\Box B \to B) : \Box B \text{ es subfórmula de } A\} \to A.$$

Teorema 4.2 (Completitud aritmética para GLS). *Sea $A \in FORM_{\mathcal{L}_\Box}$, son equivalentes:*

a) **GL** $\vdash A^s$*,*

b) **GLS** $\vdash A$*,*

c) Para toda realización **,* A^* *es verdadera.*

Demostración.

a)⇒b) Si **GL** $\vdash A^s$ entonces **GLS** $\vdash A^s$ y además, como **GLS** $\vdash \Box B \to B$ se tiene que **GLS** $\vdash A$.

b)⇒c) Constituye el Teorema 3.7

c)⇒a) Esta demostración bebe mucho de la demostración del teorema de la completitud aritmética de **GL**, por lo que omitiremos algunas explicaciones de argumentos similares que han aparecido en la demostración del teorema anterior.
Por contraposición suponemos que **GL** $\nvdash A^s$, entonces por el teorema de la completitud semántica de **GL** existe un modelo finito, transitivo e irreflexivo donde A^s no se cumple. Tomando $M', M, S_0, \ldots, S_n$ y * como en la demostración del teorema anterior, tenemos que $M', 1 \nvDash' A^s$ lo que implica, por definición de A^s, que para toda subfórmula $\Box B$ de A se tiene $M', 1 \vDash' \Box B \to B$ y $M', 1 \nvDash A$.
A continuación vamos a demostrar que para toda B subfórmula de A, si $M', 1 \vDash' B$ entonces **PA** $\vdash S_0 \to B^*$ y si $M', 1 \nvDash B$ entonces **PA** $\vdash S_0 \to \neg B^*$:

Sea $B = p$:
Si $M', 1 \vDash' p$ entonces $M, 1 \vDash p$ por lo tanto $1Vp$ se tiene que $0Vp$ y finalmente **PA** $\vdash S_0 \to B^*$.

De la misma forma, si $M', 1 \not\models' p$ entonces $M, 1 \not\models p$ por lo tanto $\neg(1Vp)$ entonces $\neg(0Vp)$ y finalmente $\mathbf{PA} \vdash S_0 \to \neg B^*$.

Sea $B = \neg C$:
Si $M', 1 \models' \neg C$ entonces $M', 1 \not\models C$ esto implica que $\mathbf{PA} \vdash S_0 \to \neg C$ y finalmente se tiene que $\mathbf{PA} \vdash S_0 \to B^*$.
Si se tiene $M', 1 \not\models' \neg C$ implica que $M', 1 \models C$ por lo tanto $\mathbf{PA} \vdash S_0 \to C$ y $\mathbf{PA} \vdash S_0 \to \neg B^*$.

Los caso de $B = C \to D$ y $B = \Box C$ son similares a los de la demostración del Aserto 9, por lo que omitiremos los razonamientos de cada paso.

Sea $B = C \to D$:
Si $M', 1 \models C \to D$ entonces

(1) $M', 1 \not\models' C \vee M', 1 \models' D$

(2) $\mathbf{PA} \vdash S_0 \to \neg C^* \vee \mathbf{PA} \vdash S_0 \to D^*$

(3) $\mathbf{PA} \vdash S_0 \to (\neg C \vee D) *$

(4) $\mathbf{PA} \vdash S_0 \to B^*$

Si $M', 1 \not\models C \to D$ entonces

(1) $M', 1, \models' C \wedge M', 1 \not\models' D$

(2) $\mathbf{PA} \vdash S_0 \to C^* \wedge \mathbf{PA} \vdash S_0 \to \neg D^*$

(3) $\mathbf{PA} \vdash S_0 \to (C \wedge \not D)^*$

(4) $\mathbf{PA} \vdash S_0 \to \neg B^*$

Sea $B = \Box C$
Si $M', 1 \models' \Box C$ entonces para todo i tal que $1 < i \leq n$ entonces $M', i \models' C$ y :

(1) $\mathbf{PA} \vdash S_i \to C^*$

(2) $M', 1 \models' \Box C \to C$

(3) $M', 1 \models' C$

(4) $\mathbf{PA} \vdash S_1 \to C^*$

(5) $\mathbf{PA} \vdash S_0 \to C^*$

(6) $\mathbf{PA} \vdash S_0 \vee \cdots \vee S_n$

(7) $\mathbf{PA} \vdash C^*$

(8) $\mathbf{PA} \vdash Prov(\ulcorner C^* \urcorner)$

(9) $\quad$ $\mathbf{PA} \vdash (\Box C)^*$

(10) $\quad$ $\mathbf{PA} \vdash B^*$

(11) $\quad$ $\mathbf{PA} \vdash S_0 \to B^*$

Si $M', 1 \not\models' B$ entonces para todo i tal que $1 < i \leq n$ entonces $M', i \not\models' C$:

(1) $\quad$ $\mathbf{PA} \vdash S_i \to \neg C^*$

(2) $\quad$ $\mathbf{PA} \vdash \neg Prov(\ulcorner \neg S_i \urcorner) \to \neg (\Box C)^*$

(3) $\quad$ $\mathbf{PA} \vdash S_0 \to \neg Prov(\ulcorner \neg S_1 \urcorner)$

(4) $\quad$ $\mathbf{PA} \vdash S_0 \to \neg B^*$

Como $M', 1 \not\models' A$, razonando igual que en la demostración del teorema anterior, se tiene que $\mathbf{PA} \vdash S_0 \to \neg A^*$ y $S_0 \to \neg A^*$ es verdadera; como S_0 es también verdadera tenemos que $\neg A^*$ es verdadera y entonces A^* es falsa.

■

4.3 Completitud aritmética uniforme de GL

Teorema 4.3. *Existe una realización* * *tal que para toda sentencia modal* A*, si se cumple* $\mathbf{PA} \vdash A^*$ *entonces* $\mathbf{GL} \vdash A$.

Demostración.

Sea $f : \mathbb{N} \to \mathbb{N}$ una función tal que $f(k)$ codifique la quíntupla $\langle W_k, R_k, V_k, w_k, A_k \rangle$ donde W_k es un conjunto finito de enteros positivos, R_k es una relación transitiva e irreflexiva en W_k, denotaremos por $M_k = \langle W_k, R_k, V_k \rangle$, $W_k = \{w_k\} \cup \{i : w_k R_k i\}$ y se cumple que si p_n es una variable modal que no ocurre en A_k entonces para todo mundo $i \in W_k$ se tiene que $\neg(iVp_n)$, además $M_k, w_k \not\models A_k$.
Asimismo para $i \neq j$ se tiene que W_i, W_j son disjuntos, también para todo $i \geq 1$ tenemos que $i \in \bigcup_k W_k$ y cada fórmula modal que no sea un teorema de **GL** será A_k para algún k.
Si $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$ no es un teorema de **GL** y contiene k símbolos, por la demostración del Teorema 4.1 existe un modelos $\langle W, R, V \rangle$ donde A no es válida. Como $\#(W) \leq 2^k, \#(R) \leq 2^{(2^k)^2}, \#(V) \leq 2^{k \cdot 2^k}$ entonces habrá a lo más $2^k \cdot 2^{(2^k)^2} \cdot 2^{k \cdot 2^k}$ modelos posibles $\langle W, R, V \rangle$ donde esto ocurre.

Sea $F(x, y)$ el Σ p-término que define a f, Sea

$$R' = \bigcup_k R_k \cup \{\langle 0, i \rangle : i \in W_k, k \geq 1\}$$

es fácil ver que R' es transitivo e IBF.

A continuación, sea $V' = \bigcup_k V_k$, y sea $R(x,y)$ una fórmula que cumpla:

1. $\mathbf{PA} \vdash R(\mathbf{0}, y) \leftrightarrow y \neq \mathbf{0}$.
2. Para $i \geq 1$ tenemos $\mathbf{PA} \vdash R(\boldsymbol{i}, y) \leftrightarrow \bigvee_{j:iR'j} y = \boldsymbol{j}$.
3. Para todo mundo x, y, z se tiene que $R(x,y) \wedge R(y,z) \rightarrow R(x,z)$.
4. Para toda fórmula aritmética $Q(x)$ se cumple que

$$\mathbf{PA} \vdash \forall x[\forall y[R(x,y) \rightarrow Q(y)] \rightarrow Q(x)] \rightarrow \forall x Q(x)$$

Tenemos que si $R(x,y)$ cumple dichas propiedades, entonces $R(x,y)$ define aritméticamente a R'.

Sea $Ex(m,r,j)$ el Σ p-término que define la función cuyo valor en $(\boldsymbol{m}, \boldsymbol{r})$ es $\boldsymbol{j}$ si $\boldsymbol{r}$ es el numeral de Gödel de la demostración de $(\neg\exists c \forall a)\big[a \geq c \rightarrow \exists b[b = \boldsymbol{j} \wedge F_m]\big]$. Se tiene que $\mathbf{PA} \vdash ex(x,y) \neq 0 \rightarrow Pf(y, notlim(x, ex(x,y)))$

Como en la demostración del Teorema 4.1, definimos $g : \mathbb{N} \rightarrow \mathbb{N}$ de la forma:

$$\begin{cases} g(0) = 0, \\ g(m+1) = \begin{cases} j \ \ si \ \ g(m) = i \wedge iRj \wedge Pf(\mathbf{m}, \ulcorner l \neq \mathbf{j} \urcorner), \\ g(m) \ \text{ en caso contrario.} \end{cases} \end{cases}$$

Por el lema diagonal se tiene que existe una fórmula $G(a,b)$ con número de Gödel g tal que

$$\begin{aligned} \mathbf{PA} \vdash G(a,b) \leftrightarrow \exists s \Big[& FinSeq(s) \wedge long(s) = a + \mathbf{1} \wedge s_0 = \mathbf{0} \wedge s_a = b \\ & \wedge (\forall x < a) \Big\{ \big[R(s_x, ex(\boldsymbol{g}, x)) \rightarrow s_{x+\mathbf{1}} = ex(\boldsymbol{g}, x)\big] \\ & \wedge \big[\neg R(s_x, ex(\boldsymbol{g}, x)) \rightarrow s_{x+\mathbf{1}} = s_x\big] \Big\} \Big] \end{aligned}$$

$G(a,b)$ es un Σ p-término ya que $R(x,y), Ex(m,r,j)$ lo son y define aritméticamente a h. Definimos $S(x) \equiv \exists c \forall a\big[a \geq c \rightarrow \exists b[b = x \wedge G(a,b)]\big]$, $S(\boldsymbol{i})$ nos dice que el límite de g es i.

Aserto 10. $\mathbf{PA} \vdash \exists! b G(a,b)$.

Demostración.

Demostración similar a la del Aserto 1.

■

Aserto 11 (Unicidad del límite)**.** Para $i \neq j$, $\mathbf{PA} \vdash \neg(S(\boldsymbol{i}) \wedge S(\boldsymbol{j}))$.

Demostración.

Debido a $\mathbf{PA} \vdash \exists! b G(a,b)$, se demuestra igual al Aserto 2.

■

Aserto 12. $\mathbf{PA} \vdash G(a,x) \rightarrow (S(x) \vee \exists y[R(x,y) \wedge S(y)])$.

Demostración.

Lo demostraremos por inducción en el inverso de R. Sea x un mundo, sea $Q(x) \equiv G(a,x) \rightarrow (S(x) \vee \exists y[R(x,y) \wedge S(y)])$, supongamos que para todo mundo y $R(x,y) \rightarrow Q(y)$ y $G(a,x)$:

(1) $\mathbf{PA} \vdash (\forall d)[d \geq a \rightarrow G(d,x) \vee \exists y[R(x,y) \wedge G(d,y)]]$

(2) $\mathbf{PA} \vdash (\forall d)\Big[d \geq a \rightarrow G(d,x) \vee \exists y\big[R(x,y) \wedge \big(S(y) \vee \exists v[R(y,v) \wedge S(v)]\big)\big]\Big]$

(3) $\mathbf{PA} \vdash S(x) \vee \exists y\big[R(x,y) \wedge \big(S(y) \vee \exists v[R(y,v) \wedge S(v)]\big)\big]$

(4) $\mathbf{PA} \vdash S(x) \vee \exists y[R(x,y) \wedge S(y)]$

Por lo tanto todo mundo x lo cumple.

■

Aserto 13. Sean i, j mundos tal que $iR'j$, entonces $\mathbf{PA} \vdash S(\boldsymbol{i}) \rightarrow \neg Prov(\ulcorner \neg S(\boldsymbol{j}) \urcorner)$.

Demostración.

Similar a la del Aserto 5.

■

Aserto 14. Dado un mundo i con ≥ 1 se tiene que $\mathbf{PA} \vdash S(\boldsymbol{i}) \rightarrow Prov(\ulcorner \neg S(\boldsymbol{i}) \urcorner)$.

Demostración.

Similar a la del Aserto 6.

■

Aserto 15. Si $i \geq 1$ entonces $\mathbf{PA} \vdash S(\boldsymbol{i}) \to Prov(\ulcorner \bigvee_{j:iR'j} S(\boldsymbol{j}) \urcorner)$.

Demostración.

Debido a que para algún $m \in \mathbb{N}$ se tiene que $\mathbf{PA} \vdash \exists r G(r, \boldsymbol{i}) \to G(\boldsymbol{m}, i)$, por el Aserto se tiene

$$\mathbf{PA} \vdash \exists r G(r, \boldsymbol{i}) \to S(\boldsymbol{i}) \vee \exists y \big[R(\boldsymbol{i}, y) \wedge S(y)\big]$$

Por (2) de nuestra definición de $R(x, y)$ tenemos que

$$\mathbf{PA} \vdash \exists r G(r, \boldsymbol{i}) \to S(\boldsymbol{i}) \vee \exists y \Bigg(\bigwedge_{j:iR'j} y = \boldsymbol{j} \wedge S(y) \Bigg)$$

Simplificando:

$$\mathbf{PA} \vdash \exists r G(r, \boldsymbol{i}) \to S(\boldsymbol{i}) \vee \Bigg(\bigwedge_{j:iR'j} S(\boldsymbol{j}) \Bigg)$$

Y argumentando de la misma forma que en el Aserto 7 se obtiene el resultado.

■

Sea $V(x, y)$ una Δ fórmula que define la relación $\{\langle i, n\rangle : iVp_n\}$. Para cada n, definimos $p_n^* = \exists x[S(x) \wedge V(x, \boldsymbol{n})]$.

Aserto 16. Para toda k, para toda subfórmula B de A_k, y todo $i \in W_k$ se tiene:
$M_k, i \vDash B \Rightarrow \mathbf{PA} \vdash S(\boldsymbol{i}) \to B^*$
$M_k, i \nvDash B \Rightarrow \mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg B^*$.

Demostración.

Lo demostraremos por inducción en la complejidad de B:

$B = p_n$:
Si $M_k, i \vDash B$ entonces $iV_k p_n$, luego iVp_n, así $\mathbf{PA} \vdash V(\boldsymbol{i}, \boldsymbol{n})$ y
$\mathbf{PA} \vdash S(\boldsymbol{i}) \to \exists x[S(x) \wedge V(x, \boldsymbol{n})]$ por lo tanto $\mathbf{PA} \vdash S(\boldsymbol{i}) \to \mathbf{B}^*$.
Si $M_k, i \nvDash B$ entonces $\neg(iV_k B)$, luego $\neg(iVB)$, así $\mathbf{PA} \vdash \neg V(\boldsymbol{i}, \boldsymbol{n})$, por la unicidad del límite $\mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg\exists x[S(x) \wedge V(x, \boldsymbol{n})]$ y finalmete $\mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg B^*$.

$B = \neg C$ con C cumpliendo el aserto.
Si $M_k, i \vDash B$ entonces:

(1) $\quad M_k, i \nvDash C$

(2) $\quad \mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg C^*$

(3) $\quad \mathbf{PA} \vdash S(\boldsymbol{i}) \to B^*$

Si $M_k, i \nvDash B$ entonces:

(1) $M_k, i \models \neg B$

(2) $M_k, i \models C$

(3) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to C^*$

(4) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg B^*$

$B = C \to D$ con C, D cumpliendo el aserto: Si $M_k, i \models B$ entonces:

(1) $M_k, i \not\models C \vee M_k, i \models \neg D$

(2) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg C^* \vee \mathbf{PA} \vdash S(\boldsymbol{i}) \to D^*$

(3) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to (\neg C \vee D)^*$

(4) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to B^*$

Si $M_k, i \not\models B$ entonces:

(1) $M_k, i \models C \wedge M_k, i \not\models \neg D$

(2) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to C^* \wedge \mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg D^*$

(3) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to (C \wedge \neg D)^*$

(4) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg B^*$

Si $B = \Box C$ (i.e. $B^* = Prov(\ulcorner C^* \urcorner)$) con C cumpliendo el aserto:

Si $M_k, i \models B$:

(1) $(\forall j.iR_kj)[M_k, j \models C]$

(2) $\mathbf{PA} \vdash \bigvee_{j:iR_kj} S(\boldsymbol{j}) \to C^*$

(3) $\mathbf{PA} \vdash Prov(\ulcorner \bigvee_{j:iR_kj} S(\boldsymbol{j}) \urcorner) \to B^*$

(4) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to Prov(\ulcorner \bigvee_{j:iR_kj} S(\boldsymbol{j}) \urcorner)$

(5) $\mathbf{PA} \vdash S(\boldsymbol{i}) \to B^*$

Si $M_k, i \not\models B$:

(1) $(\exists j.iR_kj)[M_k, j \not\models C]$

(2) $\mathbf{PA} \vdash S(\boldsymbol{j}) \to \neg C^*$

(3) $\mathbf{PA} \vdash C^* \to \neg S(\boldsymbol{j})$

(4) $\mathbf{PA} \vdash Prov(\ulcorner C^* \urcorner) \to Prov(\ulcorner \neg S(\boldsymbol{j}) \urcorner)$

(5) $\mathbf{PA} \vdash \neg Prov(\ulcorner \neg S(\boldsymbol{j}) \urcorner) \to \neg Prov(\ulcorner C^* \urcorner)$

(6) $\quad \mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg Prov(\ulcorner \neg S(\boldsymbol{j}) \urcorner)$

(7) $\quad \mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg Prov(\ulcorner C^* \urcorner)$

(8) $\quad \mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg B^*$

■

Para concluir la demostración, supongamos $\mathbf{GL} \nvdash A$, entonces existe una k tal que $A_k = A$ y $M_k, w_k \nvDash A_k$. Sea $i = w_k$, por el aserto anterior $\mathbf{PA} \vdash S(\boldsymbol{i}) \to \neg A^*$ entonces $\mathbf{PA} \vdash \neg Prov(\ulcorner \neg S(\boldsymbol{i}) \urcorner) \to \neg Prov(\ulcorner A^* \urcorner)$, $0Ri$ y por el aserto $(5')$
$\mathbf{PA} \vdash S(\mathbf{0}) \to \neg Prov(\ulcorner A^* \urcorner)$. Del aserto $(2')$ y $(4')$ sacamos la conclusión de que solo existe un i tal que $S(\boldsymbol{i})$ sea verdadera, y del aserto 7' concluimos que $i = 0$ por lo tanto $S(\mathbf{0})$ es verdadera y A^* no demostrable.

■

Capítulo 5

El teorema del punto fijo

En este capítulo daremos una demostración semántica del teorema del punto fijo para el sistema modal **GL** basándonos en el trabajo de Lisa Reidhaar-Olson en [Rei89].

Supondremos que todo modelo $M = \langle W, R, V \rangle$ es finito, transitivo e irreflexivo. Supongamos que existen $w_0, \ldots, w_n \in W$ tal que $w_n R w_{n-1} R \ldots R w_0$. Debido a la transitividad e irreflexividad, se tendrá que si $j > i$ entonces $w_j R w_i$ para $w_i \neq w_j$. De esta forma podemos comprobar que para todo mundo $w \in W$ existe un $n \in \mathbb{N}$ menor que el número de elementos de W tal que existen mundos $w_0, \ldots, w_n$ con $w = w_n R w_{n-1} R \ldots R w_0$.

Definición 5.0.1. Sea $w \in W$, definimos el rango de w $rango(w)$ como el mayor $n \in \mathbb{N}$ tal que existen mundos $w_0, \ldots, w_n$ con $w = w_n R w_{n-1} R \ldots R w_0$.

Si w es un mundo tal que no existe $x \in W$ que cumpla wRx entonces $rango(w) = 0$.

Definición 5.0.2. Dada $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$ y p una variable modal, se dirá que A está modalizada por p si y solo si cada ocurrencia de p está en el rango de $\Box$.

Definición 5.0.3. Sea $A \in \mathrm{FORM}_{\mathcal{L}_\Box}$, diremos que A es $(n+1)$-divisible si y solo si existen:

1. Una sucesión de variables modales distintas $q_0, \ldots, q_n$ que no ocurren en A.
2. Una fórmula $B(q_0, \ldots, q_n)$ que contiene a $q_0, \ldots, q_n$ pero no contiene a p.
3. Una sucesión de fórmulas modales distintas $D_0(p), \ldots, D_n(p)$ cada una conteniendo p, tal que $A = B(\Box D_0(p), \ldots, \Box D_n(p))$.

Se dirá que A es 0-divisible si existe una fórmula B que no contiene a p y $A = B$.

Si A está modalizada por p entonces existe un $k \in \mathbb{N}$ para el cual A es k-divisible.

Ejemplo. Sea $A = \Box(q \to \Box p) \vee \Box\Box(\Box p \wedge q)$, $C_0(p) = q \to \Box p, C_1(p) = \Box(\Box p \wedge q), B(q_0, q_1) = q_0 \vee q_1$ por lo tanto A es 2-divisible.
También A puede ser 1-divisible de la siguiente forma $C_0(p) = p, B(q_0) = \Box(q \to q_0) \vee \Box\Box(q_0 \wedge q)$.

Recordemos que $\boxdot A$ se define como $\Box A \wedge A$.

Lema 5.1. *Sea $M = \langle W, R, V\rangle$ un modelo, $w \in W$ y $A \in FORM_{\mathcal{L}_\Box}$, si $M, w \vDash \Box A$ entonces para todo mundo $x \in W$ tal que wRx se cumple que $M, x \vDash \Box A$.*
Además $M, x \vDash \boxdot A$.

Demostración.

Suponemos $M, w \vDash \Box A$, sean $x, y \in W$ con wRx y xRy, por transitividad wRy y $M, y \vDash A$, como y es arbitrario se tiene $M, x \vDash \Box A$ y así $M, x \vDash \boxdot A$.

■

Lema 5.2. *Sea $M = \langle W, R, V\rangle$ un modelo, $w \in W$ y $A \in FORM_{\mathcal{L}_\Box}$, si $M, w \nvDash \Box A$ entonces existe un mundo x con wRx tal que $M, x \nvDash A$ y $M, x \vDash \Box A$.*

Demostración.

Supongamos que $M, w \nvDash \Box A$, por definición existe un mundo $x \in W$ con wRx y elegimos a x el de menor rango que cumpla $M, x \nvDash A$. Sea $y \in W$ que cumpla xRy, como x es de rango menor se tiene que $M, y \vDash A$ y como y se eligió de forma arbitraria se tiene que $M, x \vDash \Box A$.

■

Lema 5.3 (Lema de la sustitución semántica)**.** *Dadas $A, B, C \in FORM_{\mathcal{L}_\Box}$ se tiene que $\boxdot(B \leftrightarrow C) \to (A(B) \leftrightarrow A(C))$ es válida.*

Demostración.

Lo demostraremos en la complejidad de A, solo haremos el caso estrictamente modal, la demostración completa se hace de forma similar a demostraciones por complejidad ya realizadas en capítulos anteriores.

Supongamos que $A = \Box D$ con $\boxdot(B \leftrightarrow C) \to (D(B) \leftrightarrow D(C))$ válida. Sea M un modelo y w un mundo en W, supongamos la existencia de un mundo $x \in W$ tan que wRx. Si $M, w \vDash \boxdot(B \leftrightarrow C)$ por el Lema 5.1 se tiene que $M, x \vDash \boxdot(B \leftrightarrow C)$ y por hipótesis $M, x \vDash D(B) \leftrightarrow D(C)$. Como x es un mundo arbitrario entonces $M, w \vDash \Box(D(B) \leftrightarrow D(C))$ y por el Lema 2.7 se tiene finalmente $M, w \vDash \Box D(B) \leftrightarrow \Box D(C)$

■

Definición 5.0.4. Dado un mundo $w \in W$ definimos $acc(w) = \{y \in W : wRy\}$.

A continuación demostraremos el teorema del punto fijo, cuya demostración nos dará el algoritmo a seguir para calcular puntos fijos de fórmulas modales.

Teorema 5.4 (Teorema del punto fijo)**.** *Dada $A \in FORM_{\mathcal{L}_\Box}$ modalizada por p existe $H \in FORM_{\mathcal{L}_\Box}$ que contiene solo las variables modales que contiene A, no conteniendo a p y cumpliendo*

$$\mathbf{GL} \vdash \boxdot(p \leftrightarrow A) \to (p \leftrightarrow H)$$

Diremos que H es un punto fijo de A

Demostración.

Haremos la demostración por inducción en la divisibilidad de A. Si A es 0-divisible, entonces existe H fórmula modal que no contiene a p y $A = H$ y A es un punto fijo de sí misma.

Supongamos que toda fórmula modal n-divisible tiene un punto fijo, si A es $(n+1)$-divisible entonces existen $B(q_0, \ldots, q_n), C_0(p), \ldots, C_n(p)$ tal que:

$$A = B(\Box C_0(p), \ldots, \Box C_n(p))$$

Para cada $0 \leq i \leq n$ definimos:

$$A_i = B(\Box C_0(p), \ldots, \Box C_{i-1}(p), \top, \Box C_{i+1}(p), \ldots, \Box C_n(p)$$

Cada A_i es n-divisible, por lo que cada una tiene un punto fijo H_i, definimos $H = B(\Box C_0(H_0), \ldots, \Box C_n(H_n))$, a continuación veremos que H va a ser el punto fijo de A.

Aserto 17. Para todo $0 \leq i \leq n$ se cumple:

$$\mathbf{GL} \vdash \boxdot(p \leftrightarrow A) \to \boxdot(\Box C_i(p) \leftrightarrow \Box C_i(H_i))$$

Demostración.

Por la completitud de **GL** basta con probar que para todo modelo $M = \langle W, R, V \rangle$ y para todo mundo $w \in W$ se tiene que

$$M, w \vDash \boxdot(p \leftrightarrow A) \to \boxdot(\Box C_i(p) \leftrightarrow \Box C_i(H_i))$$

Fijémonos que demostrar $M, w \vDash \boxdot(\Box C_i(p) \leftrightarrow \Box C_i(H_i))$ es equivalente a demostrar, para todo mundo $x \in acc(w) \cup \{w\}$ que $M, x \vDash \Box C_i(p) \leftrightarrow \Box C_i(H_i)$. Por lo tanto, fijemos i y sea $x \in acc(w) \cup \{w\}$.

(1)	$M, w \vDash \boxdot(p \leftrightarrow A)$	Suposición
(2)	$M, x \vDash \Box C_i(p)$	Suposición
(3)	$M, x \vDash \Box C_i(p) \leftrightarrow \top$	Consecuencia lógica; (2)
(4)	Para todo y con xRy se tiene: $M, y \vDash \Box C_i(p)$	Lema 5.1; (2)

	(5)	$M, y \models \Box C_i(p) \leftrightarrow \top$	Consecuencia lógica; (4)
	(6)	$M, x \models \Box(\Box C_i(p) \leftrightarrow \top)$	Cálculo modal; (5)
	(7)	$M, x \models \boxdot(\Box C_i(p) \leftrightarrow \top)$	Definición de $\boxdot$; $(3), (6)$
	(8)	$M, x \models A_i \leftrightarrow A$	Lema 5.3; (7)
	(9)	$M, w \models \Box(A_i \leftrightarrow A)$	Cálculo modal; (8)
	(10)	$M, x \models \boxdot(A_i \leftrightarrow A)$	Lema 5.1; (9)
	(11)	$M, x \models \boxdot(p \leftrightarrow A)$	Lema 5.1; (1)
	(12)	$M, x \models \boxdot(p \leftrightarrow A_i)$	Cálculo modal; $(10), (11)$
	(13)	$M, x \models (p \leftrightarrow H_i)$	Hipótesis de inducción; (12)
	(14)	$M, w \models \Box(p \leftrightarrow H_i)$	Cálculo modal; (13)
	(15)	$M, x \models \boxdot(p \leftrightarrow H_i)$	Lema 5.1; (14)
$F1$	(16)	$M, x \models C_i(p) \leftrightarrow C_i(H_i)$	Lema 5.3; (15)
	(17)	$M, x \models \Box C_i(p) \leftrightarrow \Box C_i(H_i)$	Lema 5.3; (15)

(1)	$M, w \models \boxdot(p \leftrightarrow A)$	Suposición
(2)	$M, x \not\models \Box C_i(p)$	Suposición
(3)	Existe un mundo y con xRy cumpliendo: $M, y \not\models C_i(p)$ y $M, y \models \Box C_i(p)$	Lema 5.2
(4)	$M, y \models C_i(p) \leftrightarrow C_i(H_i)$	F1
(5)	$M, y \not\models C_i(H_i)$	Consecuencia lógica; $(3), (4)$
(6)	$M, x \not\models \Box C_i(H_i)$	Cálculo modal; (5)
(7)	$M, x \models \Box C_i(H_i) \rightarrow \Box C_i(p)$	Consecuencia lógica; (6)
(8)	$M, x \models \Box C_i(p) \leftrightarrow \Box C_i(H_i)$	Consecuencia lógica; $(2), (7)$

Por definición de $\boxdot$ concluimos el resultado.

■

Sean $M = \langle W, R, V \rangle$ y $w \in W$ con $M, w \models \boxdot(p \leftrightarrow A)$. Por el Aserto 17 se tiene para todo $0 \leq i \leq n$ $M, w \models \boxdot(\Box C_i(p) \leftrightarrow \Box C_i(H_i))$. Aplicando el teorema semántico de sustitución $n+1$ veces:

$$M, w \vDash \boxdot(p \leftrightarrow A) \rightarrow (B(\Box C_0(p), \ldots, \Box C_n(p)) \leftrightarrow B(\Box C_0(H_0), \ldots, \Box C_n(H_n)))$$

Esto es:

$$M, w \vDash \boxdot(p \leftrightarrow A) \rightarrow (A \leftrightarrow H)$$

Como M y w fueron escogidos de forma arbitraria, por completitud se tiene

$$\mathbf{GL} \vdash \boxdot(p \leftrightarrow A) \rightarrow (A \leftrightarrow H)$$

■

Teorema 5.5. *Sea $A(p)$ modalizada por p y sea H un punto fijo de A, entonces* $\mathbf{GL} \vdash \boxdot(p \leftrightarrow D) \rightarrow (p \leftrightarrow A)$

Demostración.

Supongamos que $M = \langle W, R, V \rangle$ es un modelo donde $\boxdot(p \leftrightarrow H) \rightarrow (p \leftrightarrow A)$ no es válido. Sea $w \in W$ un mundo de mínimo rango en M cumpliendo

$$M, w \vDash \boxdot(p \leftrightarrow H) \text{ y } M, w \nvDash p \leftrightarrow A$$

Sea $x \in W$ con wRx, por ser w de rango mínimo se tiene que $M, x \vDash p \leftrightarrow A$ y entonces $M, w \vDash \Box(p \leftrightarrow A)$. Definimos ahora V' como $wV'p$ si y solo si $\neg(wVp)$ y sea $M' = \langle W, R, V' \rangle$. Por inducción en la complejidad de las fórmulas se tiene que para toda fórmula modal D y para todo mundo $x \in W$ con wRx:

$$M, w \vDash D \text{ si y solo si } M', w \vDash D$$

De esta forma se tiene que $M, w \vDash \Box D$ si y solo si $M', w \vDash \Box D$, debido a esto $M', w \vDash \Box(p \leftrightarrow A)$, además para toda variable modal q distinta de p se tiene que $M, w \vDash q$ si y solo si $M', w \vDash q$.

Gracias a que p no ocurre en H y A está modalizada por p, el valor de verdad de p en w no afecta al valor de verdad de H y de A en w, por lo tanto $M, w \vDash H$ si y solo si $M', w \vDash H$ y $M, w \vDash A$ si y solo si $M', w \vDash A$. Como $M, w \nvDash (p \leftrightarrow A)$ y $M, w \vDash (p \leftrightarrow H)$ entonces $M', w \vDash (p \leftrightarrow A)$ y $M', w \nvDash (p \leftrightarrow H)$. De esta forma $M', w \vDash \boxdot(p \leftrightarrow A)$ pero por el Teorema del punto fijo $M', w \vDash (p \leftrightarrow H)$ que contradice el resultado y por completitud se tiene el teorema.

■

Teorema 5.6. *Sea $A(p)$ modalizada por p y sea H un punto fijo de A, entonces* $\mathbf{GL} \vdash H \leftrightarrow A(H)$

Demostración.

Por el Aserto 17 y el Teorema 5.5, el resultado de sustituir p por H en $\boxdot(p \leftrightarrow H) \rightarrow (p \leftrightarrow A)$ es un teorema de $\mathbf{GL}$, así $\mathbf{GL} \vdash \boxdot(H \leftrightarrow H) \rightarrow (H \leftrightarrow A)$ y como $\mathbf{GL} \vdash \boxdot(H \leftrightarrow H)$ tenemos $\mathbf{GL} \vdash H \leftrightarrow A(H)$.

■

Bibliografía

[Bal21] Roberta Ballarin. “Modern Origins of Modal Logic”. In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Fall 2021. Metaphysics Research Lab, Stanford University, 2021.

[Boo95] George Boolos. *The Logic of Provability*. Cambridge University Press, 1995. ISBN: 9780521483254.

[Dea21] Walter Dean. *Recursive Functions*. 2021. URL: `https://plato.stanford.edu/archives/win2021/entries/recursive-functions`.

[Gar21] James Garson. “Modal Logic”. In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Summer 2021. Metaphysics Research Lab, Stanford University, 2021.

[Gir10] Rod Girle. *Modal Logics and Philosophy; 2nd ed. edition*. McGill-Queen’s University Press, 2010. ISBN: 9780773536531.

[Ivo] Carlos Ivorra. *Lógica Matemática*. URL: `https://www.uv.es/ivorra/Libros/LM.pdf`.

[Lew12] C. I. Lewis. “IV.—Implication and the algebra of logic”. In: *Mind* XXI.84 (Jan. 1912), pp. 522–531. ISSN: 0026-4423. DOI: `10.1093/mind/XXI.84.522`.

[Mac80] Hugh MacColl. “Symbolic Reasoning (I-VIII)”. In: *Mind* (1880).

[Mar16] Edwin Mares. In: *The Bulletin of Symbolic Logic* 22.2 (2016), pp. 289–291. ISSN: 10798986. URL: `http://www.jstor.org/stable/43830162`.

[Mon76] J. Donald Monk. *Mathematical Logic*. Springer, 1976. ISBN: 9781468494549.

[Rei89] Lisa Reidhaar-Olson. “A new proof of the fixed-point theorem of provability logic.” In: *Notre Dame Journal of Formal Logic* 31.1 (1989), pp. 37–43. DOI: `10.1305/ndjfl/1093635331`. URL: `https://doi.org/10.1305/ndjfl/1093635331`.

[Sha13] Amit Shah. “Solovay’s Arithmetical Completeness Theorem for Provability Logic”. PhD thesis. Apr. 2013.

[Smo85] C. Smoryński. *Modal Logics and Philosophy*. Springer, 1985. ISBN: 9780387962092.

[Sol76] R.M Solovay. “Provability interpretations of modal logic”. In: *Israel J. Math* (1976). DOI: `https://doi.org/10.1007/BF02757006`.

[Ver17] Rineke (L.C.) Verbrugge. "Provability Logic". In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Fall 2017. Metaphysics Research Lab, Stanford University, 2017.

[Zac19] Richard Zach. *Incompleteness and Computability*. Open Logic Project. 2019. ISBN: 9781077323391.