Subsistemas de la Aritmética de Segundo Orden y Matemática Inversa

Borja Sierra Miranda

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por
Andrés Cordón Franco

Especiales agradecimientos a:

Mis padres, Guillermo y Concha, por apoyarme y ayudarme en todas mis decisiones.

Mi profesor, José Carlos, por descubrirme e invitarme al paraíso de las matemáticas.

Mi tutor, Andrés Cordón, por guiarme en el camino para recorrer dicho paraíso.

Resumen

Este trabajo de fin de grado consiste en una introducción a la matemática inversa. En él introduciremos la aritmética de segundo orden y nos centraremos en el estudio de los subsistemas $\mathrm{RCA}_0, \mathrm{WKL}_0, \mathrm{ACA}_0, \mathrm{ATR}_0$ y Π^1_1-CA_0, los llamados "Big Five". En RCA_0 desarrollaremos una codificación de la matemática y usaremos RCA_0 como teoría base para demostrar la equivalencia de ciertos teoremas de las matemáticas con alguno de los restantes subsistemas. Además, estudiaremos la parte de primer orden de los tres primeros subsistemas y hablaremos de cómo usar la matemática inversa para obtener una realización parcial del programa de Hilbert.

Abstract

This final degree project is an introduction to reverse mathematics. We will introduce second order arithmetic and we will focus on the study of the subsystems RCA_0, WKL_0, ACA_0, ATR_0 and Π^1_1-CA_0, which are called the Big Five. We will develop a coding of mathematics inside RCA_0 and we will use RCA_0 as a base theory to prove equivalences between some mathematical theorems and the other subsystems. In addition, we will study the first order part of the first three subsystems and we will explain how to use reverse mathematics to obtain a partial realization of Hilbert's program.

Índice general

Introducción

El programa de la matemática inversa es un programa de investigación bien establecido en el campo de la lógica matemática y de los fundamentos de la matemática iniciado en los años 1970 por H. Friedman y S. Simpson. La pregunta central que inicia el área de la matemática inversa es la siguiente:

¿Qué axiomas de existencia de conjuntos son necesarios para hacer matemáticas?

Para ser más específicos, nos referimos al proceso siguiente. El objetivo primordial es usar las herramientas de la lógica matemática para calibrar la *potencia lógica* de un determinado teorema de las matemáticas, A. Para ello, escogemos ciertas teorías que, mediante codificaciones adecuadas, permitan desarrollar la matemática en ellas.[1] Necesitamos también fijar una teoría base, llamémosla T_0, que sea una subteoría de todas las teorías consideradas. El problema central es el siguiente: dada la codificación de un teorema matemático A en el lenguaje de la teoría base T_0, encontrar una teoría T que cumpla que i) $T \vdash A$, y ii) $T_0 + A \vdash T$. Esto es, sobre T_0, el teorema A y los nuevos axiomas necesarios para demostrarlo son equivalentes. De esta manera, se tendría que los axiomas de existencia que conforman la teoría T no se pueden evitar en una prueba de A y, en este sentido, son los axiomas "correctos" para demostrar el teorema matemático A. Estamos invirtiendo pues el proceso estándar en matemáticas al demostrar un axioma a partir de algún teorema. Esto da el nombre de *matemáticas inversas* al tema.

Distintas elecciones de las teorías T, T_0 y del tipo de resultados matemáticos A considerados dan a lugar a distintas aproximaciones al problema central arriba descrito. En el caso de la matemática inversa, las matemáticas ordinarias del día a día (es decir, las que tratan con objetos numerables o separables, independientes del desarrollo de conceptos abstractos elevados de la Teoría de Conjuntos) se formalizan en el lenguaje de la

[1] La teoría de conjuntos ZFC es la elección estándar para desarrollar las matemáticas en la actualidad. Mas, mediante codificaciones adecuadas, pueden usarse otras teorías para este propósito. De hecho, notemos que en ZFC también se está llevando a cabo una codificación de los conceptos mátematicos, puesto que sería extraño pensar que, por ejemplo, el número natural 1 es *realmente* el conjunto $\{\varnothing\}$ o que *realmente* $1 \in 2$; y no, que esos hechos son consecuencias de estar realizando una determinada codificación de esos conceptos.

aritmética de segundo orden Z_2 (un sistema formal diseñado para tratar con números naturales y subconjuntos de números naturales) y, a continuación, los teoremas centrales de las matemáticas ordinarias se demuestran en subsistemas convenientes de la aritmética de segundo orden. Estos subsistemas se axiomatizan típicamente sobre una determinada teoría base mediante formas restringidas del Axioma de Comprensión (CA) u otros principios de existencia de conjuntos.

Forman parte pues del campo de estudio de la matemática inversa las matemáticas que tratan con objetos numerables o con objetos que pueden ser caracterizados por objetos matemáticos numerables. Un ejemplo de esto último serían los espacios métricos separables, ya que podemos recuperar los puntos de ese espacio métrico tomando las sucesiones de Cauchy de los elementos del subconjunto denso numerable. Así, por ejemplo, la recta real $\mathbb{R}$ entraría dentro del campo de estudio de la matemática inversa. De manera análoga, resultados fundamentales de geometría, teoría de números, cálculo, ecuaciones diferenciales, análisis real y complejo, álgebra numerable, topología de los espacios métricos separables, lógica matemática o computabilidad están representados en el estudio de la matemática inversa.

Cabe destacar que, aunque la matemática inversa se suela centrar en esas teorías y en esos teoremas arriba mencionados, el problema central descrito anteriormente es más general, y, por ejemplo, Friedman [2] propuso un programa que llamó "Strict Reverse Mathematics" donde una de las ideas que plantea es cambiar los subsistemas de Z_2 por unas teorías "puramente matemáticas" (como hemos mencionado, los subsistemas de Z_2 están caracterizadas por principios lógico-matemáticos, como la comprensión para cierto tipo de conjuntos, y Friedman propone considerar en su lugar teorías con axiomas puramente matemáticos). No entramos en más detalle pues esta aproximación está fuera del alcance de este texto.

Los subsistemas "Big Five"

Habiendo descrito las particularidades habituales en la matemática inversa, destaquemos uno de sus hechos más sorprendentes. A priori uno podría pensar que, con la variedad de teoremas existentes en las mátematicas, sería necesario tener muchas teorías para poder encontrar equivalentes a los teoremas y que muchas de esas teorías resultarían además incomparables entre sí. Aunque esto sea en parte cierto, la investigación en el campo ha puesto de manifiesto que solo unos pocos axiomas específicos de existencia de conjuntos surgen repetidamente en este contexto (las llamadas teorías "big five"de la Matemática Inversa), a saber, RCA_0 (axiomatizada por Axiomas de Comprensión Recursiva), el Lema Débil de König WKL_0, Comprensión Aritmética ACA_0, Recursión Aritmética Transfinita ATR_0 y comprensión para conjuntos en el nivel Π^1_1 de la Jerarquía Aritmética Π^1_1-CA_0.

Tomando como base RCA_0, gran parte de los teoremas de la matemática no-conjuntista

resultan o bien demostrables en RCA_0 o bien equivalentes sobre RCA_0 a alguna de las otras cuatro teorías. Por eso se les dio el nombre de los "Big Five"; y su descripción y la demostración de algunos de sus equivalentes más importantes será la parte central de este texto (en particular, para las tres primeras teorías, RCA_0, WKL_0, ACA_0).

Cabe señalar también que los Big Five forman una jerarquía lineal estricta, esto es:

$$\mathrm{RCA}_0 \subset \mathrm{WKL}_0 \subset \mathrm{ACA}_0 \subset \mathrm{ATR}_0 \subset \Pi^1_1\text{-CA}_0$$

donde cada sistema es estrictamente más potente que el anterior. Como consecuencia, una gran parte de los teoremas de las matemáticas numerables del día a día pueden clasificarse en alguna de estas cinco categorías y resultan por tanto, desde el punto de vista de su potencia lógica, comparables entre sí.

Como indica Simpson en [8], cada uno de estos subsistemas se puede identificar con diversos programas de fundamentos de las matemáticas. Resumidos en una tabla, quedaría:

Teoría	Programa	Impulsor(es)
RCA_0	Constructivismo	Bishop
WKL_0	Reduccionismo finitista	Hilbert
ACA_0	Predicativismo	Weyl, Feferman
ATR_0	Reduccionismo predicativista	Friedman, Simpson
$\Pi^1_1\text{-CA}_0$	Impredicativismo	Feferman y otros

También sale fuera del contenido de este trabajo el entrar en detalle en cada una de estas corrientes, pero es importante saber que el estudio de la matemática inversa puede ayudarnos a entender mejor cada uno de estos programas.

Contenidos del trabajo

Este trabajo consta de la presente Introducción, seis capítulos y unas conclusiones. Exponemos brevemente de qué tratará cada uno de los capítulos.

En el capítulo 1, **Lenguaje de la aritmética de segundo orden**, introduciremos el lenguaje formal donde estarán cada una de las teorías de los Big Five, además definiremos su semántica y hablaremos de la aritmética de segundo orden, introduciendo la jerarquía aritmética.

En el capítulo 2, de título RCA_0, definiremos la teoría que usaremos como base, RCA_0. Además veremos cómo codificar las matemáticas en él, desde pares de números, funciones o conjuntos cocientes hasta los sistemas numéricos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$. Al igual que RCA_0 es nuestra teoría base, este capítulo será nuestra base para todo el desarrollo posterior. Como ejemplo de teorema matemático demostrable en RCA_0, veremos que el teorema de categorías de Baire es demostrable en esta teoría.

En el capítulo 3, de título WKL_0, definiremos la teoría WKL_0 y nos encontraremos con nuestro primer resultado estrictamente de matemática inversa, la equivalencia de WKL_0 con el teorema Heine-Borel en $[0, 1]$. Veremos también que WKL_0 es equivalente al principio de Σ^0_1 separación, lo que nos servirá en el capítulo 6.

En el capítulo 4, de título ACA_0, definiremos la teoría ACA_0 y demostraremos varios equivalentes a ella, centrándose en los números reales (estudiaremos propiedades de completitud secuencial en $\mathbb{R}$ en ACA_0) y en la combinatoria infinita (estudiaremos el lema de Köning y el teorema de Ramsey en ACA_0).

En el capítulo 5, de título ATR_0 **y** Π^1_1-CA_0, introduciremos estas dos teorías para completar los "Big Five". Nos centraremos en la definición de ATR_0 y sus propiedades básicas. Un análisis detallado de estas teorías excede los contenidos del presente trabajo.

Finalmente, en el capítulo 6, **Algunos resultados metateorícos**, hablaremos de la parte de primer orden de las tres primeras teorías RCA_0, WKL_0 y ACA_0; y daremos una idea detallada de un prominente resultado de conservación para WKL_0: WKL_0 es conservativa sobre la aritmética primitivo recursiva PRA para fórmulas Π_2. Además, explicaremos cómo este resultado de conservación relaciona WKL_0 con el programa de Hilbert.

Desde el punto de vista bibliográfico, la principal referencia en la que se basa el presente trabajo es el libro de S.G. Simpson [8], la referencia estándar para el estudio de los subsistemas de la aritmética de segundo orden en la actualidad. Se han consultado también otras monografías sobre el tema ([10],[3]), así como otras referencias más particulares para recabar información sobre algún aspecto concreto del trabajo.

Sobre las demostraciones

Como se apreciará más adelante, gran parte de las demostraciones de este texto se han procurado hacer en un estilo más formal que de costumbre. Esta decisión ha sido motivada por la importancia actual de los asistentes de la demostración (se puede ver en los mensajes en FOM [9] en los meses de Mayo de 2020, Febrero de 2021 y Marzo de 2021) y por un artículo de Leslie Lamport [6]. En particular, se ha seguido los consejos de este artículo para hacer demostraciones estructuradas. Para que se entienda este estilo de hacer demostraciones, sigamos el mismo ejemplo que se sigue en [6] demostrando un colorario al teorema del valor medio. El corolario es el siguiente:

Corolario. *Si $f'(x) > 0$ para toda x es un intervalo entonces f es creciente en el intervalo.*

La demostración sin estructurar (tomada del libro *Calculus* de Spivak) es:

Demostración: Sean a, b dos puntos en el intervalo tales que $a < b$. Entonces existe un

x en (a, b) tal que

$$f'(x) = \frac{f(b) - f(a)}{b - a}.$$

Pero $f'(x) > 0$ para todo x en (a, b), por tanto

$$\frac{f(b) - f(a)}{b - a} > 0.$$

Como $b - a > 0$ concluimos que $f(b) > f(a)$. □

Ahora estructuraremos la demostración. Para ello intentaremos desgranarla en varios pasos, probándolos uno a uno de forma que un paso sólo dependa de los anteriores (o de teoremas ya demostrados). Cuando se crea conveniente, se podrá crear una subdemostración para un paso, que tenga pasos propios, creando así varios niveles en la demostración. Cada paso tendrá una etiqueta de la forma $\langle n \rangle m$ con $n, m \in \mathbb{N}^+$, la primera indica el nivel de profundidad de la demostración y la segunda el número del paso en la demostración. Así por ejemplo si estamos en un paso con la etiqueta $\langle 2 \rangle 3$ y creamos una nueva demostración, el primer paso de la nueva demostración será $\langle 3 \rangle 1$, pues es el primer paso de una demostracón en un nivel más profundo. Permitiremos a un paso depender de los pasos anteriores, siempre que estos estén en la misma demostración o en las demostraciones en las que el paso está anidado. Para que quede más claro, pongamos un ejemplo. Supongamos que tenemos una demostración de la forma (a cada paso le hemos puesto una letra para poder referirnos a ellos):

DEMOSTRACIÓN:

⟨1⟩1. A

⟨1⟩2. B

  ⟨2⟩1. C

    ⟨3⟩1. D

    ⟨3⟩2. E

    ⟨3⟩3. F

  ⟨2⟩2. G

  ⟨2⟩3. H

⟨1⟩3. I

  ⟨2⟩1. J

  ⟨2⟩2. K

    ⟨3⟩1. L

    ⟨3⟩2. M

  ⟨2⟩3. N

Por ejemplo el paso E claramente puede depender del paso D (pues es uno anterior en la misma demostración), pero también del paso A (pues es un paso anterior en una demostración a la que está anidado). En particular E puede depender de A, B y D (no puede depender C pues se supone que D, E, F es lo que demuestra C). Siguiendo los mismos razonamientos, el paso M puede depender de lo demostrado en A, B, J, L, no puede depender ni de I ni de K porque K se demuestra con L y M, y I con J, K (que incluye a M) y N. Tampoco podrá depender de los pasos C, D, E, F, G, H, pues todos pertenecen a demostraciones a la que no está anidada M (son demostraciones que ya han terminado, sus pasos no deben ser ya mencionados, lo que aportan esos pasos es que han demostrado B). Esto nos permite que aunque haya dos etiquetas $\langle 2\rangle 1$, una para el paso C y otra para el paso J, si en la demostración de M hacemos referencia al paso $\langle 2\rangle 1$ sabemos que nos referimos a J, pues C ya no se puede usar en M. Por último tomaremos el convenio de que cada último paso de una demostración sea de la forma Q.E.D. y lo que afirma es que lo que se quería demostrar ha sido demostrado. Así el esquema anterior quedaría como:

DEMOSTRACIÓN:
⟨1⟩1. A

⟨1⟩2. B

  ⟨2⟩1. C

    ⟨3⟩1. D

    ⟨3⟩2. E

    ⟨3⟩3. Q.E.D.

  ⟨2⟩2. G

  ⟨2⟩3. Q.E.D.

⟨1⟩3. Q.E.D.

  ⟨2⟩1. J

  ⟨2⟩2. K

    ⟨3⟩1. L

    ⟨3⟩2. Q.E.D.

  ⟨2⟩3. Q.E.D.

Finalizamos la introducción viendo cómo se estructuraría la demostración del colorario anterior:

DEMOSTRACIÓN:
⟨1⟩1. Sean a y b puntos del intervalo tales que $a < b$.
Es suficiente probar que $f(b) > f(a)$.

DEMOSTRACIÓN: Por definifición de función creciente.

⟨1⟩2. Existe x en (a, b) con $f'(x) = \dfrac{f(b) - f(a)}{b - a}$.

⟨2⟩1. f es diferenciable en $[a, b]$.

DEMOSTRACIÓN: Por ⟨1⟩1, ya que f es derivable en I por hipótesis.

⟨2⟩2. f es continua en $[a, b]$.

DEMOSTRACIÓN: Por ⟨2⟩1 y porque derivable implica continua (probado en un teorema anterior).

⟨2⟩3. Q.E.D.

DEMOSTRACIÓN: Por ⟨2⟩1 y ⟨2⟩2 y el teorema del valor medio.

⟨1⟩3. $f'(x) > 0$ para todo x en (a, b).

DEMOSTRACIÓN: Por hipótesis del corolario y el paso ⟨1⟩1.

⟨1⟩4. $\dfrac{f(b) - f(a)}{b - a} > 0$

DEMOSTRACIÓN: Por ⟨1⟩2 y ⟨1⟩3.

⟨1⟩5. Q.E.D.

DEMOSTRACIÓN: ⟨1⟩1 $b - a > 0$, por tanto ⟨1⟩4 implica que $f(b) - f(a) > 0$, por tanto $f(b) > f(a)$. Por ⟨1⟩1 esto demuestra el corolario.

□

Capítulo 1

Lenguaje de la aritmética de segundo orden

Puesto que vamos a trabajar en subsistemas formales de la aritmética de segundo orden, a partir de ahora Z_2, necesitamos definir primero el lenguaje formal de Z_2, al que llamaremos L_2.

Definición 1.1. El *lenguaje de la aritmética de segundo orden*, denotado L_2, consiste en los siguientes símbolos:

- Una cantidad infinita numerable de *variables numéricas*.
- Una cantidad infinita numerable de *variables de conjuntos*.
- Los *operadores lógicos* $\neg, \wedge, \vee, \rightarrow$.
- Los *cuantificadores* $\forall, \exists$.
- La *igualdad* $=$.
- Los *símbolos de constante* $0, 1$.
- Los *símbolos de función* $+, \cdot$.
- Los *símbolos de relación* $=, <, \in$.

Al conjunto de las variables numéricas lo denotaremos $\mathrm{Var_N}$ y al de variables conjuntistas, $\mathrm{Var_C}$. A la unión de ambos lo denotamos $\mathrm{Var} = \mathrm{Var_N} \cup \mathrm{Var_C}$ y a sus elementos los llamamos variables.

Notemos que al haber dos categorías distintas de variables, estamos trabajando en un lenguaje con dos tipos de términos, los que representarán números (en un sentido amplio de la palabra) y los que representarán conjuntos de dichos números. ■

Notación. Usaremos, con o sin subíndices, las siguientes variables sintácticas:

1. $x, y, z, \ldots$ para designar variables numéricas.
2. $X, Y, Z, \ldots$ para designar variables de conjuntos.
3. ν para designar cualquier tipo de variable.

■

Definimos ahora la noción de modelo de L_2, porque así luego podremos definir los términos y las fórmulas no solo para L_2 sino para L_2 ampliado con constantes de cualquier modelo.

Definición 1.2. Un *modelo de* L_2 es una 7-tupla ordenada

$$\mathfrak{M} = (M, \mathcal{S}_{\mathfrak{M}}, +_{\mathfrak{M}}, \cdot_{\mathfrak{M}}, 0_{\mathfrak{M}}, 1_{\mathfrak{M}}, <_{\mathfrak{M}})$$

donde

1. M es un conjunto no vacío.
2. $\mathcal{S}_{\mathfrak{M}}$ es un conjunto de subconjuntos de M no vacío y disjunto de M.
3. $+_{\mathfrak{M}}, \cdot_{\mathfrak{M}}$ son operaciones binarias en M.
4. $0_{\mathfrak{M}}, 1_{\mathfrak{M}}$ son elementos de M.
5. $<_{\mathfrak{M}}$ es una relación binaria en M.

■

Nota. Para distinguir sintáxis de semántica acostumbraremos a escribir los elementos del modelo, ya sean los de M o los de $\mathcal{S}_{\mathfrak{M}}$, en negrita, i.e. $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots$ ■

Nota. Notemos que $\in$ es tanto un símbolo de nuestro lenguaje objeto como de nuestro metalenguaje. Intentaremos usarlo sin crear confusión, y aclararlo en los momentos donde pueda ser ambiguo. ■

Vamos a definir ahora los distintos conjuntos de expresiones asociados a L_2. Para la definición asumiremos que L_2 ha sido expandido con constantes que hagan referencia a los elementos en un conjunto $\mathcal{B}$, contenido este conjunto en un modelo. Si queremos únicamente las expresiones asociadas a L_2 nos podemos olvidar del modelo y escoger $\mathcal{B} = \varnothing$.

Definición 1.3. Sea $\mathfrak{M}$ un modelo de L_2, sea $\mathcal{B} \subseteq M \cup \mathcal{S}_{\mathfrak{M}}$. Definimos el lenguaje $L_2(\mathcal{B})$ como el lenguaje L_2 extendido con una nueva constante $c_{\mathbf{a}}$ por cada elemento $\mathbf{a} \in \mathcal{B}$. El lenguaje $L_2(M \cup \mathcal{S}_{\mathfrak{M}})$ será denotado como $L_2(\mathfrak{M})$. ■

Definición 1.4. Sea $\mathfrak{M}$ un modelo, y $\mathcal{B} \subseteq M \cup \mathcal{S}_{\mathfrak{M}}$. Definimos los siguientes conjuntos de expresiones de $L_2(\mathcal{B})$:

1. *Términos numéricos*: El conjuntos de los términos numéricos, denotado como $\mathrm{TNum}(\mathcal{B})$, se define recursivamente como:
   a) $0 \in \mathrm{TNum}(\mathcal{B})$ y $1 \in \mathrm{TNum}(\mathcal{B})$.
   b) $\mathrm{Var_N} \subseteq \mathrm{TNum}(\mathcal{B})$.
   c) Para todo $\mathbf{a} \in \mathcal{B} \cap M$, $c_{\mathbf{a}} \in \mathrm{TNum}(\mathcal{B})$.
   d) Si $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$, entonces $+t_1t_2 \in \mathrm{TNum}(\mathcal{B})$ y $\cdot t_1t_2 \in \mathrm{TNum}(\mathcal{B})$.
2. *Términos conjuntistas*: El conjunto de los términos conjuntistas, denotado como $\mathrm{TSet}(\mathcal{B})$, se define como:
   a) $\mathrm{Var_C} \subseteq \mathrm{TSet}(\mathcal{B})$.
   b) Para todo $\mathbf{a} \in \mathcal{B} \cap \mathcal{S}_M$, $c_{\mathbf{a}} \in \mathrm{TSet}(\mathcal{B})$.
3. *Términos*: El conjunto de los términos, denotado como $\mathrm{Term}(\mathcal{B})$, se define como $\mathrm{Term}(\mathcal{B}) = \mathrm{TNum}(\mathcal{B}) \cup \mathrm{TSet}(\mathcal{B})$.
4. *Fórmulas atómicas*: El conjunto de las fórmulas atómicas, denotado por $\mathrm{Atom}(\mathcal{B})$, se define como:
   a) Si $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$, entonces $= t_1t_2 \in \mathrm{Atom}(\mathcal{B})$ y $< t_1t_2 \in \mathrm{Atom}(\mathcal{B})$.
   b) Si $t_1 \in \mathrm{TNum}(\mathcal{B})$ y $t_2 \in \mathrm{TSet}(\mathcal{B})$ entonces $(\in t_1t_2) \in \mathrm{Atom}(\mathcal{B})$ (los paréntesis son únicamente para notar donde empieza y acaba la fórmula y no es parte de esta, ya que nuestro lenguaje no contiene paréntesis).
5. *Fórmulas*: El conjunto de las fórmulas, denotado por $\mathrm{Form}(\mathcal{B})$, se define recursivamente como:
   a) $\mathrm{Atom}(\mathcal{B}) \subseteq \mathrm{Form}(\mathcal{B})$.
   b) Si $\varphi \in \mathrm{Form}(\mathcal{B})$, entonces $\neg\varphi \in \mathrm{Form}(\mathcal{B})$.
   c) Si $\varphi, \psi \in \mathrm{Form}(\mathcal{B})$, entonces $\vee\varphi\psi \in \mathrm{Form}(\mathcal{B})$, $\wedge\varphi\psi \in \mathrm{Form}(\mathcal{B})$, $\rightarrow \varphi\psi \in \mathrm{Form}(\mathcal{B})$.
   d) Si $\varphi \in \mathrm{Form}(\mathcal{B})$ es una fórmula y ν es una variable, entonces $\forall\nu.\varphi \in \mathrm{Form}(\mathcal{B})$, $\exists\nu.\varphi \in \mathrm{Form}(\mathcal{B})$.

■

Notación. En el caso de que estemos trabajando con las expresiones asociadas a L_2 no será necesario añadir $\varnothing$ al final de cada conjunto. Por ejemplo, los términos numéricos de L_2 se denotan como TNum, no como $\mathrm{TNum}(\varnothing)$. ■

Nota. Usaremos $\equiv$ para denotar la igualdad sintáctica de expresiones. Cuando estemos definiendo una fórmula (o una notación para una fórmula) será habitual escribir $:\equiv$ en lugar de $\equiv$. ■

Notación. Estableceremos los siguientes convenios de notación para hacer las fórmulas más legibles:

1. Aunque oficialmente nuestra notación es la notación polaca, realmente escribiremos $\varphi \vee \psi, \varphi \wedge \psi$ y $\varphi \to \psi$, usando paréntesis cuando sea necesario para evitar la ambigüedad.
2. (Si y sólo si) $\varphi \leftrightarrow \psi :\equiv (\varphi \to \psi) \wedge (\psi \to \varphi)$.
3. Como es habitual, $\wedge, \vee$ y $\to$ asociarán a la derecha.
4. Establecemos una prioridad para los símbolos lógicos, siendo de mayor prioridad a menor:
   - $\neg$.
   - $\wedge, \vee$.
   - $\to, \leftrightarrow$.
   - $\forall, \exists$.

   Así por ejemplo
   $$\neg\varphi \to \psi \equiv (\neg\varphi) \to \psi.$$
   $$\forall x.\varphi \wedge \exists y.\psi \to \theta \equiv \forall x.(\varphi \wedge \exists y.(\psi \to \theta)).$$
5. (Bloques de cuantificadores) $\forall x_1, \ldots, x_n.\varphi :\equiv \forall x_1.\cdots\forall x_n.\varphi$,
   $\exists x_1, \ldots, x_n.\varphi :\equiv \exists x_1.\cdots\exists x_n.\varphi$.
6. (Cuantificadores alternados) $\forall x_1, \ldots, x_n.\exists y_1, \ldots, y_m.\varphi :\equiv \forall x_1, \ldots, x_n.\exists y_1, \ldots, y_m.\varphi$,
   $\exists x_1, \ldots, x_n\forall y_1, \ldots, y_m.\varphi :\equiv \exists x_1, \ldots, x_n.\forall y_1, \ldots, y_m.\varphi$.
7. (Existe un único) $\exists^1 x.\varphi :\equiv \exists x.\varphi \wedge \forall y.\varphi[x \mapsto y] \to x = y$.
8. (Desigualdad) $t_1 \neq t_2 :\equiv \neg t_1 = t_2$ (en general si tenemos un símbolo de ralación binario $\sim$, primitivo o definido, $t_1 \not\sim t_2 :\equiv \neg t_1 \sim t_2$).
9. (Contenido) $X \subseteq Y :\equiv \forall n.n \in X \to n \in Y$.
10. (Igualdad de conjuntos) $X = Y :\equiv \forall n.n \in X \leftrightarrow n \in Y$

Señalar que usaremos paréntesis innecesarios para ayudar a la legibilidad de algunas fórmulas, por ejemplo escribir $(\varphi \wedge \psi) \to \theta$ en lugar de $\varphi \wedge \psi \to \theta$ para fórmulas largas nos ayudará a leerlas mejor.

■

1.1. Sustitución

En esta sección supondremos que $\mathfrak{M}$ es un modelo de L_2 y $\mathcal{B} \subseteq M \cup \mathcal{S}_{\mathfrak{M}}$. Recordemos que si no tenemos modelo y $\mathcal{B} = \varnothing$ las definiciones siguen siendo válidas.

Definición 1.5 (**Variables libres**)**.** Definimos recursivamente la función $\mathrm{Vl} : \mathrm{Term}(\mathcal{B}) \longrightarrow 2^{\mathrm{Var}}$, como:

1. $\mathrm{Vl}(\nu) = \{\nu\}$ si ν es una variable.
2. $\mathrm{Vl}(c) = \varnothing$ si c es una constante.
3. $\mathrm{Vl}(t_1 + t_2) = \mathrm{Vl}(t_1 \cdot t_2) = \mathrm{Vl}(t_1) \cup \mathrm{Vl}(t_2)$, donde $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$.

De la misma manera, definimos $\mathrm{Vl} : \mathrm{Form}(\mathcal{B}) \longrightarrow 2^{\mathrm{Var}}$ recursivamente como:

1. $\mathrm{Vl}(t_1 = t_2) = \mathrm{Vl}(t_1 < t_2) = \mathrm{Vl}(t_1) \cup \mathrm{Vl}(t_2)$, donde $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$.
2. $\mathrm{Vl}(t_1 \in t_2) = \mathrm{Vl}(t_1) \cup \mathrm{Vl}(t_2)$, donde $t_1 \in \mathrm{TNum}(\mathcal{B})$ y $t_2 \in \mathrm{TSet}(\mathcal{B})$.
3. $\mathrm{Vl}(\neg\varphi) = \mathrm{Vl}(\varphi)$, donde $\varphi \in \mathrm{Form}(\mathcal{B})$.
4. $\mathrm{Vl}(\varphi \wedge \psi) = \mathrm{Vl}(\varphi \vee \psi) = \mathrm{Vl}(\varphi \to \psi) = \mathrm{Vl}(\varphi) \cup \mathrm{Vl}(\psi)$, donde $\varphi, \psi \in \mathrm{Form}(\mathcal{B})$.
5. $\mathrm{Vl}(\forall\nu.\phi) = \mathrm{Vl}(\exists\nu.\phi) = \mathrm{Vl}(\phi) \setminus \{\nu\}$, donde $\phi \in \mathrm{Form}(\mathcal{B})$ y ν una variable.

Dado $\varphi \in \mathrm{Form}(\mathcal{B})$ decimos que ν *es una variable libre de* φ si $\nu \in \mathrm{Vl}(\varphi)$. ■

Notación. Dada un fórmula ϕ, usaremos las notaciones:

1. $\phi(\nu_1, \ldots, \nu_n)$, para indicar que $\mathrm{Vl}(\phi) \subseteq \{\nu_1, \ldots, \nu_n\}$.
2. $\phi[\nu_1, \ldots, \nu_n]$, para indicar que $\mathrm{Vl}(\phi) = \{\nu_1, \ldots, \nu_n\}$.
3. $\phi\{\nu_1, \ldots, \nu_n\}$, para indicar que $\mathrm{Vl}(\phi) \supseteq \{\nu_1, \ldots, \nu_n\}$.

■

Definición 1.6. Definimos los siguientes conjuntos, relacionados con las variables libres de una expresión:

- Los términos númericos cerrados serán los elementos del conjunto

$$\mathrm{TNum}_0(\mathcal{B}) = \{t \in \mathrm{TNum}(\mathcal{B}) \mid \mathrm{Vl}(t) = \varnothing\}.$$

- Los términos conjuntistas cerrados serán los elementos del conjunto

$$\mathrm{TSet}_0(\mathcal{B}) = \{t \in \mathrm{TSet}(\mathcal{B}) \mid \mathrm{Vl}(t) = \varnothing\}.$$

- Los términos cerrados serán los elementos del conjunto

$$\mathrm{Term}_0(\mathcal{B}) = \mathrm{TNum}_0(\mathcal{B}) \cup \mathrm{TSet}_0(\mathcal{B}).$$

- Las fórmulas cerradas o sentencias serán los elementos del conjunto

$$\mathrm{Sent}(\mathcal{B}) = \{\varphi \in \mathrm{Form}(\mathcal{B}) \mid \mathrm{Vl}(\varphi) = \varnothing\}.$$

■

Queremos ahora definir la sustitución de variables libres por un término. Sin embargo, como tenemos términos de dos tipos nos tenemos que asegurar que las sustituciones están bien tipadas, es decir, que no sustituyen una variable numérica por un término conjuntista, ni una variable conjuntista por un término numérico.

Definición 1.7 (**Sustitución bien tipada**)**.** Definimos el conjunto de sustituciones bien tipadas (con parámetros en $\mathcal{B}$) como

$$\mathrm{WSust}(\mathcal{B}) = \{h : \mathrm{Var} \to \mathrm{Term}(\mathcal{B}) \mid h(\mathrm{Var_N}) \subseteq \mathrm{TNum}(\mathcal{B}) \text{ y } h(\mathrm{Var_C}) \subseteq \mathrm{TSet}(\mathcal{B})\}.$$

■

Con esto definimos la sustitución:

Definición 1.8 (**Sustitución**)**.** Definimos la función $\mathrm{Sust} : \mathrm{Term}(\mathcal{B}) \times \mathrm{WSust}(\mathcal{B}) \longrightarrow \mathrm{Term}(\mathcal{B})$ recursivamente como:

1. $\mathrm{Sust}(\nu, h) \equiv h(\nu)$, con $\nu \in \mathrm{Var}$.
2. $\mathrm{Sust}(c, h) \equiv c$, donde c es un símbolo de constante.
3. $\mathrm{Sust}(t_1 + t_2, h) \equiv \mathrm{Sust}(t_1, h) + \mathrm{Sust}(t_2, h)$ y $\mathrm{Sust}(t_1 \cdot t_2, h) \equiv \mathrm{Sust}(t_1, h) \cdot \mathrm{Sust}(t_2, h)$, con $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$.

Notemos que para todo $h \in \mathrm{WSust}(\mathcal{B})$, $t_1 \in \mathrm{TNum}(\mathcal{B})$, $t_2 \in \mathrm{TSet}(\mathcal{B})$ se tiene que $\mathrm{Sust}(t_1, h) \in \mathrm{TNum}(\mathcal{B})$ y $\mathrm{Sust}(t_2, h) \in \mathrm{TSet}(\mathcal{B})$.

De la misma manera, definimos $\mathrm{Sust} : \mathrm{Form}(\mathcal{B}) \times \mathrm{WSust}(\mathcal{B}) \longrightarrow \mathrm{Form}(\mathcal{B})$ recursivamente como:

1. $\mathrm{Sust}(t_1 = t_2, h) \equiv \mathrm{Sust}(t_1, h) = \mathrm{Sust}(t_2, h)$, con $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$.
2. $\mathrm{Sust}(t_1 < t_2, h) \equiv \mathrm{Sust}(t_1, h) < \mathrm{Sust}(t_2, h)$, con $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$.
3. $\mathrm{Sust}(t_1 \in t_2, h) \equiv \mathrm{Sust}(t_1, h) \in \mathrm{Sust}(t_2, h)$, con $t_1 \in \mathrm{TNum}(\mathcal{B})$ y $t_2 \in \mathrm{TSet}(\mathcal{B})$.
4. $\mathrm{Sust}(\neg\varphi, h) \equiv \neg\,\mathrm{Sust}(\varphi, h)$ con $\varphi \in \mathrm{Form}(\mathcal{B})$.
5. $\mathrm{Sust}(\varphi \wedge \psi, h) \equiv \mathrm{Sust}(\varphi, h) \wedge \mathrm{Sust}(\psi, h)$ con $\varphi, \psi \in \mathrm{Form}(\mathcal{B})$.
6. $\mathrm{Sust}(\varphi \vee \psi, h) \equiv \mathrm{Sust}(\varphi, h) \vee \mathrm{Sust}(\psi, h)$ con $\varphi, \psi \in \mathrm{Form}(\mathcal{B})$.
7. $\mathrm{Sust}(\varphi \to \psi, h) \equiv \mathrm{Sust}(\varphi, h) \to \mathrm{Sust}(\psi, h)$ con $\varphi, \psi \in \mathrm{Form}(\mathcal{B})$.
8. $\mathrm{Sust}(\forall\nu.\varphi, h) \equiv \forall\nu.\,\mathrm{Sust}(\varphi, h_\nu)$ con $\nu \in \mathrm{Var}, \varphi \in \mathrm{Form}(\mathcal{B})$ y $h_\nu(\nu') = \begin{cases} h(\nu'), & \text{si } \nu' \not\equiv \nu \\ \nu, & \text{si } \nu' \equiv \nu \end{cases}$
9. $\mathrm{Sust}(\exists\nu.\varphi, h) \equiv \exists\nu.\,\mathrm{Sust}(\varphi, h_\nu)$ con $\nu \in \mathrm{Var}, \varphi \in \mathrm{Form}(\mathcal{B})$ y $h_\nu(\nu') = \begin{cases} h(\nu'), & \text{si } \nu' \not\equiv \nu \\ \nu, & \text{si } \nu' \equiv \nu \end{cases}$

■

Usaremos unas notaciones útiles para la sustitución:

Notación. Cuando la sustitución sea finita, es decir, $h : \mathrm{Var} \longrightarrow \mathrm{Term}(\mathcal{B})$ cumple que existe $\{\nu_1, \ldots, \nu_n\}$ tal que $\forall\nu \notin \{\nu_1, \ldots, \nu_n\}.h(\nu) = \nu$, denotaremos $\mathrm{Sust}(\varphi, h)$ como $\varphi[\nu_1, \ldots, \nu_n \mapsto h(\nu_1), \ldots, h(\nu_n)]$.

Notemos que esta notación no se confunde con $\phi[\nu_1, \ldots, \nu_n]$ ya que esta notación no tiene $\mapsto$.

Además si introducimos una fórmula con la notación $\varphi(\nu_1, \ldots, \nu_n)$, denotaremos $\mathrm{Sust}(\varphi, h)$ como $\varphi(h(\nu_1), \ldots, h(\nu_n))$ (de igual manera cambiando () por [] o por {}).

■

Notemos que no nos interesan todas las sustituciones, ya que algunas cambian el significado de las fórmulas. Por ejemplo, intuitivamente la fórmula

$$\exists x.y \neq x$$

quiere decir que hay algún elemento distinto de y. Sin embargo, la fórmula

$$(\exists x.y \neq x)[y \mapsto x] \equiv \exists x.x \neq x$$

quiere decir que hay un elemento distinto de sí mismo. Mientras que lo primero se cumple en cualquier modelo con 2 elementos, esta no se cumple nunca. El problema aquí es que al sustituir hay fórmulas del término nuevo que se han ligado a un cuantificador. Definamos esta noción formalmente.

Definición 1.9 (**Sustitución correcta**)**.** Sea $\varphi \in \mathrm{Form}(\mathcal{B})$ y $h \in \mathrm{WSust}(\mathcal{B})$. Diremos que h correcta en φ si la aplicación de h no genera la aparición de estancias ligadas nuevas en la fórmula.

A partir de ahora, siempre que hagamos una sustitución (salvo que se especifique lo contrario) asumiremos que la sustitución es correcta. ■

1.2. Semántica

En esta sección $\mathfrak{M}$ será un modelo de L_2.

Dado un modelo y un término cerrado de $L_2(\mathfrak{M})$, ese término denotará un elemento de $M \cup \mathcal{S}_{\mathfrak{M}}$. Es importante que el término no tenga variables libres, pues estas variables no tienen significado semántico. Definimos así la función que dado un término cerrado nos da el elemento del modelo que representa.

Definición 1.10. Definimos la función $\mathfrak{M}(\_) : \mathrm{Term}_0(\mathfrak{M}) \longrightarrow M \cup \mathcal{S}_{\mathfrak{M}}$ recursivamente como:

1. $\mathfrak{M}(c_{\mathbf{a}}) = \mathbf{a}$, para todo $\mathbf{a} \in M \cup \mathcal{S}_{\mathfrak{M}}$.
2. $\mathfrak{M}(0) = 0_{\mathfrak{M}}$.
3. $\mathfrak{M}(1) = 1_{\mathfrak{M}}$.
4. $\mathfrak{M}(t_1 + t_2) = \mathfrak{M}(t_1) +_{\mathfrak{M}} \mathfrak{M}(t_2)$, donde $t_1, t_2 \in \mathrm{TNum}(\mathfrak{A})$.
5. $\mathfrak{M}(t_1 \cdot t_2) = \mathfrak{M}(t_1) \cdot_{\mathfrak{M}} \mathfrak{M}(t_2)$, donde $t_1, t_2 \in \mathrm{TNum}(\mathfrak{A})$.

Notemos que $\mathfrak{M}(\mathrm{TNum}_0(\mathfrak{M})) \subseteq M$ y $\mathfrak{M}(\mathrm{TSet}_0(\mathfrak{M})) \subseteq \mathcal{S}_{\mathfrak{M}}$.

■

Notación. Para simplificar la notación, dado $\mathbf{a} \in M \cup \mathcal{S}_{\mathfrak{M}}$ escribiremos directamente $\mathbf{a}$ en lugar de $c_{\mathbf{a}}$. ■

Análogamente a los términos cerrados, las sentencias también tendrán interpretación en el modelo. Así cualquier modelo separará el conjunto de sentencias en dos, las verdaderas y las falsas (no verdaderas).

Definición 1.11. Por recursión en $\varphi \in \mathrm{Sent}(\mathfrak{M})$, definimos si φ es verdadera en $\mathfrak{M}$, denotado $\mathfrak{M} \vDash \varphi$, como

1. $\mathfrak{M} \vDash t_1 = t_2$ si y sólo si $\mathfrak{M}(t_1)$ es igual a $\mathfrak{M}(t_2)$ donde $t_1, t_2 \in \mathrm{TNum}_0(\mathfrak{M})$.

2. $\mathfrak{M} \vDash t_1 < t_2$ si y sólo si $\mathfrak{M}(t_1) <_{\mathfrak{M}} \mathfrak{M}(t_2)$ donde $t_1, t_2 \in \mathrm{TNum}_0(\mathfrak{M})$.
3. $\mathfrak{M} \vDash t_1 \in t_2$ si y sólo si $\mathfrak{M}(t_1)$ pertenece a $\mathfrak{M}(t_2)$ donde $t_1 \in \mathrm{TNum}_0(\mathfrak{M}), t_2 \in \mathrm{TSet}_0(\mathfrak{M})$.
4. $\mathfrak{M} \vDash \neg\varphi$ si y sólo si $\mathfrak{M} \nvDash \varphi$, donde $\varphi \in \mathrm{Sent}_0(\mathfrak{M})$.
5. $\mathfrak{M} \vDash \varphi \wedge \psi$ si y sólo si $\mathfrak{M} \vDash \varphi$ y $\mathfrak{M} \vDash \psi$, donde $\varphi, \psi \in \mathrm{Sent}_0(\mathfrak{M})$.
6. $\mathfrak{M} \vDash \varphi \vee \psi$ si y sólo si $\mathfrak{M} \vDash \varphi$ o $\mathfrak{M} \vDash \psi$, donde $\varphi, \psi \in \mathrm{Sent}_0(\mathfrak{M})$.
7. $\mathfrak{M} \vDash \varphi \to \psi$ si y sólo si $\mathfrak{M} \nvDash \varphi$ o $\mathfrak{M} \vDash \psi$, donde $\varphi, \psi \in \mathrm{Sent}_0(\mathfrak{M})$.
8. $\mathfrak{M} \vDash \forall x.\varphi$ si y sólo si para todo $\mathbf{a} \in M, \mathfrak{M} \vDash \varphi[x \mapsto \mathbf{a}]$, donde $\varphi \in \mathrm{Sent}_0(\mathfrak{M})$ y $x \in \mathrm{Var}_{\mathrm{N}}$.
9. $\mathfrak{M} \vDash \exists x.\varphi$ si y sólo si existe $\mathbf{a} \in M, \mathfrak{M} \vDash \varphi[x \mapsto \mathbf{a}]$, donde $\varphi \in \mathrm{Sent}_0(\mathfrak{M})$ y $x \in \mathrm{Var}_{\mathrm{N}}$.
10. $\mathfrak{M} \vDash \forall X.\varphi$ si y sólo si para todo $\mathbf{A} \in \mathcal{S}_{\mathfrak{M}}, \mathfrak{M} \vDash \varphi[X \mapsto \mathbf{A}]$, donde $\varphi \in \mathrm{Sent}_0(\mathfrak{M})$ y $X \in \mathrm{Var}_{\mathrm{C}}$.
11. $\mathfrak{M} \vDash \exists X.\varphi$ si y sólo si existe $\mathbf{A} \in \mathcal{S}_{\mathfrak{M}}, \mathfrak{M} \vDash \varphi[X \mapsto \mathbf{A}]$, donde $\varphi \in \mathrm{Sent}_0(\mathfrak{M})$ y $X \in \mathrm{Var}_{\mathrm{C}}$.

■

Podemos extender la semántica al conjunto de todas las fórmulas (no necesariamente cerradas) si las variables libres son interpretadas de todas las formas posibles. Esto es:

Definición 1.12. Sea $\mathfrak{M}$ un modelo de L_2 y sea $\varphi[x_1, \ldots, x_n, X_1, \ldots X_m] \in \mathrm{Form}(\mathfrak{M})$, decimos que φ es válida en $\mathfrak{M}$, denotado $\mathfrak{M} \vDash \varphi$, si para cualesquiera $\mathbf{a}_1, \ldots, \mathbf{a}_n \in M, \mathbf{A}_1, \ldots, \mathbf{A}_m \in \mathcal{S}_{\mathfrak{M}}$, $\mathfrak{M} \vDash \varphi[\mathbf{a}_1, \ldots, \mathbf{a}_n, \mathbf{A}_1, \ldots, \mathbf{A}_m]$. ■

Para entender la semántica de las fórmulas definamos la clausura universal.

Definición 1.13. Sea $\varphi[\nu_1, \ldots, \nu_n] \in \mathrm{Form}(\mathcal{B})$. Entonces la clausura universal de φ, denotado $\mathrm{cl}(\varphi)$, se define como la sentencia $\forall \nu_1, \ldots, \nu_n.\varphi[\nu_1, \ldots, \nu_n]$. ■

La semántica asociada a una fórmula es entonces la de su clausura universal, como se ve en el siguiente lema.

Lema 1.1. *Sea $\mathfrak{M}$ un modelo y $\varphi \in \mathrm{Form}(\mathfrak{M})$. Entonces son equivalentes:*

- $\mathfrak{M} \vDash \varphi$.
- $\mathfrak{M} \vDash \mathrm{cl}(\varphi)$.

Demostración: Es una simple inducción (en la metateoría) en el número de variables libres de φ. □

1.3. Sistema deductivo

Definición 1.14 (**Teoría**)**.** Entenderemos que una teoría viene dada por:

- Un lenguaje, con un subconjunto de las expresiones del lenguaje que serán las fórmulas.
- Un conjunto de fórmulas llamadas axiomas lógicos.
- Unas reglas de inferencia.
- Un conjunto de fórmulas llamados axiomas (no lógicos).

Así definiremos una demostración en T como una sucesión finita de fórmulas en el lenguaje de la teoría tal que cada fórmula en la sucesión o bien es un axioma (lógico o no lógico) de la teoría o bien es la conclusión de una regla de inferencia aplicada a elementos anteriores en la sucesión. Escribiremos $T \vdash \varphi$ para indicar que hay una demostración tal que φ es parte de la sucesión, y se dirá entonces que φ es un teorema de T. Para un conjunto de fórmulas Γ, escribiremos $T \vdash \Gamma$ para indicar que cada elemento de Γ es un teorema de T.

En todas nuestras teorías (ya sean de segundo orden o de primer orden como en el capítulo 6) asumiremos que el aparato lógico es el de lógica clásica (con el tercio excluso), así que podremos identificar a una teoría por sus axiomas no lógicos (y el lenguaje al que estos pertenezcan, que salvo en el capítulo 6 será L_2). Es decir, a partir de ahora entenderemos que si T es una teoría, entonces T vendrá descrita por el conjunto de axiomas no lógicos.

■

Notación. Cuando añadamos fórmulas a los axiomas de una teoría será habitual denotar la unión como $+$, por ejemplo $T + \varphi$ para $T \cup \{\varphi\}$ o $T + \Gamma$ para $T \cup \Gamma$. ■

Definición 1.15. Sea T una teoría en L_2 y y $\mathfrak{M}$ un modelo de L_2. Decimos que $\mathfrak{M}$ es un modelo de T si para toda $\varphi \in T$, $\mathfrak{M} \vDash \varphi$. Se denotará $\mathfrak{M} \vDash T$.

Sea $\varphi \in \text{Form}$, entonces decimos que $T \vDash \varphi$ si para todo $\mathfrak{M}$ modelo de T se cumple que $\mathfrak{M} \vDash \varphi$. ■

El siguiente teorema es un resultado fundamental en el estudio de la lógica matemática: el teorema de completitud para la lógica de primer orden (demostrado por primera vez por Kurt Gödel en 1929).

Teorema 1.2 (**Validez y completitud**)**.** *$T \vdash \varphi$ si y sólo si $T \vDash \varphi$.*

Por el teorema de completitud de Gödel aplicado al lenguaje L_2 (es importante destacar que, aunque con 2 tipos de variables, L_2 es equivalente a un lenguaje de primer orden),

se tiene el siguiente principio de capital importancia: una fórmula cerrada φ del lenguaje L_2 es un teorema de una teoría T si, y solo si, todos los modelos de T satisfacen la fórmula φ. Usaremos ampliamente este resultado a lo largo del presente trabajo. Para demostrar que una cierta fórmula φ es un teorema de un subsistema de la aritmética de segundo orden, consideraremos un modelo arbitrario de dicho subsistema y justificaremos que dicho modelo arbitrario satisface la fórmula φ.

1.4. Aritmética de segundo orden

Procedemos ahora a definir qué es la arimética de segundo orden. Empezamos con unos axiomas que tan sólo reflejan el comportamiento del $0, 1$, la adición, la multiplicación y el menor que.

Definición 1.16 (**Axiomas básicos**)**.** Definimos los axiomas básicos de la aritmética como las clausuras universales de las fórmulas:

1. $n + 1 \neq 0$
2. $m + 1 = n + 1 \to m = n$
3. $m + 0 = m$
4. $m + (n + 1) = (m + n) + 1$
5. $m \cdot 0 = 0$
6. $m \cdot (n + 1) = (m \cdot n) + m$
7. $m \not< 0$
8. $m < n + 1 \leftrightarrow m < n \vee m = n$

Denotamos el conjunto de estas sentencias como BASIC. ■

Ahora, otro de los principios básicos de la aritmética, el de inducción.

Definición 1.17 (**Axioma de inducción**)**.** Definimos el axioma de inducción, denotado IND, como la clausura universal de la fórmula:

$$0 \in X \wedge (\forall n.n \in X \to n + 1 \in X) \to \forall n.n \in X.$$

■

Y, por último, el axioma que permite definir conjuntos de números, el axioma de comprensión.

Definición 1.18 (**Axioma de comprensión**)**.** Definimos el axioma-esquema de comprensión como las clausuras universales de las fórmulas:

$$\exists X \forall n. n \in X \leftrightarrow \varphi\{n\},$$

donde $X \in \mathrm{Var_C}, n \in \mathrm{Var_N}, \varphi\{n\} \in \mathrm{Form}$ tal que $X \notin \mathrm{Vl}(\varphi)$. El conjunto de todos estos axiomas se denotará COMP. ■

Que sea un axioma esquemático tan sólo quiere decir que cada vez que cambiemos φ por una fórmula que cumpla las condiciones tendremos un axioma. Por ejemplo, tomando $\varphi_1[n] \equiv \exists y. n = y \cdot y$, obtenemos el axioma

$$\exists X \forall n. n \in X \leftrightarrow \exists y. n = y \cdot y,$$

que expresa la existencia del conjunto de los cuadrados perfectos. Tomando $\varphi_2[n, Y, Z] \equiv n \in Y \vee n \in Z$, obtenemos el axioma

$$\forall Y \forall Z \exists X \forall n. n \in X \leftrightarrow n \in Y \vee n \in Z,$$

que expresa la existencia de la unión de dos conjuntos dados.

Definición 1.19. La teoría de la aritmética de segundo orden, denotada Z_2, es la teoría en el lenguaje L_2 con los axiomas:

$$Z_2 = \mathrm{BASIC} + \textsc{Ind} + \mathrm{COMP}.$$

■

Un subsistema de la artimética de segundo orden será una teoría T en el lenguaje L_2 "contenida en Z_2", esto es, tal que todos los axiomas de dicha teoría T sean teoremas de Z_2. A lo largo del presente trabajo, estudiaremos los ejemplos más prominentes de subsistemas de la aritmética de segundo orden, los llamados "Big Five".

El modelo pensado para L_2 de manera natural es

$$(\omega, \wp(\omega), +, \cdot, 0, 1, <)$$

donde ω son los números naturales, $\wp(\omega)$ los subconjuntos de números naturales y el resto de operaciones y relaciones son las típicas de los números naturales. Es claro que dicho modelo satisface todos los axiomas de la aritmética de segundo orden Z_2.

En el capítulo 6 introduciremos la noción de ω-modelo, que a grandes rasgos consiste en un modelo $(\omega, S, +, \cdot, 0, 1, <)$ igual al anterior salvo que $\varnothing \neq S \subseteq \wp(\omega)$, es decir los conjuntos que sirven para interpretar las variables de conjuntos no tienen porque ser todos los subconjuntos de los números naturales.

1.5. Jerarquía aritmética

Para obtener los subsistemas de Z_2 será habitual restringir los axiomas de comprensión e inducción. La manera de hacerlo será permitir que se usen sólo para ciertos conjuntos de fórmulas. Para ello definimos la jerarquía aritmética. Empezamos introduciendo la noción de cuantificador acotado, que nos permitirá definir la base de esta jerarquía.

Definición 1.20 (**Cuantificadores acotados**)**.** Sea $\phi \in \text{Form}, n \in \text{Var}_\text{N}, t \in \text{TNum}$ tal que $n \notin \text{Vl}(t)$. Definimos

$$\forall n < t.\phi :\equiv \forall n.n < t \to \phi$$
$$\exists n < t.\phi :\equiv \exists n.n < t \wedge \phi$$

Los cuantificadores $\forall n < t$ y $\exists n < t$ se llaman cuantificadores acotados. ■

Notación. Introducimos una notación para cuando tengamos varias variables acotadas por un mismo término en el mismo bloque de cuantificadores:

$$\forall n_1, \ldots, n_k < t.\varphi :\equiv \forall n_1 < t \cdots \forall n_k < t.\varphi.$$
$$\exists n_1, \ldots, n_k < t.\varphi :\equiv \exists n_1 < t \cdots \exists n_k < t.\varphi.$$

En general, usaremos estas notaciones y las de la definición 1.20 para cualquier símbolo de operación binario, primitivo o definido. Por ejemplo $\forall x \in X.\varphi \equiv \forall x.x \in X \to \varphi$. ■

Ahora definimos la base de la jerarquía, el conjunto de fórmulas acotadas Σ^0_0.

Definición 1.21 (**Fórmulas acotadas**)**.** Se define $\Sigma^0_0 \subseteq \text{Form}$ como:

1. Las fórmulas atómicas están en Σ^0_0.
2. Si $\varphi \in \Sigma^0_0$ entonces $\neg\varphi \in \Sigma^0_0$.
3. Si $\varphi, \psi \in \Sigma^0_0$ entonces $\varphi \wedge \psi, \varphi \vee \psi, \varphi \to \psi \in \Sigma^0_0$.
4. Si $\varphi \in \Sigma^0_0, n \in \text{Vl}_\text{N}, t \in \text{TNum}$ con $n \notin \text{Vl}(t)$ entonces $\forall n < t.\varphi, \exists n < t.\varphi \in \Sigma^0_0$.
5. Los elementos de Σ^0_0 son tan sólo los exigidos por 1-4.

■

Y finalmente cada escalón de la jerarquía.

Notación. Usaremos la notación $\overline{x} \in \mathrm{Var}_{\mathrm{N}}^{+}$ para indicar que $\overline{x} \equiv x_1, \ldots, x_n$ para algún $n > 0$ y los $x_i \in \mathrm{Var}_{\mathrm{N}}$. Así por ejemplo tenemos que:

$$\exists \overline{x}.\varphi \equiv \exists x_1, \ldots, x_n.\varphi \equiv \exists x_1 \cdots \exists x_n.\varphi.$$

■

Definición 1.22. Definimos para $k \in \omega$:

$$\Sigma_{k+1}^{0} = \{\exists \overline{x}.\varphi \mid \varphi \in \Pi_k^0\}$$
$$\Pi_{k+1}^{0} = \{\forall \overline{x}.\varphi \mid \varphi \in \Sigma_k^0\}$$

donde $\Pi_0^0 := \Sigma_0^0$, $\overline{x} \in \mathrm{Var}_{\mathrm{N}}^{+}$. ■

Ahora bien, como estamos trabajando en un sistema de segundo orden, es decir, no únicamente con números también con conjuntos de números, podemos establecer otra jerarquía encima de la anterior.

Definición 1.23 (**Fórmulas aritméticas**)**.** Definimos el conjunto de fórmulas aritméticas como $\Sigma_0^1 = \{\varphi \in \mathrm{Form} \mid \varphi \text{ no tiene cuantificadores de conjuntos}\}$. ■

Definición 1.24. Definimos para $k \in \omega$:

$$\Sigma_{k+1}^{1} = \{\exists X.\varphi \mid \varphi \in \Pi_k^1\}$$
$$\Pi_{k+1}^{1} = \{\forall X.\varphi \mid \varphi \in \Sigma_k^1\}$$

donde $\Pi_0^1 = \Sigma_0^1$. ■

Definición 1.25. Sea T una teoría de L_2, definimos para $i \in \{0, 1\}, k \in \omega$

$$\Delta_k^i(T) = \{\varphi \mid \varphi \in \Sigma_k^i \text{ y existe } \psi \in \Pi_k^i \text{ tal que } T \vdash \varphi \leftrightarrow \psi\}.$$

En el caso de escribir Δ_k^i nos referimos a $\Delta_k^i(\varnothing)$. De manera análoga se define $\Delta_k^i(\mathfrak{M})$ donde $\mathfrak{M}$ es un modelo de L_2. ■

Veamos cómo extender el concepto de la jerarquía aritmética a un lenguaje extendido por parámetros en $\mathcal{B}$, la idea es simple, serán las fórmulas de la jerarquía reemplazando algunas variables por los parámetros.

Definición 1.26. Sea $\Gamma \subseteq \mathrm{Form}$ y $\mathfrak{M}$ un modelo de L_2 tal que $\mathcal{B} \subseteq M \cup S_{\mathfrak{M}}$. Entonces definimos el conjunto de fórmulas de Γ con parámetros en $\mathcal{B}$ como

$$\Gamma_{\mathcal{B}} = \{\varphi\{\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k\} \mid \varphi\{\nu_1, \ldots, \nu_k\} \in \Gamma \text{ y } \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k \in \mathcal{B}\}$$

Como es habitual si $\mathcal{B} = M \cup S_{\mathfrak{M}}$ lo denotaremos por $\Gamma_{\mathfrak{M}}$. ■

El lema importante aquí es el siguiente:

Lema 1.3. *Si $T \vdash \Gamma$ y $\mathfrak{M}$ es un modelo de T entonces $\mathfrak{M} \vDash \Gamma_{\mathfrak{M}}$.*

Esta será la jerarquía de fórmulas que utilizaremos. Introducimos un poco de notación que nos será útil más adelante.

Notación. Usaremos las siguientes notaciones para el orden:

1. $t_1 \leq t_2 :\equiv t_1 < t_2 + 1$ donde $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$.
2. $t_1 > t_2 :\equiv t_2 < t_1$ donde $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$.
3. $t_1 \geq t_2 :\equiv t_2 \leq t_1$ donde $t_1, t_2 \in \mathrm{TNum}(\mathcal{B})$.

Notemos que $\forall x \leq t_1$ donde $x \notin \mathrm{Vl}(t_1)$ es un cuantificador acotado, y de la misma manera $\exists x \leq t_1$.

■

Como hemos dicho antes, vamos a limitar nuestro uso de ciertos principios únicamente a ciertas fórmulas de la teoría. Sin embargo, muchas veces querremos usarlos para fórmulas fuera de la jerarquía (en el sentido de que sintácticamente no pertenecen a la jerarquía). Vamos a ver cómo esto es posible mediante el concepto de fórmulas equivalentes.

Definición 1.27. En una teoría T, decimos que dos fórmulas del lenguaje de la teoría φ, ψ son equivalentes en T si $T \vdash \varphi \leftrightarrow \psi$. Si la teoría no tiene axiomas no lógicos, i.e. $T = \varnothing$, diremos simplemente que son equivalentes.

Si en lugar de una teoría tenemos un modelo $\mathfrak{M}$ y $\mathcal{B} \subseteq M \cup \mathcal{S}_{\mathfrak{M}}$, diremos que dos fórmulas $\varphi, \psi \in L_2(\mathcal{B})$ son equivalentes si $\mathfrak{M} \vDash \varphi \leftrightarrow \psi$. ■

El resultado importante sobre la equivalencia es el siguiente:

Lema 1.4. *Sean T una teoría y φ, ψ, χ tres fórmulas de la teoría tales que $T \vDash \psi \leftrightarrow \chi$. Sea φ' una fórmula obtenida al cambiar algunas apariciones de la fórmula ψ en φ por la fórmula χ, entonces $T \vDash \varphi \leftrightarrow \varphi'$.*

Lo mismo ocurre cambiando la teoría T por un modelo $\mathfrak{M}$.

Entonces, a un conjunto de fórmulas estará asociado otro conjunto de fórmulas que nos interese, el conjunto de fórmulas equivalentes.

Definición 1.28. Dado un conjunto $\Gamma \subseteq \mathrm{Form}$ y una teoría T definimos

$$\boldsymbol{\Gamma}^T = \{\phi \in \mathrm{Form} \mid \text{existe } \psi \in \Gamma \text{ tal que } T \vdash \phi \leftrightarrow \psi\}.$$

En caso de que $T = \varnothing$ escribiremos $\boldsymbol{\Gamma}$ en lugar de $\boldsymbol{\Gamma}^{\varnothing}$. ■

El lema importante sobre la equivalencia es claro:

Lema 1.5. *Si $T \vdash \Gamma$, entonces $T \vdash \mathbf{\Gamma}^T$.*

Veamos algunos resultados básicos que nos ayudarán en el manejo de la jerarquía aritmética. (Aviso para el lector, los siguientes teoremas son fáciles y bastantes ajenos a la matemática inversa, se incluyen únicamente porque serán usados sin mención para el razonamiento de a qué escalón de la jerarquía pertenece una fórmula, o mejor dicho, su fórmula equivalente).

Lema 1.6. *Si $\Gamma \subseteq \mathbf{\Delta}^T$ entonces $\mathbf{\Gamma}^T \subseteq \mathbf{\Delta}^T$.*

Demostración: Sea $\varphi \in \mathbf{\Gamma}^T$. Entonces existe $\varphi' \in \Gamma$ tal que $T \vdash \varphi \leftrightarrow \varphi'$. Como $\varphi' \in \Gamma \subseteq \mathbf{\Delta}^T$, existe $\psi \in \Delta$ tal que $T \vdash \varphi' \leftrightarrow \psi$ y, por transitividad de $\leftrightarrow$, $T \vdash \varphi \leftrightarrow \psi$, como queríamos. □

Lema 1.7. *Sean $k \in \omega, i \in \{0,1\}$. Entonces*

1. *Si $\varphi \in \Pi^i_k$ entonces $\neg\varphi \in \mathbf{\Sigma^i_k}$.*
2. *Si $\varphi \in \Sigma^i_k$ entonces $\neg\varphi \in \mathbf{\Pi^i_k}$.*
3. *Si $\varphi \in \Delta^i_k$ entonces $\neg\varphi \in \mathbf{\Delta^i_k}$.*

Demostración: 3. se sigue de 1. y 2., y como 1. y 2. son análogos veamos tan sólo 1. Podemos suponer que $i = 0$, ya que para $i = 1$ el procedimiento es totalmente análogo. Así sea $\varphi \equiv \forall\overline{x}_1 \cdots Q\overline{x}_k.\varphi_0$, con φ_0 en Σ^0_0. Por tanto

$$\vdash (\neg\forall\overline{x}_1 \cdots Q\overline{x}_k.\varphi_0) \leftrightarrow (\exists\overline{x}_1.\neg\exists\overline{x}_2 \cdots Q\overline{x}_k.\varphi_0') \leftrightarrow \cdots \leftrightarrow \exists\overline{x}_1 \cdots Q'\overline{x}_k.\neg\varphi_0,$$

donde los cuantificadores han pasado a ser $\exists$ si eran $\forall$ y $\forall$ si eran $\exists$. La fórmula más a la derecha de las equivalencias pertenece a Σ^0_k, por tanto $\neg\varphi \in \mathbf{\Sigma^0_k}$. □

Lema 1.8. *Sean $k \in \omega$ e $i \in \{0,1\}$. Entonces se tiene que:*

1. $\Delta^i_k \subseteq \mathbf{\Pi^i_k}$.
2. $\Delta^i_k \subseteq \mathbf{\Sigma^i_k}$.
3. $\Pi^i_k \subseteq \mathbf{\Delta^i_{k+1}}$
4. $\Sigma^i_k \subseteq \mathbf{\Delta^i_{k+1}}$.

Demostración: 1. y 2. son triviales por la definición de Δ^i_k. 3. y 4. son análogos, así que veamos 3. Supongamos que $i = 0$, si $i = 1$ es análogo. Sea $\varphi \in \Pi^i_k$. Entonces $\varphi \equiv \forall\overline{x}_1 \cdots Q\overline{x}_k.\varphi_0$, donde Q es $\forall$ o $\exists$ y $\varphi_0 \in \Sigma^0_0$. Sea $y \notin \mathrm{Vl}(\varphi_0)$, entonces $\vdash \varphi_0 \leftrightarrow$

$(\forall y.\varphi_0) \leftrightarrow (\exists y.\varphi_0)$. Por tanto $\vdash (\forall \overline{x}_1 \cdots Q\overline{x}_k.\varphi_0) \leftrightarrow (\forall \overline{x}_1 \cdots Q\overline{x}_k Q' y.\varphi_0)$ donde Q' es $\forall$ si Q es $\exists$ y es $\exists$ si Q es $\forall$. Así $(\forall \overline{x}_1, \ldots, Q\overline{x}_k Q' y.\varphi_0) \in \Pi^0_{k+1}$, por tanto $\varphi \in \mathbf{\Pi^0_{k+1}}$. Por otro lado, como $y \notin \mathrm{Vl}(\varphi_0)$, $y \notin \mathrm{Vl}(\varphi)$ y así $\vdash \varphi \leftrightarrow (\exists y.\varphi)$ y $\exists y.\varphi \in \Sigma^0_{k+1}$, por tanto $\varphi \in \mathbf{\Sigma^0_{k+1}}$. Así $\varphi \in \mathbf{\Delta^0_{k+1}}$, como queríamos. □

Veamos ahora que los escalones de la primera jerarquía aritmética están cerrados bajo $\vee$.

Lema 1.9. *Sea $k \in \omega$, entonces*

1. *$\varphi, \psi \in \Pi^0_k$ implica $\varphi \vee \psi \in \mathbf{\Pi^0_k}$.*
2. *$\varphi, \psi \in \Sigma^0_k$ implica $\varphi \vee \psi \in \mathbf{\Sigma^0_k}$.*
3. *$\varphi, \psi \in \Delta^0_k$ implica $\varphi \vee \psi \in \mathbf{\Delta^0_k}$.*

Demostración: La demostración es estándar (se hace mediante las equivalencias lógicas habituales, al igual que las anteriores) y la omitimos aquí para ahorrar espacio. □

Nota. El hecho de que $\vdash (\varphi \wedge \psi) \leftrightarrow \neg(\neg\varphi \vee \neg\psi)$ y $\vdash (\varphi \to \psi) \leftrightarrow (\neg\varphi \vee \psi)$ nos permite usar los lemas 1.7 y 1.9 para fórmulas con esas conectivas (adaptándolos de forma adecuada).

Como consecuencia directa si $t \in \mathrm{TNum}$, $x \notin \mathrm{Vl}(t)$ y $\varphi \in \Pi^0_k$, por el lema anterior $(x < t \to \varphi) \in \mathbf{\Pi^0_k}$ y así $(\forall x < t.\varphi) \in \mathbf{\Pi^0_k}$. Análogamente si $\varphi \in \Sigma^0_k$ tenemos que $(\exists x < t.\varphi) \in \mathbf{\Sigma^0_k}$.

■

Notación. Será muy habitual para aplicar los axiomas el buscar primero una fórmula equivalente que esté en la jerarquí aritmética y luego sustituir sus variables por parámetros. Por ello introducimos la notación siguiente: escribiremos $(\mathbf{\Gamma}^T)_{\mathcal{B}}$ como $\mathbf{\Gamma}^T_{\mathcal{B}}$. ■

1.6. Axiomas-esquemas importantes

Ahora veamos los axiomas esquemas que usaremos en los subsistemas de Z_2. Primero inducción únicamente para un conjunto de fórmulas.

Definición 1.29 (Γ-**inducción**)**.** Para $\Gamma \subseteq \mathrm{Form}$ el axioma-esquema de Γ-inducción consiste en la clausuras universales de las fórmulas:

$$\varphi\{0\} \wedge (\forall n.\varphi\{n\} \to \varphi\{n+1\}) \to \forall n.\varphi\{n\},$$

donde $n \in \mathrm{Var_N}, \varphi\{n\} \in \Gamma$. Al conjunto con todos los axiomas de Γ-inducción lo llamaremos Γ-IND. ■

Ahora comprensión para un conjunto de fórmulas.

Definición 1.30 (**Γ-comprensión**)**.** Para $\Gamma \subseteq \mathrm{Form}$ el axioma-esquema de Γ-comprensión consiste en las clausuras universales de las fórmulas:

$$\exists X \forall n. n \in X \leftrightarrow \varphi\{n\},$$

donde $X \in \mathrm{Var_C}, n \in \mathrm{Var_N}, \varphi\{x\} \in \Gamma$ y $X \notin \mathrm{Vl}(\varphi)$. Al conjunto con todos los axiomas de Γ-comprensión lo llamaremos Γ-COMP. ■

Definición 1.31 (Δ^0_k**-comprensión**)**.** Para $k \in \omega$ el axioma-esquema de Δ^0_k-comprensión consiste en las clausuras universales de las fórmulas:

$$(\forall n. \varphi\{n\} \leftrightarrow \psi\{n\}) \rightarrow \exists X \forall n. n \in X \leftrightarrow \varphi\{n\}$$

donde $X \in \mathrm{Var_C}, n \in \mathrm{Var_N}, \varphi\{n\} \in \Sigma^0_k, \psi\{n\} \in \Pi^0_k$ y $X \notin \mathrm{Vl}(\varphi)$. Al conjunto con todos los axiomas de Δ^0_k-comprensión lo llamaremos Δ^0_k-COMP. ■

Nota. Gracias a los lemas 1.5 y 1.3 tenemos un resultado básico pero que usaremos constantemente. Si T es tal que $T \vdash \Gamma$ y $\mathfrak{M}$ es un modelo de T entonces no sólo $\mathfrak{M} \vDash \Gamma$, sino que $\mathfrak{M} \vDash \mathbf{\Gamma}^T_{\mathfrak{M}}$. Por ejemplo, si $T \vdash \Sigma^0_1$-IND, entonces $\mathfrak{M} \vDash \mathbf{\Sigma^0_1}\text{-}\mathbf{IND}^T_{\mathfrak{M}}$ y en particular $\mathfrak{M} \vDash (\mathbf{\Sigma^0_1})^T_{\mathfrak{M}}$-IND. ■

Nota. A lo largo de la memoria aparecerán ciertos conjuntos sin justificación de su existencia. Será sencillo encontrar una fórmula que los defina y que cumpla el axioma de comprensión necesario para la teoría, por tanto no se desarrollará explícitamente. ■

Capítulo 2

$\mathbf{RCA_0}$

En este capítulo introducimos el primero de los subsistemas de la aritmética de segundo orden que estudiaremos, la teoría RCA_0. Dicha teoría fue introducida (con una axiomatizacón diferente) en Friedman [1] y su nombre es el acrónimo de *recursive comprehension axiom* (axioma de comprensión recursiva). Eso expresa que en RCA_0 se demuestra la existencia de cualquier conjunto A que sea recursivo en unos conjuntos $B_1, \ldots, B_k$ ya dados. Además, hay una estrecha correspondencia entre RCA_0 y lo que se suele denominar matemáticas computables, siendo el ω-modelo mínimo (no tendría por qué existir ω-modelo mínimo pero en este caso existe) de RCA_0, REC, un modelo que tiene exactamente los conjuntos recursivos como su parte de segundo orden. No es de extrañar lo relacionado con la computabilidad que está este sistema, ya que se sabe que los conjuntos recursivos (de ω) son los Δ^0_1-definibles en el modelo estándar (sin parámetros de segundo orden).

RCA_0 será fundamental para el desarrollo del texto ya que será la teoría base, donde las equivalencias de los teoremas matemáticos con los otros subsistemas serán demostradas. En el capítulo X de Simpson [8], se plantea la posibilidad de cambiar la teoría base RCA_0 por RCA^*_0, que, al ser más débil que RCA_0, nos permitiría hacer matemática inversa de RCA_0. RCA^*_0 es la teoría resultante de quitar Σ^0_1-IND, añadir un símbolo primitivo para la exponenciación y Σ^0_0-IND. Notemos que para poder demostrar que la exponenciación es total es fundamental tenerla como símbolo primitivo, ya que por el teorema de Parikh sabemos que la Σ^0_0-IND no es suficiente para demostrarlo. En ambos casos (RCA_0 y RCA^*_0) la presencia de la exponencial es importante ya que ella nos permite un tratamiento natural para la codificación de los conjuntos finitos.

Tras estos comentarios previos definimos RCA_0.

Definición 2.1 (**La teoría** RCA_0)**.** Definimos la teoría RCA_0 como:

$$\mathrm{RCA}_0 = \mathrm{BASIC} + \Sigma^0_1\text{-IND} + \Delta^0_1\text{-COMP}.$$

■

Gracias a Σ^0_0-comprensión se puede demostrar la existencia de un conjunto que contiene a todos los elementos:

Lema 2.1. *$RCA_0 \vdash \exists^1 X.\forall x.x \in X \leftrightarrow x = x$. Llamaremos $\mathbb{N}$ a ese conjunto único. Además $(n \in \mathbb{N}) \in (\mathbf{\Sigma^0_0})^{RCA_0}$ y $RCA_0 \vdash \forall n.n \in \mathbb{N}$.*

Demostración: La existencia se tiene por Σ^0_0-comprensión y la unicidad por la definición de igualdad de conjuntos. Por otro lado, $n \in \mathbb{N}$ es equivalente en RCA$_0$ a $n = n$, que es Σ^0_0. La última afirmación es trivial. □

Nota. A partir de ahora distinguiremos $\mathbb{N}$, que dado un modelo de RCA$_0$ será el conjunto de todos los elementos, de ω que será en conjunto de los naturales en la metateoría. Además, fijado un modelo $\mathfrak{M}$, y aunque $\mathcal{S}_{\mathfrak{M}}$ no sea un conjunto de la teoría objeto sino de la metateoría, puesto que denotamos a M por $\mathbb{N}$, escribiremos a veces también $\wp(\mathbb{N})$ para denotar a $\mathcal{S}_{\mathfrak{M}}$ (que, por supuesto, en general no será el conjunto de las partes de $\mathbb{N}$). ■

El resultado que nos permite ver la similitud (que no igualdad) entre $\mathbb{N}$ y los números naturales usuales (ω) es el siguiente:

Lema 2.2. *Si T es una teoría tal que $T \vdash BASIC + \Sigma^0_0\text{-}IND$ entonces T demuestra que $\mathbb{N}, +, \cdot, 0, 1, <$ es un semianillo conmutativo ordenado con cancelación.*

Demostración: Es una prueba estándar por inducción en la fórmula que expresa cada una de las propiedades requeridas. Véase, por ejemplo, el lema II.2.1 de [Simpson]. □

Como consecuencia se tiene que:

Lema 2.3. *RCA_0 demuestra que $\mathbb{N}, +, \cdot, 0, 1, <$ es un semianillo conmutativo ordenado con cancelación.*

2.1. Pares de números

Será muy importante disponer en la teoría RCA$_0$ de una función que codifique cada par de números naturales mediante un número natural.

Notación. Para cada $k \in \omega$ y t número definimos la notación t^k como:

$$t^0 :\equiv 1$$
$$t^{k+1} :\equiv t \cdot t^k.$$

■

Como es habitual, vamos a hacer una codificación de los pares de números en los números, pudiendo codificar así tuplas de longitud un número de ω con un solo número.

Definición 2.2 (**Función de emparejamiento**)**.** En RCA_0, definimos la función de emparejamiento como

$$(i,j) :\equiv (i+j)^2 + i.$$

■

La primera propiedad importante de los pares ordenados es que sus componentes pueden ser acotadas por el par, lo que nos permitirá muchas veces demostrar que fórmulas con pares ordenados son equivalentes a fórmulas en Σ^0_0.

Lema 2.4. *$RCA_0 \vdash \forall i,j.i \leq (i,j) \wedge j \leq (i,j)$.*

Demostración:
⟨1⟩1. Sean $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{i},\mathbf{j} \in \mathbb{N}$.

⟨1⟩2. $\mathrm{RCA}_0 \vdash \forall n.n \leq n^2$.

⟨2⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0.

⟨2⟩2. $\mathfrak{M} \vDash 0 \leq 0^2$.

Demostración: Como $\mathfrak{M} \vDash \mathrm{BASIC}$ tenemos que $\mathfrak{M} \vDash 0^2 = 0$ y por tanto $\mathfrak{M} \vDash 0 \leq 0^2$.

⟨2⟩3. $\mathfrak{M} \vDash \forall n.(n+1) \leq (n+1)^2$.

Demostración: Sea $\mathbf{n} \in \mathbb{N}$. Entonces tenemos que $\mathfrak{M} \vDash 1 \leq \mathbf{n}+1$. Por el lema 2.3 y gracias a que $\mathfrak{M} \vDash \mathbf{n}+1 \neq 0$, tenemos que $\mathfrak{M} \vDash \mathbf{n}+1 = (\mathbf{n}+1)\cdot 1 \leq (\mathbf{n}+1)\cdot(\mathbf{n}+1) = (\mathbf{n}+1)^2$.

⟨2⟩4. Q.E.D.

Demostración: Por el lema 2.3 dado $\mathbf{n} \in \mathbb{N}$ tenemos que o bien $\mathfrak{M} \vDash \mathbf{n} = 0$ en cuyo caso usamos ⟨2⟩2 o bien que existe $\mathbf{m} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{m}+1 = \mathbf{n}$, en cuyo caso usamos ⟨2⟩3.

⟨1⟩3. $\mathfrak{M} \vDash \mathbf{i} \leq (\mathbf{i}+\mathbf{j})^2 + \mathbf{i}$.

⟨2⟩1. $\mathfrak{M} \vDash (\mathbf{i}+\mathbf{j})^2 = \mathbf{0} \to \mathbf{i} \leq (\mathbf{i}+\mathbf{j})^2 + \mathbf{i}$.

Demostración: Pues $\mathfrak{M} \vDash \mathbf{i} = \mathbf{0} + \mathbf{i} = (\mathbf{i}+\mathbf{j})^2 + \mathbf{i}$.

⟨2⟩2. $\mathfrak{M} \vDash (\mathbf{i}+\mathbf{j})^2 = \mathbf{n}+\mathbf{1} \to \mathbf{i} \leq (\mathbf{i}+\mathbf{j})^2 + \mathbf{i}$.

Demostración: Por ⟨1⟩3 y el lema 2.3 $\mathfrak{M} \vDash \mathbf{i} < \mathbf{n}+\mathbf{1}+\mathbf{i} = (\mathbf{i}+\mathbf{j})^2 + \mathbf{i}$.

⟨2⟩3. Q.E.D.

Demostración: Por el lema 2.3 dado $\mathbf{i} \in \mathbb{N}$ tenemos que o bien $\mathfrak{M} \vDash (\mathbf{i}+\mathbf{1})^2 = 0$ en cuyo caso usamos ⟨2⟩1 o bien que existe $\mathbf{m} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{m}+1 = (\mathbf{i}+\mathbf{1})^2$, en cuyo caso usamos ⟨2⟩2.

⟨1⟩4. $\mathfrak{M} \vDash \mathbf{j} \leq (\mathbf{i}+\mathbf{j})^2 + \mathbf{i}$.

DEMOSTRACIÓN: Tenemos que $\mathfrak{M} \vDash \mathbf{j} \leq \mathbf{i}+\mathbf{j}$ y por ⟨1⟩3 tenemos que $\mathfrak{M} \vDash \mathbf{i}+\mathbf{j} \leq (\mathbf{i}+\mathbf{j})^2 \leq (\mathbf{i}+\mathbf{j})^2 + \mathbf{i}$, como queríamos.

⟨1⟩5. Q.E.D.

□

La segunda propiedad es que RCA_0 demuestra que efectivamente los pares ordenados se comportan como esperaríamos de un par ordenado: dos pares ordenados son iguales si sus elementos lo son componente a componente.

Lema 2.5. *$RCA_0 \vdash \forall i, j, i', j'.(i, j) = (i', j') \to i = i' \wedge j = j'$.*

DEMOSTRACIÓN:
⟨1⟩1. $\mathrm{RCA}_0 \vdash \forall i, j \exists^1 m.m^2 \leq (i, j) < (m+1)^2$.

⟨2⟩1. Sean $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{i}, \mathbf{j} \in \mathbb{N}$ cualesquiera.

⟨2⟩2. Existencia, $\mathfrak{M} \vDash \exists m.m^2 \leq (\mathbf{i}, \mathbf{j}) < (m+1)^2$.

DEMOSTRACIÓN: Basta tomar $m = \mathbf{i}+\mathbf{j}$ ya que $\mathfrak{M} \vDash (\mathbf{i}, \mathbf{j}) = (\mathbf{i}+\mathbf{j})^2 + \mathbf{i}$ por definicón y $\mathfrak{M} \vDash (\mathbf{i}+\mathbf{j}+\mathbf{1})^2 = (\mathbf{i}+\mathbf{j})^2 + \mathbf{2}(\mathbf{i}+\mathbf{j}) + \mathbf{1}$ por ser semianillo ordenado (en particular hemos usado la propiedad distributiva), y las desigualdades se obtienen otra vez por ser semianillo ordenado.

⟨2⟩3. Unicidad

⟨3⟩1. $\mathrm{RCA}_0 \vdash \forall m, n.m < n \to m^2 < n^2$.
DEMOSTRACIÓN: Sean $\mathbf{m}, \mathbf{n} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{m} < \mathbf{n}$. Si $\mathfrak{M} \vDash \mathbf{n} = 0$ trivial, pues $\mathfrak{M} \vDash \mathrm{BASIC}$. Supongamos entonces que $\mathfrak{M} \vDash \mathbf{n} \neq 0$. Ahora bien, si $\mathfrak{M} \vDash \mathbf{m} = 0$ vuelve a ser trivial (pues $\mathfrak{M} \vDash \mathbf{m}^2 = 0$ pero $\mathfrak{M} \vDash 0 < \mathbf{n}$ ya que $\mathfrak{M} \vDash \mathbf{n} \neq 0$), por tanto podemos suponer que $\mathfrak{M} \vDash \mathbf{m} \neq 0$. Usando el lema 2.3 y la hipótesis de que $\mathfrak{M} \vDash \mathbf{m} < \mathbf{n}$ tenemos que
$$\mathfrak{M} \vDash \mathbf{m}^2 = \mathbf{m} \cdot \mathbf{m} < \mathbf{m} \cdot \mathbf{n} < \mathbf{n} \cdot \mathbf{n} = \mathbf{n}^2.$$

⟨3⟩2. Sean $\mathbf{m_i} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{m}_i^2 \leq (\mathbf{i}, \mathbf{j}) < (\mathbf{m}_i + \mathbf{1})^2$ para $i \in \{1, 2\}$.

⟨3⟩3. $\mathfrak{M} \vDash \mathbf{m}_1 \not< \mathbf{m}_2$.
DEMOSTRACIÓN: Si $\mathfrak{M} \vDash \mathbf{m}_1 < \mathbf{m}_2$ entonces $\mathfrak{M} \vDash \mathbf{m}_1 + 1 \leq \mathbf{m}_2$ y así $\mathfrak{M} \vDash (\mathbf{m}_1+1)^2 \leq \mathbf{m}_2^2$. Pero por ⟨3⟩2, $\mathfrak{M} \vDash \mathbf{m}_2^2 \leq (\mathbf{i}, \mathbf{j}) < (\mathbf{m}_1+1)^2$, por tanto $\mathfrak{M} \vDash \mathbf{m}_2^2 < (\mathbf{m}_1+1)^2$ absurdo.

⟨3⟩4. $\mathfrak{M} \vDash \mathbf{m}_2 \not< \mathbf{m}_1$.
DEMOSTRACIÓN: Análogo a ⟨3⟩3.

⟨3⟩5. Q.E.D.
DEMOSTRACIÓN: Por ⟨3⟩3 y ⟨3⟩4 y tricotomía de $<$ por el lema 2.3.

⟨2⟩4. Q.E.D.

⟨1⟩2. $\mathrm{RCA}_0 \vdash \forall i, j, m. m^2 \leq (i, j) < (m+1)^2 \to i + m^2 = (i, j) \wedge i + j = m$.

DEMOSTRACIÓN: Por la demostración de la existencia y unicidad en ⟨1⟩1 sabemos que dado un modelo de RCA_0, $\mathfrak{M}$, y dados $\mathbf{i}, \mathbf{j}, \mathbf{m} \in \mathbb{N}$ que cumplan eso, necesariamente (por unicidad) $\mathfrak{M} \vDash \mathbf{m} = \mathbf{i} + \mathbf{j}$ y de ahí se concluye fácilmente.

⟨1⟩3. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{i}, \mathbf{j}, \mathbf{i}', \mathbf{j}' \in \mathbb{N}$ tal que $\mathfrak{M} \vDash (\mathbf{i}, \mathbf{j}) = (\mathbf{i}', \mathbf{j}')$.

⟨1⟩4. $\mathfrak{M} \vDash \mathbf{i} = \mathbf{i}' \wedge \mathbf{j} = \mathbf{j}'$.

DEMOSTRACIÓN: Por ⟨1⟩1 sabemos que existe un $\mathbf{m} \in \mathbb{N}$ tal que que $\mathfrak{M} \vDash \mathbf{m}^2 \leq (\mathbf{i} + \mathbf{j}) < (\mathbf{m}+1)^2$, además el mismo $\mathbf{m}$ cumplirá lo mismo para $(\mathbf{i}', \mathbf{j}')$ ya que son iguales. Por ⟨1⟩2 eso quiere decir que $\mathfrak{M} \vDash \mathbf{i} + \mathbf{m}^2 = (\mathbf{i}, \mathbf{j}) = (\mathbf{i}', \mathbf{j}') = \mathbf{i}' + \mathbf{m}^2$, y por semianillo ordenado con cancelación se concluye $\mathfrak{M} \vDash \mathbf{i} = \mathbf{i}'$. Otra vez por ⟨1⟩2, se tiene que $\mathfrak{M} \vDash \mathbf{i} + \mathbf{j} = \mathbf{m} = \mathbf{i}' + \mathbf{j}'$ y por $\mathfrak{M} \vDash \mathbf{i} = \mathbf{i}'$ y ser semianillo ordenado con cancelación obtenemos que $\mathfrak{M} \vDash \mathbf{j} = \mathbf{j}'$.

⟨1⟩5. Q.E.D.

□

2.2. Funciones

Vamos a introducir las definiciones y resultados necesarios para definir el concepto de función en RCA_0. Primero introducimos algunas notaciones útiles para hablar de conjuntos:

Notación. Introducimos las siguientes notaciones:

- $X = \{n \mid \varphi\{n\}\} :\equiv \forall n. n \in X \leftrightarrow \varphi\{n\}$.
- $X = \{t[\nu_1, \ldots, \nu_k] \mid \varphi\} :\equiv X = \{n \mid \exists \nu_1, \ldots, \nu_k. n = t \wedge \varphi\}$ donde $n \notin \mathrm{Vl}(t) \cup \mathrm{Vl}(\varphi)$.

■

Veamos que en RCA_0 se puede demostrar la existencia del producto cartesiano de dos conjuntos (recordando que los pares ordenados de números son tan sólo una codificación en los números).

Lema 2.6 (**Producto de dos conjuntos**).

$$RCA_0 \vdash \forall X, Y \exists^1 Z. Z = \{(i, j) \mid i \in X \wedge j \in Y\}).$$

A ese único Z lo llamamos el producto de X e Y, y lo denotamos como $X \times Y$.

DEMOSTRACIÓN: Sean $\mathfrak{M}$ un modelo de RCA$_0$ y $\mathbf{X}, \mathbf{Y} \in \mathcal{S}_{\mathfrak{M}}$. La existencia se tiene por Σ^0_0-comprensión en la fórmula $\exists i, j \leq k.k = (i, j) \wedge i \in \mathbf{X} \wedge j \in \mathbf{Y}$, que es equivalente por el lema 2.4 a $\exists i, j.k = (i, j) \wedge i \in \mathbf{X} \wedge j \in \mathbf{Y}$. La unicidad sale de la definición de igualdad de conjuntos. □

Nota. A partir de ahora será usual no indicar explícitamente la acotación de los cuantificadores cuando estos hagan referencia a variables de un par ordenado, como se ha hecho en la demostración anterior, ya que estos siempre se pueden acotar por la variable que sea igual al par ordenado. ■

Notación. Tomaremos el convenio de que $\times$ asocia a la derecha, i.e. $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \equiv \mathbb{N} \times (\mathbb{N} \times \mathbb{N})$. De la misma forma $(i, j, k) \equiv (i, (j, k))$. ■

Lema 2.7. *Sean* $(x \in t_1), (y \in t_2) \in (\mathbf{\Sigma^0_0})^{RCA_0}$ *con* $t_1, t_2 \in$ TSet*. Entonces* $(z \in t_1 \times t_2) \in (\mathbf{\Sigma^0_0})^{RCA_0}$.

DEMOSTRACIÓN: Sean $\varphi, \psi \in \Sigma^0_0$ que son equivalentes a $(x \in t_1)$ y a $(y \in t_2)$ en RCA$_0$ respectivamente. Basta con usar la fórmula $\exists x, y.z = (x, y) \wedge \varphi \wedge \psi$ que será equivalente en RCA$_0$ a $z \in t_1 \times t_2$. □

Corolario 2.8. $(x \in \mathbb{N} \times \mathbb{N}), (x \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}) \in (\mathbf{\Sigma^0_0})^{RCA_0}$.

Ahora como es habitual definimos las funciones como ciertos conjuntos de pares ordenados.

Definición 2.3 (**Funciones**)**.** Definimos

$$f : X \longrightarrow Y :\equiv f \subseteq X \times Y \wedge (\forall i, j, k.(i, j) \in f \wedge (i, k) \in f \rightarrow j = k) \wedge (\forall i \in X \exists j.(i, j) \in f).$$

Se dice que f es una función de X en Y. Se demuestra fácilmente que

$$\text{RCA}_0 \vdash \forall f, X, Y.f : X \longrightarrow Y \rightarrow \forall x \in X \exists^1 y \in Y.(x, y) \in f,$$

a ese y se le denotará $f(x)$. □

Notación. Usaremos la notacion $\forall f : X \longrightarrow Y.\phi$ para denotar $\forall f.f : X \longrightarrow Y \rightarrow \phi$. De la misma forma, $\exists f : X \longrightarrow Y.\phi$ denotará $\exists f.f : X \longrightarrow Y \wedge \phi$. ■

Veamos como establecer igualdad de funciones.

Teorema 2.9 (**Igualdad de funciones**)**.**

$$RCA_0 \vdash \forall X_1, X_2, Y_1, Y_2 \forall f_1 : X_1 \longrightarrow Y_1 \forall f_2 : X_2 \longrightarrow Y_2.$$

$$f_1 = f_2 \leftrightarrow (X_1 = X_2 \wedge \forall x \in X_1.f_1(x) = f_2(x)).$$

Demostración:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{f}_1, \mathbf{f}_2 \in \wp(\mathbb{N})$, tales que $\mathfrak{M} \vDash \mathbf{f}_1 : \mathbf{X}_1 \longrightarrow \mathbf{Y}_1$ y $\mathfrak{M} \vDash \mathbf{f}_2 : \mathbf{X}_2 \longrightarrow \mathbf{Y}_2$.

⟨1⟩2. $\mathfrak{M} \vDash \mathbf{f}_1 = \mathbf{f}_2 \to (\mathbf{X}_1 = \mathbf{X}_2 \wedge \forall x \in \mathbf{X}_1.\mathbf{f}_1(x) = \mathbf{f}_2(x))$.

⟨2⟩1. Supongamos que $\mathfrak{M} \vDash \mathbf{f}_1 = \mathbf{f}_2$.

⟨2⟩2. $\mathbf{X}_1 \subseteq \mathbf{X}_2$.

Demostración: Sea $\mathbf{x} \in \mathbf{X}_1$. Como $\mathbf{f}_1$ es una función por ⟨1⟩1, existe $\mathbf{y} \in \mathbf{Y}_1$ tal que $\mathfrak{M} \vDash (\mathbf{x}, \mathbf{y}) \in \mathbf{f}_1$, gracias a ⟨2⟩1 eso quiere decir que $\mathfrak{M} \vDash (\mathbf{x}, \mathbf{y}) \in \mathbf{f}_2$. Ahora como por ⟨1⟩1 $\mathbf{f}_2$ es una función, en particular $\mathfrak{M} \vDash \mathbf{f}_2 \subseteq \mathbf{X}_2 \times \mathbf{Y}_2$, y gracias a que $\mathfrak{M} \vDash (\mathbf{x}, \mathbf{y}) \in \mathbf{f}_2$ tenemos que $\mathfrak{M} \vDash \mathbf{x} \in \mathbf{X}_2$.

⟨2⟩3. $\mathbf{X}_2 \subseteq \mathbf{X}_1$.

Demostración: Análogo a ⟨2⟩2.

⟨2⟩4. $\mathbf{X}_1 = \mathbf{X}_2$.

Demostración: Gracias a ⟨2⟩2 y ⟨2⟩3.

⟨2⟩5. $\forall x \in \mathbf{X}_1.\mathbf{f}_1(x) = \mathbf{f}_2(x)$.

Demostración: Sea $\mathbf{x} \in \mathbf{X}_1$. Como por ⟨1⟩1 $\mathbf{f}_1$ y $\mathbf{f}_2$ son funciones y por ⟨2⟩4 $\mathfrak{M} \vDash \mathbf{x} \in \mathbf{X}_2$ tenemos que existen $\mathbf{y}_1 \in \mathbf{Y}_1, \mathbf{y}_2 \in \mathbf{Y}_2$ tales que $\mathfrak{M} \vDash (\mathbf{x}, \mathbf{y}_1) \in \mathbf{f}_1 \wedge (\mathbf{x}, \mathbf{y}_2) \in \mathbf{f}_2$. Ahora por ⟨2⟩1, $\mathfrak{M} \vDash (\mathbf{x}, \mathbf{y}_1) \in \mathbf{f}_2 \wedge (\mathbf{x}, \mathbf{y}_2) \in \mathbf{f}_2$, y por ser $\mathbf{f}_2$ un función $\mathfrak{M} \vDash \mathbf{y}_1 = \mathbf{y}_2$, como queríamos.

⟨2⟩6. Q.E.D.

Demostración: Gracias a ⟨2⟩4 y ⟨2⟩5.

⟨1⟩3. $\mathfrak{M} \vDash (\mathbf{X}_1 = \mathbf{X}_2 \wedge \forall x \in \mathbf{X}_1.\mathbf{f}_1(x) = \mathbf{f}_2(x)) \to \mathbf{f}_1 = \mathbf{f}_2$.

⟨2⟩1. Supongamos que $\mathfrak{M} \vDash \mathbf{X}_1 = \mathbf{X}_2 \wedge \forall x \in \mathbf{X}_1.\mathbf{f}_1(x) = \mathbf{f}_2(x)$

⟨2⟩2. $\mathfrak{M} \vDash \mathbf{f}_1 \subseteq \mathbf{f}_2$.

Demostración: Sea $\mathbf{a} \in \mathbf{f}_1$. Por ⟨1⟩1 $\mathbf{f}_1$ es una función y así existen $\mathbf{x} \in \mathbf{X}_1, \mathbf{y} \in \mathbf{Y}_1$ tales que $\mathfrak{M} \vDash \mathbf{a} = (\mathbf{x}, \mathbf{y}) \in \mathbf{f}_1$. Pero por ⟨2⟩1, particularizando la parte derecha de la conjunción con $\mathbf{x}$ obtenemos que $\mathfrak{M} \vDash (\mathbf{x}, \mathbf{y}) \in \mathbf{f}_2$, como queríamos.

⟨2⟩3. $\mathfrak{M} \vDash \mathbf{f}_2 \subseteq \mathbf{f}_1$.

Demostración: Análogo a ⟨2⟩2 (para este apartado necesitamos la parte izquierda de la conjunción de ⟨2⟩1 para usar la parte derecha)

⟨2⟩4. Q.E.D.

Demostración: Gracias a ⟨2⟩2 y ⟨2⟩3.

⟨1⟩4. Q.E.D.

Demostración: Las dos direcciones quedan probadas con ⟨1⟩2 y ⟨1⟩3.

□

Definimos el concepto de función inyectiva, ya que nos será útil más adelante.

Definición 2.4 (**Función inyectiva**)**.** Definimos

$$\textsc{Iny}[f] :\equiv \exists X, Y \exists f : X \longrightarrow Y \forall x, y. f(x) = f(y) \longrightarrow x = y.$$

■

Teorema 2.10 (**Composición**)**.**

$$RCA_0 \vdash \forall X, Y, Z \forall f : X \longrightarrow Y \forall g : Y \longrightarrow Z \exists^1 h : X \longrightarrow Z \forall i \in X. h(i) = g(f(i)).$$

A esa única h se le llama composición de f y g y se le denota gf o $g \circ f$.

Demostración:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA$_0$, $\mathbf{X}, \mathbf{Y}, \mathbf{Z}, \mathbf{f}, \mathbf{g} \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \mathbf{f} : \mathbf{X} \longrightarrow \mathbf{Y}$ y $\mathfrak{M} \vDash \mathbf{g} : \mathbf{Y} \longrightarrow \mathbf{Z}$.

⟨1⟩2. $\mathfrak{M} \vDash \exists h : \mathbf{X} \longrightarrow \mathbf{Z} \forall i \in \mathbf{X}. h(i) = \mathbf{g}(\mathbf{f}(i))$.

⟨2⟩1. $\mathfrak{M} \vDash (\exists j.(i,j) \in \mathbf{f} \wedge (j,k) \in \mathbf{g}) \leftrightarrow (i \in \mathbf{X} \wedge \forall j.(i,j) \in \mathbf{f} \rightarrow (j,k) \in \mathbf{g})$.

Demostración: Por ⟨1⟩1.

⟨2⟩2. $\mathfrak{M} \vDash (\exists i, k \leq c.c = (i,k) \wedge (\exists j.(i,j) \in \mathbf{f} \wedge (j,k) \in \mathbf{g})) \leftrightarrow$
$(\exists i, k \leq c.c = (i,k) \wedge (i \in \mathbf{X} \wedge \forall j.(i,j) \in \mathbf{f} \rightarrow (j,k) \in \mathbf{g}))$

Demostración: Por ⟨2⟩1, sustituyendo fórmulas equivalentes.

⟨2⟩3. Existe $\mathbf{h} \in \wp(\mathbb{N})$ tal que
$\mathfrak{M} \vDash \forall c.c \in \mathbf{h} \leftrightarrow (\exists i, k \leq c.c = (i,k) \wedge \exists j.(i,j) \in \mathbf{f} \wedge (j,k) \in \mathbf{g})$.

Demostración: De ⟨2⟩2 se demuestra que la fórmula es Δ^0_1, ya que gracias la parte izquierda de la equivalencia es Σ^0_1 y la derecha Π^0_1. Por tanto para demostrar ⟨2⟩3 sólo hace falta aplicar Δ^0_1-comprensión.

⟨2⟩4. $\mathfrak{M} \vDash \mathbf{h} : \mathbf{X} \longrightarrow \mathbf{Z}$.

Demostración: Se demuestra usando ⟨2⟩3 y las hipótesis de $\mathbf{f}, \mathbf{g}$ de ⟨1⟩1.

⟨2⟩5. Sea $\mathbf{i} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{i} \in \mathbf{X}$ cualquiera, entonces $\mathfrak{M} \vDash \mathbf{h}(\mathbf{i}) = \mathbf{g}(\mathbf{f}(\mathbf{i}))$.

Demostración: Se sigue de que $\mathbf{f}, \mathbf{g}, \mathbf{h}$ son funciones por ⟨1⟩1 y ⟨2⟩4 y de la definición de $\mathbf{h}$ de ⟨2⟩3.

⟨2⟩6. Q.E.D.

⟨1⟩3. Unicidad

Demostración: Se sigue del teorema 2.9 de igualdad de funciones.

⟨1⟩4. Q.E.D.

□

Lema 2.11 (**Función característica**). $RCA_0 \vdash \forall X \exists^1 f : \mathbb{N} \longrightarrow \{0,1\} \forall i. i \in X \leftrightarrow f(i) = 1$. *La única función que cumple eso se llama función característica de X y se denota χ_X.*

Demostración: Sea $\mathfrak{M}$ un modelo de RCA_0 y sea $\mathbf{X} \in \wp(\mathbb{N})$. La existencia se tiene por Σ^0_0-comprensión en la fórmula:

$$\varphi[n] :\equiv \exists i, j. n = (i,j) \wedge (i \in \mathbf{X} \to j = 1) \wedge (i \notin \mathbf{X} \to j = 0).$$

Es sencillo probar que es una función y la igualdad sale del teorema de igualdad de funciones. □

Lema 2.12 (**Proyecciones**).

$$RCA_0 \vdash \exists^1 f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \exists^1 g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \forall n \in \mathbb{N} \times \mathbb{N}. n = (f(n), g(n)).$$

A f la llamaremos fst *y a g la llamaremos* snd.

Demostración: Basta con definir los conjuntos por Σ^0_0-COMP:

$$\varphi_f[n] :\equiv \exists i, j. n = ((i,j), i),$$
$$\varphi_g[n] :\equiv \exists i, j. n = ((i,j), j).$$

□

Lema 2.13 (**Función producto**).

$$RCA_0 \vdash \forall X_1, X_2, Y_1, Y_2 \forall f_1 : X_1 \longrightarrow Y_1, f_2 : X_2 \longrightarrow Y_2 \exists! g : X_1 \times X_2 \longrightarrow Y_1 \times Y_2$$

$$\forall x_1 \in X_1 \forall x_2 \in X_2. g(x_1, x_2) = (f(x_1), f(x_2)).$$

Esta función se llama función producto de f_1 y f_2 y se denotará como $f_1 \times f_2$.

Demostración: Sea $\mathfrak{M}$ un modelo de RCA_0 y sean $\mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}_1, \mathbf{Y}_2 \subseteq \mathbb{N}$ y $\mathbf{f}_1 : \mathbf{X}_1 \longrightarrow \mathbf{Y}_1$, $\mathbf{f}_2 : \mathbf{X}_2 \longrightarrow \mathbf{Y}_2$. Para demostrar la existencia, usamos Σ^0_0-COMP en la fórmula:

$$\varphi[n] :\equiv \exists x_1, x_2, y_1, y_2. n = ((x_1, x_2), (y_1, y_2)) \wedge (x_1, y_1) \in \mathbf{f}_1 \wedge (x_2, y_2) \in \mathbf{f}_2.$$

Se demuestra sin problemas que es una función y que cumple lo pedido. La unicidad viene de la igualdad de funciones. □

Lema 2.14 (**Restricción de funciones**).

$$RCA_0 \vdash \forall X, X', Y \forall f : X \longrightarrow Y. X' \subseteq X \to \exists^1 f' : X' \longrightarrow X \forall x \in X'. f'(x) = f(x).$$

A esta única función la llamaremos $f \restriction X'$.

Demostración: Basta usar Σ^0_0-COMP en la fórmula

$$\varphi[n] :\equiv \exists i, j. n = (i,j) \wedge i \in \mathbf{X}' \wedge (i,j) \in \mathbf{f}.$$

Probar que cumple lo pedido es fácil. □

Lema 2.15 (**Función diagonal**)**.**

$$RCA_0 \vdash \exists^1 f : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N} \forall i. f(i) = (i, i).$$

A esta función la llamaremos diag*.*

Demostración: Basta con usar Σ^0_0-COMP en la fórmula

$$\varphi[n] :\equiv \exists i. n = (i, i).$$

□

Nota. Cabe destacar que la restricción de los principios únicamente a ciertos escalones de la jerarquía y el uso de funciones definidas (que no están en el lenguaje) puede causar cierta preocupación. Una forma de resolver tal conflicto es el siguiente. Supongamos que tenemos una variable que representa una función $f : \mathbb{N} \longrightarrow \mathbb{N}$ y consideramos la fórmula $f(i) < j$. Esta fórmula es una abreviatura de $\exists x.(i, x) \in f \wedge x < j$, pero por ser f una función será equivalente a $\forall x.(i, x) \in f \to x < j$ y por tanto la fórmula será Δ^0_1. Puesto que tenemos tanto Δ^0_1-COMP como Σ^0_1-IND en RCA$_0$, todos los principios se pueden aplicar a esta fórmula sin ningún problema.

Otra forma de solucionarlo sería la siguiente. Se puede demostrar por Σ^0_0-COMP que las funciones primitivas $+, \cdot$ tienen cada una un conjunto que cumple nuestra condición de función. Además de la misma forma se demuestra que las relaciones primitivas $=, <$ tienen un conjunto (subconjunto de $\mathbb{N} \times \mathbb{N}$) que representa la relación, y por el lema 2.11, estos conjuntos tienen función característica. Por tanto, cuando tengamos algo de la forma $\mathbf{R}(t_1, \ldots, t_n)$, donde R es una relación (primitiva o definida) y $t_1, \ldots, t_n$ son términos (con funciones y constantes primitivas o definidas), podemos ver que $\mathbf{R}(t_1, \ldots, t_n)$ es una fórmula Σ^0_0 con un parámetro. La idea sería usar la función producto y el teorema de la composición, para que al final la fórmula atómica sea equivalente a una de la forma $x \in \mathbf{X}$. Veamos un ejemplo, sean $\mathbf{f}_1 : \mathbf{X}_1 \times \mathbf{X}_2 \longrightarrow \mathbf{Y}, \mathbf{f}_2 : \mathbf{Y} \longrightarrow \mathbf{Y}, \mathbf{f}_3 : \mathbf{Z} \longrightarrow \mathbf{Y}, \mathbf{R} \subseteq \mathbf{Y} \times \mathbf{Y}$ y escribimos la fórmula $\mathbf{R}(\mathbf{f}_2(\mathbf{f}_1(x_1, x_2)), \mathbf{f}_3(z))$. Esta fórmula se entiende como $(((x_1, x_2), z), 1) \in \chi_{\mathbf{R}} \circ ((\mathbf{f}_2 \circ \mathbf{f}_1) \times \mathbf{f}_3)$ y notemos que esta fórmula es Σ^0_0 con un parámetro $\chi_{\mathbf{R}} \circ ((\mathbf{f}_2 \circ \mathbf{f}_1) \times \mathbf{f}_3)$, donde este conjunto existe gracias a los teoremas demostrados anteriormente. Por lo dicho antes lo mismo ocurriría si no solo aparecen símbolos no primitivos, sino si aparecen $+, -, =, <, \in$ Así cualquier fórmula que sea de esta manera será considerada Σ^0_0 con parámetros. Esta forma tiene la desventaja que se necesita que las funciones estén interpretadas, no se podría hacer si por ejemplo f_2 fuera una variable. ■

2.3. Algunos principios que se deducen de la inducción

En esta sección veremos algunos principios que se siguen de la Σ^0_1-IND, ya que nos será útil razonar con ellos más adelante. El primer principio que vamos a ver es la Π^0_1-IND,

ya que vamos a usar el concepto de función definido en la sección anterior.

Lema 2.16 (**Resta truncada**).

$RCA_0 \vdash \exists^1 f : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N} \forall n, m, r. f(m,n) = r \leftrightarrow (n \leq m \rightarrow n+r = m) \wedge (n > m \rightarrow r = 0)$.

A $f(m,n)$ lo denotaremos como $m \dot{-} n$.

Demostración: Mediante una Σ^0_0-COMP se prueba la existencia, el resto de propiedades son fáciles de comprobar. □

Con esta operación definida ya podemos probar la Π^0_1-IND.

Teorema 2.17. *$RCA_0 \vdash \Pi^0_1$-IND.*

Demostración:
⟨1⟩1. Sea $\varphi\{n\} \in \Pi^0_1$, $\nu_1, \ldots, \nu_k = \mathrm{Vl}(\varphi\{n\}) \setminus \{n\}$ y $\mathfrak{M}$ un modelo de RCA_0.

⟨1⟩2. Definimos $\psi :\equiv \varphi\{0\} \wedge (\forall n.\varphi\{n\} \rightarrow \varphi\{n+1\}) \rightarrow \forall n.\varphi\{n\}$.

⟨1⟩3. $\mathrm{Vl}(\psi) = \{\nu_1, \ldots, \nu_k\}$

Demostración: Se comprueba fácilmente por definición de variable libre y las hipótesis de ⟨1⟩1 y ⟨1⟩2.

⟨1⟩4. Sean $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k \in \mathbb{N} \cup \wp(\mathbb{N})$ denotemos $\varphi[n] :\equiv \varphi[n, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k]$. Entonces:
$$\boldsymbol{\psi} :\equiv \psi[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k] \equiv \varphi[0] \wedge (\forall n.\varphi[n] \rightarrow \varphi[n+1]) \rightarrow \forall n.\varphi[n]$$
y es suficiente probar que $\mathfrak{M} \vDash \boldsymbol{\psi}$.

Demostración: Que sean iguales es gracias a la definición de sustitución y que sea suficiente probar eso es gracias a la completitud.

⟨1⟩5. Supongamos que $\mathfrak{M} \vDash \varphi[0]$ y $\mathfrak{M} \vDash \forall n.\varphi[n] \rightarrow \varphi[n+1]$ pero que $\mathfrak{M} \vDash \neg\forall n.\varphi[n]$.

⟨1⟩6. Existe $\mathbf{n} \in \mathfrak{M}$ tal que $\mathfrak{M} \vDash \neg\varphi[\mathbf{n}]$.

Demostración: Por la última hipótesis de ⟨1⟩5.

⟨1⟩7. $\mathfrak{M} \vDash \neg\varphi[\mathbf{n} \dot{-} 0]$.

Demostración: Ya que $\mathfrak{M} \vDash \mathbf{n} \dot{-} 0 = \mathbf{n}$ y ⟨1⟩6.

⟨1⟩8. $\mathfrak{M} \vDash \forall m.\neg\varphi[\mathbf{n} \dot{-} m] \rightarrow \neg\varphi[\mathbf{n} \dot{-} (m+1)]$.

Demostración: Sea $\mathbf{m} \in \mathbb{N}$ y probemos el contrapuesto, i.e. $\mathfrak{M} \vDash \varphi[\mathbf{n} \dot{-} (\mathbf{m}+1)] \rightarrow \varphi[\mathbf{n} \dot{-} \mathbf{m}]$. Ahora bien, si $\mathfrak{M} \vDash \mathbf{n} \dot{-} \mathbf{m} = 0$, entonces también $\mathfrak{M} \vDash \mathbf{n} \dot{-} (\mathbf{m}+1) = 0$ y la implicación a probar es trivial. En caso contrario, es fácil ver que $\mathfrak{M} \vDash (\mathbf{n} \dot{-} (\mathbf{m}+1)) + 1 = \mathbf{n} \dot{-} \mathbf{m}$ y por tanto la implicación se deduce de ⟨1⟩5.

⟨1⟩9. $\mathfrak{M} \vDash \neg\varphi[0]$.

DEMOSTRACIÓN: Sabemos que $\neg\varphi[\mathbf{n} \dot{-} m] \in (\mathbf{\Sigma_1^0})_{\mathfrak{M}}$, por ser la negación de una fórmula en Π_1^0, por tanto le podemos aplicar Σ_1^0-IND a ⟨1⟩7 y ⟨1⟩8 para obtener que $\mathfrak{M} \vDash \forall m.\neg\varphi[\mathbf{n} \dot{-} m]$, el resultado se obtiene escogiendo $m = \mathbf{n}$.

⟨1⟩10. Q.E.D.

DEMOSTRACIÓN: ⟨1⟩9 se contradice con la hipótesis de ⟨1⟩2 que dice que $\mathfrak{M} \vDash \varphi[0]$, por tanto hemos llegado a un absurdo y $\mathfrak{M} \vDash \forall n.\varphi[n]$.

□

Veamos ahora el principio de acotación. Este lo usaremos más adelante fuera de RCA$_0$, así que no lo probamos sólo para RCA$_0$ o extensiones de esta, sino para cualquier modelo de L_2 que cumpla los axiomas básicos y Σ_1^0-IND.

Definición 2.5 (**Γ-acotación**)**.** Sea $\Gamma \subseteq \text{Form}$. Definimos el conjunto de los axiomas de acotación para Γ, denotado Γ-BOUND, como el conjunto de todas las fórmulas

$$(\forall n < t \exists m.\varphi\{n, m\}) \to (\exists p \forall n < t \exists m < p.\varphi\{n, m\}),$$

donde $n, m, p \in \text{Var}_{\text{N}}$, $t \in \text{TNum}$, $\varphi\{n, m\} \in \Gamma$, $n \notin \text{Vl}(t)$, $p \notin \text{Vl}(\varphi) \cup \text{Vl}(t)$. ■

Teorema 2.18. *Sea $\mathfrak{M}$ un modelo de L_2 tal que $\mathfrak{M} \vDash BASIC + \Sigma_1^0\text{-}IND$. Entonces*

$$\mathfrak{M} \vDash \Sigma_1^0\text{-}BOUND.$$

DEMOSTRACIÓN:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de L_2 tal que $\mathfrak{M} \vDash \text{BASIC} + \Sigma_1^0\text{-IND}$.

⟨1⟩2. $\mathfrak{M} \vDash \Sigma_0^0\text{-BOUND}$.

⟨2⟩1. Sea $\varphi\{n, m\} \in \Sigma_0^0$, $t \in \text{TNum}$ y $p \in \text{Var}_{\text{N}}$ cualesquiera tales que $\{\nu_1, \ldots, \nu_k\} = (\text{Vl}(\varphi\{n, m\}) \cup \text{Vl}(t)) \setminus \{n, m\}$, $n \notin \text{Vl}(t)$, $p \notin \text{Vl}(\varphi) \cup \text{Vl}(t)$.

⟨2⟩2. Definamos
$$\psi :\equiv (\forall n < t \exists m.\varphi\{n, m\}) \to (\exists p \forall n < t \exists m < p.\varphi\{n, m\}).$$

⟨2⟩3. $\text{Vl}(\psi) = \{\nu_1, \ldots, \nu_k\}$.

DEMOSTRACIÓN: Gracias a la definición de Vl y a las hipótesis de ⟨2⟩1 y ⟨2⟩2.

⟨2⟩4. Sean $\boldsymbol{\nu}_1 \ldots . \boldsymbol{\nu}_k \in \mathbb{N} \cup \wp(\mathbb{N})$ denotamos $\varphi[n, m] :\equiv \varphi[n, m, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k]$ y $\mathbf{t} :\equiv t[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k]$. Entonces
$$\boldsymbol{\psi} :\equiv \psi[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k] \equiv (\forall n < \mathbf{t} \exists m.\varphi[n, m]) \to (\exists p \forall n < \mathbf{t} \exists m < p.\varphi[n, m]),$$
es suficiente probar $\mathfrak{M} \vDash \boldsymbol{\psi}$.

DEMOSTRACIÓN: Que sean iguales es gracias a la definición de sustitución y que sea suficiente probar eso es gracias a la completitud.

⟨2⟩5. Supongamos que $\mathfrak{M} \vDash \forall n < \mathbf{t} \exists m.\varphi[n, m]$.

⟨2⟩6. $\mathfrak{M} \vDash \forall a.(\exists p \forall n < a \exists m < p.\varphi[n, m]) \vee a > \mathbf{t}$.

⟨3⟩1. Sea $\theta[a] :\equiv (\exists p \forall n < a \exists m < p.\varphi[n, m]) \vee a > \mathbf{t}$.

⟨3⟩2. $\mathfrak{M} \vDash \theta[0]$.

DEMOSTRACIÓN: Trivial.

⟨3⟩3. $\mathfrak{M} \vDash \forall a.\theta[a] \to \theta[a + 1]$.

DEMOSTRACIÓN: Sea $\mathbf{a} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \theta[\mathbf{a}]$. Si $\mathfrak{M} \vDash \mathbf{a} + 1 > \mathbf{t}$ entonces hemos terminado pues se cumple la segunda parte de la disyunción. Así supongamos que $\mathfrak{M} \vDash \mathbf{a} + 1 \leq \mathbf{t}$ y por tanto $\mathfrak{M} \vDash \mathbf{a} < \mathbf{t}$, así que como $\mathfrak{M} \vDash \theta[a]$ tenemos que existe $\mathbf{p} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall n < \mathbf{a} \exists m < \mathbf{p}.\varphi[n, m]$. Ahora, por ⟨2⟩5 sabemos que existe $\mathbf{m} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \varphi[\mathbf{a}, \mathbf{m}]$ así que tomando como $\mathbf{p}'$ el mayor entre $\mathbf{p}$ y $\mathbf{m} + 1$ tenemos que

$$\mathfrak{M} \vDash \forall n < \mathbf{a} + 1 \exists m < \mathbf{p}'.\varphi[n, m],$$

de donde se sigue que $\mathfrak{M} \vDash \theta[\mathbf{a} + 1]$.

⟨3⟩4. Q.E.D.

DEMOSTRACIÓN: Por Σ^0_1-IND, siendo ⟨3⟩2 el caso base y ⟨3⟩3 el paso inductivo.

⟨2⟩7. Q.E.D.

DEMOSTRACIÓN: Se sigue de ⟨2⟩5 tomando $a = \mathbf{t}$.

⟨1⟩3. Q.E.D.

DEMOSTRACIÓN: Para ver que se tiene Σ^0_1-BOUND, basta notar que, dada $\varphi[n, m] \in \Sigma^0_1$ (podemos suponer ya que las otras variables libres han sido sustituidas por constantes del modelo), existe $\theta(n, m, y) \in (\Sigma^0_0)_{\mathfrak{M}}$ tal que $\varphi[n, m] \equiv \exists y.\theta(n, m, y)$. Por tanto, de $\mathfrak{M} \vDash \forall n < \mathbf{t} \exists m, y.\theta(n, m, y)$ se sigue que $\mathfrak{M} \vDash \forall n < \mathbf{t} \exists z.\exists m, y \leq z.z = (m, y) \wedge \theta(n, m, y)$, pues gracias a las propiedades del par ordenado son fórmulas equivalentes. Pero a esta fórmula se le puede aplicar Σ^0_0-BOUND y, por tanto,

$$\mathfrak{M} \vDash \exists p \forall n < t \exists z < p.\exists m, y \leq z.z = (m, y) \wedge \theta(n, m, y).$$

Por las propiedades del par ordenado (en particular que $\mathfrak{M} \vDash m \leq (m, y)$) tenemos que por tanto

$$\mathfrak{M} \vDash \exists p \forall n < t \exists m < p \exists y.\theta(n, m, y) \equiv \exists p \forall n < t \exists m < p.\varphi[n, m]$$

como queríamos.

□

Corolario 2.19. *$RCA_0 \vdash \Sigma^0_1$-BOUND.*

Gracias a este teorema podemos demostrar algunas propiedades más sobre la jerarquía aritmética que nos serán útiles más adelante.

Lema 2.20. *Sean $t \in \mathrm{TNum}$, $x \notin \mathrm{Vl}(t)$.*

1. *Si $\varphi \in \Pi^0_1$, entonces $\exists x < t.\varphi \in (\mathbf{\Pi^0_1})^{RCA_0}$.*
2. *Si $\varphi \in \Sigma^0_1$, entonces $\forall x < t.\varphi \in (\mathbf{\Sigma^0_1})^{RCA_0}$.*

Demostración: Claramente 1. se sigue de 2. usando que $\vdash (\exists x < t.\varphi) \leftrightarrow (\neg\forall x < t.\neg\varphi)$. Para probar 2. basta usar el corolario anterior (en particular Σ^0_0-BOUND). □

Nota. Esto se podría generalizar a que Σ^0_k-IND (con BASIC) demuestra Σ^0_k-BOUND y eso implica el lema 2.20 para fórmulas en Π^0_k y Σ^0_k.

Con esto podríamos probar (siempre que nuestra teoría tenga un principio de inducción suficientemente fuerte) que toda fórmula $\varphi \in \Sigma^0_{k+1}$ es equivalente a otra fórmula Σ^0_{k+1} de la forma $\exists z.\theta$ con $\theta \in \Pi^0_k$. La clave es que $\varphi \equiv \exists x_1, \ldots, x_n.\varphi'$ con $\varphi' \in \Pi^0_k$, por definición de Σ^0_{k+1}, así que basta con construir fórmula $\exists z.\exists x_1, \ldots, x_n \leq z.z = (x_1, \ldots, x_n) \wedge \varphi'$ donde z es una variable nueva. Claramente las fórmulas son equivalentes y $\exists x_1, \ldots, x_n \leq z.z = (x_1, \ldots, x_n) \wedge \varphi'$ es equivalente a una en Π^0_k (por ser el lema 2.20 cierto para Π^0_k). Si θ es la fórmula a la que es equivalente, entonces la fórmula buscada será $\exists z.\theta$.

Así, cuando la teoría en la que estemos trabajando lo permita, será habitual hacer el siguiente razonamiento: sea $\varphi \in \Sigma^0_{k+1}$, entonces existe $\psi \in \Pi^0_k$ tal que $\varphi \equiv \exists z.\psi$. Realmente detrás de este razonamiento se esconde todo el proceso anterior y estamos abusando de notación, ya que no son iguales sintácticamente, aún así cuando este razonamiento se use eso no supondrá ningún problema. Obviamente si $\varphi \in \Pi^0_{k+1}$ el proceso es análogo. ■

Gracias a esto podemos probar el principio de inducción fuerte.

Definición 2.6 (**Γ-inducción fuerte**)**.** Sea $\Gamma \subseteq \mathrm{Form}$. Definimos el conjunto de los axiomas de inducción fuerte para Γ, denotado Γ-SIND, como el conjunto de todas las fórmulas

$$(\forall n.(\forall m < n.\varphi\{m\}) \to \varphi\{n\}) \to \forall n.\varphi\{n\}$$

donde $n, m \in \mathrm{Var_N}, \varphi\{n\} \in \Gamma, m \notin \mathrm{Vl}(\varphi)$. ■

Teorema 2.21. *$RCA_0 \vdash \Sigma^0_1 - SIND$ y $RCA_0 \vdash \Pi^0_1 - SIND$.*

Demostración: Es fácil aplicando Σ^0_1-IND (o Π^0_1-IND) en n sobre la fórmula

$$\forall m < n.\varphi\{m\},$$

donde $\varphi \in \Sigma^0_1$ (o $\varphi \in \Pi^0_1$). Podemos aplicar la inducción gracias al lema 2.20. □

Probamos ahora el principio de existencia del elemento mínimo, que definimos a continuación.

Definición 2.7 (**Γ-elemento mínimo**)**.** Sea $\Gamma \subseteq \text{Form}$. Definimos el conjunto de los axiomas del elemento mínimo para Γ, denotado Γ-MIN, como el conjunto de todas las fórmulas

$$(\exists n.\varphi\{n\}) \to \exists n.\varphi\{n\} \wedge \neg\exists m < n.\varphi\{m\},$$

donde $n, m \in \text{Var}_{\text{N}}$, $\varphi\{n\} \in \Gamma$, $m \notin \text{Vl}(\varphi)$. ■

Teorema 2.22. *$RCA_0 \vdash \Sigma^0_1$-MIN y $RCA_0 \vdash \Pi^0_1$-MIN.*

Demostración: Se prueba como es habitual usando el principio de inducción fuerte. □

2.4. Conjunto cociente

Primero definimos qué es una relación binaria sobre un conjunto.

Definición 2.8 (**Relación binaria**)**.** Definimos

$$\text{BinRel}[R, X] :\equiv R \subseteq X \times X$$

y en ese caso decimos que R es una relación binaria en X o sobre X.

Si R es una relación binaria sobre X y $x \in X \times X$ escribiremos $R(x)$ directamente en lugar de $x \in R$, y $\neg R(x)$ en lugar de $x \notin R$. ■

Definimos ahora la noción de relación de equivalencia.

Definición 2.9 (**Relación de equivalencia**)**.** Definimos

$$\text{Equiv}[R, X] :\equiv \text{BinRel}[R, X] \wedge (\forall x \in X.R(x, x)) \wedge (\forall x, y \in X.R(x, y) \to R(y, x)) \wedge$$

$$(\forall x, y, z \in X.R(x, y) \wedge R(y, z) \to R(x, z))$$

y en ese caso se dice que R es una relación de equivalencia sobre X. ■

Como de costumbre, cuando tenemos una relación de equivalencia nos interesa identificar los elementos equivalentes como el mismo. Sin embargo, no podemos proceder con la construcción habitual de clases de equivalencia, ya que para ello sería necesario usar conjuntos de conjuntos, es decir, trabajar en la aritmética de tercer orden. Sin embargo, podemos usar la sección anterior ya que dada una fórmula con ciertas condiciones podemos encontrar un elemento mínimo que la cumpla (si existe alguno que la cumple). Así, en lugar de trabajar con clases de equivalencia tomaremos un representante de cada clase, el mínimo respecto al orden $<$.

Lema 2.23 (**Conjunto cociente**)**.**

$$RCA_0 \vdash \forall X \forall R.\textsc{Equiv}[R, X] \to \exists^1 Y.Y = \{y \mid y \in X \wedge \neg\exists x < y.R(x, y)\}.$$

A este único conjunto Y lo denotamos X/R y lo llamamos cociente de X sobre R.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{X}, \mathbf{R} \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \textsc{Equiv}[\mathbf{R}, \mathbf{X}]$.

⟨1⟩2. Existencia

Demostración: Se obtiene de Σ^0_0-COMP aplicada a la fórmula
$$\varphi[y] :\equiv y \in \mathbf{X} \wedge \neg\exists x < y.(x, y) \in \mathbf{R}$$
donde $\mathbf{X}$ y $\mathbf{R}$ son parámetros.

⟨1⟩3. Unicidad

Demostración: Se obtiene a partir de la definición de igualdad de conjuntos.

⟨1⟩4. Q.E.D.

□

La siguiente propiedad expresa que cada clase de equivalencia tiene un único representante en X/R (aunque lo expresa sin usar clases de equivalencia).

Lema 2.24. $RCA_0 \vdash \forall X, R.\textsc{Equiv}[R, X] \to \forall x \in X \exists^1 y \in X/R.R(x, y)$.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 con $\mathbf{X}, \mathbf{R} \in \wp(\mathbb{N})$ con $\mathfrak{M} \vDash \textsc{Equiv}[\mathbf{R}, \mathbf{X}]$ y $\mathbf{x} \in \mathbf{X}$.

⟨1⟩2. $\mathfrak{M} \vDash \exists y.\mathbf{R}(\mathbf{x},y)$

Demostración: Basta con poner $y = \mathbf{x}$.

⟨1⟩3. Existe un único $\mathbf{y} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{R}(\mathbf{x}, \mathbf{y}) \wedge \neg\exists z < \mathbf{y}.\mathbf{R}(\mathbf{x}, z)$

Demostración: Basta con aplicar Σ^0_0-MIN a $(\mathbf{R}(\mathbf{x}, y)) \in \Sigma^0_0$.

⟨1⟩4. $\exists^1 y.\mathbf{R}(\mathbf{x}, y) \wedge \neg\exists z < y.\mathbf{R}(y, z)$

⟨2⟩1. $\mathfrak{M} \vDash \mathbf{R}(\mathbf{x}, \mathbf{y}) \wedge \neg\exists z < \mathbf{y}.\mathbf{R}(\mathbf{y}, z)$

Demostración: Sea $\mathbf{z} \in \mathbf{N}$ tal que $\mathfrak{M} \vDash \mathbf{z} < \mathbf{y} \wedge \mathbf{R}(\mathbf{y}, \mathbf{z})$, como $\mathfrak{M} \vDash \mathbf{R}(\mathbf{x}, \mathbf{z})$ por ⟨1⟩3 y $\mathfrak{M} \vDash \textsc{Equiv}[\mathbf{R}, \mathbf{X}]$ por ⟨1⟩1 obtenemos $\mathfrak{M} \vDash \mathbf{z} < \mathbf{y} \wedge \mathbf{R}(\mathbf{x}, \mathbf{z})$, lo cual entra encontradicción con ⟨1⟩3. Por tanto $\mathfrak{M} \vDash \neg\exists z < \mathbf{y}.\mathbf{R}(\mathbf{y}, z)$ y por ⟨1⟩3, $\mathfrak{M} \vDash \mathbf{R}(\mathbf{x}, \mathbf{y}) \wedge \neg\exists z < \mathbf{y}.\mathbf{R}(\mathbf{y}, z)$.

⟨2⟩2. $\mathfrak{M} \vDash \forall y'.\mathbf{R}(\mathbf{x}, y') \wedge \neg\exists z < y'.\mathbf{R}(y', z) \to \mathbf{y} = y'$.

DEMOSTRACIÓN: Sea $\mathbf{y}' \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{R}(\mathbf{x}, \mathbf{y}') \wedge \neg\exists z < \mathbf{y}'.\mathbf{R}(\mathbf{y}', z)$. Eso implica que $\mathfrak{M} \vDash \mathbf{R}(\mathbf{x}, \mathbf{y}') \wedge \neg\exists z < \mathbf{y}'.\mathbf{R}(\mathbf{x}, z)$ y por $\langle 1\rangle 3$ $\mathfrak{M} \vDash \mathbf{y} = \mathbf{y}'$.

$\langle 2\rangle 3$. Q.E.D.

DEMOSTRACIÓN: $\langle 2\rangle 1$ da la existencia y $\langle 2\rangle 2$ da la unicidad.

$\langle 1\rangle 5$. Q.E.D.

DEMOSTRACIÓN: Ya que por definición de $\mathbf{X}/\mathbf{R}$,

$$\mathfrak{M} \vDash (\exists^1 y \in \mathbf{X}/\mathbf{R}.\mathbf{R}(\mathbf{x}, y)) \leftrightarrow (\exists^1 y.y \in \mathbf{X} \wedge (\neg\exists z < y.\mathbf{R}(z, y)) \wedge \mathbf{R}(\mathbf{x}, y)) \leftrightarrow$$
$$\leftrightarrow (\exists^1 y.y \in \mathbf{X} \wedge \mathbf{R}(\mathbf{x}, y) \wedge (\neg\exists z < y.\mathbf{R}(y, z))) \leftrightarrow (\exists^1 y.\mathbf{R}(\mathbf{x}, y) \wedge (\neg\exists z < y.\mathbf{R}(y, z)))$$

donde la segunda equivalencia es por conmutatividad de $\wedge$ y de $\mathbf{R}$ y la útlima gracias a que $\mathfrak{M} \vDash (x \in \mathbf{X} \wedge \mathbf{R}(x, y)) \leftrightarrow \mathbf{R}(x, y)$, por ser $\mathbf{R}$ una relación binaria sobre $\mathbf{X}$.

□

Con este lema podemos probar varias cosas que se usan normalmente en el razonamiento de conjuntos cociente. El primer ejemplo es que si $x, y \in X/R$ cumple que $R(x, y)$ entonces $x = y$.

Lema 2.25. $RCA_0 \vdash \forall X, R.\text{EQUIV}[R, X] \to \forall x, y \in X/R.R(x, y) \to x = y$.

DEMOSTRACIÓN: Trivial por lema 2.24 usando que $X/R \subseteq X$ por su definición. □

También podemos construir una función que dado un elemento de X nos dé su representante en X/R.

Lema 2.26. $RCA_0 \vdash \forall X, R.\text{EQUIV}[R, X] \to \exists^1 f : X \longrightarrow X/R \forall x \in X.R(x, f(x))$.

A esta función la denotaremos $\pi_{X/R}$.

DEMOSTRACIÓN:
$\langle 1\rangle 1$. Sea $\mathfrak{M}$ un modelo de RCA_0, $\mathbf{X}, \mathbf{R} \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \text{EQUIV}[\mathbf{R}, \mathbf{X}]$.

$\langle 1\rangle 2$. Existencia

DEMOSTRACIÓN: Basta usar Σ^0_0-comprensión en la fórmula con parámetros

$$\phi[z] :\equiv \exists x, y \leq z.z = (x, y) \wedge y \in \mathbf{X}/\mathbf{R} \wedge (x, y) \in \mathbf{R}.$$

Cumple que es una función gracias al lema 2.24.

$\langle 1\rangle 3$. Unicidad

DEMOSTRACIÓN: Sean $\mathbf{f}_1, \mathbf{f}_2$ funciones que cumplan la propiedad. Usando lema 2.9 para demostrar igualdad de funciones, ya que tienen el mismo dominio basta ver que $\mathfrak{M} \vDash \forall x \in \mathbf{X}.\mathbf{f}_1(x) = \mathbf{f}_2(x)$. Sea $\mathbf{x} \in \mathbf{X}$, como $\mathfrak{M} \vDash \mathbf{R}(\mathbf{x}, \mathbf{f}_1(\mathbf{x})) \wedge \mathbf{R}(\mathbf{x}, \mathbf{f}_2(\mathbf{x}))$, al ser $\mathbf{R}$

de equivalencia tenemos $\mathfrak{M} \vDash \mathbf{R}(\mathbf{f}_1(\mathbf{x}), \mathbf{f}_2(\mathbf{x}))$ y como ambos son elementos de $\mathbf{R}/\mathbf{X}$ se tiene por lema 2.26 que son iguales, como queríamos.

⟨1⟩4. Q.E.D.

□

2.5. Algo de teoría de números elemental

Nuestro objetivo es ser capaces de codificar conjuntos finitos mediante elementos de $\mathbb{N}$. Para ello primero necesitamos desarrollar dos conceptos de teoría de números, el de divisibilidad y el de coprimalidad.

Definición 2.10 (**Divisibilidad**)**.** Definimos $m \mid n :\equiv \exists q.mq = n$ y se dice que m divide a n o que n es divisible por m. ■

Lema 2.27. $(m \mid n) \in (\mathbf{\Sigma_0^0})^{RCA_0}$.

Demostración:
⟨1⟩1. Vamos a probar que $\mathrm{RCA}_0 \vdash m \mid n \leftrightarrow (\exists q' \leq n.mq' = n)$.

⟨1⟩2. Sea $\mathfrak{M}$ un modelo de RCA_0, $\mathbf{m}, \mathbf{n} \in \mathbb{N}$ cualesquiera.

⟨1⟩3. $\mathfrak{M} \vDash \exists q' \leq \mathbf{n}.\mathbf{m}q' = \mathbf{n} \rightarrow \mathbf{m} \mid \mathbf{n}$.

Demostración: Es trivial.

⟨1⟩4. $\mathfrak{M} \vDash \mathbf{m} \mid \mathbf{n} \rightarrow \exists q' \leq \mathbf{n}.\mathbf{m}q' = \mathbf{n}$

Demostración: Sea $\mathbf{q} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{mq} = \mathbf{n}$. Lo hacemos por casos:
Si $\mathfrak{M} \vDash \mathbf{m} = 0$ entonces $\mathfrak{M} \vDash 0 = \mathbf{mq} = \mathbf{n}$ y basta escoger $\mathbf{q}' = 0$ ya que $\mathfrak{M} \vDash 0 \leq \mathbf{n}$.
Si $\mathfrak{M} \vDash \mathbf{m} \neq 0$, entonces $\mathfrak{M} \vDash 1 \leq \mathbf{m}$ y multiplicando por $\mathbf{q}$ se tiene que $\mathfrak{M} \vDash \mathbf{q} \leq \mathbf{mq} = \mathbf{n}$, así tomando $q' = \mathbf{q}$ se tiene lo pedido.

⟨1⟩5. Q.E.D.

□

A continuación enunciamos un par de lemas que usaremos más adelante.

Lema 2.28. $RCA_0 \vdash \forall n \neq 1.\neg(n \mid 1)$.

Demostración: Sean $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{n} \neq 1$. Supongamos que $\mathfrak{M} \vDash \mathbf{n} \mid 1$. Por la demostración de la propiedad anterior, existe un $\mathbf{q} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{q} \leq 1 \wedge 1 = \mathbf{nq}$, lo cual es fácil ver que es imposible distinguiendo casos sobre $\mathfrak{M} \vDash \mathbf{q} = 0 \vee \mathbf{q} = 1$. □

Lema 2.29. $RCA_0 \vdash \forall m, n, p.p \mid m + n \wedge p \mid n \to p \mid m$.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{m}, \mathbf{n}, \mathbf{p} \in \mathbb{N}$. Además supongamos que $\mathfrak{M} \vDash \mathbf{p} \mid \mathbf{m} + \mathbf{n}$ y que $\mathfrak{M} \vDash \mathbf{p} \mid \mathbf{n}$.

⟨1⟩2. Existen $\mathbf{q}_1, \mathbf{q}_2 \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{pq}_1 = \mathbf{m} + \mathbf{n}$ y $\mathfrak{M} \vDash \mathbf{pq}_2 = \mathbf{n}$.

Demostración: Gracias a la definición de | y ⟨1⟩1.

⟨1⟩3. Suponemos que $\mathfrak{M} \vDash \mathbf{m} \neq 0$.

Demostración: Si $\mathfrak{M} \vDash \mathbf{m} = 0$ entonces tendríamos trivialmente que $\mathfrak{M} \vDash \mathbf{p} \mid \mathbf{m} = 0$.

⟨1⟩4. Existe $\mathbf{q}_3 \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{q}_1 = \mathbf{q}_2 + \mathbf{q}_3$.

Como $\mathfrak{M} \vDash \mathbf{m} \neq \mathbf{0}$ se tiene que $\mathfrak{M} \vDash \mathbf{pq}_2 = \mathbf{n} < \mathbf{m} + \mathbf{n} = \mathbf{pq}_1$ y como $\mathfrak{M} \vDash \mathbf{p} \neq 0$ (por ser $\mathbf{m}$ no nulo y $\mathfrak{M} \vDash \mathbf{pq}_1 = \mathbf{m} + \mathbf{n}$) se tiene que $\mathfrak{M} \vDash \mathbf{q}_2 < \mathbf{q}_1$ (gracias a ser semianillo ordenado con cancelación). Por ser semianillo ordenado con cancelación se obtiene ⟨1⟩4.

⟨1⟩5. Q.E.D.

Demostración: Multiplicando ⟨1⟩4 por $\mathbf{p}$ obtenemos que $\mathfrak{M} \vDash \mathbf{pq}_1 = \mathbf{pq}_2 + \mathbf{pq}_3$ i.e. por ⟨1⟩2 $\mathfrak{M} \vDash \mathbf{m} + \mathbf{n} = \mathbf{n} + \mathbf{pq}_3$. Por ser un semianillo ordenado con cancelación se obtiene que $\mathfrak{M} \vDash \mathbf{m} = \mathbf{pq}_3$, como queríamos.

□

Definición 2.11 (**Números coprimos**)**.** Definimos

$$\textsc{Coprimes}[m_1, m_2] := m_1 \neq 0 \wedge m_2 \neq 0 \wedge \forall n.m_2 \mid m_1 n \to m_2 \mid n$$

y decimos que m_1 y m_2 son coprimos. ■

Como resulta natural, que m_1 y m_2 sean coprimos es equivalente a que m_2 y m_1 sean coprimos.

Lema 2.30. $RCA_0 \vdash \forall m_1, m_2.\textsc{Coprimes}[m_1, m_2] \to \textsc{Coprimes}[m_2, m_1]$.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{m}_1, \mathbf{m}_2 \in \mathbb{N}$, tales que $\mathfrak{M} \vDash \textsc{Coprimes}[\mathbf{m}_1, \mathbf{m}_2]$.

⟨1⟩2. $\mathfrak{M} \vDash \mathbf{m}_1 \neq 0 \wedge \mathbf{m}_2 \neq 0$.

Demostración: Por definición de Coprimes y ⟨1⟩1.

⟨1⟩3. $\mathfrak{M} \vDash \forall n.\mathbf{m}_1 \mid \mathbf{m}_2 n \to \mathbf{m}_1 \mid n$.

⟨2⟩1. Sea $\mathbf{n} \in \mathbb{N}$ cualquiera tal que $\mathfrak{M} \vDash \mathbf{m}_1 \mid \mathbf{m}_2 \mathbf{n}$.

⟨2⟩2. Existe un $\mathbf{q} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{m}_1\mathbf{q} = \mathbf{m}_2\mathbf{n}$.

DEMOSTRACIÓN: Por definición de $\mid$ y ⟨2⟩1.

⟨2⟩3. Existe un $\mathbf{r} \in \mathbb{N}$ tal que $\mathbf{m}_2\mathbf{r} = \mathbf{q}$.

DEMOSTRACIÓN: Por la igualdad ⟨2⟩2 se tiene que $\mathfrak{M} \vDash \mathbf{m}_2 \mid \mathbf{m}_1\mathbf{q}$ y como $\mathfrak{M} \vDash$ COPRIMES$[\mathbf{m}_1, \mathbf{m}_2]$ se obtiene que $\mathfrak{M} \vDash \mathbf{m}_2 \mid \mathbf{q}$.

⟨2⟩4. $\mathfrak{M} \vDash \mathbf{m}_1\mathbf{r} = \mathbf{n}$.

DEMOSTRACIÓN: Por las igualdades vistas hasta ahora $\mathfrak{M} \vDash \mathbf{m}_1\mathbf{m}_2\mathbf{r} = \mathbf{m}_1\mathbf{q} = \mathbf{m}_2\mathbf{n}$ y usando que $\mathfrak{M} \vDash \mathbf{m}_2 \neq 0$, cancelamos $\mathbf{m}_2$ de la igualdad y nos queda $\mathfrak{M} \vDash \mathbf{m}_1\mathbf{r} = \mathbf{n}$.

⟨2⟩5. Q.E.D.

⟨1⟩4. Q.E.D.

□

Ahora probamos que para cada número k existe un número que es divisible por cada $i < k$.

Lema 2.31. *$RCA_0 \vdash \forall k \exists m > 0 \forall i < k . i + 1 \mid m$.*

DEMOSTRACIÓN: La demostración es una simple Σ^0_1-IND en k. □

Finalmente demostramos el lema que nos permitirá la codificación de conjuntos finitos como elementos de $\mathbb{N}$, usando esa especie de "factorial"que nos da el lema anterior.

Lema 2.32.

$$RCA_0 \vdash \forall k \forall m > 0 . (\forall i < k . i + 1 \mid m) \rightarrow$$

$$(\forall i, j . i < j < k \rightarrow \textit{COPRIMES}[m(i+1)+1, m(j+1)+1]).$$

DEMOSTRACIÓN:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0, sean $\mathbf{k}, \mathbf{m} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{m} > 0$ y que $\mathfrak{M} \vDash \forall i < \mathbf{k} . i + 1 \mid \mathbf{m}$. Sean además $\mathbf{i}, \mathbf{j} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{i} < \mathbf{j} < \mathbf{k}$.

⟨1⟩2. $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \neq 0 \wedge \mathbf{m}(\mathbf{j}+1)+1 \neq 0$.

DEMOSTRACIÓN: Gracias a que $\mathfrak{M} \vDash$ BASIC.

⟨1⟩3. $\mathfrak{M} \vDash \forall n . \mathbf{m}(\mathbf{i}+1)+1 \mid (\mathbf{m}(\mathbf{j}+1)+1)n \rightarrow \mathbf{m}(\mathbf{i}+1)+1 \mid n$.

⟨2⟩1. $\mathfrak{M} \vDash \forall n . \mathbf{m} \mid \mathbf{m}(\mathbf{i}+1)n + n \rightarrow \mathbf{m} \mid n$.

DEMOSTRACIÓN: Gracias al lema 2.29.

⟨2⟩2. $\mathfrak{M} \vDash$ COPRIMES$[\mathbf{m}, \mathbf{m}(\mathbf{i}+1)+1]$.

DEMOSTRACIÓN: Aplicando el lema 2.30 y que $\mathfrak{M} \vDash \textsc{Coprimes}[\mathbf{m}(\mathbf{i}+1)+1, \mathbf{m}]$ gracias a que $\mathfrak{M} \vDash \mathbf{m} \neq 0$ por $\langle 1\rangle 1$, $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \neq 0$ por $\langle 1\rangle 2$ y la última conjunción es $\langle 2\rangle 1$.

$\langle 2\rangle 3$. Sea $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \mid (\mathbf{m}(\mathbf{j}+1)+1)\mathbf{n}$.

$\langle 2\rangle 4$. Existe $\mathbf{l} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{i}+\mathbf{l}+1 = \mathbf{j}$.

DEMOSTRACIÓN: Gracias a que $\mathfrak{M} \vDash \mathbf{i} < \mathbf{j}$ por $\langle 1\rangle 1$.

$\langle 2\rangle 5$. $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \mid \mathbf{m}(\mathbf{l}+1)\mathbf{n}$.

DEMOSTRACIÓN: Se tiene que
$\mathfrak{M} \vDash (\mathbf{m}(\mathbf{j}+1)+1)\mathbf{n} = (\mathbf{m}(\mathbf{i}+\mathbf{l}+1+1)+1)\mathbf{n} = (\mathbf{m}(\mathbf{i}+1)+1)\mathbf{n} + \mathbf{m}(\mathbf{l}+1)\mathbf{n}$
gracias a $\langle 2\rangle 4$ y a ser un semianillo. Ahora usando $\langle 2\rangle 3$ obtenemos que
$\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \mid (\mathbf{m}(\mathbf{i}+1)+1)\mathbf{n} + \mathbf{m}(\mathbf{l}+1)\mathbf{n}$ y por el lema 2.29 obtenemos lo pedido.

$\langle 2\rangle 6$. $\mathfrak{M} \vDash \mathbf{l}+1 \mid \mathbf{m}$.

DEMOSTRACIÓN: Por $\langle 2\rangle 4$ $\mathfrak{M} \vDash \mathbf{l} < \mathbf{k}$ y por $\langle 1\rangle 1$ $\mathbf{m}$ era divisible por todo número no nulo menor o igual que $\mathbf{k}$.

$\langle 2\rangle 7$. $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \mid \mathbf{n}$.

DEMOSTRACIÓN: Por $\langle 2\rangle 2$ y por $\langle 2\rangle 5$ se sigue que $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \mid (\mathbf{l}+1)\mathbf{n}$. Ahora de $\langle 2\rangle 6$ se tiene que $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \mid \mathbf{mn}$, y usando otra vez $\langle 2\rangle 2$ llegamos a que $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \mid \mathbf{n}$.

$\langle 2\rangle 8$. Q.E.D.

Por $\langle 1\rangle 2$ y $\langle 2\rangle 7$ tenemos que $\mathfrak{M} \vDash \textsc{Coprimes}[\mathbf{m}(\mathbf{i}+1)+1, \mathbf{m}(\mathbf{j}+1)+1]$ y usando el lema 2.30 deducimos $\langle 1\rangle 3$.

$\langle 1\rangle 4$. Q.E.D.

□

2.6. Conjuntos finitos

Nuestra definición de conjunto finito será la de conjunto acotado. Notemos que, en nuestra metateoría, en ω ser acotado y ser finito es lo mismo.

Definición 2.12 (**Conjunto finito y conjunto infinito**)**.** Definimos

- $\textsc{FinSet}[X] :\equiv \exists k \forall i. i \in X \to i < k$.
- $\textsc{InfSet}[X] :\equiv \neg \textsc{FinSet}[X]$.

■

Nota. Esta definición de conjunto finito no implica que en el modelo la interpretación de un conjunto finito sea lo que en ZFC llamamos un conjunto finito. En particular, si hay elementos no estándar $\mathbf{k}$ en el modelo $\mathfrak{M}$, i.e. si la parte de primer orden de $\mathfrak{M}$ contiene propiamente a (una copia isomorfa de) ω, el modelo estándar de la aritmética de primer orden y $\omega < \mathbf{k}$, entonces el conjunto $\{\mathbf{i} \in \mathbb{N} \mid \mathbf{i} < \mathbf{k}\}$ sería finito según la definición anterior pero no es finito (según ZFC) en la metateoría. ■

Ahora definimos una fórmula que nos dice que un conjunto finito X está codificado por k, m, n.

Definición 2.13 (**Codificación de pertenencia y conjunto finito**)**.** Definimos

$$\textsc{In}[i,k,m,n] :\equiv i < k \wedge m(i+1)+1 \mid n$$

$$\textsc{SetCodify}[X,k,m,n] :\equiv \forall i.i \in X \leftrightarrow \textsc{In}[i,k,m,n].$$

■

Nota. Si un conjunto está codificado entonces el conjunto es finito, ya que $i \in X$ implica $\textsc{In}[i,k,m,n]$ y eso implica $i < k$.

Notemos que aunque a priori estemos codificando el conjunto con tres elementos de $\mathbb{N}$ esto no es un problema, ya que una terna de elementos de $\mathbb{N}$ es codificable como un elemento de $\mathbb{N}$ (gracias a que los pares ordenados son codificables como un solo elemento). Por tanto, podemos expresar un conjunto finito con un solo número.

■

Teorema 2.33. $RCA_0 \vdash \forall X.\textsc{FinSet}[X] \to \exists k,m,n.\textsc{SetCodify}[X,k,m,n]$.

Demostración:
⟨1⟩1. Sean $\mathfrak{M}$ un modelo de RCA$_0$ y $\mathbf{X} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \textsc{FinSet}[\mathbf{X}]$.

⟨1⟩2. Existe un $\mathbf{k} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall i.i \in \mathbf{X} \to i < \mathbf{k}$.

Demostración: Por definición de FinSet y ⟨1⟩1.

⟨1⟩3. Existe un $\mathbf{m} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall i,j.i < j < \mathbf{k} \to \textsc{Coprimes}[\mathbf{m}(i+1)+1, \mathbf{m}(j+1)+1]$ y $\mathfrak{M} \vDash \mathbf{m} > 0$.

Demostración: Por lemas 2.31 y 2.32.

⟨1⟩4. Definimos $\phi[j] :\equiv j > \mathbf{k} \vee \exists n \forall i < \mathbf{k}.\mathbf{m}(i+1)+1 \mid n \leftrightarrow i \in \mathbf{X} \wedge i < j$.

⟨1⟩5. $\mathfrak{M} \vDash \forall j.\phi[j]$.

⟨2⟩1. $\mathfrak{M} \vDash \phi[0]$.

DEMOSTRACIÓN: Tomamos $n = 1$. Como ningún $\mathbf{i}$ puede ser menor que 0, tenemos que ver que $\mathfrak{M} \vDash \forall i < \mathbf{k}.\neg(\mathbf{m}(i+1)+1 \mid 1)$. Eso se tiene gracias a que $\mathfrak{M} \vDash \mathbf{m} \neq 0$, por tanto para todo $\mathbf{i} \in \mathbb{N}$ $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 > 1$ y aplicamos el lema 2.28

$\langle 2\rangle 2$. Sea $\mathbf{j} \in \mathbb{N}$ cualquiera tal que $\mathfrak{M} \vDash \phi[\mathbf{j}]$, probemos que $\mathfrak{M} \vDash \phi[\mathbf{j}+1]$.

$\langle 2\rangle 3$. Podemos suponer que $\mathfrak{M} \vDash \mathbf{j}+1 \leq \mathbf{k}$.

DEMOSTRACIÓN: Si no, se tendría que $\mathfrak{M} \vDash \mathbf{j}+1 > \mathbf{k}$ y por tanto $\mathfrak{M} \vDash \phi[\mathbf{j}+1]$ por cumplirse la primera parte de la disyunción.

$\langle 2\rangle 4$. Existe $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall i < \mathbf{k}.\mathbf{m}(i+1)+1 \mid \mathbf{n} \leftrightarrow i \in \mathbf{X} \wedge i < \mathbf{j}$.

DEMOSTRACIÓN: Gracias a la hipótesis de inducción de $\langle 2\rangle 2$ y a que $\mathfrak{M} \vDash \mathbf{j} \leq \mathbf{k}$ por $\langle 2\rangle 3$.

$\langle 2\rangle 5$. Definimos $\mathbf{n}' = \mathbf{n}(\mathbf{m}(\mathbf{j}+\mathbf{1})+\mathbf{1})$ si $\mathbf{j} \in \mathbf{X}$ y $\mathbf{n}' = \mathbf{n}$ si $\mathbf{j} \notin \mathbf{X}$.

$\langle 2\rangle 6$. $\mathfrak{M} \vDash \forall i < \mathbf{k}.\mathbf{m}(i+1)+1 \mid \mathbf{n}' \leftrightarrow (i = \mathbf{j} \wedge \mathbf{j} \in \mathbf{X}) \vee \mathbf{m}(i+1)+1 \mid \mathbf{n}$.

DEMOSTRACIÓN: Este paso se tiene distinguiendo casos sobre si $\mathfrak{M} \vDash \mathbf{j} \in \mathbf{X}$ y usando $\langle 1\rangle 3$.

$\langle 2\rangle 7$. $\mathfrak{M} \vDash \forall i < \mathbf{k}.\mathbf{m}(i+1)+1 \mid \mathbf{n}' \leftrightarrow (i \in \mathbf{X} \wedge i < \mathbf{j}+1)$.

DEMOSTRACIÓN: Usando $\langle 2\rangle 4$ en $\langle 2\rangle 6$.

$\langle 2\rangle 8$. $\mathfrak{M} \vDash \phi[\mathbf{j}+1]$.

DEMOSTRACIÓN: Juntando los pasos anteriores salvo $\langle 2\rangle 1$.

$\langle 2\rangle 9$. Q.E.D.

DEMOSTRACIÓN: Por Σ^0_1-IND en $\phi[j]$.

$\langle 1\rangle 6$. Q.E.D.

DEMOSTRACIÓN: Gracias a $\langle 1\rangle 5$ se tiene que $\mathfrak{M} \vDash \phi[\mathbf{k}]$, como queríamos.

□

Notemos entonces que con 3 números codificamos un conjunto finito. Así podemos crear una relación de equivalencia en $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ que relacione las ternas que representan el mismo conjunto.

Lema 2.34.

$$RCA_0 \vdash \exists! R.\textit{BinRel}[R, \mathbb{N} \times \mathbb{N} \times \mathbb{N}] \wedge \forall k, m, n, k', m', n'.$$

$$R((k,m,n),(k',m',n')) \leftrightarrow (\forall i.\textit{In}[i,k,m,n] \leftrightarrow \textit{In}[i,k',m',n']).$$

A la relación anterior la denotaremos en esta sección $\cong$.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0.

⟨1⟩2. Existe $\mathbf{R}$, tal que

$$\mathfrak{M} \vDash \textsc{BinRel}[\mathbf{R}, \mathbb{N} \times \mathbb{N} \times \mathbb{N}] \wedge \forall (k,m,n),(k',m',n').$$
$$R((k,m,n),(k',m',n')) \leftrightarrow (\forall i < k + k'.\textsc{In}[i,k,m,n] \leftrightarrow \textsc{In}[i,k',m',n'])$$

Demostración: Se tiene por Σ^0_0-comprensión en la fórmula:

$$\phi[x] :\equiv \exists k,m,n,k',m',n' \leq x.x = ((k,(m,n)),(k',(m',n'))) \wedge$$
$$\forall i < k + k'.\textsc{In}[i,k,m,n] \leftrightarrow \textsc{In}[i,k',m',n'].$$

⟨1⟩3. Existencia

⟨2⟩1. $\mathfrak{M} \vDash \textsc{BinRel}[\mathbf{R}, \mathbb{N} \times \mathbb{N} \times \mathbb{N}]$.

Demostración: Directamente de ⟨1⟩2

⟨2⟩2. Sean $\mathbf{k}, \mathbf{m}, \mathbf{n}, \mathbf{k}', \mathbf{m}', \mathbf{n}' \in \mathbb{N}$ arbitrarios.

⟨2⟩3. $\mathfrak{M} \vDash \mathbf{R}((\mathbf{k},\mathbf{m},\mathbf{n}),(\mathbf{k}',\mathbf{m}',\mathbf{n}')) \rightarrow (\forall i.\textsc{In}[i,\mathbf{k},\mathbf{m},\mathbf{n} \leftrightarrow \textsc{In}[i,\mathbf{k}',\mathbf{m}',\mathbf{n}'])$.

Demostración: Supongamos que $\mathfrak{M} \vDash \mathbf{R}((\mathbf{k},\mathbf{m},\mathbf{n}),(\mathbf{k}',\mathbf{m}',\mathbf{n}'))$ y que $i \in \mathbb{N}$. Si $\mathfrak{M} \vDash \mathbf{i} < \mathbf{k} + \mathbf{k}'$ se sigue de ⟨1⟩2, así que supongamos que $\mathfrak{M} \vDash \mathbf{i} \geq \mathbf{k} + \mathbf{k}'$. Eso implica que $\mathfrak{M} \vDash \mathbf{i} \geq \mathbf{k}$, por tanto $\mathfrak{M} \vDash \neg\textsc{In}[\mathbf{i},\mathbf{k},\mathbf{m},\mathbf{n}]$ y que $\mathfrak{M} \vDash \mathbf{i} \geq \mathbf{k}'$ por tanto $\mathfrak{M} \vDash \neg\textsc{In}[\mathbf{i},\mathbf{k}',\mathbf{m}',\mathbf{n}']$, como queríamos.

⟨2⟩4. $\mathfrak{M} \vDash (\forall i.\textsc{In}[i,\mathbf{k},\mathbf{m},\mathbf{n} \leftrightarrow \textsc{In}[i,\mathbf{k}',\mathbf{m}',\mathbf{n}']) \rightarrow \mathbf{R}((\mathbf{k},\mathbf{m},\mathbf{n}),(\mathbf{k}',\mathbf{m}',\mathbf{n}'))$.

Demostración: Obvia por ⟨1⟩2.

⟨2⟩5. Q.E.D.

Demostración: De ⟨2⟩1 se obtiene que es relación binario y de ⟨2⟩2 y ⟨2⟩3 que cumple la equivalencia.

⟨1⟩4. Unicidad

Demostración: Se tiene por la igualdad de conjuntos.

⟨1⟩5. Q.E.D.

□

Lema 2.35. *$RCA_0 \vdash \textsc{Equiv}[\cong, \mathbb{N} \times \mathbb{N} \times \mathbb{N}]$, denotaremos al conjunto $(\mathbb{N} \times \mathbb{N} \times \mathbb{N})/\cong$ como FinCode.*

Demostración:
Se sigue directamente del lema anterior, usando las propiedades de reflexividad, simetría y transitividad de $\leftrightarrow$.

□

Lema 2.36. $(x \in \textit{FinCode}) \in (\mathbf{\Sigma_0^0})^{RCA_0}$.

Demostración: Se ve sin problemas que

$$\mathrm{RCA}_0 \vdash (x \in \textsc{FinCode}) \leftrightarrow (\exists k, m, n \leq x . x = (k, (m, n)) \wedge$$
$$\neg\exists y < x . \exists k', m', n' . y = (k', (m', n')) \wedge \forall i < k + k' . \textsc{In}[i, k, m, n] \leftrightarrow \textsc{In}[i, k', m', n']),$$

que es Σ_0^0. □

Notación. Escribiremos

$$\textsc{SetCodify}[X, x] :\equiv \exists k, m, n \leq x . x = (k, (m, n)) \wedge \textsc{SetCodify}[X, k, m, n],$$

donde el SetCodify de la derecha del $:\equiv$ es el codifica que ya teníamos definido. ■

Corolario 2.37. *$RCA_0 \vdash \forall X . \textit{FinSet}[X] \to \exists^1 x \in \textit{FinCode} . \textit{SetCodify}[X, x]$, además a este número lo llamaremos código de X y se denotará como* $\mathrm{Cod}(X)$.

Demostración: Para la existencia basta notar que

$$\mathrm{RCA}_0 \vdash \forall X \forall x, y \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} . \textsc{SetCodify}[X, x] \wedge x \cong y \to \textsc{SetCodify}[X, y].$$

Una vez visto esto, la existencia se tiene por el lema 2.24 y por el teorema 2.33. La unicidad viene de que si existieran 2, estarían relacionados y por el lema 2.26 serían iguales.

□

Corolario 2.38. *$RCA_0 \vdash \forall x \in \textit{FinCode} \exists^1 X . \textit{FinSet}[X] \wedge \textit{SetCodify}[X, x]$. Al conjunto se le llama conjunto codificado por x y se le denotará* $\mathrm{Set}(x)$.

Demostración: Sea $\mathfrak{M}$ un modelo de RCA_0 y sea $(\mathbf{k}, (\mathbf{m}, \mathbf{n})) \in \textsc{FinCode}$. La existencia es sencilla, basta con usar Σ_0^0-COMP en la fórmula con parámetros $\mathbf{k}, \mathbf{m}, \mathbf{n}$:

$$\varphi[i] :\equiv \textsc{In}[i, \mathbf{k}, \mathbf{m}, \mathbf{n}].$$

Por construcción claramente $(\mathbf{k}, (\mathbf{m}, \mathbf{n}))$ codifica el conjunto. Además, la unicidad se tiene porque si codificase otro conjunto, por la definición de SetCodify estos serían iguales.

□

Corolario 2.39.

$$RCA_0 \vdash \forall x \in \textit{FinCode} \forall X . \textit{FinSet}[X] \to (x = \mathrm{Cod}(\mathrm{Set}(x))) \wedge (X = \mathrm{Set}(\mathrm{Cod}(X))).$$

Nota. Estos tres últimos colorarios nos establecen una biyección (en la metateoría) en cualquier modelo entre los conjuntos finitos y el conjunto de sus códigos, que además respeta la única relación primitiva en la que aparecen los conjuntos, la pertenencia. Esto nos permite dejar de distinguir entre los conjuntos finitos y sus códigos, lo que tiene dos ventajas:

1. Podemos ser ambigüos a la hora de decir si estamos usando conjuntos finitos o sus representantes. Así, usaremos la misma notación en ambos casos, por tanto a partir de ahora en lugar de $\textsc{In}[i, k, m, n]$ escribiremos $i \in (k, m, n)$.

2. Hemos bajado la complejidad sintáctica de fórmulas en la jerarquía aritmética; por ejemplo, $(x \in \text{FinCode}) \in (\mathbf{\Sigma^0_0})^{\text{RCA}_0}$, mientras que $\text{FinSet}[X] \in (\mathbf{\Sigma^0_2})^{\text{RCA}_0}$.

Gracias a lo visto en esta sección dejaremos de distinguir entre los conjuntos finitos y sus códigos y por ejemplo si $x \in \text{FinCode}$ con $x = (k, m, n)$ expresaremos $\text{In}[i, k, m, n]$ directamente como $i \in x$ (que también es Σ^0_0). ■

Finalmente veamos algunos resultados que nos permiten saber que un conjunto es finito sabiendo que otros lo son.

Lema 2.40. *$RCA_0 \vdash \forall X, Y.\text{FinSet}[X] \wedge Y \subseteq X \to \text{FinSet}[Y]$.*

Demostración: Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{X}, \mathbf{Y} \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \mathbf{X} \subseteq \mathbf{Y}$ y $\mathfrak{M} \vDash \text{FinSet}[\mathbf{X}]$. Por tanto existe $\mathbf{k} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall x \in \mathbf{X}.x < \mathbf{k}$, pero como $\mathfrak{M} \vDash \forall y \in \mathbf{Y}.y \in \mathbf{X}$ tenemos que $\mathfrak{M} \vDash \forall y \in Y.y < \mathbf{k}$, como queríamos. □

Lema 2.41. *$RCA_0 \vdash \forall X, Y.\text{FinSet}[X] \wedge \text{FinSet}[Y] \to \text{FinSet}[X \times Y]$.*

Demostración: Sea $\mathfrak{M}$ un modelo de RCA_0, y $\mathbf{k}_1, \mathbf{k}_2$ las cotas de $\mathbf{X}$ y $\mathbf{Y}$ respectivamente. Entonces una cota de $\mathbf{X} \times \mathbf{Y}$ será $(\mathbf{k}_1, \mathbf{k}_2)$. □

Lema 2.42. *$RCA_0 \vdash \forall x \in \text{FinCode} \exists^1 Y.Y = \{y \mid y \in \text{FinCode} \wedge y \subseteq x\}$.*

A este conjunto lo llamaremos $\wp(x)$.

Demostración: La demostración es sencilla usando Σ^0_0-COMP (recordemos que $x \subseteq y$ es una fórmula acotada, pues x, y son códigos de conjuntos finitos y por tanto son números, así que $x \subseteq y$ será equivalente en RCA_0 a $\forall i < x.i \in x \to i \in y$) y la igualdad de conjuntos. □

Lema 2.43. *$RCA_0 \vdash \forall x, y \in \text{FinCode}.x \subseteq y \to x \leq y$.*

Demostración:
⟨1⟩1. $\text{RCA}_0 \vdash \forall x \in \text{FinCode} \forall i.x \setminus \{i\} \leq x$.

⟨2⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{x}, \mathbf{i} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{x} \in \text{FinCode}$.

⟨2⟩2. Podemos suponer que $\mathfrak{M} \vDash \mathbf{i} \in \mathbf{x}$.

Demostración: Si $\mathfrak{M} \vDash \mathbf{i} \notin \mathbf{x}$, entonces $\mathfrak{M} \vDash \mathbf{x} \setminus \{\mathbf{i}\} = \mathbf{x}$ y por tanto se cumple lo pedido.

⟨2⟩3. Existe $\mathbf{k}, \mathbf{m}, \mathbf{n}$ tal que $\mathfrak{M} \vDash \mathbf{x} = (\mathbf{k}, \mathbf{m}, \mathbf{n}) \wedge \text{SetCodify}[\text{Set}(\mathbf{x}), \mathbf{k}, \mathbf{m}, \mathbf{n}]$.

Demostración: Por hipótesis en ⟨2⟩1.

⟨2⟩4. Existe $\mathbf{n}'$ tal que $\mathfrak{M} \vDash \mathbf{n}' \leq \mathbf{n} \wedge \text{SetCodify}[\text{Set}(\mathbf{x} \setminus \{\mathbf{i}\}), \mathbf{k}, \mathbf{m}, \mathbf{n}']$.

DEMOSTRACIÓN: Por ⟨2⟩2 $\mathfrak{M} \vDash \mathbf{m}(\mathbf{i}+1)+1 \mid \mathbf{n}$, por tanto existe $\mathbf{n}'$ tal que $\mathfrak{M} \vDash (\mathbf{m}(\mathbf{i}+1)+1)\mathbf{n}' = \mathbf{n}$. Claramente $\mathfrak{M} \vDash \mathbf{n}' \leq \mathbf{n}$, además es fácil comprobar que $\mathfrak{M} \vDash \text{SetCodify}[\text{Set}(\mathbf{x} \setminus \{\mathbf{i}\}), \mathbf{k}, \mathbf{m}, \mathbf{n}']$. Notemos que a priori sólo hemos dividido $\mathbf{n}$ entre $\mathbf{m}(\mathbf{i}+1)+1$ una vez, y podría ser divisible por ese número más veces. Pero si fuera divisible más veces por $\mathbf{m}(\mathbf{i}+1)+1$ entonces $\mathbf{n}$ no sería el número más pequeño y lo tiene que ser por la definición de codifica.

⟨2⟩5. Q.E.D.

DEMOSTRACIÓN: Por ⟨2⟩4, $\mathfrak{M} \vDash \mathbf{x} \setminus \{\mathbf{i}\} \leq (\mathbf{k}, \mathbf{m}, \mathbf{n}')$, pues ambos codifican el mismo conjunto pero $\mathbf{x} \setminus \{\mathbf{i}\}$ tiene que ser el menor que lo codifique. Además, por ⟨2⟩4 otra vez, como $\mathfrak{M} \vDash \mathbf{n}' \leq \mathbf{n}$ tenemos que $\mathfrak{M} \vDash (\mathbf{k}, \mathbf{m}, \mathbf{n}') \leq (\mathbf{k}, \mathbf{m}, \mathbf{n}) = \mathbf{x}$ y componiendo las dos desigualdades llegamos al resultado.

⟨1⟩2. Sea $\mathfrak{M}$ un modelo de RCA_0.

⟨1⟩3. Definimos $\varphi[x] :\equiv x \in \text{FinCode} \to \forall y \in \text{FinCode}.y \subseteq x \to y \leq x$.

⟨1⟩4. $\mathfrak{M} \vDash \forall x.(\forall z < x.\varphi[z]) \to \varphi[x]$.

⟨2⟩1. Sea $\mathbf{x} \in \text{FinCode}$ tal que $\mathfrak{M} \vDash \forall z < \mathbf{x}.\varphi[z]$.

⟨2⟩2. Supongamos que $\mathfrak{M} \vDash \mathbf{x} \in \text{FinCode}$ y sea $\mathbf{y}$ cualquiera tal que $\mathfrak{M} \vDash \mathbf{y} \in \text{FinCode} \wedge \mathbf{y} \subseteq \mathbf{x}$.

⟨2⟩3. Podemos suponer que $\mathfrak{M} \vDash \mathbf{y} \subset \mathbf{x}$.

DEMOSTRACIÓN: Si $\mathfrak{M} \vDash \mathbf{x} = \mathbf{y}$ entonces no habría nada que probar.

⟨2⟩4. Existe $\mathbf{i} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{y} \subseteq \mathbf{x} \setminus \{\mathbf{i}\} \wedge \mathbf{x} \neq \mathbf{x} \setminus \{\mathbf{i}\}$.

DEMOSTRACIÓN: Gracias a ⟨2⟩3 tiene que haber un $\mathbf{i} \in \mathbf{x}$ que podamos quitar.

⟨2⟩5. Q.E.D.

DEMOSTRACIÓN: Por ⟨2⟩1 tenemos que $\mathfrak{M} \vDash \mathbf{x} \setminus \{\mathbf{i}\} < \mathbf{x} \to (\mathbf{x} \setminus \{\mathbf{i}\} \in \text{FinCode} \to \forall y \in \text{FinCode}.y \subseteq \mathbf{x} \setminus \{\mathbf{i}\} \to y \leq \mathbf{x} \setminus \{\mathbf{i}\})$. La primera suposición se tiene de que por ⟨1⟩1, $\mathfrak{M} \vDash \mathbf{x} \setminus \{\mathbf{i}\} \leq \mathbf{x}$ y como por ⟨2⟩4, $\mathfrak{M} \vDash \mathbf{x} \neq \mathbf{x} \setminus \{\mathbf{i}\}$, podemos concluir que $\mathfrak{M} \vDash \mathbf{x} \setminus \{\mathbf{i}\} < \mathbf{x}$. Que $\mathfrak{M} \vDash \mathbf{x} \setminus \{\mathbf{i}\} \in \text{FinCode}$ es obvio, y poniendo $y = \mathbf{y}$, gracias a ⟨2⟩4 concluimos que $\mathfrak{M} \vDash \mathbf{y} \leq \mathbf{x} \setminus \{\mathbf{i}\} < \mathbf{x}$, como queríamos.

⟨1⟩5. Q.E.D.

DEMOSTRACIÓN: Por Π^0_1-SIND aplicado a ⟨1⟩3 gracias a que $\varphi[x] \in (\mathbf{\Pi^0_1})^{\text{RCA}_0}_{\mathfrak{M}}$

□

Corolario 2.44. *$RCA_0 \vdash \forall x \in \text{FinCode}.\text{FinSet}[\wp(x)]$*

DEMOSTRACIÓN: Usando el lema anterior. □

2.7. Sucesiones finitas

Con los conjuntos finitos definidos y codificados, podemos ahora definir y codificar las sucesiones finitas como un tipo especial de conjunto finito:

Definición 2.14 (**Sucesión finita**)**.** Definimos la fórmula:

$$\textsc{FinSeq}[f] :\equiv \exists l.f : \{0,\dots,l-1\} \longrightarrow \mathbb{N}.$$

■

Lema 2.45. *$RCA_0 \vdash \forall l \forall f : \{0,\dots,l-1\} \longrightarrow \mathbb{N}.\textit{FinSet}[f]$.*

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA$_0$, $l \in \mathbb{N}$, $f \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \mathbf{f} : \{0,\dots,\mathbf{l}-1\} \longrightarrow \mathbb{N}$.

⟨1⟩2. $\mathfrak{M} \vDash \forall i < \mathbf{l} \exists j.\mathbf{f}(i) = j$.

Demostración: Por ⟨1⟩1 al ser $\mathbf{f}$ función de dominio $\{0,\dots,\mathbf{l}-1\}$.

⟨1⟩3. Existe $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall i < \mathbf{l} \exists j < \mathbf{n}.\mathbf{f}(i) = j$.

Demostración: Por Σ^0_0-BOUND aplicado a ⟨1⟩2.

⟨1⟩4. Q.E.D.

Demostración: Sea $\mathbf{x} \in \mathbf{f}$, por ser función existen $\mathbf{i},\mathbf{j} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{x} = (\mathbf{i},\mathbf{j})$ además por el dominio de $\mathbf{f}$, $\mathfrak{M} \vDash \mathbf{i} < \mathbf{l}$. Por ⟨1⟩3, $\mathfrak{M} \vDash \mathbf{j} < \mathbf{n}$ y así $\mathfrak{M} \vDash (\mathbf{i},\mathbf{j}) < (\mathbf{l},\mathbf{n})$. Así hemos demostrado que $\mathfrak{M} \vDash \forall x \in \mathbf{f}.x < (\mathbf{l},\mathbf{n})$, como queríamos.

□

Con esto tenemos que toda sucesión finita es un conjunto finito, por tanto tiene un código y por tanto la podemos entender como un número. Como dijimos anteriormente, confundiremos el uso y la notación de la sucesión finita cuando es un conjunto y cuando es un número. Como son números, lo primero es ver que el conjunto de sucesiones finitas existe en cualquier modelo:

Lema 2.46 (**Códigos de sucesiones finitas**)**.**

$$RCA_0 \vdash \exists^1 X.X = \{s \mid s \in \textit{FinCode} \wedge \exists l.s : \{0,\dots,l-1\} \longrightarrow \mathbb{N}\}.$$

A este conjunto lo llamaremos $\mathbb{N}^{<\mathbb{N}}$, y es el conjunto de códigos de sucesiones finitas.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA$_0$.

⟨1⟩2. $(s : \{0, \ldots, l-1\} \longrightarrow \mathbb{N}) \in (\mathbf{\Sigma_0^0})^{\mathrm{RCA}_0}$.

DEMOSTRACIÓN: En RCA_0 es equivalente a
$(\forall x \leq s.x \in s \to x < l) \wedge (\forall i, j, k \leq s.(i,j) \in s \wedge (i,k) \in s \to j = k) \wedge (\forall i < l \exists j \leq s.(i,j) \in s)$.

⟨1⟩3. $(\exists l.s : \{0, \ldots, l-1\} \longrightarrow \mathbb{N}) \in (\mathbf{\Sigma_0^0})^{\mathrm{RCA}_0}$

DEMOSTRACIÓN: En RCA_0 es equivalente a
$$\exists l \leq s+1.s : \{0, \ldots, l-1\} \longrightarrow \mathbb{N}.$$
Para ver la equivalencia tan solo es necesario darse cuenta de que dado $\mathfrak{N}$ un modelo cualquiera de RCA_0, como existe $\mathbf{j} \in \mathbb{N}$ tal que $\mathfrak{N} \vDash (\mathbf{l}-1, \mathbf{j}) \in \mathbf{s}$, entonces $\mathfrak{N} \vDash \mathbf{l}-1 \leq \mathbf{s}$ y por tanto $\mathfrak{N} \vDash \mathbf{l} \leq \mathbf{s}+1$ (para ser exactos, habría que hacer casos sobre si $\mathbf{l}$ es 0 o no, ya que $\mathbf{l}-1$ como tal no existe).

⟨1⟩4. Q.E.D.

DEMOSTRACIÓN: El conjunto existe por Σ_0^0-COMP y la unicidad viene de la igualdad de conjuntos.

□

A continuación damos la primera definición importante para sucesiones finitas, la longitud de una tal sucesión.

Lema 2.47 (**Longitud**). *$RCA_0 \vdash \forall s \in \mathbb{N}^{<\mathbb{N}} \exists^1 l \forall i.i < l \leftrightarrow \exists j.(i,j) \in s$, a este número lo llamaremos longitud de s.*

DEMOSTRACIÓN:
⟨1⟩1. Sea $\mathfrak{M}$ modelo de RCA_0 y $\mathbf{s} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{s} \in \mathbb{N}^{<\mathbb{N}}$.

⟨1⟩2. $\mathfrak{M} \vDash \exists l \forall i.i < l \leftrightarrow \exists j.(i,j) \in \mathbf{s}$.

DEMOSTRACIÓN: Gracias a que la definición de $\mathbb{N}^{<\mathbb{N}}$ implica que existe $\mathbf{l}$ tal que $\mathfrak{M} \vDash \mathbf{s} \subseteq \{0, \ldots, \mathbf{l}-1\} \times \mathbb{N}$ y que $\mathfrak{M} \vDash \forall i < \mathbf{l} \exists j.(i,j) \in \mathbf{s}$.

⟨1⟩3. Unicidad

⟨2⟩1. Sean $\mathbf{l}_k \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \forall i.i < \mathbf{l}_k \leftrightarrow \exists j.(i,j) \in \mathbf{s}$ con $k \in \{1,2\}$.

⟨2⟩2. $\mathfrak{M} \vDash \mathbf{l}_1 \not< \mathbf{l}_2$.

DEMOSTRACIÓN: Supongamos que $\mathfrak{M} \vDash \mathbf{l}_1 < \mathbf{l}_2$, entonces por ⟨2⟩1 se tendría que $\mathfrak{M} \vDash \exists j.\langle \mathbf{l}_1, j \rangle \in \mathbf{s}$. Pero otra vez por ⟨2⟩1 y que $\mathfrak{M} \vDash \mathbf{l}_1 \not< \mathbf{l}_1$ se tiene que $\mathfrak{M} \vDash \neg \exists j.\langle \mathbf{l}_1, j \rangle \in \mathbf{s}$, absurdo.

⟨2⟩3. $\mathfrak{M} \vDash \mathbf{l}_2 \not< \mathbf{l}_1$.

DEMOSTRACIÓN: Análogo a ⟨2⟩2.

⟨2⟩4. Q.E.D.

Demostración: Por tricotomía y $\langle 2\rangle 2$, $\langle 2\rangle 3$.

$\langle 1\rangle 4$. Q.E.D.

□

No sólo tenemos la longitud para cada sucesión finita, además existe una función que asocia a cada sucesión su longitud.

Corolario 2.48.

$$RCA_0 \vdash \exists^1 f : \mathbb{N}^{<\mathbb{N}} \longrightarrow \mathbb{N} \forall s \in \mathbb{N}^{<\mathbb{N}} \forall l.(s,l) \in f \leftrightarrow (\forall i.i < l \leftrightarrow \exists j.(i,j) \in s).$$

A esa función la denotaremos lh.

Demostración: Basta con usar Σ^0_0-comprensión en la fórmula

$$\varphi[x] :\equiv \exists s, l \leq x.x = (s,l) \wedge s \in \mathbb{N}^{<\mathbb{N}} \wedge (\forall i < l \to \exists j \leq s.(i,j) \in s) \wedge$$
$$(\forall i \leq s.(\exists j \leq s.(i,j) \in s) \to i < l).$$

Sea $\mathfrak{M}$ un modelo de RCA$_0$ y $\mathbf{f}$ el conjunto definido por esa fórmula. Está claro que $\mathbf{f}$ cumple la propiedad, que sea una función es consecuencia del lema anterior.

□

Nota. Notemos que RCA$_0 \vdash \forall s \in \mathbb{N}^{<\mathbb{N}}.\mathrm{lh}(s) \leq s$, ya que si no habría un j tal que $(s,j) \in s$ y por tanto $s > s$, absurdo. Así $\exists x < s.x < \mathrm{lh}(s) \wedge \varphi$ es equivalente a $\exists x < \mathrm{lh}(s), \varphi$ y $\forall x < s.x < \mathrm{lh}(s) \to \varphi$ es equivalente a $\forall x < \mathrm{lh}(s).\varphi$. Por tanto trataremos $\exists x < \mathrm{lh}(s)$ y $\forall x < \mathrm{lh}(s)$ como cuantificadores acotados, aunque a priori no lo sean ya que $\mathrm{lh}(s) \notin \mathrm{TNum}$. ■

Vamos a introducir una función que dada una sucesión finita y un número menor que la longitud de dicha sucesión nos devuelva el elemento de la sucesión finita en dicha posición.

Lema 2.49.

$$RCA_0 \vdash \exists^1 f : \{(s,i) \mid s \in \mathbb{N}^{<\mathbb{N}} \wedge i < \mathrm{lh}(s)\} \longrightarrow \mathbb{N} \forall s \in \mathbb{N}^{<\mathbb{N}} \forall i < \mathrm{lh}(s).s(i) = f(s,i).$$

A está función la denotaremos como $s(i)$, es decir, es igual a la aplicación en el punto i de la función s.

Demostración: Sea $\mathfrak{M}$ un modelo de RCA$_0$. Notemos que, como $s \in \mathbb{N}^{<\mathbb{N}} \wedge i < \mathrm{lh}(s)$ es equivalente a una fórmula Σ^0_0 en RCA$_0$, efectivamente define un conjunto y, por tanto, puede ser el dominio de la función. Para definir la función basta con usar Σ^0_0-COMP en la fórmula:

$$\varphi[x] :\equiv \exists s, i, j.x = ((s,i),j) \wedge s \in \mathbb{N}^{<\mathbb{N}} \wedge i < \mathrm{lh}(s) \wedge (i,j) \in s.$$

□

Veamos para qué queremos esa función. Supongamos que tenemos un modelo de RCA_0 $\mathfrak{M}$ y sea la fórmula $f(i) < j$. Cuando fijamos el significado de f e i, es decir, cuando ponemos $\mathbf{f}(\mathbf{i}) < j$, sabemos que esta fórmula es Σ^0_0, pues es un símbolo de relación binario ($<$) aplicado a una constante ($\mathbf{f}(\mathbf{i})$ es una constante al estar fijado el significado de la función y del punto donde se aplica). Sin embargo, supongamos que queremos ver de manera rápida que $\mathbf{f}(i) < j$ es equivalente a una fórmula Σ^0_0, como expusimos en la nota del final de la sección de funciones. Esto se puede ver notando que la fórmula es equivalente a la fórmula $((i,j),1) \in < \circ(\mathbf{f} \times \mathrm{id})$. La clave para usar esto es que lo que hay a la derecha del $\in$ es un elemento del universo de conjuntos (una constante), puesto que el significado de $\mathbf{f}$ está fijado y el de id también (en cualquier modelo sólo hay un conjunto que sea la función identidad) entonces el de $\mathbf{f} \times \mathrm{id}$ lo estará y por tanto el de la composición con $<$ también (pues en cada modelo sólo hay un conjunto que sea el "grafo"de $<$). El problema surge cuando consideramos la fórmula $f(i) < j$. A esta fórmula ya no se le puede aplicar lo de antes, pues como f no está fijado, no tenemos una constante que represente $< \circ(\mathbf{f} \times \mathrm{id})$. Notemos que, estrictamente hablando, esa fórmula sería $\exists k.(i,k) \in f \wedge k < j$ o equivalentemente $\forall k.(i,k) \in f \to k < j$. Por tanto, a priori parece que lo mejor que podemos aspirar es a que sea Δ^0_1. Sin embargo, supongamos que f fuera una sucesión finita. Entonces, gracias al lema anterior, esa fórmula volvería a ser Σ^0_0 ya que será equivalente a la fórmula $(((f,i),j),1) \in < \circ(\mathbf{g} \times \mathrm{id})$, donde $\mathbf{g}$ es la función definida por el lema anterior, es decir la que recibe una sucesión finita y un número menor que la longitud de dicha sucesión y devuelve el elemento en dicha posición. Para eso sirve dicha función, y nos será útil, por ejemplo, si quisiésemos expresar que $\forall f \in \mathbb{N}^{<\mathbb{N}}.f(i) < j$, ya que al cuantificar sucesiones finitas estamos cuantificando sobre una variable numérica.

Introducimos una notación muy común para las sucesiones finitas:

Notación. Será habitual usar

$$\langle s(0), \ldots, s(\mathrm{lh}(s) - 1)\rangle$$

o

$$\langle s(i) \mid i < \mathrm{lh}(s)\rangle$$

para denotar variables númericas que vayan a usarse para representar sucesiones finitas. Por tanto, si tenemos $\langle p_i \mid i < l\rangle$, entonces intuitivamente esa variable se va a usar para representar una sucesión finita de longitud l, aunque hay que expresarlo en la fórmula. En tal caso s_i sería una notación para expresar $\langle p_i \mid i < l\rangle(i)$, definido en el lema anterior. ■

Lema 2.50 (**Concatenación**).

$$RCA_0 \vdash \exists^1 f : \mathbb{N}^{<\mathbb{N}} \times \mathbb{N}^{<\mathbb{N}} \longrightarrow \mathbb{N}^{<\mathbb{N}} \forall s_1, s_2, t \in \mathbb{N}^{<\mathbb{N}}.f(s_1,s_2) = t \leftrightarrow$$
$$(\mathrm{lh}(s_1) + \mathrm{lh}(s_2) = \mathrm{lh}(t) \wedge (\forall i < \mathrm{lh}(t_1).s_1(i) = t(i)) \wedge$$
$$(\forall i < \mathrm{lh}(t_2).s_2(i) = t(\mathrm{lh}(t_1) + i))).$$

Será habitual denotar $f(s_1,s_2)$ *como* $s_1{}^\frown s_2$.

Demostración: Por Σ^0_0-COMP en la fórmula

$$\varphi[x] :\equiv \exists s_1, s_2, t.x = ((s_1, s_2), t) \wedge s_1 \in \mathbb{N}^{<\mathbb{N}} \wedge s_2 \in \mathbb{N}^{<\mathbb{N}} \wedge t \in \mathbb{N}^{<\mathbb{N}} \wedge$$
$$(\mathrm{lh}(s_1) + \mathrm{lh}(s_2) = \mathrm{lh}(t)) \wedge (\forall i < \mathrm{lh}(t_1) \exists x \leq s_1.s_1(i) = x \wedge t(i) = x) \wedge$$
$$(\forall i < \mathrm{lh}(t_2) \exists x \leq s_2.s_2(i) = x \wedge t(\mathrm{lh}(t_1) + i) = x).$$

□

Definición 2.15 (**Segmento inicial**)**.** Dadas dos sucesiones finitas s, t si $s \subseteq t$ diremos que s es un segmento inicial de t. Notemos que

$$\mathrm{RCA}_0 \vdash \forall s, t \in \mathbb{N}^{<\mathbb{N}}.s \subseteq t \leftrightarrow (\mathrm{lh}(s) \leq \mathrm{lh}(t) \wedge \forall i < \mathrm{lh}(s).s(i) = t(i))$$

y que como s es un conjunto finito, $(s \subseteq t) \in (\mathbf{\Sigma^0_0})^{\mathrm{RCA}_0}$. ■

Nota. Notemos que si s, t son sucesiones finitas, $\forall s \subseteq t.\varphi$ es equivalente en RCA_0 a $\forall s \leq t.s \subseteq t \to \varphi$ y por tanto el cuantificador cuenta como acotado. ■

Lema 2.51.

$$RCA_0 \vdash \forall X \exists^1 Y.Y = \{s \mid s \in \mathbb{N}^{<\mathbb{N}} \wedge \forall i < \mathrm{lh}(s).s(i) \in X\}$$

y

$$RCA_0 \vdash \forall k \forall X \exists^1 Y.Y = \{s \mid s \in \mathbb{N}^{<\mathbb{N}} \wedge \mathrm{lh}(s) = k \wedge \forall i < k.s(i) \in X\}.$$

Al primer conjunto lo notaremos como $X^{<\mathbb{N}}$ y al segundo X^k.

Demostración: Se tiene por Σ^0_0-COMP.

□

Notemos que, por ser la fórmula que define a los conjuntos equivalente en RCA_0 a un fórmula Σ^0_0, tenemos que $x \in X^{<\mathbb{N}}$ y $x \in X^k$ serán equivalentes en RCA_0 a una fórmula Σ^0_0.

Nota. Esto nos permite hablar de funciones de $\mathbb{N}^k$ en $\mathbb{N}$, y también hablar de una sucesión finita $\langle f_1, \ldots, f_m \rangle$ de funciones $\mathbb{N}^k \longrightarrow \mathbb{N}$ identificándola con la función correspondiente en $\mathbb{N}^k \longrightarrow \mathbb{N}^m$. Así mediante el teorema 2.10 se demuestra que si $g : \mathbb{N}^m \longrightarrow \mathbb{N}$ y $f_i : \mathbb{N}^k \longrightarrow \mathbb{N}$ para $1 \leq i \leq m$, entonces tenemos $h : \mathbb{N}^k \longrightarrow \mathbb{N}$ definida como $h(\langle n_1, \ldots, n_k \rangle) = g(\langle f_1(\langle n_1, \ldots, n_k \rangle), \ldots, f_m(\langle n_1, \ldots, n_k \rangle) \rangle)$ (si $f : \mathbb{N}^k \longrightarrow \mathbb{N}^m$ es la función que codifica los f_i, entonces $h = g \circ f$). ■

Notación. Será habitual cuando tengamos funciones $f : \mathbb{N}^k \longrightarrow X$ denotar $f(\langle x_1, \ldots, x_k \rangle)$ directamente como $f(x_1, \ldots, x_k)$ como es habitual.

■

Lema 2.52. $RCA_0 \vdash \forall X \forall k. \textit{FinSet}[X] \to \textit{FinSet}[X^k]$.

Demostración: Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{X} \in \wp(\mathbb{N}), \mathbf{k} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \textsc{FinSet}[\mathbf{X}]$. Notemos que $\mathfrak{M} \vDash \mathbf{X^k} = \{s \mid s \in \textsc{FinCode} \wedge s : \{0, \dots \mathbf{k}-1\} \longrightarrow \mathbf{X}\} \subseteq \wp(\{0, \dots, \mathbf{k}-\mathbf{1}\} \times \mathbf{X})$. Notemos que $\{0, \dots, \mathbf{k}-\mathbf{1}\} \times \mathbf{X}$ es finito por lema 2.41 (pues $\mathbf{X}$ es finito por hipótesis y $\{0, \dots, \mathbf{k}-\mathbf{1}\}$ es claramente finito), por tanto $\wp(\{0, \dots, \mathbf{k}-\mathbf{1}\} \times \mathbf{X})$ será finito por lema 2.44. Concluimos que $\mathbf{X^k}$ es finito gracias al lema 2.40. □

2.8. Recursión primitiva

Ya vimos antes cómo definir el concepto de función y que, sobre RCA_0, las funciones son cerradas bajo la composición. Trataremos ahora los otros dos métodos básicos para definir funciones de forma recursiva, la recursión primitiva y la minimización.

Teorema 2.53 (Recursión primitiva).

$$RCA_0 \vdash \forall k \in \mathbb{N} \forall f : \mathbb{N}^k \longrightarrow \mathbb{N} \forall g : \mathbb{N}^{k+2} \longrightarrow \mathbb{N} \exists^1 h : \mathbb{N}^{k+1} \longrightarrow \mathbb{N}.$$

$$(\forall \langle n_1, \dots, n_k \rangle \in \mathbb{N}^k . h(0, n_1, \dots, n_k) = f(n_1, \dots, n_k)) \wedge$$
$$(\forall m \in \mathbb{N} \forall \langle n_1, \dots, n_k \rangle \in \mathbb{N}^k . h(m+1, n_1, \dots, n_k) = g(h(m, n_1, \dots, n_k), m, n_1, \dots, n_k)).$$

Demostración:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0, $\mathbf{k} \in \mathbb{N}$ y $\mathbf{f}, \mathbf{g} \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \mathbf{f} : \mathbb{N}^{\mathbf{k}} \longrightarrow \mathbb{N}$ y $\mathfrak{M} \vDash \mathbf{g} : \mathbb{N}^{\mathbf{k}+2} \longrightarrow \mathbb{N}$

⟨1⟩2. Definimos

$$\theta[s, m, \langle n_1, \dots, n_{\mathbf{k}} \rangle] :\equiv$$
$$s \in \mathbb{N}^{m+1} \wedge s(0) = \mathbf{f}(n_1, \dots, n_{\mathbf{k}}) \wedge \forall i < m . s(i+1) = \mathbf{g}(s(i), i, n_1, \dots, n_{\mathbf{k}}).$$

⟨1⟩3. $\mathfrak{M} \vDash \forall \langle n_1, \dots, n_{\mathbf{k}} \rangle \in \mathbb{N}^{\mathbf{k}} \forall m \exists^1 s . \theta[s, m, \langle n_1, \dots, n_{\mathbf{k}} \rangle]$

⟨2⟩1. Sea $\langle \mathbf{n}_1, \dots, \mathbf{n}_{\mathbf{k}} \rangle \in \mathbb{N}^{\mathbf{k}}$.

⟨2⟩2. $\mathfrak{M} \vDash \forall m \exists s . \theta[s, m, \langle \mathbf{n}_1, \dots, \mathbf{n}_{\mathbf{k}} \rangle]$

Demostración: Mediante Σ^0_1-IND sale directamente.

⟨2⟩3. Si $\mathbf{m}, \mathbf{s}, \mathbf{s}' \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \theta[\mathbf{s}, \mathbf{m}, \langle \mathbf{n}_1, \dots, \mathbf{n}_{\mathbf{k}} \rangle]$ y $\mathfrak{M} \vDash \theta[\mathbf{s}', \mathbf{m}, \langle \mathbf{n}_1, \dots, \mathbf{n}_{\mathbf{k}} \rangle]$ entonces $\mathfrak{M} \vDash \mathbf{s} = \mathbf{s}'$.

Demostración: Se demuestra fácilmente que $\mathfrak{M} \vDash \forall i \leq \mathbf{m} . \mathbf{s}(i) = \mathbf{s}'(i)$ usando Σ^0_1-IND (en i). La igualdad sale entonces del teorema 2.9, ya que las sucesiones finitas son funciones.

⟨2⟩4. Q.E.D.

Demostración: La existencia se tiene por ⟨2⟩2 y la unicidad por ⟨2⟩3.

$\langle 1\rangle 4$. Existencia

DEMOSTRACIÓN: La existencia viene de que gracias a la existencia y unicidad que demuestra $\langle 1\rangle 3$ se tiene que para cualesquiera $\langle \mathbf{n_1}, \ldots, \mathbf{n_k}\rangle \in \mathbb{N}^{\mathbf{k}}, \mathbf{m}, \mathbf{j} \in \mathbb{N}$,

$\mathfrak{M} \vDash (\exists s.\theta[s, \mathbf{m}, \langle \mathbf{n_1}, \ldots, \mathbf{n_k}\rangle] \wedge s(\mathbf{m}) = \mathbf{j}) \leftrightarrow (\forall s.\theta[s, \mathbf{m}, \langle \mathbf{n_1}, \ldots, \mathbf{n_k}\rangle] \wedge s(\mathbf{m}) = \mathbf{j})$.

Y de la Δ_1^0-comprensión se sigue la existencia de un $\mathbf{h} \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \mathbf{h} = \{(\langle m, n_1, \ldots, n_{\mathbf{k}}\rangle, j) \mid \exists s.\theta[s, m, \langle n_1, \ldots, n_{\mathbf{k}}\rangle]) \wedge s(m) = j\}.$$

De $\langle 1\rangle 3$ se sigue que $\mathbf{h} : \mathbb{N}^{\mathbf{k}+1} \longrightarrow \mathbb{N}$ y cumple lo pedido.

$\langle 1\rangle 5$. Unicidad

DEMOSTRACIÓN: Bastaría usar el teorema 2.9. Sean entonces $\mathbf{h}_1, \mathbf{h}_2 : \mathbb{N}^{\mathbf{k}+1} \longrightarrow \mathbb{N}$ que cumplan lo pedido. Claramente tienen el mismo dominio por hipótesis, faltaría ver que $\mathfrak{M} \vDash \forall s \in \mathbb{N}^{\mathbf{k}+1}.\mathbf{h}_1(s) = \mathbf{h}_2(s)$. Notemos que eso es equivalente a que dado $\langle \mathbf{n_1}, \ldots, \mathbf{n_k}\rangle \in \mathbb{N}^{\mathbf{k}}$ arbitrario tengamos que $\mathfrak{M} \vDash \forall i.\mathbf{h}_1(i, \mathbf{n_1}, \ldots, \mathbf{n_k}) = \mathbf{h}_2(i, \mathbf{n_1}, \ldots, \mathbf{n_k})$, lo cual se demuestra por $\Sigma_0^0 - \text{IND}$.

$\langle 1\rangle 6$. Q.E.D.
DEMOSTRACIÓN: Por $\langle 1\rangle 4$ y $\langle 1\rangle 5$. □

Teorema 2.54 (**Minimización**).

$$RCA_0 \vdash \forall k \forall f : \mathbb{N}^{k+1} \longrightarrow \mathbb{N}.(\forall \langle n_1, \ldots, n_k\rangle \in \mathbb{N}^k \exists m \in \mathbb{N}.f(m, n_1, \ldots, n_k) = 1) \rightarrow$$

$$\exists^1 g : \mathbb{N}^k \longrightarrow \mathbb{N} \forall \langle n_1, \ldots, n_k\rangle.f(g(n_1, \ldots, n_k), n_1, \ldots, n_k) = 1 \wedge$$

$$\neg \exists m < g(n_1, \ldots, n_k).f(m, n_1, \ldots, n_k) = 1.$$

Esta función será denotada como $\mu m.f(m, n_1, \ldots, n_k)$.

DEMOSTRACIÓN:
$\langle 1\rangle 1$. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{k} \in \mathbb{N}, \mathbf{f} : \mathbb{N}^{\mathbf{k}+1} \longrightarrow \mathbb{N}$ donde

$$\mathfrak{M} \vDash \forall \langle n_1, \ldots, n_{\mathbf{k}}\rangle \in \mathbb{N}^{\mathbf{k}} \exists m \in \mathbb{N}.\mathbf{f}(m, n_1, \ldots, n_{\mathbf{k}}) = 1.$$

$\langle 1\rangle 2$. Existe $\mathbf{g} \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \mathbf{g} = \{(\langle n_1, \ldots, n_{\mathbf{k}}\rangle, m) \mid \langle n_1, \ldots, n_{\mathbf{k}}\rangle \in \mathbb{N}^{\mathbf{k}} \wedge (\langle m, n_1, \ldots, n_{\mathbf{k}}\rangle, 1) \in \mathbf{f} \wedge \neg \exists j < m.(\langle j, n_1, \ldots, n_{\mathbf{k}}\rangle, 1) \in \mathbf{f}\}.$$

DEMOSTRACIÓN: La existencia se tiene aplicando Σ_0^0-comprensión.

$\langle 1\rangle 3$. $\mathfrak{M} \vDash \mathbf{g} : \mathbb{N}^{\mathbf{k}} \longrightarrow \mathbb{N}$.

DEMOSTRACIÓN: Por $\langle 1\rangle 2$ claramente $\mathfrak{M} \vDash \mathbf{g} \subseteq \mathbb{N}^{\mathbf{k}} \times \mathbb{N}$. Que $\mathfrak{M} \vDash \forall \langle n_1, \ldots, n_{\mathbf{k}}\rangle \in \mathbb{N}^{\mathbf{k}} \exists m.\mathbf{g}(n_1, \ldots, n_{\mathbf{k}}) = m$ se tiene gracias a que dado $\langle \mathbf{n_1}, \ldots, \mathbf{n_k}\rangle \in \mathbb{N}^{\mathbf{k}}$ podemos usar la hipótesis $\langle 1\rangle 1$ y $\Sigma_0^0 - \text{MIN}$ en la fórmula

$$\mathbf{f}(m, \mathbf{n_1}, \ldots, \mathbf{n_k}) = 1 \wedge \neg \exists j < m.\mathbf{f}(j, \mathbf{n_1}, \ldots, \mathbf{n_k}) = 1.$$

Que $\mathfrak{M} \vDash \forall \langle n_1, \ldots, n_{\mathbf{k}} \rangle \forall m, m'.(\langle n_1, \ldots, n_{\mathbf{k}} \rangle, m) \in \mathbf{g} \wedge (\langle n_1, \ldots, n_{\mathbf{k}} \rangle, m') \in \mathbf{g} \to m = m'$, se sigue también de la Σ_0^0-MIN ya que nos da la unicidad aparte de la existencia.

⟨1⟩4. Sea $\langle \mathbf{n}_1, \ldots, \mathbf{n}_{\mathbf{k}} \rangle$ cualquiera. Entonces
$\mathfrak{M} \vDash \mathbf{f}(\mathbf{g}(\mathbf{n}_1, \ldots, \mathbf{n}_{\mathbf{k}}), \mathbf{n}_1, \ldots, \mathbf{n}_{\mathbf{k}}) = 1 \wedge \neg \exists m < \mathbf{g}(\mathbf{n}_1, \ldots, \mathbf{n}_{\mathbf{k}}).\mathbf{f}(m, \mathbf{n}_1, \ldots, \mathbf{n}_{\mathbf{k}}) = 1.$

Demostración: Se sigue de ⟨1⟩2.

⟨1⟩5. Unicidad

Demostración: Se sigue fácilmente de la igualdad de funciones y de la unicidad cuando existe un elemento mínimo.

⟨1⟩6. Q.E.D.

□

Nota. Será muy habitual usar $\mu m.\varphi[m]$, donde φ es una fórmula. La idea es que φ siempre será una fórmula de la cual se puede construir el conjunto de elementos que la cumplen, y por tanto también su función característica. Entonces estamos aplicando minimización a la función característica. ■

2.9. Aplicaciones de la recursión primitiva

El primer lema que es consecuencia de la recusión primitiva nos dice que en un modelo de RCA_0 todos los conjuntos infinitos tienen una enumeración en el modelo (es decir, con los números del modelo, no con los números naturales de ω) y además (gracias a la infinitud) será creciente (y por tanto inyectiva). En la demostración se aprecia cómo se usa la recursión.

Lema 2.55.

$$RCA_0 \vdash \forall X.\textsc{InfSet}[X] \to \exists^1 f : \mathbb{N} \longrightarrow \mathbb{N}.$$

$$(\forall k, m.k < m \to f(k) < f(m)) \wedge (\forall n.n \in X \leftrightarrow \exists m.f(m) = n).$$

A esta función la denotaremos π_X.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{X}$ tal que $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{X}]$.

⟨1⟩2. Existe $\nu_X : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\nu_X(m) = \mu n.n \in X \wedge n \geq m$.

Demostración: Gracias a la minimización y que por ⟨1⟩1 $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{X}]$, es decir $\mathfrak{M} \vDash \forall m \exists n.n \geq m \wedge n \in X$.

⟨1⟩3. Existencia

⟨2⟩1. Existe $\pi_{\mathbf{X}} : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\pi_{\mathbf{X}}(0) = \nu_X(0)$ y $\pi_{\mathbf{X}}(m+1) = \nu_X(\pi_{\mathbf{X}}(m) + 1)$.

Demostración: Usando recursión primitiva.

⟨2⟩2. $\mathfrak{M} \vDash \forall k, m.k < m \to \pi_{\mathbf{X}}(k) < \pi_{\mathbf{X}}(m)$.

DEMOSTRACIÓN: Se prueba por Σ^0_0-inducción que $\mathfrak{M} \vDash \forall m.\pi_{\mathbf{X}}(m) < \pi_{\mathbf{X}}(m+1)$. Sea $\mathbf{k} \in \mathbb{N}$ arbitrario. Claramente $\mathfrak{M} \vdash \mathbf{k} < 0 \to \pi_{\mathbf{X}}(\mathbf{k}) < \pi_{\mathbf{X}}(0)$. Supongamos ahora que $\mathbf{m} \in \mathbb{N}$ arbitrario y $\mathfrak{M} \vDash \mathbf{k} < \mathbf{m} \to \pi_{\mathbf{X}}(\mathbf{k}) < \pi_{\mathbf{X}}(\mathbf{m})$. Si $\mathfrak{M} \vDash \mathbf{k} < \mathbf{m}$ o $\mathfrak{M} \vDash \mathbf{k} > \mathbf{m}$ tenemos trivialmente que $\mathfrak{M} \vDash \mathbf{k} < \mathbf{m}+\mathbf{1} \to \pi_{\mathbf{X}}(\mathbf{k}) < \pi_{\mathbf{X}}(\mathbf{m})$ y para el caso $\mathfrak{M} \vDash \mathbf{k} = \mathbf{m}$ se cumple porque tenemos que $\mathfrak{M} \vDash \pi_{\mathbf{X}}(\mathbf{m}) < \pi_{\mathbf{X}}(\mathbf{m}+1)$. Por tanto usando Σ^0_0-inducción obtenemos que $\mathfrak{M} \vDash \forall m.\mathbf{k} < m \to \pi_{\mathbf{X}}(\mathbf{k}) < \pi_{\mathbf{X}}(m)$ y como $\mathbf{k}$ era arbitrario, tenemos que $\mathfrak{M} \vDash \forall k, m.k < m \to \pi_{\mathbf{X}}(k) < \pi_{\mathbf{X}}(m)$

⟨2⟩3. $\mathfrak{M} \vDash \forall n.n \in X \leftrightarrow \exists m \leq n.\pi_{\mathbf{X}}(m) = n$.

DEMOSTRACIÓN: Por Σ^0_0-inducción.

⟨2⟩4. Q.E.D.

DEMOSTRACIÓN: Que sea una existencia de la función y creciente se tiene por ⟨2⟩1 y ⟨2⟩2. La última parte de la conjunción se tiene por ⟨2⟩3.

⟨1⟩4. Unicidad

⟨2⟩1. Sean $\mathbf{f}, \mathbf{g} \in \wp(\mathbb{N})$ que cumplen la propiedad.

⟨2⟩2. $\mathfrak{M} \vDash \mathbf{f}(0) = \mathbf{g}(0)$.

DEMOSTRACIÓN: Si $\mathfrak{M} \vDash \mathbf{f}(0) < \mathbf{g}(0)$, como $\mathfrak{M} \vDash \mathbf{f}(0) \in \mathbf{X}$, existe $\mathbf{m} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{g}(\mathbf{m}) = \mathbf{f}(0)$. $\mathfrak{M} \vDash m \neq 0$, pues si no $\mathfrak{M} \vDash \mathbf{f}(0) = \mathbf{f}(\mathbf{m}) = \mathbf{g}(0)$, pero entonces $\mathfrak{M} \vDash 0 < \mathbf{m}$ y así $\mathfrak{M} \vDash \mathbf{g}(\mathbf{m}) = \mathbf{f}(0) < \mathbf{g}(0)$ y $\mathbf{g}$ no sería creciente. Si $\mathbf{M} \vDash \mathbf{g}(0) < \mathbf{f}(0)$, entonces es análogo así que por tricotomía nos queda que son iguales.

⟨2⟩3. Sea $\mathbf{n} \in \mathbb{N}$ cualquiera, entonces $\mathfrak{M} \vDash \mathbf{f}(\mathbf{n}) = \mathbf{g}(\mathbf{n}) \to \mathbf{f}(\mathbf{n}+\mathbf{1}) = \mathbf{g}(\mathbf{n}+\mathbf{1})$.

DEMOSTRACIÓN: Supongamos que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{n}) = \mathbf{g}(\mathbf{n})$. Supongamos que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{n}+1) < \mathbf{g}(\mathbf{n}+1)$ (si $\mathfrak{M} \vDash \mathbf{f}(\mathbf{n}+1) > \mathbf{g}(\mathbf{n}+1)$ es análogo). Como $\mathfrak{M} \vDash \mathbf{f}(\mathbf{n}+1) \in \mathbf{X}$, tenemos que existe $\mathbf{m} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{g}(\mathbf{m}) = \mathbf{f}(\mathbf{n}+1)$. Por un lado $\mathfrak{M} \vDash \mathbf{g}(\mathbf{n}) = \mathbf{f}(\mathbf{n}) < \mathbf{f}(\mathbf{n}+1) = \mathbf{g}(\mathbf{m})$, y por otro $\mathfrak{M} \vDash \mathbf{g}(\mathbf{m}) = \mathbf{f}(\mathbf{n}+1) < \mathbf{g}(\mathbf{n}+\mathbf{1})$, es decir $\mathfrak{M} \vDash \mathbf{g}(\mathbf{n}) < \mathbf{g}(\mathbf{m}) < \mathbf{g}(\mathbf{n}+1)$, lo cual no es posible, pues $\mathbf{g}$ creciente. Por tricotomía nos queda que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{n}+1) = \mathbf{g}(\mathbf{n}+1)$.

⟨2⟩4. Q.E.D.

Por igualdad de funciones, por hipótesis el dominio es el mismo, por lo que basta probar que $\forall n.\mathbf{f}(n) = \mathbf{g}(n)$. Pero eso se obtiene por Σ^0_0-induccón en la fórmula $((n,n),1) \in= \circ(\mathbf{f} \times \mathbf{g})$, cuyo caso base es ⟨2⟩2 y el paso inductivo es ⟨2⟩3.

⟨1⟩5. Q.E.D.

□

Un corolario es que todo conjunto finito tiene una sucesión finita con todos sus elementos, que además están ordenados según $<$.

Corolario 2.56.

$$RCA_0 \vdash \forall X \in \textit{FinSet} \exists^1 s \in \mathbb{N}^{<\mathbb{N}}.$$
$$(\forall i, j < \mathrm{lh}(s).i < j \to s(i) < s(j)) \wedge (\forall x.x \in X \leftrightarrow \exists i < \mathrm{lh}(s).s(i) = x).$$

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{X} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \textsc{FinSet}[\mathbf{X}]$.

⟨1⟩2. Existe $\mathbf{l}$ tal que $\mathfrak{M} \vDash \forall x.x \in \mathbf{X} \to x < \mathbf{l}$.

Demostración: Por ⟨1⟩1.

⟨1⟩3. Existe $\pi_{\mathbf{X} \cup \{\mathbf{l}, \mathbf{l}+1, \ldots\}}$.

Demostración: Por el lema 2.55.

⟨1⟩4. Existe $\mathbf{m}$ tal que $\mathfrak{M} \vDash \pi_{\mathbf{X} \cup \{\mathbf{l}, \mathbf{l}+1, \ldots\}}(\mathbf{m}) = \mathbf{l}$.

Demostración: Ya que $\mathfrak{M} \vDash \mathbf{l} \in \mathbf{X} \cup \{\mathbf{l}, \mathbf{l}+1, \ldots\}$.

⟨1⟩5. Existencia

Demostración: Basta con tomar la sucesión finita $\pi_{\mathbf{X} \cup \{\mathbf{l}, \mathbf{l}+1, \ldots,\}}[\mathbf{m}]$.

⟨1⟩6. Unicidad

Demostración: Si existiesen dos sucesiones finitas distintas cumpliendo los requerimientos del corolario, se podrían extender a sucesiones infinitas crecientes que enumerasen $\mathbf{X} \cup \{\mathbf{l}, \mathbf{l}+1, \ldots\}$ distintas, lo cual es imposible por el lema 2.55.

⟨1⟩7. Q.E.D.

□

Otro uso de la recursión es, dada una función, poder definir la sucesión finita de sus primeros n elementos.

Lema 2.57.

$$RCA_0 \vdash \forall f : \mathbb{N} \longrightarrow \mathbb{N} \exists^1 h : \mathbb{N} \longrightarrow \mathbb{N}^{<\mathbb{N}} \forall n.h(n) \in \mathbb{N}^n \wedge \forall i < n.f(i) = (h(n))(i).$$

A una tal función le llamamos $f[\_]$.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{f} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{f} : \mathbb{N} \longrightarrow \mathbb{N}$.

⟨1⟩2. Existencia

Demostración: Gracias a la recursión, existe una función $\mathbf{h} : \mathbb{N} \longrightarrow \mathbb{N}$ tal que
$$\mathbf{h}(0) = \langle\rangle.$$

$$\mathbf{h}(n+1) = \mathbf{h}(n)^\frown\langle \mathbf{f}(n)\rangle.$$

Por Σ^0_0-inducción se demuestran las propiedades.

⟨1⟩3. Unicidad

DEMOSTRACIÓN: Por igualdad de funciones.

⟨1⟩4. Q.E.D.

□

El siguiente lema nos permite ver que, para toda fórmula Σ^0_1, la clase que define es o bien un conjunto finito o bien la imagen de una función inyectiva (en RCA$_0$ no es cierto que la imagen de un conjunto bajo una función sea necesariamente un conjunto).

Lema 2.58. *Sea $\varphi\{n\} \in \Sigma^0_1$ tal que $X, f \notin \mathrm{Vl}(\varphi\{n\})$. Entonces*

$$RCA_0 \vdash (\exists X \in \textit{FinSet}\forall n.n \in X \leftrightarrow \varphi\{n\}) \vee (\exists f : \mathbb{N} \longrightarrow \mathbb{N}.\textit{Iny}[f] \wedge \forall n.\varphi\{n\} \leftrightarrow \exists m.f(m) = n)$$

DEMOSTRACIÓN:

⟨1⟩1. Supongamos que $\mathfrak{M}$ es un modelo de RCA$_0$ y $\{\nu_1, \ldots, \nu_k\} = \mathrm{Vl}(\varphi\{n\}) \setminus \{n\}$.

⟨1⟩2. Denotamos $\psi :\equiv (\exists X \in \textsc{FinSet}\forall n.n \in X \leftrightarrow \varphi\{n\}) \vee (\exists f : \mathbb{N} \longrightarrow \mathbb{N}.\textsc{Iny}[f] \wedge \forall n.\varphi\{n\} \leftrightarrow \exists m.f(m) = n)$.

⟨1⟩3. $\mathrm{Vl}(\psi) = \{\nu_1, \ldots, \nu_k\}$.

DEMOSTRACIÓN: Por la definición de variable libre y ⟨1⟩1.

⟨1⟩4. Sean $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k$ y denotamos $\varphi[n] :\equiv \varphi(n, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k)$. Entonces
$$\boldsymbol{\psi} :\equiv \psi[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k] \equiv$$
$(\exists X \in \textsc{FinSet}\forall n.n \in X \leftrightarrow \varphi[n]) \vee (\exists f : \mathbb{N} \longrightarrow \mathbb{N}.\textsc{Iny}[f] \wedge \forall n.\varphi[n] \leftrightarrow \exists m.f(m) = n)$
es suficiente probar que $\mathfrak{M} \vDash \boldsymbol{\psi}$.

DEMOSTRACIÓN: La igualdad es por la definición de sustitución y que sea suficiente es por completitud.

⟨1⟩5. Podemos suponer que $\mathfrak{M} \vDash \neg(\exists X \in \textsc{FinSet}\forall n.n \in X \leftrightarrow \varphi[n])$.

DEMOSTRACIÓN: En caso contrario habríamos terminado.

⟨1⟩6. $\varphi[n] \equiv \exists j\theta(j, n)$ donde $\theta(j, n)$ es $(\Sigma^0_0)_{\mathfrak{M}}$.

DEMOSTRACIÓN: Pues $\varphi\{n\} \in \Sigma^0_0$.

⟨1⟩7. Existe $\mathbf{Y}$ tal que $\mathfrak{M} \vDash \mathbf{Y} = \{(j, n) \mid \theta(j, n) \wedge \neg\exists i < j.\theta(i, n)\}$.

DEMOSTRACIÓN: La existencia se tiene por Σ^0_0-COMP.

⟨1⟩8. $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{Y}]$.

DEMOSTRACIÓN: Supongamos que $\mathfrak{M} \vDash \text{FINSET}[\mathbf{Y}]$, sea $\mathbf{l}$ tal que $\mathfrak{M} \vDash \forall x.x \in \mathbf{Y} \to x < \mathbf{l}$. Entonces existe $\mathbf{X}$ tal que $\mathfrak{M} \vDash \forall n.n \in \mathbf{X} \leftrightarrow \exists j < \mathbf{l}.(j,n) \in \mathbf{Y}$ por Σ^0_0-COMP y es fácil comprobar que este $\mathbf{X}$ es finito y tiene todos los elementos que cumplen $\varphi[n]$, contradiciendo ⟨1⟩5.

⟨1⟩9. Q.E.D.

DEMOSTRACIÓN: Por ⟨1⟩8 y el lema 2.55 existe $\pi_{\mathbf{Y}}$, y definimos $\mathbf{f} = p_2 \circ \pi_{\mathbf{Y}}$, donde p_2 es la proyección de la segunda coordenada, ya que los elementos de $\mathbf{Y}$ son pares de números. Además por definición de $\mathbf{Y}$, $\mathbf{f}$ es inyectiva y enumera los elementos que cumplen $\varphi[n]$, como queríamos.

□

Un lema importante, las sucesiones finitas de $n+2$ elementos con todos los elementos menores que $n+1$ necesariamente tienen un elemento repetido (es decir, no son inyectivas).

Lema 2.59.

$$RCA_0 \vdash \forall n \forall f \in \mathbb{N}^{n+2}.(\forall i < n+2.f(i) < n+1) \to \exists i,j < n+2.i \neq j \wedge f(i) = f(j).$$

DEMOSTRACIÓN:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0.

⟨1⟩2. Definimos
$$\varphi[n] :\equiv \forall f \in \mathbb{N}^{n+2}.(\forall i < n+2.f(i) < n+1) \to \exists i,j < n+2.i \neq j \wedge f(i) = f(j).$$

⟨1⟩3. $\mathfrak{M} \vDash \varphi[0]$.

DEMOSTRACIÓN: Sea $\mathbf{f} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{f} \in \mathbb{N}^2 \wedge (\forall i < 2.\mathbf{f}(i) < 1)$. Por tanto $\mathfrak{M} \vDash \mathbf{f}(0) = 0 = \mathbf{f}(1)$, y como $\mathfrak{M} \vDash \text{BASIC}$, $\mathfrak{M} \vDash 0 \neq 1$, como queríamos.

⟨1⟩4. $\mathfrak{M} \vDash \forall n.\varphi[n] \to \varphi[n+1]$.

⟨2⟩1. Sea $\mathbf{n} \in \mathbb{N}$ arbitrario tal que $\mathfrak{M} \vDash \varphi[\mathbf{n}]$.

⟨2⟩2. Sea $\mathbf{f} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{f} \in \mathbb{N}^{\mathbf{n}+3} \wedge \forall i < \mathbf{n}+3.\mathbf{f}(i) < \mathbf{n}+2$.

⟨2⟩3. Podemos suponer que $\mathfrak{M} \vDash \exists^1 i < \mathbf{n}+3.\mathbf{f}(i) = \mathbf{n}+1$.

DEMOSTRACIÓN: Si no hay dos alternativas, la primera que $\mathfrak{M} \vDash \neg\exists i < \mathbf{n}+3.\mathbf{f}(i) = \mathbf{n}+1$. En tal caso consideramos $\mathbf{f} \restriction \{0,\dots,\mathbf{n}+1\}$, que cumple las condiciones necesarias para aplicarle $\varphi[\mathbf{n}]$ (la hipótesis de inducción) y así tendríamos los dos valores buscados. La segunda alternativa es que existan al menos $\mathbf{i},\mathbf{j} \in \mathbb{N}$ distintos que cumplan que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{i}) = \mathbf{f}(\mathbf{j}) = \mathbf{n}+1$, que era lo que buscabamos.

⟨2⟩4. Sea $\mathbf{n}_0 \in \mathbb{N}$ el único tal que $\mathfrak{M} \vDash \mathbf{n}_0 < \mathbf{n}+3 \wedge \mathbf{f}(\mathbf{n}_0) = \mathbf{n}+1$.

⟨2⟩5. Existe $\mathbf{g} \in \wp(\mathbb{N})$ tal que
$$\mathfrak{M} \vDash \mathbf{g} \in \mathbb{N}^{\mathbf{n}+3} \wedge \forall i < \mathbf{n}+3.(\forall i < \mathbf{n}+3.i \neq \mathbf{n}_0 \wedge i \neq \mathbf{n}+2 \to \mathbf{g}(i) = \mathbf{f}(i)) \wedge \mathbf{g}(\mathbf{n}_0) = \mathbf{f}(\mathbf{n}+2) \wedge \mathbf{g}(\mathbf{n}+2) = \mathbf{f}(\mathbf{n}_0).$$

DEMOSTRACIÓN: Es una simple Σ^0_0-COMP.

⟨2⟩6. Q.E.D.

DEMOSTRACIÓN: Es fácil ver que $\mathbf{g} \restriction \{0, \ldots, \mathbf{n}+1\}$ cumple las condiciones para aplicarle $\varphi[\mathbf{n}]$, así que existirán dos valores que cumplirán lo pedido. Es tambíen fácil ver que esos dos valores de $\mathbf{g}$ son 2 valores de $\mathbf{f}$ que cumplen lo pedido, ya que $\mathbf{g}$ no es más que $\mathbf{f}$ intercambiando los números de dos posiciones.

⟨1⟩5. Q.E.D.

DEMOSTRACIÓN: Se sigue de Π^0_1-IND en la fórmula $\varphi[n]$, dónde ⟨1⟩3 es el caso base y ⟨1⟩4 el caso inductivo.

□

La principal aplicación de los dos resultados anteriores será demostrar que RCA$_0$ permite el uso de cierto tipo restringido de Σ^0_1-comprensión. Por supuesto, el principio general de Σ^0_1-comprensión no está disponible en RCA$_0$: RCA$_0$ más Σ^0_1-comprensión es equivalente a la teoría ACA$_0$ (como veremos en el capítulo de ACA$_0$), la cual es estrictamente más fuerte que RCA$_0$. Sin embargo, en el siguiente teorema demostraremos que RCA$_0$ prueba Σ^0_1-comprensión *acotada*.

Definición 2.16 (**Σ^0_k-comprensión acotada**)**.** Sea $\Gamma \subseteq \mathrm{Form}$. Definimos el conjunto de los axiomas de comprensión acotada para Γ, denotado Γ-BCOMP, como el conjunto de todas las fórmulas

$$\forall n \exists X \forall i. i \in X \leftrightarrow i < n \wedge \varphi\{i\}$$

donde $n, i \in \mathrm{Var_N}$, $X \in \mathrm{Var_C}$, $\varphi\{i\} \in \Gamma$ tal que $X \notin \mathrm{Vl}(\varphi)$. ■

Teorema 2.60. *RCA$_0$ $\vdash$ Σ^0_1-BCOMP.*

DEMOSTRACIÓN:

⟨1⟩1. Sean $n, i \in \mathrm{Var_N}$, $X \in \mathrm{Var_C}$ y $\varphi\{i\} \in \Sigma^0_1$ tal que $X \notin \mathrm{Vl}(\varphi\{i\})$. Sea $\mathfrak{M}$ un modelo de RCA$_0$ y $\{\nu_1, \ldots, \nu_k\} = \mathrm{Vl}(\varphi\{i\}) \setminus \{i, n\}$.

⟨1⟩2. Definimos $\psi :\equiv \forall n \exists X \forall i. i \in X \leftrightarrow i < n \wedge \varphi\{i\}$.

⟨1⟩3. $\mathrm{Vl}(\psi) = \{\nu_1, \ldots, \nu_k\}$.

DEMOSTRACIÓN: Por definición de variable libre.

⟨1⟩4. Sean $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k \in \mathbb{N} \cup \wp(\mathbb{N})$, denotamos $\varphi(i, n) :\equiv \varphi(i, n, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k)$. Entonces
$$\boldsymbol{\psi} :\equiv \psi[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k] \equiv \forall n \exists X \forall i. i \in X \leftrightarrow i < n \wedge \varphi(i, n)$$
y es suficiente probar que $\mathfrak{M} \vDash \boldsymbol{\psi}$.

DEMOSTRACIÓN: Por la definición de sustitución y el teorema de completitud.

⟨1⟩5. Sea $\mathbf{n} \in \mathbb{N}$. Denotamos $\varphi[i] :\equiv \varphi(i, \mathbf{n})$ y supongamos que
$$\mathfrak{M} \vDash \neg \exists X. X = \{i \mid i < \mathbf{n} \wedge \varphi[i]\}.$$

⟨1⟩6. Existe $\mathbf{f} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{f} : \mathbb{N} \longrightarrow \mathbb{N} \wedge \text{Iny}$ y además $\mathfrak{M} \vDash \forall m.\mathbf{f}(m) < \mathbf{n} \wedge \varphi[\mathbf{f}(m)]$.

Demostración: Por ⟨1⟩5 y por lema 2.58 tenemos la existencia de la función.

⟨1⟩7. Existen $\mathbf{m}_1, \mathbf{m}_2 \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{m}_1 \neq \mathbf{m}_2 \wedge \mathbf{f}(\mathbf{m}_1) = \mathbf{f}(\mathbf{m}_2)$.

Demostración: Sabemos que $\mathfrak{M} \vDash \mathbf{f}[\mathbf{n}+2] \in \mathbb{N}^{\mathbf{n}+2}$ y por ⟨1⟩6 $\mathfrak{M} \vDash \forall m < \mathbf{n} + 2.\mathbf{f}[\mathbf{n}+2](m) < \mathbf{n}+1$. Por el lema 2.59 tenemos que existen $\mathbf{m}_1, \mathbf{m}_2 \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{m}_1 \neq \mathbf{m}_2 \wedge \mathbf{f}[\mathbf{n}+2](\mathbf{m}_1) = \mathbf{f}[\mathbf{n}+2](\mathbf{m}_2)$, de donde se sigue el resultado.

⟨1⟩8. Q.E.D.

Demostración: Asumiendo ⟨1⟩5 hemos llegado a una contradicción, ya que por ⟨1⟩7 $\mathbf{f}$ no sería inyectiva.

□

2.10. Sistemas numéricos

Introducimos una notación que utilizaremos en esta sección para hacer las fórmulas más legibles.

Notación. Cuando definamos una fórmula como

$$\phi((x_{11},\ldots,x_{1m_1}),\ldots,(x_{k1},\ldots,x_{km_k})) :\equiv \psi(x_{11},\ldots,x_{1m_1},\ldots,x_{k1},\ldots,x_{km_k})$$

realmente estamos definiendo la fórmula

$$\phi(x_1,\ldots,x_k) :\equiv \exists x_{11},\ldots,x_{1m_1} \leq x_1 \exists \cdots \exists x_{k1},\ldots,x_{km_k} \leq x_k.$$

$$x_1 = (x_{11},\ldots,x_{1m_1}) \wedge \cdots \wedge x_k = (x_{k1},\ldots,x_{km_k}) \wedge \psi(x_{11},\ldots,x_{1m_1},\ldots,x_{k1},\ldots,x_{km_k}).$$

Lo mismo ocurre con la fórmula $\phi[(x_{11},\ldots,x_{1m_1},\ldots,(x_{k1},\ldots,x_{km_k})]$ y con la fórmula $\phi\{(x_{11},\ldots,x_{1m_1}),\ldots,(x_{k1},\ldots,x_{km_k})\}$. Por ejemplo

$$\phi[(x_1,x_2)] :\equiv x_1 = x_2$$

define la fórmula

$$\phi[x] :\equiv \exists x_1, x_2 \leq x.x = (x_1,x_2) \wedge x_1 = x_2.$$

Notemos que si $\psi \in \Sigma_0^0$ entonces $\phi \in \Sigma_0^0$. ■

En esta sección vamos a definir los distintos sistemas numéricos, $\mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$ dentro de RCA_0. Debido a nuestra elección de trabajar en la aritmética de segundo orden, los dos primeros ($\mathbb{Z}$ y $\mathbb{Q}$) se podrán definir como subconjuntos del modelo, pero el último, $\mathbb{R}$, tendrá que ser tratado de forma diferente, como veremos más adelante.

Necesitamos la definición de operación binaria:

Definición 2.17. Definimos la fórmula

$$\textsc{BinOper}[X, Y] :\equiv X : Y \times Y \longrightarrow Y.$$

■

2.10.1. $\mathbb{Z}$

Definición 2.18. Definimos las siguientes fórmulas (únicamente para esta subsección):

$$\begin{aligned}
\phi_=[(m,n),(p,q)] &:\equiv m+q = n+p,\\
\phi_<[(m,n),(p,q)] &:\equiv m+q < n+p,\\
\phi_+[(m,n),(p,q),(r,s)] &:\equiv r = m+p \wedge s = n+q,\\
\phi_-[(m,n),(p,q),(r,s)] &:\equiv r = m+q \wedge s = n+p,\\
\phi_\cdot[(m,n),(p,q),(r,s)] &:\equiv r = m\cdot p + n\cdot q \wedge m\cdot q + n\cdot p.
\end{aligned}$$

Notemos que todas son Σ_0^0.

■

Notemos que, por ser Σ_0^0, estas fórmulas definen conjuntos; es más, las dos primeras definen relaciones binarias sobre $\mathbb{N}\times\mathbb{N}$ y las otras tres, operaciones binarias sobre $\mathbb{N}\times\mathbb{N}$, como nos dice el siguiente teorema.

Lema 2.61.

1. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j \leq x. x = (i,j) \wedge \phi_=[i,j])$.
2. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j \leq x. x = (i,j) \wedge \phi_<[i,j])$.
3. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j,k \leq x. x = ((i,j),k) \wedge \phi_+[i,j,k])$.
4. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j,k \leq x. x = ((i,j),k) \wedge \phi_-[i,j,k])$.
5. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j,k \leq x. x = ((i,j),k) \wedge \phi_\cdot[i,j,k])$.

Y los llamamos $Eq_\mathbb{Z}, Le_\mathbb{Z}, Sum_\mathbb{Z}, Minus_\mathbb{Z}$ *y* $Prod_\mathbb{Z}$*, respectivamente. Además*

1. $RCA_0 \vdash \textsc{Equiv}[Eq_\mathbb{Z}, \mathbb{N}\times\mathbb{N}]$.
2. $RCA_0 \vdash \textsc{BinRel}[Le_\mathbb{Z}, \mathbb{N}\times\mathbb{N}]$.

3. $RCA_0 \vdash \textsc{BinOper}[\textsc{Sum}_{\mathbb{Z}}, \mathbb{N} \times \mathbb{N}]$.
4. $RCA_0 \vdash \textsc{BinOper}[\textsc{Minus}_{\mathbb{Z}}, \mathbb{N} \times \mathbb{N}]$.
5. $RCA_0 \vdash \textsc{BinOper}[\textsc{Prod}_{\mathbb{Z}}, \mathbb{N} \times \mathbb{N}]$.

Además $\textsc{Le}_{\mathbb{Z}}$ *respeta* $\textsc{Eq}_{\mathbb{Z}}$ *y las 3 operaciones binarias repetan* $\textsc{Eq}_{\mathbb{Z}}$.

Demostración: Inmediato a partir de las definiciones dadas. □

Definición 2.19 (**Números enteros**)**.** Gracias al lema anterior, podemos definir $\mathbb{Z}$ como el cociente de $\mathbb{N} \times \mathbb{N}$ por la relación $\textsc{Eq}_{\mathbb{Z}}$.

La relación binaria en $\mathbb{Z}$, $<_{\mathbb{Z}}$, es la resultante de restringir $\textsc{Le}_{\mathbb{Z}}$ al cociente (ya que $\mathbb{Z} \subseteq \mathbb{N} \times \mathbb{N}$)

Las operaciones binarias en $\mathbb{Z}$, $+_{\mathbb{Z}}$, $-_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$; son las resultantes de restringir el dominio de $\textsc{Sum}_{\mathbb{Z}}$, $\textsc{Minus}_{\mathbb{Z}}$ y $\textsc{Prod}_{\mathbb{Z}}$ (respectivamente) a $\mathbb{Z}$ y luego componer con π.

$=_Z$ será la misma relación binaria sobre $\mathbb{Z}$ que $=$, $0_{\mathbb{Z}}$ será $(0,0)$ y $1_{\mathbb{Z}}$ será $(1,0)$, que se pueden demostrar que pertenecen a $\mathbb{Z}$. ■

Nota. Como es habitual podemos ver $\mathbb{N}$ dentro de $\mathbb{Z}$, ya que dado $n \in \mathbb{N}$ lo podemos identificar con $(n,0)$. Esto nos define una función de $\mathbb{N}$ en $\mathbb{Z}$, aunque nunca la escribiremos explícitamente, pero entenderemos que la estamos usando siempre que un natural esté donde debería haber un entero. ■

El teorema importante para que podamos trabajar con naturalidad con los enteros es el siguiente:

Teorema 2.62. RCA_0 *demuestra que el sistema*

$$\mathbb{Z}, +_{\mathbb{Z}}, -_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, 0_{\mathbb{Z}}, 1_{\mathbb{Z}}, <_{\mathbb{Z}}$$

es un dominio integral, que además es euclidiano, etc.

Demostración: Es directa usando el teorema 2.3 y usando la nota anterior para ver $\mathbb{N}$ dentro de $\mathbb{Z}$. □

Notación. Usaremos $-_{\mathbb{Z}} n$ como una notación para $0 -_{\mathbb{Z}} n$. ■

2.10.2. $\mathbb{Q}$

Lema 2.63. $RCA_0 \vdash \exists^1 X. X = \{i \mid i \in \mathbb{Z} \wedge 0 <_{\mathbb{Z}} i\}$.

A este conjunto único lo llamaremos $\mathbb{Z}^+$.

Demostración:
Como es habitual, la existencia es por Σ^0_0-COMP y la unicidad por igualdad de conjuntos. □

Definición 2.20. Definimos las siguientes fórmulas (únicamente para esta subsección):

$$\phi_{=}[(a,b),(c,d)] :\equiv a \cdot_{\mathbb{Z}} d =_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c,$$
$$\phi_{<}[(a,b),(c,d)] :\equiv a \cdot_{\mathbb{Z}} d <_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c,$$
$$\phi_{+}[(a,b),(c,d),(r,s)] :\equiv r =_{\mathbb{Z}} a \cdot_{\mathbb{Z}} d +_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c \wedge s =_{\mathbb{Z}} b \cdot_{\mathbb{Z}} d,$$
$$\phi_{-}[(a,b),(c,d),(r,s)] :\equiv r =_{\mathbb{Z}} a \cdot_{\mathbb{Z}} d -_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c \wedge s =_{\mathbb{Z}} b \cdot_{\mathbb{Z}} d,$$
$$\phi_{\cdot}[(a,b),(c,d),(r,s)] :\equiv r =_{\mathbb{Z}} a \cdot_{\mathbb{Z}} c \wedge s =_{\mathbb{Z}} b \cdot_{\mathbb{Z}} d.$$

Notemos que, dado un modelo $\mathfrak{M}$, todas son $(\mathbf{\Sigma^0_0})^{\mathrm{RCA}_0}_{\mathfrak{M}}$, por la nota 2.2.

■

Veamos que estas fórmulas definen conjuntos; es más las dos primeras definen relaciones binarias sobre $\mathbb{Z} \times \mathbb{Z}^+$ y las otras tres, operaciones binarias sobre $\mathbb{Z} \times \mathbb{Z}^+$, como nos dice el siguiente teorema.

Lema 2.64.

1. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j \leq x. x = (i,j) \wedge \phi_{=}[i,j])$.
2. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j \leq x. x = (i,j) \wedge \phi_{<}[i,j])$.
3. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j,k \leq x. x = ((i,j),k) \wedge \phi_{+}[i,j,k])$.
4. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j,k \leq x. x = ((i,j),k) \wedge \phi_{-}[i,j,k])$.
5. $RCA_0 \vdash \exists^1 X \forall x. x \in X \leftrightarrow (\exists i,j,k \leq x. x = ((i,j),k) \wedge \phi_{\cdot}[i,j,k])$.

Y los llamamos $Eq_{\mathbb{Q}}, Le_{\mathbb{Q}}, Sum_{\mathbb{Q}}, Minus_{\mathbb{Q}}$ *y* $Prod_{\mathbb{Q}}$*, respectivamente. Además*

1. $RCA_0 \vdash Equiv[Eq_{\mathbb{Q}}, \mathbb{Z} \times \mathbb{Z}^+]$.
2. $RCA_0 \vdash BinRel[Le_{\mathbb{Q}}, \mathbb{Z} \times \mathbb{Z}^+]$.
3. $RCA_0 \vdash BinOper[Sum_{\mathbb{Q}}, \mathbb{Z} \times \mathbb{Z}^+]$.
4. $RCA_0 \vdash BinOper[Minus_{\mathbb{Q}}, \mathbb{Z} \times \mathbb{Z}^+]$.
5. $RCA_0 \vdash BinOper[Prod_{\mathbb{Q}}, \mathbb{Z} \times \mathbb{Z}^+]$.

Además $Le_{\mathbb{Q}}$ *respeta* $Eq_{\mathbb{Q}}$ *y las tres operaciones binarias respetan* $Eq_{\mathbb{Q}}$.

Demostración:
Inmediato a partir de las definiciones dadas. □

Definición 2.21 (**Números racionales**)**.** Gracias al lema anterior, podemos definir $\mathbb{Q}$ como el cociente de $\mathbb{Z} \times \mathbb{Z}^+$ por la relación $\text{EQ}_{\mathbb{Q}}$.

La relación binaria en $\mathbb{Q}$, $<_{\mathbb{Q}}$, es la resultante de restringir $\text{LE}_{\mathbb{Q}}$ al cociente (ya que $\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{Z}^+$)

Las operaciones binarias en $\mathbb{Q}$, $+_{\mathbb{Q}}$, $-_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$; son las resultantes de restringir el dominio de $\text{SUM}_{\mathbb{Q}}$, $\text{MINUS}_{\mathbb{Q}}$ y $\text{PROD}_{\mathbb{Q}}$ al cociente (respectivamente) y luego componer con $\pi : \mathbb{Z} \times \mathbb{Z}^+ \longrightarrow \mathbb{Q}$.

$=_{\mathbb{Q}}$ será la misma relación binaria sobre $\mathbb{Q}$ que $=$ y $0_{\mathbb{Q}}$ será el representante de $(0_{\mathbb{Z}}, 1_{\mathbb{Z}})$ y $1_{\mathbb{Q}}$ será el representante de $(1_{\mathbb{Z}}, 1_{\mathbb{Z}})$. ■

Nota. Como es habitual podemos ver $\mathbb{Z}$ dentro de $\mathbb{Q}$, para ello basta identificar $z \in \mathbb{Z}$ con el representante de $(z, 1_{\mathbb{Z}})$. Esto nos define una función de $\mathbb{Z}$ en $\mathbb{Q}$, aunque nunca la escribiremos explícitamente, pero entenderemos que la estamos usando siempre que un entero (o un natural, que como vimos antes se puede entender como un entero) esté donde debería haber un racional. ■

Además, RCA_0 prueba el siguiente resultado fundamental sobre $\mathbb{Q}$.

Teorema 2.65. *RCA_0 demuestra que el sistema*

$$\mathbb{Q}, +_{\mathbb{Q}}, -_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, 0_{\mathbb{Q}}, 1_{\mathbb{Q}}, <_{\mathbb{Q}}$$

es un cuerpo ordenado.

Además invertir un racional no nulo es una función.

Teorema 2.66 (**Función inverso**)**.** $RCA_0 \vdash \exists^1 f : \mathbb{Q} \setminus \{0_{\mathbb{Q}}\} \longrightarrow \mathbb{Q} \setminus \{0_{\mathbb{Q}}\} \forall r \in \mathbb{Q} \setminus \{0_{\mathbb{Q}}\}. f(r) \cdot_{\mathbb{Q}} r =_{\mathbb{Q}} 1_{\mathbb{Q}}$.

A esta función la llamaremos $\cdot^{-1}$ y expresaremos $\cdot^{-1}(q)$ como q^{-1}.

Demostración: Por Σ^0_0-COMP existe el conjunto $\mathbf{X} \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \mathbf{X} = \{(p, q) \mid p \in \mathbb{Q} \setminus \{0_{\mathbb{Q}}\} \wedge p \cdot_{\mathbb{Q}} q = 1_{\mathbb{Q}}\}.$$

Por 2.65 $\mathbb{Q}$ es un cuerpo tenemos que ese conjunto define la función buscada y la unicidad es por igualdad de funciones. □

Notación. Usaremos las notaciones:

- $-_{\mathbb{Q}} p :\equiv 0 -_{\mathbb{Q}} p$.
- $\dfrac{p}{q} :\equiv p \cdot_{\mathbb{Q}} q^{-1}$.
- $2^{-k} :\equiv 1/2^k$.

■

Por último, nótese que también disponemos de la función valor absoluto en $\mathbb{Q}$.

Lema 2.67 (**Valor absoluto**)**.**

$$RCA_0 \vdash \exists^1 f : \mathbb{Q} \longrightarrow \mathbb{Q} \forall q \in \mathbb{Q}.(q \geq 0_{\mathbb{Q}} \to f(q) =_{\mathbb{Q}} q) \wedge (q <_{\mathbb{Q}} 0_{\mathbb{Q}} \to f(q) =_{\mathbb{Q}} -_{\mathbb{Q}} q).$$

A esta función la llamaremos $|\cdot|$ *y expresaremos* $|\cdot|(a)$ *como* $|a|$*.*

Demostración: Usando Σ^0_0-COMP e igualdad de conjuntos. □

2.10.3. $\mathbb{R}$

Los reales ya no pueden ser tratados de la misma manera que los enteros y los racionales. Para definir a los reales, usaremos a los conjuntos como representantes de los reales. En lugar de definir un representante único de cada real, lo que haremos será no trabajar con la igualdad, sino con otra relación binaria definida que dirá cuando dos conjuntos que representan a números reales representan el mismo número real.

Siguiendo la construcción clásica de Georg Cantor, usaremos sucesiones de Cauchy de números racionales para definir los números reales. Para ello, damos primero la definición de sucesión de números racionales.

Definición 2.22 (**Sucesión**)**.** Definimos $f \in X^{\mathbb{N}} :\equiv f : \mathbb{N} \longrightarrow X$ y en ese caso decimos que f es una sucesión de elementos de X. ■

Notación. Igual que con las sucesiones finitas, será habitual el uso variables de la fórma $\langle x_k : k \in \mathbb{N} \rangle$ para denotar sucesiones de elementos de X, y en ese caso escribiremos x_i en lugar de $\langle x_k : k \in \mathbb{N} \rangle(i)$.

Como caso particular, escogiendo $X = \mathbb{Q}$, tendremos las sucesiones de racionales, con las que vamos a definir $\mathbb{R}$. En particular, los elementos de $\mathbb{R}$ serán sucesiones de Cauchy con cierto ratio de convergencia.

Definición 2.23 (**Números reales**)**.** Definimos

$$\langle q_k : k \in \mathbb{N} \rangle \in \mathbb{R} :\equiv \langle q_k : k \in \mathbb{N} \rangle \in \mathbb{Q}^{\mathbb{N}} \wedge \forall k, i.|q_k - q_{k+i}| \leq_{\mathbb{Q}} 2^{-k}.$$

Y en ese caso se dice que $\langle q_k : k \in \mathbb{N} \rangle$ es un número real. ■

Por supuesto, $\mathbb{R}$ no es un conjunto en nuestro lenguaje y solo escribiremos, por abuso de notación, $x \in \mathbb{R}$ como una abreviatura de la fórmula anterior. Será usual hacer este tipo de notación cuando queramos hablar de conjuntos que realmente no son conjuntos en nuestras teorías (entendiendo siempre que son notaciones).

Notemos que a priori podríamos definir los números reales como sucesiones de Cauchy, sin la imposición de que tengan un ratio de convergencia ya establecido. Sin embargo como aparece en el libro de Simpson [8], para trabajar con esos números reales necesitamos al menos la teoría ACA_0 (que veremos posteriormente). Como RCA_0 es más débil necesitamos este enriquecimiento de la definición habitual de número real donde exigimos ese ratio de convergencia.

Definición 2.24 (**Igualdad en** $\mathbb{R}$)**.** Ahora definimos la igualdad de reales como la fórmula:

$$\langle q_k : k \in \mathbb{N}\rangle =_{\mathbb{R}} \langle q'_k : k \in \mathbb{N}\rangle :\equiv \langle q_k : k \in \mathbb{N}\rangle \in \mathbb{R} \wedge \langle q'_k : k \in \mathbb{N}\rangle \in \mathbb{R} \wedge \forall k.|q_k - q_{k'}| \leq_{\mathbb{Q}} 2^{-k+1}$$

■

Notación. Será importante distinguir entre $\exists^1 x \in \mathbb{R}.\varphi\{x\}$ y $\exists^1 x \in \mathbb{Q}^{\mathbb{N}}.\varphi\{x\}$. La primera fórmula se interpretará como

$$\exists x.x \in \mathbb{R} \wedge \varphi\{x\} \wedge \forall y \in \mathbb{R}.\varphi\{y\} \to x =_{\mathbb{R}} y,$$

mientras que la segunda será

$$\exists x.x \in \mathbb{Q}^{\mathbb{N}} \wedge x \in \mathbb{R} \wedge \varphi\{x\} \wedge \forall y \in \mathbb{Q}^{\mathbb{N}}.y \in \mathbb{R} \wedge \varphi\{y\} \to x = y,$$

donde $y \notin \mathrm{Vl}(\varphi\{x\})$.

Es decir, la primera fórmula interpreta la unicidad como unicidad en $\mathbb{R}$ (es decir, mediante $=_{\mathbb{R}}$), mientras que la segunda fórmula interpreta la unicidad como unicidad en $\mathbb{Q}^{\mathbb{N}}$ (es decir, mediante la igualdad de conjuntos). ■

Lo primero de todo, podemos ver $\mathbb{Q}$ dentro de $\mathbb{R}$ como dice el siguiente lema.

Lema 2.68. *$RCA_0 \vdash \forall q \in \mathbb{Q}\exists^1 x \in \mathbb{Q}^{\mathbb{N}}.x \in \mathbb{R} \wedge \forall k.x_k = q$. De esta forma podemos ver $\mathbb{Q}$ como subconjunto de $\mathbb{R}$ (no en sentido literal, ya que $\mathbb{R}$ no es un conjunto).*

Demostración: La existencia es por Σ^0_0-COMP, la unicidad por la igualdad de funciones y comprobar que es un real es trivial. □

Notación. Cuando una variable que sea racional q aparezca en una fórmula se distinguirá por contexto cuando la usemos si nos referimos al número racional o al número real (que será la sucesión con valor constante q), pero denotaremos ambas por q. ■

Notemos que un real que sea racional no es necesariamente de la forma del lema anterior, ya que no estamos tomando la igualdad como igualdad de reales (y no como la igualdad del sistema lógico). Para que un número real x sea racional basta con que cumpla que $\exists q \in \mathbb{Q}.x =_{\mathbb{R}} q$.

Lema 2.69 (**Suma en $\mathbb{R}$**)**.**

$$RCA_0 \vdash \forall\langle q_k : k \in \mathbb{N}\rangle, \langle q'_k : k \in \mathbb{N}\rangle \in \mathbb{R}\exists^1\langle p_k : k \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}.\langle p_k : k \in \mathbb{N}\rangle \in \mathbb{R} \wedge \forall k.p_k = q_{k+1} +_{\mathbb{Q}} q'_{k+1}.$$

Si llamamos $x = \langle q_k : k \in \mathbb{N}\rangle$ e $y = \langle q'_k : k \in \mathbb{N}\rangle$ entonces el único real que cumple eso se llamará $x +_{\mathbb{R}} y$.

Demostración:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA$_0$ y $\langle \mathbf{q}_k : k \in \mathbb{N}\rangle, \langle \mathbf{q}'_k : k \in \mathbb{N}\rangle \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \langle \mathbf{q}_k : k \in \mathbb{N}\rangle \in \mathbb{R} \wedge \mathbf{q}'_k : k \in \mathbb{N}\rangle \in \mathbb{R}$.

⟨1⟩2. Existencia

⟨2⟩1. Existe $\langle \mathbf{p}_k : k \in \mathbb{R}\rangle \in \wp(\mathbb{N})$, tal que
$$\mathfrak{M} \vDash \langle \mathbf{p}_k : k \in \mathbb{R}\rangle \in \mathbb{Q}^{\mathbb{N}} \wedge \forall k.\mathbf{p}_k =_{\mathbb{Q}} \mathbf{q}_{k+1} +_{\mathbb{Q}} \mathbf{q}'_{k+1}.$$
Demostración: Gracias a lema 2.13 existe $\langle \mathbf{q}_k : k \in \mathbb{N}\rangle \times \langle \mathbf{q}'_k : k \in \mathbb{N}\rangle : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Q} \times \mathbb{Q}$, basta componer Diag : $\mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ con esa función y luego con $+_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$.

⟨2⟩2. $\mathfrak{M} \vDash \langle \mathbf{q}_k : k \in \mathbb{N}\rangle \in \mathbb{R}$.

Demostración: Sean $\mathbf{k}, \mathbf{i} \in \mathbb{N}$, entonces
$$\mathfrak{M} \vDash |\mathbf{p_{k+1}} -_{\mathbb{Q}} \mathbf{p_{k+i+1}}| \leq_{\mathbb{Q}} |(\mathbf{q_{k+1}} +_{\mathbb{Q}} \mathbf{q'_{k+1}}) -_{\mathbb{Q}} (\mathbf{q_{k+i+1}} +_{\mathbb{Q}} \mathbf{q'_{k+i+1}})| \leq_{\mathbb{Q}}$$
$$|\mathbf{q_{k+1}} -_{\mathbb{Q}} \mathbf{q_{k+i+1}}| +_{\mathbb{Q}} |\mathbf{q'_{k+1}} -_{\mathbb{Q}} \mathbf{q'_{k+i+1}}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}+1} +_{\mathbb{Q}} 2^{-\mathbf{k}+1} =_{\mathbb{Q}} 2^{-\mathbf{k}}.$$

⟨2⟩3. Q.E.D.

⟨1⟩3. Unicidad

Demostración: Por igualdad de funciones.

⟨1⟩4. Q.E.D.

□

Lema 2.70 (**Opuesto en $\mathbb{R}$**)**.**

$$RCA_0 \vdash \forall\langle q_k : k \in \mathbb{N}\rangle \in \mathbb{R}\exists^1\langle p_k : k \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}.\langle p_k : k \in \mathbb{N}\rangle \in \mathbb{R} \wedge \forall k.p_k = -_{\mathbb{Q}} q_k.$$

Si llamamos $x = \langle q_k : k \in \mathbb{N}\rangle$ entonces el único conjunto que cumple eso se denotará $-_{\mathbb{R}} x$.

Demostración: Análoga a la anterior, pero siendo ahora la demostración de que la sucesión es un real trivial. □

Notación. Si $x, y \in \mathbb{R}$, $x -_{\mathbb{R}} y$ denotará $x +_{\mathbb{R}} (-_{\mathbb{R}} y)$. ■

Definición 2.25 (**Desigualdad en** $\mathbb{R}$)**.** Definimos

$$\langle q_k : k \in \mathbb{N}\rangle \leq_{\mathbb{R}} \langle q'_k : k \in \mathbb{N}\rangle :\equiv \langle q_k : k \in \mathbb{N}\rangle \in \mathbb{R} \wedge \langle q'_k : k \in \mathbb{N}\rangle \in \mathbb{R} \wedge \forall k.q_k \leq_{\mathbb{Q}} q'_k +_{\mathbb{Q}} 2^{-k+1}.$$

También definimos $x <_{\mathbb{R}} y :\equiv y \not\leq_{\mathbb{R}} x$. ■

Teorema 2.71. *RCA_0 prueba que el sistema*

$$\mathbb{R}, +_{\mathbb{R}}, -_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}}, <_{\mathbb{R}}, =_{\mathbb{R}}$$

cumple los axiomas de grupo abeliano ordenado.

Nota. Suponiendo que $x, y \in \mathbb{R}$ entonces fórmulas como $x \leq_{\mathbb{R}} y, x =_{\mathbb{R}} y, x +_{\mathbb{R}} y =_{\mathbb{R}} z, \ldots$ son $(\mathbf{\Pi^0_1})^{\mathrm{RCA}_0}$ y $x <_{\mathbb{R}} y, x \neq_{\mathbb{R}} 0_{\mathbb{R}}, \ldots$ son $(\mathbf{\Sigma^0_1})^{\mathrm{RCA}_0}$.

Lema 2.72 (**Producto en** $\mathbb{R}$)**.**

$$RCA_0 \vdash \forall \langle q_k : k \in \mathbb{N}\rangle, \langle q'_k : k \in \mathbb{N}\rangle \in \mathbb{R} \exists^1 \langle p_k : k \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}.\langle p_k : k \in \mathbb{N}\rangle \in \mathbb{R} \wedge \forall k.p_k = q_{n+k} \cdot_{\mathbb{Q}} q'_{n+k}$$

donde n es una abreviatura de $\mu m.2^m \geq_{\mathbb{Q}} |q_0| +_{\mathbb{Q}} |q'_0| +_{\mathbb{Q}} 2$.

Si llamamos $x = \langle q_k : k \in \mathbb{N}\rangle$ e $y = \langle q'_k : k \in \mathbb{N}\rangle$ entonces el único real que cumple eso se llamará $x \cdot_{\mathbb{R}} y$.

Demostración: Similar a los anteriores. □

El teorema fundamental de los reales en RCA_0 es el que sigue.

Teorema 2.73. *RCA_0 demuestra que el sistema*

$$\mathbb{R}, +_{\mathbb{R}}, -_{\mathbb{R}}, \cdot_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}}, <_{\mathbb{R}}, =_{\mathbb{R}}$$

cumple los axiomas de un cuerpo arquimediano ordenado.

Definimos tambíen el valor absoluto de números reales (el cual escribiremos igual que el de números racionales y distinguiremos por contexto).

Teorema 2.74 (**Valor absoluto en** $\mathbb{R}$)**.**

$$RCA_0 \vdash \forall x \in \mathbb{R} \exists^1 y \in \mathbb{Q}^{\mathbb{N}}.y \in \mathbb{R} \wedge$$

$$(x \geq_{\mathbb{R}} 0 \to y = x) \wedge (x <_{\mathbb{R}} 0 \to y = -_{\mathbb{R}} x).$$

DEMOSTRACIÓN: La demostración es sencilla usando que todo número real tiene opuesto y usando el tercio excluso. □

Vamos a necesitar hablar de sucesiones de números reales. A priori esto no es posible, ya que una sucesión de números reales sería una función $f : \mathbb{N} \longrightarrow \mathbb{R}$, sin embargo $\mathbb{R}$ no es un conjunto y por tanto ello no es expresable tal cual en nuestro lenguaje. El truco será definir las sucesiones de reales como funciones $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Q}$, donde si fijamos el primer valor del par ordenado, la función resultante es un real.

Lema 2.75.

$$RCA_0 \vdash \forall X, Y, Z \forall f : X \times Y \longrightarrow Z \forall x \in X \exists^1 f' : Y \longrightarrow Z \forall y \in Y. f'(y) = f(x, y).$$

Además a esta única función f' la llamaremos $(f)_x$.

DEMOSTRACIÓN: Basta con usar el lema 2.14 definiendo $f' = f \restriction \{x\} \times Y$. □

Definición 2.26 (**Sucesiones en $\mathbb{R}$**)**.** Definimos

$$f \in \mathbb{R}^{\mathbb{N}} :\equiv f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Q} \wedge \forall n \in \mathbb{N}.(f)_n \in \mathbb{R}.$$

Usaremos notaciones como $\langle x_n : n \in \mathbb{N} \rangle$ para la sucesión f donde $(f)_n = x_n$. ■

Definición 2.27 (**Límite**)**.** Definimos

$$x =_{\mathbb{R}} \lim_n x_n :\equiv \langle x_n : n \in \mathbb{N} \rangle \in \mathbb{R}^{\mathbb{N}} \wedge x \in \mathbb{R} \wedge \forall \epsilon >_{\mathbb{R}} 0 \exists n \forall i. |x -_{\mathbb{R}} x_{n+i}| <_{\mathbb{R}} \epsilon.$$

Seremos algo laxos con el uso de la notación para esta fórmula, por ejemplo nos permitiremos escribir $\lim_n x_n =_{\mathbb{R}} x$ o $x =_{\mathbb{R}} \lim_n x_n =_{\mathbb{R}} \lim_n y_n$, asumiendo que el lector entiende el significado. ■

Está claro que no se puede hablar de completitud de $\mathbb{R}$, pues para ello haría falta conjuntos de números reales y eso es algo que no tenemos. Sin embargo, podríamos pensar en la completitud de las sucesiones de números reales, sin embargo (como veremos demostrando la equivalencia de este teorema a ACA$_0$) esto no se puede probar en RCA$_0$. Lo que sí es capaz de probar es la completitud de intervalos encajados.

Teorema 2.76 (**Completitud de intervalos encajados**)**.**

$$RCA_0 \vdash \forall \langle a_n : n \in \mathbb{N} \rangle, \langle b_n : n \in \mathbb{N} \rangle \in \mathbb{R}^{\mathbb{N}}.(\forall n. a_n \leq_{\mathbb{R}} a_{n+1} \leq_{\mathbb{R}} b_{n+1} \leq_{\mathbb{R}} b_n) \wedge \lim_n |a_n -_{\mathbb{R}} b_n| =_{\mathbb{R}} 0 \rightarrow$$

$$\exists x \in \mathbb{R}. x =_{\mathbb{R}} \lim_n a_n =_{\mathbb{R}} \lim_n b_n \wedge \forall n. a_n \leq_{\mathbb{R}} x \leq_{\mathbb{R}} b_n.$$

DEMOSTRACIÓN:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 con $\langle \mathbf{a}_n : n \in \mathbb{N}\rangle = \langle \mathbf{q}_{nk} : n, k \in \mathbb{N}\rangle, \langle \mathbf{b}_n : n \in \mathbb{N}\rangle = \langle \mathbf{q}'_{nk} : n, k \in \mathbb{N}\rangle$ sucesiones de reales tales que

$$\mathfrak{M} \vDash \forall n.\mathbf{a}_n \leq_{\mathbb{R}} \lim_n x_n \mathbf{a}_{n+1} \leq_{\mathbb{R}} \mathbf{b}_{n+1} \leq_{\mathbb{R}} \mathbf{b}_n,$$
$$\mathfrak{M} \vDash \lim_n |\mathbf{a}_n -_{\mathbb{R}} \mathbf{b}_n| =_{\mathbb{R}} 0.$$

⟨1⟩2. $\mathfrak{M} \vDash (\forall m, n.\mathbf{a}_m \leq_{\mathbb{R}} \mathbf{b}_n) \wedge (\forall m, i.\mathbf{a}_m \leq_{\mathbb{R}} \mathbf{a}_{m+i}) \wedge (\forall m, i.\mathbf{b}_m \geq_{\mathbb{R}} \mathbf{b}_{m+i})$.

⟨2⟩1. Sean $\mathbf{m}, \mathbf{n} \in \mathbb{N}$.

⟨2⟩2. $\mathfrak{M} \vDash \forall i.\mathbf{a}_{\mathbf{m}} \leq_{\mathbb{R}} \mathbf{a}_{\mathbf{m}+i}$.

DEMOSTRACIÓN: Por Π^0_1-inducción y ser $\leq_{\mathbb{R}}$ transitiva.

⟨2⟩3. $\mathfrak{M} \vDash \forall i.\mathbf{b}_{\mathbf{m}} \geq_{\mathbb{R}} \mathbf{b}_{\mathbf{m}+i}$.

DEMOSTRACIÓN: Por Π^0_1-inducción y ser $\leq_{\mathbb{R}}$ transitiva.

⟨2⟩4. Q.E.D.

DEMOSTRACIÓN: Por casos. Si $\mathfrak{M} \vDash \mathbf{m} \leq \mathbf{n}$, sabemos que existe $\mathbf{r} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{m} + \mathbf{r} = \mathbf{n}$, por tanto usando ⟨1⟩1 y ⟨2⟩2 obtenemos:

$$\mathfrak{M} \vDash \mathbf{a}_{\mathbf{m}} \leq_{\mathbb{R}} \mathbf{a}_{\mathbf{m}+\mathbf{r}} = \mathbf{a}_{\mathbf{n}} \leq_{\mathbb{R}} \mathbf{b}_{\mathbf{n}}.$$

El caso $\mathfrak{M} \vDash \mathbf{m} \geq \mathbf{n}$ es análogo, usando ahora ⟨1⟩1 y ⟨2⟩3.

⟨1⟩3. $\mathfrak{M} \vDash \forall k \exists n \geq k + 2.|\mathbf{q}_{nn} -_{\mathbb{Q}} \mathbf{q}'_{nn}| \leq_{\mathbb{Q}} 2^{-k-2}$.

⟨2⟩1. Sea $\mathbf{k} \in \mathbb{N}$.

⟨2⟩2. Existe $\mathbf{m} \in \mathbb{N}$, tal que $\mathfrak{M} \vDash \forall i.|\mathbf{q}_{\mathbf{m}+i,\mathbf{m}+i} -_{\mathbb{Q}} \mathbf{q}'_{\mathbf{m}+i,\mathbf{m}+i}| \leq 2^{-\mathbf{k}-3} +_{\mathbb{Q}} 2^{-\mathbf{m}-i+1}$.

DEMOSTRACIÓN: Por ⟨1⟩1 sabemos que $\mathfrak{M} \vDash \exists m \forall i.|\mathbf{a}_{m+i} -_{\mathbb{R}} \mathbf{b}_{m+i}| \leq_{\mathbb{R}} 2^{-\mathbf{k}-3}$, es decir, por definición de $\leq_{\mathbb{R}}$, tenemos:

$$\mathfrak{M} \vDash \exists m \forall i, j.|\mathbf{q}_{m+i,j} -_{\mathbb{Q}} \mathbf{q}'_{m+i,j}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}-3} +_{\mathbb{Q}} 2^{-j+1}.$$

Sea $\mathbf{m}$ que cumpla lo anterior, basta con fijar $j = \mathbf{m} + i$ para obtener lo pedido.

⟨2⟩3. Caso 1: Si $\mathfrak{M} \vDash \mathbf{m} < \mathbf{k} + 4$.

DEMOSTRACIÓN: Cogemos $n = \mathbf{k} + 4$ y por ⟨2⟩2 (como $\mathfrak{M} \vDash \mathbf{m} < \mathbf{k} + 4$ se tiene que $\mathfrak{M} \vDash \exists r.\mathbf{m} + r = \mathbf{k} + 4$ y se puede aplicar ⟨2⟩2):

$$\mathfrak{M} \vDash |\mathbf{q}_{\mathbf{k}+4,\mathbf{k}+4} -_{\mathbb{Q}} \mathbf{q}'_{\mathbf{k}+4,\mathbf{k}+4}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}-3} +_{\mathbb{Q}} 2^{-\mathbf{k}-3} \leq_{\mathbb{Q}} 2^{-\mathbf{k}-2}.$$

⟨2⟩4. Caso 2: Si $\mathfrak{M} \vDash \mathbf{m} \geq \mathbf{k} + 4$.

DEMOSTRACIÓN: Cogemos $n = \mathbf{m}$, y por ⟨2⟩2

$$\mathfrak{M} \vDash |\mathbf{q}_{\mathbf{m},\mathbf{m}} -_{\mathbb{Q}} \mathbf{q}'_{\mathbf{m},\mathbf{m}}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}-3} +_{\mathbb{Q}} 2^{-\mathbf{m}+1} \leq_{\mathbb{Q}} 2^{-\mathbf{k}-3} +_{\mathbb{Q}} 2^{-\mathbf{k}-3} =_{\mathbb{Q}} 2^{-\mathbf{k}-2}.$$

⟨2⟩5. Q.E.D.

DEMOSTRACIÓN: ⟨2⟩3 y ⟨2⟩4 cubren todas las posibilidades.

⟨1⟩4. Existe $\mathbf{x} = \langle \mathbf{q}_{\mathbf{f}(k),\mathbf{f}(k)} : k \in \mathbb{N}\rangle$ donde $\mathbf{f}(k) = \mu n.n \geq k + 2 \wedge |\mathbf{q}_{nn} -_{\mathbb{Q}} \mathbf{q}'_{nn}| \leq_{\mathbb{Q}} 2^{-k-2}$

DEMOSTRACIÓN: $\mathbf{f}$ existe gracias a minimización y a $\langle 1\rangle 3$, $\mathbf{x}$ existe por composición de funciones.

$\langle 1\rangle 5$. $\mathfrak{M} \vDash \mathbf{x} \in \mathbb{R}$.

$\langle 2\rangle 1$. $\mathfrak{M} \vDash \mathbf{x} \in \mathbb{Q}^{\mathbb{N}}$.

DEMOSTRACIÓN: Por $\langle 1\rangle 4$.

$\langle 2\rangle 2$. $\mathfrak{M} \vDash \forall k, i.|\mathbf{q}_{\mathbf{f}(k),\mathbf{f}(k)} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f}(k+i),\mathbf{f}(k+i)}| \leq_{\mathbb{Q}} 2^{-k}$.

$\langle 3\rangle 1$. Sean $\mathbf{k}, \mathbf{i} \in \mathbb{N}$.

$\langle 3\rangle 2$. $\mathfrak{M} \vDash |\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k+i)}}| \leq_{\mathbb{Q}} |\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}}| +_{\mathbb{Q}} 2^{-\mathbf{k}-2}$.

DEMOSTRACIÓN:

$\mathfrak{M} \vDash |\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k+i)}}| =_{\mathbb{Q}} |\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} +_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k+i)}}| \leq_{\mathbb{Q}}$
$|\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}}| +_{\mathbb{Q}} |\mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k+i)}}| \leq_{\mathbb{Q}} |\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}}| +_{\mathbb{Q}} 2^{-\mathbf{f(k)}} \leq_{\mathbb{Q}}$
$|\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}}| +_{\mathbb{Q}} 2^{-\mathbf{k}-2}$

usando que $\mathfrak{M} \vDash \mathbf{a}_{\mathbf{f(k)}} \in \mathbb{R}$ en la penúltima desigualdad (además de que $\mathbf{f}$ es no decreciente por $\langle 1\rangle 4$) y que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{k}) \geq \mathbf{k} + 2$ por $\langle 1\rangle 4$ en la última desigualdad.

$\langle 3\rangle 3$. Caso 1: $|\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}}| =_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}}$

DEMOSTRACIÓN: Como por $\langle 1\rangle 2$ $\mathfrak{M} \vDash \mathbf{a}_{\mathbf{f(k)}} \leq_{\mathbb{R}} \mathbf{a}_{\mathbf{f(k+i)}}$, por tanto

$$\mathfrak{M} \vDash \mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} \leq_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} + 2^{-\mathbf{f(k)}+1}.$$

Se deduce entonces que

$\mathfrak{M} \vDash \mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} \leq_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{f(k)}+1} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} =_{\mathbb{Q}} 2^{-\mathbf{f(k)}+1} \leq_{\mathbb{Q}} 2^{-\mathbf{k}-1}$.

Juntando esta cota a la de $\langle 3\rangle 2$ nos queda

$\mathfrak{M} \vDash |\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k+i)}}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}-1} +_{\mathbb{Q}} 2^{-\mathbf{k}-2} \leq_{\mathbb{Q}} 2^{-\mathbf{k}-1} +_{\mathbb{Q}} 2^{-\mathbf{k}-1} =_{\mathbb{Q}} 2^{-\mathbf{k}}$.

$\langle 3\rangle 4$. Caso 2: $|\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}}| =_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}}$.

DEMOSTRACIÓN: Como por $\langle 1\rangle 2$ $\mathfrak{M} \vDash \mathbf{a}_{\mathbf{f(k+i)}} \leq_{\mathbb{R}} \mathbf{b}_{\mathbf{f(k)}}$, por tanto

$$\mathfrak{M} \vDash \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} \leq_{\mathbb{Q}} \mathbf{q}'_{\mathbf{f(k)},\mathbf{f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{f(k)}+1},$$

Usando $\langle 1\rangle 4$ se deduce que

$$\mathfrak{M} \vDash \mathbf{q}'_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} =_{\mathbb{Q}} |\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}'_{\mathbf{f(k)},\mathbf{f(k)}}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}-2}.$$

Con las dos desigualdades anteriores obtenemos

$\mathfrak{M} \vDash \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} \leq_{\mathbb{Q}} \mathbf{q}'_{\mathbf{f(k)},\mathbf{f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}-1} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} \leq_{\mathbb{Q}} 2^{-\mathbf{k}-2} +_{\mathbb{Q}} 2^{-\mathbf{k}-1}$

Juntando esta cota a la de $\langle 3\rangle 2$ nos queda

$$\mathfrak{M} \vDash |\mathbf{q}_{\mathbf{f(k)},\mathbf{f(k)}} -_{\mathbb{Q}} \mathbf{q}_{\mathbf{f(k+i)},\mathbf{f(k+i)}}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}-2} +_{\mathbb{Q}} 2^{-\mathbf{k}-1} +_{\mathbb{Q}} 2^{-\mathbf{k}-2} =_{\mathbb{Q}} 2^{-\mathbf{k}}.$$

$\langle 3\rangle 5$. Q.E.D.

Gracias a que $\langle 3\rangle 3$ y $\langle 3\rangle 4$ cubren todos los casos.

$\langle 2\rangle 3$. Q.E.D.

DEMOSTRACIÓN: Por $\langle 2\rangle 1$ y $\langle 2\rangle 2$.

$\langle 1\rangle 6$. $\mathfrak{M} \vDash \mathbf{x} =_{\mathbb{R}} \lim_n \mathbf{a}_n =_{\mathbb{R}} \lim_n \mathbf{b}_n \wedge \forall n.\mathbf{a}_n \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathbf{b}_n$.

$\langle 2\rangle 1$. $\mathfrak{M} \vDash \forall n.\mathbf{x} \leq_{\mathbb{R}} \mathbf{b}_n$.

$\langle 3\rangle 1$. Es lo mismo que que $\mathfrak{M} \vDash \forall n, k.\mathbf{q}_{\mathbf{f}(k),\mathbf{f}(k)} \leq_{\mathbb{Q}} \mathbf{q}'_{n,k} +_{\mathbb{Q}} 2^{-k+1}$.

⟨3⟩2. Sean $\mathbf{n}, \mathbf{k} \in \mathbb{N}$.

⟨3⟩3. $\mathfrak{M} \vDash \mathbf{q_{f(k),f(k)}} \leq_{\mathbb{Q}} \mathbf{q'_{n,f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}}$.
DEMOSTRACIÓN: Como por ⟨1⟩2 $\mathfrak{M} \vDash \mathbf{a_{f(k)}} \leq_{\mathbb{R}} \mathbf{b_n}$ implica que
$$\mathfrak{M} \vDash \mathbf{q_{f(k),f(k)}} \leq_{\mathbb{Q}} \mathbf{q'_{n,f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{f(k)}+1} \leq_{\mathbb{Q}} \mathbf{q'_{n,f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}}.$$

⟨3⟩4. Caso 1: Si $\mathfrak{M} \vDash \mathbf{q'_{n,f(k)}} \leq_{\mathbb{Q}} \mathbf{q'_{n,k}}$.
DEMOSTRACIÓN: Usando ⟨3⟩3 obtenemos:
$$\mathfrak{M} \vDash \mathbf{q_{f(k),f(k)}} \leq_{\mathbb{Q}} \mathbf{q'_{n,f(k)}} + 2^{-\mathbf{k}} \leq_{\mathbb{Q}} \mathbf{q'_{n,k}} + 2^{-\mathbf{k}+1}.$$

⟨3⟩5. Caso 2: Si $\mathfrak{M} \vDash \mathbf{q'_{n,f(k)}} >_{\mathbb{Q}} \mathbf{q'_{n,k}}$.
DEMOSTRACIÓN: Como $\mathfrak{M} \vDash \mathbf{b_n} \in \mathbb{R}$ tenemos que
$$\mathfrak{M} \vDash \mathbf{q'_{n,f(k)}} -_{\mathbb{Q}} \mathbf{q'_{n,k}} =_{\mathbb{Q}} |\mathbf{q'_{n,f(k)}} -_{\mathbb{Q}} \mathbf{q'_{n,k}}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}},$$
y aplicando la desigualdad a ⟨3⟩4 obtenemos
$$\mathfrak{M} \vDash \mathbf{q_{f(k),f(k)}} \leq_{\mathbb{Q}} \mathbf{q'_{n,f(k)}} + 2^{-\mathbf{k}} \leq_{\mathbb{Q}} \mathbf{q'_{n,k}} +_{\mathbb{Q}} 2^{-\mathbf{k}} +_{\mathbb{Q}} 2^{-\mathbf{k}} =_{\mathbb{Q}} \mathbf{q'_{n,k}} +_{\mathbb{Q}} 2^{-\mathbf{k}+1}.$$

⟨3⟩6. Q.E.D.
DEMOSTRACIÓN: Gracias a que ⟨3⟩4 y ⟨3⟩5 cubren todos los casos.

⟨2⟩2. $\mathfrak{M} \vDash \forall n.\mathbf{a}_n \leq_{\mathbb{R}} \mathbf{x}$.

⟨3⟩1. Basta probar que $\mathfrak{M} \vDash \forall n, k.\mathbf{q}_{n,k} \leq_{\mathbb{Q}} \mathbf{q}_{\mathbf{f}(k),\mathbf{f}(k)} +_{\mathbb{Q}} 2^{-k+1}$.

⟨3⟩2. Sean $\mathbf{n}, \mathbf{k} \in \mathbb{N}$.

⟨3⟩3. $\mathfrak{M} \vDash \mathbf{q_{n,f(k)}} \leq_{\mathbb{Q}} \mathbf{q'_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}-1}$.
DEMOSTRACIÓN: Gracias a ⟨1⟩2 $\mathfrak{M} \vDash \mathbf{a_n} \leq_{\mathbb{R}} \mathbf{b_{f(k)}}$ y por tanto
$$\mathfrak{M} \vDash \mathbf{q_{n,f(k)}} \leq_{\mathbb{Q}} \mathbf{q'_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{f(k)}+1} \leq_{\mathbb{Q}} \mathbf{q'_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}-1}.$$

⟨3⟩4. $\mathfrak{M} \vDash \mathbf{q'_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}-1} \leq_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}}$.
DEMOSTRACIÓN: Si $\mathfrak{M} \vDash \mathbf{q'_{f(k),f(k)}} \leq_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}}$, entonces es trivial.
Si no, $\mathfrak{M} \vDash \mathbf{q'_{f(k),f(k)}} >_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}}$ y por ⟨1⟩4 $\mathfrak{M} \vDash |\mathbf{q'_{f(k),f(k)}} -_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}-2}$, pero $\mathfrak{M} \vDash |\mathbf{q'_{f(k),f(k)}} -_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}}| =_{\mathbb{Q}} \mathbf{q'_{f(k),f(k)}} -_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}}$, asi que usando la desigualdad anterior y ⟨3⟩3 llegamos a lo pedido.

⟨3⟩5. Caso 1: Si $\mathfrak{M} \vDash \mathbf{q_{n,k}} \leq_{\mathbb{Q}} \mathbf{q_{n,f(k)}}$.
DEMOSTRACIÓN: Usando ⟨3⟩3 y ⟨3⟩4 tenemos:
$$\mathfrak{M} \vDash \mathbf{q_{n,k}} \leq_{\mathbb{Q}} \mathbf{q_{n,f(k)}} \leq_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}} \leq_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}+1}.$$

⟨3⟩6. Caso 2: Si $\mathfrak{M} \vDash \mathbf{q_{n,k}} >_{\mathbb{Q}} \mathbf{q_{n,f(k)}}$.
DEMOSTRACIÓN: Como $\mathfrak{M} \vDash \mathbf{a_n} \in \mathbb{R}$ tenemos que
$$\mathfrak{M} \vDash \mathbf{q_{n,k}} -_{\mathbb{Q}} \mathbf{q_{n,f(k)}} =_{\mathbb{Q}} |\mathbf{q_{n,k}} -_{\mathbb{Q}} \mathbf{q_{n,f(k)}}| \leq_{\mathbb{Q}} 2^{-\mathbf{k}},$$
es decir
$$\mathfrak{M} \vDash \mathbf{q_{n,k}} \leq_{\mathbb{Q}} \mathbf{q_{n,f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}}.$$
Uniendo esa igualdad a la que queda de unir las de ⟨3⟩3 y ⟨3⟩4 (sumando $2^{-\mathbf{k}}$ a cada lado) obtenemos:
$$\mathfrak{M} \vDash \mathbf{q_{n,k}} \leq_{\mathbb{Q}} \mathbf{q_{n,f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}} \leq_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}} +_{\mathbb{Q}} 2^{-\mathbf{k}} =_{\mathbb{Q}} \mathbf{q_{f(k),f(k)}} +_{\mathbb{Q}} 2^{-\mathbf{k}+1}.$$

⟨3⟩7. Q.E.D.
Gracias a que ⟨3⟩5 y ⟨3⟩6 cubren todos los casos.

⟨2⟩3. $\mathfrak{M} \vDash \forall n.\mathbf{a}_n \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathbf{b}_n$.

DEMOSTRACIÓN: Por ⟨2⟩2 y ⟨2⟩1.

⟨2⟩4. Q.E.D.

DEMOSTRACIÓN: Sea $\boldsymbol{\epsilon} \in \wp(\mathbb{N})$ con $\mathfrak{M} \vDash \boldsymbol{\epsilon} \in \mathbb{R} \wedge \boldsymbol{\epsilon} >_{\mathbb{R}} 0$. Por ⟨1⟩1 existe $\mathbf{n}$ tal que

$$\mathfrak{M} \vDash \forall i.|\mathbf{a_{n+i}} -_{\mathbb{R}} \mathbf{b_{n+i}}| <_{\mathbb{R}} \boldsymbol{\epsilon}.$$

Pero como por ⟨2⟩3 para cualquier $\mathbf{i}$ se tendrá que $\mathfrak{M} \vDash \mathbf{a_{n+i}} \leq \mathbf{x} \leq \mathbf{b_{n+i}}$ en particular $\mathfrak{M} \vDash |\mathbf{a_{n+i}} -_{\mathbb{R}} \mathbf{x}| +_{\mathbb{R}} |\mathbf{b_{n+i}} -_{\mathbb{R}} \mathbf{x}| =_{\mathbb{R}} \mathbf{x} -_{\mathbb{R}} \mathbf{a_{n+i}} +_{\mathbb{R}} \mathbf{b_{n+i}} -_{\mathbb{R}} \mathbf{x} =_{\mathbb{R}} \mathbf{b_{n+i}} -_{\mathbb{R}} \mathbf{a_{n+i}} =_{\mathbb{R}} |\mathbf{b_{n+i}} -_{\mathbb{R}} \mathbf{a_{n+i}}| <_{\mathbb{R}} \boldsymbol{\epsilon}$.
Así

$$\mathfrak{M} \vDash |\mathbf{a_{n+i}} -_{\mathbb{R}} \mathbf{x}| \leq_{\mathbb{R}} |\mathbf{a_{n+i}} -_{\mathbb{R}} \mathbf{x}| +_{\mathbb{R}} |\mathbf{b_{n+i}} -_{\mathbb{R}} \mathbf{x}| <_{\mathbb{R}} \boldsymbol{\epsilon}$$
$$\mathfrak{M} \vDash |\mathbf{b_{n+i}} -_{\mathbb{R}} \mathbf{x}| \leq_{\mathbb{R}} |\mathbf{a_{n+i}} -_{\mathbb{R}} \mathbf{x}| +_{\mathbb{R}} |\mathbf{b_{n+i}} -_{\mathbb{R}} \mathbf{x}| <_{\mathbb{R}} \boldsymbol{\epsilon}$$

Por tanto

$$\mathfrak{M} \vDash (\forall \epsilon > 0 \exists n \forall i.|\mathbf{x} - \mathbf{a}_{n+i}| < \epsilon) \wedge (\forall \epsilon > 0 \exists n \forall i.|\mathbf{x} - \mathbf{b}_{n+i}| < \epsilon),$$

como queríamos.

⟨1⟩7. Q.E.D.

DEMOSTRACIÓN: Juntando ⟨1⟩5 y ⟨1⟩6.

□

Usando la completitud en intervalos encajados, podemos probar que $\mathbb{R}$ no es numerable, en el sentido de que dada una sucesión de reales, existe un real que no pertenece a la sucesión. La forma de demostrarlo es una especie de diagonalización, dada la sucesión de reales $\langle x_n : n \in \mathbb{N}\rangle$ podemos la de los racionales que la define $\langle q_{n,m} : n, m \in \mathbb{N}\rangle$ y ahora para cada n definimos usando recursión unos intervalos (encajado en los anteriores) que (cogiendo una aproximación racional suficientemente buena para estar en Σ_0^0, ya que comparar reales se nos va a Σ_1^0 o a Π_1^0) no contenga a x_n.

Teorema 2.77 ($\mathbb{R}$ **no es numerable**)**.**

$$RCA_0 \vdash \forall \langle x_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}} \exists y \in \mathbb{R} \forall n.x_n \neq_{\mathbb{R}} y.$$

DEMOSTRACIÓN:

⟨1⟩1. Sean $\mathfrak{M}$ un modelo de RCA_0 y $\langle \mathbf{x}_n : n \in \mathbb{N}\rangle = \langle \mathbf{q}_{nk} : n, k \in \mathbb{N}\rangle \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \langle \mathbf{x}_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}$.

⟨1⟩2. Existe $\langle (\mathbf{a}_n, \mathbf{b}_n) : n \in \mathbb{N}\rangle \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \langle (\mathbf{a}_n, \mathbf{b}_n) : n \in \mathbb{N}\rangle \in \mathbb{N} \longrightarrow \mathbb{Q} \times \mathbb{Q} \wedge (\mathbf{a}_0, \mathbf{b}_0) = (0, 1) \wedge$$
$$\forall n.(\mathbf{q}_{n,2n+3} \leq_{\mathbb{Q}} (\mathbf{a}_n +_{\mathbb{Q}} \mathbf{b}_n)/2 \to (\mathbf{a}_{n+1}, \mathbf{b}_{n+1}) = ((\mathbf{a}_n +_{\mathbb{Q}} 3\mathbf{b}_n)/4, \mathbf{b}_n)) \wedge$$
$$(\mathbf{q}_{n,2n+3} >_{\mathbb{Q}} (\mathbf{a}_n +_{\mathbb{Q}} \mathbf{b}_n)/2 \to (\mathbf{a}_{n+1}, \mathbf{b}_{n+1}) = (\mathbf{a}_n, (3\mathbf{a}_n +_{\mathbb{Q}} \mathbf{b}_n)/4)) \quad .$$

DEMOSTRACIÓN: La existencia se tiene por recursión y a que al cambiar los reales por aproximaciones con racionales estamos en fórmulas Σ_0^0.

⟨1⟩3. $\mathfrak{M} \vDash \lim_n |\mathbf{a}_n -_{\mathbb{Q}} \mathbf{b}_n| =_{\mathbb{R}} 0$.

⟨2⟩1. Definimos $\varphi[n] :\equiv |\mathbf{a}_n -_{\mathbb{Q}} \mathbf{b}_n| =_{\mathbb{Q}} 2^{-2n}$.

⟨2⟩2. $\mathfrak{M} \vDash \varphi[0]$.

DEMOSTRACIÓN: Sale directamente de la definición en ⟨1⟩2.

⟨2⟩3. $\mathfrak{M} \vDash \forall n.\varphi[n] \to \varphi[n+1]$.

DEMOSTRACIÓN: Sea $n \in \mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash |\mathbf{a_n} -_{\mathbb{Q}} \mathbf{b_n}| =_{\mathbb{Q}} 2^{-2\mathbf{n}}$. Por casos, si $\mathfrak{M} \vDash \mathbf{q_{n,2n+3}} \leq_{\mathbb{Q}} (\mathbf{a_n} + \mathbf{b_n})/2$, entonces

$$\mathfrak{M} \vDash |\mathbf{a_{n+1}} -_{\mathbb{Q}} \mathbf{b_{n+1}}| =_{\mathbb{Q}} |(\mathbf{a_n} +_{\mathbb{Q}} 3\mathbf{b_n})/4 -_{\mathbb{Q}} \mathbf{b_n}| =_{\mathbb{Q}} |(\mathbf{a_n} -_{\mathbb{Q}} \mathbf{b_n})/4| =_{\mathbb{Q}}$$

$$|(\mathbf{a_n} -_{\mathbb{Q}} \mathbf{b_n})|/4 =_{\mathbb{Q}} 2^{-2\mathbf{n}}2^{-2} =_{\mathbb{Q}} 2^{-2(\mathbf{n}+1)}.$$

El caso $\mathfrak{M} \vDash \mathfrak{M} \vDash \mathbf{q_{n,2n+3}} >_{\mathbb{Q}} (\mathbf{a_n} + \mathbf{b_n})/2$ es análogo.

⟨2⟩4. $\mathfrak{M} \vDash \forall n.|\mathbf{a}_n -_{\mathbb{Q}} \mathbf{b}_n| =_{\mathbb{Q}} 2^{-2n}$.

DEMOSTRACIÓN: Sale por Σ_0^0-IND en la fórmula $\varphi[n]$ donde ⟨2⟩2 es el caso base y ⟨2⟩3 es el paso inductivo.

⟨2⟩5. Q.E.D.

DEMOSTRACIÓN: Sale directamente de ⟨2⟩4.

⟨1⟩4. Existe $\mathbf{y} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{y} \in \mathbb{R} \wedge \mathbf{y} =_{\mathbb{R}} \lim_n \mathbf{a}_n =_{\mathbb{R}} \lim_n \mathbf{b}_n \wedge \forall n.\mathbf{a}_n \leq_{\mathbb{R}} \mathbf{y} \leq_{\mathbb{R}} \mathbf{b}_n$.

DEMOSTRACIÓN: Del lema 2.76 usando ⟨1⟩3 y verificando

$$\mathfrak{M} \vDash \forall n.\mathbf{a}_n \leq_{\mathbb{Q}} \mathbf{a}_{n+1} \leq_{\mathbf{Q}} \mathbf{b}_{n+1} \leq_{\mathbb{Q}} \mathbf{b}_n,$$

lo cual es fácil por su definición en ⟨1⟩2.

⟨1⟩5. Q.E.D.

DEMOSTRACIÓN: Sea $\mathbf{n} \in \mathbb{N}$ arbitrario, por casos. Si $\mathfrak{M} \vDash \mathbf{q_{n,2n+3}} \leq_{\mathbb{Q}} \frac{1}{2}(\mathbf{a_n} + \mathbf{b_n})$, entonces

$$\mathfrak{M} \vDash \mathbf{x_n} \leq_{\mathbb{R}} \frac{1}{2}(\mathbf{a_n} +_{\mathbb{Q}} \mathbf{b_n}) +_{\mathbb{Q}} 2^{-2\mathbf{n}-3} <_{\mathbb{R}} \mathbf{a_{n+1}} \leq_{\mathbb{R}} \mathbf{y}.$$

Si $\mathfrak{M} \vDash \mathbf{q_{n,2n+3}} >_{\mathbb{Q}} \frac{1}{2}(\mathbf{a_n} + \mathbf{b_n})$, entonces

$$\mathfrak{M} \vDash \mathbf{x_n} \geq_{\mathbb{R}} \frac{1}{2}(\mathbf{a_n} +_{\mathbb{Q}} \mathbf{b_n}) -_{\mathbb{Q}} 2^{-2\mathbf{n}-3} >_{\mathbb{R}} \mathbf{b_{n+1}} \geq_{\mathbb{R}} \mathbf{y}.$$

Por tanto se deduce que $\mathfrak{M} \vDash \mathbf{x_n} \neq_{\mathbb{R}} \mathbf{y}$.

□

2.10.4. El teorema de categorías de Baire en RCA_0

Como ya hemos explicado anteriormente, la teoría RCA_0 se usa típicamente como teoría base para obtener resultados de Matemática Inversa. Esto es, para calibrar cómo de fuerte es un cierto teorema de las matemáticas ordinarias, A, (o mejor, su formalización en el lenguaje de la aritmética se segundo orden) se considera un cierto principio de existencia en la aritmética de segundo orden, Φ, y se ha de probar que: i) Φ implica A, y ii) $\mathrm{RCA}_0 + A$ implica Φ. La investigación en Matemática Inversa ha puesto de manifiesto que RCA_0 es una teoría adecuada para este propósito: por una parte, es suficientemente débil como para ser una teoría base y, por otra parte, permite ciertos métodos de razonamiento básicos (Σ^0_1-inducción, recrsión primitiva, ...).
A pesar de que este es su uso principal, cabe destacar que existen ciertos teoremas importantes de las matemáticas ordinarias que ya son demostrables en la propia teoría RCA_0. Cerraremos el presente capítulo con un ejemplo de ello: el teorema de categorías de Baire.

Veamos que RCA_0 es suficiente para demostrar el teorema de categorías de Baire en $\mathbb{R}^k$: esto es, toda familia numerable de abiertos densos de $\mathbb{R}^k$ tiene intersección no vacía. Para demostrarlo, necesitamos antes algunas definiciones.

Definición 2.28 ($\mathbb{R}^k$)**.** Definimos

$$f \in \mathbb{R}^k :\equiv f : \{0, \dots, k-1\} \times \mathbb{N} \longrightarrow \mathbb{Q} \wedge \forall n < k.(f)_n \in \mathbb{R}.$$

En ese caso diremos que f es un punto de $\mathbb{R}^k$. Usaremos notaciones como $\langle x_n : n < k\rangle$ o $\langle x_0, \dots, x_{k-1}\rangle$ para la sucesión finita de longitud k, f donde $(f)_n = x_n$. Escribiremos $f \in \mathbb{R}^{<\mathbb{N}} :\equiv \exists k.f \in \mathbb{R}^k$. ■

Definición 2.29 (**Abiertos básicos y abiertos de** $\mathbb{R}^k$)**.** Definimos

$$\textsc{Basic}[k, \langle a_0, b_0, \dots, a_{k-1}, b_{k-1}\rangle] :\equiv \langle a_0, b_0, \dots, a_{k-1}, b_{k-1}\rangle \in \mathbb{Q}^{2k} \wedge \forall i < k.a_i <_{\mathbb{Q}} b_i,$$

decimos que $\langle a_0, b_0, \dots, a_{k-1}, b_{k-1}\rangle$ es un (código de un) abierto básico de $\mathbb{R}^k$.

$$\textsc{Open}[k, U] :\equiv \forall u \in U.\textsc{Basic}[k, u],$$

decimos que U es un abierto de $\mathbb{R}^k$. Si $\langle x_0, \dots, x_n\rangle \in \mathbb{R}^k$ y $\textsc{Open}[k, U]$, definimos:

$$\langle x_0, \dots, x_{k-1}\rangle \in U :\equiv \exists \langle a_0, b_0, \dots, a_{k-1}, b_{k-1}\rangle \in U \forall i < k.a_i < x_i < b_i.$$

■

Que un abierto sea denso:

Definición 2.30 (**Abierto denso en $\mathbb{R}^k$**)**.** Definimos

$$\textsc{Dense}[k,U] :\equiv (\textsc{Open}[k,U]) \wedge \forall \langle a_0, b_0, \ldots, a_{k-1}, b_{k-1}\rangle . \textsc{Basic}[k, \langle a_0, b_0, \ldots, a_{k-1}, b_{k-1}\rangle] \rightarrow$$
$$\exists \langle x_0, \ldots, x_{k-1}\rangle \in \mathbb{R}^k . \langle x_0, \ldots, x_{k-1}\rangle \in \langle a_0, b_0, \ldots, a_{k-1}, b_{k-1}\rangle \wedge \langle x_0, \ldots, x_{k-1}\rangle \in U.$$

□

Notación. Dados $\langle a_0, b_0, \ldots, a_{k-1}, b_{k-1}\rangle$, $\langle c_0, d_0, \ldots, c_{k-1}, d_{k-1}\rangle$ abiertos básicos definimos:

$$\langle a_0, b_0, \ldots, a_{k-1}, b_{k-1}\rangle < \langle c_0, d_0, \ldots, c_{k-1}, d_{k-1}\rangle :\equiv \forall i < k . a_i < c_i \wedge d_i < b_i.$$

Dados $\langle a_0, b_0, \ldots, a_{k-1}, b_{k-1}\rangle$ abierto básico y U un abierto definimos:

$$\langle a_0, b_0, \ldots, a_{k-1}, b_{k-1}\rangle < U :\equiv \exists u \in U . \langle a_0, b_0, \ldots, a_{k-1}, b_{k-1}\rangle < u.$$

■

Por último, antes del teorema tenemos que ver como se codifica en RCA_0 la sucesiones de conjuntos. La idea es que una sucesión de conjuntos $\langle U_i : i \in \mathbb{N}\rangle$ estará representada por un conjunto $U = \{\langle i, j\rangle \mid j \in U_i\}$. Para ello probamos el siguiente lema:

Lema 2.78. *$RCA_0 \vdash \forall U \forall k \exists^1 Y . Y = \{\langle k, n\rangle \mid \langle k, n\rangle \in U\}$. A este conjunto lo llamaremos U_k.*

Demostración: La existencia es por Σ^0_0-COMP y la unicidad por la igualdad de conjuntos. □

Así todo conjunto puede ser intepretado como una familia de conjuntos, pero cuando tengamos en mente que un conjunto está codificando a una familia de conjuntos será habitual en lugar de escribir U para el conjunto escribirlo como $\langle U_i : i \in \mathbb{N}\rangle$ y U_i será el i-ésimo miembro de la familia.

Finalmente podemos probar el teorema de categorías de Baire en RCA_0.

Teorema 2.79 (**Teorema de categorías de Baire**)**.**

$$RCA_0 \vdash \forall k \forall \langle U_n : n \in \mathbb{N}\rangle . (\forall n . \textit{Dense}[k, U_n]) \rightarrow \exists x \in \mathbb{R}^k \forall n . x \in U_n.$$

Demostración:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y sea $\mathbf{k} \in \mathbb{N}$, $\langle \mathbf{U}_n : n \in \mathbb{N}\rangle$ una sucesión de conjuntos tal que $\mathfrak{M} \vDash \forall n . \textsc{Dense}[\mathbf{k}, \mathbf{U}_n]$.

⟨1⟩2. Definimos

$$\varphi[n, \langle a_0, b_0, \ldots, a_{\mathbf{k}-1}, b_{\mathbf{k}-1}\rangle, \langle c_0, d_0, \ldots, c_{\mathbf{k}-1}, d_{\mathbf{k}-1}\rangle] :\equiv$$
$$\textsc{Basic}[\mathbf{k}, \langle a_0, b_0, \ldots, a_{\mathbf{k}-1}, b_{\mathbf{k}-1}\rangle] \wedge \textsc{Basic}[\mathbf{k}, \langle c_0, d_0, \ldots, c_{\mathbf{k}-1}, d_{\mathbf{k}-1}\rangle] \wedge$$
$$(\forall i < \mathbf{k} . a_i < c_i \wedge d_i < b_i) \wedge \langle c_0, d_0, \ldots, c_{\mathbf{k}-1}, d_{\mathbf{k}-1}\rangle < \mathbf{U}_n \wedge \forall i < \mathbf{k} . |c_i -_{\mathbb{Q}} d_i| <_{\mathbb{Q}} 2^{-n}.$$

⟨1⟩3. Existe $\theta(n, \langle a_0, b_0, \ldots, a_{\mathbf{k}-1}, b_{\mathbf{k}-1}\rangle, \langle c_0, d_0, \ldots, c_{\mathbf{k}-1}, d_{\mathbf{k}-1}\rangle, r) \in (\Sigma^0_0)_{\mathfrak{M}}$ tal que
$$\mathfrak{M} \vDash \varphi \leftrightarrow \exists r.\theta.$$

DEMOSTRACIÓN: Ya que $\varphi \in (\mathbf{\Sigma^0_1})^{\mathrm{RCA}_0}_{\mathfrak{M}}$, cada una de las fórmulas de las conjunciones son $(\mathbf{\Sigma^0_0})^{\mathrm{RCA}_0}_{\mathfrak{M}}$ salvo $\langle c_0, d_0, \ldots, c_{\mathbf{k}-1}, d_{\mathbf{k}-1}\rangle < \mathbf{U}_n$ que es $(\mathbf{\Sigma^0_1})^{\mathrm{RCA}_0}_{\mathfrak{M}}$

⟨1⟩4. Existe $\langle \mathbf{p}_0, \mathbf{q}_0, \ldots, \mathbf{p}_{\mathbf{k}-1}, \mathbf{q}_{\mathbf{k}-1}\rangle \in \mathbb{N}$ tal que
$\mathfrak{M} \vDash \textsc{Basic}[\mathbf{k}, \langle \mathbf{p}_0, \mathbf{q}_0, \ldots, \mathbf{p}_{\mathbf{k}-1}, \mathbf{q}_{\mathbf{k}-1}\rangle] \wedge \langle \mathbf{p}_0, \mathbf{q}_0, \ldots, \mathbf{p}_{\mathbf{k}-1}, \mathbf{q}_{\mathbf{k}-1}\rangle < \mathbf{U}_0 \wedge \forall i < \mathbf{k}.|\mathbf{p}_i -_{\mathbb{Q}} \mathbf{q}_i| <_{\mathbb{Q}} 1.$

DEMOSTRACIÓN: Como $\mathbf{U}_0$ es denso será no vácio, ahora podemos coger cualquier básico suyo y reducir los intervalos los $(\mathbf{p}_i, \mathbf{q}_i)$ lo suficiente para que sean menores de 1.

⟨1⟩5. Existe una función $\mathbf{f} : \mathbb{N} \longrightarrow \mathbb{Q}^{2\mathbf{k}}$ tal que
$$\mathfrak{M} \vDash \mathbf{f}(0) = \langle \mathbf{p}_0, \mathbf{q}_0, \ldots, \mathbf{p}_{\mathbf{k}-1}, \mathbf{q}_{\mathbf{k}-1}\rangle$$
$$\mathfrak{M} \vDash \forall n.\mathbf{f}(n+1) = \mu x.\exists u, r.x = (u, r) \wedge \theta(n+1, \mathrm{fst}(\mathbf{f}(n)), u, r).$$

DEMOSTRACIÓN: La existencia es por recursión, y que la funcón que da el mínimo esté bien definida se tiene gracias a la densidad de los $\mathbf{U}_n$ (y a la densidad de $\mathbb{Q}$ en $\mathbb{R}$).

⟨1⟩6. Q.E.D.

DEMOSTRACIÓN: Basta aplicar la completitud para intervalos encajados para cada $i < \mathbf{k}$ usando la sucesión de intervalos que nos da $\mathbf{f}$. Así que tendremos unos reales $\mathbf{x}_i$ tal que $\langle \mathbf{x}_0, \ldots, \mathbf{x}_{\mathbf{k}-1}\rangle$ pertenecerá a todos los $\mathbf{U}_n$ por ⟨1⟩5.

□

2.11. Resultados adicionales de RCA$_0$.

A título informativo, cerramos este capítulo enunciando otros teoremas importantes que son demostrables en nuestra teoría base RCA$_0$. Omitimos los detalles (en particular, habría que desarrollar un inmenso trabajo de codificaión en el lenguaje de la aritmética de los objetos matemáticos correspondientes) y remitimos al lector al capítulo II del libro de Simpson [8] para más información al respecto.

Teorema 2.80. *Los siguientes teoremas son demostrables en RCA$_0$.*

1. *(**El teorema del valor intermedio**) Si $\phi(x)$ es continua en el intervalo unidad $0 \leq x \leq 1$ y $\phi(0) < 0 < \phi(1)$, entonces existe x tal que $0 < x < 1$ y $\phi(x) = 0$.*

2. *(**El teorema de extensión de Tietze**) Sea X un espacio métrico completamente separable. Dado (el código de) un cerrado $C \subseteq X$ y (el código de) una función continua $f : C \to [-1, 1]$, es posible dar de manera efectiva (el código de) una función continua $g : X \to [-1, 1]$ tal que $f(x) = g(x)$ para todo $x \in C$.*

3. *(**Existencia del cierre algebraico de un cuerpo**) Todo cuerpo numerable K tiene un cierre algebraico.*

4. *(**Adecuación de la lógica de primer orden**) Si X es un conjunto de fórmulas cerradas y existe un modelo numerable M tal que $M(\sigma) = 1$ para toda $\sigma \in X$, entonces X es consistente.*

5. *(**Completitud débil de la lógica de primer orden**) Si X es un conjunto de fórmulas cerradas consistente y completo, entonces existe un modelo numerable M tal que $M(\sigma) = 1$ para toda $\sigma \in X$.*

Capítulo 3

$\mathbf{WKL}_0$

En este capítulo estudiaremos el segundo de los subsistemas de la aritmética de segundo orden que abordaremos en este trabajo, la teoría WKL_0 concida como Lema Débil de Köning (*Weak Köning Lemma*). Dicha teoría fue introducida por Friedman [1] y la principal motivación para su consideración fue precisamente una cuestión del programa de la Matemática Inversa: la existencia de importantes teoremas de la matemática del día a día cuya potencia lógica se situaba estrictamente entre la teoría base RCA_0 y la teoría dada por el esquema de Σ^0_1-comprensión ACA_0. De hecho, la posterior investigación en este campo ha puesto de manifiesto la relevancia de la teoría WKL_0 y muchos teoremas importantes de la matemática ordinaria han resultado ser exactamente equivalentes a este principio combinatorio (véase el final de capítulo para más información al respecto).

La teoría WKL_0 consiste en añadir a RCA_0 el lema débil de König como axioma. Dicho resultado habla sobre árboles binarios, así que lo primero será ver cómo se codifican los árboles en RCA_0.

Recordemos que $\mathbb{N}^{<\mathbb{N}}$ denota el conjunto de (los códigos de) sucesiones finitas. Además, variables numéricas del tipo σ, τ se supondrán que denotarán sucesiones finitas. Un árbol T será un conjunto de sucesiones finitas tal que cualquier segmento inicial de una sucesión finita $\sigma \in T$ también está en T. Una rama o camino de T será una función $f : \mathbb{N} \to \mathbb{N}$ tal que para todo $k \in \mathbb{N}$ se tiene el segmento inicial $f[k] = \langle f(0), f(1), \ldots, f(k-1)\rangle$ pertenece a T. Más formalmente:

Definición 3.1. (**Árboles y caminos**)

$$\textsc{Tree}[T] :\equiv T \subseteq \mathbb{N}^{<\mathbb{N}} \wedge \forall \sigma, \tau . \sigma \in \mathbb{N}^{<\mathbb{N}} \wedge \sigma \subseteq \tau \wedge \tau \in T \to \sigma \in T.$$

$$\textsc{Path}[p, T] :\equiv p : \mathbb{N} \longrightarrow \mathbb{N} \wedge \forall n . p[n] \in T.$$

■

Notación. Usaremos la notación $2^{<\mathbb{N}} :\equiv \{0,1\}^{<\mathbb{N}}$ y $2^{\mathbb{N}} :\equiv \{0,1\}^{\mathbb{N}}$. ■

Finalmente, WKL$_0$ será RCA$_0$ más el axioma que expresa que "todo árbol binario (i.e. $T \subseteq 2^{<\mathbb{N}}$) infinito tiene una rama". El concepto de árbol binario no debe confundirse con el de árbol 2-Ario, que quiere decir que todo nodo tiene a lo sumo 2 sucesores, pero que no tienen por qué ser 0 o 1 como en el caso del binario.

Definición 3.2. (**La teoría** WKL$_0$) Definimos el subsistema WKL$_0$ como:

$$\mathrm{WKL}_0 = \mathrm{RCA}_0 + \forall T.\textsc{Tree}(T) \wedge T \subseteq 2^{<\mathbb{N}} \wedge \textsc{InfSet}(T) \to \exists p.\textsc{Path}[p,T].$$

■

Como ya hemos mencionado, esta teoría desempeña un papel muy relevante para el estudio de la Matemática Inversa. Además, en el capítulo 6 de la presente memoria, veremos que también está estrechamente relacionada con el programa de Hilbert y los fundamentos de las Matemáticas.

3.1. Σ^0_1-SEP

En primer lugar veremos que WKL$_0$ es equivalente sobre RCA$_0$ al principio de Σ^0_1 separación, que introducimos justo a continuación.

Definición 3.3 (Γ**-separación**)**.** Sea $\Gamma \subseteq$ Form. Definimos el conjunto de axiomas de separación en Γ, denotado Γ-SEP, como el conjunto de las fórmulas:

$$(\neg\exists n.\varphi_0\{n\} \wedge \varphi_1\{n\}) \to \exists X \forall n.(\varphi_0\{n\} \to n \in X) \wedge (\varphi_1\{n\} \to n \notin X),$$

donde $n \in \mathrm{Var_N}$, $X \in \mathrm{Var_C}$ y $\varphi_0\{n\}, \varphi_1\{n\} \in \Gamma$ tal que $X \notin \mathrm{Vl}(\varphi_0\{n\}) \cup \mathrm{Vl}(\varphi_1\{n\})$. ■

Veamos la primera dirección de la mencionada equivalencia.

Lema 3.1. *WKL$_0 \vdash \Sigma^0_1$-SEP.*

Demostración:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de WKL$_0$ y $\varphi_0\{n\}, \varphi_1\{n\} \in \Sigma^0_1$ tal que $X \notin \mathrm{Vl}(\varphi_0\{n\}) \cup \mathrm{Vl}(\varphi_1\{n\})$. Sean $\{\nu_1, \ldots, \nu_r\} = (\mathrm{Vl}(\varphi_0\{n\}) \cup \mathrm{Vl}(\varphi_1\{n\})) \setminus \{n\}$

⟨1⟩2. Sea $\psi :\equiv (\neg\exists n.\varphi_0\{n\} \wedge \varphi_1\{n\}) \to \exists X \forall n.(\varphi_0\{n\} \to n \in X) \wedge (\varphi_1\{n\} \to n \notin X)$.

⟨1⟩3. $\mathrm{Vl}(\psi) = \{\nu_1, \ldots, \nu_r\}$.

Demostración: Por definición de variable libre.

⟨1⟩4. Sean $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r \in \mathbb{N} \cup \wp(\mathbb{N})$, denotamos $\varphi_0[n] :\equiv \varphi_0[n, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r]$ y $\varphi_1[n] :\equiv \varphi_1[n, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r]$. Entonces
$\boldsymbol{\psi} :\equiv \psi[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r] \equiv (\neg\exists n.\varphi_0[n] \wedge \varphi_1[n]) \to \exists X \forall n.(\varphi_0[n] \to n \in X) \wedge (\varphi_1[n] \to n \notin X)$
y es suficiente probar que $\mathfrak{M} \vDash \boldsymbol{\psi}$.

DEMOSTRACIÓN: La igualdad es por definición de sustitución y que sea suficiente es por el teorema de completitud.

⟨1⟩5. Supongamos que $\mathfrak{M} \vDash \neg\exists n.\varphi_0[n] \wedge \varphi_1[n]$.

⟨1⟩6. Para $i = 0, 1$ existen $\theta_i(m, n) \in (\Sigma^0_0)_{\mathfrak{M}}$ tales que $\varphi_i[n] \equiv \exists m.\theta_i(m, n)$.

DEMOSTRACIÓN: Por ⟨1⟩1 $\varphi_i\{n\} \in \Sigma^0_1$, por tanto $\varphi_i[n] \in (\Sigma^0_1)_{\mathfrak{M}}$, de donde se obtiene lo pedido.

⟨1⟩7. Existe $\mathbf{T} \in \wp(\mathbb{N})$ tal que
$\mathfrak{M} \vDash \mathbf{T} = \{t \mid t \in 2^{<\mathbb{N}} \wedge \forall m, n < \mathrm{lh}(t).(\theta_0(m, n) \to t(n) = 1) \wedge (\theta_1(m, n) \to t(n) = 0)\}$.

DEMOSTRACIÓN: Por Σ^0_0-COMP.

⟨1⟩8. $\mathfrak{M} \vDash \textsc{Tree}[\mathbf{T}]$.

DEMOSTRACIÓN: Trivial por la definición de TREE.

⟨1⟩9. $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{T}]$.

⟨2⟩1. $\mathfrak{M} \vDash \exists \tau \in 2^{<\mathbb{N}}.\, \mathrm{lh}(\tau) = 0 \wedge \tau \in \mathbf{T}$.

DEMOSTRACIÓN: Es claro que $\mathfrak{M} \vDash \langle\rangle \in \mathbf{T}$.

⟨2⟩2. $\mathfrak{M} \vDash \forall n.(\exists \tau \in 2^{<\mathbb{N}}.\, \mathrm{lh}(\tau) = n \wedge \tau \in \mathbf{T}) \to (\exists \tau \in 2^{<\mathbb{N}}.\, \mathrm{lh}(\tau) = n + 1 \wedge \tau \in \mathbf{T})$.

DEMOSTRACIÓN: Sean $\mathbf{n}, \boldsymbol{\tau} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathrm{lh}(\boldsymbol{\tau}) = \mathbf{n} \wedge \boldsymbol{\tau} \in \mathbf{T}$. Distingamos casos sobre si $\mathfrak{M} \vDash \varphi_i[\mathbf{n} + 1]$.
Si $\mathfrak{M} \nvDash \varphi_0[\mathbf{n} + 1]$ y $\mathfrak{M} \nvDash \varphi_1[\mathbf{n} + 1]$, entonces $\mathfrak{M} \vDash \boldsymbol{\tau}^\frown\langle 0\rangle \in \mathbf{T} \wedge \boldsymbol{\tau}^\frown\langle 1\rangle \in \mathbf{T}$.
Si $\mathfrak{M} \vDash \varphi_0[\mathbf{n} + 1]$ y $\mathfrak{M} \nvDash \varphi_1[\mathbf{n} + 1]$, entonces $\mathfrak{M} \vDash \boldsymbol{\tau}^\frown\langle 1\rangle \in \mathbf{T}$.
Si $\mathfrak{M} \nvDash \varphi_0[\mathbf{n} + 1]$ y $\mathfrak{M} \vDash \varphi_1[\mathbf{n} + 1]$, entonces $\mathfrak{M} \vDash \boldsymbol{\tau}^\frown\langle 0\rangle \in \mathbf{T}$.
El caso $\mathfrak{M} \vDash \varphi_0[\mathbf{n} + 1]$ y $\mathfrak{M} \vDash \varphi_1[\mathbf{n} + 1]$ es imposible por ⟨1⟩5.

⟨2⟩3. Q.E.D.

DEMOSTRACIÓN: Por Σ^0_1-IND aplicada a ⟨2⟩1 y ⟨2⟩2 tenemos que $\mathfrak{M} \vDash \forall n \exists \tau \in 2^{<\mathbb{N}}.\, \mathrm{lh}(\tau) = n \wedge \tau \in \mathbf{T}$, lo cual demuestra que $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{T}]$.

⟨1⟩10. Existe $\mathbf{g} : \mathbb{N} \longrightarrow \{0, 1\}$ tal que $\mathfrak{M} \vDash \textsc{Path}[\mathbf{g}, \mathbf{T}]$.

DEMOSTRACIÓN: Por el lema débil de König y ⟨1⟩8, ⟨1⟩9.

⟨1⟩11. Q.E.D.

DEMOSTRACIÓN: Por Σ^0_0-COMP existe $\mathbf{X} \in \wp(\mathbb{N})$ tal que
$$\mathfrak{M} \vDash \mathbf{X} = \{n \mid \mathbf{g}(n) = 1\}.$$
Es claro que tal $\mathbf{X}$ cumple lo pedido.

□

Y finalmente la otra dirección de la equivalencia.

Lema 3.2. *RCA$_0$ +Σ^0_1-SEP $\vdash$ WKL$_0$.*

⟨1⟩1. Sean $\mathfrak{M}$ un modelo de RCA$_0$ +Σ^0_1-SEP y $\mathbf{T} \in \wp(\mathbb{N})$ tal que
$$\mathfrak{M} \vDash \mathbf{T} \subseteq 2^{<\mathbb{N}} \wedge \textsc{Tree}[\mathbf{T}] \wedge \textsc{InfSet}[\mathbf{T}].$$

⟨1⟩2. Definimos
$$\theta[n,\sigma] :\equiv \exists \tau \in 2^{<\mathbb{N}}.\, \mathrm{lh}(\tau) = n \wedge \tau \in T \wedge \tau \supseteq \sigma.$$
$$\varphi[\sigma,i] :\equiv \exists n.\theta[n,\sigma^\frown\langle i\rangle] \wedge \neg\theta[n,\sigma^\frown\langle 1-i\rangle].$$

⟨1⟩3. $\varphi[\sigma,i] \in (\mathbf{\Sigma^0_1})^{\mathrm{RCA}_0}_{\mathfrak{M}}$.

⟨2⟩1. Definimos
$$\theta'[n,\sigma,c] :\equiv \exists \tau < c.\tau \in 2^{\mathbb{N}} \wedge \mathrm{lh}(\tau) = n \wedge \tau \in T \wedge \tau \supseteq \sigma.$$
$$\varphi'[\sigma,i] :\equiv \exists c,n.\theta'[n,\sigma^\frown\langle i\rangle,c] \wedge \neg\theta'[n,\sigma^\frown\langle 1-i\rangle,c].$$

⟨2⟩2. $\theta' \in (\mathbf{\Sigma^0_0})^{\mathrm{RCA}_0}_{\mathfrak{M}}$ y por tanto $\varphi' \in (\mathbf{\Sigma^0_1})^{\mathrm{RCA}_0}_{\mathfrak{M}}$.

⟨2⟩3. $\mathfrak{M} \vDash \varphi'[\sigma,i] \to \varphi[\sigma,i]$.

DEMOSTRACIÓN: Basta con olvidarse de la cota c.

⟨2⟩4. $\mathfrak{M} \vDash \varphi[\sigma,i] \to \varphi'[\sigma,i]$.

DEMOSTRACIÓN: Sean $\boldsymbol{\sigma}, \boldsymbol{i} \in \mathbb{N}$ arbitrarios y supongamos que $\mathfrak{M} \vDash \varphi[\boldsymbol{\sigma},\boldsymbol{i}]$. Sea entonces $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \theta[\mathbf{n},\boldsymbol{\sigma}^\frown\langle\mathbf{i}\rangle] \wedge \neg\theta[\mathbf{n},\boldsymbol{\sigma}^\frown\langle 1-\mathbf{i}\rangle]$. Como $\{0,1\}^{\mathbf{n}}$ es un conjunto finito sea $\mathbf{c} = \{0,1\}^{\mathbf{n}}$ (el código de dicho conjunto). Como pertenecer al conjunto finito implica ser menor que su código, tenemos que $\mathfrak{M} \vDash \theta'[\mathbf{n},\boldsymbol{\sigma}^\frown\langle\mathbf{i}\rangle,\mathbf{c}] \wedge \neg\theta'[\mathbf{n},\boldsymbol{\sigma}^\frown\langle 1-\mathbf{i}\rangle,\mathbf{c}]$ y así $\mathfrak{M} \vDash \varphi'[\boldsymbol{\sigma},\boldsymbol{i}]$.

⟨2⟩5. Q.E.D.

⟨1⟩4. $\mathfrak{M} \vDash \neg\exists\sigma.\varphi[\sigma,0] \wedge \varphi[\sigma,1]$.

DEMOSTRACIÓN: Trivial por la definición de φ.

⟨1⟩5. $\mathfrak{M} \vDash (\neg\exists\sigma.\varphi[\sigma,0] \wedge \varphi[\sigma,1]) \to \exists X\forall\sigma.(\varphi[\sigma,0] \to \sigma \in X) \wedge (\varphi[\sigma,1] \to \sigma \notin X)$.

DEMOSTRACIÓN: Por Σ^0_1-SEP.

⟨1⟩6. Existe $\mathbf{X}$ tal que $\mathfrak{M} \vDash \forall\sigma.(\varphi[\sigma,0] \to \sigma \in \mathbf{X}) \wedge (\varphi[\sigma,1] \to \sigma \notin \mathbf{X})$.

DEMOSTRACIÓN: Por ⟨1⟩4 y ⟨1⟩5.

⟨1⟩7. Existe $\langle \boldsymbol{\sigma}_k : k \in \mathbb{N}\rangle : \mathbb{N} \longrightarrow 2^{\mathbb{N}}$ tal que
$$\mathfrak{M} \vDash \boldsymbol{\sigma}_0 = \langle\rangle \wedge \forall n.(\boldsymbol{\sigma}_n \in \mathbf{X} \to \boldsymbol{\sigma}_{n+1} = \boldsymbol{\sigma}_n{}^\frown\langle 0\rangle) \wedge (\boldsymbol{\sigma}_n \notin \mathbf{X} \to \boldsymbol{\sigma}_{n+1} = \boldsymbol{\sigma}_n{}^\frown\langle 0\rangle).$$

DEMOSTRACIÓN: Por recursión primitiva.

⟨1⟩8. $\forall k,n.\boldsymbol{\sigma}_k \subseteq \boldsymbol{\sigma}_{k+n}$.

DEMOSTRACIÓN: Por Σ^0_0-IND en n.

⟨1⟩9. $\mathfrak{M} \vDash \forall k.\, \mathrm{lh}(\boldsymbol{\sigma}_k) = k$.

DEMOSTRACIÓN: Es una Σ^0_0-IND sencilla.

⟨1⟩10. $\mathfrak{M} \vDash \forall n \forall k \leq n. \theta[n, \boldsymbol{\sigma}_k]$.

⟨2⟩1. Sea $\mathbf{n} \in \mathbb{N}$, definimos

$$\psi[k] :\equiv \forall k \leq \mathbf{n}. \theta[\mathbf{n}, \boldsymbol{\sigma}_k].$$

⟨2⟩2. $\mathfrak{M} \vDash \psi[0]$.

DEMOSTRACIÓN: Basta ver que $\mathfrak{M} \vDash \theta[\mathbf{n}, \boldsymbol{\sigma}_0]$, lo cual es cierto ya que $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{T}]$.

⟨2⟩3. $\mathfrak{M} \vDash \forall k. \psi[k] \to \psi[k+1]$.

DEMOSTRACIÓN: Sea $\mathbf{k} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \psi[\mathbf{k}]$. Pordemos asumir que $\mathfrak{M} \vDash \mathbf{k} < \mathbf{n}$, ya que si no $\mathfrak{M} \vDash \mathbf{k} + 1 > \mathbf{n}$ y el resultado se sigue trivialmente. Como $\mathfrak{M} \vDash \theta[\mathbf{n}, \boldsymbol{\sigma}_\mathbf{k}]$ y $\mathfrak{M} \vDash \mathbf{k} < \mathbf{n}$ se tiene que $\mathfrak{M} \vDash \theta[\mathbf{n}, \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 0\rangle] \vee \theta[\mathbf{n}, \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 1\rangle]$, además si $\mathfrak{M} \vDash \theta[\mathbf{n}, \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 0\rangle] \wedge \theta[\mathbf{n}, \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 1\rangle]$ entonces es claro que $\mathfrak{M} \vDash \theta[\mathbf{n}, \boldsymbol{\sigma}_{\mathbf{k+1}}]$ pues $\mathfrak{M} \vDash \boldsymbol{\sigma}_{\mathbf{k+1}} = \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 0\rangle \vee \boldsymbol{\sigma}_{\mathbf{k+1}} = \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 1\rangle$. Si $\mathfrak{M} \vDash \neg\theta[\mathbf{n}, \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 0\rangle]$, entonces $\mathfrak{M} \vDash \theta[\mathbf{n}, \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 1\rangle]$, por tanto $\mathfrak{M} \vDash \varphi[\boldsymbol{\sigma}_\mathbf{k}, 1]$, y así $\mathfrak{M} \vDash \boldsymbol{\sigma}_\mathbf{k} \notin \mathbf{X}$. Eso quiere decir que $\mathfrak{M} \vDash \boldsymbol{\sigma}_{\mathbf{k}+1} = \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 1\rangle$, y por tanto $\mathfrak{M} \vDash \theta[\mathbf{n}, \boldsymbol{\sigma}_{\mathbf{k}+1}]$. El caso $\mathfrak{M} \vDash \neg\theta[\mathbf{n}, \boldsymbol{\sigma}_\mathbf{k}{}^\frown\langle 1\rangle]$ es análogo.

⟨2⟩4. Q.E.D.

DEMOSTRACIÓN: Por Σ^0_0-IND siendo ⟨2⟩2 el caso base y ⟨2⟩3 el paso inductivo.

⟨1⟩11. Q.E.D.

DEMOSTRACIÓN: Por Σ^0_0-COMP tenemos la existencia de un $\mathbf{f}$ tal que $\mathfrak{M} \vDash \forall i. \mathbf{f}(i) = \boldsymbol{\sigma}_{i+1}(i)$. Por ⟨1⟩8 y ⟨1⟩10 se tendrá que $\mathfrak{M} \vDash \textsc{Path}[\mathbf{f}, \mathbf{T}]$, como queríamos.

□

Finalmente lo unimos todo en un solo teorema.

Teorema 3.3. *En RCA_0 se demuestran equivalentes:*

1. *WKL_0.*
2. *Σ^0_1-SEP.*
3. *$\forall f, g : \mathbb{N} \longrightarrow \mathbb{N}. \textsc{Iny}[f] \wedge \textsc{Iny}[g] \wedge (\forall m, n. f(m) \neq g(n)) \to$ $\exists X \forall m. f(m) \in X \wedge g(m) \notin X$.*

DEMOSTRACIÓN: La equivalencia de 1. y 2. se tiene por los lemas 3.1 y 3.2. La de 2. y 3. se obtiene fácilmente por el lema 2.58. □

La anterior equivalencia es una reformulación muy útil para trabajar con WKL$_0$. Además, también nos servirá más adelante, cuando veamos la relación del programa de Hilbert con WKL$_0$.

3.2. Heine-Borel en $[0,1]$

En esta sección damos con detalle la prueba de un resultado típico de la matemática inversa de WKL$_0$: la teoría WKL$_0$ es equivalente al teorema de Heine-Borel para $[0,1] \subseteq \mathbb{R}$ sobre RCA$_0$. Esto es, al principio que declara que todo recubrimiento de $[0,1]$ por abiertos básicos tiene un subrecubrimiento finito.

Lo primero es demostrar algunos lemas auxiliares en RCA$_0$. En particular, vamos a probar que sobre las sucesiones finitas (que no necesariamente son sucesiones finitas en la metateoría ZFC) se puede iterar una función binaria.

Lema 3.4.

$$RCA_0 \vdash \forall g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \forall n_0 \exists^1 f : \mathbb{N}^{<\mathbb{N}} \longrightarrow \mathbb{N}.$$

$$f(\langle\rangle) = n_0 \wedge \forall s \in \mathbb{N}^{<\mathbb{N}} \forall n. f(s^\frown\langle n\rangle) = g(f(s), n).$$

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA$_0$ y $\mathbf{g} \in \wp(\mathbb{N}), \mathbf{n}_0 \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{g} : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.

⟨1⟩2. Existencia

⟨2⟩1. Existe $\mathbf{h} \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \mathbf{h} : \mathbb{N} \times \mathbb{N}^{<\mathbb{N}} \longrightarrow \mathbb{N} \wedge (\forall s \in \mathbb{N}^{<\mathbb{N}}. \mathbf{h}(0, s) = \mathbf{n}_0) \wedge$$
$$(\forall s \in \mathbb{N}^{<\mathbb{N}} \forall i. (i < \mathrm{lh}(s) \to \mathbf{h}(i{+}1, s) = \mathbf{g}(\mathbf{h}(i, s), s(i))) \wedge (i \geq \mathrm{lh}(s) \to \mathbf{h}(i{+}1, s) = 0)).$$

Demostración: Existen los conjuntos $\mathbf{h}_0, \mathbf{h}_1 \in \wp(\mathbb{N})$ tales que

$$\mathfrak{M} \vDash \mathbf{h}_0 : \mathbb{N} \longrightarrow \mathbb{N} \wedge \forall s. \mathbf{h}(s) = \mathbf{n}_0.$$
$$\mathfrak{M} \vDash \mathbf{h}_1 : \mathbb{N}^3 \longrightarrow \mathbb{N} \wedge \forall acum, i, s. (s \notin \mathbb{N}^{<\mathbb{N}} \vee i \geq \mathrm{lh}(s) \to \mathbf{h}_1(acum, i, s) = 0) \wedge$$
$$(s \in \mathbb{N}^{<\mathbb{N}} \wedge i < \mathrm{lh}(s) \to \mathbf{h}_1(acum, i, s) = \mathbf{g}(acum, s(i))).$$

Ambas funciones se definen por Σ^0_0-COMP. La recursión primitiva nos da la existencia de una función $\mathbf{h}' : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, la restricción de esa función a $\mathbb{N} \times \mathbb{N}^{<\mathbb{N}}$ es la función buscada.

⟨2⟩2. $\mathfrak{M} \vDash \forall n \forall s \in \mathbb{N}^{<\mathbb{N}}. \mathbf{h}(\mathrm{lh}(s), s^\frown\langle n\rangle) = \mathbf{h}(\mathrm{lh}(s), s)$.

Demostración: Gracias a Π^0_1-IND se obtiene que

$$\mathfrak{M} \vDash \forall k \forall n \forall s \in \mathbb{N}^{<\mathbb{N}}. \mathrm{lh}(s) = k \to \mathbf{h}(\mathrm{lh}(s), s^\frown\langle n\rangle) = \mathbf{h}(\mathrm{lh}(s), s).$$

El resultado es consecuencia de esto.

⟨2⟩3. Q.E.D.

DEMOSTRACIÓN: Finalmente, por composición de funciones, existe la función $\mathbf{f} : \mathbb{N}^{<\mathbb{N}} \longrightarrow \mathbb{N}$ tal que

$$\mathfrak{M} \vDash \mathbf{f} = \mathbf{h} \circ (\mathrm{lh} \times \mathrm{id}) \circ (\mathrm{diag} \restriction \mathbb{N}^{<\mathbb{N}}).$$

Se comprueba sin dificultad que cumple las propiedades, usando $\langle 2 \rangle 2$.

$\langle 1 \rangle 3$. Unicidad

DEMOSTRACIÓN: Sean $\mathbf{f}_1, \mathbf{f}_2 : \mathbb{N}^{<\mathbb{N}} \longrightarrow \mathbb{N}$ que cumplen lo pedido. Por Π^0_1-IND se cumple que:

$$\mathfrak{M} \vDash \forall k \forall s \in \mathbb{N}^{<\mathbb{N}}. \mathrm{lh}(s) = k \to \mathbf{f}_1(s) = \mathbf{f}_2(s).$$

Por tanto se tiene la unicidad.

□

Como corolario, podemos particularizar un poco los conjuntos donde se hacen las definiciones.

Corolario 3.5.

$$RCA_0 \vdash \forall X, Y \forall g : Y \times X \longrightarrow Y \forall y_0 \in Y \exists^1 f : X^{<\mathbb{N}} \longrightarrow Y.$$

$$f(\langle\rangle) = y_0 \wedge \forall s \in X^{<\mathbb{N}} \forall n \in X. f(s^\frown\langle n\rangle) = g(f(s), n).$$

DEMOSTRACIÓN: La idea es extender la función $\mathbf{g}$ a todo $\mathbb{N} \times \mathbb{N}$, dándole el valor 0 a los elementos fuera de $\mathbf{Y} \times \mathbf{X}$. Entonces usamos el lema anterior para probar la existencia de un $\mathbf{f}' : \mathbb{N}^{<\mathbb{N}} \longrightarrow \mathbb{N}$ y ese lo restringimos a $\mathbf{X}^{<\mathbb{N}}$. □

Finalmente con este resultado podemos definir la suma de una sucesión finita de racionales y el mínimo de una sucesión finita de racionales (y, por tanto, de un conjunto finito de racionales, ya que como vimos anteriormente todo conjunto finito tiene una sucesión finita que lo enumera).

Corolario 3.6.

$$RCA_0 \vdash \exists^1 f : \mathbb{Q}^{<\mathbb{N}} \longrightarrow \mathbb{Q}. f(\langle\rangle) =_{\mathbb{Q}} 0 \wedge \forall s \in \mathbb{Q}^{<\mathbb{N}} \forall q \in \mathbb{Q}. f(s^\frown\langle q\rangle) =_{\mathbb{Q}} f(s) +_{\mathbb{Q}} q.$$

A esta función la llamaremos $\sum_{\mathbb{Q}}$.

Notación. Dada $\langle p_i : i < k\rangle \in \mathbb{Q}^{<\mathbb{N}}$ será habitual denotar

$$\sum_{\mathbb{Q}}(\langle p_i : i < k\rangle) :\equiv \sum_{i<k} p_i.$$

Se entenderá que hablamos de suma de racionales por ser la sucesión de racionales. ■

Corolario 3.7.

$RCA_0 \vdash \exists^1 f : \mathbb{Q}^{<\mathbb{N}} \setminus \{\langle\rangle\} \longrightarrow \mathbb{Q}.(\forall q \in \mathbb{Q}.f(\langle q\rangle) =_{\mathbb{Q}} q) \wedge \forall s \in \mathbb{Q}^{<\mathbb{N}} \forall q \in \mathbb{Q}.f(s^\frown\langle q\rangle) =_{\mathbb{Q}} \min_{\mathbb{Q}}(f(s), q)$.

A esa función la llamamos $\min_{\mathbb{Q}}$.

Demostración: Gracias al colorario 3.5, fijado $\mathbf{q} \in \mathbb{Q}$ podemos definir $\min_{\mathbb{Q}}(\mathbf{q}, s)$ que dada la sucesión vacía devuelve $\mathbf{q}$ y si la sucesión no es vacía itera la función mínimo. Claramente dada $\mathbf{s} \in \mathbb{Q}^{<\mathbb{N}}$ no vacía tenemos que $\min_{\mathbb{Q}}(\mathbf{s}(0), \mathbf{s})$ es el mínimo de la sucesión. Esto justifica que el siguiente conjunto, que existe por Σ^0_0-COMP,

$\mathbf{f} = \{(s, n) \mid s \in \mathbb{Q}^{<\mathbb{N}} \wedge s \neq \langle\rangle \wedge (\exists i < \mathrm{lh}(s).s(i) = n) \wedge (\forall i < \mathrm{lh}(s).n \leq_{\mathbb{Q}} s(i)\}$,

define una función. □

Corolario 3.8. $RCA_0 \vdash \forall s \in \mathbb{Q}^{<\mathbb{N}} \forall i < \mathrm{lh}(s).\, \min_{\mathbb{Q}}(s) \leq s(i)$.

Demostración: Por Π^0_1-IND en la longitud de s. □

Los corolarios anteriores se pueden reproducir de manera análoga para obtener la función $\max_{\mathbb{Q}}$, que aplicada a una sucesión finita de racionales nos devuelva su máximo.

Ahora definimos la codificación del teorema Heine-Borel $[0, 1]$ en RCA_0. También introducimos una versión para el caso cuando los intervalos del recubrimiento son racionales, pues nos servirá luego en la demostración.

Definición 3.4 (**Heine-Borel**)**.** Definimos:

$$\text{Heine-Borel} :\equiv \forall\langle c_i : i \in \mathbb{N}\rangle, \langle d_i : i \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}.(\forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to \exists i.c_i <_{\mathbb{R}} x <_{\mathbb{R}} d_i) \to$$
$$\exists n \forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to \exists i \leq n.c_i <_{\mathbb{R}} x <_{\mathbb{R}} d_i.$$

$$\text{Heine-Borel}\mathbb{Q} :\equiv \forall\langle c_i : i \in \mathbb{N}\rangle, \langle d_i : i \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}.(\forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to \exists i.c_i <_{\mathbb{R}} x <_{\mathbb{R}} d_i) \to$$
$$\exists n \forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to \exists i \leq n.c_i <_{\mathbb{R}} x <_{\mathbb{R}} d_i.$$

■

Veamos en primer lugar una prueba del hecho de que WKL_0 demuestra Heine-Borel. El truco va a ser probarlo primero para el caso en el que los intervalos son de extremos racionales, para así poder manejarlos mejor (recordemos que los racionales son números, mientras que los reales son conjuntos). Después se observa que, gracias a la densidad de $\mathbb{Q}$ en $\mathbb{R}$, basta con el caso racional para probar el real.

Lema 3.9. *$WKL_0 \vdash$ Heine-Borel.*

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de WKL_0.

⟨1⟩2. $\mathfrak{M} \vDash$ Heine-Borel$\mathbb{Q}$.

⟨2⟩1. Sean $\langle \mathbf{c}_i : i \in \mathbb{N}\rangle, \langle \mathbf{d}_i : i \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}$ cualesquiera tal que
$$\mathfrak{M} \vDash \forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to \exists i.\mathbf{c}_i <_{\mathbb{R}} x <_{\mathbb{R}} \mathbf{d}_i.$$

⟨2⟩2. Existen funciones $\mathbf{a}_s, \mathbf{b}_s : 2^{<\mathbb{N}} \longrightarrow \mathbb{Q}$ tales que:
$$\mathbf{a}_s = \sum_{i<\mathrm{lh}(s)} \frac{s(i)}{2^{i+1}}.$$
$$\mathbf{b}_s = \mathbf{a}_s +_{\mathbb{Q}} \frac{1}{2^{\mathrm{lh}(s)}}.$$
Intuitivamente le estamos asignando a cada s un intervalo $(\mathbf{a}_s, \mathbf{b}_s)$ tal que (como veremos en el siguiente paso) tomando todos los s de una misma longitud, obtenemos intervalos de la misma longitud que recubren $[0,1]$ y, además, al terminar un intervalo comienza otro.

⟨2⟩3. $\mathfrak{M} \vDash \forall x \in \mathbb{R}.(0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1) \to \forall n \exists s \in \{0,1\}^n.\mathbf{a}_s \leq_{\mathbb{R}} x \leq_{\mathbb{R}} \mathbf{b}_s$.

⟨3⟩1. Existe $\mathbf{sig} \in \wp(\mathbb{N})$ tal que
$\mathfrak{M} \vDash \mathbf{sig} : 2^{<\mathbb{N}} \longrightarrow 2^{<\mathbb{N}} \wedge \mathbf{sig}(\langle\rangle) = \langle\rangle \wedge \mathbf{sig}(s^\frown\langle 0\rangle) = s^\frown\langle 1\rangle \wedge \mathbf{sig}(s^\frown\langle 1\rangle) = \mathbf{sig}(s)^\frown\langle 0\rangle$.
Es decir, si vemos cada $\mathbf{s}$ como el intervalo $(\mathbf{a_s}, \mathbf{b_s})$, $\mathbf{sig}(\mathbf{s})$ nos dará el intervalo de la misma longitud que empieza donde acaba s, volviendo al primero si s es el intervalo más a la derecha.
Demostración: Por recursión primitiva.

⟨3⟩2. $\mathfrak{M} \vDash \forall n \forall s \in \{0,1\}^n.\mathbf{sig}(s) \in \{0,1\}^n$.
Demostración: Por Π^0_1-IND.

⟨3⟩3. $\mathfrak{M} \vDash \forall n \forall s \in \{0,1\}^n.\mathbf{b}_s \neq_{\mathbb{Q}} 1 \to \mathbf{b}_s = \mathbf{a}_{\mathbf{sig}(s)}$ (i.e. el siguiente empieza donde acaba el anterior, siempre que no estemos en el último).
Demostración: Se obtiene por Π^0_1-IND en n. En el paso inductivo, cuando estemos con $\mathbf{s}^\frown\langle 1\rangle$ será necesario usar que $\mathfrak{M} \vDash \forall s.\mathbf{a}_s = \mathbf{a}_{s^\frown\langle 0\rangle} \wedge \mathbf{b}_s = \mathbf{b}_{s^\frown\langle 1\rangle}$, lo cual se deduce directamente de la definición.

⟨3⟩4. Sea $\mathbf{x} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{x} \in \mathbb{R} \wedge 0 \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} 1$ y $\mathbf{n} \in \mathbb{N}$.

⟨3⟩5. $\mathfrak{M} \vDash$ FinSet$[\{0,1\}^{\mathbf{n}}]$, sea $\mathbf{k}$ su cota superior.
Demostración: Por lema 2.52.

⟨3⟩6. Existe $\mathbf{Y} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{Y} = \{s \mid s \in \{0,1\}^{\mathbf{n}} \wedge \mathbf{a}_s \leq_{\mathbb{R}} \mathbf{x}\} \neq \varnothing$.
Demostración: Por Σ^0_1-BCOMP, se tiene la existencia de
$$\mathfrak{M} \vDash \mathbf{Z} = \{s \mid s < \mathbf{k} \wedge s \in \{0,1\}^{\mathbf{n}} \wedge \mathbf{a}_s >_{\mathbb{R}} \mathbf{x}\}$$
y entonces por Σ^0_0-COMP existe $\mathbf{Y}$ tal que
$$\mathfrak{M} \vDash \mathbf{Y} = \{0,1\}^{\mathbf{n}} \setminus \mathbf{Z}.$$
Es fácil ver que ese $\mathbf{Y}$ es el buscado y que gracias la hipótesis de ⟨3⟩4
$\mathfrak{M} \vDash \langle 0, \ldots, 0\rangle \in \mathbf{Y}$.

⟨3⟩7. Existe $\mathbf{s} \in \mathbf{Y}$ tal que $\mathfrak{M} \vDash \forall s' \in \mathbf{Y}.\mathbf{a}'_s \leq_{\mathbb{Q}} \mathbf{a_s}$.

DEMOSTRACIÓN: Como $\mathfrak{M} \vDash \mathbf{Y} \subseteq \{0,1\}^{\mathbf{n}}$ y este último es finito, tenemos que $\mathbf{Y}$ también lo será, así que por el corolario 2.56 tendremos una sucesión finita con todos sus elementos. Por ser finita, tenemos que existe $\mathbf{s}$ tal que $\mathbf{a_s}$ sea el máximo de la sucesión.

⟨3⟩8. Q.E.D.

DEMOSTRACIÓN: Veamos que $\mathfrak{M} \vDash \mathbf{a_s} \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathbf{b_s}$. Por ⟨3⟩7 se tiene que $\mathfrak{M} \vDash \mathbf{a_s} \leq_{\mathbb{R}} \mathbf{x}$. Supongamos que $\mathfrak{M} \vDash \mathbf{b_s} <_{\mathbb{R}} \mathbf{x}$, entonces por ⟨3⟩4 se tiene que $\mathfrak{M} \vDash \mathbf{b_s} \neq_{\mathbb{R}} 1$ y por tanto por ⟨3⟩3 $\mathfrak{M} \vDash \mathbf{b_s} = \mathbf{a_{sig(s)}}$. Pero entonces $\mathfrak{M} \vDash \mathbf{a_{sig(s)}} = \mathbf{b_s} \leq_{\mathbb{R}} \mathbf{x}$ y por ⟨3⟩2 $\mathfrak{M} \vDash \mathbf{sig}(\mathbf{s}) \in \{0,1\}^{\mathbf{n}}$, por tanto $\mathfrak{M} \vDash \mathbf{sig}(\mathbf{s}) \in \mathbf{Y}$. Así $\mathfrak{M} \vDash \mathbf{a_{sig(s)}} = \mathbf{b_s} >_{\mathbb{Q}} \mathbf{a_s}$, absurdo por ⟨3⟩7.

⟨2⟩4. Existe $\mathbf{T} \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \forall s.s \in \mathbf{T} \leftrightarrow (s \in 2^{<\mathbb{N}} \wedge \neg\exists i \leq \mathrm{lh}(s).\mathbf{c}_i <_{\mathbb{Q}} \mathbf{a}_s <_{\mathbb{Q}} \mathbf{b}_s <_{\mathbb{Q}} \mathbf{d}_i),$$

y además $\mathfrak{M} \vDash \mathbf{T} \subseteq 2^{<\mathbb{N}} \wedge \textsc{Tree}[\mathbf{T}]$.

DEMOSTRACIÓN: La existencia se tiene por Σ^0_0-COMP y las propiedades salen directamente de su definición.

⟨2⟩5. $\mathfrak{M} \vDash \neg\exists p.\textsc{Path}[p, \mathbf{T}]$.

⟨3⟩1. Supongamos lo contrario, sea $\mathbf{f} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \textsc{Path}[\mathbf{f}, \mathbf{T}]$.

⟨3⟩2. Sabemos que existe $\mathbf{x} \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \mathbf{x} \in \mathbb{R} \wedge \mathbf{x} =_{\mathbb{R}} \lim_n \mathbf{a_{f}}_{[n]} =_{\mathbb{R}} \lim_n \mathbf{b_{f}}_{[n]} \wedge \forall n.\mathbf{a_{f}}_{[n]} \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathbf{b_{f}}_{[n]}.$$

DEMOSTRACIÓN: Por la completitud de intervalos encajados (i.e. el teorema 2.76).

⟨3⟩3. Existe $\mathbf{i} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{c_i} <_{\mathbb{R}} \mathbf{x} <_{\mathbb{R}} \mathbf{d_i}$.

DEMOSTRACIÓN: Por el paso ⟨2⟩1.

⟨3⟩4. Existe $\mathbf{n}$ tal que $\mathfrak{M} \vDash \mathbf{c_i} <_{\mathbb{Q}} \mathbf{a_{f[n]}} <_{\mathbb{Q}} \mathbf{b_{f[n]}} <_{\mathbb{Q}} \mathbf{d_i}$.

DEMOSTRACIÓN: Por ⟨3⟩2 sabemos que $\mathfrak{M} \vDash \mathbf{x} = \lim_n \mathbf{a_{f}}_{[n]} = \lim_n \mathbf{b_{f}}_{[n]}$, así que podemos buscar un intervalo tan cercano como se quiera.

⟨3⟩5. Q.E.D.

DEMOSTRACIÓN: Por ⟨3⟩4 llegamos a un absurdo, pues $\mathfrak{M} \vDash \mathbf{f}[\mathbf{n}] \notin \mathbf{T}$, pero por ⟨3⟩1 se tiene que $\mathfrak{M} \vDash \textsc{Path}[\mathbf{f}, \mathbf{T}]$.

⟨2⟩6. $\mathfrak{M} \vDash \textsc{Finite}[\mathbf{T}]$.

DEMOSTRACIÓN: Usando ⟨2⟩4, ⟨2⟩5 y el lema débil de König.

⟨2⟩7. Existe $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall s \in \mathbf{T}.\,\mathrm{lh}(s) < \mathbf{n}$.

DEMOSTRACIÓN: Por ⟨2⟩6 existe un $\mathbf{l}$ tal que $\mathfrak{M} \vDash \forall s \in \mathbf{T}.s \leq \mathbf{l}$, como $\mathfrak{M} \vDash \forall s \in \mathbb{N}^{<\mathbb{N}}.\,\mathrm{lh}(s) \leq s$, obtenemos lo pedido.

⟨2⟩8. Q.E.D.

DEMOSTRACIÓN: Por ⟨2⟩7 tenemos que ninguna rama de longitud $\mathbf{n}$ pertenecerá a $\mathbf{T}$, por tanto $\mathfrak{M} \vDash \forall s \in 2^{<\mathbb{N}}.\,\mathrm{lh}(s) = \mathbf{n} \rightarrow \exists i \leq \mathbf{n}.\mathbf{c}_i <_{\mathbb{Q}} \mathbf{a}_s <_{\mathbb{Q}} \mathbf{b}_s <_{\mathbb{Q}} \mathbf{d}_i$. Ahora

dado $\mathbf{x}$ tal que $\mathfrak{M} \vDash 0 \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} 1$, por $\langle 2\rangle 3$ tenemos que existe $\mathbf{s} \in 2^{<\mathbb{N}}$ tal que $\mathfrak{M} \vDash \mathrm{lh}(\mathbf{s}) = \mathbf{n} \wedge \mathbf{a_s} \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathbf{b_s}$, por tanto juntado con lo anterior tenemos que $\mathfrak{M} \vDash \exists i \leq \mathbf{n}.\mathbf{c}_i <_{\mathbb{R}} \mathbf{x} <_{\mathbb{R}} \mathbf{d}_i$, como queríamos.

$\langle 1\rangle 3$. Sean $\langle \mathbf{c}_i : i \in \mathbb{N}\rangle, \langle \mathbf{d}_i : i \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}$ cualesquiera tal que
$$\mathfrak{M} \vDash \forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to \exists i.\mathbf{c}_i <_{\mathbb{R}} x <_{\mathbb{R}} \mathbf{d}_i.$$

$\langle 1\rangle 4$. Definimos la fórmula $\varphi[q,r] :\equiv q \in \mathbb{Q} \wedge r \in \mathbb{Q} \wedge \exists i.\mathbf{c}_i <_{\mathbb{R}} q <_{\mathbb{R}} r <_{\mathbb{R}} \mathbf{d}_i$.

$\langle 1\rangle 5$. Existe una función $\mathbf{f} : \mathbb{N} \longrightarrow \mathbb{Q} \times \mathbb{Q}$ tal que
$$\mathfrak{M} \vDash \forall q, r.\varphi[q,r] \leftrightarrow \exists j.\mathbf{f}(j) = (q,r).$$

$\langle 2\rangle 1$. Supongamos que existe $\mathbf{X}$ tal que $\mathfrak{M} \vDash \textsc{FinSet}[\mathbf{X}]$ y
$$\mathfrak{M} \vDash \forall n.n \in \mathbf{X} \leftrightarrow (\exists q, r \leq n.n = (q,r) \wedge \varphi[q,r]).$$

$\langle 2\rangle 2$. Existe $\mathbf{q} \in \mathbb{Q}$ tal que $\mathfrak{M} \vDash \exists r.(\mathbf{q},r) \in \mathbf{X} \wedge \neg\exists q' <_{\mathbb{Q}} \mathbf{q} \exists r.(q',r) \in \mathbf{X}$.

Demostración: Por ser $\mathbf{X}$ finito y gracias al lema 2.56, sabemos que existe una sucesión finita que enumera sus elementos, luego nos quedamos con las primeras coordenadas de esa sucesión y despúes tomamos el mínimo (en $\mathbb{Q}$) de la sucesión.

$\langle 2\rangle 3$. $\mathfrak{M} \vDash \neg\exists X.\textsc{FinSet}[X] \wedge X = \{(q,r) \mid q \in \mathbb{Q} \wedge r \in \mathbb{Q} \wedge \varphi[q,r]\}$.

Demostración: Por $\langle 2\rangle 2$ sea $\mathbf{r} \in \mathbb{Q}$ y $\mathbf{i} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{c_i} <_{\mathbb{R}} \mathbf{q} <_{\mathbb{R}} \mathbf{r} <_{\mathbb{R}} \mathbf{d_i}$. Como $\mathfrak{M} \vDash \mathbf{c_i} <_{\mathbb{R}} \mathbf{q}$, sabemos que tiene que existir $\mathbf{q'} \in \mathbb{Q}$ tal que $\mathfrak{M} \vDash \mathbf{c_i} <_{\mathbb{R}} \mathbf{q'} <_{\mathbb{R}} \mathbf{q}$, por tanto $\mathfrak{M} \vDash \mathbf{q'} \in \mathbf{X}$ y $\mathfrak{M} \vDash \mathbf{q'} <_{\mathbb{Q}} \mathbf{q}$, absurdo. Como suponiendo $\langle 2\rangle 1$ hemos llegado a un absurdo, podemos concluir lo contrario.

$\langle 2\rangle 4$. Q.E.D.

Demostración: Aplicando el lema 2.58 ya que $\exists q, r \leq n.n = (q,r) \wedge \varphi[q,r]$ es equivalente a fórmula en Σ^0_1.

$\langle 1\rangle 6$. Q.E.D.

Demostración: Podemos aplicar Heine-Borel$\mathbb{Q}$ (probado en $\langle 1\rangle 2$) a las sucesiones $\langle \mathbf{q}_i : i \in \mathbb{N}\rangle, \langle \mathbf{r}_i : i \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}$. Eso nos da un $\mathbf{n} \in \mathbb{N}$ tal que
$$\mathfrak{M} \vDash \forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to \exists i \leq \mathbb{N}.\mathbf{q}_i <_{\mathbb{R}} x <_{\mathbb{R}} \mathbf{r}_i.$$
Por $\langle 1\rangle 5$ eso nos da que
$$\mathfrak{M} \vDash \forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to \exists i \leq \mathbb{N}.\mathbf{c}_i <_{\mathbb{R}} x <_{\mathbb{R}} \mathbf{f}_i$$
(ya que $(\mathbf{c}_i, \mathbf{d}_i)$ contiene a $(\mathbf{q}_i, \mathbf{r}_i)$).

□

Para probar la otra dirección, y así la equivalencia, utilizaremos el conjunto de Cantor $C \subseteq [0,1]$. Empezamos definiendo una función que asocia una sucesión de $\{0,1\}^n$ a los extremos izquierdo y derecho de un intervalo del conjunto de Cantor en su n-ésima iteración.

Definición 3.5. RCA_0 demuestra la existencia de funciones $\mathrm{LC}, \mathrm{RC} : 2^{<\mathbb{N}} \longrightarrow \mathbb{Q}$ tales que

$$\mathrm{LC}(s) = \sum_{i<\mathrm{lh}(s)} \frac{2s(i)}{3^{i+1}}.$$

$$\mathrm{RC}(s) = \mathrm{LC}(s) +_{\mathbb{Q}} \frac{1}{3^{\mathrm{lh}(s)}}.$$

■

Veamos un par de propiedades importantes de las funciones LC y RC.

Lema 3.10. *$RCA_0 \vdash \forall t \in 2^{<\mathbb{N}} \forall s \subseteq t.\, \mathrm{LC}(s) \leq_{\mathbb{Q}} \mathrm{LC}(t) \leq_{\mathbb{Q}} \mathrm{RC}(t) \leq_{\mathbb{Q}} \mathrm{RC}(s)$.*

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{s} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{s} \in 2^{\mathbb{N}}$.

⟨1⟩2. $\forall t \in 2^{\mathbb{N}}.\, \mathrm{LC}(t) \leq_{\mathbb{Q}} \mathrm{RC}(t)$.

Demostración: Trivial por definición.

⟨1⟩3. Definimos
$$\varphi[n] :\equiv \forall t \in 2^{\mathbb{N}}.\, \mathrm{lh}(t) = n \wedge \mathbf{s} \subseteq t \to \mathrm{LC}(\mathbf{s}) \leq_{\mathbb{Q}} \mathrm{LC}(t) \wedge \mathrm{RC}(t) \leq_{\mathbb{Q}} \mathrm{RC}(\mathbf{s}).$$

⟨1⟩4. $\mathfrak{M} \vDash \varphi[0]$.

Demostración: Sea $\mathbf{t} \in 2^{\mathbb{N}}$ tal que $\mathfrak{M} \vDash \mathrm{lh}(\mathbf{t}) = 0 \wedge \mathbf{s} \subseteq \mathbf{t}$, por tanto $\mathfrak{M} \vDash \mathbf{s} = \mathbf{t} = \langle\rangle$ y el resultado se sigue trivialmente.

⟨1⟩5. $\mathfrak{M} \vDash \forall n.\varphi[n] \to \varphi[n+1]$.

⟨2⟩1. Sea $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \varphi[\mathbf{n}]$.

⟨2⟩2. Sea $\mathbf{t} \in 2^{\mathbb{N}}$ tal que $\mathfrak{M} \vDash \mathrm{lh}(\mathbf{t}) = \mathbf{n} + 1 \wedge \mathbf{s} \subseteq \mathbf{t}$.

⟨2⟩3. Existen $\mathbf{t}_0 \in 2^{\mathbb{N}}, \mathbf{i} \in \{0, 1\}$ tal que $\mathfrak{M} \vDash \mathbf{t} = \mathbf{t}_0 {}^\frown \langle \mathbf{i} \rangle$.

Demostración: Ya que $\mathfrak{M} \vDash \mathrm{lh}(\mathbf{t}) \neq 0$.

⟨2⟩4. Podemos suponer que $\mathfrak{M} \vDash \mathbf{s} \subseteq \mathbf{t}_0$.

Demostración: En caso contrario $\mathfrak{M} \vDash \mathbf{s} = \mathbf{t}$ y se tendría el resultado trivialmente.

⟨2⟩5. $\mathfrak{M} \vDash \mathrm{LC}(\mathbf{s}) \leq_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}_0) \wedge \mathrm{RC}(\mathbf{t}_0) \leq_{\mathbb{Q}} \mathrm{RC}(\mathbf{s})$.

Demostración: Ya que como $\mathfrak{M} \vDash \mathbf{s} \subseteq \mathbf{t}_0$ por ⟨2⟩5 y $\mathfrak{M} \vDash \mathbf{t}_0 = \mathbf{n}$ podemos aplicar $\mathfrak{M} \vDash \varphi[\mathbf{n}]$ para obtener lo pedido.

⟨2⟩6. $\mathfrak{M} \vDash \mathrm{LC}(\mathbf{s}) \leq_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}_0 {}^\frown \langle 0 \rangle) \wedge \mathrm{RC}(\mathbf{t}_0 {}^\frown \langle 0 \rangle) \leq_{\mathbb{Q}} \mathrm{RC}(\mathbf{s})$.

Demostración: Usando ⟨2⟩5 tenemos que
$$\mathfrak{M} \vDash \mathrm{LC}(\mathbf{s}) \leq_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}_0) =_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}_0 {}^\frown \langle 0 \rangle).$$

Y también

$$\mathfrak{M} \vDash \mathrm{RC}(\mathbf{t}_0{}^\frown\langle 0\rangle) =_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}_0{}^\frown\langle 0\rangle) +_{\mathbb{Q}} \frac{1}{3^{\mathbf{n}+1}} =_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}_0) +_{\mathbb{Q}} \frac{1}{3^{\mathbf{n}+1}} \leq_{\mathbb{Q}}$$
$$\mathrm{LC}(\mathbf{t}_0) +_{\mathbb{Q}} \frac{1}{3^{\mathbf{n}}} =_{\mathbb{Q}} \mathrm{RC}(\mathbf{t}_0) \leq_{\mathbb{Q}} \mathrm{RC}(\mathbf{s}).$$

$\langle 2\rangle 7$. $\mathfrak{M} \vDash \mathrm{LC}(\mathbf{s}) \leq_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}_0{}^\frown\langle 1\rangle) \wedge \mathrm{RC}(\mathbf{t}_0{}^\frown\langle 1\rangle) \leq_{\mathbb{Q}} \mathrm{RC}(\mathbf{s})$.

DEMOSTRACIÓN: Análogo a $\langle 2\rangle 6$.

$\langle 2\rangle 8$. Q.E.D.

DEMOSTRACIÓN: Distinguiendo casos sobre el valor de $\mathbf{i}$ y gracias a $\langle 2\rangle 6$ y $\langle 2\rangle 7$.

$\langle 1\rangle 6$. Q.E.D.

DEMOSTRACIÓN: Por Π^0_1-IND en $\varphi[n]$, siendo $\langle 1\rangle 4$ el caso base y $\langle 1\rangle 5$ el paso inductivo, obtenemos que $\mathfrak{M} \vDash \forall n.\varphi[n]$. Sea $\mathbf{s} \in 2^{\mathbb{N}}$ cualquiera tal que $\mathfrak{M} \vDash \mathbf{s} \subseteq \mathbf{t}$, como $\mathfrak{M} \vDash \varphi[\mathrm{lh}(\mathbf{s})]$ se cumple lo pedido.

□

Lema 3.11. *$RCA_0 \vdash \forall s,t \in 2^{<\mathbb{N}}.s \not\subseteq t \wedge t \not\subseteq s \to \mathrm{RC}(s) <_{\mathbb{Q}} \mathrm{LC}(t) \vee \mathrm{RC}(t) <_{\mathbb{Q}} \mathrm{LC}(s)$.*

$\langle 1\rangle 1$. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{s},\mathbf{t} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{s} \in 2^{<\mathbb{N}} \wedge \mathbf{t} \in 2^{<\mathbb{N}} \wedge \mathbf{s} \not\subseteq \mathbf{t} \wedge \mathbf{t} \not\subseteq \mathbf{s}$.

$\langle 1\rangle 2$. Supongamos sin pérdida de generalidad que $\mathfrak{M} \vDash \mathrm{lh}(\mathbf{s}) \leq \mathrm{lh}(\mathbf{t})$, el otro caso es análogo cambiando los papeles de $\mathbf{s}$ y $\mathbf{t}$.

$\langle 1\rangle 3$. $\mathfrak{M} \vDash \exists i < \mathrm{lh}(\mathbf{s}).\mathbf{s}(i) \neq \mathbf{t}(i)$.

DEMOSTRACIÓN: En caso contrario $\mathfrak{M} \vDash \forall i < \mathrm{lh}(\mathbf{s}).\mathbf{s}(i) = \mathbf{t}(i)$ y por tanto $\mathfrak{M} \vDash \mathbf{s} \subseteq \mathbf{t}$, absurdo por $\langle 1\rangle 1$.

$\langle 1\rangle 4$. Existe $\mathbf{i} \in \mathbb{N}$ tal que
$$\mathfrak{M} \vDash \mathbf{i} < \mathrm{lh}(\mathbf{s}) \wedge \mathbf{s}(\mathbf{i}) \neq \mathbf{t}(\mathbf{i}) \wedge \neg\exists i' < i.i' < \mathrm{lh}(\mathbf{s}) \wedge \mathbf{s}(i') \neq \mathbf{t}(i).$$

DEMOSTRACIÓN: Aplicando Σ^0_0-MIN a $\langle 1\rangle 3$.

$\langle 1\rangle 5$. Sean $\mathbf{s}' = \mathbf{s} \restriction \{0,\ldots,\mathbf{i}\}, \mathbf{t}' = \mathbf{t} \restriction \{0,\ldots,\mathbf{i}\}$, entonces
$$\mathfrak{M} \vDash \mathrm{RC}(\mathbf{s}') <_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}') \vee \mathrm{RC}(\mathbf{t}') <_{\mathbb{Q}} \mathrm{LC}(\mathbf{s}').$$

DEMOSTRACIÓN: Como por $\langle 1\rangle 1$ ni $\mathbf{s}$ ni $\mathbf{t}$ son la cadena vacía (pues si no, una sí estaría contenida en la otra) tampoco lo serán $\mathbf{s}'$ ni $\mathbf{t}'$. Por tanto existen $\mathbf{s}'_0, \mathbf{t}'_0, \mathbf{i}_0, \mathbf{i}_1$ tales que $\mathfrak{M} \vDash \mathbf{s}' = \mathbf{s}'_0{}^\frown\langle \mathbf{i}_0\rangle \wedge \mathbf{t}' = \mathbf{t}'_0{}^\frown\langle \mathbf{i}_1\rangle$. Es más, por $\langle 1\rangle 4$ tenemos que $\mathfrak{M} \vdash \mathbf{s}'_0 = \mathbf{t}'_0$ y que $\mathfrak{M} \vDash \mathbf{i}_0 \neq \mathbf{i}_1$; es fácil demostrar lo pedido distinguiendo casos en los valores de $\mathbf{i}_0, \mathbf{i}_1$.

$\langle 1\rangle 6$. Q.E.D.

DEMOSTRACIÓN: Por $\langle 1\rangle 5$ supongamos que $\mathfrak{M} \vDash \mathrm{RC}(\mathbf{s}') <_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}')$ (el otro caso es

análogo). Notemos que $\mathfrak{M} \vDash \mathbf{s}' \subseteq \mathbf{s} \wedge \mathbf{t}' \subseteq \mathbf{t}$, por tanto aplicando el lema 3.10 obtenemos que:

$$\mathfrak{M} \vDash \mathrm{RC}(\mathbf{s}) \leq_{\mathbb{Q}} \mathrm{RC}(\mathbf{s}') <_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}') \leq_{\mathbb{Q}} \mathrm{LC}(\mathbf{t}).$$

□

Tomando el límite, es decir, un camino del árbol binario completo (o dicho de otro modo, una función de $\mathbb{N}$ en $\{0,1\}$) obtenemos los elementos del conjunto de Cantor.

Lema 3.12. *$RCA_0 \vdash \forall f \in 2^{\mathbb{N}} \exists^1 x \in \mathbb{R} \forall n.\, \mathrm{LC}(f[n]) \leq_{\mathbb{R}} x \leq_{\mathbb{R}} \mathrm{RC}(f[n])$. Llamaremos $\mathrm{Cantor}(f)$ a tal real.*

Demostración: Por la completitud de intervalos encajados de $\mathbb{R}$. □

La idea es que C sea el conjunto de Cantor, aunque como es un conjunto de números reales no será realmente un conjunto. Eso no será un problema, ya que podemos introducir una fórmula que diga que un número real es de Cantor.

Definición 3.6 (**Conjunto de Cantor**)**.** Definimos $x \in C :\equiv \exists f \in 2^{\mathbb{N}}.x =_{\mathbb{R}} \mathrm{Cantor}(f)$.

■

Aunque sea fácil ver con los lemas ya establecidos, el siguiente resultado es importante, y es la base de la demostración de la dirección que nos falta. Lo que nos dice es que (aunque no haya una función en la teoría que exprese esa correspondencia) hay una correspondencia 1 a 1 entre los números de Cantor y los caminos del árbol binario completo (las sucesiones de 0's y 1's).

Lema 3.13. *$RCA_0 \vdash \forall x \in C \exists^1 f \in 2^{\mathbb{N}}.x =_{\mathbb{R}} \mathrm{Cantor}(f)$.*

Demostración: La existencia es por definición, la unicidad es consecuencia del lema 3.11.

□

Otro resultado importante: si un número real entre 0 y 1 no está en el conjunto de Cantor, entonces está en uno de los conjuntos intermedios que se van eliminando en cada iteración del proceso de creación del conjunto de Cantor. Pra esta demostración probaremos el contrarecíproco, así que crearemos una función f tal que $x = \mathrm{Cantor}(f)$. Para ello será necesario coger una aproximación racional suficientemente buena (que dado el intervalo que vamos a partir en 3 nos distinga si x esta en el intervalo de la izquierda o en el de la derecha, no estará en el centro por hipótesis del contrarecíproco) en cada paso, para poder definir f por recursión, ya que si nos quedaramos en los racionales la fórmula estaría demasiado alto en la jerarquía aritmética.

Lema 3.14.

$$RCA_0 \vdash \forall x \in \mathbb{R}.0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \wedge x \notin C \rightarrow$$
$$\exists s \in 2^{<\mathbb{N}}. \mathrm{RC}(s^\frown\langle 0\rangle) <_{\mathbb{R}} x <_{\mathbb{R}} \mathrm{LC}(s^\frown\langle 1\rangle).$$

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA_0 y $\mathbf{x} = \langle \mathbf{q}_n : n \in \mathbb{N}\rangle \in \wp(\mathbb{N})$ tal que
$$\mathfrak{M} \vDash \mathbf{x} \in \mathbb{R} \wedge 0 \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} 1.$$

⟨1⟩2. Es suficiente probar que
$$\mathfrak{M} \vDash (\forall s \in 2^{<\mathbb{N}}.\mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(s^\frown\langle 0\rangle) \vee \mathrm{LC}(s^\frown\langle 1\rangle) \leq_{\mathbb{R}} \mathbf{x}) \rightarrow \mathbf{x} \in C.$$
Por tanto supongamos que $\mathfrak{M} \vDash \forall s \in 2^{<\mathbb{N}}.\mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(s^\frown\langle 0\rangle) \vee \mathrm{LC}(s^\frown\langle 1\rangle) \leq_{\mathbb{R}} \mathbf{x}$.

Demostración: Es suficiente por ser el contrarrecíproco.

⟨1⟩3. Existe una función $\mathbf{f} : \mathbb{N} \longrightarrow \{0,1\}$ tal que
$$\mathfrak{M} \vDash \forall n.(\mathbf{q}_{2n+3} \leq_{\mathbb{Q}} (\mathrm{LC}(\mathbf{f}[n]) +_{\mathbb{Q}} \mathrm{RC}(\mathbf{f}[n]))/2 \rightarrow \mathbf{f}(n) = 0) \wedge$$
$$(\mathbf{q}_{2n+3} >_{\mathbb{Q}} (\mathrm{LC}(\mathbf{f}[n]) +_{\mathbb{Q}} \mathrm{RC}(\mathbf{f}[n]))/2 \rightarrow \mathbf{f}(n) = 1)$$

Demostración: Por recursión primitiva (notemos que $\mathbf{f}[n]$ depende únicamente de los valores anteriores i.e. $\mathbf{f}(0), \ldots, \mathbf{f}(n-1)$, por tanto se puede usar para la recursión), y es una función bien definida por la hipótesis de ⟨1⟩2.

⟨1⟩4. $\mathfrak{M} \vDash \forall n.\, \mathrm{LC}(\mathbf{f}[n]) \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[n])$.

⟨2⟩1. $\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[0]) \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[0])$.

Demostración: Notemos que $\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[0]) = \mathrm{LC}(\langle\rangle) = 0$ y $\mathfrak{M} \vDash \mathrm{RC}(\mathbf{f}[0]) = \mathrm{RC}(\langle\rangle) = 1$, por tanto el paso se cumple por hipótesis de ⟨1⟩1.

⟨2⟩2. $\mathfrak{M} \vDash \forall n.\, \mathrm{LC}(\mathbf{f}[n]) \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[n]) \rightarrow \mathrm{LC}(\mathbf{f}[n+1]) \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[n+1])$.

Demostración: Sea $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[\mathbf{n}]) \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[\mathbf{n}])$. Supongamos que $\mathfrak{M} \vDash \mathbf{q}_{2\mathbf{n}+3} \leq_{\mathbb{Q}} (\mathrm{LC}(\mathbf{f}[\mathbf{n}]) +_{\mathbb{Q}} \mathrm{RC}(\mathbf{f}[\mathbf{n}]))/2 =_{\mathbb{Q}} \mathrm{LC}(\mathbf{f}[\mathbf{n}]) + \dfrac{1}{2 \cdot_{\mathbb{Q}} 3^n}$ (si $>_{\mathbb{Q}}$ es análogo, ya que esto es que $\mathbf{x}$ está en el intervalo izquiedo y el otro caso que está en el derecho) y por tanto $\mathfrak{M} \vDash \mathbf{f}[\mathbf{n}] = 0$.
Tenemos que probar que
$$\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[\mathbf{n}+1]) =_{\mathbb{R}} \mathrm{LC}(\mathbf{f}[\mathbf{n}]^\frown\langle 0\rangle) =_{\mathbb{R}} \mathrm{LC}(\mathbf{f}[\mathbf{n}]) \leq_{\mathbb{R}} \mathbf{x},$$
lo cual es trivial por hipótesis y que
$$\mathfrak{M} \vDash \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[\mathbf{n}+1]) =_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[\mathbf{n}^\frown\langle 0\rangle]).$$
Por ⟨1⟩2 tenemos que $\mathfrak{M} \vDash \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[\mathbf{n}]^\frown\langle 0\rangle) \vee \mathrm{LC}(\mathbf{f}[\mathbf{n}]^\frown\langle 1\rangle) \leq_{\mathbb{R}} \mathbf{x}$.
Si $\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[\mathbf{n}]^\frown\langle 1\rangle) \leq_{\mathbb{R}} \mathbf{x}$ entonces $\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[n]) +_{\mathbb{Q}} \dfrac{2}{3^n} \leq_{\mathbb{R}} \mathbf{x}$ y por tanto
$$\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[n]) +_{\mathbb{Q}} \frac{2}{3^n} \leq_{\mathbb{Q}} \mathbf{q}_{2\mathbf{n}+3} +_{\mathbb{Q}} \frac{1}{2^{2(\mathbf{n}+1)}},$$
equivalentemente
$$\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[\mathbf{n}]) +_{\mathbb{Q}} (\frac{2}{3^n} -_{\mathbb{Q}} \frac{1}{2^{2(\mathbf{n}+1)}}) \leq_{\mathbb{Q}} \mathbf{q}_{2\mathbf{n}+3}.$$

Pero $\mathfrak{M} \vDash \dfrac{1}{2 \cdot_{\mathbb{Q}} 3^{\mathbf{n}}} <_{\mathbb{Q}} (\dfrac{2}{3^{\mathbf{n}}} -_{\mathbb{Q}} \dfrac{1}{2^{2(\mathbf{n}+1)}})$ por tanto

$$\mathfrak{M} \vDash \mathrm{LC}(\mathbf{f}[\mathbf{n}]) +_{\mathbb{Q}} \frac{1}{2 \cdot_{\mathbb{Q}} 3^{\mathbf{n}}} < \mathbf{q}_{\mathbf{2n+3}}$$

absurdo por hipótesis anterior, por tanto como uno de los casos de la disyunción anterior es imposible concluimos que $\mathfrak{M} \vDash \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{f}[\mathbf{n}]^\frown\langle 0\rangle)$.

⟨2⟩3. Q.E.D.

DEMOSTRACIÓN: Por Σ^0_1-IND, donde ⟨2⟩1 es el caso base y ⟨2⟩2 el paso inductivo.

⟨1⟩5. Q.E.D.

DEMOSTRACIÓN: Por ⟨1⟩4 y el lema de 3.12 tenemos que $\mathfrak{M} \vDash \mathbf{x} =_{\mathbb{R}} \mathrm{Cantor}(\mathbf{f})$, por tanto $\mathfrak{M} \vDash \mathbf{x} \in C$, como queríamos.

□

Finalmente, estamos ya preparados para demostrar la dirección que nos faltaba.

Lema 3.15. *RCA$_0$ +HEINE-BOREL ⊢ WKL$_0$.*

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de RCA$_0$ +HEINE-BOREL y $\mathbf{T} \subseteq 2^{<\mathbb{N}}$ tal que $\mathfrak{M} \vDash \mathrm{TREE}[\mathbf{T}] \wedge \neg\exists p.\mathrm{PATH}[p, \mathbf{T}]$.

⟨1⟩2. Existen funciones $\mathbf{a}_s, \mathbf{b}_s : 2^{<\mathbb{N}} \longrightarrow \mathbb{Q}$ tales que:

$$\mathbf{a}_s = \mathrm{LC}(s) -_{\mathbb{Q}} \frac{1}{3^{\mathrm{lh}(s)+1}}.$$
$$\mathbf{b}_s = \mathrm{RC}(s) +_{\mathbb{Q}} \frac{1}{3^{\mathrm{lh}(s)+1}}.$$

⟨1⟩3. $\mathfrak{M} \vDash \forall s, t \in 2^{\mathbb{N}}.s \not\subseteq t \wedge t \not\subseteq s \rightarrow \mathbf{b}_s <_{\mathbb{Q}} \mathbf{a}_t \wedge \mathbf{b}_t <_{\mathbb{Q}} \mathbf{a}_s$.

DEMOSTRACIÓN: La demonstración se puede hacer como las demostración del lema 3.11.

⟨1⟩4. Existe $\widetilde{\mathbf{T}}$ tal que

$$\mathfrak{M} \vDash \widetilde{\mathbf{T}} = \{u \mid u \in 2^{<\mathbb{N}} \wedge u \notin \mathbf{T} \wedge \forall t \subset u.t \in \mathbf{T}\}.$$

DEMOSTRACIÓN: Por Σ^0_0-COMP.

⟨1⟩5. $\mathfrak{M} \vDash \forall t \in \mathbf{T}\exists u \in \widetilde{\mathbf{T}}.t \subset u$.

⟨2⟩1. Supongamos lo contrario, sea $\mathbf{t} \in \mathbf{T}$ tal que $\mathfrak{M} \vDash \neg\exists u \in \widetilde{\mathbf{T}}.\mathbf{t} \subset u$.

⟨2⟩2. $\mathfrak{M} \vDash \forall s \in \mathbf{T}.\mathbf{t} \subseteq s \rightarrow (s^\frown\langle 0\rangle \in \mathbf{T} \wedge s^\frown\langle 1\rangle \in \mathbf{T})$.

DEMOSTRACIÓN: Supongamos que $\mathbf{s} \in \mathbf{T}$ pero $\mathfrak{M} \vDash \mathbf{t} \subseteq \mathbf{s} \wedge \mathbf{s}^\frown\langle 0\rangle \notin \mathbf{T}$. Entonces está claro que $\mathfrak{M} \vDash \mathbf{s}^\frown\langle 0\rangle \in \widetilde{\mathbf{T}}$, pero $\mathfrak{M} \vDash \mathbf{t} \subseteq \mathbf{s}^\frown\langle 0\rangle$, absurdo por ⟨2⟩1. Si $\mathfrak{M} \vDash \mathbf{s}^\frown\langle 1\rangle \notin \mathbf{T}$ análogo.

⟨2⟩3. Existe $\mathbf{f} \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \mathbf{f} : \mathbb{N} \longrightarrow \mathbb{N} \wedge \forall i.(i < \mathrm{lh}(\mathbf{t}) \to \mathbf{f}(i) = \mathbf{t}(i)) \wedge (i \geq \mathrm{lh}(\mathbf{t}) \to \mathbf{f}(i) = 0).$$

DEMOSTRACIÓN: Por Σ^0_0-COMP.

⟨2⟩4. $\mathfrak{M} \vDash \textsc{Path}[\mathbf{f}, \mathbf{T}]$.

DEMOSTRACIÓN: Directo por Σ^0_0-inducción, gracias a que $\mathfrak{M} \vDash \mathbf{t} \in \mathbf{T}$ y a ⟨2⟩2.

⟨2⟩5. Q.E.D.

DEMOSTRACIÓN: Hemos llegado a un absurdo con ⟨1⟩1 y ⟨2⟩4.

⟨1⟩6. $\mathfrak{M} \vDash \textsc{FinSet}[\widetilde{\mathbf{T}}]$.

⟨2⟩1. $\mathfrak{M} \vDash \forall x \in C \exists u \in \widetilde{\mathbf{T}}.\mathbf{a}_u <_{\mathbb{R}} x <_{\mathbb{R}} \mathbf{b}_u$.

DEMOSTRACIÓN: Sea $\mathbf{f} : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{x} =_{\mathbb{R}} \mathrm{Cantor}(\mathbf{f})$. Como $\mathfrak{M} \vDash \neg\textsc{Path}[\mathbf{f}, \mathbf{T}]$ tenemos que $\mathfrak{M} \vDash \exists n.\mathbf{f}[n] \notin \mathbf{T}$ y por Σ^0_0-MIN existirá $\mathbf{n}_0$ el mínimo que cumple eso. Sea $\mathbf{u} = \mathbf{f} \upharpoonright \{0, \ldots, \mathbf{n}_0\}$, es fácil ver que $\mathfrak{M} \vDash \mathbf{u} \in \widetilde{\mathbf{T}}$ por la definición de $\widetilde{\mathbf{T}}$ y

$$\mathfrak{M} \vDash \mathbf{a_u} <_{\mathbb{R}} \mathrm{LC}(\mathbf{u}) \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} \mathrm{RC}(\mathbf{u}) < \mathbf{b_u},$$

pues $\mathfrak{M} \vDash \mathbf{x} =_{\mathbb{R}} \mathrm{Cantor}(\mathbf{f})$.

⟨2⟩2. $\mathfrak{M} \vDash \forall x, 0 \leq_{\mathbb{R}} x \leq_{\mathbb{R}} 1 \to (\exists u \in \widetilde{\mathbf{T}}.\mathbf{a}_u <_{\mathbb{R}} x <_{\mathbb{R}} \mathbf{b}_u) \vee (\exists s \in 2^{\mathbb{N}}.\, \mathrm{RC}(s^\frown\langle 0\rangle) <_{\mathbb{R}} x <_{\mathbb{R}} \mathrm{LC}(s^\frown\langle 1\rangle))$.

DEMOSTRACIÓN: Sea $\mathbf{x}$ tal que $\mathfrak{M} \vDash 0 \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} 1$. Si $\mathfrak{M} \vDash \mathbf{x} \in C$ usamos ⟨2⟩1 y si $\mathfrak{M} \vDash \mathbf{x} \notin C$ usamos el lema 3.14.

⟨2⟩3. Q.E.D.

DEMOSTRACIÓN: Como $\mathfrak{M} \vDash$ HEINE-BOREL, lo usamos en ⟨2⟩2 y por tanto hay una cantidad finita de esos intervalos. Ahora bien, está claro que los intervalos $\mathrm{RC}(s^\frown\langle 0\rangle) <_{\mathbb{R}} x <_{\mathbb{R}} \mathrm{LC}(s^\frown\langle 1\rangle)$ no contienen elementos de C y C no puede ser cubierto por cualquier subconjunto propio de los intervalos $\mathbf{a}_u <_{\mathbb{R}} x <_{\mathbb{R}} \mathbf{b}_u$ con $u \in \widetilde{\mathbf{T}}$, así todos esos intervalos están en el subrecubrimiento finito y por tanto $\widetilde{\mathbf{T}}$ es finito.

⟨1⟩7. $\mathfrak{M} \vDash \textsc{FinSet}[\mathbf{T}]$.

DEMOSTRACIÓN: Directamente de ⟨1⟩5 y ⟨1⟩6 (recordemos que si $\mathbf{s}, \mathbf{t} \in \mathbb{N}^{<\mathbb{N}}$ entonces $\mathfrak{M} \vDash \mathbf{s} \subseteq \mathbf{t}$ implica $\mathfrak{M} \vDash \mathbf{s} \leq \mathbf{t}$).

⟨1⟩8. Q.E.D.

DEMOSTRACIÓN: Hemos probado un contrarecíproco del único axioma de WKL_0 que no es axioma de RCA_0.

□

Finalmente hemos demostrado las dos direcciones.

Teorema 3.16. *En RCA_0 son equivalentes:*

1. *WKL_0.*
2. *Heine-Borel.*

Demostración: Gracias a los lemas 3.9 y 3.15. □

3.3. Otros resultados de la matemática inversa de $\mathbf{WKL_0}$

Cerramos el capítulo enumerando otros teoremas de las matemáticas del día a día que se demuestran equivalentes a WKL_0 sobre RCA_0. Omitimos los detalles (tanto las demostraciones como las codificaciones nuevas) y remitimos al lector al capítulo IV del libro de Simpson [8] para más información al respecto. En todo caso, estos resultados ponen de manifiesto que WKL_0 es mucho más potente que RCA_0 desde el punto de vista de las matemáticas que se pueden formalizar en el sistema, y que WKL_0 es lo suficientemente fuerte como para demostrar resultados matemáticos fundamentales que se saben no constructivos (y, por tanto, no demostrables es RCA_0).

Teorema 3.17. *En RCA_0 son equivalentes:*

1. *WKL_0.*
2. *Toda función real continua en $[0,1]$ es uniformemente continua.*
3. *Toda función real continua en $[0,1]$ es acotada.*
4. *(**El principio del máximo**) Toda función real continua en $[0,1]$ tiene máximo.*
5. *(**Continua en intervalo cerrado implica integrable**) Toda función real continua en $[0,1]$ es Riemann integrable.*
6. *(**El teorema de completitud de Gödel para la lógica de primer orden**) Todo conjunto numerable consistente X de fórmulas cerradas tiene un modelo, i.e. existe un modelo numerable M tal que $\forall\sigma.\sigma \in X \to M(\sigma) = 1$.*
7. *(**El teorema de compacidad para la lógica de primer orden**) Si cada subconjunto finito de X tiene un modelo, entonces X tiene un modelo.*
8. *(**Existencia de ideales primos**) Todo anillo conmutativo numerable contiene un ideal primo.*
9. *(**Unicidad del cierre algebraico**) Todo cuerpo numerable (de característica 0) tiene un único (salvo isomorfismo) cierre algebraico.*

Capítulo 4

$\mathbf{ACA}_0$

Pasamos al estudio del siguiente subsistema de la aritmética de segundo orden que consideraremos en el presente trabajo, ACA_0, un sistema que resultará de enorme importancia desde el punto de vista del programa de la matemática inversa. El nombre proviene del término *arithmetical comprehension*, ya que el principio que caracteriza a dicho sistema es la comprensión para las fórmulas aritméticas (i.e. para la clase Σ^1_0). Esto es, los axiomas de ACA_0 garantizarán la existencia de los subconjuntos de $\mathbb{N}$ que sean definibles a partir de conjuntos dados usando para su definición fórmulas sin cuantificadores de conjuntos. Como veremos a lo largo del capítulo, este principio de existencia resultará lo suficientemente fuerte como para poder formalizar una gran cantidad de resultados fundamentales de diversas áreas de las matemáticas.

Por su parte, el principio de inducción se podrá aplicar a todos los conjuntos que existan en el modelo, esto es, se incluye también el axioma Ind.

Definición 4.1. (**La teoría $\mathbf{ACA}_0$**)

$$\mathrm{ACA}_0 = \mathrm{BASIC} + \mathrm{Ind} + \Sigma^1_0\text{-COMP}.$$

■

Obsérvese que hemos pasado directamente del principio de Δ^0_1-comprensión presente en RCA_0 o en WKL_0 al principio de comprensión para toda la jerarquía aritmética Σ^1_0. Es natural preguntarse qué sucede si en lugar de admitir directamente comprensión sobre todas las fórmulas aritméticas solo lo permitiésemos para un cierto nivel Σ^0_k con $k \in \omega \backslash \{0\}$. El siguiente lema nos muestra que obtendríamos una teoría equivalente a ACA_0.

Lema 4.1. *$RCA_0 + \Sigma^0_1$-COMP $\vdash \Sigma^1_0$-COMP.*

Demostración:
⟨1⟩1. $\mathrm{RCA}_0 + \Sigma^0_1$-COMP $\vDash \Sigma^0_0$-COMP.

Demostración: Trivial.

⟨1⟩2. Si $\mathrm{RCA}_0 + \Sigma^0_1$-COMP $\vDash \Sigma^0_k$-COMP entonces $\mathrm{RCA}_0 + \Sigma^0_1$-COMP $\vDash \Sigma^0_{k+1}$-COMP.

⟨2⟩1. Sea $\mathfrak{M}$ un modelo de $\mathrm{RCA}_0 + \Sigma^0_1$-COMP tal que $\mathfrak{M} \vDash \Sigma^0_k$-COMP.

⟨2⟩2. Sea $\varphi\{n\} \in \Sigma^0_{k+1}, X \in \mathrm{Var_C}$ tal que $X \notin \mathrm{Vl}(\varphi)$ $\{\nu_1, \ldots, \nu_r\} = \mathrm{Vl}(\varphi) \setminus \{n\}$.

⟨2⟩3. Definamos $\theta :\equiv \exists X \forall n. n \in X \leftrightarrow \varphi\{n\}$.

⟨2⟩4. $\mathrm{Vl}(\theta) = \{\nu_1, \ldots, \nu_r\}$.

Por las hipótesis en ⟨1⟩2 y ⟨2⟩3.

⟨2⟩5. Sean $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r \in \mathbb{N} \cup \wp(\mathbb{N})$, denotamos $\varphi[n] :\equiv \varphi[n, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r]$. Entonces
$$\boldsymbol{\theta} :\equiv \theta[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r] \equiv \exists X \forall n. n \in X \leftrightarrow \varphi[n],$$
es suficiente probar $\mathfrak{M} \vDash \boldsymbol{\theta}$.

Demostración: Que sean iguales es gracias a la definición de sustitución y que sea suficiente probar eso es gracias a la completitud.

⟨2⟩6. $\varphi[n] \equiv \exists j. \psi(n, j)$ con $\psi \in (\Pi^0_k)_{\mathfrak{M}}$. (Podemos suponer, sin pérdida de generalidad, que el bloque $\exists j$ consta de un solo cuantificador)

⟨2⟩7. Existe $\mathbf{Y} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{Y} = \{(n, j) \mid \neg\psi(n, j)\}$.

Demostración: Por Σ^0_k-COMP.

⟨2⟩8. Existe $\mathbf{X} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{X} = \{n \mid \exists j. (n, j) \notin \mathbf{Y}\}$.

Demostración: Por Σ^0_1-COMP.

⟨2⟩9. Q.E.D.

Demostración: Es fácil comprobar que $\mathbf{X}$ es el conjunto deseado.

⟨1⟩3. Q.E.D.

Demostración: El resultado se sigue de que: por inducción en la metateoría, para cualquier $k \in \omega$, $\mathrm{RCA}_0 + \Sigma^0_1$-COMP $\vDash \Sigma^0_k$-COMP; y cualquier fórmula Σ^1_0 es equivalente a una fórmula en Σ^0_k para algún k (poniéndola en forma normal prefija si fuera necesario).

□

Por otra parte, es importante observar que, al incluir el axioma de inducción y la comprensión aritmética, ACA_0 también nos proporciona el esquema de inducción para cualquier fórmula aritmética. Por tanto, ACA_0 es una extensión de la Aritmética de Peano PA (véase la definición 6.2).

Lema 4.2. *$ACA_0 \vdash \Sigma^1_0$-IND.*

DEMOSTRACIÓN: Sean un modelo $\mathfrak{M}$ de ACA_0 y una fórmula $\varphi[x] \in \Sigma^1_0$ con parámetros en $\mathbb{N} \cup \wp(\mathbb{N})$ (realmente estamos cogiendo una fórmula arbitraria y sustituyendo las variables libres por parámetros cualesquiera, pero como ya hemos hecho muchas veces este proceso anteriormente nos lo ahorramos) tal que $\mathfrak{M} \vdash \varphi[0] \wedge \forall n.\varphi[n] \to \varphi[n+1]$. En $\mathfrak{M}$ existe el conjunto $\mathfrak{M} \vDash \mathbf{X} = \{x \mid \varphi[x]\}$ por Σ^1_0-COMP y podemos probar que $\mathfrak{M} \vDash \forall x.x \in \mathbf{X}$ por IND. De ahí se concluye el resultado. □

Enunciamos las primeras equivalencias a ACA_0 sobre RCA_0, estas nos permitirán establecer los resultados de matemática inversa.

Teorema 4.3. *En RCA_0 se demuestran equivalentes:*

1. *ACA_0.*
2. *Σ^0_1-COMP.*
3. *$\forall f : \mathbb{N} \longrightarrow \mathbb{N}.\mathit{INY}(f) \to \exists X.X = \{n \mid \exists m.f(m) = n\}$.*

DEMOSTRACIÓN: Que 1. implica 2. es trivial y que 2. implica 1. se sigue del lema 4.1 y de Σ^0_1-IND implica IND. Que 2. implica a 3. es trivial y que 3. implica a 2. es gracias al lema 2.58. □

4.1. Completitud secuencial

Como hemos mencionado, ACA_0 es una subsistema de enorme importancia desde el punto de vista de la matemática inversa y una gran cantidad de teoremas de las matemáticas han resultado ser exactamente equivalentes a este principio.

En este sección, elegimos uno de esos teoremas fundamentales de la matemática y probamos con detalle su equivalencia a ACA_0: el teorema de Bolzano-Weierstrass (*toda sucesión acotada de reales contiene una subsucesión convergente*). Más aún, veremos que ACA_0 es lo suficientemente fuerte para desarrollar una buena teoría de completitud secuencial.

Empezamos definiendo el concepto de límite superior de una sucesión de números reales.

Definición 4.2 (**Límite superior**)**.** Definimos

$$x =_{\mathbb{R}} \limsup_n x_n :\equiv \langle x_n : n \in \mathbb{N} \rangle \in \mathbb{R}^{\mathbb{N}} \wedge x \in \mathbb{R} \wedge$$

$$(\forall \epsilon >_{\mathbb{R}} 0 \exists m \forall n > m.x_n \leq_{\mathbb{R}} x +_{\mathbb{R}} \epsilon) \wedge (\forall \epsilon >_{\mathbb{R}} 0 \forall m \exists n > m.|x -_{\mathbb{R}} x_n| <_{\mathbb{R}} \epsilon).$$

Al igual que cuando definimos la noción de límite, seremos algo laxos con la notación de esta fórmula, permitiendo escribir $\lim\sup_n x_n =_{\mathbb{R}} x$ o $x =_{\mathbb{R}} \lim\sup_n x_n =_{\mathbb{R}} \lim\sup_n y_n$ que se entienden de forma natural. ■

En ACA_0 se puede demostrar la existencia del límite superior de una sucesión y con eso probar que toda sucesión pose una subsucesión convergente, que en particular converge al límite superior.

Teorema 4.4.

$$ACA_0 \vdash \forall\langle x_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}.(\exists M \in \mathbb{R}\forall n.|x_n| <_{\mathbb{R}} M) \to$$

$$\exists x \in \mathbb{R}.(\lim_n \sup x_n =_{\mathbb{R}} x) \wedge (\exists\langle n_k : k \in \mathbb{N}\rangle \in \mathbb{N}^{\mathbb{N}}.(\forall k.n_k < n_{k+1}) \wedge x =_{\mathbb{R}} \lim_k x_{n_k})$$

Demostración:

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de ACA_0 y sea $\langle \mathbf{x}_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}$ tal que existe $\mathbf{M} \in \mathbb{R}$ tal que $\mathfrak{M} \vDash \forall n.|\mathbf{x}_n| <_{\mathbb{R}} \mathbf{M}$.

⟨1⟩2. Podemos suponer que $\mathfrak{M} \vDash \forall n.0 \leq_{\mathbb{R}} \mathbf{x}_n \leq_{\mathbb{R}} 1$.

Demostración: Gracias a que lím y lím sup se conservan mediante transformaciones lineales y por tanto podemos considerar la sucesión $\langle(\mathbf{x}_n +_{\mathbb{R}} \mathbf{M})/2\mathbf{M} : n \in \mathbb{N}\rangle$ y suponer que esta era la original.

⟨1⟩3. Existe $\mathbf{f} : \mathbb{N} \longrightarrow \mathbb{N}$ función tal que
$$\mathfrak{M} \vDash \forall k, i.\mathbf{f}(k) = i \leftrightarrow i < 2^k \wedge \varphi[i,k] \wedge \neg\exists j > i.\varphi[j,k],$$
donde $\varphi[i,k] :\equiv \forall m\exists n > m.i2^{-k} \leq_{\mathbb{R}} \mathbf{x}_n \leq_{\mathbb{R}} (i+1)2^{-k}$, es decir, $\varphi[i,k]$ quiere decir que hay infinitos elementos de la sucesión $\langle \mathbf{x}_n : n \in \mathbb{N}\rangle$ en el intervalo $[i2^{-k}, (i+1)2^{-k}]$.

Demostración: Por Σ^1_0-COMP.

⟨1⟩4. Existe $\mathbf{x} = \langle \mathbf{q}_k : n \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}$ con $\mathbf{q}_k = \mathbf{f}(k)2^{-k}$.

Demostración: Por composición de funciones.

⟨1⟩5. $\mathfrak{M} \vDash \mathbf{x} \in \mathbb{R}$ y además $\mathfrak{M} \vDash \forall k.\mathbf{f}(k)2^{-k} \leq_{\mathbb{R}} \mathbf{x} \leq_{\mathbb{R}} (\mathbf{f}(k)+1)2^{-k}$

Demostración: Por la completitud de intervalos encajados de $\mathbb{R}$.

⟨1⟩6. $\mathfrak{M} \vDash \mathbf{x} =_{\mathbb{R}} \lim\sup_n \mathbf{x}_n$.

⟨2⟩1. $\mathfrak{M} \vDash \forall\epsilon > 0\exists m\forall n.m < n \to \mathbf{x}_n \leq_{\mathbb{R}} \mathbf{x} + \epsilon$.

⟨3⟩1. Sea $\boldsymbol{\epsilon} > 0$.

⟨3⟩2. Existe $\mathbf{k} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash 2^{-\mathbf{k}} <_{\mathbb{R}} \boldsymbol{\epsilon}$.

⟨3⟩3. Existe un $\mathbf{m}$ tal que $\mathfrak{M} \vDash \forall n > \mathbf{m}.\mathbf{x}_n \leq_{\mathbb{R}} (\mathbf{f}(\mathbf{k})+1)2^{-\mathbf{k}}$.

DEMOSTRACIÓN: Por la definición de $\mathbf{f}$ en el paso $\langle 1\rangle 3$ gracias a que $\neg\exists j > \mathbf{f}(\mathbf{k}).\varphi[j,\mathbf{k}]$ (es decir, no hay un intervalo por encima del escogido con infinitos valores de la sucesión, por tanto a partir de un punto todos los valores de la sucesión están debajo del intervalo escogido, que es lo que se afirma).

$\langle 3\rangle 4$. Q.E.D.
DEMOSTRACIÓN: Como por $\langle 1\rangle 5$ $\mathfrak{M} \vDash \mathbf{f}(\mathbf{k})2^{-\mathbf{k}} \leq_{\mathbb{R}} \mathbf{x}$, entonces $\mathfrak{M} \vDash \mathbf{f}(\mathbf{k})2^{-\mathbf{k}} + 2^{-\mathbf{k}} = (\mathbf{f}(\mathbf{k})+1)2^{-\mathbf{k}} \leq_{\mathbb{R}} \mathbf{x} + 2^{-\mathbf{k}} <_{\mathbb{R}} \mathbf{x} + \boldsymbol{\epsilon}$, usando también $\langle 3\rangle 2$. Juntando esa desigualdad con la de $\langle 3\rangle 3$ obtenemos lo pedido.

$\langle 2\rangle 2$. $\mathfrak{M} \vDash \forall \epsilon > 0 \forall m \exists n. m < n \wedge |\mathbf{x} - \mathbf{x}_n| < \epsilon$.

$\langle 3\rangle 1$. Sean $\boldsymbol{\epsilon} > 0$ y $\mathbf{m} \in \mathbb{N}$ cualesquiera.

$\langle 3\rangle 2$. Existe $\mathbf{k} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash 2^{-\mathbf{k}} <_{\mathbb{R}} \boldsymbol{\epsilon}$.

$\langle 3\rangle 3$. Existe $\mathbf{n}$ tal que $\mathfrak{M} \vDash \mathbf{n} > \mathbf{m}$ tal que $\mathbf{f}(\mathbf{k})2^{-\mathbf{k}} \leq_{\mathbb{R}} \mathbf{x_n} \leq_{\mathbb{R}} (\mathbf{f}(\mathbf{k})+1)2^{-\mathbf{k}}$.
DEMOSTRACIÓN: Por la definición de $\mathbf{f}$ en $\langle 1\rangle 3$.

$\langle 3\rangle 4$. Q.E.D.
DEMOSTRACIÓN: Gracias a $\langle 1\rangle 5$ y a $\langle 3\rangle 3$ tanto $\mathbf{x_n}$ como $\mathbf{x}$ pertenecen al intervalo $[\mathbf{f}(\mathbf{k})2^{-\mathbf{k}}, (\mathbf{f}(\mathbf{k})+1)2^{-\mathbf{k}}]$, cuya longitud es $2^{-\mathbf{k}}$ menor que $\boldsymbol{\epsilon}$ por $\langle 3\rangle 2$. Por tanto basta escoger $n = \mathbf{n}$ ya que gracias a $\langle 3\rangle 3$ también $\mathbf{n} > \mathbf{m}$.

$\langle 2\rangle 3$. Q.E.D.

$\langle 1\rangle 7$. $\exists \langle n_k : k \in \mathbb{N}\rangle \in \mathbb{N}^{\mathbb{N}}.(\forall k. n_k < n_{k+1}) \wedge \mathbf{x} = \lim_k \mathbf{x}_{n_k}$.

DEMOSTRACIÓN: Basta con definir recursivamente $\mathbf{n}_k$:

$$\mathbf{n}_0 = \mathbf{m},$$

$$\mathbf{n}_{k+1} = \mu n. n > \mathbf{n}_k \wedge |\mathbf{x} - \mathbf{x}_n| \leq_{\mathbb{R}} 2^{-k-2}.$$

donde $\mathbf{m} = \mu n. |\mathbf{x} - \mathbf{x}_n| \leq_{\mathbb{R}} 2^{-1}$. Está bien definida gracias a $\langle 1\rangle 6$ y a que por estar en ACA_0 tenemos Σ^1_0-COMP (y por tanto la fórmula a la que estamos aplicando mínimo tiene función característica). Sin problema se demuestra que $\mathbf{x} = \lim_k \mathbf{x}_{\mathbf{n}_k}$.

$\langle 1\rangle 8$. Q.E.D.

DEMOSTRACIÓN: Gracias a $\langle 1\rangle 6$ y $\langle 1\rangle 7$.

□

Veremos a continuación que este resultado puede mejorarse a una equivalencia. De hecho, aprovecharemos para demostrar la equivalencia de ACA_0 con diversos teoremas clásicos sobre sucesiones de números reales.

Empezamos definiendo el concepto de supremo, pero como no tenemos conjuntos de reales definimos el supremo de una sucesión de reales.

Definición 4.3 (**Supremo**)**.** Definimos

$$x =_{\mathbb{R}} \sup_n x_n :\equiv \langle x_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}} \wedge x \in \mathbb{R} \wedge$$

$$(\forall n.x_n \leq_{\mathbb{R}} x) \wedge (\forall y.y <_{\mathbb{R}} x \to \exists n.y <_{\mathbb{R}} x_n).$$

■

Ahora definimos las fórmulas que expresan teoremas habituales de sucesiones de reales. Vamos a probar que todas son equivalentes a ACA_0 en RCA_0.

Definición 4.4. Definimos las siguientes fórmulas cerradas.

- Toda sucesión acotada (de reales) posee una subsucesión convergente:

$$\textsc{ExistsConvSub} :\equiv \forall\langle x_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}.(\exists M \in \mathbb{R}\forall n.|x_n| <_{\mathbb{R}} M) \to$$
$$\exists x \in \mathbb{R}\exists\langle n_k : k \in \mathbb{N}\rangle \in \mathbb{N}^{\mathbb{N}}.(\forall k.n_k < n_{k+1}) \wedge x =_{\mathbb{R}} \lim_k x_{n_k}.$$

- Toda sucesión de Cauchy es convergente:

$$\textsc{CauchyConv} :\equiv \forall\langle x_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}.(\forall \epsilon > 0\exists m\forall n.m < n \to |x_m -_{\mathbb{R}} x_n| <_{\mathbb{R}} \epsilon) \to$$
$$\exists x \in \mathbb{R}.x =_{\mathbb{R}} \lim_n x_n.$$

- Toda sucesión acotada tiene supremo (aproximación de todo conjunto no vacío acotado superiormente tiene supremo, pero como no tenemos conjuntos trabajamos con sucesiones).

$$\textsc{ExistsSup} :\equiv \forall\langle x_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}.(\exists M \in \mathbb{R}\forall n.|x_n| <_{\mathbb{R}} M) \to \exists x \in \mathbb{R}.x =_{\mathbb{R}} \sup_n x_n.$$

- Toda sucesión creciente acotada superiormente es convergente (toda sucesión monótona acotada es convergente):

$$\textsc{MonConv} :\equiv \forall\langle x_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}.(\exists M \in \mathbb{R}\forall n.x_n <_{\mathbb{R}} M) \wedge (\forall k.x_k <_{\mathbb{R}} x_{k+1}) \to$$
$$\exists x \in \mathbb{R}.x =_{\mathbb{R}} \lim_n x_n$$

■

Enunciamos ahora algunos lemas que nos permitirán establecer el teorema como consecuencia directa de estos.

Lema 4.5. *$ACA_0 \vdash$ ExistsConvSub.*

Demostración: Es consecuencia trivial del teorema 4.4. □

Lema 4.6. *$RCA_0 +$ExistsConvSub $\vdash$ CauchyConv.*

Demostración: En RCA_0 se puede emular la demostración típica. □

Lema 4.7. *$RCA_0 +$CauchyConv $\vdash$ MonConv.*

Demostración: En RCA_0 se puede emular la demostración típica. □

Lema 4.8. *$ACA_0 \vdash$ ExistsSup.*

Demostración:
$\langle 1\rangle 1$. Sea $\mathfrak{M}$ un modelo de ACA_0 y $\langle \mathbf{x}_n : n \in \mathbb{N}\rangle \in \mathbb{R}^{\mathbb{N}}$ tal que $\mathfrak{M} \vDash \exists M \forall n.|\mathbf{x}_n| <_{\mathbb{R}} M$.

$\langle 1\rangle 2$. Podemos suponer que $\mathfrak{M} \vDash \forall n.0 \leq_{\mathbb{R}} \mathbf{x}_n \leq_{\mathbb{R}} 1$.

Demostración: Gracias a que sup se conserva mediante transformaciones lineales y por tanto podemos considerar la sucesión $\langle (\mathbf{x}_n +_{\mathbb{R}} M)/2M : n \in \mathbb{N}\rangle$ y suponer que esta era la original.

$\langle 1\rangle 3$. Existe $\mathbf{f} : \mathbb{N} \longrightarrow \mathbb{N}$ función tal que
$$\mathfrak{M} \vDash \forall k, i.\mathbf{f}(k) = i \leftrightarrow i < 2^k \wedge (\exists n.i2^{-k} \leq_{\mathbb{R}} \mathbf{x}_n) \wedge (\neg\exists j > i \exists n.j2^{-k} \leq_{\mathbb{R}} \mathbf{x}_n).$$

Demostración: Por Σ^1_0-COMP.

$\langle 1\rangle 4$. Existe $\mathbf{x} = \langle \mathbf{q}_k : k \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}$ donde $\mathbf{q}_k = \mathbf{f}(k)2^{-k}$.

Demostración: Por composición de funciones.

$\langle 1\rangle 5$. $\mathfrak{M} \vDash \mathbf{x} \in \mathbb{R}$.

Demostración: Por la definición de número real y los pasos $\langle 1\rangle 3$ y $\langle 1\rangle 4$.

$\langle 1\rangle 6$. $\mathfrak{M} \vDash \sup_n \mathbf{x}_n =_{\mathbb{R}} \mathbf{x}$.

$\langle 2\rangle 1$. $\mathfrak{M} \vDash \forall n.\mathbf{x}_n \leq_{\mathbb{R}} \mathbf{x}$.

Demostración: Por reducción al absurdo, supongamos que existe $\mathbf{n}$ tal que $\mathfrak{M} \vDash \mathbf{x} <_{\mathbb{R}} \mathbf{x_n}$. Como los reales son sucesiones de Cauchy con ratio de covergencia de 2^{-k} eso quiere decir que existe $\mathbf{k} \in \mathbb{N}$ tal que
$$\mathfrak{M} \vDash \mathbf{q_k} +_{\mathbb{Q}} 2^{-\mathbf{k}} <_{\mathbb{R}} \mathbf{x_n}.$$

Por $\langle 1\rangle 4$ eso quiere decir que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{k})2^{-\mathbf{k}} +_{\mathbb{Q}} 2^{-\mathbf{k}} <_{\mathbb{R}} \mathbf{x_n}$ y por tanto
$$\mathfrak{M} \vDash (\mathbf{f}(\mathbf{k}) + 1)2^{-\mathbf{k}} <_{\mathbb{R}} \mathbf{x_n},$$
lo cual es absurdo por $\langle 1\rangle 3$ (por la tercera conjunción para mayor exactitud).

$\langle 2\rangle 2$. $\mathfrak{M} \vDash \forall y.y <_{\mathbb{R}} \mathbf{x} \to \exists n.y \leq_{\mathbb{R}} \mathbf{x}_n$.

DEMOSTRACIÓN: Sea $\mathbf{y} = \langle \mathbf{q}'_k : k \in \mathbb{N}\rangle \in \mathbb{R}$ tal que $\mathfrak{M} \vDash \mathbf{y} <_{\mathbb{R}} \mathbf{x}$, es decir existe $\mathbf{k}$ tal que $\mathfrak{M} \vDash \mathbf{q}'_{\mathbf{k}} +_{\mathbb{Q}} 2^{-\mathbf{k}+1} <_{\mathbb{Q}} \mathbf{q_k} =_{\mathbb{Q}} \mathbf{f}(\mathbf{k})2^{-\mathbf{k}}$. Pero por $\langle 1\rangle 3$ tenemos que existe $\mathbf{n}$ tal que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{k})2^{-\mathbf{k}} \leq_{\mathbb{R}} \mathbf{x_n}$, por tanto:
$$\mathfrak{M} \vDash \mathbf{q}'_{\mathbf{k}} +_{\mathbb{Q}} 2^{-\mathbf{k}+1} <_{\mathbb{R}} \mathbf{f}(\mathbf{k})2^{-\mathbf{k}} \leq_{\mathbb{R}} \mathbf{x_n},$$
lo que implica (usando que $\mathfrak{M} \vDash |\mathbf{y} - \mathbf{q}'_{\mathbf{k}}| \leq_{\mathbb{R}} 2^{-\mathbf{k}}$) que $\mathfrak{M} \vDash \mathbf{y} <_{\mathbb{R}} \mathbf{x_n}$, como queríamos.

$\langle 2\rangle 3$. Q.E.D.

DEMOSTRACIÓN: Gracias a $\langle 1\rangle 6$.

□

Lema 4.9. *RCA_0 + ExistsSup $\vdash$ MonConv.*

DEMOSTRACIÓN: En RCA_0 se puede emular la demostración típica. □

Finalmente, obtenemos el resultado deseado de matemática inversa probando que ACA_0 puede recuperarse sobre RCA_0 a partir del principio de convergencia monótonona.

Lema 4.10. *RCA_0 + MonConv $\vdash ACA_0$.*

DEMOSTRACIÓN:
$\langle 1\rangle 1$. Sea $\mathfrak{M}$ un modelo de $\mathrm{RCA}_0 + \mathrm{MonConv}$.

$\langle 1\rangle 2$. Es suficiente probar que
$$\mathfrak{M} \vDash \forall f : \mathbb{N} \longrightarrow \mathbb{N}.\mathrm{Iny}(f) \to \exists X \forall n.n \in X \leftrightarrow \exists m.f(m) = n.$$

DEMOSTRACIÓN: Por teorema 4.3.

$\langle 1\rangle 3$. Sea $\mathbf{f} : \mathbb{N} \longrightarrow \mathbb{N}$, tal que $\mathfrak{M} \vDash \mathrm{Iny}[\mathbf{f}]$.

$\langle 1\rangle 4$. Existe $\langle \mathbf{c}_n : n \in \mathbb{N}\rangle \in \mathbb{Q}^{\mathbb{N}}$ tal que
$$\mathfrak{M} \vDash \forall n.\mathbf{c}_n =_{\mathbb{Q}} \sum_{i=0}^{n} 2^{-\mathbf{f}(i)}.$$

DEMOSTRACIÓN: Por la composición de funciones.

$\langle 1\rangle 5$. Existe $\mathbf{c} \in \mathbb{R}$ tal que $\mathfrak{M} \vDash \mathbf{c} =_{\mathbb{R}} \lim_n \mathbf{c}_n$.

$\langle 2\rangle 1$. $\mathfrak{M} \vDash \forall n.\mathbf{c}_n <_{\mathbb{R}} \mathbf{c}_{n+1}$.

DEMOSTRACIÓN: Por Σ^0_0-IND en n se demuestra que $\mathfrak{M} \vDash \forall n.\mathbf{c}_n <_{\mathbb{Q}} \mathbf{c}_{n+1}$, de donde

se sigue lo pedido.

⟨2⟩2. $\forall n.\mathbf{c}_n <_{\mathbb{R}} 2$.

DEMOSTRACIÓN: Por Σ^0_0-IND se prueba que $\mathfrak{M} \vDash \forall n. \sum_{i=0}^{n} 2^{-i} =_{\mathbb{Q}} 2 -_{\mathbb{Q}} 2^{-n} <_{\mathbb{Q}} 2$. Notemos que $\mathfrak{M} \vDash \forall n.\mathbf{c}_n \leq_{\mathbb{Q}} \sum_{i=0}^{n} 2^{-i}$, por tanto $\mathfrak{M} \vDash \forall n.\mathbf{c}_n <_{\mathbb{Q}} 2$, lo que implica lo pedido.

⟨2⟩3. Q.E.D.

DEMOSTRACIÓN: Usando que por ⟨1⟩1 $\mathfrak{M} \vDash$ MONCONV y que $\langle \mathbf{c}_n : n \in \mathbb{N} \rangle$ es una sucesión monótona gracias a ⟨2⟩1 y ⟨2⟩2.

⟨1⟩6. $\mathfrak{M} \vDash (\exists i.\mathbf{f}(i) = k) \leftrightarrow (\forall n.|\mathbf{c}_n -_{\mathbb{R}} \mathbf{c}| <_{\mathbb{R}} 2^{-k} \rightarrow \exists i \leq n.\mathbf{f}(i) = k)$.

⟨2⟩1. Sea $\mathbf{k} \in \mathbb{N}$ cualquiera.

⟨2⟩2. $\mathfrak{M} \vDash (\exists i.\mathbf{f}(i) = \mathbf{k}) \rightarrow (\forall n.|\mathbf{c}_n -_{\mathbb{R}} \mathbf{c}| <_{\mathbb{R}} 2^{-\mathbf{k}} \rightarrow \exists i \leq n.\mathbf{f}(i) = \mathbf{k})$.

DEMOSTRACIÓN: Supongamos que existe $\mathbf{i} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{i}) = \mathbf{k}$ y sea $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash |\mathbf{c_n} -_{\mathbb{R}} \mathbf{c}| =_{\mathbb{R}} \sum_{i=\mathbf{n}+1}^{\infty} 2^{-\mathbf{f}(i)} <_{\mathbb{R}} 2^{-\mathbf{k}}$, veamos que $\mathfrak{M} \vDash \mathbf{i} \leq \mathbf{n}$ y habremos terminado. Si $\mathfrak{M} \vDash \mathbf{i} > \mathbf{n}$, entonces $\mathfrak{M} \vDash \sum_{i=\mathbf{n}+1}^{+\infty} 2^{-\mathbf{f}(i)} \geq_{\mathbb{R}} 2^{-\mathbf{k}}$, ya que estamos sumando $\mathbf{2^{-k}}$ a otras cosas positivas, ya que $\mathfrak{M} \vDash 2^{-\mathbf{f(i)}} =_{\mathbb{Q}} 2^{-\mathbf{k}}$. Sin embargo eso es absurdo con lo anterior, por tanto $\mathfrak{M} \vDash \mathbf{i} \leq \mathbf{n}$.

⟨2⟩3. $\mathfrak{M} \vDash (\forall n.|\mathbf{c}_n -_{\mathbb{R}} \mathbf{c}| <_{\mathbb{R}} 2^{-\mathbf{k}} \rightarrow \exists i \leq n.\mathbf{f}(i) = \mathbf{k}) \rightarrow (\exists i.\mathbf{f}(i) = \mathbf{k})$.

DEMOSTRACIÓN: Supongamos que $\mathfrak{M} \vDash \forall n.|\mathbf{c}_n - \mathbf{c}| <_{\mathbb{R}} 2^{-\mathbf{k}} \rightarrow \exists i \leq n.\mathbf{f}(i) = \mathbf{k}$. Por ⟨1⟩5 sabemos que $\mathfrak{M} \vDash \forall \epsilon > 0 \exists n \forall i.|\mathbf{c} - \mathbf{c}_{n+i}| <_{\mathbb{R}} \epsilon$. Tomando $\epsilon = 2^{-\mathbf{k}}$, e $i = 0$ nos queda que existe $\mathbf{n}$ tal que $\mathfrak{M} \vDash |\mathbf{c} -_{\mathbb{R}} \mathbf{c_n}| < 2^{-\mathbf{k}}$, que por la hipótesis de este apartado quiere decir que $\mathfrak{M} \vDash \exists i \leq \mathbf{n}.\mathbf{f}(i) = \mathbf{k}$ y por tanto $\mathfrak{M} \vDash \exists i.\mathbf{f}(i) = \mathbf{k}$.

⟨2⟩4. Q.E.D.

⟨1⟩7. Q.E.D.

DEMOSTRACIÓN: Por ⟨1⟩6, la fórmula $\varphi[k] :\equiv \exists i.\mathbf{f}(i) = k$ es Δ^0_1. Basta pues usar Δ^0_1-COMP (disponible en RCA_0).

□

Con todos estos lemas podemos probar el resultado que queríamos como una consecuencia directa.

Teorema 4.11. *En RCA_0 se demuestran equivalentes:*

1. *ACA_0.*
2. *ExistsConvSub.*
3. *CauchyConv.*

4. *ExistsSup.*

5. *MonConv.*

Demostración: Se demuestra que $1 \to 2 \to 3 \to 5$ usando los lemas 4.5, 4.6, 4.7 y que $1 \to 4 \to 5$ con los lemas 4.8, 4.9. Finalmente $5 \to 1$ gracias al lema 4.10. □

Cabe destacar que este resultado se puede generalizar a espacios métricos completos y separables, el lector interesado es remitido al capítulo III del libro de Simpson [8].

4.2. Algo de combinatoria infinita

En esta sección vamos a estudiar la equivalencia de ACA$_0$ con dos teoremas básicos de combinatoria infinita, el lema de König y el teorema de Ramsey.

4.2.1. Lema de König

El lema de König afirma que todo árbol infinito con ramificaciones finitas tiene (al menos) un camino. Se trata por tanto de una generalización del lema débil de König que estudiamos en el capítulo anterior. Veamos las definiciones asociadas a él.

Definición 4.5 (**Árboles finitamente ramificados y el lema de König**)**.** Consideramos las siguientes definiciones:

- El concepto de árbol con ramificación finita, esto es, cada nodo tiene una cantidad finita de hijos:

$$\textsc{FinBranch}[T] :\equiv \textsc{Tree}[T] \wedge \forall \sigma \in T \exists n \forall m. \sigma^\frown \langle m \rangle \in T \to m < n.$$

- El concepto de árbol k-ario, esto es, cada nodo tiene a lo más k hijos:

$$k\text{-}\textsc{Ary}[T] :\equiv \textsc{Tree}[T] \wedge \forall \tau \in T \exists s \in \mathbb{N}^k \forall m. \tau^\frown \langle m \rangle \in T \to \exists i < k. m = s(i).$$

- El lema de König:

$$\textsc{König} :\equiv \forall T \subseteq \mathbb{N}^{<\mathbb{N}}. \textsc{Tree}[T] \wedge \textsc{InfSet}[T] \wedge \textsc{FinBran}[T] \to \exists g. \textsc{Path}[g, T].$$

- El lema de König restringido a árboles 2-arios, es decir, a árboles tales que cada nodo tiene a lo más 2 sucesores inmediatos:

$$\text{KÖNIG2} :\equiv \forall T \subseteq \mathbb{N}^{<\mathbb{N}}.\textsc{Tree}[T] \wedge \textsc{InfSet}[T] \wedge \text{2-}\textsc{Ary}[T] \to \exists g.\textsc{Path}[g, T].$$

■

Un resultado técnico que usaremos más adelante es que en ACA_0 la unón finita de conjuntos finitos es finita. Veamos primero la existencia de la únion de los n primeros elementos de una familia de conjuntos (lo probamos para cualquier conjunto en general, pero nos interesa el caso de que U sea una familia de conjuntos).

Lema 4.12. *$RCA_0 \vdash \forall n \forall U \exists^1 V.V = \{i \mid \exists k < n.(k, i) \in U\}$.*

Si denotamos a U como $\langle U_i : i \in \mathbb{N}\rangle$, entonces este único conjunto lo llamamos $\bigcup_{i=0}^{n-1} U_i$.

Demostración: La existencia es por Σ^0_0-COMP y la unicidad por la igualdad de conjuntos. □

Veamos que si la familia es de conjuntos finitos, podemos coger los n primeros y su unión será finita (otra vez lo probamos para el caso donde U es un conjunto cualquiera, pero nos interesará usarlo con familias de conjuntos).

Lema 4.13 (Unión finita de conjuntos finitos).

$$ACA_0 \vdash \forall \langle U_i : i \in \mathbb{N}\rangle.(\forall i.\textsc{FinSet}[U_i]) \to \forall n.\textsc{FinSet}[\bigcup_{i=0}^{n-1} U_i].$$

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de ACA_0 y $\langle \mathbf{U}_i : i \in \mathbb{N}\rangle \subseteq \mathbb{N} \times \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall i.\textsc{FinSet}[\mathbf{U}_i]$.

⟨1⟩2. Definimos $\varphi[n] :\equiv \textsc{FinSet}[\bigcup_{i=0}^{n-1} \mathbf{U}_i]$.

⟨1⟩3. $\mathfrak{M} \vDash \varphi[0]$.

Demostración: Es fácil ver que $\mathfrak{M} \vDash \bigcup_{i=0}^{-1} \mathbf{U}_i = \varnothing$, por tanto el resultado es trivial.

⟨1⟩4. $\mathfrak{M} \vDash \forall n.\varphi[n] \to \varphi[n+1]$.

Demostración: Sea $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \varphi[\mathbf{n}]$. Sea por tanto $\mathbf{k}$ tal que $\mathfrak{M} \vDash \forall x \in \bigcup_{i=0}^{\mathbf{n}-1} \mathbf{U}_i.x < \mathbf{k}$. Por ⟨1⟩1, tenemos que existe $\mathbf{k}'$ tal que $\mathfrak{M} \vDash \forall x \in \mathbf{U}_{\mathbf{n}}.x < \mathbf{k}'$. Nos basta tomar el más grande entre $\mathbf{k}$ y $\mathbf{k}'$.

⟨1⟩5. Q.E.D.

DEMOSTRACIÓN: El resultado se sigue de usar Σ^1_0-IND en $\varphi[n]$, donde $\langle 1\rangle 3$ es el caso base y $\langle 1\rangle 4$ el paso inductivo.

□

Con esto probamos la primera parte de la equivalencia de ACA$_0$ y KÖNIG.

Lema 4.14. *ACA$_0$ $\vdash$ KÖNIG.*

DEMOSTRACIÓN:

$\langle 1\rangle 1$. Sea $\mathfrak{M}$ un modelo de ACA$_0$ y $\mathbf{T} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \textsc{Tree}[\mathbf{T}] \wedge \textsc{InfSet}[\mathbf{T}] \wedge \textsc{FinBran}[\mathbf{T}]$.

$\langle 1\rangle 2$. Existe $\mathbf{T}^* \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{T}^* = \{\tau \mid \tau \in \mathbf{T} \wedge \forall n \exists \sigma > n.\sigma \in \mathbf{T} \wedge \tau \subseteq \sigma\}$.

DEMOSTRACIÓN: Por Σ^1_0-COMP.

$\langle 1\rangle 3$. $\mathfrak{M} \vDash \langle\rangle \in \mathbf{T}^*$.

DEMOSTRACIÓN: Ya que por $\langle 1\rangle 1$ $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{T}]$.

$\langle 1\rangle 4$. $\mathfrak{M} \vDash \forall \tau \in \mathbf{T}^* \exists n.\tau^\frown\langle n\rangle \in \mathbf{T}^*$.

$\langle 2\rangle 1$. Sea $\boldsymbol{\tau} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \boldsymbol{\tau} \in \mathbf{T}^*$ y supongamos que $\mathfrak{M} \vDash \forall n.\boldsymbol{\tau}^\frown\langle n\rangle \notin \mathbf{T}^*$.

$\langle 2\rangle 2$. Existe $\mathbf{k}$ tal que $\mathfrak{M} \vDash \forall n.\boldsymbol{\tau}^\frown\langle n\rangle \in \mathbf{T} \to n < \mathbf{k}$.

DEMOSTRACIÓN: Por $\langle 1\rangle 1$ $\mathfrak{M} \vDash \textsc{FinBran}[\mathbf{T}]$.

$\langle 2\rangle 3$. $\mathfrak{M} \vDash \forall n.\boldsymbol{\tau}^\frown\langle n\rangle \in \mathbf{T} \to \exists m \forall \sigma.\boldsymbol{\tau}^\frown\langle n\rangle \subseteq \sigma \wedge \sigma \in \mathbf{T} \to \sigma \leq m$.

DEMOSTRACIÓN: Consecuencia de que por $\langle 2\rangle 1$ $\mathfrak{M} \vDash \forall n.\boldsymbol{\tau}^\frown\langle n\rangle \notin \mathbf{T}^*$ y de la definición de $\mathbf{T}^*$ en $\langle 1\rangle 2$.

$\langle 2\rangle 4$. Existe $\langle \mathbf{U}_i : i \in \mathbb{N}\rangle \subseteq \mathbb{N} \times \mathbb{N}$ tal que
$$\mathfrak{M} \vDash \langle \mathbf{U}_i : i \in \mathbb{N}\rangle = \{(i, \sigma) \mid \boldsymbol{\tau}^\frown\langle i\rangle \subseteq \sigma \wedge \sigma \in \mathbf{T}\}.$$
DEMOSTRACIÓN: Por Σ^0_0-COMP.

$\langle 2\rangle 5$. $\mathfrak{M} \vDash \textsc{FinSet}[\bigcup_{i=0}^{\mathbf{k}-1} \mathbf{U}_i]$.

DEMOSTRACIÓN: Que $\mathfrak{M} \vDash \forall i.\textsc{FinSet}[\mathbf{U}_i]$ es consecuencia directa de $\langle 2\rangle 3$, por tanto basta con aplicar el lema 4.13.

$\langle 2\rangle 6$. $\mathfrak{M} \vDash \exists m \forall \sigma \in \mathbf{T}.\boldsymbol{\tau} \subseteq \sigma \to \sigma < m$.

DEMOSTRACIÓN: Por $\langle 2\rangle 5$ sea $\mathbf{m}' \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \forall \sigma \in \bigcup_{i=0}^{\mathbf{k}-1} \mathbf{U}_i].\sigma < \mathbf{m}'$. Sea $\mathbf{m}$ el mayor entre $\boldsymbol{\tau} + 1$ y $\mathbf{m}'$, entonces si $\mathfrak{M} \vDash \boldsymbol{\tau} \subseteq \boldsymbol{\sigma}$ tenemos dos opciones. $\mathfrak{M} \vDash \boldsymbol{\sigma} = \boldsymbol{\tau}$ y claramente entonces $\mathfrak{M} \vDash \boldsymbol{\sigma} < \mathbf{m}$ o bien $\mathfrak{M} \vDash \mathrm{lh}(\boldsymbol{\tau}) < \mathrm{lh}(\boldsymbol{\sigma})$ y por $\langle 2\rangle 2$ $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \bigcup_{i=0}^{\mathbf{k}-1} \mathbf{U}_i$, por tanto $\mathfrak{M} \vDash \boldsymbol{\sigma} < \mathbf{m}$.

$\langle 2\rangle 7$. Q.E.D.

DEMOSTRACIÓN: Suponiendo lo contrario en ⟨2⟩1, i.e. que $\mathfrak{M} \vDash \forall n.\boldsymbol{\tau}^\frown\langle n\rangle \notin \mathbf{T}^*$ hemos llegado a que $\mathfrak{M} \vDash \exists m \forall \sigma \in \mathbf{T}.\boldsymbol{\tau} \subseteq \sigma \to \sigma < m$ por ⟨2⟩6, lo cual contradice que $\mathfrak{M} \vDash \boldsymbol{\tau} \in \mathbf{T}^*$, hipótesis de ⟨2⟩1.

⟨1⟩5. $\mathfrak{M} \vDash \exists g.\text{PATH}[g, \mathbf{T}]$.

DEMOSTRACIÓN: Por recursión primitiva tenemos la existencia de una función $\mathbf{g} : \mathbb{N} \longrightarrow \mathbb{N}^{<\mathbb{N}}$, tal que

$$\mathbf{g}(0) = \langle\rangle$$
$$\mathbf{g}(k+1) = \mu n.\mathbf{g}[k]^\frown\langle n\rangle \in \mathbf{T}^*.$$

Claramente es una rama infinita de $\mathbf{T}$.

⟨1⟩6. Q.E.D.

□

Para probar la dirección inversa, primero consideramos un paso intermedio bien simple:

Lema 4.15. *$RCA_0 \vdash$ KÖNIG $\to$ KÖNIG2.*

DEMOSTRACIÓN: Es trivial, pues en RCA_0 se prueba fácilmente que

$$\text{RCA}_0 \vdash \forall T \subseteq \mathbb{N}^{<\mathbb{N}}.\text{TREE}[T] \wedge 2\text{-ARY}[T] \to \text{FINBRAN}[T].$$

□

Finalmente probamos la otra dirección de la equivalencia:

Lema 4.16. *$RCA_0 \vdash$ KÖNIG2 $\to ACA_0$.*

DEMOSTRACIÓN:
⟨1⟩1. Sean $\mathfrak{M}$ modelo de RCA_0 +KÖNIG2 y $\mathbf{f} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{f} : \mathbb{N} \longrightarrow \mathbb{N} \wedge \text{INY}[\mathbf{f}]$.

⟨1⟩2. Existe $\mathbf{T} \in \wp(\mathbb{N})$ tal que

$$\mathfrak{M} \vDash \mathbf{T} = \{\tau \mid \tau \in \mathbb{N}^{<\mathbb{N}} \wedge (\forall m, n < \text{lh}(\tau).\mathbf{f}(m) = n \leftrightarrow \tau(n) = m+1) \wedge (\forall n < \text{lh}(\tau).\tau(n) > 0 \to \mathbf{f}(\tau(n)-1) = n)\}.$$

DEMOSTRACIÓN: Existe por Σ^0_0-COMP.

⟨1⟩3. $\mathfrak{M} \vDash \text{TREE}[\mathbf{T}]$.

⟨2⟩1. $\mathfrak{M} \vDash \mathbf{T} \subseteq \mathbb{N}^{<\mathbb{N}}$.

DEMOSTRACIÓN: Trivial por definición de $\mathbf{T}$ en ⟨1⟩2.

⟨2⟩2. Sean $\boldsymbol{\sigma}, \boldsymbol{\tau} \in \mathbb{N}$ arbitrarios, entonces $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbb{N}^{<\mathbb{N}} \wedge \boldsymbol{\sigma} \subseteq \boldsymbol{\tau} \wedge \boldsymbol{\tau} \in \mathbf{T} \to \boldsymbol{\sigma} \in \mathbf{T}$.

⟨3⟩1. Supongamos que $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbb{N}^{<\mathbb{N}} \wedge \boldsymbol{\sigma} \subseteq \boldsymbol{\tau} \wedge \boldsymbol{\tau} \in \mathbf{T}$.

⟨3⟩2. $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbb{N}^{<\mathbb{N}}$.
DEMOSTRACIÓN: Hipótesis de ⟨3⟩1.

⟨3⟩3. $\forall m, n < \mathrm{lh}(\boldsymbol{\sigma}).\mathbf{f}(m) = n \leftrightarrow \boldsymbol{\sigma}(n) = m + 1$
DEMOSTRACIÓN: Sean $\mathbf{m}, \mathbf{n} \in \mathbb{N}$ arbitrarios tales que $\mathfrak{M} \vDash \mathbf{m} < \mathrm{lh}(\boldsymbol{\sigma}) \wedge \mathbf{n} < \mathrm{lh}(\boldsymbol{\sigma})$. Como $\mathfrak{M} \vDash \boldsymbol{\sigma} \subseteq \boldsymbol{\tau}$, se tiene que $\mathfrak{M} \vDash \mathbf{m} < \mathrm{lh}(\boldsymbol{\tau}) \wedge \mathbf{n} < \mathrm{lh}(\boldsymbol{\tau})$, y como $\mathfrak{M} \vDash \boldsymbol{\tau} \in \mathbf{T}$ se tiene que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{m}) = \mathbf{n} \leftrightarrow \boldsymbol{\sigma}(\mathbf{n}) = \boldsymbol{\tau}(\mathbf{n}) = \mathbf{m} + 1$.

⟨3⟩4. $\mathfrak{M} \vDash \forall n < \mathrm{lh}(\boldsymbol{\sigma}).\boldsymbol{\sigma}(n) > 0 \rightarrow \mathbf{f}(\boldsymbol{\sigma}(n) - 1) = n)$.
DEMOSTRACIÓN: Sea $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{n} < \mathrm{lh}(\boldsymbol{\sigma}) \wedge \boldsymbol{\sigma}(\mathbf{n}) > 0$. Como $\mathfrak{M} \vDash \boldsymbol{\sigma} \subseteq \boldsymbol{\tau}$ tenemos que $\mathfrak{M} \vDash \mathbf{n} < \mathrm{lh}(\boldsymbol{\tau}) \wedge \boldsymbol{\tau}(\mathbf{n}) > 0$, y como $\mathfrak{M} \vDash \boldsymbol{\tau} \in \mathbf{T}$ tenemos que $\mathfrak{M} \vDash \mathbf{f}(\boldsymbol{\sigma}(\mathbf{n}) - 1) = \mathbf{f}(\boldsymbol{\tau}(\mathbf{n}) - 1) = \mathbf{n}$.

⟨3⟩5. Q.E.D.
DEMOSTRACIÓN: De ⟨3⟩2,⟨3⟩3,⟨3⟩4 tenemos que $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbf{T}$.

⟨2⟩3. Q.E.D.

DEMOSTRACIÓN: ⟨2⟩1 y ⟨2⟩2 son las dos condiciones para ser un árbol.

⟨1⟩4. $\mathfrak{M} \vDash$ 2-ARY[$\mathbf{T}$].

DEMOSTRACIÓN: Dado $\boldsymbol{\tau} \in \mathbf{T}$, sabemos que a lo más existe un único $\mathbf{m}$ tal que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{m}) = \mathrm{lh}(\boldsymbol{\tau})$, pues por ⟨1⟩1 $\mathfrak{M} \vDash$ INY[$\mathbf{f}$]. Sea $\mathbf{m}$ ese tal $\mathbf{m}$ si existe y si no, 0. Veamos que $\mathfrak{M} \vDash \forall n.\boldsymbol{\tau}^\frown\langle n\rangle \in \mathbf{T} \rightarrow n = 0 \vee n = \mathbf{m}$, por lo que $\mathfrak{M} \vDash$ 2-ARY[$\mathbf{T}$]. Sea entonces $\mathbf{n}$ tal que $\mathfrak{M} \vDash \boldsymbol{\tau}^\frown\langle \mathbf{n}\rangle \in \mathbf{T}$, si $\mathfrak{M} \vDash \mathbf{n} = 0$ hemos terminado y si no, por definición de $\mathbf{T}$ tenemos que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{n}) = \mathrm{lh}(\boldsymbol{\tau}) = \mathbf{f}(\mathbf{m})$ y por ser inyectiva $\mathfrak{M} \vDash \mathbf{n} = \mathbf{m}$.

⟨1⟩5. $\mathfrak{M} \vDash$ INFSET[$\mathbf{T}$].

⟨2⟩1. Sea $\mathbf{k} \in \mathbb{N}$.

⟨2⟩2. Existe $\mathbf{Y} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \mathbf{Y} = \{n \mid n < \mathbf{k} \wedge \exists m.\mathbf{f}(m) = n\}$.
DEMOSTRACIÓN: Por Σ^0_1-BCOMP.

⟨2⟩3. Existe $\boldsymbol{\sigma} \in \mathbb{N}$ tal que
$\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbb{N}^{\mathbf{k}} \wedge \forall n < \mathbf{k}.(n \notin \mathbf{Y} \rightarrow \boldsymbol{\sigma}(n) = 0) \wedge (\forall m.n \in \mathbf{Y} \wedge \mathbf{f}(m) = n \rightarrow \boldsymbol{\sigma}(n) = m+1)$.
DEMOSTRACIÓN: Por Σ^0_0-COMP existe un conjunto $\mathbf{f}$ tal que
$$\mathfrak{M} \vDash \{(n, m) \mid (n < \mathbf{k} \wedge n \notin \mathbf{Y} \wedge m = 0) \vee (n \in \mathbf{Y} \wedge \mathbf{f}(m - 1) = n)\}.$$
Que define una función se sigue de la definición de $\mathbf{Y}$ en ⟨2⟩2 y de que por ⟨1⟩1 $\mathbf{f}$ es inyectiva. Es fácil comprobar que cumple las condiciones.

⟨2⟩4. $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbf{T}$.

⟨3⟩1. $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbb{N}^{<\mathbb{N}}$.
DEMOSTRACIÓN: Pues $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbb{N}^{\mathbf{k}}$.

⟨3⟩2. $\mathfrak{M} \vDash \forall m, n < \mathbf{k}.\mathbf{f}(m) = n \leftrightarrow \boldsymbol{\sigma}(n) = m + 1$.
DEMOSTRACIÓN: Sean $\mathbf{m}, \mathbf{n} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{n} < \mathbf{k} \wedge \mathbf{m} < \mathbf{k}$.
Si $\mathfrak{M} \vDash \mathbf{f}(\mathbf{m}) = \mathbf{n}$ entonces $\mathfrak{M} \vDash \mathbf{n} \in \mathbf{Y}$ y por tanto $\mathfrak{M} \vDash \boldsymbol{\sigma}(\mathbf{n}) = \mathbf{m} + 1$.

Si $\mathfrak{M} \vDash \boldsymbol{\sigma}(\mathbf{n}) = \mathbf{m} + 1$, por definición de $\boldsymbol{\sigma}$ tenemos que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{m}) = \mathbf{n}$, como queríamos.

⟨3⟩3. $\mathfrak{M} \vDash \forall n < \mathbf{k}.\boldsymbol{\sigma}(n) > 0 \to \mathbf{f}(\boldsymbol{\sigma}(n) - 1) = n$.
DEMOSTRACIÓN: Sea $\mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{n} < \mathbf{k} \wedge \boldsymbol{\sigma}(\mathbf{n}) > 0$, por tanto $\mathfrak{M} \vDash \mathbf{n} \in \mathbf{Y}$, así existe $\mathbf{m} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{f}(\mathbf{m}) = \mathbf{n}$ y por definición de $\boldsymbol{\sigma}$, $\mathfrak{M} \vDash \boldsymbol{\sigma}(\mathbf{n}) = \mathbf{m} + 1$.

⟨3⟩4. Q.E.D.

⟨2⟩5. Q.E.D.

DEMOSTRACIÓN: Esta claro que $\mathfrak{M} \vDash \boldsymbol{\sigma} \geq \mathbf{k}$ pues $\mathfrak{M} \vDash \boldsymbol{\sigma} \in \mathbb{N}^{\mathbf{k}}$ y por ⟨2⟩4 tenemos lo pedido.

⟨1⟩6. Existe $\mathbf{g} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \textsc{Path}[\mathbf{g}, \mathbf{T}] \wedge (\forall m, n.\mathbf{f}(m) = n \leftrightarrow \mathbf{g}(n) = m + 1)$.

DEMOSTRACIÓN: Gracias a que $\mathfrak{M} \vDash$ KÖNIG2 y a ⟨1⟩3,⟨1⟩4 y ⟨1⟩5 tenemos la existencia del camino, por la definición de $\mathbf{T}$ en ⟨1⟩2 tenemos que cumple la propiedad.

⟨1⟩7. Q.E.D.

DEMOSTRACIÓN: Por Σ^0_1-COMP existe $\mathbf{X} \in \wp(\mathbb{N})$ tal que
$$\mathfrak{M} \vDash \mathbf{X} = \{n \mid \mathbf{g}(n) > 0\}.$$
Por ⟨1⟩6 se tiene que $\mathfrak{M} \vDash \forall n.(\exists m.\mathbf{f}(m) = n) \leftrightarrow n \in \mathbf{X}$.

□

Reuniendo todos los resultados en un teorema nos queda que:

Teorema 4.17. *En RCA_0 se demuestran equivalentes:*

1. *ACA_0.*
2. *KÖNIG.*
3. *KÖNIG2.*

DEMOSTRACIÓN: Basta con aplicar los lemas 4.14, 4.15 y 4.16. □

Nota. Como consecuencia directa del teorema anterior, se obtiene que ACA_0 demuestra el lema débil de Köning y, por tanto, ACA_0 extiende a la teoría WKL_0. Obtenemos pues:

$$\mathrm{RCA}_0 \subset \mathrm{WKL}_0 \subset \mathrm{ACA}_0$$

Además, es bien conocido que cada una de las inclusiones anteriores es estricta y que las tres teorías pueden separarse por ω-modelos. Esto es, existen $S_1, S_2 \subset \wp(\omega)$ tales que

$$(\omega, S_1, +, \cdot, 0, 1, <) \models \mathrm{RCA}_0 + \neg\, \mathrm{WKL}_0$$
$$(\omega, S_2, +, \cdot, 0, 1, <) \models \mathrm{WKL}_0 + \neg\, \mathrm{ACA}_0$$

De hecho, como S_1 basta tomar la clase $REC \subset \wp(\omega)$ formada por todos los subconjuntos computables de ω. (Para describir S_2 serían necesarias nociones de la teoría de la computalidad que exceden los contenidos de la presente memoria.) ■

4.2.2. Teorema de Ramsey

En esta sección discutiremos la matemática inversa del teorema de Ramsey, un resultado fundamental en el campo de la combinatoria.

Introducimos algunas definiciones que nos serán útiles para el teorema.

Lema 4.18. $RCA_0 \vdash \forall k \forall X \exists Y^1 . Y = \{s \mid s \in X^k \wedge \forall j < k \forall i < j . s(i) < s(j)\}$.

A ese único conjunto lo llamamos $[X]^k$.

Demostración: La existencia es por Σ^0_0-COMP y la unicidad es por la definición de igualdad de conjuntos. □

Entendemos el conjunto $[X]^k$ como los subconjuntos de X de tamaño k, ya que cada sucesión creciente de longitud k representa el conjunto de los elementos de la sucesión. Además cada uno de esos conjuntos tendrá "cardinalidad" k por ser la sucesión creciente.

Definición 4.6 (**El teorema de Ramsey para k-tuplas**)**.** Definimos la fórmula:

$$\mathrm{RT}[k] :\equiv \forall l \in \mathbb{N}^+ \forall f : [\mathbb{N}]^k \longrightarrow \{0, \ldots, l-1\} \exists i < l \exists X \subseteq \mathbb{N}.$$
$$\textsc{InfSet}[X] \wedge \forall \langle m_1, \ldots, m_k \rangle \in [X]^k . f(m_1, \ldots, m_k) = i.$$

■

Si entendemos el conjunto $\{0, \ldots, l-1\}$ como "colores", el teorema de Ramsey nos dice que, dada una coloración de los subconjuntos de $\mathbb{N}$ de tamaño k, existe un subconjunto infinito H de $\mathbb{N}$ tal que todos los subconjuntos tamaño k formados por elementos de H tienen el mismo color. En la literatura es común encontrarse la notación RT^k_l, que representa el teorema de Ramsey para conjuntos de cardinalidad k y l colores. Aquí nos centraremos en la matemática inversa de $\mathrm{RT}[k]$. Esto no es una omisión importante, pues es bien conocido que, fijado un k, los principios RT^k_l resultan equivalentes entre sí al variar el número de colores $l \geq 2$.

Lema 4.19. $ACA_0 \vdash RT[0] \wedge \forall k.RT[k] \to RT[k+1]$.

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de ACA_0.

⟨1⟩2. $\mathfrak{M} \vDash \mathrm{RT}[0]$.

Demostración: Trivial, pues $\mathbf{f}$ es una función cuyo dominio tiene un único elemento, $\langle\rangle$. Basta tomar $i = \mathbf{f}(\langle\rangle)$ y $X = \mathbb{N}$ y se cumple.

⟨1⟩3. $\mathfrak{M} \vDash \forall k.\mathrm{RT}[k] \to \mathrm{RT}[k+1]$

⟨2⟩1. Sea $\mathbf{k} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathrm{RT}[\mathbf{k}]$. Sean $\mathbf{l} \in \mathbb{N}^+$ y $\mathbf{f} \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \mathbf{f} : [\mathbb{N}]^{\mathbf{k}+1} \longrightarrow \{0, \ldots, \mathbf{l}-1\}$.

⟨2⟩2. Definimos la fórmula

$$\begin{gathered}\varphi[t,n,j] :\equiv (\forall m < n.t(m) < j) \wedge \\ \forall m \leq n \forall \langle m_1, \ldots, m_{\mathbf{k}}\rangle \in [\{0, \ldots, m-1\}]^{\mathbf{k}}. \\ \mathbf{f}(t(m_1), \ldots, t(m_{\mathbf{k}}), j) = \mathbf{f}(t(m_1), \ldots, t(m_{\mathbf{k}}), t(m)).\end{gathered}$$

⟨2⟩3. Existe $\mathbf{T} \in \wp(\mathbb{N})$, tal que

$$\mathfrak{M} \vDash \mathbf{T} = \{t \mid t \in \mathbb{N}^{<\mathbb{N}} \wedge \forall n < \mathrm{lh}(t).\varphi[t,n,t(n)] \wedge \neg\exists j < t(n).\varphi[t,n,j]\}.$$

Demostración: Existe por Σ^0_0-COMP.

⟨2⟩4. $\mathfrak{M} \vDash \textsc{Tree}[\mathbf{T}]$.

Demostración: Se comprueba sin dificultad.

⟨2⟩5. $\mathfrak{M} \vDash \textsc{FinBran}[\mathbf{T}]$.

⟨3⟩1. Sean $\mathbf{t}, \mathbf{n} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{t} \in \mathbf{T} \wedge \mathrm{lh}(\mathbf{t}) = \mathbf{n}$.

⟨3⟩2. Existen $\mathbf{X}, \mathbf{Y} \in \wp(\mathbb{N})$ tales que

$$\mathfrak{M} \vDash \mathbf{X} = \{m \mid \exists n < \mathrm{lh}(\mathbf{t}).\mathbf{t}(n) = m\},$$
$$\mathfrak{M} \vDash \mathbf{Y} = \{j \mid \mathbf{t}^\frown j \in \mathbf{T}\}.$$

Queremos probar que $\mathfrak{M} \vDash \textsc{FinSet}[\mathbf{Y}]$.
Demostración: Por Σ^1_0-COMP.

⟨3⟩3. $\mathfrak{M} \vDash \textsc{FinSet}[[\mathbf{X}]^{\mathbf{k}}]$.
Demostración: Se tiene que $\mathfrak{M} \vDash \textsc{FinSet}[\mathbf{X}]$, pues todo elemento suyo será menor o igual que $\mathbf{t}$. Por tanto, $\mathfrak{M} \vDash \textsc{FinSet}[\mathbf{X}^{\mathbf{k}}]$ por el lema 2.52. Como $\mathfrak{M} \vDash [\mathbf{X}]^{\mathbf{k}} \subseteq [\mathbf{X}^{\mathbf{k}}]$, tenemos lo pedido (usando lema 2.40).

⟨3⟩4. Q.E.D.
Demostración: Como $[\mathbf{X}]^{\mathbf{k}}$ y $\{0, \ldots, \mathbf{l}-1\}$ son conjuntos finitos, tendremos que el conjunto de funciones $[\mathbf{X}]^{\mathbf{k}} \longrightarrow \{0, \ldots, \mathbf{l}\}$ será finito, y por tanto podremos definir una función de ese conjunto en $\mathbf{Y}$, pues fijada una función de esas existe a lo sumo un $\mathbf{j}$ tal que $\mathfrak{M} \vDash \mathbf{t}^\frown\langle\mathbf{j}\rangle \in \mathbf{T}$, por ser un mínimo. Así podemos definir la función que toma ese $\mathbf{j}$ si existe o da 0 si no existe. Como el dominio de la función era finito, también lo será su imagen, que era lo que queríamos.

⟨2⟩6. $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{T}]$.

⟨3⟩1. Es suficiente probar que $\mathfrak{M} \vDash \forall j \exists s \in \mathbf{T} \exists n < \mathrm{lh}(s).s(n) = j$.
DEMOSTRACIÓN: Ya que, en tal caso, dado $\mathbf{j} \in \mathbb{N}$, existe $\mathbf{s} \in \mathbf{T}$ y $\mathbf{n} \in \mathbb{N}$ tales que $\mathfrak{M} \vDash \mathbf{s}(\mathbf{n}) = \mathbf{j}$ y por tanto $\mathfrak{M} \vDash \mathbf{j} \leq \langle \mathbf{n}, \mathbf{j} \rangle \leq \mathbf{s}$ (siendo la última desigualdad cierta por $\mathfrak{M} \vDash \langle \mathbf{n}, \mathbf{j} \rangle \in \mathbf{s}$). Por tanto $\mathfrak{M} \vDash \forall j \exists s \geq j.s \in \mathbf{T}$, como queríamos.

⟨3⟩2. Sea $\mathbf{j} \in \mathbb{N}$.

⟨3⟩3. Existe $\mathbf{t} \in \mathbb{N}$ tal que
$$\mathfrak{M} \vDash \mathbf{t} \in \mathbf{T} \wedge \varphi[\mathbf{t}, \mathrm{lh}(\mathbf{t}), \mathbf{j}] \wedge \neg \exists s \in \mathbf{T}.s \supset \mathbf{t} \wedge \varphi[s, \mathrm{lh}(s), \mathbf{j}].$$
DEMOSTRACIÓN: Que existe algún $\mathbf{t}$ es trivial ($\langle\rangle$ vale); que existe uno maximal se sigue argumentando por reducción al absurdo.

⟨3⟩4. $\mathfrak{M} \vDash \mathbf{t}^\frown\langle \mathbf{j} \rangle \in \mathbf{T}$.
DEMOSTRACIÓN: Por la definición de $\mathbf{T}$ en ⟨2⟩3.

⟨3⟩5. Q.E.D.
DEMOSTRACIÓN: Por ⟨3⟩4 hemos probado ⟨3⟩1 que era suficiente.

⟨2⟩7. Existe $\mathbf{g} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \textsc{Path}[\mathbf{g}, \mathbf{T}]$.

DEMOSTRACIÓN: Por ⟨2⟩4,⟨2⟩5 y ⟨2⟩6 usando el lema de König.

⟨2⟩8. Existe $\mathbf{f}' \in \wp(\mathbb{N})$ tal que
$$\mathfrak{M} \vDash \mathbf{f}' : [\mathbb{N}]^{\mathbf{k}} \longrightarrow \{0, \ldots, \mathbf{l} - 1\} \forall m \forall \langle m_1, \ldots, m_{\mathbf{k}} \rangle \in [\{0, \ldots, m - 1\}]^{\mathbf{k}}.$$
$$\mathbf{f}'(m_1, \ldots, m_{\mathbf{k}}) = f(\mathbf{g}(m_1), \ldots, \mathbf{g}(m_{\mathbf{k}}), \mathbf{g}(m)).$$
DEMOSTRACIÓN: Tan solo hay que notar dos cosas, por la definición de $\mathbf{T}$ en ⟨2⟩3 $\mathbf{g}$ es estrictamente creciente, por tanto efectivamente $\mathbf{g}(m_1), \ldots, \mathbf{g}(m_{\mathbf{k}}), \mathbf{g}(m) \in [\mathbb{N}]^{\mathbf{k}+1}$ y además $\mathbf{f}$ no depende del m, por tanto $\mathbf{f}'$ bien definida.

⟨2⟩9. Q.E.D.

DEMOSTRACIÓN: Por ⟨2⟩1, $\mathfrak{M} \vDash \mathrm{RT}[\mathbf{k}]$, así que existen $\mathbf{i} \in \mathbb{N}$ y $\mathbf{X}' \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash \mathbf{i} < \mathbf{l} \wedge \textsc{InfSet}[\mathbf{X}'] \wedge \forall \langle m_1, \ldots, m_{\mathbf{k}} \rangle \in [\mathbf{X}']^{\mathbf{k}}.\mathbf{f}(m_1, \ldots, m_{\mathbf{k}}) = \mathbf{i}$. Así llamando $\mathbf{X} = \{\mathbf{g}(m) \mid m \in \mathbf{X}'\}$ (que existe porque estamos en ACA_0), tenemos que $\mathfrak{M} \vDash \forall \langle m_1, \ldots, m_{\mathbf{k}}, m \rangle \in [\mathbf{X}]^{(\mathbf{k}+1)}.\mathbf{f}(m_1, \ldots, m_{\mathbf{k}}, m) = \mathbf{i}$, como queríamos.

⟨1⟩4. Q.E.D.

□

Corolario 4.20. *Dado $k \in \omega$, $ACA_0 \vdash RT[k]$.*

DEMOSTRACIÓN: Usando el lema 4.19 e inducción **en la metateoría** (no en ACA_0). □

Notemos que con esto no hemos probado que $\mathrm{ACA}_0 \vdash \forall k.\mathrm{RT}[k]$; para esto sería necesario poder aplicar inducción en $\mathrm{RT}[k]$ en la teoría. Sin embargo esto no es posible, ya que $\mathrm{RT}[k]$ no es una fórmula aritmética.

Para la dirección inversa solo necesitamos RT[3].

Lema 4.21. *$RCA_0 + RT[3] \vdash ACA_0$.*

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de $\mathrm{RCA}_0 + \mathrm{RT}[3]$.

⟨1⟩2. $\mathfrak{M} \vDash \Sigma^0_1$-COMP.

Demostración:
⟨2⟩1. Sean $k \in \mathrm{Var_N}, X \in \mathrm{Var_C}$ y $\varphi\{k\} \in \Sigma^0_1$ tal que $X \notin \mathrm{Vl}(\varphi\{k\})$ y $\{\nu_1, \ldots, \nu_r\} = \mathrm{Vl}(\varphi\{k\}) \setminus \{k\}$.

⟨2⟩2. Definimos $\psi :\equiv \exists X \forall k. k \in X \leftrightarrow \varphi\{k\}$.

⟨2⟩3. Sean $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r \in \mathbb{N} \cup \wp(\mathbb{N})$ y llamemos $\varphi[k] :\equiv \varphi(k, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r)$. Entonces tenemos que
$$\boldsymbol{\psi} :\equiv \psi[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r] \equiv \exists X \forall k. k \in X \leftrightarrow \varphi[k].$$
y es sufciente probar que $\mathfrak{M} \vDash \boldsymbol{\psi}$.

⟨2⟩4. Existe $\theta[m, n] \in (\Sigma^0_0)_{\mathfrak{M}}$ tal que $\varphi[m] \equiv \exists n. \theta[m, n]$.
Demostración: Por ⟨2⟩1 $\varphi\{k\} \in \Sigma^0_1$, por tanto $\varphi[k] \in (\Sigma^0_1)_{\mathfrak{M}}$.

⟨2⟩5. Existe $\mathbf{f} : [\mathbb{N}]^3 \longrightarrow \{0, 1\}$ tal que
$\mathfrak{M} \vDash \forall \langle a, b, c\rangle \in [\mathbb{N}]^3. \mathbf{f}(a, b, c) = 1 \leftrightarrow \forall m < a. (\exists n < b. \theta[m, n]) \leftrightarrow (\exists n < c. \theta[m, n])$.
Demostración: Por Σ^0_0-COMP.

⟨2⟩6. Existe $\mathbf{i} \in \mathbb{N}, \mathbf{X} \in \wp(\mathbb{N})$ tal que
$$\mathfrak{M} \vDash \mathbf{i} < 2 \wedge \textsc{InfSet}[\mathbf{X}] \wedge \forall \langle a, b, c\rangle \in [\mathbf{X}]^3. \mathbf{f}(a, b, c) = \mathbf{i}.$$
Demostración: Por Rt[3].

⟨2⟩7. $\mathfrak{M} \vDash \mathbf{i} = 1$.

⟨3⟩1. Es suficiente probar que $\mathfrak{M} \vDash \exists \langle a, b, c\rangle \in [\mathbf{X}]^3. \mathbf{f}(a, b, c) = 1$.
Demostración: Por ⟨2⟩6, si tiene ese valor en una tupla lo tendrá en todas.

⟨3⟩2. Sea $\mathbf{a} \in \mathbf{X}$.

⟨3⟩3. Existe $\wp(\mathbf{Y})$ tal que $\mathfrak{M} \vDash \mathbf{Y} = \{m \mid m < \mathbf{a} \wedge \exists n. \theta[m, n]\}$.
Demostración: Σ^0_1-BCOMP.

⟨3⟩4. $\mathfrak{M} \vDash \forall j \exists k \forall m < j. m \in \mathbf{Y} \rightarrow \exists n < k. \theta[m, n]$.
Demostración: Por Σ^0_1-COMP.

⟨3⟩5. Existe $\mathbf{k}$ tal que $\mathfrak{M} \vDash \forall m. m \in \mathbf{Y} \rightarrow \exists n < \mathbf{k}. \theta[m, n]$.
Demostración: Por ⟨3⟩3 tomando $j = \mathbf{a}$.

⟨3⟩6. Q.E.D.
Demostración: Por ⟨2⟩6 $\mathfrak{M} \vDash \textsc{InfSet}[\mathbf{X}]$ existen $\mathbf{b}, \mathbf{c}$ tales que
$$\mathfrak{M} \vDash \mathbf{b} \in \mathbf{X} \wedge \mathbf{c} \in \mathbf{X} \wedge \mathbf{a} < \mathbf{b} < \mathbf{c} \wedge \mathbf{k} \leq \mathbf{b}.$$
Por tanto $\mathfrak{M} \vDash \langle \mathbf{a}, \mathbf{b}, \mathbf{c}\rangle \in [\mathbf{X}]^3$ y por ⟨2⟩5, ⟨3⟩5 (usando que $\mathfrak{M} \vDash \mathbf{k} \leq \mathbf{b}$) tenemos $\mathfrak{M} \vDash \mathbf{f}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = 1$.

⟨2⟩8. $\mathfrak{M} \vDash (\exists n.\theta[m,n]) \leftrightarrow (\forall a, b.a \in \mathbf{X} \wedge b \in \mathbf{X} \wedge m < a < b \rightarrow \exists n < b.\theta[m,n])$.

DEMOSTRACIÓN: Como $\mathfrak{M} \vDash$ InfSet$[\mathbf{X}]$ tenemos $\leftarrow$, veamos $\rightarrow$. Sea $\mathbf{n}$ tal que $\mathfrak{M} \vDash \theta[\mathbf{m}, \mathbf{n}]$, entonces como $\mathfrak{M} \vDash$ InfSet$[\mathbf{X}]$ tenemos que existe $\mathbf{c} \in \mathbb{N}$ tal que $\mathfrak{M} \vDash \mathbf{n} < \mathbf{c} \wedge \mathbf{b} < \mathbf{c} \wedge \mathbf{c} \in \mathbf{X}$. Por tanto $\mathfrak{M} \vDash \mathbf{f}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = 1$ por ⟨2⟩7, y por la definición de $\mathbf{f}$ en ⟨2⟩5 $\mathfrak{M} \vDash \forall m < \mathbf{a}.(\exists n < \mathbf{b}.\theta[m,n]) \leftrightarrow (\exists n < \mathbf{c}.\theta[m,n])$. Como $\mathfrak{M} \vDash \exists n < \mathbf{c}.\theta[m,n]$ y $\mathfrak{M} \vDash \mathbf{m} < \mathbf{a}$ tenemos lo pedido.

⟨2⟩9. Q.E.D.

DEMOSTRACIÓN: Por Δ^0_1-COMP en ⟨2⟩8 existe el conjunto.

⟨1⟩3. Q.E.D.

DEMOSTRACIÓN: Por ⟨1⟩2 y 4.3.

□

Con esto ya tenemos las dos direcciones para establecer equivalencias.

Teorema 4.22. *Para cualquiera $k \in \omega, k \geq 3$, RCA_0 demuestra equivalentes:*

1. *ACA_0.*
2. *$RT[k]$.*

DEMOSTRACIÓN: Por los lemas 4.19 y 4.21. □

Nota (Ramsey para pares RT^2_2)**.** Por completitud, vamos a hablar un poco de qué sucede con RT^k_l en general, sin entrar en detalles. En Hirschfeldt [3] en el capítulo 6 se menciona que únicamente hay que considerar los siguientes casos del teorema de Ramsey (los otros se prueban equivalentes a uno de estos):

1. RT^2_2.
2. $\mathrm{RT}[k]$ con $k \geq 1$.
3. $\mathrm{RT} :\equiv \forall k \geq 1.\mathrm{RT}[k]$.

Aquí hemos desarrollado el segundo caso (aunque no al completo, pues sólo hemos conseguido la equivalencia con ACA_0 para $k \geq 3$). Los otros dos casos son curiosos, ambos se salen de los Big Five.

Por una parte, se puede demostrar que $\mathrm{ACA}_0 \nvdash \mathrm{RT}$. De hecho, RT será equivalente sobre RCA_0 a ACA'_0, un subsistema de Z_2 que es estrictamente más fuerte que ACA_0.

Por otro lado, el caso de RT^2_2 ha sido más complicado de resolver, pese a iniciarse su estudio en 1971. De hecho, determinar la potencia lógica del teorema de Ramsey para pares RT^2_2 ha sido uno de los principales problemas abiertos en el campo de la matemática inversa en los últimos años. En la actualidad, con los resultados de Specker 1971, Seetapun-Slaman 1995, Jockusch 1972 y Liu 2012, se tiene ya un conocimiento decente de la potencia de dicho principio. Se sabe que RT^2_2 se sitúa estrictamente entre las teorías RCA_0 y ACA_0; y resulta incomparable con la teoría WKL_0, esto es, ni WKL_0 implica RT^2_2 ni RT^2_2 implica WKL_0. Además, se sabe que RT^2_2 demuestra el esquema de Σ^0_2-$BOUND$ (Hirst 1987) pero no demuestra el esquema de Σ^0_2-IND (Chong-Slaman-Yang 2017). ■

4.3. Otros resultados de la matemática inversa de ACA_0

Como está siendo habitual, cerramos el capítulo con una recopilación informativa de más teoremas equivalentes a ACA_0 sobre RCA_0, para que el lector pueda hacerse una idea de la relevancia de la teoría ACA_0 en el campo de la matemática inversa. De nuevo, no haremos la demostración (ni las codificaciones adicionales necesarias) y remitimos al lector al capítulo III del libro de Simpson [8].

Teorema 4.23. *En RCA_0 son equivalentes*

1. *ACA_0.*
2. *(**Existencia de ideal maximal, I**) Todo anillo conmutativo numerable tiene un ideal maximal.*
3. *(**Existencia de ideal maximal, II**) Todo dominio de integridad numerable tiene un ideal maximal.*
4. *(**Subgrupo de torsión**) Todo grupo abeliano numerable posee un subgrupo formado por los elementos con torsión.*
5. *(**Existencia de base en e.v.**) Todo espacio vectorial numerable sobre un cuerpo numerable tiene una base.*
6. *(**Existencia de base de trascendencia**) Todo cuerpo numerable (de característica 0) tiene una base de trascendencia.*

Capítulo 5

$\mathbf{ATR_0}$ y $\mathbf{\Pi^1_1}$-$\mathbf{CA_0}$

Por completitud, en este capítulo definiremos los otros dos subsistemas de la aritmética de segundo orden más importantes: ATR_0 y Π^1_1-CA_0, aunque no vayamos a hablar mucho de ellos. Con esto, y junto con los sistemas RCA_0, WKL_0 y ACA_0 que hemos estudiado en capítulos anteriores, ya hemos definido los Big Five.

5.1. $\mathbf{ATR_0}$

Trataremos en primer lugar la teoría ATR_0, que es algo más complicada de definir que el resto de subsistemas. Intuitivamente, ATR_0 extiende la teoría ACA_0 con un principio de recursión aritmética transfinita (*Arithmetical Transfinte Recursion*). Es por ello que, en primer lugar, necesitaremos algunas definiciones sobre buenos órdenes en el lenguaje de la aritmética.

Definición 5.1 (**Relaciones reflexivas**)**.** Introducimos algunas definiciones:

$$\textsc{Refl}[X] :\equiv X \subseteq \mathbb{N} \times \mathbb{N} \wedge \forall i, j.(i, j) \in X \to (i, i) \in X \wedge (j, j) \in X.$$

$$i \leq_X j :\equiv \textsc{Refl}[X] \wedge (i, j) \in X.$$

$$i <_X j :\equiv \textsc{Refl}[X] \wedge (i, j) \in X \wedge (j, i) \notin X.$$

■

Teorema 5.1.

$$RCA_0 \vdash \forall X.\textsc{Refl}[X] \to \exists^1 Y.Y = \{i \mid (i,i) \in X\}.$$

A ese conjunto único lo llamamos $\mathrm{fd}(X)$*. Además notemos que* RCA_0 *prueba que la fórmula* $i \in \mathrm{fd}(X)$ *es equivalente a una fórmula* Σ^0_0*.*

Demostración: La existencia es por Σ^0_0-comprensión, la unicidad por la igualdad de conjuntos, y la equivalencia porque RCA_0 prueba que $i \in \mathrm{fd}(X) \leftrightarrow (i,i) \in X$.

□

Definición 5.2 (**Órdenes bien fundamentados, órdenes lineales y buenos órdenes numerables**)**.** Definimos

$$\textsc{Wf}[X] :\equiv \textsc{Refl}[X] \wedge \neg\exists f : \mathbb{N} \longrightarrow \mathrm{fd}(X) \forall n.f(n+1) <_X f(n).$$

$$\textsc{Lo}[X] :\equiv \textsc{Refl}[X] \wedge (\forall i,j,k.i \leq_X j \wedge j \leq_X k \to i \leq_X k) \wedge$$
$$(\forall i,j.i \leq_X j \wedge j \leq_X i \to i = j) \wedge (\forall i,j \in \mathrm{fd}(X).i \leq_X j \vee j \leq_X i).$$

$$\textsc{Wo}[X] :\equiv \textsc{Wf}[X] \wedge \textsc{Lo}[X].$$

■

Nótese que la fórmula que expresa que X es un buen orden numerable, $\textsc{Wo}[X]$, es una fórmula de complejidad Π^1_1 con un único parámetro X.

En la práctica matemática habitual, una propiedad fundamental de los buenos órdenes es que es posible desarrollar demostraciones mediante inducción transfinita sobre un buen orden dado. Es decir, si X es un buen orden numerable y queremos obtener que una cierta propiedad $\varphi(j)$ se cumple para todo $x \in \mathrm{fd}(X)$, un método de prueba válido es suponer $\varphi(i)$ para todo $i <_X j$ y deducir $\varphi(j)$. El siguiente teorema muestra que este principio de inducción es aún demostrable en la teoría ACA_0 siempre que la fórmula $\varphi(j)$ sea aritmética (a diferencia del principio de *recursión* aritmética transfinita, que ya no es demostrable en ACA_0 y dará lugar a la nueva teoría ATR_0).

Teorema 5.2 (**Inducción aritmética transfinita**)**.** *Sea* $\varphi\{i\} \in \Sigma^1_0$ *tal que* $j \notin \mathrm{Vl}(\varphi)$*. Entonces tenemos que:*

$$ACA_0 \vdash \forall X.(\textsc{Wo}[X] \wedge \forall j \in \mathrm{fd}(X).(\forall i \in \mathrm{fd}(X).i <_X j \to \varphi\{i\}) \to \varphi\{j\}) \to \forall j \in \mathrm{fd}(X).\varphi\{j\}.$$

Demostración:
⟨1⟩1. Sea $\varphi(x, \nu_1, \ldots, \nu_k) \in \Sigma^1_0$ donde $\nu_1, \ldots, \nu_k \in \mathrm{Vl}(\varphi) \setminus \{x\}$ con $i, j \notin \mathrm{Vl}(\varphi)$.

⟨1⟩2. Sea $\mathfrak{M}$ un modelo de ACA$_0$ y sean $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k \in \mathbb{N} \cup \wp(\mathbb{N})$, donde denotamos $\varphi(x) :\equiv \varphi(x, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_k)$.

⟨1⟩3. Sea $\mathbf{X} \in \wp(\mathbb{N})$ tal que
$$\mathfrak{M} \vDash \mathrm{Wo}[\mathbf{X}] \wedge \forall j \in \mathrm{fd}(\mathbf{X}).(\forall i \in \mathrm{fd}(\mathbf{X}).i <_{\mathbf{X}} j \to \varphi(i)) \to \varphi(j).$$

⟨1⟩4. Existe $\mathbf{Y} \in \wp(\mathbb{N})$ tal que $\mathfrak{M} \vDash \forall i.i \in \mathbf{Y} \leftrightarrow i \in \mathrm{fd}(\mathbf{X}) \wedge \neg\varphi(i)$.

Demostración: Por Σ^1_0-comprensión.

⟨1⟩5. $\mathfrak{M} \vDash \forall j \in \mathbf{Y} \exists i \in \mathbf{Y}.i <_{\mathbf{X}} j$.

Demostración: Supongamos lo contrario, i.e. sea $\mathbf{j} \in \mathbf{Y}$ tal que $\mathfrak{M} \vDash \forall i \in \mathbf{Y}.\mathbf{j} \leq_{\mathbf{X}} i$. Sea entonces $\mathbf{i} \in \mathrm{fd}(\mathbf{X})$ tal que $\mathfrak{M} \vDash \mathbf{i} <_{\mathbf{X}} \mathbf{j}$. Por lo anterior, $\mathfrak{M} \vDash \mathbf{i} \notin \mathbf{Y}$ y, por tanto, por definición de $\mathbf{Y}$, $\mathfrak{M} \vDash \varphi(\mathbf{i})$. Hemos probado así que $\mathfrak{M} \vDash \forall i \in \mathrm{fd}(\mathbf{X}).i <_{\mathbf{X}} \mathbf{j} \to \varphi(i)$ y de ⟨1⟩3 obtenemos que $\mathfrak{M} \vDash \varphi(\mathbf{j})$. Otra vez por definición de $\mathbf{Y}$, tenemos que $\mathfrak{M} \vDash \mathbf{j} \notin \mathbf{Y}$, absurdo.

⟨1⟩6. Si $\mathfrak{M} \vDash \mathbf{Y} \neq \varnothing$ entonces existe $\mathbf{f} : \mathbb{N} \longrightarrow \mathrm{fd}(\mathbf{X})$ tal que $\mathfrak{M} \vDash \forall n.\mathbf{f}(n+1) <_{\mathbf{X}} \mathbf{f}(n)$.

Demostración: Por hipótesis $\mathfrak{M} \vDash \exists i \in \mathbf{Y}$, por tanto, por recursión, podemos definir $\mathbf{f}(0) = \mu i.i \in \mathbf{Y}$ y por ⟨1⟩5 es correcta la definición de $\mathbf{f}(n+1) = \mu i.i <_{\mathbf{X}} \mathbf{f}(n)$.

⟨1⟩7. Q.E.D.

Demostración: Por ⟨1⟩6, si $\mathfrak{M} \vDash \mathbf{Y} \neq \varnothing$ entonces tenemos un absurdo con la hipótesis de que $\mathfrak{M} \vDash \mathrm{Wf}[\mathbf{X}]$ ya que por ⟨1⟩3, $\mathfrak{M} \vDash \mathrm{Wo}[\mathbf{X}]$. Por tanto, $\mathfrak{M} \vDash \mathbf{Y} = \varnothing$, de donde se deduce que $\mathfrak{M} \vDash \forall j \in \mathrm{fd}(\mathbf{X}).\varphi(j)$.

□

El problema es que, aunque ACA$_0$ prueba el principio de inducción transfinita, ACA$_0$ no es capaz sin embargo de hacer definiciones por recursión transfinita; para eso necesitaremos pasar al siguiente subsistema de la aritmética, ATR$_0$.

La idea de la recursión transfinita es la siguiente. Supongamos que tenemos un buen orden numerable X y una fórmula aritmética $\theta(n, Y)$. Entonces a cada $j \in \mathrm{fd}(X)$ le queremos asignar un conjunto, Y_j, que signifique que hemos hecho j pasos en la recursión. Supongamos que tenemos definidos los Y_i para $i <_X j$, definimos

$$Y^j = \{(m, i) \mid i <_X j \wedge m \in Y_i\},$$

es decir, el conjunto de todos los elementos de Y_i con $i <_X j$ anotando a qué conjunto

pertenecen. Tras eso definimos Y_j como

$$Y_j = \{n \mid \theta(n, Y^j)\},$$

es decir, consideramos una iteración más. Veamos ahora la definición formal. Primero veamos la definición del conjunto Y^j a partir del parámetro Y.

Lema 5.3.

$$RCA_0 \vdash \forall X.Lo[X] \to \forall j \in \mathrm{fd}(X)\forall Y\exists^1 Z.Z = \{(m,i) \mid i <_X j \wedge (m,i) \in Y\}.$$

A este único Z lo llamaremos Y^j.

Demostración: Por Σ^0_0-COMP. □

Y ahora definimos las fórmulas:

Definición 5.3. Sea $\theta\{n, Y\} \in$ Form. Definimos la fórmulas

$$H_\theta\{X, Y\} :\equiv \mathrm{Lo}[X] \wedge Y = \{(n,j) \mid j \in \mathrm{fd}(X) \wedge \theta\{n, Y^j\}\}.$$

$$H_\theta\{k, X, Y\} :\equiv \mathrm{Lo}[X] \wedge k \in \mathrm{fd}(X) \wedge Y = \{(n,j) \mid j \in \mathrm{fd}(X) \wedge j <_X k \wedge \theta\{n, Y^j\}\}.$$

■

La primera fórmula quiere decir que Y es el resultado de iterar θ a lo largo de X y la segunda fórmula dice lo mismo pero únicamente hasta un elemento k del orden. Es entonces fácil ver que $H_\theta\{X, Y\}$ y $k \in \mathrm{fd}(X)$ implican $H_\theta\{k, X, Y^k\}$. Algo importante para que esta definición tenga sentido es que, cuando se defina un conjunto, exista a lo sumo un conjunto que cumpla la definición. Veámoslo:

Lema 5.4. *Sea $\theta\{n, Y\} \in$ Form. Entonces*

$$ACA_0 \vdash \forall X.Wo[X] \to \forall Y, Z.H_\theta\{X, Y\} \wedge H_\theta\{X, Z\} \to Y = Z.$$

Demostración:

⟨1⟩1. Sea $\theta\{n, Y\}$ tal que $\mathrm{Vl}(\theta) \setminus \{n, Y\} = \{\nu_1, \ldots, \nu_r\}$ y $\mathfrak{M}$ un modelo de ACA$_0$.

⟨1⟩2. Definimos $\psi :\equiv \forall X.\mathrm{Wo}[X] \to \forall Y, Z.H_\theta\{X, Y\} \wedge H_\theta\{X, Z\} \to Y = Z$.

⟨1⟩3. $\mathrm{Vl}(\psi) = \{\nu_1, \ldots, \nu_r\}$.

Demostración: Por definición de Vl y las hipótesis de ⟨1⟩1 y ⟨1⟩2.

⟨1⟩4. Sean $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r \in \mathbb{N} \cup \wp(\mathbb{N})$ y llamemos $\theta[n, Y] :\equiv \theta[X, Y, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r], H_\theta[X, Y] :\equiv H_\theta[X, Y, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r]$, entonces
$\boldsymbol{\psi} :\equiv \psi[\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r] \equiv \forall X.\mathrm{Wo}[X] \to \forall Y, Z.H_\theta[X, Y] \wedge H_\theta[X, Z] \to Y = Z$,
y es suficiente probar que $\mathfrak{M} \vDash \boldsymbol{\psi}$.

⟨1⟩5. Sea $\mathbf{X} \in \wp(\mathbb{N})$, tal que $\mathfrak{M} \vDash \text{WO}[\mathbf{X}]$ y $\mathbf{Y}, \mathbf{Z} \in \wp(\mathbb{N})$ tales que $\mathfrak{M} \vDash H_\theta[\mathbf{X}, \mathbf{Y}] \wedge H_\theta[\mathbf{X}, \mathbf{Z}]$.

⟨1⟩6. $\mathfrak{M} \vDash \forall j \in \text{fd}(\mathbf{X}).\mathbf{Y}^j = \mathbf{Z}^j$.

⟨2⟩1. Sea $\mathbf{j} \in \text{fd}(\mathbf{X})$ y supongamos que
$$\mathfrak{M} \vDash \forall i \in \text{fd}(\mathbf{X}).i <_{\mathbf{X}} \mathbf{j} \to \mathbf{Y}^i = \mathbf{Z}^i.$$

⟨2⟩2. $\mathfrak{M} \vDash \forall i <_{\mathbf{X}} \mathbf{j}.\mathfrak{M} \vDash \mathbf{Y}_i = \mathbf{Z}_i$.

DEMOSTRACIÓN: Sea $\mathbf{i} \in \text{fd}(\mathbf{X})$ tal que $\mathfrak{M} \vDash \mathbf{i} <_{\mathbf{X}} \mathbf{j}$. Por ⟨2⟩1 $\mathfrak{M} \vDash \mathbf{Y}^{\mathbf{i}} = \mathbf{Z}^{\mathbf{i}}$. Así
$$\mathfrak{M} \vDash \mathbf{Y}_{\mathbf{i}} = \{m \mid \theta[m, \mathbf{Y}^{\mathbf{i}}]\} = \{m \mid \theta[m, \mathbf{Z}^{\mathbf{i}}]\} = \mathbf{Z}_{\mathbf{i}}.$$

⟨2⟩3. $\mathfrak{M} \vDash \mathbf{Y}^{\mathbf{j}} = \mathbf{Z}^{\mathbf{j}}$.

DEMOSTRACIÓN: Usando ⟨2⟩2 es fácil obtener que
$$\mathfrak{M} \vDash \mathbf{Y}^{\mathbf{j}} = \{(m, i) : i <_{\mathbf{X}} \mathbf{j} \wedge m \in \mathbf{Y}_i\} = \{(m, i) : i <_{\mathbf{X}} \mathbf{j} \wedge m \in \mathbf{Z}_i\} = \mathbf{Z}^{\mathbf{j}}.$$

⟨2⟩4. Q.E.D.

DEMOSTRACIÓN: Por inducción transfinita, i.e. el lema 5.2.

⟨1⟩7. Q.E.D.

DEMOSTRACIÓN: Usando ⟨1⟩6 y que por ⟨1⟩5 $\mathfrak{M} \vDash H_\theta[\mathbf{X}, \mathbf{Y}] \wedge H_\theta[\mathbf{X}, \mathbf{Z}]$, se concluye que $\mathfrak{M} \vDash \mathbf{Y} = \mathbf{Z}$.

□

Igual que en la demostración anterior, se prueba que:

Lema 5.5. *Sea* $\theta\{n, Y\} \in \text{Form}$. *Entonces*

$$ACA_0 \vdash \forall X.WO[X] \to \forall k \forall Y, Z.H_\theta\{k, X, Y\} \wedge H_\theta\{k, X, Z\} \to Y = Z.$$

Habiendo garantizado en ACA$_0$ la unicidad de los conjuntos necesarios, podemos añadir las definiciones por recursión transfinita para expandir ACA$_0$ en ATR$_0$. Notemos que lo haremos únicamente para fórmulas aritméticas,

Definición 5.4 (**La teoría** ATR$_0$)**.** Definimos ATR$_0$ como el subsistema de Z_2 dado por
$$\text{ATR}_0 = \text{ACA}_0 + \{\text{cl}(\forall X.\text{WO}[X] \to \exists Y.H_\theta\{X, Y\}) \mid \theta \in \Sigma^1_0\}.$$

La teoría ATR$_0$ es más fuerte que ACA$_0$, de hecho ATR$_0$ prueba la consistencia de la teoría ACA$_0$. Más aún, ATR$_0$ es también mucho más fuerte que ACA$_0$ desde el punto de vista de las matemáticas ordinarias que se pueden formalizar en dicho sistema. Es bien conocido que ATR$_0$ es la teoría (natural) más débil que es capaz de demostrar que los ordinales numerables (una vez convenientemente formalizados en el lenguaje de Z_2)

están linealmente ordenados. Este hecho explica que muchos resultados matemáticos que dependen (explícita o implícitamente) del manejo de ordinales numerables necesiten de ATR$_0$ para su demostración. De hecho, ATR$_0$ es ya capaz de demostrar varios teoremas fundamentales de la teoría descriptiva de conjuntos relativos a conjuntos de Borel y conjuntos analíticos.

Cabe destacar que, a pesar de su elaborada definición, el sistema ATR$_0$ puede reformularse en términos del axioma-esquema de separación (en analogía al sistema WKL$_0$). Enunciamos el siguiente teorema, cuya prueba excede el contenido del presente trabajo pero puede consultarse en el teorema V.5.1 del libro [8].

Teorema 5.6. *En RCA$_0$, son equivalentes:*

1. *ATR$_0$*
2. *Σ^1_1-SEP:*

$$(\neg\exists n.\varphi_0\{n\} \wedge \varphi_1\{n\}) \to \exists X \forall n.(\varphi_0\{n\} \to n \in X) \wedge (\varphi_1\{n\} \to n \notin X),$$

donde $n \in \mathrm{Var}_N$, $X \in \mathrm{Var}_C$ y $\varphi_0\{n\}, \varphi_1\{n\} \in \Sigma^1_1$ tal que $X \notin \mathrm{Vl}(\varphi_0\{n\}) \cup \mathrm{Vl}(\varphi_1\{n\})$.

5.2. Π^1_1-CA$_0$

El último sistema por introducir, el esquema de Π^1_1-comprensión Π^1_1-CA$_0$, resultará mucho más sencillo de definir: tan solo es necesario sustituir el esquema de comprensión de Z_2 por uno más débil.

Definición 5.5. (**La teoría** Π^1_1-CA$_0$) Definimos Π^1_1-CA$_0$ como el subsistema de Z_2 dado por los axiomas básicos, el axioma de inducción y el axioma-esquema de Π^1_1-comprensión, esto es:

$$\Pi^1_1\text{-CA}_0 = \text{BASIC} + \textsc{Ind} + \Pi^1_1\text{-COMP}.$$

■

La teoría Π^1_1-CA$_0$ es más fuerte que ATR$_0$ (prueba la consistencia de esta última), y en Π^1_1-CA$_0$ es posible formalizar de manera natural las demostraciones habituales de varios resultados clásicos de la teoría descriptiva de conjuntos sobre conjuntos de Borel y conjuntos analíticos. En particular, el teorema de Souslin (un conjunto S es Borel si y solo si tanto S como su complementario son conjuntos analíticos) y el teorema de Lusin (dos conjuntos analíticos disjuntos cualesquiera pueden separarse por un conjunto de Borel) son demostrables en Π^1_1-CA$_0$.

Nótese que Π^1_1-CA$_0$ podría haberse definido equivalentemente usando Σ^1_1-COMP en lugar de Π^1_1-COMP, y que análogamente podemos considerar las teorías Π^1_k-CA$_0$ con $k \in \omega$.

Definición 5.6. (Π^1_k-CA_0) Definimos el sistema Π^1_k-CA_0, con $k \in \omega$, como el subsistema de Z_2 con los axiomas básicos, el axioma de inducción y el esquema de Π^1_k-comprensión. En particular, Π^1_0-CA_0 es ACA_0 y para todo $k \in \omega, \Pi^1_k$-$\mathrm{CA}_0 \subseteq \Pi^1_{k+1}$-$\mathrm{CA}_0$. Además, se tiene que

$$\mathrm{Z}_2 = \Pi^1_\infty\text{-}\mathrm{CA}_0 = \bigcup_{k\in\omega} \Pi^1_k\text{-}\mathrm{CA}_0.$$

■

Con ello, hemos concluido la definición de los cinco subsistemas más importantes de la aritmética de segundo orden

$$\mathrm{RCA}_0 \subset \mathrm{WKL}_0 \subset \mathrm{ACA}_0 \subset \mathrm{ATR}_0 \subset \Pi^1_1\text{-}\mathrm{CA}_0.$$

5.3. Otros resultados de la matemática inversa de RCA_0 y Π^1_1-CA_0

Finalmente cerramos el capítulo exponiendo (sin demostración ni haciendo las codificaciones nuevas necesarias) algunos equivalentes de ATR_0 y Π^1_1-CA_0 sobre RCA_0, para que el lector pueda adquirir una cierta intuición sobre la potencia de estos sistemas. Remitimos al lector que quiera profundizar en estos resultados a los capítulos V y VI (respectivamente) de Simpson [8].

Teorema 5.7. *En RCA_0 son equivalentes:*

1. *ATR_0.*
2. *(**Comparabilidad de buenos ordenes**) Dos buenos órdenes numerables cualesquiera son comparables (o son isomorfos o hay un isomorfismo de una sección inicial de uno al otro).*
3. *(**Forma normal de Cantor, [4]**) Si β es un buen orden entonces existe una sucesión finita $\gamma_0 > \gamma_1 > \gamma_n$ de buenos órdenes y una colección finita $d_1, \ldots, d_n$ de enteros positivos tal que*
$$\beta = \omega^{\gamma_0} d_0 + \cdots + \omega^{\gamma_n} d_n.$$
(ω será la codificacón del ordinal ω en RCA_0, no el ω de la metateoría).
4. *(**El teorema del conjunto perfecto, I**) Sea A un conjunto analítico (dado por un código analítico). Si A es no numerable, entonces A contiene un conjunto perfecto no vacío.*
5. *(**El teorema del conjunto perfecto, II**) Sea T un árbol binario. Si T tiene una cantidad no numerable de ramas, entonces T contiene un subárbol perfecto no vacío.*

6. *(**El teorema de separación de Lusin**) Dos conjuntos analíticos disjuntos cualesquiera pueden separarse por un conjunto de Borel.*

7. *(**Determinación abierta**) Todo subconjunto abierto A del espacio de Baire $\mathbb{N}^{\mathbb{N}}$ está determinado.*

Teorema 5.8. *En RCA_0 son equivalentes:*

1. Π^1_1-CA_0.

2. *Para toda sucesión de árboles $\langle T_k : k \in \mathbb{N}\rangle$ existe el conjunto $\{k \mid \exists g.\textsc{Path}[g, T_k]\}$.*

3. *Todo árbol puede ser podado, es decir, para todo árbol $T \subseteq \mathbb{N}^{\mathbb{N}}$ existe un subárbol $T' \subseteq T$ tal que T' contiene, exactamente, a las sucesiones σ de T que pertenecen a alguna rama de T.*

4. *(**El teorema de Cantor-Bendixson para el espacio de Baire**) Todo conjunto cerrado del espacio de Baire $\mathbb{N}^{\mathbb{N}}$ es la unión de un cerrado perfecto y un conjunto numerable.*

5. *(**El teorema de Cantor-Bendixson para el espacio de Cantor**) Todo conjunto cerrado del espacio de Cantor $2^{\mathbb{N}}$ es la unión de un cerrado perfecto y un conjunto numerable.*

6. *(**Determinación** $\Sigma^0_1 \wedge \Pi^0_1$) Todo subconjunto A del espacio de Baire $\mathbb{N}^{\mathbb{N}}$ que sea la intersección de un abierto y un cerrado está determinado.*

Capítulo 6

Algunos resultados metateóricos

En este último capítulo, presentamos algunos resultados clave sobre las propiedades lógicas de los sistemas introducidos. En particular, estudiaremos su relación con los sistemas de la aritmética de primer orden y presentaremos un resultado de conservación para WKL_0 sobre una teoría que captura el "razonamienro finitista" y, por tanto, relacionaremos este subsistema con los fundamentos de la matemática y el programa de Hilbert.

6.1. Partes de primer orden de $\mathbf{RCA}_0, \mathbf{WKL}_0, \mathbf{ACA}_0$

Lo primero que haremos será relacionar las teorías de la aritmética de segundo orden $\mathrm{RCA}_0, \mathrm{WKL}_0$ y ACA_0 con las teorías de la aritmética de primer orden. Es decir, vamos a estudiar la parte de primer orden de estas teorías, para ello necesitamos algunas definiciones.

Lo primero de todo es introducir el lenguaje de la aritmética de primer orden.

Definición 6.1 (**El lenguaje** L_1)**.** Definimos el lenguaje de L_1, conocido como el lenguaje de la aritmética de primer orden, como el mismo de L_2, pero eliminando las variables de conjuntos y el símbolo $\in$. Entonces, un modelo $\mathfrak{M}$ de L_1 será únicamente una 6-tupla:

$$\mathfrak{M} = (M, +_{\mathfrak{M}}, \cdot_{\mathfrak{M}}, 0_{\mathfrak{M}}, 1_{\mathfrak{M}}, <_{\mathfrak{M}}).$$

Igual que con L_2, definimos los conjuntos de fórmulas, términos (ahora solamente numéricos), etc. Para distinguirlos pondremos el subíndice $_{L_1}$ al final de esos conjuntos.

□

Ahora introducimos las teorías en el lenguaje L_1 que vamos a usar.

Definición 6.2 (**La aritmética de Peano y sus fragmentos**)**.** La aritmética de Peano, denotada PA, es la teoría de L_1:

$$\text{PA} = \text{BASIC} + \text{Form}_{L_1}\text{-IND}.$$

Los llamados fragmentos de la aritmética $I\Sigma_k$ se definen como:

$$I\Sigma_k = \text{BASIC} + (\Sigma^0_k)_{L_1}\text{-IND}.$$

■

También definimos un concepto del que hemos hablado antes, el de ω-modelo.

Definición 6.3 (**ω-modelo**)**.** Un ω-modelo es un L_2-modelo $\mathfrak{M}$ de la forma

$$\mathfrak{M} = (\omega, \mathcal{S}_M, +, \cdot, 0, 1, <).$$

Donde $+, \cdot, 0, 1, <$ denotan los típicos elementos, operaciones y relaciones de ω. Por tanto para determinar un ω-modelo basta con dar la correspondiente familia $\mathcal{S}_\mathfrak{M}$ de subconjuntos de ω. ■

Definimos ahora de forma precisa a qué nos referimos con parte de primer orden, ya sea de un modelo o de una teoría.

Definición 6.4 (**Parte de primer orden**)**.** Sea $\mathfrak{M} = (M, \mathcal{S}_M, +_\mathfrak{M}, \cdot_\mathfrak{M}, 0_\mathfrak{M}, 1_\mathfrak{M}, <_\mathfrak{M})$ un modelo de L_2. Llamamos parte de primer orden de $\mathfrak{M}$ al modelo de L_1:

$$(M, +_\mathfrak{M}, \cdot_\mathfrak{M}, 0_\mathfrak{M}, 1_\mathfrak{M}, <_\mathfrak{M}).$$

Por otro lado, si T_0 es una teoría en L_2, la parte de primer orden de T_0 es la teoría en L_1 cuyos teoremas son exactamente las fórmulas de L_1 que son teoremas de T_0. ■

Como nos interesa estudiar la parte de primer orden, introducimos el concepto de ω-submodelo.

Definición 6.5 (**ω-submodelo**)**.** Sean $\mathfrak{M}, \mathfrak{N}$ modelos de L_2. Decimos que $\mathfrak{M}$ es un ω-submodelo de $\mathfrak{M}'$, escrito $\mathfrak{M} \subseteq_\omega \mathfrak{N}$, si $\mathfrak{M}$ es submodelo de $\mathfrak{N}$ y comparten la misma parte de primer orden. ■

6.1.1. La parte de primer orden de $\mathbf{ACA}_0$

Definición 6.6 (**Aritméticamente definible**). Sea $\mathfrak{M}$ un modelo de L_2 y sea $X \subseteq M$. Decimos que X es aritméticamente definible en $\mathfrak{M}$ si existe $\varphi[n]$ aritmética con parámetros en $M \cup \mathcal{S}_{\mathfrak{M}}$ tal que

$$X = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \varphi[\mathbf{a}]\}.$$

Además definimos el conjunto

$$\text{Arith-Def}(\mathfrak{M}) = \{X \subseteq M \mid X \text{ es aritméticamente definible en } \mathfrak{M}\}.$$

□

La idea clave será que para expandir un modelo con inducción en las fórmulas aritméticas a un modelo de ACA_0 basta con añadir los conjuntos aritméticamente definibles a la parte de segundo orden.

Lema 6.1. *Sea $\mathfrak{M}$ un modelo de L_2 tal que $\mathfrak{M} \vDash BASIC + \Sigma^1_0\text{-}IND$. Entonces existe $\mathfrak{N}$ tal que $\mathfrak{N} \vDash ACA_0$ y $\mathfrak{M} \subseteq_\omega \mathfrak{N}$.*

Demostración:
⟨1⟩1. Sea $\mathfrak{M}$ un modelo de $\text{BASIC} + \Sigma^1_0\text{-IND}$.

⟨1⟩2. Definimos $\mathfrak{N} = (M, \text{Arith-Def}(\mathfrak{M}), +_{\mathfrak{M}}, \cdot_{\mathfrak{M}}, 0_{\mathfrak{M}}, 1_{\mathfrak{M}}, <_{\mathfrak{M}})$.

⟨1⟩3. $\mathfrak{M} \subseteq_\omega \mathfrak{N}$.

Demostración: Trivial por la definición de ω-submodelo.

⟨1⟩4. $\mathfrak{N} \vDash \text{ACA}_0$.

⟨2⟩1. $\mathfrak{N} \vDash \text{BASIC}$.

Demostración: Trivial, pues comparte parte de primer orden con $\mathfrak{M}$.

⟨2⟩2. $\mathfrak{N} \vDash \text{Ind}$.

Demostración: Sea $\mathbf{X} \in \text{Arith-Def}(\mathfrak{M})$. Por definición de Arith-Def tenemos que existe $\varphi[n] \in (\Sigma^1_0)_{\mathfrak{M}}$ tal que $\mathbf{X} = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \varphi[\mathbf{a}]\}$. Como $\mathfrak{M} \vDash \Sigma^1_0\text{-IND}$ y $\varphi[n] \in (\Sigma^1_0)_{\mathfrak{M}}$ tenemos que $\mathfrak{M} \vDash (\varphi[0] \wedge \forall n.\varphi[n] \to \varphi[n+1]) \to \varphi[n]$ y de ahí se deduce (por la definición de $\mathbf{X}$) que

$$\mathfrak{N} \vDash (0 \in \mathbf{X} \wedge \forall n.n \in \mathbf{X} \to n+1 \in \mathbf{X}) \to \forall n.n \in \mathbf{X}.$$

⟨2⟩3. $\mathfrak{N} \vDash \Sigma^1_0\text{-COMP}$.

Demostración: Sea $\varphi[n] \in (\Sigma^1_0)_{\mathfrak{N}}$ (como ha sido habitual en muchos teoremas anteriores, habría que desarrollar más esta parte, viendo qué sucede si hay otras variables libres aparte de n, pero como ya se ha hecho muchas veces, por ejemplo en el lema 2.17, lo omitimos para no extender la demostración). Supongamos

que $\mathbf{Y}_1, \ldots, \mathbf{Y}_l \in$ Arith-Def($\mathfrak{M}$) ($l \in \omega$) son todos los parámetros de conjuntos que aparecen en la fórmula. Como pertenecen a Arith-Def($\mathfrak{M}$), tenemos que existen $\varphi_i[m] \in (\Sigma^1_0)_{\mathfrak{M}}$ tales que

$$\mathbf{Y}_i = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \varphi_i[\mathbf{a}]\}.$$

Sea $\widetilde{\varphi}[n]$ el resultado de sustituir cada fórmula atómica $x \in \mathbf{Y}_i$ por $\varphi_i[x]$ (para $i = 1, \ldots, l$), así $\widetilde{\varphi}[n] \in (\Sigma^1_0)_{\mathfrak{M}}$ y por $\langle 1\rangle 2$ tenemos que

$$\mathfrak{N} \vDash \exists X \forall n. n \in X \leftrightarrow \widetilde{\varphi}[n]$$

(ya que los conjuntos del modelo son los aritméticamente definibles en $\mathfrak{M}$). Además tenemos que por la definición de $\widetilde{\varphi}[n]$

$$\mathfrak{N} \vDash \forall n. \varphi[n] \leftrightarrow \widetilde{\varphi}[n].$$

Podemos concluir que

$$\mathfrak{N} \vDash \exists X \forall n. n \in X \leftrightarrow \varphi[n],$$

como queríamos.

$\langle 1\rangle 5$. Q.E.D.

□

Teorema 6.2. *Sea $\mathfrak{M}$ un modelo de L_1. Entonces $\mathfrak{M}$ es un modelo de PA si y sólo si es la parte de primer orden de un modelo de ACA_0.*

Demostración: Que la primera parte de un modelo de ACA_0 es un modelo de PA se tiene por el lema 4.2. Y si $\mathfrak{M} \vDash \mathrm{PA}$, entonces, visto como un modelo de L_2, por el lema 6.1 tenemos que es la primera parte de un modelo de ACA_0. □

Corolario 6.3. *PA es la parte de primer orden de ACA_0, i.e. la teoría ACA_0 es conservativa sobre PA.*

Demostración: El lema 4.2 implica que PA está incluido en la parte de primer orden de ACA_0. Veamos la otra dirección. Sea $\varphi \in \mathrm{Sent}_{L_1}$ tal que $\mathrm{PA} \nvdash \varphi$. Por el teorema de completitud de Gödel, existe un modelo $\mathfrak{M}$ de PA tal que $\mathfrak{M} \nvDash \varphi$. Aplicando el teorema 6.2, se tiene que $\mathfrak{M}$ es la parte de primer orden de un modelo $\mathfrak{N}$ de ACA_0, y, por tanto, $\mathfrak{N} \nvDash \varphi$. Aplicando ahora el teorema de validez, obtenemos que $\mathrm{ACA}_0 \nvdash \varphi$. □

6.1.2. La parte de primer orden de RCA_0

Pasamos a estudiar la parte de primer orden de RCA_0, el procedimiento es análogo al de ACA_0.

Definición 6.7 ($\boldsymbol{\Delta^0_1}$ definible). Sea $\mathfrak{M}$ un modelo de L_2 y sea $X \subseteq M$. Decimos que X es Δ^0_1 definible en $\mathfrak{M}$ si existen fórmulas $\varphi[n] \in \Sigma^0_1$ y $\psi[n] \in \Pi^0_1$ con parámetros en

$M \cup \mathcal{S}_{\mathfrak{M}}$ tal que

$$X = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \varphi[\mathbf{a}]\} = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \psi[\mathbf{a}]\}.$$

Además definimos el conjunto Δ^0_1-Def$(\mathfrak{M}) = \{X \subseteq M \mid X$ es Δ^0_1 definible en $\mathfrak{M}\}$. ■

En el siguiente lema nos permitiremos (como es habitual) ser algo libres en la distinción entre ser Σ^0_1 o ser equivalente a una fórmula Σ^0_1 (de igual manera con el resto de la jerarquía), ya que la demostración es suficientemente larga sin entrar en esas consideraciones.

Lema 6.4. *Sea $\mathfrak{M}$ un modelo de L_2 tal que $\mathfrak{M} \vDash BASIC + \Sigma^0_1$-IND. Entonces existe $\mathfrak{N}$ tal que $\mathfrak{N} \vDash RCA_0$ y $\mathfrak{M} \subseteq_\omega \mathfrak{N}$.*

⟨1⟩1. Sea $\mathfrak{M}$ un modelo de BASIC + Σ^0_1-IND.

⟨1⟩2. $\mathfrak{M}$ satisface Σ^0_1-BOUND.

Demostración: Por el lema 2.18.

⟨1⟩3. Definimos el L_2 modelo $\mathfrak{N}$ dado por:
$$\mathfrak{N} = (M, \Delta^0_1\text{-Def}(\mathfrak{M}), +_{\mathfrak{M}}, \cdot_{\mathfrak{M}}, 0_{\mathfrak{M}}, 1_{\mathfrak{M}}, <_{\mathfrak{M}}).$$

⟨1⟩4. $\mathfrak{M} \subseteq_\omega \mathfrak{N}$.

Demostración: Trivial por la definición de submodelo.

⟨1⟩5. Para toda $\theta \in \text{Form}(\mathfrak{N})$ con $\text{Vl}(\theta) \cap \text{Var}_{\text{C}} = \varnothing$ y $\theta \in \Sigma^0_0$ existen $\theta_\Sigma, \theta_\Pi \in \text{Form}(\mathfrak{M})$, tal que:
- $\theta_\Sigma \in (\Sigma^0_1)_{\mathfrak{M}}, \theta_\Pi \in (\Pi^0_1)_{\mathfrak{M}}$.
- $\text{Vl}(\theta) = \text{Vl}(\theta_\Sigma) = \text{Vl}(\theta_\Pi)$.
- $\mathfrak{N} \vDash \theta_\Sigma \leftrightarrow \theta_\Pi \leftrightarrow \theta$.

⟨2⟩1. Supondremos, sin pérdida de generalidad, que las únicas conectivas lógicas son la negación y la conjunción y el único cuantificador (acotado pues la fórmula es Σ^0_0)) es el universal.

Demostración: Toda fórmula es equivalente a una fórmula de esas características, respetando variables libres.

⟨2⟩2. Por inducción en θ.

⟨2⟩3. $\theta \equiv t_1 = t_2$ o $\theta \equiv t_1 < t_2$.

Demostración: En ese caso $\theta \equiv \theta_\Sigma \equiv \theta_\Pi$.

⟨2⟩4. $\theta \equiv t \in \mathbf{X}$.

Demostración: Sabemos que $\mathbf{X} \in \mathcal{S}_{\mathfrak{N}}$, ya que no puede ser una variable por hipótesis de ⟨1⟩5. Como $\mathcal{S}_{\mathfrak{N}} = \Delta^0_1$-Def$(\mathfrak{M})$, existen $\varphi[n], \psi[n] \in \text{Form}(\mathfrak{M})$ con $\varphi \in (\Sigma^0_1)_{\mathfrak{M}}$

y $\psi \in (\Pi^0_1)_{\mathfrak{M}}$ tal que $\mathbf{X} = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \varphi[\mathbf{a}]\} = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \psi[\mathbf{a}]\}$. Entonces definimos $\theta_\Sigma :\equiv \varphi[t]$ y $\theta_\Pi :\equiv \psi[t]$, claramente cumplen lo pedido.

⟨2⟩5. Caso $\theta \equiv \neg\theta'$.

DEMOSTRACIÓN: Por hipótesis de inducción existen θ'_Σ y θ'_Π, entonces definimos $\theta_\Sigma :\equiv \neg\theta'_\Pi$ y $\theta_\Pi :\equiv \neg\theta'_\Sigma$.

⟨2⟩6. Caso $\theta \equiv \theta' \wedge \theta''$.

DEMOSTRACIÓN: Por hipótesis existen $\theta'_\Sigma, \theta'_\Pi, \theta''_\Sigma$ y θ''_Π. Además, por las condiciones se tiene que $\theta'_\Sigma \equiv \exists j.\theta'_0, \theta''_\Sigma \equiv \exists j.\theta''_0, \theta'_\Pi \equiv \forall j.\theta'_1, \theta''_\Pi \equiv \forall j.\theta''_1$. Definimos:

$$\theta_\Sigma :\equiv \exists m.(\exists j' < m.\theta'_0[j \mapsto j']) \wedge (\exists j'' < m.\theta''_0[j \mapsto j''])$$

donde m, j', j'' son variables nuevas, y definimos

$$\theta_\Pi :\equiv \forall j.\theta'_1 \wedge \theta''_2.$$

⟨2⟩7. Caso $\theta \equiv \forall i < t.\theta'$ con $i \notin \mathrm{Vl}(t)$.

DEMOSTRACIÓN: Por hipótesis de inducción existen θ'_Σ y θ'_Π. Además $\theta'_\Sigma \equiv \exists j.\theta'_0, \theta'_\Pi \equiv \forall j.\theta'_1$ (supongamos que $j \notin \mathrm{Vl}(t)$). Entonces definimos

$$\theta_\Sigma :\equiv \exists n \forall i < t \exists j < n.\theta'_0,$$

donde n es una variable nueva, y definimos

$$\theta_\Pi :\equiv \forall j \forall i < t.\theta'_1.$$

Para la equivalencia de θ_Σ con θ usamos el principio de Σ^0_1-BOUND.

⟨2⟩8. Q.E.D.

DEMOSTRACIÓN: El resultado se sigue de la inducción.

⟨1⟩6. Sea $\varphi \in \mathrm{Form}(\mathfrak{N})$ con $\mathrm{Vl}(\varphi) \cap \mathrm{Var}_{\mathrm{C}} = \varnothing$ y $\varphi \in (\Sigma^0_1)_{\mathfrak{N}}$. Entonces existe $\varphi' \in \mathrm{Form}(\mathfrak{M})$ tal que:

- $\varphi' \in (\Sigma^0_1)_{\mathfrak{M}}$.
- $\mathrm{Vl}(\varphi) = \mathrm{Vl}(\varphi')$.
- $\mathfrak{N} \vDash \varphi' \leftrightarrow \varphi$.

DEMOSTRACIÓN: Por hipótesis $\varphi \equiv \exists j.\theta$, donde $\theta \in \mathrm{Form}(\mathfrak{N})$ y $\theta \in \Sigma^0_0$. Por ⟨1⟩5 existe $\theta_\Sigma, \in \mathrm{Form}(\mathfrak{M})$ tal que $\theta_\Sigma \equiv \exists m.\theta_0$, con $\theta_0 \in \Sigma^0_0$. Definimos

$$\varphi' :\equiv \exists k \exists j < k \exists m < k.\theta_0,$$

donde k es una nueva variable. Está claro que cumple lo pedido.

⟨1⟩7. $\mathfrak{N} \vDash \mathrm{RCA}_0$.

⟨2⟩1. $\mathfrak{N} \vDash$ BASIC.

DEMOSTRACIÓN: Por ⟨1⟩4, $\mathfrak{M}$ y $\mathfrak{N}$ comparten la parte de primer orden.

⟨2⟩2. $\mathfrak{N} \vDash \Sigma^0_1$-IND.

DEMOSTRACIÓN: Sea $\varphi[n] \in (\Sigma^0_1)_{\mathfrak{N}}$. Por $\langle 1\rangle 6$ existe $\varphi'[n]$ que cumple las tres propiedades allí enunciadas. Como $\mathfrak{M} \vDash \Sigma^0_1$-IND tenemos que

$$\mathfrak{M} \vDash (\varphi'[0] \wedge \forall n.\varphi'[n] \to \varphi'[n+1]) \to \forall n.\varphi'[n],$$

de donde concluimos que

$$\mathfrak{N} \vDash (\varphi[0] \wedge \forall n.\varphi[n] \to \varphi[n+1]) \to \forall n.\varphi[n].$$

$\langle 2\rangle 3$. $\mathfrak{N} \vDash \Delta^0_1$-COMP.

DEMOSTRACIÓN: Sean $\varphi[n] \in (\Sigma^0_1)_{\mathfrak{N}}$ y $\psi[n] \in (\Pi^0_1)_{\mathfrak{N}}$ tales que $\mathfrak{N} \vDash \forall n.\varphi[n] \leftrightarrow \psi[n]$. Por $\langle 1\rangle 6$ existen $\varphi'[n]$ y $\psi'[n]$ que cumplen las propiedades allí enunciadas (notemos que para aplicarlo a la fórmula $\psi \in (\Pi^0_1)_{\mathfrak{N}}$ nos basta aplicarlo a $\theta \equiv \neg\psi$: ello nos dará un θ' y luego tomamos $\psi' :\equiv \neg\theta'$). Entonces se tiene que:

$$\mathfrak{N} \vDash \forall n.\varphi[n] \leftrightarrow \varphi'[n]$$

y

$$\mathfrak{M} \vDash \forall n.\varphi'[n] \leftrightarrow \psi'[n].$$

Tomando $\mathbf{X} = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \varphi'[\mathbf{a}]\}$ se tiene claramente que $\mathbf{X} \in \Delta^0_1$-Def$(\mathfrak{M})$, y por tanto

$$\mathfrak{N} \vDash \exists X \forall n.n \in X \leftrightarrow \varphi[n].$$

$\langle 1\rangle 8$. Q.E.D.

□

Teorema 6.5. *Sea $\mathfrak{M}$ un L_1-modelo. Entonces son equivalentes*

1. *$\mathfrak{M}$ es la parte de primer orden de un modelo de RCA_0.*
2. *$\mathfrak{M}$ es un modelo de $I\Sigma_1$.*

DEMOSTRACIÓN: Trivialmente, la parte de primer orden de un modelo de RCA_0 es un modelo de $I\Sigma_1$. Supongamos que $\mathfrak{M}$ es un modelo de $I\Sigma_1$. Entonces, visto como un L_2-modelo, satisface Σ^0_1-IND, y, por el lema anterior, es la parte de primer orden de algún modelo de RCA_0. □

Corolario 6.6. *La parte de primer orden de RCA_0 es $I\Sigma_1$.*

DEMOSTRACIÓN: Completamente análogo al caso de ACA_0. □

6.1.3. La parte de primer orden de $\mathbf{WKL}_0$

Se puede demostrar que la parte de primer orden de WKL_0 es la misma que la de RCA_0, i.e. $I\Sigma_1$. Este resultado puede obtenerse como consecuencia de un resultado de conservación para WKL_0 (que es de interés independiente) y del hecho de que la parte de primer orden de RCA_0 es $I\Sigma_1$.

En este caso, omitimos la demostración por falta de espacio, pero cabe destacar que el argumento sigue un esquema distinto a los dos anteriores (el manejo de árboles y el uso de una cierta técnica de construcción de tipo forcing desempeñan un papel fundamental); remitimos al lector a la sección IX.2 del libro de Simpson [8].

Teorema 6.7 (Teorema de conservación, Harrington 1977)**.** *Sea ψ una Π^1_1 fórmula cerrada. Si $WKL_0 \vdash \psi$, entonces $RCA_0 \vdash \psi$.*

Corolario 6.8. *La parte de primer orden de WKL_0 es $I\Sigma_1$.*

6.2. WKL_0 y el programa de Hilbert

En esta sección demostraremos que WKL_0 es conservativa sobre PRA (la aritmética primitivo recursiva) para Π^0_2 fórmulas cerradas (notemos que, por tanto, serán fórmulas sin variables de conjuntos). Para ello nos valdremos de la sección anterior, usando que la parte de primer orden de WKL_0 es $I\Sigma_1$. Este resultado de conservación tiene especial interés desde el punto de vista de los fundamentos de las matemáticas. Al final de la sección, hablaremos brevemente de cómo este resultado relaciona el programa de Hilbert (reduccionismo finitista) con el subsistema WKL_0.

Empezamos introduciendo todas la definiciones necesarias para definir la teoría de primer orden PRA.

Definición 6.8 (**Lenguaje $L_{\mathbf{PRA}}$**)**.** El lenguaje de la aritmética primitiva recursiva, denotado L_{PRA}, es un lenguaje de primer orden con igualdad (y una cantidad infinita numerable de variables) con los siguientes símbolos no lógicos:

- La constante $\underline{0}$.
- Los símbolos de función unarios $\underline{Z}, \underline{S}$.
- Para cada i, k tales que $1 \leq i \leq k < \omega$ un símbolo de función k-ario $\underline{P}^k_i$.
- Para cada símbolo de función m-ario $\underline{g}$ y $\underline{h}_1, \ldots, \underline{h}_m$ símbolos de función k-arios, $C(\underline{g}, \underline{h}_1, \ldots, \underline{h}_m)$ es un símbolo de función k-ario.
- Para cada símbolo de función k-ario $\underline{g}$ y cada símbolo de funcón $k+2$-ario $\underline{h}$, $R(\underline{g}, \underline{h})$ es un símbolo de función $k+1$-ario.
- Para cada $\underline{f}$ símbolo de función k-ario un símbolo de relación k-ario $\underline{R}_{\underline{f}}$.

Los símbolos de función de PRA se denominan símbolos de función primitivos recursivos y los de relación, símbolos de relación primitivos recursivos. ■

Como es habitual, con los símbolos del 0 y del sucesor podemos expresar cualquier elemento de ω con un término cerrado.

Notación. Dado $k \in \omega \setminus \{0\}$, definimos $\underline{k}$ como:

$$\underline{1} = \underline{S}(\underline{0}),$$

$$\underline{k+1} = \underline{S}(\underline{k}).$$

■

Notemos entonces que cada función primitiva recursiva tiene un símbolo de función asocidado. Será común (al igual que en las funciones primitivo recursivas) no explicitar la construcción del símbolo, sino poner las ecuaciones que lo definen.

Definición 6.9 (**La teoría** PRA)**.** El modelo estándar de PRA, $\mathfrak{M}_{\text{PRA}}$, es el modelo de L_{PRA} cuyo dominio es $\omega = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots\}$, las interpretaciónes de las funciones (y constantes) son:

- $\underline{0}_{\mathfrak{M}_{\text{PRA}}} = \mathbf{0}$.
- $\underline{S}_{\mathfrak{M}_{\text{PRA}}}(\mathbf{x}) = \mathbf{x} +_\omega \mathbf{1}$ es la función sucesor.
- $\underline{Z}_{\mathfrak{M}_{\text{PRA}}}(\mathbf{x}) = \mathbf{0}$ es la función constante cero.
- $\underline{P}^k_i(\mathbf{x}_1, \ldots, \mathbf{x}_k) = \mathbf{x}_i$.
- $C(\underline{g}, \underline{h}_1, \ldots \underline{h}_m)_{\mathfrak{M}_{\text{PRA}}}(\mathbf{x}_1, \ldots, \mathbf{x}_k) = \underline{g}_{\mathfrak{M}_{\text{PRA}}}(\underline{h}_{1,\mathfrak{M}_{\text{PRA}}}(\mathbf{x}_1, \ldots, \mathbf{x}_k), \ldots, \underline{h}_{m,\mathfrak{M}_{\text{PRA}}}(\mathbf{x}_1, \ldots, \mathbf{x}_k))$.
- $R(\underline{g}, \underline{h})_{\mathfrak{M}_{\text{PRA}}}$ es la función definida recursivamente por las ecuaciones:

$$R(\underline{g}, \underline{h})_{\mathfrak{M}_{\text{PRA}}}(\mathbf{0}, \mathbf{x}_1, \ldots, \mathbf{x}_k) = \underline{g}_{\mathfrak{M}_{\text{PRA}}}(\mathbf{x}_1, \ldots, \mathbf{x}_k)$$

$$R(\underline{g}, \underline{h})_{\mathfrak{M}_{\text{PRA}}}(\mathbf{y} + \mathbf{1}, \mathbf{x}_1, \ldots, \mathbf{x}_k) = \underline{h}_{\mathfrak{M}_{\text{PRA}}}(\mathbf{y}, R(\underline{g}, \underline{h})_{\mathfrak{M}_{\text{PRA}}}(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_k), \mathbf{x}_1, \ldots, \mathbf{x}_k).$$

Y finalmente, para cada símbolo de relación $\underline{R}_{\underline{f}}$ se tiene que $(\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \underline{R}_{\underline{f},\mathfrak{M}_{\text{PRA}}}$ si y sólo si $\underline{f}_{\mathfrak{M}_{\text{PRA}}}(\mathbf{x}_1, \ldots, \mathbf{x}_k) = \mathbf{1}$. ■

Definición 6.10. Los axiomas no lógicos de PRA son los siguientes:

1. Axiomas para el $\underline{0}$ y $\underline{S}$:

$$\underline{Z}(x) = \underline{0}.$$

$$\underline{S}(x) = \underline{S}(y) \to x = y.$$

$$x \neq \underline{0} \leftrightarrow \exists y. \underline{S}(y) = x.$$

2. Axiomas para los $\underline{P}_i^k$. Sean $1 \leq i \leq k < \omega$, tenemos el axioma

$$\underline{P}_i^k(x_1 \ldots, x_k) = x_i.$$

3. Para cada $\underline{f} \equiv C(\underline{g}, \underline{h}_1, \ldots, \underline{h}_m)$, tenemos el axioma

$$\underline{f}(x_1, \ldots, x_k) = \underline{g}(\underline{h}_1(x_1, \ldots, x_k), \ldots, \underline{h}_m(x_1, \ldots, x_k)).$$

4. Para cada $\underline{f} = R(\underline{g}, \underline{h})$ tenemos los axiomas:

$$\underline{f}(\underline{0}, x_1, \ldots, x_k) = \underline{g}(x_1, \ldots, x_k).$$

$$\underline{f}(\underline{S}(y), x_1, \ldots, x_k) = \underline{h}(y, \underline{f}(y, x_1, \ldots, x_k), x_1, \ldots, x_k).$$

5. Para cada $\underline{f}$ símbolo de función, el axioma

$$\underline{R}_{\underline{f}}(x_1, \ldots, x_k) \leftrightarrow \underline{f}(x_1, \ldots, x_k) = \underline{1}.$$

6. Y, por último, el esquema de inducción primitiva recursiva, que serán las fórmulas de la forma
$$(\theta\{\underline{0}\} \wedge \forall x.\theta\{x\} \rightarrow \theta\{\underline{S}(x)\}) \rightarrow \forall x.\theta\{x\}.$$
donde $\theta\{x\} \in \mathrm{Form}_{L_{\mathrm{PRA}}}$ libre de cuantificadores.

■

Nota. PRA será la teoría con esos axiomas. Dado un modelo de PRA, llamaremos funciones primitivo recursivas a la interpretación de los símbolos de función primitivo recursivos; y predicados primitivo recursivos, a la interpretación de los símbolos de relación primitivo recursivos. ■

Llamaremos de una forma espacial a ciertos símbolos de función (primitivo recursivos) comunes.

Definición 6.11. Llamamos + (suma) al símbolo de función binario definido por las ecuaciones

$$x + \underline{0} = x,$$
$$x + \underline{S}(y) = \underline{S}(x + y).$$

Llamamos · (producto) al símbolo de función binario definido por las ecuaciones

$$x \cdot \underline{0} = \underline{0},$$

$$x \cdot \underline{S}(y) = (x \cdot y) + x.$$

Llamamos $\underline{P}$ (predecesor) al símbolo de función unario definido por las ecuaciones

$$\underline{P}(\underline{0}) = \underline{0},$$

$$\underline{P}(\underline{S}(y)) = y.$$

Llamamos $\dot{-}$ (resta truncada) al símbolo de función binario definido por las ecuaciones

$$x \dot{-} \underline{0} = \underline{0},$$

$$x \dot{-} \underline{S}(y) = \underline{P}(x \dot{-} y).$$

En PRA usaremos la notación $t_1 < t_2 :\equiv t_2 \dot{-} t_1 \neq \underline{0}$.

Llamamos $\underline{\text{neg}}$ (negación) al símbolo de función unario definido por las ecuaciones

$$\underline{\text{neg}}(\underline{0}) = \underline{1},$$

$$\underline{\text{neg}}(\underline{S}(x)) = \underline{0}.$$

Dado $\underline{f}(y, x_1, \ldots, x_k)$ símbolo de función $k+1$-ario, llamamos $\prod_{y<z} \underline{f}(y, x_1, \ldots, x_k)$ al símbolo de función $\underline{g}(z, x_1, \ldots, x_k)$ $k+1$-ario definido por:

$$\underline{g}(\underline{0}, x_1, \ldots, x_k) = \underline{1},$$

$$\underline{g}(\underline{S}(z), x_1, \ldots, x_k) = \underline{g}(z, x_1, \ldots, x_k) \cdot \underline{f}(z, x_1, \ldots, x_k).$$

■

Gracias a las definiciones anteriores, podemos tratar las fórmulas de L_1 como fórmulas de L_{PRA}, mediante la llamada interpretación canónica.

Definición 6.12 (**Interpretación canónica**)**.** Definimos la interpretación canónica de L_1 en L_{PRA} como la función $\text{CanInterp} : \text{Term}_{L_1} \longrightarrow \text{Term}_{L_{\text{PRA}}}$ definida como:

1. $\text{CanInterp}(0) \equiv \underline{0}$.
2. $\text{CanInterp}(1) \equiv \underline{1}$.
3. $\text{CanInterp}(t_1 + t_2) \equiv \text{CanInterp}(t_1) + \text{CanInterp}(t_2)$.
4. $\text{CanInterp}(t_1 \cdot t_2) \equiv \text{CanInterp}(t_1) \cdot \text{CanInterp}(t_2)$.

Y podemos extenderlo a $\text{CanInterp} : \text{Form}_{L_1} \longrightarrow \text{Form}_{L_{\text{PRA}}}$ si definimos

$$\text{CanInterp}(t_1 < t_2) \equiv \text{CanInterp}(t_1) - \text{CanInterp}(t_2) \neq 0.$$

■

La interpretación canónica nos permite además relacionar modelos de $I\Sigma_1$ con modelos de PRA.

Lema 6.9. *Para todo $\mathfrak{M}$ modelo de $I\Sigma_1$ existe una expansión a un modelo $\mathfrak{N}$ de PRA tal que*

$$\mathfrak{M} \vDash \theta \text{ implica } \mathfrak{N} \vDash \mathrm{CanInterp}(\theta).$$

Demostración: Por el teorema 6.5, sabemos que $\mathfrak{M}$ se puede expandir a un modelo de RCA_0. Una vez tengamos ese modelo, usando el lema 2.53 podemos definir funciones primitivo recursivas dentro de RCA_0 y así podemos definir las interpretaciones de los símbolos de PRA. □

Y como consecuencia del lema anterior:

Teorema 6.10. *Sea $\theta \in \mathrm{Form}_{L_1}$. Si $PRA \vdash \mathrm{CanInterp}(\theta)$, entonces $I\Sigma_1 \vdash \theta$.*

Demostración:
⟨1⟩1. Supongamos que $I\Sigma_1 \nvdash \theta$

⟨1⟩2. Existe $\mathfrak{M}$ modelo de $I\Sigma_1$ tal que $\mathfrak{M} \nvDash \theta$.

Demostración: Por el teorema de completitud aplicado a ⟨1⟩1.

⟨1⟩3. Existe $\mathfrak{M}'$ modelo de PRA tal que $\mathfrak{M} \nvDash \mathrm{CanInterp}(\theta)$.

Demostración: Gracias al lema 6.9 aplicado a ⟨1⟩2.

⟨1⟩4. PRA $\nvdash \mathrm{CanInterp}(\theta)$.

Demostración: Gracias al teorema de validez aplicado a ⟨1⟩3.

⟨1⟩5. Q.E.D.

□

Con esto hemos demostrado (que bajo la interpretación canónica) PRA está incluido en $I\Sigma_1$. Ahora probaremos que toda Π^0_2 fórmula cerrada que sea demostrable en $I\Sigma_1$ (de hecho, en WKL_0) lo será también en PRA.

En PRA podemos definir el conjunto Σ^0_0 como el conjunto imagen de la interpretación canónica aplicada en Σ^0_0.

Definición 6.13. Definimos el conjunto de $\mathrm{Form}_{L_{\mathrm{PRA}}}$ (fórmulas Σ^0_0 generalizadas) como $\mathrm{GEN}\Sigma^0_0 = \mathrm{CanInterp}(\Sigma^0_0)$. ■

Podemos ver que toda fórmula de $\mathrm{GEN}\Sigma^0_0$ es equivalente a un predicado primitivo recursivo.

Lema 6.11. *Para toda $\theta[x_1, \dots, x_k] \in GEN\Sigma^0_0$ existe un símbolo de función k-ario $\underline{f}_\theta$ en L_{PRA} tal que*

1. $PRA \vdash \underline{f}_\theta(x_1, \dots, x_k) = \underline{1} \leftrightarrow \theta$.
2. $PRA \vdash \underline{f}_\theta(x_1, \dots, x_k) = \underline{0} \leftrightarrow \neg\theta$.

Por tanto toda fórmula de $GEN\Sigma^0_0$ es equivalente a un símbolo de relación $\underline{R_f}$.

Demostración:

⟨1⟩1. Supondremos sin pérdida de generalidad que las únicas conectivas lógicas son la negación y la conjunción y el único cuantificador (acotado pues la fórmula es Σ^0_0)) es el universal.

Demostración: Toda fórmula es equivalente a una fórmula de esas características.

⟨1⟩2. Por inducción en θ

⟨1⟩3. Caso $\theta \equiv t_1 = t_2$.

Demostración: Definimos $\underline{f}_\theta(x_1, \dots, x_k) :\equiv \underline{\text{neg}}((t_2 \dot{-} t_1) + (t_1 \dot{-} t_2))$.

⟨1⟩4. Caso $\theta \equiv t_1 < t_2$.

Demostración: Definimos $\underline{f}_\theta(x_1, \dots, x_k) :\equiv \underline{\text{neg}}(\underline{\text{neg}}(t_2 \dot{-} t_1))$.

⟨1⟩5. Caso $\theta \equiv \neg\theta'$.

Demostración: Existe $\underline{f}_{\theta'}(x_1, \dots, x_k)$ por hipótesis de inducción. Definimos
$$\underline{f}_\theta(x_1, \dots, x_k) :\equiv \underline{\text{neg}}(\underline{f}_{\theta'}(x_1, \dots, x_k)).$$

⟨1⟩6. Caso $\theta \equiv \theta' \wedge \theta''$.

Demostración: Existen $\underline{f}_{\theta'}(x_1, \dots, x_k)$ y $\underline{f}_{\theta''}(x_1, \dots, x_k)$ por hipótesis de inducción (en principio podrían tener menos variables libres ya que nada garantiza que las dos subfórmulas tengan todas las variables libres de la fórmula, pero bastaría con coger un símbolo de función k-ario que ignorase las variables que sobren). Definimos
$$\underline{f}_\theta(x_1, \dots, x_k) :\equiv \underline{f}_{\theta'}(x_1, \dots, x_k) \cdot \underline{f}_{\theta''}(x_1, \dots, x_k).$$

⟨1⟩7. Caso $\theta \equiv \forall y < t.\theta'(y, x_1, \dots, x_k)$.

Demostración: Existe $\underline{f}_{\theta'}(y, x_1, \dots, x_k)$ por hipótesis de inducción (en caso de que y no sea una variable libre hacemos como en ⟨1⟩6). Definimos
$$\underline{f}_\theta(x_1, \dots, x_k) :\equiv \prod_{y<t} \underline{f}_{\theta'}(y, x_1, \dots, x_k).$$

⟨1⟩8. Q.E.D.

□

Con el lema anterior hemos visto que en un modelo las fórmulas Σ_0^0 generalizadas son predicados primitivos recursivos.

Definición 6.14. Sea $\mathfrak{M}$ un modelo de PRA. Un conjunto $\mathfrak{M}$-finito es un conjunto $X \subseteq M$ tal que

$$X = \{\mathbf{a} \in M \mid \mathfrak{M} \vDash \mathbf{a} < \mathbf{b} \wedge \underline{R}(\mathbf{a}, \mathbf{c}_1, \ldots, \mathbf{c}_k)\},$$

para algún símbolo de predicado primitivo recursivo $\underline{R}$ y algún $\mathbf{b}, \mathbf{c}_1, \ldots, \mathbf{c}_k \in M$. ■

Definición 6.15. Sea $\mathfrak{M}$ un modelo de PRA y sea X un conjunto $\mathfrak{M}$-finito, definimos la $\mathfrak{M}$-cardinalidad de X como $\mathrm{Card}_{\mathfrak{M}}(X) = \mathrm{Card}_{\mathfrak{M}}(X, b)$ donde $X \subseteq \{a \mid a <_{\mathfrak{M}} b\}$ y

$$\mathrm{Card}_{\mathfrak{M}}(X, 0) = 0$$

$$\mathrm{Card}_{\mathfrak{M}}(X, a+1) = \begin{cases} \mathrm{Card}_{\mathfrak{M}}(X, a) + 1 & \text{si } a \in X \\ \mathrm{Card}_{\mathfrak{M}}(X, a) & \text{si } a \notin X \end{cases}$$

■

Notemos que para que esta definición sea totalmente precisa, deberíamos usar que realmente es la interpretación de un símbolo de función el que está definido por esas ecuaciones recursivas donde a X lo cambiamos por la fórmula que lo define.

Igual que hicimos en RCA_0, en PRA se pueden codificar los conjuntos $\mathfrak{M}$-finitos mediante elementos de M de forma primitiva recursiva. Podríamos usar otra vez el mismo estilo de codificación que hemos usado, pero ahora usaremos uno basado en las potencias de 2.

Definición 6.16. Sea $\mathfrak{M}$ un modelo de PRA, decimos que $\mathbf{c} \in M$ codifica el conjunto $\mathfrak{M}$-finito X si y sólo si para todo $\mathbf{a} \in M$ se cumple que

$$\mathbf{a} \in X \text{ si y sólo si } \mathfrak{M} \vDash \exists u < \mathbf{c} \exists v < \underline{2}^{\mathbf{a}}.\mathbf{c} = \underline{2}^{\mathbf{a}+1} \cdot u + \underline{2}^{\mathbf{a}} + v.$$

■

Se demuestra entonces que

Lema 6.12. *Sea $\mathfrak{M}$ un modelo de PRA. Entonces para todo conjunto X $\mathfrak{M}$-finito, existe un único $\mathbf{c} \in M$ que codifica X. Además $X \subseteq \{\mathbf{a} \mid \mathfrak{M} \vDash \mathbf{a} < \mathbf{b}\}$ si y sólo si $\mathfrak{M} \vDash \mathbf{c} < \underline{2}^{\mathbf{b}}$.*

Con esto podemos definir el concepto de corte semirregular (introducido por Kirby y Paris [5]) que será fundamental para la demostración.

Definición 6.17. Sea $\mathfrak{M}$ un modelo de PRA.

1. Un corte en $\mathfrak{M}$ es un conjunto $I \subseteq M, 1_{\mathfrak{M}} \in I \neq M$ tal que si $\mathbf{a} <_{\mathfrak{M}} \mathbf{b}, \mathbf{b} \in I$ entonces $\mathbf{a} \in I$.

2. Sea I un corte de $\mathfrak{M}$. Un conjunto $X \subseteq I$ se dice que es $\mathfrak{M}$-codificado si existe un conjunto X^* $\mathfrak{M}$-finito tal que $X^* \cap I = X$. Denotamos

$$\mathrm{Coded}_{\mathfrak{M}}(I) = \{X \subseteq I \mid X \text{ es } \mathfrak{M}\text{-codificado}\}.$$

3. Sea I un corte de $\mathfrak{M}$. Un conjunto X se dice que está acotado en I si existe $\mathbf{b} \in I$ tal que $X \subseteq \{\mathbf{a} \mid \mathbf{a} <_{\mathfrak{M}} \mathbf{b}\}$.

4. Un corte I se dice semirregular si para todo los conjuntos X $\mathfrak{M}$-finitos con $\mathrm{Card}_{\mathfrak{M}}(X) \in I$ se cumple que $X \cap I$ está acotado en I.

■

Lema 6.13. *Sea $\mathfrak{M}$ un modelo de PRA y sea I un corte semirregular en $\mathfrak{M}$. Entonces*

$$(I, \mathrm{Coded}_{\mathfrak{M}}(I), +_{\mathfrak{M}} \restriction I, \cdot_{\mathfrak{M}} \restriction I, 0_{\mathfrak{M}}, 1_{\mathfrak{M}}, <_{\mathfrak{M}} \restriction I)$$

es un modelo de WKL_0.

Demostración:
⟨1⟩1. I está cerrado bajo $+_{\mathfrak{M}}$.

Demostración: Supongamos que $\mathbf{b}, \mathbf{c} \in I$ y que $\mathbf{b} +_{\mathfrak{M}} \mathbf{c} \notin I$. Entonces, tenemos el conjunto $X = \{\mathbf{a} \mid \mathbf{b} \leq_{\mathfrak{M}} \mathbf{a} <_{\mathfrak{M}} \mathbf{b} +_{\mathfrak{M}} \mathbf{c}\}$ que es $\mathfrak{M}$-finito y cumple que $\mathrm{Card}(X) = \mathbf{c}$. Sin embargo $X \cap I = \{\mathbf{a} \in I \mid \mathbf{b} \leq_{\mathfrak{M}} \mathbf{a}\}$ no está acotado en I, en contradicción con que sea semirregular.

⟨1⟩2. I está cerrado bajo $\cdot_{\mathfrak{M}}$.

Demostración: Supongamos que $\mathbf{b}, \mathbf{c} \in I$ y que $\mathbf{b} \cdot_{\mathfrak{M}} \mathbf{c} \notin I$. Entonces, tenemos el conjunto $Y = \{\mathbf{b} \cdot_{\mathfrak{M}} \mathbf{a} \mid \mathbf{a} <_{\mathfrak{M}} \mathbf{c}\}$ que es $\mathfrak{M}$-finito y cumple que $\mathrm{Card}(Y) = \mathbf{c}$. Sin embargo $Y \cap I$ no está acotado en I, en contradicción con que sea semirregular.

⟨1⟩3. Definimos el L_2-modelo $\mathfrak{N} = (I, \mathrm{Coded}_{\mathfrak{M}}(I), +_{\mathfrak{M}} \restriction I, \cdot_{\mathfrak{M}} \restriction I, 0_{\mathfrak{M}}, 1_{\mathfrak{M}}, <_{\mathfrak{M}} \restriction I)$.

⟨1⟩4. $\mathfrak{N} \vDash \Sigma^0_1$-IND.

⟨2⟩1. Todo conjunto $\mathfrak{M}$-finito (no vacío) tiene un elemento mínimo para $<_{\mathfrak{M}}$.

Demostración: Gracias a que $\mathfrak{M}$ es un modelo de PRA y por tanto cumple la inducción primitiva recursiva, se puede hacer entonces la demostración habitual de existencia de mínimo.

⟨2⟩2. Sea $\varphi[x] \in (\mathrm{Form}_{L_{\mathrm{PRA}}})_{\mathfrak{N}}$, queremos probar que

$$\mathfrak{N} \vDash (\varphi[0] \wedge \forall x.\varphi[x] \to \varphi[x+1]) \to \forall \varphi[x].$$

Por tanto supongamos que $\mathfrak{N} \vDash \varphi[0] \wedge \forall x.\varphi[x] \to \varphi[x+1]$.

Demostración: Como es habitual, realmente tendríamos que coger una fórmula cualquiera con variable libre x y sustituir cada una de todas sus variables libres

por parámetros cualesquiera. Como hemos repetido muchas veces el proceso nos lo saltamos (ver 2.18).

⟨2⟩3. Podemos suponer que existe $\mathbf{c} \in I$ tal que $\mathfrak{N} \vDash \neg\varphi[\mathbf{c}]$.

DEMOSTRACIÓN: En caso contrario se tendría que $\mathfrak{N} \vDash \forall x.\varphi[x]$ y no habría nada que probar.

⟨2⟩4. Definimos $Y = \{\mathbf{a} : \mathbf{a} <_{\mathbf{M}} \mathbf{c} \text{ y } \mathfrak{N} \vDash \varphi[\mathbf{a}]\}$.

⟨2⟩5. Y es $\mathfrak{M}$-finito.

⟨3⟩1. Sea $\varphi^*[x]$ el resultado de sustituir cada parámetro $\mathbf{X} \in \mathrm{Coded}_{\mathfrak{M}}(I)$ por la fórmula que describe al conjunto $\mathfrak{M}$-finito X^* tal que $X^* \cap I = \mathbf{X}$. $\varphi^*[x] \equiv \exists y.\theta^*(x, y)$ con $\theta^* \in \mathrm{GEN}\Sigma_0^0$ con parámetros en M.

DEMOSTRACIÓN: Estamos pasando una fórmula de L_2 a L_{PRA}, sustituyendo todas las fórmulas atómicas $t \in \mathbf{X}$ por una fórmula Σ_0^0 en PRA y luego usando la interpretación canónica para el resto de símbolos, por tanto está claro que la fórmula resultante será $\mathrm{GEN}\Sigma_0^0$ (pues la original era Σ_1^0). Estamos siendo laxos con la diferencia entre ser $\mathrm{GEN}\Sigma_0^0$ y ser equivalente a una fórmula $\textsc{Gen}\Sigma_0^0$ con parámetros en M, pero como es habitual esto no será un problema.

⟨3⟩2. Sea $\mathbf{d} \in M$ tal que $\mathbf{d} \notin I$. Definimos

$$Z = \{(\mathbf{a}, \mathbf{b}) \mid \mathfrak{M} \vDash \mathbf{a} < \mathbf{c} \wedge \mathbf{b} < \mathbf{d} \wedge \theta^*(\mathbf{a}, \mathbf{b}) \wedge \neg\exists b' < \mathbf{b}.\theta^*(\mathbf{a}, b')\}.$$

⟨3⟩3. $Z \cap I$ es $\mathfrak{M}$-finito

DEMOSTRACIÓN: Por el lema 6.11 y ⟨3⟩2 tenemos que Z es $\mathfrak{M}$-finito. Además la $\mathfrak{M}$-cardinalidad de Z es a lo sumo $\mathbf{c}$. Por semirregularidad $Z \cap I$ está acotado en I y así $Z \cap I$ es $\mathfrak{M}$-finito.

⟨3⟩4. Q.E.D.

DEMOSTRACIÓN: Por el 6.11 y por ⟨3⟩3 tenemos que $Y = \{\mathbf{a} \mid \exists b.(\mathbf{a}, b) \in Z \cap I\}$ es $\mathfrak{M}$-finito.

⟨2⟩6. Q.E.D.

DEMOSTRACIÓN: Por ⟨2⟩5 Y es $\mathfrak{M}$-finito, además $\mathbf{c} \notin Y$ y por ⟨2⟩1 sea $\mathbf{b}$ el elemento mínimo para $<_{\mathfrak{M}}$ tal que $\mathbf{b} \notin Y$. Por tanto $\mathbf{b} \leq_{\mathfrak{M}} \mathbf{c}$ y como $\mathbf{c} \in I$ se tiene que $\mathbf{b} \in I$. Ahora si $\mathbf{b} = 0_{\mathfrak{M}}$ se tendría que $\mathfrak{N} \vDash \neg\varphi[\underline{0}]$ lo que contradice ⟨2⟩2. Si no es cero, entonces $\mathbf{b} = \underline{S}_{\mathfrak{M}}(\mathbf{b}')$ y por ser mínimo $\mathfrak{N} \vDash \mathbf{b}'$ así que por ⟨2⟩2 tenemos que $\mathfrak{N} \vDash \varphi[\mathbf{b}]$, absurdo.

⟨1⟩5. $\mathfrak{N} \vDash \Sigma_1^0$-SEP.

⟨2⟩1. Sean $\varphi_i[x] \in (\Sigma_1^0)_{\mathfrak{N}}$ para $i = 0, 1$.

⟨2⟩2. Para $i = 0, 1$ definimos

$$A_i = \{\mathbf{a} \in I \mid \mathfrak{N} \vDash \varphi_i[\mathbf{a}]\},$$

y supongamos que $A_0 \cap A_1 = \varnothing$. Es suficiente probar que A_0 y A_1 se pueden separan por un subconjunto de I $\mathfrak{M}$-codificado.

DEMOSTRACIÓN: Por la semántica y la definición de $\mathfrak{N}$.

⟨2⟩3. Sea $\varphi_i^*[x]$ el resultado de sustituir cada parámetro $\mathbf{X} \in \mathrm{Coded}_{\mathfrak{M}}(I)$ por la fórmula que describe al conjunto $\mathfrak{M}$-finito X^* tal que $X^* \cap I = \mathbf{X}$. $\varphi_i^*[x] \equiv \exists y.\theta_i^*(x, y)$ con $\theta_i^* \in \mathrm{GEN}\Sigma_0^0$ con parámetros en M.

DEMOSTRACIÓN: Estamos pasando una fórmulas de L_2 a L_{PRA}, sustituyendo todas las fórmulas atómicas $t \in \mathbf{X}$ por una fórmula Σ_0^0 en PRA y luego usando la interpretación canónica para el resto de símbolos, por tanto está claro que la fórmula resultante será $\mathrm{GEN}\Sigma_1^0$ con parámetros en M (pues la original era Σ_1^0).

⟨2⟩4. Sea $\mathbf{d} \in M$ tal que $\mathbf{d} \notin I$ y definimos

$$Y^* = \{\mathbf{a} \mid \mathfrak{M} \vDash \mathbf{a} < \mathbf{d} \wedge \exists b < \mathbf{d}.\theta_1^*(\mathbf{a}, b) \wedge \forall b' < b.\neg\theta_0^*(\mathbf{a}, b')\}.$$

⟨2⟩5. $A_1 \subseteq Y^*$ y $A_0 \cap Y_1 = \varnothing$.

DEMOSTRACIÓN: Por definición en ⟨2⟩4.

⟨2⟩6. Q.E.D.

DEMOSTRACIÓN: Por lema 6.11 tenemos que $Y = Y^* \cap I$ es un subconjunto de I $\mathfrak{M}$-codificado. Por ⟨2⟩5 separa A_0 y A_1, pero por ⟨2⟩2 eso es suficiente para demostrar lo que queríamos.

⟨1⟩6. $\mathfrak{N} \vDash \Delta_1^0$-COMP.

DEMOSTRACIÓN: Sale directamente de ⟨1⟩5.

⟨1⟩7. Q.E.D.

DEMOSTRACIÓN: Claramente $\mathfrak{N} \vDash$ BASIC, por ⟨1⟩4 tenemos que $\mathfrak{N} \vDash \Sigma_1^0$-IND, por ⟨1⟩6 $\mathfrak{N} \vDash \Delta_1^0$-COMP y gracias al teorema 3.3 y por ⟨1⟩5 tenemos que $\mathfrak{N}$ será un modelo de WKL$_0$.

□

Definición 6.18. Sea $\mathfrak{M}$ un modelo de PRA. Dados $\mathbf{b}, \mathbf{c} \in M$ entonces escribimos $\mathbf{b} \ll_{\mathfrak{M}} \mathbf{c}$ si para todo símbolo de función 1-ario primitivo recursivo $\underline{f}$ se tiene que $\underline{f}_{\mathfrak{M}}(\mathbf{b}) <_{\mathfrak{M}} \mathbf{c}$.

■

La noción anterior se usa para probar la existencia de los cortes semirregulares, aunque no entraremos en la demostración del teorema, ya que está más relacionada con modelos de la aritmética de primer orden y excede el contenido del presente trabajo. (Se puede encontrar una prueba en la sección IX.3 de Simpson [8], la cual está basada como dijimos anteriormente en el trabajo de Kirby y Paris [5]).

Lema 6.14 (**Existencia de cortes semirregulares**). *Sea $\mathfrak{M}$ un modelo numerable de PRA. Sean $\mathbf{b}, \mathbf{c} \in M$ tales que $\mathbf{b} \ll_{\mathfrak{M}} \mathbf{c}$. Entonces existe un corte semirregular I de $\mathfrak{M}$ tal que $\mathbf{b} \in I$ pero $\mathbf{c} \notin I$.*

Y, finalmente, obtenemos el teorema que queríamos demostrar:

Teorema 6.15. *Sea* $\psi \in \Pi^0_2 \cap \mathrm{Sent}$. *Si* $WKL_0 \vdash \psi$, *entonces* $PRA \vdash \mathrm{CanInterp}(\psi)$.

Demostración:
⟨1⟩1. Supongamos que $\mathrm{PRA} \nvdash \mathrm{CanInterp}(\psi)$.

⟨1⟩2. Existe $\mathfrak{M}'$ un modelo contable de PRA tal que $\mathfrak{M}' \nvDash \psi$.

Demostración: Por el teorema de completitud de Gödel.

⟨1⟩3. $\psi \equiv \forall y \exists z.\theta[y,z]$ donde $\theta[y,z] \in \Sigma^0_0$.

Demostración: Por ser $\psi \in \Pi^0_2 \cap \mathrm{Sent}$.

⟨1⟩4. Existe $\mathbf{b}' \in M'$ tal que $\mathfrak{M}' \vDash \neg\exists z.\theta[\mathbf{b}', z]$.

Demostración: Por ⟨1⟩2 y ⟨1⟩3.

⟨1⟩5. Sean $\underline{b}, \underline{c}$ son constantes nuevas y sea la teoría
$T = \mathrm{PRA} + (\neg\exists z.\theta[\underline{b}, z]) + \{\underline{f}(\underline{b}) < \underline{c} \mid \underline{f}$ es un símbolo 1-ario primitivo recursivo$\}$.

⟨1⟩6. Existe $\mathfrak{M}$ modelo del T.

Demostración: Para cualquier subconjunto finito T_0 de los axiomas T podemos escoger un elemento $\mathbf{c}'_0 \in M'$ tal que $\underline{f}_{\mathfrak{M}'}(\mathbf{b}) <_{\mathfrak{M}'} \mathbf{c}'_0$ para la cantidad finita de símbolos de función 1-arios primitivos recursivos $\underline{f}$ que aparezcan en T_0. Así $\mathfrak{M}' \vDash T_0$ donde $\underline{b}_{\mathfrak{M}'} = \mathbf{b}'$ y $\underline{c}_{\mathfrak{M}'} = \mathbf{c}'_0$. Por el teorema de compacidad, T tiene un modelo numerable.

⟨1⟩7. Existe $\mathfrak{M}$ un modelo de PRA tal que existen $\mathbf{b}, \mathbf{c} \in M$ tales que $\mathbf{b} \ll_{\mathfrak{M}} \mathbf{c}$ y $\mathfrak{M} \vDash \neg\exists z.\theta[\mathbf{b}, z]$.

Demostración: Directamente por ⟨1⟩6.

⟨1⟩8. Existe un corte semirregular I de $\mathfrak{M}$ tal que $\mathbf{b} \in I$ pero $\mathbf{c} \notin I$.

Demostración: Gracias al lema 6.14 y a ⟨1⟩7.

⟨1⟩9. $\mathfrak{N} = (I, \mathrm{Coded}_{\mathfrak{M}}(I), +_{\mathfrak{M}} \restriction I, \cdot_{\mathfrak{M}} \restriction I, 0_{\mathfrak{M}}, 1_{\mathfrak{M}}, <_{\mathfrak{M}} \restriction I)$ es un modelo de WKL_0.

Demostración: Por ⟨1⟩8 y el lema 6.13.

⟨1⟩10. Q.E.D.

Demostración: Como $\mathbf{b} \in I$ y por ⟨1⟩7 tenemos que $\mathfrak{N} \vDash \neg\exists z.\theta[\mathbf{b}, z]$, por tanto $\mathfrak{N} \nvDash \psi$ y por el teorema de validez $\mathrm{WKL}_0 \nvdash \psi$.

□

Una vez demostrado el teorema deseado, expongamos brevemente su relación con el programa de Hilbert. La idea principal del programa de Hilbert era justificar la matemática infinita mediante métodos finitistas, es decir, probar la consistencia de (una gran porción) de las matemáticas cuya metodología incluye métodos de construcción infinitos mediante métodos finitistas. Idealmente, una realización plena del programa de Hilbert habría sido dada por la existencia de, digamos, una prueba de la consistencia de la teoría de conjuntos ZFC en la matemática finitista. Aunque Hilbert no dio una definición precisa, gracias al trabajo de Tait, se ha llegado al consenso general de que la matemática finitista está caracterizada por un sistema como PRA. Entonces, para cumplir el programa de Hilbert, sería necesario demostrar la consistencia de la teoría de conjuntos en PRA, pero es bien sabido que por el segundo teorema de incompletitud de Gödel esto es imposible (más aún, ni tan siquiera la consistencia de la propia matemática finistista PRA puede demostrada en PRA).

Los teoremas de incompletitud de Gödel destruyen por tanto la posibilidad de una realización plena del programa de Hilbert. Sin embargo, no sería justo afirmar que el programa de Hilbert fracasó en su totalidad. De hecho, varios autores han propuesto diversas realizaciones parciales del programa de Hilbert.

Simpson [8] en la sección IX.3 propone una tal realización parcial del programa de Hilbert, argumentando que una buena porción de las matemáticas numerables del día a día sí se pueden justificar por métodos finitistas, pues son *reducibles* a métodos finitistas.

Más concretamente, Simpson propone estudiar la siguiente cuestión: *¿Qué subsistemas de la aritmética de segundo orden son conservativos para* Π^0_1 *fórmulas cerradas sobre* RCA_0*?* Nótese que si un tal sistema demuestra la consistencia de una teoría, entonces PRA también lo prueba (ya que la fórmula que afirma la consistencia de una teoría es de complejidad sintáctica Π^0_1). Simpson interpreta este hecho como un argumento a favor de la tesis de que los teoremas demostrados en un tal sistema estarían justificada por métodos finitistas; serían, en terminología de Simpson, reducibles a métodos finitistas. Esto explica la relevancia de nuestro teorema de conservación 6.15. Con este teorema hemos demostrado que WKL_0 es reducible-finitista y, por tanto, de acuerdo a la tesis de Simpson, los teoremas demostrados en WKL_0 tienen una justificacón finitista.

Conclusiones

En este trabajo hemos realizado una primera aproximación a la matemática inversa. Hemos estudiado los cinco subsistemas de la aritmética de segundo orden más relevantes, los Big Five, y hemos codificado una buena parte de la matemática en RCA_0 a la vez que hemos establecido la equivalencia de diversos teoremas matemáticos con alguno de los subsistemas; por ejemplo, el teorema Heine-Borel en $[0, 1]$ con WKL_0 o el teorema de Ramsey para conjuntos de cardinalidad n (con $n \in \omega, n \geq 3$) con ACA_0. Esto nos ha permitido clasificar los teoremas según la potencia del subsistema al que son equivalentes. Se ha estudiado con especial detalle la codificación en el lenguaje de la aritmética del conjunto de los reales $\mathbb{R}$ vía sucesiones de Cauchy, al tratarse de la codificación más elaborada.

Además hemos realizado un estudio de las partes de primer orden de $\mathrm{RCA}_0, \mathrm{WKL}_0$ y ACA_0, viendo que se corresponden con $I\Sigma_1$ (para las dos primeras teorías) y con PA (para la tercera de ellas). Además, hemos demostrado que WKL_0 es conservativa sobre PRA para Π^0_2 fórmulas cerradas y hemos expuesto la relación que tiene este resultado con los fundamentos de la matemática y el programa de Hilbert.

Para el futuro, podría ser interesante estudiar la matemática inversa de alto orden, que consiste en cambiar el paradigma lógico de lógica de segundo orden a una teoría de tipos simples. Esto permitiría eliminar la codificación de muchos conceptos matemáticos y poder estudiarlos sin miedo a que la codificación afecte a los resultados obtenidos. Otra continuación interesante sería centrarse en el estudio de la teoría de modelos de los subsistemas, ya que este trabajo no ha desarrollado nada a ese aspecto. También sería muy interesante estudiar la relación entre la teoría de la computación y la matemática inversa, ya que esta proporciona una visión complementaria a la centrada en la teoría de la demostración y en la teoría de modelos.

Bibliografía

[1] Harvey M. Friedman, *Systems of second order arithmetic with restricted induction, I, II* (abstracts), The Journal of Symbolic Logic, vol. 41, 1976.

[2] Harvey M. Friedman, *The inevitability of logical strength: Strict reverse mathematics*, manuscrito, 2009.

[3] Denis R. Hirschfeldt, *Slicing the Truth*, Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore, vol. 28, 2014.

[4] Jeffry L. Hirst, *A survey of the reverse mathematics of ordinal arithmetic*, en *Reverse Mathematics 2001*, Cambridge University Press, 2005.

[5] Laurence A. S. Kirby and Jeff B. Paris *Initial segments of models of Peano's axioms*. In Alistair Lachlan, Marian Srebrny, and Andrzej Zarach, editors. Set Theory and Hierarchy Theory V, volume 619 of Lecture Notes in Mathematics, pp. 211-226. Springer-Verlag, Berlin, 1977.

[6] Leslie Lamport, *How to write a* 21^{st} *century proof*, J. Fixed Point Theory Appl. 11, pp. 43-63, 2012.

[7] Stephen G. Simpson, *Partial Realizations of Hilbert's Program*, The Journal of Symbolic Logic, vol. 53, pp. 349-363, 1988.

[8] Stephen G. Simpson, *Subsystems of Second Order Arithmetic*, Cambridge University Press, segunda edición, 2009.

[9] S. Simpson, H. Friedman et al. (editores), *FOM – Foundations of Mathematics* (e-mail list).

[10] John Stillwell, *Reverse Mathematics, Proofs from the Inside Out*, Princeton University Press, 2018.