UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE FILOSOFÍA

Departamento de Lógica y Filosofía de la Ciencia

TÉCNICAS DE DEMOSTRACIÓN DE INDECIBILIDAD E INSEPARABILIDAD EN TEORIAS FORMALES

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Enrique Gallego Castaño

Bajo la dirección del doctor

José F. Prida

Madrid, 2001

ISBN: 84-669-2391-8

UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE FILOSOFÍA
DEPARTAMENTO DE LÓGICA Y FILOSOFÍA DE LA CIENCIA

TESIS DOCTORAL

Técnicas de demostración de indecidibilidad e inseparabilidad en teorías formales

Enrique Gallego Castaño

Director: Dr. José F. Prida

Madrid, Mayo de 2001

Técnicas de demostración de indecidibilidad e inseparabilidad en teorías formales

Memoria presentada para optar al grado de doctor por Enrique Gallego Castaño

Dirigida por D. José F. Prida, doctor en Ciencias Matemáticas, catedrático de Lógica y Filosofía de la Ciencia de la U.C.M.

Madrid, Mayo de 2001

Agradecimientos

Este trabajo se ha realizado fundamentalmente gracias a la dirección del profesor D. José F. Prida, a quien quiero manifestar mi sincero reconocimiento. De él he aprendido Lógica, Computación y Fundamentos de Matemática. Muchas ideas y textos que aquí aparecen tienen su origen en sus clases y publicaciones.

Varios profesores de la Universidad Complutense me orientaron amablemente en asuntos colaterales al tema central. Tengo un especial recuerdo de Rodolfo Fernández que me animó y ayudó muy cordialmente.

Las bibliotecas de la UCM y la UNED me han permitido consultar la literatura necesaria.

Durante el curso 1997/98 disfruté de una “licencia por estudios” concedida por el MEC. En ese tiempo estudié las relaciones entre la lógica modal y la teoría de la demostración. Pero lo estudiado entonces ha tenido escaso reflejo en el texto de esta memoria.

ÍNDICE

UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE FILOSOFÍA
DEPARTAMENTO DE LÓGICA Y FILOSOFÍA DE LA CIENCIA

TESIS DOCTORAL

Técnicas de demostración de indecidibilidad e inseparabilidad en teorías formales

Enrique Gallego Castaño

Director: Dr. José F. Prida

Madrid, Mayo de 2001

PALABRAS CLAVE: Lógica formal, Recursión, Fundamentos de Matemáticas

RESUMEN

El objetivo de esta memoria es analizar las técnicas para la demostración de la indecidibilidad de las teorías matemáticas que aparecen habitualmente en Matemáticas : teoría de grupos, teoría de anillos, teoría de grafos, etc.
Los teoremas fundamentales de indecidibilidad se obtuvieron en la década de 1930 por Church, Turing, Gödel y Rosser. Posteriormente se obtuvieron nuevos resultados de indecidibilidad utilizando la idea de Tarski de interpretar unas teorías en otras. Revisamos los conceptos fundamentales y presentamos formas refinadas de los principales resultados. Pero el método de Tarski no es adecuado para teorías con modelos finitos.
Una alternativa es considerar la cuestión utilizando la noción de inseparabilidad, más general que la de no recursividad.
El punto de partida es la inseparabilidad finita del cálculo de predicados de primer orden. Simplificamos la demostración de Büchi al utilizar máquinas de registros y un teorema de Minsky.
Damos una forma fuerte de un teorema, utilizado por Rabin y Ershov, que nos permite demostrar la inseparabilidad finita de diversas teorías.

UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE FILOSOFÍA
DEPARTAMENTO DE LÓGICA Y FILOSOFÍA DE LA CIENCIA

TESIS DOCTORAL

Techniques of proving undecidability and inseparability in formal theories

Enrique Gallego Castaño

Director: Dr. José F. Prida

Madrid, Noviembre de 2001

KEYWORDS: Formal Logic, Recursion, Foundations of Mathematics

ABSTRACT

In this dissertation, techniques for proving undecidability of a number of important classical theories arising in Mathematics (the theory of groups, the theory of rings, the theory of graphs, etc) are considered and discussed.
The fundamental theorems on undecidability were obtained in the 1930's by Church, Turing , Gödel and Rosser. Subsequently the first general method for establishing the undecidability of elementary theories was proposed by Tarski. The main idea is the procedure of interpretation of one theory into another. We present a survey of the fundamental concepts and main results in a refined way. But the method is unable to manage theories with finite models.
An alternative approach is developed. We present the results in a more general setting using the notion of inseparability.
Starting point is the finite inseparability of the first-order predicate calculus. We simplify the proof of Büchi, making use of register machines, and taking advantage of a theorem of Minsky.
A stronger form of a theorem used by Rabin and Ershov is established allowing to proof the finite inseparability of several theories.

1. INTRODUCCIÓN

El objeto de este trabajo es analizar métodos para la demostración de la indecidibilidad de las teorías formales que aparecen en Matemáticas. Los fundamentos lógicos de dichos métodos son en gran parte independientes de las características concretas de las teorías a considerar, por lo que es pertinente un estudio de los mismos desde un punto de vista lógico. Aquí se abordarán las bases lógicas de los métodos y se mostrarán desde una perspectiva unificada sus posibilidades y limitaciones. Se reelaborarán y fortalecerán algunos resultados anteriores y se aplicarán a la demostración de la indecidibilidad de las teorías matemáticas habituales. Algunos refinamientos de los teoremas básicos permiten simplificar claramente algunas demostraciones. El ámbito de estudio se limita a las teorías formuladas en lógica clásica de primer orden (con lenguajes finitos). El concepto de decidibilidad es el clásico (en el marco de la tesis de Church) correspondiendo al concepto formal de recursividad.

En los textos de teoría de la computabilidad suelen presentarse ejemplos de conjuntos no recursivos, pero son habitualmente conjuntos de índices en una enumeración de las funciones recursivas (de las funciones totales, funciones de rango infinito, teorema de Rice, ...) u otros sin importancia real para el matemático. Los conjuntos no recursivos presentados en este trabajo corresponderán a teorías que aparecen naturalmente en el ámbito de las matemáticas habituales: teoría de grupos, teoría de anillos, teoría de grafos, etc. Nótese que en la revisión sobre *Unsolvable Problems* de Martin Davis en 1977 en el *Handbook of Mathematical Logic* [12] se tratan problemas relacionados con la teoría de grupos o semigrupos (problemas de palabras en semigrupos, ...) pero no se abordan los problemas de decisión globales de las teorías de grupos, anillos, etc.

Decidibilidad y computabilidad

Estaremos interesados en un tipo particular de problemas de decisión: el problema de decisión correspondiente a una teoría formal. Las teorías son ciertos conjuntos de sentencias en un lenguaje dado cerrados bajo la relación de consecuencia.
Históricamente este es el tipo de problemas que se plantearon en el programa formalista de Hilbert : establecer para las teorías matemáticas procedimientos de tipo finitista para decidir si una fórmula dada es o no un teorema de la teoría. Este es el problema de decisión de la teoría o *Entscheidungsproblem*.
Plantear este problema constituía la expresión de una creencia muy generalizada en la posibilidad de resolver las cuestiones matemáticas por procedimientos mecánicos de cálculo. Tradicionalmente se hace remontar esta idea al sueño de Leibniz de tener un

calculus ratiocinator que decidiera sobre las verdades lógicas mediante la reducción del razonamiento al cálculo aritmético.
Diremos que un conjunto de sentencias Φ es decidible si existe un procedimiento efectivo de determinar, dada una sentencia φ del lenguaje, si $\varphi \in \Phi$ o si $\varphi \notin \Phi$.
Obsérvese que la existencia de conjuntos de sentencias no decidibles se deduce fácilmente por un argumento de cardinalidad : la cantidad de procedimientos efectivos es a lo sumo numerable, pues un procedimiento efectivo es una cantidad finita de instrucciones en un lenguaje; sin embargo el cardinal de la familia de conjuntos de sentencias es no numerable. Un razonamiento similar vale también para teorías.

El problema de encontrar un procedimiento que decida si una sentencia es o no un teorema de la lógica está muy relacionado con otro problema planteado en la escuela de Hilbert: el problema de satisfactibilidad, a saber, dada una sentencia, determinar si es satisfactible o no en algún dominio.
Estos dos problemas están relacionados, pues en virtud del teorema de completitud de la lógica de primer orden una sentencia α es un teorema lógico si y sólo si α es verdadera en todas las estructuras, y por lo tanto α es satisfactible si y sólo si su negación $\neg\alpha$, no es un teorema lógico.

Puesto que las teorías consideradas tienen una sintaxis basada en un lenguaje de tipo finito (o numerable) es posible, por las conocidas técnicas debidas a Gödel, codificar las expresiones del lenguaje mediante números naturales; tanto la codificación como la decodificación se realizan de una forma efectiva. Mediante la codificación, a cada fórmula α se le asigna un número natural $\alpha^{\#}$ y por tanto a una teoría T le corresponde un conjunto de números naturales $T^{\#}$. De esta forma el problema de determinar si $\alpha \in T$ se traduce en un problema de decisión numérica, a saber, si $\alpha^{\#} \in T^{\#}$.

Así pues, bastará considerar problemas de decisión numéricos, esto es, el problema de decisión asociado a un conjunto $A \subset \omega$. Pero el problema de decidir si un número natural $n \in \omega$ verifica o no que $n \in A$ consiste exactamente en calcular su función característica

$$c_A : \omega \to \omega$$
$$c_A(n) = \begin{cases} 1 & si\ n \in A \\ 0 & si\ n \notin A \end{cases}$$

Así el problema de determinar si A es decidible se reduce al problema de determinar si la función c_A es computable. Esto indica que la noción de *decidibilidad* se reduce a la noción de *computabilidad*.

Es claro que para mostrar que cierta función f es computable basta con exhibir el algoritmo que calcula f. La situación es distinta para ver que un conjunto *no* es decidible o que una función *no* es computable. Se trata ahora de una afirmación sobre el total de la clase de algoritmos. Esto nos obliga a determinar claramente el concepto intuitivo de algoritmo o sea a precisar la noción intuitiva de función computable.

Capturar la noción intuitiva de función computable en una definición parece una cuestión destinada al fracaso. La mayor parte de los conceptos matemáticos intuitivos no constituyen conceptos categóricos, sino que dependen del formalismo considerado: la

noción de “constructible” es claramente dependiente del sistema formal considerado: lo que no es constructible con regla y compás lo es con otros medios; el concepto de “medible” depende del sistema considerado: integral de Cauchy, integral de Riemann, integral de Lebesgue, ... ; el concepto de “definible” no es absoluto sino relativo al lenguaje considerado : lo que no es definible en un lenguaje de primer orden bien puede serlo en un lenguaje de segundo orden. Parece que lo extraordinario sería que se pudiera dar una noción precisa de “computable” - o de “algoritmo”- independiente del formalismo considerado. Más aún si consideramos el siguiente argumento diagonal.
Puesto que los algoritmos están expresados por una sucesión finita de instrucciones, podremos considerar una enumeración de los mismos : A_1, A_2, A_3, ... Llamaremos φ_n a la función computable calculada por el algoritmo A_n. Podremos definir entonces la función $f(n) = \varphi_n(n) + 1$. Tal función debería ser obviamente computable. Pero en tal caso sería una cierta φ_d con lo que tendríamos la siguiente contradicción :

$$\varphi_d(d) = \varphi_d(d) + 1$$

Por lo tanto *f* no podría ser computable.

El hecho sorprendente es que los distintos intentos de formalizar el concepto de algoritmo o de función computable : máquinas de Turing, λ-cálculo, funciones recursivas, máquinas de registros, sistemas de producción de Post, algoritmos de Markov, ... dan lugar a conjuntos extensionalmente coincidentes. Esto hace que tales nociones sean equivalentes, por lo que parece que cualquiera de ellas es una adecuada formalización del concepto intuitivo de “función computable”. Esta afirmación suele ser denominada *Tesis de Church* o *Tesis de Turing-Church*.
Las consideraciones que nosotros haremos darán por buena esta tesis por lo que identificaremos la noción intuitiva de “computable” con cualquiera de las nociones anteriores, por ejemplo, con “calculable por una máquina de registros” o bien con “calculable por una función recursiva parcial”.

Indecidibilidad e inseparabilidad

Los estudios sobre el problema de decisión deben enmarcarse en el ámbito del programa de Hilbert y los teoremas de Gödel. Los primeros resultados sobre indecidibilidad de teorías matemáticas son los relativos a la indecidibilidad de la aritmética. Estos resultados se basan en problemas indecidibles relativos a máquinas de Turing (cf. [62]) y en la posibilidad de representar las funciones efectivamente calculables en la aritmética (cf. Church [6]).
Basándose en la indecidibilidad de un fragmento de la aritmética Church demostró en 1936 (cf. [6]) la indecidibilidad del cálculo de predicados .
En 1953 se publicó el libro *Undecidable theories* de A. Tarski, A. Mostowski y R. M. Robinson [60] que es la referencia clásica en este tema. Tarski y su escuela emplearon la idea de interpretar unas teorías en otras y estudiaron la transmisión de la indecidibilidad

por este método[1]. La idea básica subyacente en la noción de "interpretación" de Tarski consiste en reemplazar los símbolos de una cierta teoría por expresiones en otra teoría de forma que los axiomas de la primera se traduzcan en teoremas de la otra. En 1949 Julia Robinson demostró, en su tesis doctoral bajo la dirección de Tarski, siguiendo este procedimiento, la indecidibilidad de la teoría de cuerpos [48]. En el libro de Tarski, Mostowski y Robinson se aplica la técnica a demostrar la indecidibilidad de la teoría de grupos. Las ideas y terminología del libro son fundamentales pero insuficientes[2] : al final del mismo se plantea como problema abierto la indecidibilidad de la teoría de grupos finitos, que no puede ser abordada con las técnicas propuestas.
Hay que señalar que en la técnica de Tarski se parte de una teoría aritmética **Q**, cuya indecidibilidad se va transmitiendo a otras teorías. Como **Q** no tiene modelos finitos las fórmulas finitamente refutables coinciden con las refutables por lo que no tiene interés en el contexto del trabajo de Tarski el concepto de fórmula finitamente refutable. Sin embargo al estudiar la teoría de los grupos finitos estamos considerando una clase de estructuras finitas y las fórmulas que se verifican o no en dicha clase.
El problema es abordable utilizando el concepto de inseparabilidad, introducido por Trakhenbrot y Kleene hacia 1950 [25]. La presentación de la teoría de la recursión y el estudio de la incompletitud en la tesis de Smullyan, publicada, en forma revisada, en 1961 con el nombre *Theory of Formal Systems* [56], utiliza la noción aplicada a sistemas formales que denomina "sistemas de Rosser". El concepto de inseparabilidad se utiliza por la escuela de Novosibirsk en el estudio de teorías algebraicas. Un resumen de dicha línea de investigación es el artículo *Elementary Theories* de Ershov *et al.* de 1965 [15].

Concretamos a continuación el trabajo realizado en esta memoria :

- Se han revisado los trabajos originales de los autores que han creado las técnicas y se han formulado dichas técnicas de una forma en general más sencilla que las exposiciones originales y con una nomenclatura unificada . En el caso de la noción básica de interpretación de Tarski se ha usado una formulación más cómoda.
- Se han señalado las limitaciones y potencia de las técnicas.
- Se ha estudiado sistemáticamente la característica de inseparabilidad de las teorías (más fuerte que la de indecidibilidad).
- Se han formulado los teoremas fundamentales en términos de clases de estructuras, lo que permite en algunos casos una presentación más clara e intuitiva.
- Se ha simplificado la demostración de Büchi de la indecidibilidad del cálculo de predicados, obteniendo el resultado más fuerte de inseparabilidad finita.
- Se ha dado una versión más fuerte del importante teorema de Rabin-Ershov necesaria en algún caso.
- Se ha obtenido algún resultado nuevo : inseparabilidad de la teoría de retículos atómicos distributivos (que aparece erróneamente en Ershov [15] como ejemplo de

[1] Esta noción quizá fuese sugerida por los estudios dedicados a la consistencia relativa de teorías, en donde la consistencia de una teoría se prueba "interpretando" la teoría en otro modelo ; por ejemplo las pruebas de consistencia relativa de las geometrías o del álgebra de los números complejos.(cf. [27])

[2] Por otra parte el libro de Tarski adolece de ciertos defectos, fundamentalmente la falta de formulación precisa de muchos conceptos o cierta notación hoy mejorada.

teoría con teoría finita decidible), codificación de una relación binaria en la teoría de grafos sin igualdad, (sugerencia de J. F. Prida) ...

- Se ha dado una versión rápida del teorema de inseparabilidad de la aritmética de Robinson.

Descripción de los capítulos

En el segundo capítulo se han revisado algunos temas básicos de la teoría de la recursión : productividad, creatividad y completitud. Se da una demostración del importante teorema de Myhill relativo a la relación entre creatividad y equivalencia.
En el tercer capítulo, se desarrolla el concepto de inseparabilidad y se establece la teoría básica de los pares de conjuntos inseparables. Un teorema de Smullyan permite caracterizar los pares de conjuntos efectivamente inseparables en términos de creatividad y de completitud. Desde la perspectiva del programa de Klein, éste teorema permite considerar como iguales, desde el punto de vista de la teoría de la recursión, los pares de conjuntos efectivamente inseparables.
En el cuarto capítulo se presenta rápidamente la terminología básica acerca de las teorías de primer orden : teorías axiomatizables, teorías completas, teorías decidibles e indecidibles,... Se establece la terminología adecuada para clases de estructuras y se señalan las propiedades básicas.
En el capítulo quinto se da una definición de la noción básica de interpretación. La definición dada aquí *no* es la original de Tarski, pero permite obtener más cómodamente los resultados de transmisión de la indecidibilidad e inseparabilidad por medio de interpretaciones de unas teorías en otras y de unas clases de estructuras en otras. En este capítulo se demuestra una versión más fuerte del teorema de Rabin-Scott-Ershov sobre la transmisión de la inseparabilidad. Este teorema será la base para la técnica de inmersión semántica utilizada sistemáticamente en el décimo capítulo.
El capítulo sexto presenta las ideas básicas de la técnica basada en el teorema del punto fijo o lema de diagonalización, que es la forma en que suele aparecer en los manuales la demostración de la indecidibilidad de la aritmética. Las ideas de esta demostración tienen su origen en la demostración de Gödel del teorema de incompletitud.
El capítulo séptimo expone la técnica usada por Tarski en la demostración de la indecidibilidad de la teoría de grupos. Se parte de la indecidibilidad de la aritmética de Robinson y se obtiene la indecidibilidad de diversas teorías : cálculo de predicados, teoría de anillos, teoría de grupos.
El capítulo octavo se dedica a demostrar la inseparabilidad de las teorías matemáticas fundamentales sin modelos finitos : la aritmética y la teoría de conjuntos.
El capítulo noveno establece la inseparabilidad finita del cálculo de predicados siguiendo las ideas de Büchi, pero simplificando la demostración al utilizar máquinas de registros y sacar partido a un teorema de Minski relativo a la posibilidad de simular una máquina de registros por una máquina de dos registros.
Partiendo de la inseparabilidad del cálculo de predicados en el capítulo décimo se demuestra la inseparabilidad de diversas teorías importantes desde el punto de vista matemático : teoría de grafos, teoría de retículos, teoría de anillos, teoría de grupos. Para

ello se realizan sucesivas aplicaciones del método de inmersión semántica de Rabin-Ershov.
El capítulo undécimo expone algunas conclusiones del trabajo.

Nota Previa : Glosario de notaciones utilizadas

Prácticamente la totalidad de las notaciones usadas son absolutamente estándar. Algunas de estas nociones elementales de teoría de la recursión, teoría de modelos, lógica o teoría de conjuntos se utilizan sin dar definiciones o explicaciones de las mismas. No obstante se incluye aquí una referencia rápida de las notaciones utilizadas en el texto, para facilitar posibles consultas o resolver ambigüedades.

Teoría de la recursión

ω : Conjunto de los números naturales {0, 1, 2, ...}
$\mathbb{Z}$: Conjunto de los números enteros {..., -2, -1, 0 , 1, 2 , ...}
φ_x : Función recursiva parcial de índice x
W_x : Dominio de φ_x
$W_{x,s}$: Conjunto de los $a \in \omega$ tales que el programa de número x produce un output en s pasos cuando comienza con input a
$\varphi(x)\downarrow$: La función φ está definida en x
$\varphi(x)\uparrow$: La función φ diverge en x

Escribiremos $\varphi(x) = \psi(x)$ para indicar que, o bien ambas funciones están indefinidas en x, o bien ambas están definidas en x y su valor en x coincide. (Lo que Kleene [24] llama "igualdad completa", que en muchos textos suele indicarse por $\varphi(x) \simeq \psi(x)$)

Teoría de modelos

c^A, f^A, P^A : Constante, función y predicado designados en la estructura A con universo A por los símbolos de constante, función y predicado c, f, y P
$\mathsf{I} = (\mathsf{A} ; v)$: Interpretación sobre la estructura A con valoración de variables v
v_z^a : Valoración que coincide con v salvo en la variable z, siendo v(z) = a
$\mathsf{I} \vDash \alpha$: La fórmula α es verdadera en la interpretación I
$\mathsf{I} \nvDash \alpha$: La fórmula α es falsa en la interpretación I
$\mathsf{A} \vDash \alpha$: La estructura A es un modelo de la fórmula α (Para toda interpretación I en A se verifica $\mathsf{I} \vDash \alpha$)
$\mathsf{A} \nvDash \alpha$: La estructura A no es un modelo de la fórmula α
$\mathsf{A} \vDash \Phi$: La estructura A es modelo del conjunto de fórmulas Φ
$\Phi \vDash \alpha$: Todo modelo de Φ es modelo de α, e.e., α es consecuencia de Φ
$\vDash \alpha$: Abreviatura de $\varnothing \vDash \alpha$, esto es, α es válida en toda estructura
$\mathsf{A} \vDash \alpha$ [a] : La fórmula $\alpha(x)$ es válida en A en una asignación de variables con v(x)=a
$\Phi \vdash_S \alpha$: α se deriva sintácticamente de Φ en el sistema formal S
$\mathsf{A} \equiv \mathsf{B}$: A y B son dos estrucuturas elementalmente equivalentes ($\mathsf{A} \vDash \alpha \Leftrightarrow \mathsf{B} \vDash \alpha$)

$=$: El signo de igualdad en un lenguaje formal. pero también lo usamos en el metalenguaje si no da lugar a confusión.
$\equiv$: La identidad entre dos elementos de una estructura cuando queremos distinguirlo del símbolo de igualdad en el lenguaje
$\approx$: Isomorfía de dos estructuras

Lógica

Se utilizan x, y, z , v, ... como metavariables recorriendo el conjunto de variables. El conjunto de variables del lenguaje es x_0, x_1, x_2, ...
var(α) : Variables que aparecen en la fórmula α
lib(α) : Variables libres de la fórmula α
Escribiremos $\alpha(x)$ para indicar que la fórmula α tiene la variable libre x, esto es, $x \in$ lib(α). En tal caso $\alpha(t)$ indica la sustitución en α de la variable x por el término t.

Los símbolos lógicos usuales $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\neg$, $\forall$, $\exists$ se usarán en expresiones del lenguaje formal, pero alguna vez los utilizaremos en el metalenguaje, como ocurre en matemáticas no formales, cuando el contexto no induzca a confusión. Para "y" usaremos también en el metalenguaje &. Se usará en el metalenguaje el signo de implicación $\Rightarrow$ y el de equivalencia $\Leftrightarrow$.

$\equiv$: se usa para indicar que dos cadenas de símbolos son sintácticamente la misma fórmula (ver a continuación un ejemplo).
$\exists!$ es una abreviatura de "existe un único". Formalmente

$$\exists! z\, \alpha(z) \equiv \exists z\, \forall w\, (\alpha(z) \leftrightarrow w = z)$$

Teoría de conjuntos

$\mathsf{P}(A)$: Conjunto de partes del conjunto A
$\varnothing$: Conjunto vacío
$\in$: Símbolo de pertenencia de un elemento a un conjunto
$\notin$: No pertenencia
$\subset$: Inclusión de conjuntos (no necesariamente estricta; otros textos escriben $\subseteq$)
$\cup$: Unión de conjuntos
$\cap$: Intersección de conjuntos
$\bigcap_{A \in F} T(A)$: Intersección de los conjuntos T(A) cuando A recorre la familia de conjuntos F
{a} : Conjunto unitario cuyo único elemento es a
$\overline{A}$: Complementario del conjunto A
$A - B$: $A \cap \overline{B}$
$A \times B$: producto cartesiano
(a, b) : par ordenado
<a, b> : otra notación para un par ordenado
(a_1, a_2, ..., a_n) : n-upla ordenada
<a_1, a_2, ..., a_n> : n-upla ordenada

dom f : dominio de la función f
rg f : rango de f
$g \circ f$: composición de f y g.También se denota por gf . Esto es, $(g \circ f)(x)=gf(x)=g(f(x))$
$f \subset g$: g es una extensión de f
f^{-1} : función inversa de f : $f^{-1} \circ f$ = Identidad

En el enunciado de un teorema o en la demostración se han usado los símbolos $\Rightarrow$ para indicar “si...entonces”, y $\Leftrightarrow$ o bien syss para indicar “si y sólo si”. El fin de una demostración (o la ausencia de tal, por fácil o conocida) se ha señalado por .
Las referencias a la bibliografía se realizan señalando el número de orden en la lista, por ejemplo, [60].
Las definiciones y proposiciones tienen una numeración según un sistema del tipo [i-j] en que i indica el número de capítulo y j un número de orden dentro del capítulo. Una referencia a un enunciado se hace mencionando el par correspondiente al capítulo y al enunciado. Cada capítulo está dividido en apartados. Una referencia al apartado m del capítulo n se hace mediante § m.n.

2. TEORÍA DE LA RECURSIÓN.

El marco adecuado para tratar la noción de indecidibilidad es la teoría de la recursión. Presentamos en este capítulo algunos de los conceptos básicos de la teoría de la recursión o teoría de la computabilidad. Los conceptos y resultados presentados aquí son una revisión rápida de contenidos básicos bien conocidos. En el siguiente capítulo se presentarán, de una forma análoga, las nociones de inseparabilidad y los teoremas correspondientes.

2.1 Conceptos y teoremas básicos

El concepto básico de la teoría de la recursión es el de función recursiva parcial. La clase de las funciones recursivas parciales es la menor clase de funciones que contiene la función cero, la función sucesor y las proyecciones y es cerrada por sustitución, recursión primitiva y minimización. Es bien sabido que la clase de funciones recursivas parciales coincide con la clase de funciones computadas en diversas formalizaciones del concepto intuitivo de algoritmo : máquinas de Turing, máquinas de registros, algoritmos de Markov, sistemas de producción de Post, λ-cálculo, etc. Alonzo Church propuso identificar el concepto intuitivo de función computable con el concepto formal de función definible en el λ-cálculo. Esta tesis, conocida habitualmente por el nombre de Tesis de Church es usualmente admitida en el campo de la teoría de la computabilidad. La equivalencia del λ-cálculo con los demás formalismos introducidos para expresar la noción de computabilidad es, en palabras de Gödel, "una especie de milagro" pues se ha capturado formalmente de modo absoluto una noción intuitiva epistemológicamente interesante.

Utilizando una codificación adecuada se puede asociar a cada programa un número natural. Se denotará por φ_m la función definida por el programa de número m. Con la notación φ_m^n indicamos que la función de número m tiene n argumentos. El dominio de φ_m se denotará por W_m. Denotaremos por $W_{m,s}$ el subconjunto de W_m que consta de los $a \in \omega$ tal que el programa de número m produce un output tras s pasos cuando comienza con input a.

Las funciones recursivas parciales que son totales se denominan funciones recursivas.

Un conjunto es recursivo si su función característica es recursiva. Un conjunto es recursivamente enumerable (r.e.) si es el dominio de una función recursiva parcial. Por lo tanto los conjuntos r.e. son los W_m. Un conjunto es recursivo si él y su complementario son r.e. Se denotan por Σ_0 la familia de conjuntos recursivos y por Σ_1 la familia de conjuntos recursivamente enumerables.

El concepto de conjunto recursivo formaliza la noción intuitiva de conjunto decidible.
Es muy utilizada en teoría de la recursión una biyección recursiva $J : \omega^2 \to \omega$, que permite codificar pares, y las funciones recursivas asociadas $L : \omega \to \omega$ y $R : \omega \to \omega$ tales que $J(L(z), R(z)) = z$, $L(J(x, y)) = x$, $R(J(x, y) = y$ para todo $x, y, z \in \omega$.

Usaremos los siguientes teoremas básicos y bien conocidos de la teoría de funciones recursivas :

Teorema s-m-n o teorema de iteración

Para cada n, m ≥1 hay una función recursiva inyectiva *h* tal que

$$\varphi^n_{h(x,a_1,\ldots,a_m)}(y_1, \ldots, y_n) = \varphi^{n+m}_x (a_1, \ldots , a_m, y_1, \ldots, y_n)$$

Teorema de recursión

Para toda una función recursiva $f : \omega^{n+1} \to \omega$ existe una función recursiva e inyectiva $r : \omega^n \to \omega$ tal que para todo m y todo $\bar{x} = (x_1, \ldots, x_n)$ se verifica

$$\varphi^m_{r(\bar{x})} = \varphi^m_{f(\bar{x}, r(\bar{x}))}$$

Teorema del punto fijo

Si *f* es recursiva existe $e \in \omega$ tal que $\varphi_e = \varphi_{f(e)}$

Utilizaremos una generalización del teorema de recursión debida a Smullyan [53] :

Teorema de doble recursión

Para todo par de funciones recursivas *m*, *n* : $\omega^3 \to \omega$ existen dos funciones recursivas *p*, *q* : $\omega^2 \to \omega$ tales que

$$\varphi_{p(x)} = \varphi_{m\,(x,\, p(x),\, q(x))}$$
$$\varphi_{q(x)} = \varphi_{n\,(x,\, p(x),\, q(x))}$$

Demostración

Consideremos *b*, *a* , *p*, *q*, funciones que verifiquen las igualdades siguientes.
Por el teorema de recursión existe *b* verificando

$$\varphi_{b(x,\, y)} = \varphi_{n\,(x,\, y,\, b(x,y))}$$

Por el teorema s-m-n existe a verificando

$$\varphi_{a(x,\, y)} = \varphi_{m\,(x,\, y,\, b(x,\, y))}$$

Por el teorema de recursión existe *p* verificando

$$\varphi_{p(x)} = \varphi_{a(x,\, p(x))}$$

Sea $q(x) = b(x, p(x))$
Se tiene

$$\varphi_{p(x)} = \varphi_{a(x,\, p(x))} = \varphi_{m\,(x,\, p(x),\, b(x,\, p(x))} = \varphi_{m\,(x,\, p(x),\, q(x))}$$
$$\varphi_{q(x)} = \varphi_{b(x,\, p(x))} = \varphi_{n\,(x,\, p(x),\, b(x,\, p(x))} = \varphi_{n\,(x,\, p(x),\, q(x))}$$

Corolario
Para todo par de funciones recursivas f, $g : \omega^2 \to \omega$ existe una función recursiva $h : \omega \to \omega$ tal que

$$\varphi_{Lh(x)} = \varphi_{f(x,\, h(x))}$$
$$\varphi_{Rh(x)} = \varphi_{g(x,\, h(x))}$$

Demostración
Por el teorema s-m-n existirán funciones recursivas u y v tales que

$$\varphi_{u(x,\, y,\, z)} = \varphi_{f(x,\, J(y,\, z))}$$
$$\varphi_{v(x,\, y,\, z)} = \varphi_{g(x,\, J(y,\, z))}$$

Por el teorema de doble recursión existirán p, $q : \omega \to \omega$ tales que

$$\varphi_{p(x)} = \varphi_{u(x,\, p(x),\, q(x))}$$
$$\varphi_{q(x)} = \varphi_{v(x,\, p(x),\, q(x))}$$

Definiendo h mediante

$$h(x) = J(p(x), q(x))$$

se tiene

$$\varphi_{Lh(x)} = \varphi_{p(x)} = \varphi_{u(x,\, p(x),\, q(x))\,)} = \varphi_{f(x,\, J(p(x),\, q(x)))} = \varphi_{f(x,\, h(x))}$$
$$\varphi_{Rh(x)} = \varphi_{q(x)} = \varphi_{v(x,\, p(x),\, q(x))\,)} = \varphi_{g(x,\, J(p(x),\, q(x)))} = \varphi_{g(x,\, h(x))}$$

2.2 Conjuntos productivos

La noción de conjunto productivo tiene cierta similitud con la de conjunto no numerable. Para ver que un conjunto P no es numerable basta ver que para cada conjunto numerable N tal que $N \subset P$ podemos encontrar un elemento $x \in P\text{-}N$. De forma parecida un conjunto P no es r.e. si para cualquier R r.e. tal que $R \subset P$ existe $x \in P\text{-}R$. La noción de conjunto productivo impone que este elemento pueda encontrarse efectivamente.

[2-1] Definición

Sea $A \subset \omega$. Diremos que A es *productivo* si existe una función recursiva f tal que

$$\forall x\, (W_x \subset A \Rightarrow f(x) \in A - W_x)$$

La función f se llama *función productiva* de A.

Observación

La función *f* sólo necesita estar definida cuando $W_x \subset A$

[2-2] Proposición

A productivo $\Rightarrow$ *A* no es r.e.

Por tanto la menor clase en la jerarquía aritmética donde buscar conjuntos productivos es en Π_1

[2-3] Ejemplo

$K = \{x : x \in W_x\}$ no es productivo por ser r.e.
$\overline{K} = \{x : x \notin W_x\}$ es productivo . La identidad es una función de producción de $\overline{K}$

[2-4] Proposición

Todo conjunto productivo posee una función de producción total
Demostración
Sea *f* una función de producción de *A*. Consideremos la función recursiva parcial

$$g(x, y, z) = \begin{cases} \varphi_y(z) & \text{si } f(x)\downarrow \\ \uparrow & \text{e.o.c.} \end{cases}$$

Por el teorema s-m-n existe *h* recursiva inyectiva total tal que $g(x, y, z) = \varphi_{h(x,y)}(z)$
Por el teorema de recursión existe *r* recursiva total tal que

$$\varphi_{r(y)}(z) = \varphi_{h(r(y),y)}(z)$$

con lo que

$$\varphi_{r(y)}(z) = \begin{cases} \varphi_y(z) & \text{si } f(r(y))\downarrow \\ \uparrow & \text{e.o.c.} \end{cases}$$

Así pues

$$f(r(y))\uparrow \Rightarrow W_{r(y)} = \varnothing \subset A \Rightarrow f(r(y))\downarrow$$

De forma que *fr* es una función total
Además $\varphi_{r(y)} = \varphi_y$ luego

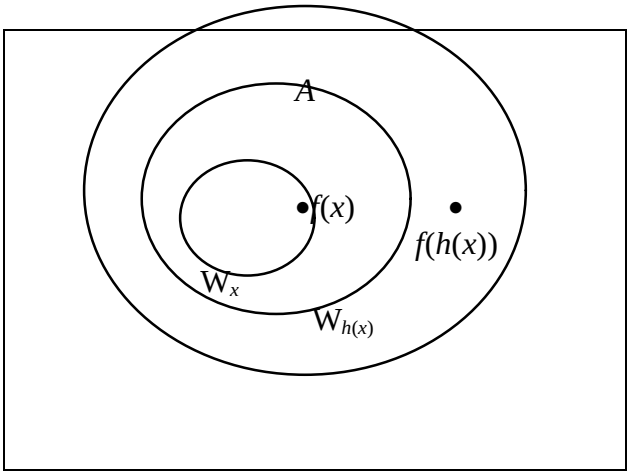
$$W_y \subset A \Rightarrow W_{r(y)} \subset A \Rightarrow fr(y) \in A - W_{r(y)} \Rightarrow fr(y) \in A - W_y$$

luego *fr* es una función productiva de *A*

[2-5] Proposición

Si *A* es productivo existe una función productiva total e inyectiva
Demostración
Sea *f* una función productiva total de *A*. Construiremos una sucesión infinita de funciones productivas de *A* distintas, a partir de la cual construiremos una función productiva estrictamente creciente, y por tanto inyectiva

La idea es que si $W_x \subset A$ y *f* es la función productiva de *A*, $W_x \cup \{f(x)\}$ es un conjunto r.e. contenido en *A* y por tanto un cierto $W_{h(x)} \subset A$, con lo que $fh(x) \in A - W_{h(x)}$



Por el teorema s-m-n existe *h* recursiva total inyectiva tal que

$$\varphi_{h(x)}(y)= \begin{cases} 1 & \text{si } \varphi_x(y)\downarrow \vee\, y = f(x) \\ \uparrow & \text{e.o.c.} \end{cases}$$

Es fácil ver que $W_x \subset W_{h(x)} \subset W_{hh(x)} \subset ... \subset A$, pues

$W_{h(x)} = W_x \cup \{f(x)\} \subset A$,

$W_{hh(x)} = W_{h(x)} \cup \{fh(x)\} \subset A$,

...

Denotaremos por h^j a la función *h* ... *h* (j veces).

Obsérvese que si $W_x \subset A$ todos los elementos del conjunto $S = \{f(x), fh(x), fh^2(x), ...\}$ son distintos por ser *f* función productiva de *A*. Debido a esto, si $W_x \subset A$, dado cualquier número $k \in \omega$, recorriendo la lista de *S* encontraremos con seguridad entre los k+1 primeros algún elemento mayor que k.

Nótese que todas las fh^j son funciones productivas de *A* :

$$W_x \subset A \Rightarrow W_{hj(x)} \subset A \Rightarrow fh^j(x) \in A - W_{hj(x)} \Rightarrow fh^j(x) \subset A - W_x$$

Definamos la función *g* mediante

$g(0) = 0$

$$g(n+1) = \begin{cases} fh^r(n+1) & \text{siendo } r = mj \le g(n)\ (fh^j(n+1) > g(n)) \text{ si existe} \\ g(n)+1 & \text{e.o.c.} \end{cases}$$

La función *g* es recursiva total y estrictamente creciente y por tanto inyectiva.Además es función productiva de *A* ; pues si $W_x \subset A$, al ser los elementos de *S* todos distintos, existirá j tal que $g(x) = fh^j(x)$ y por tanto $g(x) = fh^j(x) \subset A - W_x$

[2-6] Proposición

a) $A \cap B$ productivo & B r.e. $\Rightarrow A$ productivo
b) $A \cup B$ productivo & B r.e. $\Rightarrow A$ productivo

Demostración

a) Sea f la función productiva de $A \cap B$ y consideremos $W_x \subset A$. Como B es r.e., aplicando el teorema s-m-n existe h recursiva tal que $W_{h(x)} = W_x \cap B$. Entonces

$$W_x \subset A \Rightarrow W_{h(x)} \subset A \cap B$$
$$\Rightarrow fh(x) \in (A \cap B) - W_{h(x)} = (A \cap B) - (W_x \cap B)$$
$$\Rightarrow fh(x) \in A - W_x$$

Luego fh es una función productiva de A.

b) Análoga

2.3 Conjuntos creativos

Un conjunto productivo es un conjunto para el que la prueba de ser no r.e. se realiza recursivamente. Un conjunto creativo es un conjunto r.e. para el que la prueba de ser no recursivo se realiza recursivamente por medio de una función productiva de su complementario.

[2-7] Definición

A es *creativo* si es r.e. y $\overline{A}$ es productivo

[2-8] Proposición

A creativo $\Rightarrow A$ es r.e. pero no recursivo

[2-9] Ejemplo

K es creativo pues es r.e. y su complementario es productivo

2.4 Reducibilidad

[2-10] Definición

Se dice que A es *m-reducible* a B vía f , lo que denotamos por $A \underset{m}{\leq} B$, si f es una función recursiva tal que

$$x \in A \Leftrightarrow f(x) \in B$$

[2-11] Definición

Se dice que A es *1-reducible* a B vía f , lo que denotamos por $A \underset{1}{\leq} B$, si f es una función recursiva inyectiva tal que

$$x \in A \Leftrightarrow f(x) \in B$$

[2-12] Proposición

$A \underset{m}{\leq} B,\ B \in \Sigma_0 \Rightarrow A \in \Sigma_0$

Demostración

Si A es m-reducible a B vía f entonces la función característica de A es $c_A = c_B f$

[2-13] Proposición

$A \underset{m}{\leq} B,\ A \notin \Sigma_0 \Rightarrow B \notin \Sigma_0$

[2-14] Proposición

$A \underset{m}{\leq} B$, A productivo $\Rightarrow$ B productivo

Demostración

Sea A reducible a B vía f y sea g una función de producción de A. Supongamos que $W_x \subset B$. Sea h la función recursiva tal que $f^{-1}(W_x) = W_{h(x)}$. Entonces $W_{h(x)} \subset A$ y por tanto $gh(x) \in A - W_{h(x)}$ y $fgh(x) \in B - W_x$. Luego fgh es función productiva de B.

[2-15] Proposición

$A \underset{m}{\leq} B$, A creativo, B r.e. $\Rightarrow$ B creativo

Demostración

La reducción de A a B es una reducción de $\overline{A}$ a $\overline{B}$

[2-16] Proposición

A r.e., P productivo $\Rightarrow A \underset{1}{\leq} \overline{P}$

Demostración

Sea f una función productiva de A total estrictamente creciente

$W_x \subset P \Rightarrow f(x) \in P - W_x$

Por el teorema de recursión existe g recursiva y creciente tal que

$$\varphi_{g(x)}(y) = \begin{cases} 1 & \text{si } y = fg(x) \ \& \ x \in A \\ 0 & \text{e.o.c.} \end{cases}$$

o sea

$$W_{g(x)} = \begin{cases} fg(x) & \text{si } x \in A \\ \varnothing & \text{e.o.c.} \end{cases}$$

fg es recursiva y monótona ; veamos que reduce A a $\overline{P}$

$e \in A \Rightarrow W_{g(e)} = \{fg(e)\} \Rightarrow fg(e) \notin P - W_{g(e)} \Rightarrow W_{g(e)} \not\subset P \Rightarrow fg(e) \in \overline{P}$

$e \notin A \Rightarrow W_{g(e)} = \varnothing \subset P \Rightarrow fg(e) \in P - W_{g(e)} \Rightarrow fg(e) \notin \overline{P}$

[2-17] Proposición

A r.e., C creativo $\Rightarrow A \underset{1}{\leq} C$

2.5 Equivalencia

[2-18] Definición

A es *m-equivalente* a B , lo que denotamos por $A \underset{m}{\equiv} B$, si $A \underset{m}{\leq} B$ y $B \underset{m}{\leq} A$

A es *1-equivalente* a B , lo que denotamos por $A \underset{1}{\equiv} B$, si $A \underset{1}{\leq} B$ y $B \underset{1}{\leq} A$

Es inmediato ver que ambas son relaciones de equivalencia entre conjuntos de naturales

[2-19] Proposición

Sea C creativo. Son equivalentes

1. B es creativo
2. $C \underset{1}{\equiv} B$
3. $C \underset{m}{\equiv} B$

Demostración

1⇒2 por la proposición [2-17]
2⇒3 trivialmente
3⇒1 Si $C \underset{m}{\equiv} B$ entonces $C \underset{m}{\leq} B$. Como C es creativo y por tanto r.e. debe ser B r.e.. Como C es reducible a B, por la proposición [2-15] , B es creativo

2.6 Conjuntos completos

La m-reducibilidad es un preorden. Si consideramos la familia de conjuntos r.e. los elementos maximales se denominan completos. Los problemas correspondientes a conjuntos completos son "los más difíciles" entre los Σ_1.

[2-20] Definición

A es *S_1-completo en la m-reducibilidad* si A es r.e. y para todo B r.e. es $B \underset{m}{\leq} A$

A es *S_1-completo en la 1-reducibilidad* si A es r.e. y para todo B r.e. es $B \underset{1}{\equiv} A$

Diremos sencillamente que A es m-completo o 1-completo .

[2-21] Ejemplo

K es completo, pues es r.e. y para cada $B \in \Sigma_1$ podemos considerar

$$\varphi_{g(x)}(y) = \begin{cases} 0 & \text{si } x \in B \\ \uparrow & \text{e.o.c.} \end{cases}$$

con lo que

$$W_{g(x)} = \begin{cases} w & \text{si } x \in B \\ \varnothing & \text{si } x \notin B \end{cases}$$

que proporciona la reducción

$$x \in B \iff g(x) \in K$$

[2-22] Proposición

a) A m-completo & $A \underset{m}{\equiv} B \Rightarrow B$ m-completo

b) A m-completo $\Leftrightarrow A \underset{m}{\equiv} K$

[2-23] Proposición

A m-completo $\Rightarrow$ A creativo
Demostración
Si A es m-completo es r.e. y $K \underset{m}{\leq} A$ luego $\overline{K} \underset{m}{\leq} \overline{A}$ y como $\overline{K}$ es productivo $\overline{A}$ es productivo, por [2-14]. Por tanto A es creativo

El recíproco de este teorema también se verifica :

[2-24] Teorema

Todo conjunto creativo es 1-completo
Demostración
Sea A creativo y h una función recursiva total inyectiva productiva de $\overline{A}$ y sea B un conjunto r.e.
Definamos la función recursiva parcial

$$g(x, y, z) = \begin{cases} 0 & \text{si } y \in B \,\&\, h(x) = z \\ \uparrow & \text{e.o.c.} \end{cases}$$

Por el teorema s-m-n existe una función recursiva total f tal que

$$\varphi_{f(x, y)}(z) = g(x, y, z)$$

Por el teorema de recursión existe una función recursiva total inyectiva r tal que

$$\varphi_{r(y)}(z)=\varphi_{f(r(y),y)}(z)$$

con lo que

$$\varphi_{r(y)}(z)= \begin{cases} 0 & \text{si } y \in B \,\&\, hr(y) = z \\ \uparrow & \text{e.o.c.} \end{cases}$$

En consecuencia

$$y \in B \;\Rightarrow\; W_{r(y)} = \{hr(y)\} \;\Rightarrow\; hr(y) \in A$$

puesto que

$$hr(y) \notin A \;\Rightarrow\; W_{r(y)} \subset \overline{A} \;\Rightarrow\; hr(y) \notin W_{r(y)}$$

Por otra parte

$$y \notin B \;\Rightarrow\; W_{r(y)} = \varnothing \;\Rightarrow hr(y) \in \overline{A}$$

Con lo cual obtenemos

$$y \in B \;\Leftrightarrow\; hr(y) \in A$$

Por tanto B es 1-reducible a A y A es 1-completo

2.7 Conjuntos recursivamente isomorfos

[2-25] Definición

Una *permutación recursiva* es una aplicación $f:\omega \to \omega$ biyectiva y recursiva

[2-26] Proposición

Las permutaciones recursivas con la operación de composición forman un grupo

[2-27] Definición

Sea A y B dos conjuntos de naturales. Se dice que son *recursivamente isomorfos*, lo que denotaremos por $A \equiv B$, si existe una permutación recursiva f tal que $x \in A \Leftrightarrow f(x) \in B$

Nótese que si f es como indica la definición, la función $g(y) = \mu x(f(x) = y)$ verifica

$$y \in B \Leftrightarrow g(y) \in A$$

lo que muestra la simetría de la definición

[2-28] Proposición

$A \equiv B \Rightarrow A \underset{1}{\equiv} B$

Demostración
trivial

El recíproco de la anterior proposición también se verifica. Es decir, si dos conjuntos son 1-equivalentes son recursivamente isomorfos. Es un importante resultado, debido a Myhill [40] . Puede observarse que es un análogo en teoría de la recursión al teorema de Cantor -Schröder-Bernstein en la teoría de cardinales.

2.8 Teorema de Myhill

[2-29] Teorema

$A \underset{1}{\equiv} B \Rightarrow A \equiv B$

Demostración
Supongamos que $A \underset{1}{\leq} B$ vía f y que $B \underset{1}{\leq} A$ vía g

Construiremos una permutación recursiva h tal que $x \in A \Leftrightarrow h(x) \in B$

La construcción se efectuará construyendo una sucesión de funciones recursivas (no totales) $h_0 \subset h_1 \subset h_2 \subset ...$ y haciendo $h = \bigcup h_n$

La construcción se hará por pasos. Definiremos $h_0 = \varnothing$ y en cada paso añadiremos a lo sumo un par más. En el paso h_{2s+1} nos aseguraremos que s pertenezca al dominio de la función .En el paso h_{2s+2} nos aseguraremos que s pertenezca al rango de la función.
Definiremos pues

$$h_{2s+1} = \begin{cases} h_{2s} & \text{si } h_{2s}\downarrow \\ h_{2s} \cup (s,r) & \text{e.o.c.} \end{cases}$$

siendo $j = \mu i\ (f\ h_{2s}{}^{-1})^i\ f(s) \notin rg(h_{2s})$ y $r = (f\ h_{2s}{}^{-1})^j\ f(s)$

$$h_{2s+2} = \begin{cases} h_{2s+1} & \text{si } s \in rg(h_{2s}) \\ h_{2s} \cup (r,s) & \text{e.o.c.} \end{cases}$$

siendo $j = \mu i\ (g\ h_{2s+1}{}^{-1})^i\ g(s) \notin \text{dom}(h_{2s+1})$ y $r = (g\ h_{2s+1}{}^{-1})^j\ g(s)$

Sea $h = \bigcup h_n$ Se verifica :

1. dom $h = \omega$, por construcción
2. rg $h = \omega$, por construcción
3. h es inyectiva, por construcción
4. h es recursiva. Nótese que $h(s) = h_{2s+1}(s)$
5. $x \in A \Leftrightarrow h(x) \in B$

Demostraremos por inducción que

a. h_n es finita
b. h_n es inyectiva
c. $h_n(x)\downarrow \Rightarrow [x \in A \Leftrightarrow h_n(x) \in B]$

Para n = 0 es trivial
Supongamos que a. b. y c. se verifican para 0, 1, ..., 2s. Veamos que se verifica para 2s+1 (el caso 2s+2 es análogo)

a. h_{2s+1} es h_{2s} y a lo sumo un par más
b. h_{2s+1} es inyectiva por construcción. Si se añade el par (s,r) es porque r no aparecía en el rango
c. Sea $z \in rg(h_{2s+1})$. Veamos que $z \in B \Leftrightarrow h_{2s+1}{}^{-1}(z) \in A$
   o sea $h_{2s+1}(x)\downarrow \Rightarrow [x \in A \Leftrightarrow h_{2s+1}(x) \in B]$

Si $h_{2s+1}(x)\downarrow$ hay dos posibilidades : o bien sucede que estuviera definido $h_{2s}(x)$ con lo que se verifica por la hipótesis de inducción ; o bien $x = s$ y $h_{2s+1}(s) = r$ y entonces :

$$\begin{aligned} s \in A &\Leftrightarrow f(s) \in B \\ &\Leftrightarrow h_{2s}{}^{-1}\ f(s) \in A \text{ por hipótesis de inducción} \\ &\Leftrightarrow ... \\ &\Leftrightarrow (f\ h_{2s}{}^{-1})^j\ f(s) \in B \\ &\Leftrightarrow r \in B \\ &\Leftrightarrow h_{2s+1}(s) \in B \end{aligned}$$

Observación

La construcción de *h* no depende de *A* ni de *B* sino únicamente de *f* y *g*.

[2-30] Corolario

Si *A* y *B* son creativos $A \equiv B$

Comentario

Si T_1 y T_2 son dos teorías y los conjuntos de códigos *A* y *B* correspondientes son dos conjuntos creativos, estos dos conjuntos pueden obtenerse uno de otro mediante una permutación recursiva ; por tanto pueden considerarse iguales desde el punto de vista de la teoría de la recursión.

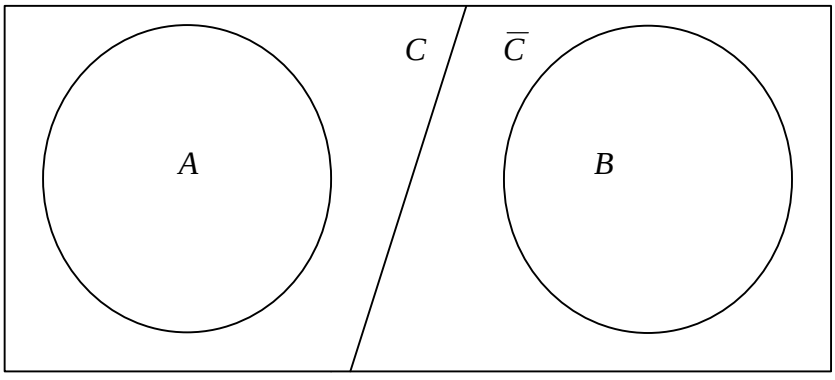
3. INSEPARABILIDAD

Un conjunto *A* es recursivo si tanto *A*, como su complementario $\overline{A}$, son recursivamente enumerables. Esto sugiere la posibilidad de extender la teoría de conjuntos r.e. a pares de conjuntos r.e. disjuntos. A continuación introducimos la noción de inseparabilidad que generaliza la de "no recursividad" con importantes ventajas técnicas y teóricas.

3.1 Conjuntos recursivamente inseparables

[3-1] Definición

Sean $A \subset \omega$ y $B \subset \omega$ dos conjuntos disjuntos de números naturales. Se dice que *A* y *B* son *recursivamente separables* si existe algún conjunto recursivo $C \subset \omega$ tal que $A \subset C$ y $B \subset \overline{C}$. En tal caso se dice que *C separa A* y *B*.
Si *A* y *B* son dos conjuntos disjuntos que no son recursivamente separables se dice que son *recursivamente inseparables*



[3-2] Proposición

A es recursivo syss *A* y $\overline{A}$ son recursivamente separables

[3-3] Proposición

Si A y B son recursivamente inseparables entonces A y B no son recursivos

La existencia de un par de conjuntos r.e. recursivamente inseparables es un hecho más fuerte que la existencia de un conjunto r.e. no recursivo. La siguiente proposición presenta el ejemplo básico de par de conjuntos recursivamente inseparables

[3-4] Proposición

Existen dos conjuntos r.e. recursivamente inseparables

Demostración

Sean $A_0 = \{x : \varphi_x(x) = 0\}$ y $A_1 = \{x : \varphi_x(x) = 1\}$. Es claro que A_0 y A_1 son disjuntos y son r.e. Además son recursivamente inseparables. En efecto: supongamos que existiera una conjunto C recursivo que los separase, esto es, tal que $A_0 \subset C \subset \overline{A_1}$. Al ser C recursivo su función característica es una función recursiva φ_r, y se verificaría

$$r \in C \Rightarrow \varphi_r(r) = 1 \Rightarrow r \in A_1 \Rightarrow r \in \overline{C} \Rightarrow r \notin C$$
$$r \notin C \Rightarrow \varphi_r(r) = 0 \Rightarrow r \in A_0 \Rightarrow r \in C$$

Esta contradicción muestra que A_0 y A_1 son recursivamente inseparables.

3.2 Transmisión de la inseparabilidad recursiva

[3-5] Proposición

Sean A y B recursivamente inseparables $A \subset A'$, $B \subset B'$ y $A' \cap B' = \varnothing$. Entonces A' y B' son recursivamente inseparables

Demostración

Si C separa A' y B' entonces separa también A y B.

Nota

La indecidibilidad de una teoría no se transmite a sus extensiones. La razón es que un conjunto no recursivo es subconjunto de conjuntos recursivos. Sin embargo la noción de inseparabilidad se transmite cómodamente a los superconjuntos. Y la demostración es trivial, como acabamos de ver.

[3-6] Proposición

Sean A y B recursivamente inseparables y f una función recursiva tal que $f(A) \subset A'$ $f(B) \subset B'$ y $A' \cap B' = \varnothing$. Entonces A' y B' son recursivamente inseparables.

Demostración

Supongamos que hay un conjunto recursivo C que separa A' y B' . Entonces $f^{-1}(C)$ sería un conjunto recursivo que separaría A y B

Este teorema permitirá transmitir fácilmente resultados de inseparabilidad utilizando transformaciones efectivas

3.3 Conjuntos efectivamente inseparables

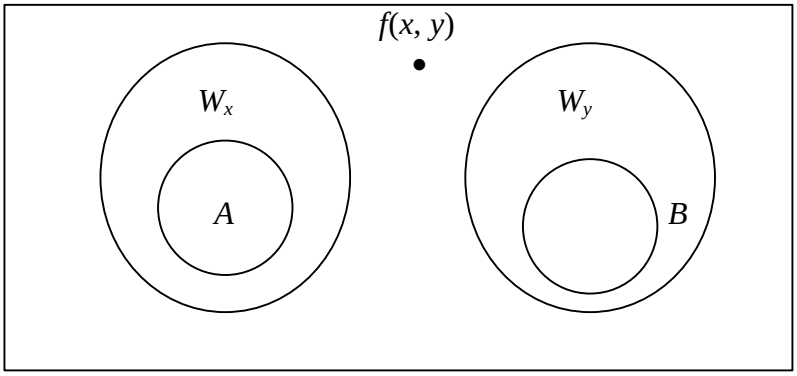
Dos conjuntos A y B disjuntos son recursivamente inseparables si no hay un conjunto recursivo que los separe. Por lo tanto si consideramos un conjunto M tal que él y su complementario N sean r.e. y suponemos que M separa A y B o sea $A \subset M$ y $B \subset N$, en realidad M y N no podrán llenar ω, sino que existirá un elemento $k \notin M \cup N$ testigo de la inseparabilidad. Si podemos construir tal elemento de forma efectiva a partir de M y N tenemos la noción de inseparabilidad efectiva.

[3-7] Definición

Sean A y B dos conjuntos disjuntos de números naturales.
Se dice que A y B son *efectivamente inseparables* si existe una función recursiva parcial de dos argumentos $f(x, y)$ tal que

$$\forall x \ \forall y \ (A \subset W_x \ \ \& \ \ B \subset W_y \ \& \ W_x \cap W_y = \varnothing \ \Rightarrow \ \ f(x, y) \in \overline{W_x} \cap \overline{W_y})$$

La función f se llama *función de separación* de A y B



[3-8] Proposición

Si A y B son efectivamente inseparables son recursivamente inseparables
Demostración
Son equivalentes
1. A y B son recursivamente inseparables

2. $\neg\exists x\exists y\,(A \subset W_x \;\&\; A \subset W_y \;\&\; W_x \cap W_y = \varnothing \;\&\; W_x \cup W_y = \omega)$
3. $\forall x\,\forall y\,((A \subset W_x \;\&\; A \subset W_y \;\&\; W_x \cap W_y = \varnothing) \Rightarrow \exists z\; z \in \overline{W_x} \cap \overline{W_y})$
4. $\forall x\,\forall y\,\exists z\,((A \subset W_x \;\&\; A \subset W_y \;\&\; W_x \cap W_y = \varnothing) \Rightarrow z \in \overline{W_x} \cap \overline{W_y})$
5. Existe una función f de dos argumentos tal que

   $\forall x\,\forall y\,((A \subset W_x \;\&\; A \subset W_y \;\&\; W_x \cap W_y = \varnothing) \Rightarrow f(x, y) \in \overline{W_x} \cap \overline{W_y})$

El hecho de ser A y B efectivamente inseparables es 5. con la condición suplementaria de ser f recursiva

Nota
Hay conjuntos recusivamente inseparables no efectivamente inseparables.(cf. [39], pág. 318)

El par de conjuntos $A_0 = \{x : \varphi_x(x) = 0\}$ y $A_1 = \{x : \varphi_x(x) = 1\}$ vistos en [3-4] es el ejemplo básico de conjuntos efectivamente inseparables.

[3-9] Proposición

A_0 y A_1 son efectivamente inseparables
Demostración
Por el teorema s-m-n existe $h(x, y)$ función recursiva total tal que

$$\varphi_{h(x,y)}(z) = \begin{cases} 1 & \text{si} \quad \exists s \;\; z \in W_{x,s} - W_{y,s} \\ 0 & \text{si} \quad \exists s \;\; z \in W_{y,s} - W_{x,s} \\ \uparrow & \text{e.o.c.} \end{cases}$$

Entonces $A_0 \subset W_x \;\&\; A_1 \subset W_y \;\&\; W_x \cap W_y = \varnothing \Rightarrow h(x, y) \in \overline{W_x} \cap \overline{W_y}$
En efecto :

$$h(x, y) \in W_x \Rightarrow \varphi_{h(x,y)}(h(x, y)) = 1 \Rightarrow h(x, y) \in A_1 \subset W_y \subset \overline{W_x}$$
$$h(x, y) \in W_y \Rightarrow \varphi_{h(x,y)}(h(x, y)) = 0 \Rightarrow h(x, y) \in A_0 \subset W_x \subset \overline{W_y}$$

3.4 Transmisión de la inseparabilidad efectiva

[3-10] Proposición

Sean A y B efectivamente inseparables $A \subset A'$, $B \subset B'$, $A' \cap B' = \varnothing$. Entonces A' y B' son efectivamente inseparables
Demostración
Para separar A' y B' vale la misma función de separación de A y B

[3-11] Proposición

Sean A y B efectivamente inseparables y f una función recursiva tal que $f(A) \subset A'$, $f(B) \subset B'$ y $A' \cap B' = \varnothing$. Entonces A' y B' son efectivamente inseparables.

Demostración

Existe una función recursiva h tal que $W_{h(z)} = f^{-1}(W_z)$.

Supongamos que $A' \subset W_x$, $B' \subset W_y$, $W_x \cap W_y = \varnothing$. Entonces

$$A \subset f^{-1}(A') \subset f^{-1}(W_x) = W_{h(x)}$$
$$B \subset f^{-1}(B') \subset f^{-1}(W_y) = W_{h(y)}$$
$$W_{g(x)} \cap W_{g(y)} = \varnothing$$

con lo que al suponer A y B efectivamente inseparables con la función de separación g

$$g(h(x), h(y)) \in \overline{W_{h(x)}} \cap \overline{W_{h(y)}}$$

y por tanto

$$f(g(h(x), h(y))) \in \overline{W_x} \cap \overline{W_y}$$

Así, $f(g(h(x), h(y)))$ es una función de separación de A y B.

3.5 Inseparabilidad y creatividad

[3-12] Proposición

Si A y B son dos conjuntos r.e. y efectivamente inseparables entonces A y B son creativos

Demostración

Por la simetría de la noción basta demostrar que A es creativo y para ello hay que ver que $\overline{A}$ es productivo. Sea f la función de separación de los conjuntos r.e. $A = W_a$ y B. Consideremos la función recursiva h tal que $W_{h(x)} = B \cup W_x$. Entonces :

$$W_x \subset \overline{A} \Rightarrow A \subset W_a \ \& \ B \subset W_{h(x)} \ \& \ W_a \cap W_{h(x)} = \varnothing$$
$$\Rightarrow f(a, h(x)) \in \overline{W_a} \cap \overline{W_{h(x)}} \subset \overline{A} \cap \overline{W_x} = \overline{A} - W_x$$

Luego $g(x) = f(a, h(x))$ es una función de producción de $\overline{A}$. Por tanto A es creativo.

3.6 Pares productivos

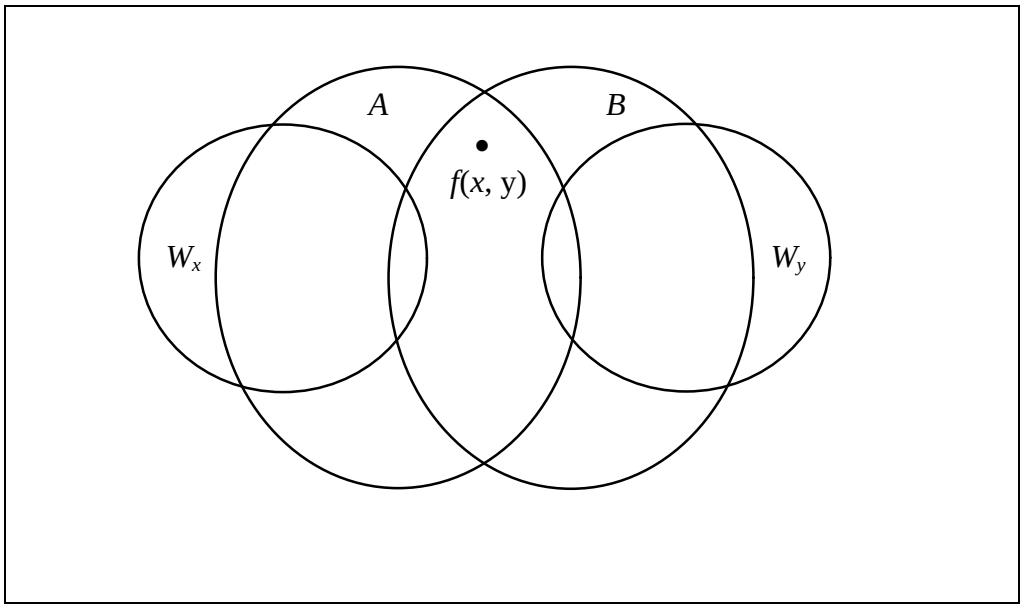
Las nociones de par productivo y par creativo se deben a Smullyan [53], que utiliza las denominaciones "pares doblemente productivos" y "pares doblemente creativos". La motivación y el interés de estos conceptos se observan en los teoremas [3-18] y [3-22], en donde se relacionan con la noción de pares de conjuntos efectivamente inseparables

[3-13] Definición

Sean A y B dos conjuntos de naturales. El par (A, B) es un *par productivo* si existe una función recursiva $f : \omega^2 \to \omega$ tal que

$(W_x \subset A \cup \overline{B}\ \&\ W_y \subset B \cup \overline{A}\ \&\ W_x \cap W_y = \varnothing) \Rightarrow f(x, y) \in A \cap B \cap \overline{W_x} \cap \overline{W_y}$

En tal caso se dice que f es una *función de productividad* del par (A, B).



Observación.
Si (A, B) es un par productivo A y B no pueden ser disjuntos. En efecto, si consideramos $W_u = \varnothing$, sería $f(u, u) \in A \cap B$.

[3-14] Proposición

Sean A y B dos conjuntos de naturales. El par $(\overline{A}, \overline{B})$ es productivo syss

$W_x \cap (A - B) = \varnothing\ \&\ W_y \cap (B - A) = \varnothing\ \&\ W_x \cap W_y = \varnothing \Rightarrow f(x, y) \in \overline{A} \cap \overline{B} \cap \overline{W_x} \cap \overline{W_y}$

Demostración.
Basta observar que $M \subset N \Leftrightarrow M \cap \overline{N} = \varnothing$ y que $M - N = M \cap \overline{N}$

[3-15] Proposición

Sean A y B dos conjuntos disjuntos de números naturales. Entonces el par $(\overline{A}, \overline{B})$ es productivo syss

$$W_x \subset \overline{A} \ \& \ W_y \subset \overline{B} \ \& \ W_x \cap W_y = \varnothing \ \Rightarrow \ f(x, y) \in \ \overline{A} \ \cap \ \overline{B} \ \cap \ \overline{W_x} \cap \overline{W_y}$$

[3-16] Proposición

El par (A, B) es productivo syss existe $h : \omega \to \omega$ tal que

$(W_{L(x)} \subset A \cup \overline{B} \ \& \ W_{R(x)} \subset B \cup \overline{A} \ \& \ W_{L(x)} \cap W_{R(x)} = \varnothing) \ \Rightarrow \ h(x) \in A \cap B \cap \overline{W}_{L(x)} \cap \overline{W}_{R(y)}$

Demostración

[$\Rightarrow$] Sea $f(x, y)$ función de producción de (A, B). Sea $h(x) = J(Lx, Rx)$

Si $W_{L(x)} \subset A \cup \overline{B} \ \& \ W_{R(x)} \subset B \cup \overline{A} \ \& \cup \overline{A} \ \& \ W_{L(x)} \cap W_{R(x)} = \varnothing$

entonces $h(x) = f(L(x), R(x)) \in A \cap B \cap \overline{W}_{L(x)} \cap \overline{W}_{R(y)}$

[$\Leftarrow$] Sea h como en el enunciado. Veamos que $f(x, y) = h(J(x, y))$ es una función de producción del par (A, B). Sea $W_x \subset A \cup \overline{B}$, $W_y \subset B \cup \overline{A}$ y $W_x \cap W_y = \varnothing$

Como $x = L(J(x, y))$ y $y = R(J(x, y))$ se verifica

$$W_{L(J(x,y))} \subset A \cup \overline{B} \ \& \ W_{R(J(x,y))} \subset B \cup \overline{A} \ \& \ W_{L(J(x,y))} \cap W_{R(J(x,y))} = \varnothing$$

luego $h(J(x, y)) \in A \cap B \cap \overline{W}_x \cap \overline{W}_y$

Diremos que h es una *función de producción* del par (A, B).

[3-17] Proposición

Si (A, B) es un par productivo entonces A y B son productivos

Demostración

Sea f la función de productividad del par (A, B). Sea $W_x \subset A$ y sea $W_v = \varnothing$. Entonces $W_x \subset A \cup \overline{B}$, $W_v \subset B \cup \overline{A}$ y $W_x \cap W_v = \varnothing$; luego $f(x, v) \in A \cap B \cap \overline{W}_x \cap \overline{W}_y$

Si consideramos la función recursiva $g(x) = f(x, v)$ es $g(x) \in A \cap \overline{W}_x$ y g es una función productiva para A, c.q.d. Análogo para B.

[3-18] Proposición

Sea $A \cap B = \varnothing$. Entonces son equivalentes :

1. A y B son efectivamente inseparables
2. $(\overline{A}, \overline{B})$ es un par productivo

Demostración

[1$\Rightarrow$2]

Sea $W_{g(x)} = B \cup W_x$ y $W_{h(y)} = A \cup W_y$

Sea f la función recursiva de separación de A y B

Se verifica $W_{h(y)} \subset A$, $W_{g(x)} \subset B$. Luego $f(h(y), g(x)) \in \overline{W_{h(y)} \cup W_{g(x)}}$

Así la función recursiva $t(x, y) = f(h(y), g(x))$ verifica $t(x, y) \in \overline{A} \ \cap \ \overline{B} \ \cap \ \overline{W}_x \cap \overline{W}_y$

[2⇒1]
Sea f función productiva de ($\overline{A}$, $\overline{B}$). Supongamos que $A \subset W_x$, $B \subset W_y$ y $W_x \cap W_y = \varnothing$. Entonces se verifica $W_y \subset \overline{W_x} \subset \overline{A}$ y $W_x \subset \overline{W_y} \subset \overline{B}$; luego $f(y, x) \in \overline{A} \cap \overline{B} \cap \overline{W_x} \cap \overline{W_y}$
Por tanto $g(x, y) = f(y, x)$ es función productiva del par (A, B)

[3-19] Proposición

Todo par productivo tiene una función de producción inyectiva
Demostración
Sea $f : \omega \to \omega$ función de producción del par (A, B)
Existe una función recursiva $q : \omega \to \omega$ tal que $W_{q(x)} = W_{Lx} \cup \{f(x)\}$
Sea $h(x) = J(Lx, q(x))$. Entonces $Lh(x) = Lx$ y $Rh(x) = q(x)$
Si consideramos el conjunto $S = \{f(x), f\,h(x), f\,h^2(x), f\,h^3(x), \ldots\}$ todos los elementos son distintos. Podemos definir g mediante

$$g(0) = 0$$

$$g(n+1) = \begin{cases} fh^r(n+1) & \text{siendo } r = mj \le g(n)\ fh^j(n+1) > g(n) \text{ si existe} \\ g(n)+1 & \text{e.o.c.} \end{cases}$$

Entonces g es estrictamente creciente y por tanto inyectiva. Y es una función productiva del par (A, B)

3.7 Pares creativos

Recordemos que un conjunto A es creativo si es r.e. y $\overline{A}$ es productivo

[3-20] Definición

(A, B) es un par creativo si A y B son r.e. y ($\overline{A}$, $\overline{B}$) es un par productivo

[3-21] Proposición

Si (A, B) es un par creativo, A y B son creativos
Demostración
Copnsecuencia de [3-16]

[3-22] Proposición

Sean A y B dos conjuntos r.e. disjuntos. Entonces son equivalentes

1. A y B son efectivamente inseparables
2. (A, B) es un par creativo

Demostración

Es una reformulación del teorema [3-17]

3.8 Reducibilidad

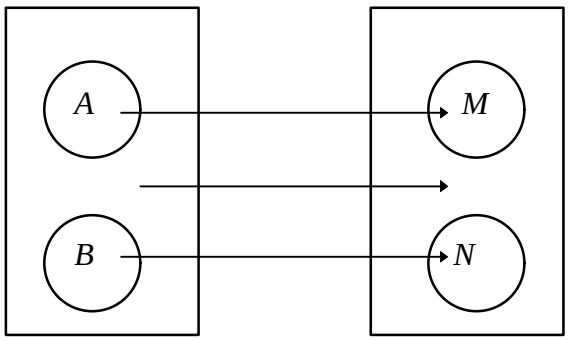
[3-23] Definición

Se dice que el par (A, B) es *reducible* al par (M, N) vía f, si f es una función recursiva verificando

$$x \in A \Leftrightarrow f(x) \in M$$
$$x \in B \Leftrightarrow f(x) \in N$$

Esta condición equivale a que $A = f^{-1}(M)$ y $B = f^{-1}(N)$. Obsérvese que esta condición significa que f aplica A en M, B en M y $\overline{A \cup B}$ en $\overline{M \cup N}$

Obsérvese también que si (A, B) es reducible al par (M, N) via f, entonces también ($\overline{A}$, $\overline{B}$) es reducible a ($\overline{M}$, $\overline{N}$) via f



[3-24] Proposición

Si (A, B) es reducible a (M, N) y (A, B) es productivo entonces (M, N) es productivo

Demostración

Sea f la función de reducción, g la función de productividad de (A, B), y h la función recursiva tal que $W_{h(x)} = f^{-1}(W_x)$

Entonces de

$W_x \subset M \cup \overline{N}$, $W_y \subset N \cup \overline{M}$, $W_x \cap W_y = \varnothing$

se deduce

$W_{h(x)} \subset A \cup \overline{B}$, $W_{h(y)} \subset B \cup \overline{A}$ y $W_{h(x)} \cap W_{h(y)} = \varnothing$;

luego

$g(h(x), h(y)) \in \overline{A} \cap \overline{B} \cap \overline{W}_{h(x)} \cap \overline{W}_{h(y)}$

y por tanto

$f(g(h(x), h(y))) \in \overline{M} \cap \overline{N} \cap \overline{W}_x \cap \overline{W}_y$.

Luego $f(g(h(x), h(y)))$ es una función de producción del par (M, N)

3.9 Pares completos

[3-25] Definición

El par (A, B) es Σ_1-*completo* si A y B son r.e. y todo par de conjuntos r.e. es reducible a (A, B)

[3-26] Proposición

Todo par Σ_1-completo es un par creativo.

Demostración

Sea (M, N) un par Σ_1-completo. Sea (A_0, A_1) el par de conjuntos disjuntos r.e. y efectivamente inseparables de [3-9]. Será (A_0, A_1) reducible a (M, N)

Por el teorema [3-18] $(\overline{A}_0, \overline{A}_1)$ es un par productivo, por ser (A_0, A_1) efectivamente inseparables, y además es reducible a $(\overline{M}, \overline{N})$. Por [3-24] $(\overline{M}, \overline{N})$ es productivo y por tanto (M, N) es creativo.

El recíproco también es cierto. La prueba es similar a la del teorema [2-22] pero requiere el teorema de doble recursión

[3-27]Teorema

Un par creativo es Σ_1-completo

Demostración

Sea (A, B) un par creativo y $f:\omega \to \omega$ una función inyectiva de producción del par ($\overline{A}$, $\overline{B}$). Dado un par de conjuntos r.e. disjuntos (M, N) sean m y n funciones recursivas e inyectivas verificando

$$\varphi_{m(x,y)}(z) = \begin{cases} 0 & \text{si} \quad x \in M \wedge f(y) = z \\ \uparrow & \text{e.o.c.} \end{cases}$$

$$\varphi_{n(x,y)}(z) = \begin{cases} 0 & \text{si} \quad x \in N \wedge f(y) = z \\ \uparrow & \text{e.o.c.} \end{cases}$$

Como consecuencia del teorema de doble recursión existe una función inyectiva h tal que

$$\varphi_{Lh(x)}(z) = \begin{cases} 0 & \text{si} \quad x \in M \wedge f(h(x)) = z \\ \uparrow & \text{e.o.c.} \end{cases}$$

$$\varphi_{Rh(x)}(z) = \begin{cases} 0 & \text{si} \quad x \in N \wedge f(h(x)) = z \\ \uparrow & \text{e.o.c.} \end{cases}$$

En consecuencia

$$W_{Lh(x)} = \begin{cases} \{ f(h(x)) & \text{si} \quad x \in M \\ \varnothing & \text{si} \quad x \notin M \end{cases}$$

$$W_{Rh(x)} = \begin{cases} \{ f(h(x)) & \text{si} \quad x \in N \\ \varnothing & \text{si} \quad x \notin N \end{cases}$$

Entonces (M, N) es reducible a (A, B) vía fh. En efecto, supongamos que $x \in M$ y $fh(x) \notin$ A. Entonces :

$W_{Lh(x)} = \{fh(x)\} \subset \overline{A} \subset \overline{A} \cup B$

$W_{Rh(x)} = \varnothing \subset \overline{B} \cup$ A

$W_{Lh(x)} \cap W_{Rh(x)} = \varnothing$

con lo que

$fh(x)\} \notin W_{Lh(x)}$,

contradicción.

Supongamos ahora que $x \notin M$ y $fh(x) \in$ A. Entonces :

$W_{Lh(x)} = \varnothing \subset \overline{A} \cup B$

$W_{Rh(x)} \subset$ A $\subset \overline{B} \cup$ A

$W_{Lh(x)} \cap W_{Rh(x)} = \varnothing$

con lo que

$fh(x) \in \overline{A}$,

contradicción.

Así pues,

$$x \in M \Leftrightarrow fh(x) \in A$$

y análogamente

$$x \in N \Leftrightarrow fh(x) \in B$$

3.10 Pares recursivamente isomorfos

Recordemos que dos conjuntos A y B de naturales son recursivamente isomorfos si hay una permutación recursiva f tal que $x \in A \Leftrightarrow f(x) \in B$. La generalización natural es :

[3-28] Definición

Dos pares de conjuntos de números naturales disjuntos (A, B) y (M, N) son *recursivamente isomorfos*, lo que se denotará por $(A, B) \equiv (M, N)$, si existe una biyección recursiva $f : \omega \rightarrow \omega$ tal que $f(A) = M$ y $f(B) = N$

3.11 Teorema de Smullyan

La demostración de Myhill de que dos conjuntos 1-equivalentes son recursivamente isomorfos [2-27] puede adaptarse sin dificultad para probar el siguiente teorema análogo para pares de conjuntos

[3-29] Teorema

Dos pares de conjuntos Σ_1-completos son recursivamente isomorfos

Demostración

Si f y g son las funciones de reducibilidad entre los pares (A, B) y (M, N) la construcción de Myhill (que únicamente depende de f y g) produce una biyección recursiva h tal que

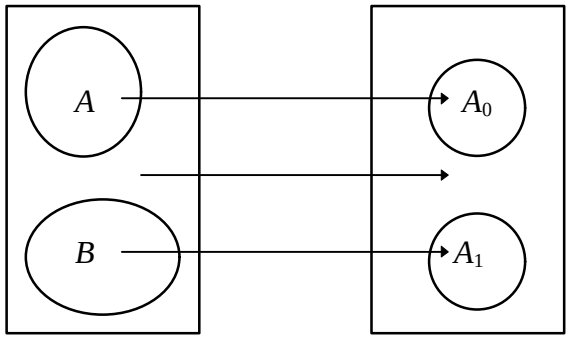
$$x \in A \Leftrightarrow h(x) \in M$$
$$x \in B \Leftrightarrow h(x) \in N$$

Como consecuencia de los resultados anteriores se obtiene el ilustrador teorema siguiente acerca de los pares de conjuntos efectivamente inseparables: todos los pares de conjuntos disjuntos efectivamente inseparables son esencialmente iguales desde el punto de vista de la teoría de la recursión; en particular, si consideramos teorías axiomatizables

en que el conjunto de teoremas y de fórmulas refutables (o finitamente refutables) sean inseparables , el teorema nos permite considerarlas, desde este punto de vista, como equivalentes.

[3-30] Teorema

Sea (A, B) un par de conjuntos disjuntos recursivamente enumerables. Son equivalentes
i. (A, B) es efectivamente inseparable
ii. (A, B) es creativo
iii. (A, B) es Σ_1-completo
iv. (A, B) $\equiv$ (A_0, A_1)



4. TEORÍAS

En este capítulo se revisa la terminología relativa a las teorías de primer orden y se presentan algunos resultados básicos. En particular, se consideran los conceptos relativos a la decidibilidad e indecidibilidad de teorías y sus propiedades fundamentales. Se tratan también los conceptos de inseparabilidad e inseparabilidad finita de teorías y sus propiedades. La idea de inseparabilidad es especialmente util en las demostraciones de indecidibilidad de teorías.

4.1 Lenguajes. Estructuras. Modelos

Consideraremos lenguajes de primer orden. Un lenguaje de primer orden está determinado por una signatura. Una signatura es una cuadrupla

$$\sigma = (\text{CONST}, \text{FUNC}, \text{PRED}, \mu)$$

donde los tres conjuntos disjuntos CONST, FUNC y PRED son respectivamente los símbolos de constante, de función y de predicado de la signatura. La función

$$\mu : \text{FUNC} \cup \text{PRED} \rightarrow \omega - \{0\}$$

determina el número de argumentos de un símbolo de función o de predicado. Denotaremos por $\text{FUNC}^{(n)}$ el conjunto de símbolos de función n-aria y por $\text{PRED}^{(n)}$ el conjunto de símbolos de predicado n-ario.

Las signaturas consideradas serán finitas, por lo que frecuentemente nos referiremos a ellas sencillamente listando los símbolos que la integran. Por ejemplo una signatura adecuada para un lenguaje en el que expresar la teoría de grupos es $\sigma_{\text{GRUPOS}} = \{e, \circ\}$ donde e es un símbolo de constante (que designa el elemento neutro del grupo) y $\circ$ una función binaria (que designa la operación del grupo). Si bien muchos de los desarrollos pueden realizarse para signaturas infinitas el hecho de ser finitas será esencial en algunas demostraciones, lo que se señalará en su momento. Puesto que las teorías matemáticas habituales se expresan en lenguajes de signatura finita no se trata de una restricción para los objetivos del trabajo.

Fijada una signatura σ, y utilizando los símbolos lógicos usuales y las variables se definen las fórmulas de la signatura. El conjunto de variables es $\text{VAR} = \{x_i : i \in \omega\}$, aunque utilizaremos también x, y, z, ... como nombres de variables. Denotaremos por L_σ el lenguaje o conjunto de fórmulas de la signatura σ. El conjunto de fórmulas cerradas o sentencias de la signatura se denota por $\text{SENT}(L_\sigma)$, o bien SENT_σ, o también, si la signatura queda clara por el contexto, sencillamente SENT.

En ocasiones será significativo el hecho de tratar de un lenguaje con igualdad o sin ella. Denotaremos en tales casos por $L_\sigma^=$, o bien L_σ , el lenguaje con igualdad, y por L_σ^0 el

lenguaje sin igualdad. El signo de igualdad en el lenguaje será "=". Como es habitual escribiremos $t \neq s$ en lugar de $\neg\, t = s$.
Si no induce a confusión nos referiremos en general a un lenguaje L sin explicitar la signatura σ.
Dada una signatura σ, una σ-estructura A consta de un universo no vacío A, una realización c^A para cada símbolo de constante $c \in$ CONST, una realización f^A para cada símbolo de función $f \in$ FUNC, y una realización P^A para cada símbolo de predicado $P \in$ PRED. (En ocasiones utilizaremos la misma notación para el símbolo del lenguaje y su realización en la estructura, si esto no induce a confusión). En el caso de lenguajes con igualdad consideraremos sólo modelos normales, esto es, modelos en los que el símbolo de igualdad designa la identidad en la estructura. Denotaremos por E_σ la clase de todas las σ-estructuras.
Una valoración en A es una asignación a cada variable de un elemento del universo de la estructura v :VAR $\rightarrow$ A. Una interpretación sobre la estructura A es un par formado por una estructura y una valoración I = (A ; v). (Nota : En este trabajo el término "interpretación" se usará fundamentalmente en otro sentido. Cf. capítulo 5.)
Se define de forma habitual que una fórmula $\varphi \in \mathsf{L}$ sea válida en una interpretación, lo que se denota $\mathsf{I} \models \varphi$ o también $\mathsf{A} \models \varphi$ [v]. Se denota por $\mathsf{A} \models \varphi$ el hecho de ser φ válida en todas las interpretaciones sobre A. Diremos en tal caso que A es un modelo de φ. Si Φ es un conjunto de fórmulas escribiremos también $\mathsf{A} \models \Phi$ para indicar que A es modelo de todas las fórmulas de Φ. Una fórmula lógicamente válida es una sentencia de la que cualquier σ-estructura es modelo. Lo denotamos por $\models \varphi$.
El conjunto de variables libres de una fórmula α se denota por lib(α). Si $x \in$ lib(α), lo que indicaremos escribiendo $\alpha(x)$, y α es válida en una interpretación con la valoración v(x) = a $\in$ A, escribiremos $\mathsf{A} \models \alpha$ [a]. Análoga notación usaremos para fórmulas con varias variables libres.
La relación de consecuencia semántica se indica como es usual por el símbolo $\models$. Si φ es una fórmula y Φ un conjunto de fórmulas, $\Phi \models \varphi$, significa que todo modelo de Φ es modelo de φ.
El teorema de completitud asegura que si $\vdash$ denota la relación de derivabilidad sintáctica en un sistema axiomático como el de Hilbert, se verifica

$$\Phi \models \varphi \quad \text{syss} \quad \Phi \vdash \varphi,$$

Si Φ es un conjunto de sentencias, el conjunto de consecuencias de Φ se denota por

$$\text{Con}(\Phi) = \{\varphi \in \text{SENT} : \Phi \vdash \varphi\} = \{\varphi \in \text{SENT} : \Phi \models \varphi\}$$

Naturalmente la relación de consecuencia depende del lenguaje que estemos considerando. Generalmente quedará claro por el contexto, pero si queremos hacer mención del mismo escribiremos Con_σ para señalar que estamos en el sistema de signatura σ.
Claramente, si Φ y Ψ son dos conjuntos de sentencias

$$\Phi \subset \Psi \Rightarrow \text{Con}(\Phi) \subset \text{Con}(\Psi)$$

Si Φ es un conjunto de sentencias, la clase de σ-estructuras que son modelo de Φ se denomina $\text{Mod}_\sigma(\Phi)$, o sencillamente Mod(Φ).

$$\text{Mod}_\sigma(\Phi) = \{ \mathsf{A} \in \mathsf{E}_\sigma : \mathsf{A} \models \Phi \}$$

Si Φ consta de una única fórmula φ escribiremos también $\text{Mod}_\sigma(\varphi)$ o bien Mod(φ) en lugar de $\text{Mod}_\sigma(\{\varphi\})$

[4-1] Proposición

1. $\mathrm{Mod}_\sigma(\Phi) = \bigcap_{\varphi\in\Phi} \mathrm{Mod}(\varphi)$
2. $\mathrm{Mod}_\sigma(\varnothing) = \mathsf{E}_\sigma$
3. $\Phi \models \alpha \Leftrightarrow \mathrm{Mod}_\sigma(\Phi) \subset \mathrm{Mod}_\sigma(\alpha)$

4.2 Teorías

Una teoría es un conjunto de sentencias cerrado bajo la relación de consecuencia, o lo que es lo mismo, cerrado bajo derivabilidad.

[4-2] Definición

Sea T un conjunto de sentencias de un lenguaje de primer orden de signatura σ. T es una *teoría sobre s* si para cada sentencia α de SENT_σ se verifica

$$\vdash \alpha \quad \Leftrightarrow \quad \alpha \in T$$

Diremos que T es una *teoría* (de primer orden) si para cierta σ, T es una teoría sobre σ.

Dada una teoría T nos referiremos al lenguaje de la misma mediante $\mathsf{L}(T)$ y a la signatura del lenguaje mediante $\sigma_{L(T)}$. Indicaremos por T^0 que la teoría se considera en un lenguaje sin igualdad.

Ejemplos

1. Teoría engendrada por un conjunto de sentencias
Sea Φ un conjunto de sentencias. Es inmediato ver que

$$\mathrm{Con}(\Phi) = \{\alpha : \Phi \vdash \alpha\}$$

es una teoría, denominada *teoría engendrada por* Φ.
Claramente se tiene

$$T \text{ es una teoría } \Leftrightarrow \mathrm{Con}(T) = T$$

2. El conjunto de todas las fórmulas lógicamente válidas $\mathrm{LVAL}_\sigma = \{\alpha \in \mathrm{SENT}_\sigma : \models \alpha\}$ es una teoría contenida en toda otra teoría. Es la mínima teoría de un lenguaje dado. El conjunto de todas las sentencias del lenguaje es claramente una teoría. Y es la máxima teoría formulable sobre el lenguaje. Es la única teoría insatisfactible. Una teoría es *consistente* si no es SENT_σ e *inconsistente* en caso contrario.

[4-3] Proposición.

Son equivalentes

1. T es inconsistente
2. Existe $\alpha \in SENT$ tal que $\alpha \in T$ y $\neg\alpha \in T$
3. T no tiene modelos

3. Si $\{T_i : i \in I\}$ es una familia arbitraria de teorías sobre σ entonces su intersección es también una teoría, pues

$$\bigcap T_i \vdash \alpha \Rightarrow \ \forall i \in I \ T_i \vdash \alpha \Rightarrow \ \forall i \in I \ \alpha \in T_i \Rightarrow \ \alpha \in \bigcap T_i$$

En general la unión de dos teorías *no* es un conjunto cerrado bajo derivabilidad. Pero podemos considerar la familia de todas las teorías en el lenguaje que contienen a ambas. Su intersección es una teoría; y es la mínima teoría que contiene a ambas. La denotaremos por $T_1 + T_2$.

Si tenemos una cadena de teorías $T_0 \subset T_1 \subset T_2 \subset ...$ entonces $\bigcup_{i\in\omega} T_i$ es una teoría pues

$$\bigcup_{i\in\omega} T_i \vdash \alpha \ \Rightarrow \text{existen } \varphi_1, ... ,\varphi_k \in \bigcup_{i\in\omega} T_i \ \{\varphi_1, ... ,\varphi_k\} \vdash \alpha$$

$$\Rightarrow \text{existe } m \in \omega \text{ y existen } \varphi_1, ... , \varphi_k \in T_m \text{ tales que } \{\varphi_1, ... , \varphi_k\} \vdash \alpha$$

$$\Rightarrow \alpha \in T_m \subset \bigcup_{i\in\omega} T_i$$

4. Teoría de una estructura.

Sea A una σ-estructura. El conjunto $Th(\mathsf{A}) = \{\alpha \in SENT_\sigma : \mathsf{A} \vDash \alpha\}$ es una teoría, pues

$$Th(\mathsf{A}) \vdash \alpha \ \Rightarrow \ \mathsf{A} \vDash \alpha \ \Rightarrow \ \alpha \in Th(\mathsf{A})$$

Un ejemplo importante consiste en la teoría de la estructura de los números naturales con las operaciones aritméticas elementales $\mathsf{N} = (\omega; 0^\omega, s^\omega, +^\omega, \cdot^\omega)$. La teoría $Th(\mathsf{N})$ se denomina la *aritmética elemental* (de primer orden)

5. Teoría de una clase de estructuras

Sea K una clase de σ-estructuras. La teoría de la clase K es el conjunto de sentencias

$$Th(\mathsf{K}) = \{\alpha \in SENT_\sigma : \text{para todo } \mathsf{A} \in \mathsf{K} \ \ \mathsf{A} \vDash \alpha\}$$

Nótese que

$$\alpha \in Th(\mathsf{K}) \ \Leftrightarrow \ \mathsf{K} \subset Mod(\alpha)$$

Es una teoría: el apartado 1 de la siguiente proposición indica que $Th(\mathsf{K})$ es intersección de una familia de teorías y por tanto una teoría.

[4-4] Proposición

1. $Th(\mathsf{K}) = \bigcap_{\mathsf{A}\in\mathsf{K}} Th(\mathsf{A})$
2. $Th(\varnothing) = L_\sigma$

3. $A \in \mathsf{K} \Rightarrow \mathrm{Th}(\mathsf{K}) \subset \mathrm{Th}(A)$

Nótese que la implicación contraria de 3. no es cierta.
Si K es una clase de estructuras sobre el mismo lenguaje nos referiremos mediante $L(\mathsf{K})$ a dicho lenguaje

Nota
En este trabajo haremos referencia continuamente a clases de estructuras. En todo momento todas las estructuras pertenecientes a una clase serán estructuras sobre una misma signatura, no mezclando nunca en una misma clase estructuras sobre diversas signaturas. En adelante no nos preocuparemos de señalar esta estipulación. De forma que expresiones como "sea K un clase de estructuras" significarán "sea K una clase de σ-estructuras" para cierta signatura σ.

La conexión de Galois (Mod,Th)

Es particularmente interesante considerar conjuntamente las dos correspondencias

$$\begin{aligned} \mathrm{Mod} : \mathsf{P}(L_\sigma) &\to \mathsf{P}(\mathsf{E}_\sigma) \\ \Phi &\to \mathrm{Mod}(\Phi) \\ \mathrm{Th} : \mathsf{P}(\mathsf{E}_\sigma) &\to \mathsf{P}(L_\sigma) \\ \mathsf{K} &\to \mathrm{Th}(\mathsf{K}) \end{aligned}$$

[4-5] Proposición

Sea K una clase de σ-estructuras y Φ un conjunto de sentencias de L_σ. Se verifica :

$$\mathsf{K} \subset \mathrm{Mod}(\Phi) \Leftrightarrow \Phi \subset \mathrm{Th}(\mathsf{K})$$

Demostración
[$\Rightarrow$]
Sea $\mathsf{K} \subset \mathrm{Mod}(\Phi)$ y $\varphi \in \Phi$. Entonces, $A \in \mathsf{K} \Rightarrow A \vDash \Phi \Rightarrow A \vDash \varphi \Rightarrow \varphi \in \mathrm{Th}(A)$
Por tanto $\varphi \in \bigcap_{A \in \mathsf{K}} \mathrm{Th}(A) = \mathrm{Th}(\mathsf{K})$
[$\Leftarrow$]
Sea $\Phi \subset \mathrm{Th}(\mathsf{K})$. Entonces, $A \in \mathsf{K} \Rightarrow A \vDash \mathrm{Th}(\mathsf{K}) \Rightarrow A \in \mathrm{Mod}(\mathrm{Th}(\mathsf{K})) \Rightarrow A \in \mathrm{Mod}(\Phi)$

La anterior proposición expresa que el par (Mod, Th) es una conexión de Galois entre los conjuntos de fórmulas y las clases de estructuras. Sean $(A, \leq^A)$ y $(B, \leq^B)$ dos conjuntos parcialmente ordenados y $\pi_* : A \to B$ y $\pi^* : B \to A$ dos aplicaciones verificando, para todo $a \in A$ y todo $b \in B$

$$a \leq^A \pi^*(b) \Leftrightarrow \pi_*(a) \leq^B b$$

Se dice entonces que el par (π_*, π^*) es una *conexión de Galois* entre ambas estructuras.

Las propiedades básicas de una conexión de Galois son :

[4-6] Proposición

Sean $\Phi_1, \Phi_2 \subset L_\sigma$ y $K_1, K_2 \subset E_\sigma$; entonces :
Ga1. $\Phi_1 \subset \Phi_2 \Rightarrow Mod(\Phi_2) \subset Mod(\Phi_1)$
Ga2. $K_1 \subset K_2 \Rightarrow Th(K_2) \subset Th(K_1)$
Ga3. $\Phi \subset Th(Mod(\Phi))$
Ga4. $K \subset Mod(Th(K))$
Demostración
1. $\Phi_1 \subset \Phi_2 \Rightarrow Mod(\Phi_2) = \bigcap_{\varphi \in \Phi_2} Mod(\varphi) \subset \bigcap_{\varphi \in \Phi_1} Mod(\varphi) \subset Mod(\Phi_1)$
2. $K_1 \subset K_2 \Rightarrow Th(K_2) = \bigcap_{A \in K_2} Th(A) \subset \bigcap_{A \in K_1} Th(A) = Th(K_1)$
3. $\alpha \in \Phi \Rightarrow Mod(\Phi) \subset Mod(\alpha) \Rightarrow \alpha \in Th(Mod(\Phi))$
4. $A \in K \Rightarrow A \models Th(K) \Rightarrow A \in Mod(Th(K))$

Como en toda conexión de Galois se verifica que Mod y Th son cuasiinversas, esto es:

[4-7] Proposición

1. $Mod(\Phi) = Mod(Th(Mod(\Phi)))$
2. $Th(K) = Th(Mod(Th(K))$

Demostración
1. Aplicando Ga4 a $Mod(\Phi)$ se tiene $Mod(\Phi) \subset Mod(Th(Mod(\Phi)))$. Y aplicando Ga1 a Ga3 $Mod(Th(Mod(\Phi)) \subset Mod(\Phi)$
2. Aplicando Ga3 a $Th(K)$: $Th(K) \subset Th(Mod(Th(K))$. Y aplicando Ga2 a Ga4 $Th(Mod(Th(K))) \subset Th(K)$

Como en toda conexión de Galois los operadores

$$\text{Th-Mod} : P(L_\sigma) \to P(L_\sigma)$$
$$\Phi \to Th(Mod(\Phi))$$

$$\text{Mod-Th} : P(E_\sigma) \to P(E_\sigma)$$
$$K \to Mod(Th(K))$$

son operadores de clausura sobre L_σ y E_σ respectivamente. Un operador de *clausura* sobre un conjunto M es una aplicación $C : P(M) \to P(M)$ verificando

1. $X \subset C(X)$
2. $X \subset Y \Rightarrow C(X) \subset C(Y)$
3. $C(C(X)) = C(X)$

[4-8] Proposición

Si Φ es un conjunto de fórmulas y consideramos la clase de todos los modelos de Φ

$$Mod(\Phi) = \{A : A \vDash \Phi\}$$

Se verifica

$$Th(Mod(\Phi)) = Con(\Phi)$$

Demostración

$$\alpha \in Th(Mod(\Phi)) \Leftrightarrow \forall A \ (A \vDash \Phi \Rightarrow A \vDash \alpha) \Leftrightarrow \Phi \vDash \alpha \Leftrightarrow \alpha \in Con(\Phi)$$

[4-9] Proposición

Sea $\Phi \subset L_\sigma$. Son equivalentes

1. Φ es una teoría
2. $\Phi = Th(Mod(\Phi))$
3. existe una clase $K \subset E^\sigma$ tal que $\Phi = Th(K)$

En particular para una teoría T se tiene siempre que

$$Th(Mod(T) = T$$

que es una propiedad más fuerte que Ga3. Y esto es lo que caracteriza a las teorías. En términos del operador clausura ThMod, las teorías son conjuntos de fórmulas cerrados, esto es coinciden con su clausura.

Obsérvese que, en general, el contenido de Ga3 y Ga4 no puede completarse a igualdad. Por ejemplo, si consideramos una clase K con una única estructura infinita A. Entonces $Th(A)$ tiene modelos de cardinalidad infinita arbitraria que no pueden ser A. Esto muestra un ejemplo en el que el contenido de Ga4 es estricto. Y hemos señalado anteriormente que $Th(Mod(\Phi))$ es siempre una teoría, con lo que si Φ no es una teoría tenemos que el contenido en Ga3 es estricto.

La clase de modelos finitos de una teoría

Sea T una teoría y Mod(T) la clase de modelos de T. Tienen interés considerar el subconjunto de Mod(T) formado por las σ-estructuras *finitas* que son modelos de T

$$Modfin(T) = \{A : A \vDash T \ \& \ A \text{ finito}\}$$

Esta clase determina una teoría

$$T_{fin} = Th(Modfin(T))$$

que contiene a las sentencias válidas en todos los modelos finitos de la teoría.
Obsérvese que siempre

$$T \subset T_{fin}$$

pues

$$Modfin(T) \subset Mod(T) \Rightarrow Th(Mod(T) \subset Th(Modfin(T) \Rightarrow T \subset T_{fin}\ .$$

Además :

$$T_1 \subset T_2 \Rightarrow Modfin(T_2) \subset Modfin(T_1)$$
$$\Rightarrow Th(Modfin(T_1) \subset Th(Modfin(T_2)$$
$$\Rightarrow T_{1_{fin}} \subset T_{2_{fin}}$$

Obsérvese que si T no tiene modelos finitos $T_{fin} = SENT_\sigma$.

En general T_{fin} puede tener modelos infinitos. En efecto, supongamos que T tiene modelos de cardinalidad arbitrariamente grande (esto es lo que ocurre en la teoría de grupos, por ejemplo). Consideremos para cada n natural la fórmula $\kappa_{\geq n}$ que expresa que la estructura tiene más de n elementos. Cada subconjunto finito de

$$S = T_{fin} \cup \{\kappa_{\geq 1}, \kappa_{\geq 2}, \kappa_{\geq 3}, ...\}$$

tiene modelo. Por el teorema de compacidad, S tiene un modelo que deberá ser modelo de T_{fin} y a la vez una estructura infinita.
Esta observación muestra de nuevo que si K es una clase de estructuras, un modelo de $Th(\mathsf{K})$ no pertenece necesariamente a K

Análogamente podríamos considerar la clase de los modelos infinitos de T. La teoría que determinan es T_{inf}

Sea K una clase de estructuras. Podemos considerar la subclase de K formada por las estructuras finitas, $\mathsf{K}^{fin} = \{\mathsf{A} : \mathsf{A} \in \mathsf{K}\ \&\ \mathsf{A}$ finita$\}$. Esta clase determina una teoría $Th(\mathsf{K}^{fin})$. Esta teoría coincide con la teoría finita de K., según indica la siguiente

[4-10] Proposición

Sea K una clase de estructruras

$$Th(\mathsf{K}^{fin}) = Th(\mathsf{K})_{fin}$$

Demostración
[$\supset$]

$$\alpha \in Th(\mathsf{K})_{fin} \Rightarrow \forall\, \mathsf{A}\ (\mathsf{A} \vDash Th(\mathsf{K})\ \&\ \mathsf{A}\text{ finita} \Rightarrow \mathsf{A} \vDash \alpha)$$
$$\Rightarrow \forall\, \mathsf{A} \in \mathsf{K}\ \ (\mathsf{A}\text{ finita} \Rightarrow \mathsf{A} \vDash \alpha)$$
$$\Rightarrow \forall\, \mathsf{A} \in \mathsf{K}^{fin}\ \ \mathsf{A} \vDash \alpha$$
$$\Rightarrow \alpha \in Th(\mathsf{K}^{fin})$$

[$\subset$]
Supongamos que para cierta fórmula α se verifica $\alpha \notin Th(\mathsf{K})_{fin}$. Existirá una cierta estructura A verificando

1. $A \in K$
2. A es finita
3. $A \nvDash \alpha$

Por ser A finita existe una fórmula $\rho \in L(K)$ tal que para toda estructura M de la misma signatura que A se verifica

4. $M \vDash \rho \quad \Leftrightarrow \quad A \approx M$

Por tanto

5. $A \vDash \rho$ (por 4.)
6. $\neg\rho \notin Th(K)$ (por 5. y 1.)
7. existe $B \in K$ tal que $B \vDash \rho$ (por 6.)
8. existe $B \in K$ tal que $B \approx A$ y $B \nvDash \alpha$ (por 7. y 3.)
9. $\alpha \notin Th(K^{fin})$ (por 8. y 2.)

[4-11] Definición

Denotaremos por Fr(K) el conjunto de fórmulas $\{\alpha$: existe $A \in K^{fin}$ tal que $A \vDash \neg\alpha\}$

4.3 Subteorías

Sean T_1 y T_2 dos teorías en dos lenguajes con signaturas σ_1 y σ_2 respectivamente. Será útil la siguiente terminología.

[4-12] Definición

Se dice que T_2 es una *extensión* de T_1 o que T_1 es una *subteoría* de T_2 si

1. $\sigma_1 \subset \sigma_2$
2. $T_1 \subset T_2$

Se dice que T_2 es una *extensión simple* de T_1 si

1. $\sigma_1 = \sigma_2$
2. $T_1 \subset T_2$

Se dice que T_2 es una *extensión conservativa* de T_1 si

1. $\sigma_1 \subset \sigma_2$
2. para toda $\alpha \in SENT_{\sigma_1}$ $\quad \alpha \in T_2 \Rightarrow \alpha \in T_1$

Si T_2 es una extensión de T_1 se dice que T_2 es una *extensión no esencial* de T_1 si los únicos símbolos de σ_2 que no están en σ_1 son símbolos de constante y T_2 es el cierre por derivación en el lenguaje σ_2 de T_1

Se dice que T_2 es una *extensión finita* de T_1 si $\sigma_1 = \sigma_2$ y existe un conjunto finito de sentencias $\Phi \subset T_2$ tal que $T_2 = Con(T_1 \cup \Phi)$

Se dice que T_1 y T_2 son *compatibles* si $\sigma_1 = \sigma_2$ y $T_1 \cup T_2$ es consistente

Ejemplos

1. Es inmediato que

$$\mathsf{A} \models T \Leftrightarrow T \subset Th(\mathsf{A}),$$

por lo que Th(A) es una extensión simple de T si A es modelo de T.

2. Sea F la aritmética con la relación del orden. F es una extensión de la teoría del orden ORD pero no es una extensión simple pues los lenguajes no coinciden.
Tampoco es una extensión conservativa pues

$$F \vdash \exists x \forall y \neg(y < x)$$

pero

$$ORD \nvdash \exists x \forall y \neg(y < x)$$

pues hay órdenes lineales sin mínimo

4.4 Teorías axiomatizables

Una de las formas más utilizadas para determinar una teoría es considerar el conjunto de sentencias que se derivan de una serie de axiomas efectivamente dados. Dada una teoría T cualquiera siempre existe un conjunto de fórmulas del que se derivan todas las sentencias de T, pues T = Con(T). Pero si T = Con(Φ) y queremos que la teoría sea decidible, al menos el conjunto Φ debe ser decidible (e.e. el conjunto de códigos $\Phi^{\#}$ debe ser recursivo)

[4-13] Definición

Una teoría T es *axiomatizable* si existe un conjunto recursivo (decidible) de sentencias Φ, tal que T = Con(Φ). Este conjunto Φ es el conjunto de axiomas de la teoría. Si Φ es finito la teoría se llama *finitamente axiomatizable.*

Una teoría axiomatizable (no finitamente axiomatizable) suele darse por medio de esquemas de axiomas. Por ejemplo, el esquema de axiomas de inducción de la aritmética de Peano de primer orden tiene la forma

$$\text{IND}: \quad \varphi(0) \wedge \forall x\,(\varphi(x) \rightarrow \varphi(sx)) \rightarrow \forall x \varphi(x)$$

siendo φ(x) una fórmula con una variable libre. La aritmética de Peano de primer orden es axiomatizable, pero *no* es finitamente axiomatizable.

Observación

Si T es una teoría axiomatizable y $\{\varepsilon_1, ... ,\varepsilon_n\}$ es el conjunto de los axiomas podemos considerar la conjunción de los mismos $\varepsilon \equiv \varepsilon_1 \wedge ... \wedge \varepsilon_n$ y será $T = Con(\{\varepsilon\})$, es decir, una teoría finitamente axiomatizable puede considerarse como axiomatizada con un único axioma. Esta observación facilita algunas demostraciones.

[4-14] Proposición

Sea $T = Con(\Phi)$. Si T es una teoría finitamente axiomatizable existe $\Phi_0 \subset \Phi$, Φ_0 finito, tal que $T = Con(\Phi_0)$.

Demostración

Sea φ la conjunción de los axiomas de T . Entonces $T = Con(\{\varphi\})$. En general $\varphi \notin \Phi$ pero siempre $\Phi \vdash \varphi$. Por compacidad existe una cantidad finita de fórmulas de Φ de las que se deriva φ. Sea $\Phi_0 \subset \Phi$ dicho conjunto. Se verifica $\Phi_0 \vdash \varphi$. Por consiguiente $Con(\{\varphi\}) \subset Con(\Phi_0) \subset Con(\Phi) = T = Con(\{\varphi\})$, de donde se deduce $T = Con(\Phi_0)$.

El siguiente teorema, demostrado por Craig en 1953, muestra que el concepto lógico de teoría axiomatizable coincide con el concepto de conjunto recursivamente enumerable en teoría de la recursión. En particular tiene interés en el estudio de la decidibilidad e indecidibilidad: las teorías decidibles deben buscarse entre las teorías axiomatizables.

[4-15] Teorema

Sea T una teoría y $T^{\#} = \{n \in \omega : \alpha_n \in T\}$ el conjunto de los códigos de sus fórmulas. Entonces T es axiomatizable syss $T^{\#}$ es recursivamente enumerable

Demostración

[$\Rightarrow$]

Si $T = Con(\Phi)$ y Φ es un conjunto recursivo, en virtud del teorema de completitud de la lógica de primer orden, se tiene que $T = \{\alpha \in L(T) : \Phi \vdash \alpha\}$. En consecuencia $\alpha \in T$ syss existe una demostración de α a partir de Φ. De donde se sigue que $T^{\#}$ es la proyección de un conjunto recursivo, y por tanto es recursivamente enumerable.

[$\Leftarrow$]

Sea $T^{\#} \in \Sigma_1$. Como $T^{\#}$ no es vacío es el rango de una función recursiva $T^{\#} = rg\ f$ y entonces $T = \{\varphi_{f(n)} : n \in \omega\}$. Definamos g(n) por $\varphi_{g(n)} = \varphi_{f(0)} \wedge ... \wedge \varphi_{f(n)}$. La función g es recursiva y creciente.

Sea $T_0^{\#} = g(\omega)$ y $\Phi_0 = \{\varphi_n : n \in T_0^{\#}\}$. $T_0^{\#}$ es recursivo por ser g creciente (con lo que $g(n)>n$)

$$n \in T_0^{\#} \Leftrightarrow \exists m<n\ g(m) = n$$

Entonces $T = \{\alpha : \Phi_0 \vdash \alpha\}$ pues $\Phi_0 \vdash \alpha$ α se deriva de una cantidad finita, luego $\Phi \vdash \alpha$

Por tanto Φ es axiomatizable.

Ejemplos

1. Aritmética de Robinson y aritmética de Peano

Especialmente importantes son las teorías que axiomatizan la aritmética. Consideraremos la signatura $\sigma_A = \{0, s, +, \cdot\}$ donde 0 es un símbolo de constante, s un símbolo de función de un argumento y los símbolos + y · representan funciones de dos argumentos. Como es habitual escribiremos $x + y$ y $x \cdot y$ en lugar de $+xy$ y $\cdot xy$. La *aritmética de Robinson* **Q** es la teoría finitamente axiomatizable de $L_{\sigma_A}^{=}$ de axiomas

Q1 $\neg\exists x\ sx = 0$
Q2 $\forall x\ (x \neq 0 \rightarrow \exists y\ sy = x)$
Q3 $\forall x\ \forall y\ (sx = sy \rightarrow x = y)$
Q4 $\forall x\ (x + 0 = 0)$
Q5 $\forall x \forall y\ s(x + y) = x + sy$
Q6 $\forall x\ x \cdot 0 = 0$
Q7 $\forall x\ \forall y\ x \cdot sy = x \cdot y + x$

La *aritmética de Peano de primer orden* es la teoría axiomatizada por los siete axiomas anteriores y los infinitos axiomas descritos en el esquema

IND $(\varphi(0) \wedge \forall x\ (\varphi(x) \rightarrow \varphi(sx))\ ) \rightarrow \forall x\ \varphi(x)$

cuando φ es una σ_A-fórmula con una variable libre

2. Teoría de grupos

Con la signatura $\sigma_e = \{e, \circ\}$ siendo e un símbolo de constante y $\circ$ un símbolo de función de dos argumentos (como es habitual escribiremos $x \circ y$ en lugar de $\circ xy$) consideremos las siguientes sentencias de $L_{\sigma_e}^{=}$:

Asociativa GR1 $\forall x\ \forall y\ \forall z\ x \circ (y \circ z) = (x \circ y) \circ z$
Neutro GR2 $\forall x\ (x \circ e = x \wedge e \circ x = x)$
Simétrico GR3 $\forall x\ \exists y\ (x \circ y = e \wedge y \circ x = e)$
Conmutativa GR4 $\forall x\ \forall y\ x \circ y = y \circ x$

La *teoría de grupos* es GRUPOS = Con{GR1, GR2, GR3}
La *teoría de grupos conmutativos* es ABEL = Con{GR1, GR2, GR3, GR4}
La *teoría de grupos infinitos* es Con{GR1, GR2, GR3, $\kappa_{\geq 1}$, $\kappa_{\geq 2}$, $\kappa_{\geq 3}$, ... }

Un conjunto D con una operación asociativa $\circ$ tiene estructura de grupo si y sólo si las ecuaciones $a \circ x = b$ y $y \circ a = b$ tienen solución para todo $a, b \in D$. Así pues, es posible axiomatizar de forma equivalente la teoría de grupos en un lenguaje con signatura $\sigma_G = \{\circ\}$, siendo $\circ$ un símbolo de operación binaria, considerando las sentencias de $L_{\sigma_G}^{=}$

Simétrico por la izquierda GR5 $\forall x \forall y\ \exists z\ x = z \circ y$
Simétrico por la derecha GR6 $\forall x \forall y\ \exists z\ x = y \circ z$

La *teoría de grupos* es Con{GR1, GR5, GR6}
La *teoría de semigrupos* es Con{GR1}

3. Teoría de anillos y teoría de cuerpos

Consideramos la signatura $\sigma_C = \{0, 1, +, \times\}$ siendo 0 y 1 símbolos de constante y + y $\times$ símbolos de funciones de dos argumentos, que escribiremos en notación infija, como es habitual; sean las sentencias de σ_C

A1 $0 \neq 1$
A2 $\forall x \forall y \forall z \quad x + (y + z) = (x + y) + z$
A3 $\forall x \, (x + 0 = x \wedge 0+x = x)$
A4 $\forall x \exists y \, (x + y = 0 \wedge y + x = 0)$
A5 $\forall x \forall y \quad x + y = y + x$
A6 $\forall x \quad (x \times 1 = x \wedge 1 \times x = x)$
A7 $\forall x \forall y \forall z \quad x \times (y \times z) = (x \times y) \times z$
A8 $\forall x \forall y \forall z \quad x \times (y + z) = x \times y + x \times z$
A9 $\forall x \forall y \quad x \times y = y \times x$
A10 $\forall x \forall y \, (x \times y = 0 \rightarrow x = 0 \vee y = 0)$
A11 $\forall x \quad (x \neq 0 \rightarrow \exists y \quad x \times y = 1)$

Teoría de anillos con elemento unidad ANU = Con{A2, A3, A4, A5, A6, A7, A8}
Teoría de anillos conmutativos con elemento unidad
ANC = Con{A2, A3, A4, A5, A6, A7, A8, A9}
Teoría de los dominios de integridad
ANCDI = Con({A2, A3, A4, A5, A6, A7, A8, A10}
Teoría de cuerpos CUERPOS = Con{A1, A2, A3, A4, A5, A6, A7, A8, A11}

Realizando consideraciones análogas a las realizadas con la teoría de grupos se pueden reformular sin dificultad los axiomas en un lenguaje de signatura {+, $\times$}. Es usual también considerar una teoría de anillos sin exigir la existencia del elemento neutro de la multiplicación.

4. Teoría de retículos

Una de las formalizaciones del concepto de retículo utiliza la signatura $\sigma_R = \{\cup, \cap\}$ siendo $\cup$ e $\cap$ símbolos de función con dos argumentos, que escribiremos como es costumbre en notación infija.

Los axiomas de la teoría son

Conmutativa R1 $\forall x \forall y \quad x \cup y = y \cup x$
R2 $\forall x \forall y \quad x \cap y = y \cap x$
Asociativa R3 $\forall x \forall y \forall z \quad x \cup (y \cup z) = (x \cup y) \cup z$
R4 $\forall x \forall y \forall z \quad x \cap (y \cap z) = (x \cap y) \cap z$
Absorción R5 $\forall x \forall y \quad x \cup (x \cap y) = x$
R6 $\forall x \forall y \quad x \cap (x \cup y) = x$

La *Teoría de retículos* es RET = Con{R1, R2, R3, R4, R5, R6}

Puede axiomatizarse la teoría de retículos en un lenguaje de signatura {≤} siendo ≤ un símbolo de relación binario. Un retículo es un orden parcial en el que cada par de elementos tiene una cota inferior máxima y una cota superior mínima. Los axiomas de la teoría son pues :

Reflexiva RR $\forall x \quad x \leq x$
Antisimétrica RA $\forall x \forall y \, (x \leq y \wedge y \leq x \rightarrow x = y)$
Transitiva RT $\forall \forall y \forall z \, (x \leq y \wedge y \leq z \rightarrow x \leq z)$

c.i.m Ri $\forall x \forall y \exists z\ (z \leq x \wedge z \leq y \wedge \forall t\ (t \leq x \wedge t \leq y \rightarrow t \leq z))$
c.s.m Rs $\forall x \forall y \exists z\ (x \leq z \wedge y \leq z \wedge \forall t\ (x \leq t \wedge y \leq t \rightarrow z \leq t))$
La *teoría de retículos en el lenguaje del orden* es Con{RR, RA, RT, Ri, Rs}

5. Teoría de grafos
Un grafo puede considerarse como un conjunto con una relación binaria simétrica y antirreflexiva. Es decir, consideramos la signatura $\sigma_F = \{R\}$ donde R es un símbolo de predicado binario y las sentencias
Simetría F1 $\forall x\ \forall y\ (Rxy \rightarrow Ryx)$
Antirreflexiva F2 $\forall x\ \neg Rxy$
La *Teoría de grafos* es GRAFOS = Con{F1, F2}

4.5 Teorías completas

Una teoría completa da respuesta a todas las preguntas que pueden formularse en un lenguaje. Exigiremos que la teoría sea consistente para evitar el caso trivial. Entre las teorías consistentes las completas son maximales respecto de la inclusión.

[4-16] Definición

Una teoría consistente T es *completa* si para cada sentencia φ del lenguaje se verifica $\varphi \in T$ o bien $\neg\varphi \in T$

[4-17] Proposición

La teoría de una estructura es completa
Demostración.
Th(A) es consistente y

$$\alpha \notin Th(A) \Rightarrow A \nvDash \alpha \Rightarrow A \vDash \neg\alpha \Rightarrow \neg\alpha \in A$$

[4-18] Proposición

Toda teoría consistente y completa es la teoría de una estructura
Demostración
Si T es una teoría consistente completa tendrá algún modelo $A \vDash T$. Por tanto $T \subset Th(A)$. Al ser T completa debe ser T = Th(A); es decir, T es la teoría de una estructura.

[4-19] Proposición

Si T_1 es una teoría compatible con la teoría T_2 y T_1 es completa entonces $T_2 \subset T_1$

Demostración
$\varphi \notin T_1 \Rightarrow \neg\varphi \in T_1 \Rightarrow \varphi \notin T_2$, por ser T_2 compatible con T_1

4.6 Clases elementales

[4-20] Definición

Sea K una clase de estructuras. Se dice que K es una *clase D-elemental* si existe un conjunto de sentencias Φ tal que $\mathsf{K} = \mathrm{Mod}(\Phi)$
Se dice que K es una *clase elemental* si existe una sentencia φ tal que $\mathsf{K} = \mathrm{Mod}(\varphi)$
(Se usan también las terminologías "elemental" y "estrictamente elemental", o "elemental en sentido amplio" y "elemental". Y a veces - más inadecuadamente, si no se exige que Φ sea recursivo -, clase "axiomatizable" y "finitamente axiomatizable")

Ejemplo

1. La clase de los grupos K_G es una clase elemental. Si φ es la conjunción de los axiomas de grupo $\mathsf{K}_G = \mathrm{Mod}(\varphi)$
2. La clase de los cuerpos de característica p es elemental. Se dice que un cuerpo $\mathsf{C} = (C ; 0^C, 1^C, +^C, \times^C)$ es de característica p si
$$\underbrace{1^C + \ldots + 1^C}_{p \text{ veces}} = 0^C$$

Sea τ_p la fórmula $1 + \ldots + 1 = 0$
Un cuerpo es de característica cero si no hay ningún primo p tal que sea de característica *p*.
La clase de cuerpos de característica *p* es Δ-elemental pues es $\mathrm{Mod}(\mathrm{CUERPOS} \cup \{\tau_p\})$
La clase de los cuerpos de característica cero es Δ-elemental pues se trata de la clase $\mathrm{Mod}(\mathrm{CUERPOS} \cup \{\neg\, \tau_p : p \text{ primo}\})$. Pero no es elemental. En efecto, sea φ una sentencia válida en todos los cuerpos de característica cero, o sea
$$\mathrm{CUERPOS} \cup \{\neg\tau_p : p \text{ primo}\}) \vDash \varphi$$
Por compacidad, la derivación de φ utiliza sólo una cantidad finita de dichas fórmulas, o sea, para cierto $n \in \omega$
$$\mathrm{CUERPOS} \cup \{\neg\tau_p : p \text{ primo}, p \leq n\}) \vDash \varphi$$
Por tanto φ será válida en todos los cuerpos de característica mayor que *n*

4.7 Equivalencia elemental

[4-21] Definición

Sea A y B dos σ-estructuras. A y B se dicen *elementalmente equivalentes* si para toda sentencia α se verifica

$$\mathsf{A} \models \alpha \Leftrightarrow \mathsf{B} \models \alpha$$

Notación. $\mathsf{A} \equiv \mathsf{B}$

Observación

Basta pedir la mitad de la equivalencia: si suponemos

$$\mathsf{A} \models \alpha \Rightarrow \mathsf{B} \models \alpha$$

se obtiene ya la implicación contraria, pues

$$\mathsf{A} \not\models \alpha \Rightarrow \mathsf{A} \models \neg\alpha \Rightarrow \mathsf{B} \models \neg\alpha \Rightarrow \mathsf{B} \not\models \alpha$$

Claramente la relación de equivalencia elemental es una relación de equivalencia en la clase de estructuras sobre una signatura dada.

[4-22] Proposición

Son equivalentes
1. $\mathsf{A} \equiv \mathsf{B}$
2. $\mathrm{Th}(\mathsf{A}) = \mathrm{Th}(\mathsf{B})$

[4-23] Proposición

Son equivalentes
1. T es completa
2. Dos modelos de T son elementalmente equivalentes

En particular , si $\mathsf{A} \models \mathrm{Th}(\mathsf{B})$ entonces $\mathsf{A} \equiv \mathsf{B}$. Utilizando esta propiedad comprobamos por ejemplo que la teoría de cuerpos no es completa: la sentencia $1 + 1 = 0$ es verdadera en unos cuerpos pero no en otros.

Es obvio que si A y B son isomorfas también son elementalmente equivalentes. Es un corolario del siguiente teorema de isomorfía, algo más general e igualmente obvio (puede demostrarse por inducción estructural)

[4-24] Proposición

Sea h un isomorfismo entre las estructuras A y B. Para toda fórmula $\varphi(x_1, \ldots, x_n)$ y todo $a = (a_1, \ldots, a_n) \in A^{\omega}$ si $b = (h(a_1), \ldots, h(a_n)) \in B^{\omega}$ se tiene

$$A \vDash \varphi\,[a] \quad \Leftrightarrow \quad B \vDash \varphi\,[b]$$

El recíproco no es cierto : en general el isomorfismo es más fuerte que la equivalencia elemental. Por ejemplo, las estructras del orden de los racionales y los reales son elementalmente equivalentes pero no isomorfos, pues tienen distinta cardinalidad.
Sin embargo en el caso finito ambos conceptos coinciden. Basta considerar las fórmulas

$$\kappa_{=n} \equiv \exists x_1 \exists x_2 \ldots \exists x_n \forall x_0\; x_1 \neq x_2 \wedge \ldots \wedge x_{n-1} \neq x_n \wedge (x_0 = x_1 \vee \ldots \vee x_0 = x_n)$$

Obviamente $A \vDash \kappa_{=n}$ syss $|A| = n$, por lo que se tiene

[4-25] Proposición

$$A \equiv B \;\;\&\;\; |A| = n \;\Rightarrow\; |B| = n$$

[4-26] Proposición

I. Si A es infinita la clase $\{\mathsf{B} : \mathsf{A} \approx \mathsf{B}\}$ no es Δ-elemental
II. La clase $\{\mathsf{B} : \mathsf{A} \equiv \mathsf{B}\}$ es Δ-elemental

Demostración
I. Supongamos que $\{\mathsf{B} : \mathsf{A} \approx \mathsf{B}\} = \mathrm{Mod}(\Phi)$
Φ tienen un modelo infinito y por tanto tendrá modelos de cualquier cardinalidad infinita, y por tanto no isomorfos a A
II. $\{\mathsf{B} : \mathsf{A} \equiv \mathsf{B}\} = \mathrm{Mod}(\mathrm{Th}(\mathsf{A}))$

I. quiere decir que ninguna estructura infinita puede caracterizarse en primer orden salvo isomorfismos; para cada estructura infinita A existen modelos elementalmente equivalentes a A pero no isomorfos a A

4.8 Teorías indecidibles

El objetivo fundamental de este trabajo es estudiar el problema de decisión de teorias de primer orden. Este tipo de problemas fue planteado por primera vez en por Skolem en 1919 (cf. [54]) y estudiado fundamentalmente por Tarski y sus colaboradores.
Una teoría T es decidible si hay un procedimiento de decisión para T, esto es un algoritmo que tomando como entrada un sentencia cualquiera φ del lenguaje de T, determine en un número finito de pasos si $\varphi \in T$ o si $\varphi \notin T$. Puesto que la formalización de este concepto intuitivo corresponde al concepto formal de conjunto recursivo, daremos la siguiente definición. Recordemos que suponemos establecida una correspondencia efectiva entre las sentencias del lenguaje y los números naturales. En esta correspondencia a un conjunto de sentencias le corresponde un determinado conjunto de naturales. En particular a una teoría T le corresponde de forma biyectiva y efectiva el conjunto de naturales $T^{\#}$.

[4-27] Definición

Sea T una teoría y $T^{\#}$ el conjunto de códigos de sus fórmulas.
T es *decidible* si $T^{\#}$ es recursivo
T es *indecidible* si $T^{\#}$ no es recursivo

Nota

La palabra “indecidible” se utiliza a veces en lógica, aplicada a una fórmula concreta, para indicar que dicha fórmula no pertenece a un determinado sistema formal y que su negación tampoco pertenece al mismo. Esta noción está pues relacionada con la incompletitud del sistema. Un caso de sentencia “indecidible” en este sentido es la sentencia de Gödel del teorema de incompletitud de la aritmética. Nuestro uso de “indecidible” se aplica a un conjunto de fórmulas considerado como un todo. Es por tanto un enunciado acerca de todo el sistema formal. Obsérvese que la noción de “indecidibilidad de una teoría” es una noción de teoría de la recursión, pues hace referencia al concepto de algoritmo ; en cambio la noción de “fórmula indecidible en una teoría” en el sentido señalado en esta nota es una noción de lógica que no necesita en principio de la teoría de la recursión.

Observación. El cardinal del conjunto de teorías

La existencia de teorías indecidibles puede mostrarse fácilmente por un argumento de cardinalidad.
El conjunto de algoritmos es un conjunto numerable pues puede verse como un subconjunto del conjunto de sucesiones finitas de un alfabeto finito (no es problema considerar el alfabeto incluso numerable). El conjunto de sucesiones finitas de elementos

de un conjunto numerable es numerable, pues es la unión numerable de los conjuntos numerables formados por las sucesiones de un elemento, de dos elementos, etc. Por lo tanto el conjunto de teorías decidibles es numerable, ya que a cada una le corresponde un algoritmo de decisión.

Veamos ahora que el conjunto de teorías no es numerable ; en consecuencia deberá haber teorías no decidibles.
Consideraremos un lenguaje sin símbolos específicos (salvo el de igualdad)
En este lenguaje podemos expresar que un modelo tiene n elementos mediante una sentencia $\kappa_{=n}$. Por ejemplo, $\kappa_{=2}$ es

$$\exists x\, \exists y\, (x \neq y) \wedge \neg \exists x\, \exists y\, \exists z\, (x \neq y \wedge y \neq z \wedge z \neq x)$$

Entonces dos estructuras son isomorfas syss tienen la misma cardinalidad. (Nótese que si dos estructuras tienen distinta cardinalidad hay una fórmula que se verifica en una pero no en otra) Se verifica, pues, en este caso

$$|A| = |B| \;\Leftrightarrow\; A \approx B \;\Leftrightarrow\; A \equiv B$$

es decir la verdad o falsedad de una fórmula en una estructura depende únicamente de la cardinalidad de la misma.
Llamemos *espectro de una fórmula* α (de un conjunto de fórmulas Φ) al conjunto $sp(\alpha)$ ($sp(\Phi)$) de cardinalidades finitas de los modelos de α (de Φ).
Identificando el cardinal n con el conjunto $\{0, 1, ..., n - 1\}$ se tiene

$$n \in sp(\alpha) \;\Leftrightarrow\; n \vDash \alpha$$

y por tanto

$$sp(\Phi) = \bigcap_{\alpha \in \Phi} sp(\alpha)$$

pues

$$n \in sp(\Phi) \;\Leftrightarrow\; n \vDash \Phi \;\Leftrightarrow\; \forall \alpha \in \Phi \;\; n \vDash \alpha \;\Leftrightarrow\; \forall \alpha \in \Phi \;\; n \in sp(\alpha) \;\Leftrightarrow\; n \in \bigcap_{\alpha \in \Phi} sp(\alpha)$$

Es inmediato observar que

$$sp(\neg \kappa_{=n}) = \omega - \{0, n\}$$

Dado un conjunto $A \subset \omega$ (que podremos suponer, sin pérdida de generalidad que incluye el 0) formemos el conjunto de fórmulas $\Phi_A = \{\neg \kappa_n : n \in A\}$ y la teoría
$T_A = \{\alpha \in SENT_\varnothing : \Phi_A \vDash \alpha\}$
Entonces se verifica

$$sp(\Phi_A) = sp(T_A) = \overline{A}$$

pues

$$sp(\Phi_A) = \bigcap_{n \in A} sp(\neg k_{=n}) = \bigcap_{n \in A} (\omega - \{0,\ n\}) = \overline{\bigcup_{n \in A} \{0,\ n\}} = \overline{A \cup \{0\}} = \overline{A}$$

De forma que

$$A \neq B \Rightarrow \overline{A} \neq \overline{B} \Rightarrow sp(T_A) \neq sp(T_B) \Rightarrow T_A \neq T_B$$

y así a cada subconjunto A de ω le corresponde una teoría T_A (de forma inyectiva). Puesto que el número de subconjuntos de ω no es numerable tenemos así una cantidad no numerable de teorías.

Observación

Si el problema de decisión general de la lógica de primer orden tuviera solución y T fuera una teoría finitamente axiomatizable con axiomas $\varepsilon_1, \ldots, \varepsilon_n$ se tendría para toda sentencia φ

$$T \vdash \varphi \Leftrightarrow \{\varepsilon_1, \ldots, \varepsilon_n\} \vdash \varphi \Leftrightarrow \vdash (\varepsilon_1 \wedge \ldots \wedge \varepsilon_n) \rightarrow \varphi$$

De ahí que el problema de decisión para T se reduce al problema de decisión de la lógica de primer orden. Esto no ofrece mucha ayuda pues la lógica de primer orden es indecidible. Sin embargo el argumento muestra la importancia del carácter finitamente axiomatizable de una teoría para efectuar la reducción. De hecho éste es el argumento para demostrar la indecidibilidad de la lógica de primer orden a partir de la indecidibilidad de un fragmento de la aritmética finitamente axiomatizable (Teorema de Church)

Que una teoría sea indecidible no quiere decir que lo sean sus extensiones o sus subteorías: La teoría de grupos es indecidible , como veremos en § 6.5, pero la teoría de grupos conmutativos que es una extensión consistente finita de la teoría de grupos, es decidible.(Ver también la observación tras el teorema [4-34])
Más aún. Consideremos una teoría arbitraria T. Si $\mathsf{A} \in$ Mod(T) entonces $T \subset Th(\mathsf{A})$. En el caso particular en que $\mathsf{A} \in$ Modfin(T) se tiene que $Th(\mathsf{A})$ es una extensión de T (en el mismo lenguaje) y, al ser A finito, $Th(\mathsf{A})$ es una teoría decidible. Por tanto, toda teoría con modelos finitos tiene extensiones decidibles (aunque la teoría de partida sea indecidible).
Son por tanto útiles los siguientes conceptos en relación a subteorías y extensiones.

[4-28] Definición

T es *esencialmente indecidible* si es indecidible y toda extensión consistente de T (en el mismo lenguaje) es indecidible
T es *hereditariamente indecidible* si es indecidible y toda subteoría de T (con el mismo lenguaje) es indecidible
T es *fuertemente indecidible* si es indecidible y toda teoría compatible con T es indecidible

La observación anterior a la definición muestra que una teoría con modelos finitos *no* puede ser esencialmente indecidible.

[4-29] Proposición

T decidible $\Rightarrow$ T axiomatizable
Demostración
Si T es decidible entonces el conjunto de teoremas de T es recursivo y vale como sistema de axiomas de T.

Una teoría axiomatizable puede no ser decidible. Veremos muchos ejemplos. El más sencillo es la lógica de primer orden que es finitamente axiomatizable.

[4-30] Proposición

Si T es axiomatizable y completa es decidible
Demostración
Si T es axiomatizable hemos visto que es recursivamente enumerable, es decir existe un algoritmo que da respuesta afirmativa en el caso en que una sentencia pertenezca a T. Apliquemos el algoritmo alternativa y simultáneamente a φ y a $\neg\varphi$. Puesto que la teoría es completa alguna de las dos fórmulas está en T ; el algoritmo lo detectará en su momento y por tanto dará siempre la respuesta adecuada si/no a la cuestión $\varphi \in T$. La teoría es por tanto decidible.

Por lo tanto un método para probar que una teoría axiomatizable es decidible es ver que es completa

Observación

La aritmética de primer orden, Th(N), por ser la teoría de una estructura es una teoría completa. Al demostrar que no es decidible se deduce como corolario que no puede ser axiomatizable.

[4-31] Proposición

Sea T una teoría completa. Son equivalentes
1. T es indecidible
2. T es esencialmente indecidible
3. T no es axiomatizable

Demostración
$1 \Leftrightarrow 2$ Si T es completa no tiene ninguna extensión estricta consistente
$1 \Leftrightarrow 3$ Son las dos proposiciones anteriores [4-29] y [4-30]

[4-32] Proposición

Sea T_2 extensión consistente de T_1
T_1 esencialmente indecidible $\Rightarrow$ T_2 esencialmente indecidible

Recordemos que si T_1 y T_2 son dos teorías en el mismo lenguaje se dice que T_2 es una extensión finita de T_1 si hay un conjunto finito de sentencias $\Phi \subset T_2$ tal que toda sentencia $\varphi \in T_2$ es derivable de $T_1 \cup \Phi$

[4-33] Proposición

Si T_2 es una extensión finita de T_1 y T_2 es indecidible entonces T_1 es indecidible
Demostración
Sea T_2 una extensión finita de T_1 y $\varphi_1, \ldots, \varphi_n \in T_2$ fórmulas tales que

$$\alpha \in T_2 \quad \text{syss} \quad T_1 \cup \{\varphi_1, \ldots, \varphi_n\} \vdash \alpha$$

Por el teorema de deducción

$$\alpha \in T_2 \quad \text{syss} \quad T_1 \vdash \varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \alpha$$

Si hubiera un procedimiento de decisión para T_1 la anterior reducción proporcionaría un procedimiento de decisión para T_2

Como aplicación de esta proposición podremos deducir, por ejemplo, la indecidibilidad de la teoría de semigrupos a partir de la indecidibilidad de la teoría de grupos, que es una extensión finita de aquella.(Ver § 6.5)

Nota

Este es el argumento fundamental para demostrar el teorema de Church de la indecidibilidad del cálculo de predicados basándose en la indecidibilidad de la aritmética de Robinson. Obsérvese la importancia que tiene en el argumento el hecho de ser la aritmética de Robinson finitamente axiomatizable, lo que convierte a dicha teoría en una extensión finita del cálculo de predicados de primer orden en el lenguaje de la aritmética.

[4-34] Proposición

Si T es esencialmente indecidible y finitamente axiomatizable entonces T es fuertemente indecidible
Demostración
Sea T' una teoría compatible con T. Sea T'' = T + T'. T'' es indecidible por ser extensión simple de T que es esencialmente indecidible. Pero T'' es una extensión finita de T' por ser T finitamente axiomatizable. Por tanto T' es indecidible.

Observación

En las proposiciones anteriores no se puede cambiar la hipótesis de ser "esencialmente indecidible" por la de ser "indecidible".
Consideremos $\sigma = \{P\}$, siendo P un predicado binario, y la sentencia

$$\kappa_{=1} \equiv \forall x \, \forall y \; x = y$$

Esta sentencia expresa que el universo tiene un único elemento.
Sean $T_1 = Con_\sigma(\varnothing)$ y $T_2 = Con_\sigma(\{\kappa_{=1}\})$. Claramente T_2 es una extensión consistente de T_1 y por tanto ambas teorías son compatibles. La teoría T_1 es finitamente axiomatizable. Veremos en § 9.1 que T_1, la teoría de una relación binaria, es indecidible. Sin embargo la teoría T_2 es claramente decidible.

Nota

El hecho de ser la aritmética de Robinson finitamente axiomatizable es lo que permite concluir, al demostrar que **Q** es esencialmente indecidible, que es una teoría fuertemente indecidible. No podríamos dar este paso si hubiéramos considerado otra formalización de la aritmética no finitamente axiomatizable, por ejemplo la aritmética recursiva primitiva.

Estructuras indecidibles y clases indecidibles de estructuras

Un caso interesante de teorías son las teorías de una estructura o de una clase de estructuras.

[4-35] Definición

Sea A una estructura y K una clase de estructuras.
Se dice que A es *indecidible* si Th(A) es indecidible
Se dice que A es *fuertemente indecidible* si toda teoría que tiene A como modelo es indecidible
Se dice que K es *indecidible* si Th(K) es indecidible
Se dice que K es *hereditariamente indecidible* si Th(K) es hereditariamente indecidible

Obsérvese que no es lo mismo decir que una clase K es indecidible y decir que todas las estructuras de la clase son indecidibles.

[4-36]Proposición

Son equivalentes :

1. A es fuertemente indecidible
2. Th(A) es hereditariamente indecidible
3. Th(A) es fuertemente indecidible

***Demostración*.**
[1⇒2] Supongamos que A es fuertemente indecidible . Entonces
$T \subset Th(\mathsf{A}) \Rightarrow \mathsf{A} \models T \Rightarrow T$ indecidible
[2⇒1] Supongamos Th(A) hereditariamente indecidible. Entonces
$\mathsf{A} \models T \Rightarrow T \subset Th(\mathsf{A}) \Rightarrow T$ indecidible
[2⇔3] Es consecuencia de ser la teoría Th(A) completa (ver [4-19])

[4-37] Proposición

Sea T una teoría consistente. Son equivalentes

1. T es esencialmente indecidible
2. Todo modelo de T es indecidible

Demostración

[1⇒2] $\mathfrak{A} \models T \Rightarrow T \subset Th(\mathfrak{A}) \Rightarrow Th(\mathfrak{A})$ indecidible $\Rightarrow \mathfrak{A}$ indecidible

[2⇒1] Supongamos que T' es una extensión simple consistente de T decidible. Existiría una extensión simple T'' completa consistente y decidible (Técnica de Lindenbaum). Un modelo de T'' sería un modelo de T decidible.

[4-38] Proposición

Sea T una teoría consistente. Son equivalentes

1. T es fuertemente indecidible
2. Todo modelo de T es fuertemente indecidible

Demostración

[1⇒2] Sea T fuertemente indecidible y $\mathfrak{A} \models T$. Entonces

$\mathfrak{A} \models T' \Rightarrow$ T y T' son compatibles ⇒ T' es indecidible

[2⇒1] Supongamos que todo modelo de T es fuertemente indecidible. Sea T' compatible con T. Entonces existe $\mathfrak{A}$ tal que $\mathfrak{A} \models T$ y $\mathfrak{A} \models T'$. Por ser $\mathfrak{A} \models T$ $\mathfrak{A}$ es fuertemente indecidible; y al ser $\mathfrak{A} \models T'$ es T' indecidible .

[4-39] Proposición

Si T tiene un modelo fuertemente indecidible entonces T es hereditariamente indecidible

Demostración

Si T' es subteoría de T y $\mathfrak{A}$ es un modelo fuertemente indecidible de T al ser modelo de T' debe ser T' indecidible

Ejemplo

Demostraremos que la estructura de los enteros es fuertemente indecidible. Si consideramos la teoría de anillos tendrá un modelo fuertemente indecidible: los enteros. Por tanto es hereditariamente indecidible. Pero podemos ver que no es esencialmente indecidible, pues tiene un modelo decidible: el cuerpo de los números reales. Otra razón: tiene extensiones decidibles, a saber, la teoría de cuerpos algebraicamente cerrados. Otra más : cualquier anillo finito es modelo de la teoría.

[4-40] Proposición

Sea $\mathfrak{K}$ una clase de σ-estructuras. Son equivalentes

1. K es hereditariamente indecidible
2. Si K' es otra clase de σ-estructuras tal que $\mathsf{K} \subset \mathsf{K}$' entonces K' es indecidible

Demostración

[1$\Rightarrow$2] $\mathsf{K} \subset \mathsf{K}' \Rightarrow \mathrm{Th}(\mathsf{K}') \subset \mathrm{Th}(\mathsf{K}) \Rightarrow \mathrm{Th}(\mathsf{K}')$ indecidible

[2$\Rightarrow$1] Sea $T \subset \mathrm{Th}(\mathsf{K})$. Entonces $\mathsf{K} \subset \mathrm{ModTh}(\mathsf{K}) \subset \mathrm{Mod}(T)$; luego Mod(T) es indecidible. Por tanto T = ThMod(T) es indecidible

Un teorema sobre las extensiones no esenciales

La teoría T_2 es una extensión de la teoría T_1 si $T_1 \subset T_2$. Pensando en las signaturas de los lenguajes de las teorías, esto puede ocurrir siendo iguales $\mathsf{L}(T_1) = \mathsf{L}(T_2)$ o siendo $\mathsf{L}(T_1) \subset \mathsf{L}(T_2)$ pero distintos.

Recordemos que T_2 es una extensión no esencial de T_1 si existe una cantidad finita de símbolos de constante $c_1, \ldots, c_p$ tales que $\sigma_{L(T_2)} = \sigma_{L(T_1)} \cup \{c_1, \ldots, c_p\}$ y T_2 es el cierre por derivación de T_1 en $\mathsf{L}(T_2)$

Ejemplo

Sea $\sigma_G = \{e, \circ\}$ la signatura del lenguaje de la teoría de grupos, y $\sigma' = \{e, \circ, a\}$ la signatura con un nuevo símbolo de constante a.

Se tiene GRUPOS $\vdash \forall x\, \forall y\, \forall z\ (x + (y + z) = (x + y) + z)$. En σ' podremos considerar la teoría generada por GRUPOS e.e. $\overline{\mathrm{GR}} = \{\alpha \in \mathsf{L}_{\sigma'} : \mathrm{GRUPOS} \vdash \alpha\}$. Se verifica que $\overline{\mathrm{GR}} \vdash \forall y \forall z\ (a + (y + z) = (a + y) + z)$. Pero esta fórmula *no* es del lenguaje de σ_G.

Sin nuevos axiomas podemos derivar nuevas fórmulas utilizando las nuevas constantes del lenguaje

Por facilidad en la escritura, consideraremos, sin pérdida de generalidad, el caso de añadir un nuevo símbolo de constante, e.e., $\sigma' = \sigma \cup \{c\}$. Nótese que cada σ-estructura A determina diversas σ'-estructuras al elegir el elemento del universo de A que designa la nueva constante. Designaremos por (A, m) la estructura obtenida al hacer que la constante c designe el elemento m del universo A de A respetando las demás designaciones de A.

[4-41] Teorema

Sea T_2 extensión no esencial de T_1. Entonces :

i. T_2 indecidible $\Rightarrow T_1$ indecidible

ii. T_2 fuertemente indecidible $\Rightarrow$ T_1 fuertemente indecidible
iii. T_2 esencialmente indecidible $\Rightarrow$ T_1 esencialmente indecidible
iv. T_2 hereditariamente indecidible $\Rightarrow$ T_1 hereditariamente indecidible
Demostración.
i. Sea $L(T_2) = L(T_1) \cup \{c\}$. Para cada fórmula $\varphi(c) \in L(T_2)$ sea $\varphi^* \equiv \forall x\, \varphi(x) \in L(T_1)$ la fórmula obtenida al cambiar en φ cada aparición de la constante c por la variable x (suponiendo que x sea la primera variable que no aparece en φ) y cuantificando universalmente. Veamos que

$$\varphi \in T_2 \Leftrightarrow \varphi^* \in T_1$$

y en consecuencia un procedimiento de decisión para T_1 proporcionaría un procedimiento de decisión para T_2 (nótese que la transformación es efectiva).
En efecto :

[$\Leftarrow$] $\varphi^* \in T_1$ $\Rightarrow \forall x\, \varphi(x) \in T_2$ por ser T_2 extensión de T_1
$\Rightarrow \varphi(c) \in T_2$ por leyes de la lógica, particularización

[$\Rightarrow$] $\varphi^* \notin T_1$ $\Rightarrow$ existe $A \models T_1$ y $A \nvDash \forall x \varphi(x)$
$\Rightarrow$ existe $A \models T_1$ y un elemento $m \in A$ tal que $A \nvDash \varphi$ [m]
$\Rightarrow (A, m) \models T_2$ y $(A, m) \nvDash \varphi$
$\Rightarrow \varphi \notin T_1$

Un procedimiento de decisión para T_1 proporcionaría un procedimiento de decisión para T_2
ii. Sea T_2 fuertemente indecidible, Probaremos que toda teoría compatible con T_1 es indecidible. Sea T_1' una teoría en el mismo lenguaje que T_1 compatible con T_1 y sea T_2' = $\{\alpha \in L(T_2): T_1' \models \alpha\}$. Entonces T_2' es una teoría compatible con T_2. En efecto, Si A es un modelo de $T_1 \cup T_1$' es inmediato que (A, m) es un modelo de $T_2 \cup T_2$', con lo que T_2 y T_2' son compatibles
Por un razonamiento análogo al del apartado i. se tiene

$$\varphi \in T_2' \Leftrightarrow \varphi^* \in T_1'$$

de donde se deduce la indecidibilidad de T_2' a partir de la de T_1'.
iii. y iv. se prueban de manera análoga.

4.9 Teorías inseparables

Una generalización del concepto de indecidibilidad que será útil, especialmente en el caso de teorías con modelos finitos, utiliza la noción de inseparabilidad.
Dada una teoría T consideraremos los conjuntos de naturales (suponiendo una codificación $\{\alpha_n: n \in \omega\}$ de las sentencias del lenguaje de T)

$$D_T = \{n \in \omega : \alpha_n \in T\}$$
$$R_T = \{n \in \omega : \neg\alpha_n \in T\}$$

$F_T = \{n \in \omega : \text{existe } A \vDash T, A \text{ finito tal que } A \vDash \neg\alpha_n\}$

Estos conjuntos son, respectivamente, los códigos de las fórmulas demostrables en la teoría, los códigos de las fórmulas refutables en la teoría y los códigos de las fórmulas finitamente refutables de la teoría.

Si T es una teoría consistente $D_T \cap R_T = \varnothing$ y $D_T \cap F_T = \varnothing$.

Obviamente si la teoría T no tiene modelos finitos $F_T = \varnothing$.

Si suponemos una codificación de las fórmulas mediante una biyección con los números naturales, F_T es el complementario del conjunto de los códigos de las fórmulas de T_{fin}.

Obsérvese que

i. $T_1 \subset T_2 \Rightarrow R_{T_1} \subset R_{T_2}$

ii. $T_1 \subset T_2 \Rightarrow F_{T_2} \subset F_{T_1}$

[4-42] Definición

T es *inseparable* si D_T y R_T son efectivamente inseparables

T es *finitamente inseparable* si D_T y F_T son efectivamente inseparables

[4-43] Definición

Sea K una clase de estructuras . Se dice que K es una *clase inseparable* si Th(K) es inseparable. Se dice que K es una *clase finitamente inseparable* si Th(K) es finitamente inseparable.

[4-44] Proposición

Si T_1 es una teoría inseparable y T_2 es una extensión simple de T_1 entonces T_2 es inseparable

Demostración

En estas hipótesis, $D_{T_1} \subset D_{T_2}$ y $R_{T_1} \subset R_{T_2}$. El resultado es consecuencia de [3-10]

En virtud de la relación entre recursividad e inseparabilidad, [3-3]

[4-45] Proposición

a) Si una teoría T es inseparable entonces es esencialmente indecidible

b) Si una teoría T es finitamente inseparable, tanto la teoría T como la teoría finita T_{fin} = Th(Modfin(T)) son indecidibles

Demostración

a) Consecuencia de la proposición anterior

b) Basta observar que

$T_{fin}^{\#}$ = Th(Modfin(T))$^{\#}$ es el complementario de F_T

(Si no suponemos la codificación biyectiva hay que observar que $F_T^{\#} = \overline{T_{fin}^{\#}} \cap SENT_s$)

Se puede obtener un teorema análogo al [4-33] para teorías finitamente inseparables

[4-46] Teorema

Sean T_1 y T_2 dos teorías consistentes. y supongamos que T_2 es una extensión finita de T_1. Si T_2 es finitamente inseparable entonces T_1 es finitamente inseparable.

Demostración

Sea T_2 una extensión finita de T_1 y $\varphi_1, \ldots, \varphi_n \in T_2$ fórmulas tales que

$$\alpha \in T_2 \text{ syss } T_1 \cup \{\varphi_1, \ldots, \varphi_n\} \vdash \alpha$$

Entonces

$$\alpha \in T_2 \Rightarrow \varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \alpha \in T_1$$

$$\alpha \in FR_{T_2} \Rightarrow \exists B \vDash T_2,\ B \text{ finita},\ B \vDash \neg\alpha$$

$$\Rightarrow \exists\ B \vDash T_1,\ B \text{ finita},\ B \vDash \varphi_1 \wedge \ldots \wedge \varphi_n,\ B \vDash \neg\alpha$$

$$\Rightarrow \exists\ B \vDash T_1,\ B \text{ finita},\ B \nvDash \varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \alpha$$

$$\Rightarrow \varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \alpha \in FR_{T_1}$$

El teorema [3-11] permite asegurar que T_1 es finitamente inseparable

Aplicaremos este resultado en el caso de considerar una clase K_1 y una subclase formada por los modelos de una sentencia (posiblemente la conjunción de un conjunto finito de sentencias) $\mathsf{K}_2 = \{A \in \mathsf{K}_1 : A \vDash \beta\}$. En tal caso $Th(\mathsf{K}_2)$ es una extensión finita de K_1. En términos de clases podemos enunciar el resultado :

[4-47] Teorema

Sea K_1 y K_2 dos clases tales que $Th(\mathsf{K}_2)$ es una extensión finita de $Th(\mathsf{K}_1)$. Si K_2 es una clase finitamente inseparable entonces K_1 es también una clase finitamente inseparable

Si sabemos que cierta teoría axiomática T_2 es finitamente inseparable este teorema permite asegurar directamente la inseparabilidad finita de otra teoría T_1 que obtengamos eliminando algún axioma de la primera. Por ejemplo, a partir de la inseparabilidad finita de la teoría de grupos obtenemos inmediatamente la inseparabilidad finita de la teoría de semigrupos. De la inseparabilidad finita de la teoría de retículos obtenemos directamente la inseparabilidad finita de la teoría de semirretículos o la teoría del orden parcial.

Nota

Para que una teoría T sea finitamente inseparable debe tener algún modelo finito $\mathfrak{A} \models T$. La teoría de dicha estructura Th($\mathfrak{A}$) será claramente decidible. Y es una extensión de T. Luego T no puede ser esencialmente indecidible. Por la proposición [4-45], T no puede ser inseparable. Una teoría no puede, pues, ser inseparable y finitamente inseparable. Ejemplos de teorías inseparables no finitamente inseparables se tienen en muchas teorías aritméticas sin modelos finitos como la aritmética de Robinson **Q**, o la aritmética completa Th($\mathfrak{N}$). Hay ejemplos menos triviales en [22]

5. INTERPRETACIONES

5.1 Representación de estructuras y traducción de lenguajes

Es habitual en matemáticas interpretar una estructura como subestructura de otra. Un ejemplo típico lo constituye la interpretación del plano proyectivo en el espacio afín tridimensional : los puntos del plano proyectivo se interpretan como rectas que pasan por el origen en el espacio afín tridimensional, las rectas del plano proyectivo se interpretan como planos que pasan por el origen del espacio, la pertenencia de un punto del plano proyectivo a una recta proyectiva se interpreta como la inclusión de una recta del plano afin en el correspondiente plano del espacio afín,... Esto quiere decir que la estructura del espacio afín tridimensional es suficiente para definir el plano proyectivo.
Un ejemplo más sencillo : los números naturales pueden definirse como una cierta subestructura de los números enteros.
Una interpretación o definición de una estructura A en otra estructura B debe determinar los elementos de B que representen los elementos de A. Por ejemplo, en el caso de la representación de los naturales en los enteros, el subconjunto de los enteros que representa al conjunto de los naturales es el conjunto de los enteros positivos. En el caso del plano proyectivo, los puntos del plano proyectivo se representan por las rectas del espacio afín tridimensional que pasan por el origen.
La interpretación debe determinar una traducción de las fórmulas en el lenguaje de la estructura A en fórmulas de la estructura B. Por ejemplo, si la estructura A es la estructura del orden en los naturales $(\omega, \leq^{\omega})$, y la estructura $\mathsf{B} = (\omega, +^{\omega}, \cdot^{\omega})$ tiene un lenguaje algebraico sobre los naturales, la fórmula en el lenguaje del orden $x \leq y$ se puede traducir por la fórmula en el lenguaje de la suma $\exists z\ z + x = y$.
La traducción de una fórmula funcional de dos argumentos, por ejemplo

$$z = \mathrm{mcd}(x,y)$$

que expresa que z es el máximo común divisor de x e y , se realiza con una fórmula con tres variables

$$\alpha_{mcd}(x,y,z) \equiv \forall t\,(\exists u\ x = t \cdot u \wedge \exists v\ \ y = t \cdot v \leftrightarrow \exists w\ z = t \cdot w)$$

que afirma que, para todo t, se verifica

$$t \mid x\ \ \&\ t \mid y\ \Leftrightarrow t \mid z$$

Nótese que la estructura de los naturales N verifica

$$\mathsf{N} \vDash \forall x \forall y \exists! z\ \alpha_{mcd}(x,y,z)$$

lo que asegura el carácter funcional del mcd.
Se estudian a continuación los fundamentos lógico-formales de estas interpretaciones de unas estructuras (o teorías) en otras. La idea de interpretar unas teorías en otras fue utilizada por Tarski [57] como técnica básica para realizar demostraciones de indecidibilidad. Aquí seguiremos esa idea pero utilizaremos una definición de interpretación algo más cómoda que la utilizada por Tarski y que está basada en consideraciones de Feferman [15].

5.2 Traducción de lenguajes

[5-1] Definición

Sean L_1 y L_2 dos lenguajes. Sea $\sigma_1 = (CONS_1, FUNC_1, PRED_1, \mu)$ la signatura de L_1 .
Una *traducción* de L_1 en L_2 es un par $\Gamma = (\gamma, g)$ donde γ es una fórmula de L_1 con una variable libre y g es una aplicación $g : \sigma_1 \rightarrow FORM_{L_2}$ tal que

1. Si $c \in CONST_1$ entonces $g(c) = \alpha_c$ es una formula de L_2 con una variable libre
2. Si $f \in FUNC_1^{(n)}$ es un símbolo de función de n argumentos $g(f) = \alpha_f$ es una fórmula de L_2 con n + 1 variables libres
3. Si $P \in PRED_1^{(n)}$ es un símbolo de predicado n-ario $g(P) = \alpha_P$ es una fórmula de L_2 con n variables libres

Para que la fórmula α_f represente adecuadamente a la función f tenemos que imponer que se conserve el carácter funcional de la relación que designa. De igual manera, la fórmula α_c debe ser satisfecha por un único individuo del dominio para ser una representación adecuada de una constante. Interesa pues realizar las consideraciones siguientes. Dada la traducción $\Gamma = (\gamma, g)$ de L_1 en L_2 sea Φ_Γ el conjunto de fórmulas de L_2 que consta de

$[\blacklozenge 1 \Phi_\Gamma]$ La fórmula $\exists x\, \gamma(x)$.

$[\blacklozenge 2\, \Phi_\Gamma]$ Para cada símbolo de función $f \in FUNC_1^{(n)}$ la fórmula

$$\varphi_f \equiv \forall x_1 ... \forall x_n\, (\gamma(x_1) \wedge ... \wedge \gamma(x_n) \rightarrow \exists z\, \forall w\, ((\gamma(w) \wedge \alpha_f(x_1, ... , x_n, w)) \leftrightarrow w = z)$$
$$\equiv \forall x_1 ... \forall x_n\, (\gamma(x_1) \wedge ... \wedge \gamma(x_n) \rightarrow \exists! z\, (\gamma(z) \wedge \alpha_f(x_1, ... , x_n, z)))$$

$[\blacklozenge 3\, \Phi_\Gamma]$ Para cada símbolo de constante $c \in CONS_1$ la fórmula

$$\varphi_c \equiv \exists x\, \forall w\, ((\gamma(w) \wedge \alpha_c(w)) \leftrightarrow w = x)$$
$$\equiv \exists! x\, (\gamma(x) \wedge \alpha_c(x))$$

En las fórmulas anteriores se supone que la variable libre de la fórmula γ es la que aparece en el cuantificador en $[\blacklozenge 1 \Phi_\Gamma]$, esto es, la variable x, que las variables libres de α_f son $x_1, ..., x_n, z$, que son las que aparecen en los cuantificadores de $[\blacklozenge 2\, \Phi_\Gamma]$ y que la variable libre de α_c es x, que es la variable que aparece en el cuantificador de la fórmula $[\blacklozenge 3\, \Phi_\Gamma]$)
La fórmula $[\blacklozenge 1 \Phi_\Gamma]$ expresa que el universo de la interpretación no será vacío. La fórmula $[\blacklozenge 2\, \Phi_\Gamma]$ permite asegurar que el predicado designado por la fórmula α_f es de

hecho el grafo de una función. La fórmula [♦3 Φ_Γ] asegura que hay un único elemento del dominio que verifica la condición expresada por la fórmula α_c, con lo que α_c es una adecuada representación de una constante. Por lo tanto, la condición [♦1Φ_Γ] es consecuencia de [♦3 Φ_Γ] . Denominaremos a este conjunto de fórmulas las *condiciones de adecuación* de la interpretación. Será importante notar que, si el lenguaje es finito, como hemos supuesto, el conjunto Φ_Γ consta de un conjunto finito de fórmulas, y por tanto las condiciones de adecuación pueden expresarse por una única fórmula, a saber, la conjunción de las fórmulas de Φ_Γ.
Obsérvese también que si el lenguaje L_1 tiene símbolos de función o de constante el lenguaje L_2 debe ser un lenguaje con igualdad para expresar las condiciones. Pero si L_1 es un lenguaje sin símbolos de función o de constante la única condición es que el universo no sea vacío.

Traducción de fórmulas

Sea Γ una traducción del lenguaje L_1 en el lenguaje L_2. Γ determina de forma natural una transformación de las fórmulas del lenguaje L_1 en fórmulas del lenguaje L_2 . Denotaremos esta transformación también por Γ :

$$\Gamma : \mathrm{FORM}_1 \rightarrow \mathrm{FORM}_2$$
$$\alpha \rightarrow \alpha^\Gamma$$

Definiremos la transformación por inducción estructural. Para que la transformación sea efectiva consideraremos v_1, v_2, v_3, ... una enumeración de las variables que no aparecen en la fórmula. Cuando en el proceso de construcción tomemos una nueva variable nos referiremos a la primera variable de la lista que no aparece en los términos o fórmulas considerados. Los casos a considerar son :

1. Fórmulas sin símbolos de la signatura :
   $(x_i = x_j)^\Gamma \equiv x_i = x_j$

2. Fórmulas con un único símbolo
   $(Px_{i_1}... x_{i_n})^\Gamma \equiv \alpha_P(x_{i_1}, ... , x_{i_n})$
   $(x_i = c)^\Gamma \equiv \alpha_c(x_i)$
   $(c = x_i)^\Gamma \equiv \alpha_c(x_i)$
   $(x_{i_0} = fx_{i_1}...x_{i_n})^\Gamma \equiv \alpha_f(x_{i_0}, x_{i_1}, ... , x_{i_n})$
   $(fx_{i_1}...x_{i_n} = x_{i_0})^\Gamma \equiv \alpha_f(x_{i_0} x_{i_1}, ... , x_{i_n})$

3. Fórmulas atómicas con más de un símbolo
   Se definirá por inducción estructural. Consideremos en primer lugar el caso de una fórmula $Pt_1...t_n$ y supongamos definida la transformación para fórmulas de menor tamaño. Sean w_1, ... ,w_n nuevas variables ; entonces
   $(Pt_1...t_n)^\Gamma \equiv \exists w_1 \exists w_2 ... \exists w_n ((w_1 = t_1)^\Gamma \wedge ... \wedge (w_n = t_n)^\Gamma \wedge \alpha_P(w_1, ... ,w_n))$

De forma análoga para fórmulas funcionales
$(t_0 = ft_1...t_n)^\Gamma \equiv \exists w_0 \exists w_1 ... \exists w_n ((w_0 = t_0)^\Gamma \wedge (w_1 = t_1)^\Gamma \wedge ... \wedge (w_n = t_n)^\Gamma \wedge \alpha_f(w_0, w_1,...,w_n))$
y para igualdades

$(t_1 = t_2)^\Gamma \equiv \exists w_1((w_1 = t_1)^\Gamma \wedge (w_1 = t_2)^\Gamma)$

4. Fórmulas moleculares

$(\neg\alpha)^\Gamma \equiv \neg \alpha^\Gamma$

$(\alpha \rightarrow \beta)^\Gamma \equiv \alpha^\Gamma \rightarrow \beta^\Gamma$

$(\exists x\, \alpha)^\Gamma \equiv \exists w (\gamma(w) \wedge \alpha(w)^\Gamma)$ siendo w una nueva variable que no aparece en γ ni en α^Γ y $\alpha(w)$ es el resultado de cambiar cada aparición de x por w (La razón de introducir la nueva variable w es que la variable x puede aparecer en γ)

Obsérvese la relativización del cuantificador al universo de la interpretación
Con esto se tiene

$(\alpha \wedge \beta)^\Gamma = \alpha^\Gamma \wedge \beta^\Gamma$

$(\alpha \vee \beta)^\Gamma \equiv \alpha^\Gamma \vee \beta^\Gamma$

$(\forall x\, \alpha)^\Gamma \equiv \forall w\, (\gamma(w) \rightarrow \alpha(w)^\Gamma)$

Es fundamental observar que, con las consideraciones hechas previamente, la transformación así descrita es una transformación efectiva (siempre que apliquemos de forma ordenada, por ejemplo, de izquierda a derecha, los pasos recursivos de la transformación)

Ejemplo

Supongamos una signatura σ = {c, f, P) en que c es un símbolo de constante, f una función unitaria y P un predicado binario. Sea Γ una interpretación del lenguaje L_σ en una teoría con signatura {o, e, h} siendo o y e constantes y h una función binaria :

$\gamma(x_0) \equiv \neg(x_0 = e)$

$\alpha_c(x_0) \equiv x_0 = hee$

$\alpha_f(x_0, x_1) \equiv hex_0 = x_1$

$\alpha_P (x_0, x_1) \equiv hx_0x_1 = hx_0e$

En este caso, la traducción de la fórmula $\exists x_0\, Pfx_0c$ es

$\exists x_1 (\neg(x_1 = e) \wedge \exists x_2 \exists x_3 (hex_1 = x_2 \wedge x_3 = hee \wedge hx_2x_3 = hx_2e))$

5.3 Estructura inducida

Sea $\Gamma = (\gamma, g)$ una traducción del lenguaje L_1 en el lenguaje L_2. Dado un modelo $\mathfrak{B} \models \Phi_\Gamma$ la traducción Γ induce de forma natural una L_1-estructura que denotaremos $\mathfrak{B}^\Gamma$.
El universo de la estructura $\mathfrak{B}^\Gamma$ será el subconjunto del universo B de $\mathfrak{B}$:

$A = \{b \in B \,/\, \mathfrak{B} \models \gamma[b]\}$

Nótese que por la condición $[\blacklozenge 1\Phi_\Gamma]$ el conjunto A no es vacío.
Cada símbolo de predicado $P \in PRED_1^{(n)}$ de la signatura σ_1 denota la relación P^A definida en A por

$$(b_1, ..., b_n) \in P^A \Leftrightarrow \mathfrak{B} \vDash \alpha_P [b_1, ..., b_n]$$

Cada símbolo de función $f \in FUNC_1^{(n)}$ designa la función f^A cuyo grafo es

$$\{(b_1,...b_n,b_{n+1})/ \mathfrak{B} \vDash \alpha_P [b_1, ... , b_n, b_{n+1}]\}$$

Tal conjunto es el grafo de una función debido a las condiciones [$\blacklozenge 2\ \Phi_\Gamma$]

Cada símbolo de constante $c \in CONST_1$ designa el único (por la condición[$\blacklozenge 3\Phi_\Gamma$]) elemento $b \in A$ tal que

$$\mathfrak{B} \vDash \gamma \wedge \alpha_c [b]$$

Observación

Si $\mathfrak{B}$ es finita $\mathfrak{B}^\Gamma$ es finita

El siguiente teorema relativo a la transformación construida de la clase $Mod(\Phi_\Gamma) \subset \mathfrak{E}_2$ en la clase $\mathfrak{E}_1$ de $\mathfrak{L}_1$-estructuras es el teorema básico de las interpretaciones.

[5-2] Teorema

Sea Γ una traducción del lenguaje $\mathfrak{L}_1$ en el lenguaje $\mathfrak{L}_2$

Dado un modelo $\mathfrak{B} \vDash \Phi_\Gamma$, para toda sentencia $\alpha \in \mathfrak{L}_1$ se verifica

$$\mathfrak{B}^\Gamma \vDash \alpha \quad \Leftrightarrow \quad \mathfrak{B} \vDash \alpha^\Gamma$$

Demostración

Bastará comprobar que si v es una valoración cualquiera en A (y por tanto, automáticamente, una valoración en B) se verifica, para toda fórmula α de $\mathfrak{L}_1$

$$\mathfrak{B}^\Gamma \vDash \alpha\ [v] \quad \Leftrightarrow \quad \mathfrak{B} \vDash \alpha^\Gamma\ [v]$$

Pues en tal caso, si α es una sentencia arbitraria de $\mathfrak{L}_1$ se tiene

[$\Rightarrow$] Si $\mathfrak{B}^\Gamma \nvDash \alpha$ entonces existe v, valoración en A, tal que $\mathfrak{B}^\Gamma \nvDash \alpha$ [v]. Por lo tanto $\mathfrak{B} \nvDash \alpha^\Gamma$ [v] . Por tratarse de una sentencia: $\mathfrak{B} \nvDash \alpha^\Gamma$

[$\Leftarrow$] Si $\mathfrak{B}^\Gamma \vDash \alpha$ entonces $\mathfrak{B}^\Gamma \nvDash \neg\alpha$. Por el mismo razonamiento que antes $\mathfrak{B} \nvDash \neg\alpha^\Gamma$ y entonces $\mathfrak{B} \vDash \alpha^\Gamma$

La comprobación de la anterior afirmación es asunto de rutina por inducción estructural.

* Para fórmulas con un único símbolo :

$$\begin{aligned}
\mathfrak{B}^\Gamma \vDash Px_{i_1} ... x_{i_n}\ [v] &\Leftrightarrow (v(x_{i_1}), ... v(x_{i_n})) \in P^A \\
&\Leftrightarrow \mathfrak{B} \vDash \alpha_P(x_{i_1} ... x_{i_n})\ [v] \\
&\Leftrightarrow \mathfrak{B} \vDash (Px_{i_1} ... x_{i_n})^\Gamma\ [v] \\
\mathfrak{B}^\Gamma \vDash x_i = c\ [v] &\Leftrightarrow v(x_i) \equiv c^A \\
&\Leftrightarrow \mathfrak{B} \vDash \alpha_c(x_i)\ [v] \\
&\Leftrightarrow \mathfrak{B} \vDash (x_i = c)^\Gamma\ [v] \\
\mathfrak{B}^\Gamma \vDash x_{i_0} = f\, x_{i_1} ... x_{i_n}\ [v] &\Leftrightarrow f^A\,(v(x_{i_1}) ... (x_{i_n})) \equiv v(x_{i_0}) \\
&\Leftrightarrow \mathfrak{B} \vDash \alpha_f(x_{i_0}, x_{i_1}, ..., x_{i_n})\ [v]
\end{aligned}$$

$$\Leftrightarrow \ B \vDash (x_{i_0} = f\ x_{i_1} \ldots x_{i_n})^{\Gamma}\ [v]$$

* Fórmulas atómicas con más de un símbolo

- Consideremos el caso $\alpha \equiv Pt_1 \ldots t_n$
Sea m_i el elemento de A designado por el término t_i en la valoración v
y sea w la valoración $v\ {}^{m_1}_{z_1} \ldots {}^{m_n}_{z_n}$
Por hipótesis de inducción para cada $i \in \{1, \ldots, n\}$

$$B^{\Gamma} \vDash z_i = t\ [v\ {}^{m_i}_{z_i}] \Leftrightarrow B \vDash (z_i = t)^{\Gamma}\ [v\ {}^{m_i}_{z_i}]$$

Por tanto

$$\begin{aligned} B^{\Gamma} \vDash Pt_1 \ldots t_n\ [v] \ &\Leftrightarrow \ (m_1, \ldots, m_n) \in P^A \text{ y para todo } i \in \{1, \ldots, n\}\ B^{\Gamma} \vDash z_i = t\ [v\ {}^{m_i}_{z_i}] \\ &\Leftrightarrow B \vDash \alpha_P\ [m_1, \ldots, m_n] \text{ y para todo } i \in \{1, \ldots, n\}\ B \vDash (z_i = t)^{\Gamma}\ [v\ {}^{m_i}_{z_i}] \\ &\Leftrightarrow \ B \vDash (z_1 = t_1)^{\Gamma} \wedge \ldots \wedge (z_n = t_n)^{\Gamma} \wedge \alpha_P\ (z_1, \ldots z_n)\ [w] \\ &\Leftrightarrow \ B \vDash \exists z_1 \ldots \exists z_n\ ((z_1 = t_1)^{\Gamma} \wedge \ldots \wedge (z_n = t_n)^{\Gamma} \wedge \alpha_P\ (z_1, \ldots z_n))\ [v] \\ &\Leftrightarrow \ B^{\Gamma} \vDash (Pt_1 \ldots t_n)^{\Gamma}\ [v] \end{aligned}$$

- Consideremos ahora el caso $\alpha \equiv t = c$
Sea m el elemento de A designado por t en la valoración v
Por hipótesis de inducción

$$B^{\Gamma} \vDash z_0 = t\ [v\ {}^{m}_{z_0}] \ \Leftrightarrow \ B \vDash (z_0 = t)^{\Gamma}\ [v\ {}^{m}_{z_0}]$$

luego

$$\begin{aligned} B^{\Gamma} \vDash t = c\ [v] \ &\Leftrightarrow \ m = c^A \ \text{ y } \ B^{\Gamma} \vDash z_0 = t\ [v\ {}^{m}_{z_0}] \\ &\Leftrightarrow \ B \vDash \alpha_c\ [v\ {}^{m}_{z_0}] \ \text{ y } B \vDash (z_0 = t)^{\Gamma}\ [v\ {}^{m}_{z_0}] \\ &\Leftrightarrow \ B \vDash (z_0 = t)^{\Gamma} \wedge \ \alpha_c\ (z_0)\ [v\ {}^{m}_{z_0}] \\ &\Leftrightarrow \ B \vDash \exists z_0\ ((z_0 = t)^{\Gamma} \wedge \ \alpha_c\ (z_0))\ [v] \\ &\Leftrightarrow \ B^{\Gamma} \vDash (t = c)^{\Gamma}\ [v] \end{aligned}$$

- Consideremos ahora le caso de una fórmula funcional $\alpha \equiv t_0 = f\ t_1 \ldots t_n$
Sea m_i el elemento de A designado por el término t_i en la valoración v
y sea w la valoración $v\ {}^{m_0}_{z_0}\ {}^{m_1}_{z_1} \ldots {}^{m_n}_{z_n}$

$$\begin{aligned} B^{\Gamma} \vDash t_0 = f\ t_1 \ldots t_n\ [v] \Leftrightarrow \\ &\Leftrightarrow \ f^A(m_1, \ldots, m_n) = m_0 \text{ y para todo } i \in \{1, \ldots, n\}\ B^{\Gamma} \vDash z_i = t\ \ [v\ {}^{m_i}_{z_i}] \\ &\Leftrightarrow \ B \vDash \alpha_f\ [m_0, m_1, \ldots, m_n] \text{ y para todo } i \in \{1, \ldots, n\}\ B \vDash (z_i = t)^{\Gamma}\ [v\ {}^{m_i}_{z_i}] \\ &\Leftrightarrow \ B \vDash (z_0 = t_0)^{\Gamma} \wedge (z_1 = t_1)^{\Gamma} \wedge \ldots \wedge (z_n = t_n)^{\Gamma} \wedge \alpha_f(z_0, z_1, \ldots, z_n)\ [w] \\ &\Leftrightarrow \ B \vDash \exists z_0\ \exists z_1 \ldots \exists z_n\ ((z_0 = t_0)^{\Gamma} \wedge (z_1 = t_1)^{\Gamma} \wedge \ldots \wedge (z_n = t_n)^{\Gamma} \wedge \alpha_P\ (z_1, \ldots z_n))\ [v] \\ &\Leftrightarrow \ B^{\Gamma} \vDash (t_0 = f\ t_1 \ldots t_n)^{\Gamma}\ [v] \end{aligned}$$

* Fórmulas moleculares

$$B^{\Gamma} \vDash \neg\alpha\ [v] \ \Leftrightarrow B^{\Gamma} \nvDash \alpha\ [v] \Leftrightarrow B \nvDash \alpha^{\Gamma}\ [v] \Leftrightarrow B \vDash (\neg\alpha)^{\Gamma}\ [v]$$

$$B^{\Gamma} \vDash \exists x\ \alpha\ [v] \ \Leftrightarrow \ \text{existe } a \in A \ \ B^{\Gamma} \vDash \alpha\ [v\ {}^{a}_{x}]$$

$\Leftrightarrow$ existe $a \in A$ $\quad B \vDash \alpha^{\Gamma}[v_x^a]$ por hipótesis de inducción
$\Leftrightarrow$ existe $a \in B$ $\quad B \vDash \gamma(w) \wedge \alpha^{\Gamma}[v_x^{\,a}{}_w^a]$
$\Leftrightarrow B \vDash \exists w\,(\gamma(w) \wedge \alpha^{\Gamma})[v]$
$\Leftrightarrow B \vDash (\exists x\,\alpha)^{\Gamma}[v]$

(Recuerdese que w es una variable nueva que no aparece en α, por lo que es irrelevante el valor asignado en principio a la variable w por la valoración v)

5.4 Interpretación de una teoría en otra

Las traducciones entre lenguajes son interesantes cuando consideramos teorías en dichos lenguajes.

[5-3] Definición

Sean L_1 y L_2 dos lenguajes de signaturas disjuntas. Sea $\Gamma = (\gamma, g)$ una traducción del lenguaje L_1 en el lenguaje L_2 , T_1 una teoría en el lenguaje L_1 y T_2 una teoría en el lenguaje L_2. Se dice que Γ es una interpretación de la teoría T_1 en la teoría T_2 si

1. $T_2 \vDash \Phi_{\Gamma}$
2. $\alpha \in T_1 \Rightarrow \alpha^{\Gamma} \in T_2$, para cada sentencia α de L_1

Notación
Escribiremos $T_1 \overset{\Gamma}{\hookrightarrow} T_2$ para indicar que Γ es una interpretación de T_1 en T_2 y $T_1 \hookrightarrow T_2$ para indicar que existe una interpretación de T_1 en T_2.

La siguiente proposición es obvia, e indica, entre otras cosas, que la interpretabilidad es un preorden.

[5-4] Proposición

Sean T_1, T_2 y T_3 teorías
1. $T_1 \hookrightarrow T_1$
2. $T_1 \hookrightarrow T_2$ & $T_2 \hookrightarrow T_3 \Rightarrow T_1 \hookrightarrow T_3$
3. Si T_2 es extensión de T_1 entonces $T_1 \hookrightarrow T_2$
4. Si T_3 es extensión de T_2 y $T_1 \hookrightarrow T_2$ entonces $T_1 \hookrightarrow T_3$
5. Si T_1 es extensión de T_3 y $T_1 \hookrightarrow T_2$ entonces $T_3 \hookrightarrow T_2$

Para comprobar que una traducción Γ es una interpretación de una teoría T_1 en otra teoría T_2 modelo de Φ_Γ, hay que comprobar que toda sentencia α de la teoría T_1 se transforma en una sentencia α^Γ de la teoría T_2. El siguiente teorema permite facilitar esta tarea en el caso de teorías axiomatizables : en este caso basta realizar la comprobación para los axiomas de T_1.
Obsérvese que hay un pequeña dificultad técnica debido a que la traducción de una fórmula lógicamente válida no es necesariamente una fórmula lógicamente válida. Por ejemplo la fórmula $\exists x\ x = x$ es una sentencia lógicamente verdadera y su transformada es $\exists x\ (\gamma(x) \wedge x = x)$ que no es una fórmula lógicamente verdadera (aunque sea verdadera en T_2 como consecuencia de ser $T_2 \vDash \Phi_\Gamma$)

[5-5] Proposición

Sea $\Gamma = (\gamma, g)$ una traducción del lenguaje de la teoría T_1 en el lenguaje de la teoría T_2 y $T_2 \vDash \Phi_\Gamma$. Supongamos que T_1 es axiomatizable y que para cada axioma ε de T_1 se verifica que $\varepsilon^\Gamma \in T_2$. Entonces Γ es una interpretación de T_1 en T_2
Demostración
Supongamos que existiera $\alpha \in T_1$ tal que $\alpha^\Gamma \notin T_2$. En tal caso existiría $\mathfrak{B} \vDash T_2$ y $\mathfrak{B} \nvDash \alpha^\Gamma$
Como $T_2 \vDash \Phi_\Gamma$ es $\mathfrak{B} \vDash \Phi_\Gamma$ y por tanto la estructura inducida $\mathfrak{B}^\Gamma$ verifica $\mathfrak{B}^\Gamma \nvDash \alpha$ y por tanto $\mathfrak{B}^\Gamma \nvDash T_1$. Como T_1 es axiomatizable existe algún axioma ε de T_1 del que $\mathfrak{B}^\Gamma$ no es modelo . Si $\mathfrak{B}^\Gamma \nvDash \varepsilon$ entonces $\mathfrak{B} \nvDash \varepsilon^\Gamma$ y como $\mathfrak{B}$ es modelo de T_2 concluimos que $\varepsilon^\Gamma \notin T_2$, contra la hipótesis. Luego siempre que $\alpha \in T_1$ se verifica que $\alpha^\Gamma \in T_2$ y por tanto Γ es una interpretación de T_1 en T_2

Observación

Si $T_1 \overset{\Gamma}{\rightarrow} T_2$ se verifica

$$\alpha \in T_1 \Rightarrow \alpha^\Gamma \in T_2$$

luego

$$T_1 \subset \{\alpha \in L_1 / \alpha^\Gamma \in T_2\}$$

En general no se da la igualdad.

Si T_1 es una teoría completa y T_2 es una teoría consistente se verifica

$$\alpha \notin T_1 \Rightarrow \neg\alpha \in T_1 \Rightarrow (\neg\alpha)^\Gamma \in T_2 \Rightarrow \neg(\alpha^\Gamma) \in T_2 \Rightarrow \alpha^\Gamma \notin T_2$$

pues $(\neg\alpha)^\Gamma \equiv \neg(\alpha^\Gamma)$. Por lo tanto en este caso

$$T_1 = \{\alpha \in L_1 / \alpha^\Gamma \in T_2\}$$

[5-6] Proposición

Si $T_1 \overset{\Gamma}{\rightarrow} T_2$ y $\mathfrak{B} \vDash T_2$ entonces $\mathfrak{B}^\Gamma \vDash T_1$
Demostración
$\alpha \in T_1 \Rightarrow \alpha^\Gamma \in T_2 \Rightarrow \mathfrak{B} \vDash \alpha^\Gamma \Rightarrow \mathfrak{B}^\Gamma \vDash \alpha$
Nota

Esta proposición indica la utilidad de las interpretaciones en pruebas de consistencia relativa. Si la teoría T_2 es consistente tendrá un modelo $\mathfrak{B}$. Si la teoría T_1 es interpretable en T_2 vía Γ la estructura inducida $\mathfrak{B}^\Gamma$ será modelo de T_1 por lo que T_1 es también consistente.

5.5 Codificación de estructuras. Codificación de clases

Hemos señalado que si T_1 es una teoría completa y $T_1 \overset{\Gamma}{\rightarrowtail} T_2$ entonces podemos recuperar T_1 a partir de T_2, pues $T_1 = \{\alpha \in L_1 / \alpha^\Gamma \in T_2\}$. Dada una estructura $\mathfrak{A}$, la teoría $Th(\mathfrak{A})$ es completa . Esto sugiere la siguiente definición:

[5-7] Definición

Sea $\mathfrak{A}$ una σ_1-estructura y $\mathfrak{B}$ una σ_2-Estructura. Se dice que $\mathfrak{A}$ es *sumergible* o *codificable* en $\mathfrak{B}$ si existe una interpretación Γ de $Th(\mathfrak{A})$ en $Th(\mathfrak{B})$.

Notación
Escribiremos $\mathfrak{A} \overset{\Gamma}{\rightarrowtail} \mathfrak{B}$ para indicar que Γ es una interpretación de $Th(\mathfrak{A})$ en $Th(\mathfrak{B})$ y $\mathfrak{A} \hookrightarrow \mathfrak{B}$ para indicar que existe alguna interpretación de $Th(\mathfrak{A})$ en $Th(\mathfrak{B})$.

[5-8] Proposición

Sean $\mathfrak{A}$ y $\mathfrak{B}$ estructuras de lenguajes L_1 y L_2 respectivamente. Sea Γ una interpretación del lenguaje L_1 en L_2 y $\mathfrak{B} \models \Phi_\Gamma$. Son equivalentes

1. $\mathfrak{A} \overset{\Gamma}{\rightarrowtail} \mathfrak{B}$
2. $\mathfrak{A} \equiv \mathfrak{B}^\Gamma$

Demostración
[1⇒2]
Sea $Th(\mathfrak{A}) \overset{\Gamma}{\rightarrowtail} Th(\mathfrak{B})$. Por ser $Th(\mathfrak{A})$ completa, según hemos observado

$$Th(\mathfrak{A}) = \{\alpha \in L_1 / \alpha^\Gamma \in Th(\mathfrak{B})\}$$

o sea

$$\alpha \in Th(\mathfrak{A}) \Leftrightarrow \alpha^\Gamma \in Th(\mathfrak{B})$$

Por lo tanto

$$\mathfrak{A} \models \alpha \Leftrightarrow \mathfrak{B} \models \alpha^\Gamma \Leftrightarrow \mathfrak{B}^\Gamma \models \alpha$$

es decir, $\mathfrak{A}$ y $\mathfrak{B}^\Gamma$ son elementalmente equivalentes
[2⇒1]

$$\alpha \in Th(\mathfrak{A}) \Rightarrow \mathfrak{A} \models \alpha \Rightarrow \mathfrak{B}^\Gamma \models \alpha \Rightarrow \mathfrak{B} \models \alpha^\Gamma \Rightarrow \alpha^\Gamma \in Th(\mathfrak{B})$$

Si en vez de equivalencia elemental consideramos isomorfía tenemos un concepto algo más fuerte:

[5-9] Definición

Sea $\mathfrak{A}$ una σ_1-estructura y $\mathfrak{B}$ una σ_2-Estructura. Se dice que $\mathfrak{A}$ es *definible* en $\mathfrak{B}$ si existe una interpretación Γ de Th($\mathfrak{A}$) en Th($\mathfrak{B}$) tal que $\mathfrak{A} \approx \mathfrak{B}$.

[5-10] Definición

Sean K_1 y K_2 dos clases de estructuras en lenguajes L_1 y L_2 respectivamente. Se dice que K_1 es *sumergible* o *codificable* en K_2 vía Γ si Γ es una interpretación de Th(K_1) en Th(K_2) tal que para cada $\mathfrak{A} \in K_1$ existe $\mathfrak{B} \in K_2$ tal que $\mathfrak{A} \overset{\Gamma}{\hookrightarrow} \mathfrak{B}$

Notación : $K_1 \overset{\Gamma}{\hookrightarrow} K_2$

Para transmitir la inseparabilidad finita necesitaremos alguna condición adicional.

[5-11] Definición

Sean K_1 y K_2 dos clases de estructuras (no necesariamente sobre la misma signatura). Se dice que K_1 es *fuertemente codificable* en K_2 vía Γ si Γ es una interpretación de Th(K_1) en Th(K_2) tal que

I. para cada $\mathfrak{A} \in K_1$ existe $\mathfrak{B} \in K_2$ tal que $\mathfrak{A} \overset{\Gamma}{\hookrightarrow} \mathfrak{B}$
II. para cada $\mathfrak{A} \in K_1^{fin}$ existe $\mathfrak{B} \in K_2^{fin}$ tal que $\mathfrak{A} \overset{\Gamma}{\hookrightarrow} \mathfrak{B}$

Notación : $K_1 \overset{\Gamma}{\hookrightarrow}_f K_2$

Observación
En los casos prácticos es más cómodo tratar las interpretaciones desde un punto de vista semántico que desde un punto de vista sintáctico. Para ver que $\mathfrak{A}$ es codificable en $\mathfrak{B}$ bastará comprobar que hay una fórmula de primer orden que define el universo de la interpretación, es decir, que determina los elementos del universo de $\mathfrak{B}^\Gamma$, una correspondencia h entre los elementos del universo de $\mathfrak{A}$ y los del universo de $\mathfrak{B}^\Gamma$, y, por ejemplo, para cada predicado P (análogo para funciones o constantes) la existencia de una fórmula α_P tal que

$$\mathfrak{A} \models P[a] \iff \mathfrak{B} \models \alpha_P[h(a)]$$

5.6 Transferencia de la indecidibilidad.

Si tenemos una interpretación Γ que permita sumergir la estructura A en la estructura B se transmite el carácter de indecidibilidad de la estructura A a la estructura B.

Teorema

$\mathsf{A} \overset{\Gamma}{\hookrightarrow} \mathsf{B}$, A indecidible $\Rightarrow$ B indecidible

Demostración

Si A es sumergible en B vía Γ se tiene que $\mathsf{A} \equiv \mathsf{B}^{\Gamma}$ y para toda sentencia α del lenguaje de A se verifica

$$\alpha \in \mathrm{Th}(\mathsf{A}) \Leftrightarrow \mathsf{A} \models \alpha \Leftrightarrow \mathsf{B}^{\Gamma} \models \alpha \Leftrightarrow \mathsf{B} \models \alpha^{\Gamma} \Leftrightarrow \alpha^{\Gamma} \in \mathrm{Th}(\mathsf{B})$$

Como α^{Γ} se obtiene a partir de α por un procedimiento efectivo, esta reducción asegura que B es indecidible si lo es A, pues si tuviéramos un procedimiento de decisión para $\mathrm{Th}(\mathsf{B})$ lo tendríamos para $\mathrm{Th}(\mathsf{A})$.

El anterior teorema permite demostrar que la teoría de ciertas estructuras es indecidible. Pero no es útil si queremos demostrar la indecidibilidad de teorías no necesariamente completas.

Observación

La indecidibilidad de teorías no se transmite por interpretaciones. Si T_1 es una teoría indecidible y $T_1 \overset{\Gamma}{\hookrightarrow} T_2$, no se deduce, en general, que T_2 sea indecidible.

Podemos observarlo en el caso de que T_1 tenga una modelo finito A. Entonces obviamente $T \subset \mathrm{Th}(\mathsf{A})$ y por tanto $T \hookrightarrow \mathrm{Th}(\mathsf{A})$. Pero al ser A finito su teoría $\mathrm{Th}(\mathsf{A})$ es decidible.

Se necesita pues algo más que la simple indecidibilidad para poder utilizar las interpretaciones en demostraciones de indecididbilidad.

A continuación formulamos un teorema que recoge el aspecto fundamental de la técnica de Tarski en demostraciones de indecidibilidad.

[5-12] Teorema

Sea T_1 fuertemente indecidible y $T_1 \hookrightarrow T_2$. Entonces T_2 es fuertemente indecidible.

Demostración

Supongamos $T_1 \overset{\Gamma}{\hookrightarrow} T_2$. Sea T_3 compatible con T_2. Se trata de demostrar que T_3 es indecidible. Sean σ_1 y σ_2 las signaturas de los lenguajes de T_1 y T_2 respectivamente

Sea δ la conjunción de las condiciones de adecuación de la interpretación Γ, es decir, del conjunto de fórmulas que hemos llamado Φ_{Γ}.

Sea $T_4 = \{\varphi \in \mathrm{SENT}_{\sigma_1} : \delta \rightarrow \varphi^{\Gamma} \in T_3\}$. Veamos que T_4 es una teoría compatible con T_1.

Lema 1.

$$\models \varphi \Rightarrow \models \delta \rightarrow \varphi^{\Gamma}$$

Demostración

Supongamos que φ es una fórmula lógicamente válida. Si $\mathfrak{B}$ es una σ_2-estructura arbitraria y suponemos $\mathfrak{B} \models \delta$, estará definida la σ_1-estructura $\mathfrak{B}^{\Gamma}$ que, por hipótesis, será modelo de φ . Por el teorema [5-2] , $\mathfrak{B} \models \varphi^{\Gamma}$

Así pues, $\delta \rightarrow \varphi^{\Gamma}$ es lógicamente válida.

Lema 2

T_4 es una teoría

Demostración

Sea $T_4 \models \varphi$. Entonces para ciertas sentencias $\alpha_1, \ldots, \alpha_n$ de T_4 se verifica

$$\{\alpha_1, \ldots, \alpha_n\} \models \varphi$$

y por tanto

$$\models \alpha_1 \wedge \ldots \wedge \alpha_n \rightarrow \varphi$$

Por el lema 1

$$\models \delta \rightarrow (\alpha_1 \wedge \ldots \wedge \alpha_n \rightarrow \varphi)^{\Gamma}$$

o sea

$$\models \delta \rightarrow (\alpha_1^{\Gamma} \wedge \ldots \wedge \alpha_n^{\Gamma} \rightarrow \varphi^{\Gamma})$$

Por lógica proposicional

$$\models ((\delta \rightarrow \alpha_1^{\Gamma}) \wedge \ldots \wedge (\delta \rightarrow \alpha_n^{\Gamma})) \rightarrow (\delta \rightarrow \varphi^{\Gamma})$$

luego

$$\{(\delta \rightarrow \alpha_1^{\Gamma}), \ldots, (\delta \rightarrow \alpha_n^{\Gamma})\} \models (\delta \rightarrow \varphi^{\Gamma})$$

Puesto que $\{\alpha_1, \ldots, \alpha_n\} \subset T_4$, por definición $(\delta \rightarrow \alpha_1^{\Gamma}), \ldots, (\delta \rightarrow \alpha_n^{\Gamma})$ son sentencias de la teoría T_3. Luego $(\delta \rightarrow \varphi^{\Gamma}) \in T_3$ y $\varphi \in T_4$

Por tanto T_4 es cerrada respecto a la relación de consecuencia.

Lema 3

T_4 es compatible con T_1

Demostración

Puesto que hemos supuesto que T_2 y T_3 son compatibles, sea $\mathfrak{B} \models T_2 + T_3$. Como $\mathfrak{B} \models T_2$ y $T_1 \xrightarrow{\Gamma} T_2$, es $\mathfrak{B}^{\Gamma} \models T_1$. Como $T_2 \models \delta$ es $\mathfrak{B} \models \delta$. Veamos que $\mathfrak{B}^{\Gamma} \models T_4$. En efecto, sea $\alpha \in T_4$, y por tanto $\delta \rightarrow \alpha^{\Gamma} \in T_3$, tal que $\mathfrak{B}^{\Gamma} \not\models \alpha$. Entonces $\mathfrak{B}^{\Gamma} \not\models \alpha^{\Gamma}$ y $\mathfrak{B} \not\models \delta$. Por tanto sería $\mathfrak{B} \not\models \delta \rightarrow \alpha^{\Gamma}$, contra la hipótesis de ser $\mathfrak{B} \models T_3$. Se tiene así que $\mathfrak{B}^{\Gamma} \models T_1 + T_4$, con lo que se ha visto que T_1 y T_4 son compatibles.

Como T_4 es una teoría compatible con T_1 que es fuertemente indecidible debe ser T_4 indecidible. Pero la reducción

$$\varphi \in T_4 \Leftrightarrow \delta \rightarrow \varphi^{\Gamma} \in T_3$$

asegura que T_3 debe ser indecidible y en consecuencia T_2 es fuertemente indecidible.

Consecuencia inmediata es :

[5-13] Teorema

Sea A fuertemente indecidible y $\mathsf{A} \hookrightarrow \mathsf{B}$. Entonces B es fuertemente indecidible

El teorema [5-12] permite demostrar que una teoría es fuertemente indecidible interpretando en ella una teoría fuertemente indecidible. Para aplicar el método debemos partir de una primera teoría fuertemente indecidible. La aritmética de Robinson **Q** es una teoría esencialmente indecidible y finitamente axiomatizable. Por tanto (teorema [4-34]) es fuertemente indecidible. Este será nuestro punto de partida para exponer la técnica de Tarski.

Según hemos comentado ya, en la práctica es más cómodo trabajar "semánticamente" concentrando la atención en modelos más que en lenguajes. El teorema [5-13] permite transmitir, por medio de una interpretación, el carácter fuertemente indecidible de una estructura a otra en la que se pueda codificar. Obtendremos así una estructura con una teoría hereditariamente indecidible. Viendo esta estructura como modelo de una teoría T obtenemos, en consecuencia, que la teoría T es hereditariamente indecidible.

5.7 Transferencia de la inseparabilidad. Teorema de Rabin-Ershov

[5-14] Proposición

Sea T_1 una teoría inseparable y supongamos que T_1 es interpretable en T_2. Entonces T_2 es inseparable.

Demostración

Es una consecuencia inmediata del teorema [3-11]. Consideraremos una enumeración $\{\alpha_n : n \in \omega\}$ de las sentencias de primer orden. Sean

$$D_1 = \{n \in \omega : \alpha_n \in T_1\}$$
$$R_1 = \{n \in \omega : \neg\alpha_n \in T_1\}$$
$$D_2 = \{n \in \omega : \alpha_n \in T_2\}$$
$$R_2 = \{n \in \omega : \neg\alpha_n \in T_2\}$$

Como $T_1 \overset{\Gamma}{\hookrightarrow} T_2$, la interpretación Γ determina una transformación efectiva de sentencias de $\mathsf{L}(T_1)$ en sentencias de $\mathsf{L}(T_2)$ tal que

$$\alpha \in T_1 \quad \Rightarrow \quad \alpha^\Gamma \in T_2$$

y por tanto

$$\neg\alpha \in T_1 \ \Rightarrow \quad \neg\alpha^\Gamma \in T_2$$

pues $(\neg\alpha)^\Gamma \equiv \neg(\alpha^\Gamma)$

Como la transformación es efectiva se tiene una función recursiva $f : \omega \to \omega$ verificando

$f(D_1) \subset D_2$
$f(R_1) \subset R_2$

En consecuencia, por el teorema señalado, al ser D_1 y R_1 efectivamente inseparables y ser el par (D_1, R_1) sumergible en el par (D_2, R_2), son también efectivamente inseparables D_2 y R_2.

[5-15] Teorema

Sea K_1 una clase de σ_1- estructuras y K_2 una clase de σ_2-estructuras y supongamos que K_1 es fuertemente codificable en K_2

Si K_1 es finitamente axiomatizable y finitamente inseparable entonces K_2 es finitamente inseparable.

Demostración

Supongamos $K_1 \overset{\Gamma}{\underset{f}{\rightarrow}} K_2$ y sea ε la conjunción de los axiomas de $Th(K_1)$. La interpretación Γ define una transformación efectiva de fórmulas de $L(K_1)$ en fórmulas de $L(K_2)$. Consideremos la siguiente transformación efectiva

$$\begin{array}{lll} h : L(K_1) & \rightarrow & L(K_2) \\ \alpha & \rightarrow & (\varepsilon \rightarrow \alpha)^{\Gamma} \end{array}$$

Veamos que h sumerge el par efectivamente inseparable (ver § 4.9) $(D_{Th(K_1)}, F_{Th(K_1)})$ en el par $(D_{Th(K_2)}, F_{Th(K_2)})$

$$\begin{array}{lll} (\varepsilon \rightarrow \alpha)^{\Gamma} \notin Th(K_2) & \Rightarrow \exists\, B \in K_2 & B \models (\varepsilon \wedge \neg\alpha)^{\Gamma} \\ & \Rightarrow \exists\, B \in K_2 & B^{\Gamma} \models \varepsilon \wedge \neg\alpha \\ & \Rightarrow \exists\, B \in K_2 & B^{\Gamma} \models Th(K_1) \;\&\; B^{\Gamma} \models \neg\alpha \\ & \Rightarrow \alpha \notin Th(K_1) & \end{array}$$

$$\begin{array}{lll} \alpha \in Fr(K_1) & \Rightarrow \exists\, A \in K_1^{fin} & A \models \neg\alpha \\ & \Rightarrow \exists\, A \in K_1^{fin} & A \models \varepsilon \wedge \neg\alpha \\ & \Rightarrow \exists\, B \in K_2^{fin} & B^{\Gamma} \models \varepsilon \wedge \neg\alpha \\ & \Rightarrow \exists\, B \in K_2^{fin} & B \models (\varepsilon \wedge \neg\alpha)^{\Gamma} \\ & \Rightarrow \exists\, B \in K_2^{fin} & B \models \neg(\varepsilon \rightarrow \alpha)^{\Gamma} \\ & \Rightarrow \varepsilon \rightarrow \alpha \in Fr(K_2) & \end{array}$$

6. LA TÉCNICA DE GÖDEL

6.1 El predicado Bew de Gödel

El resultado fundamental de indecidibilidad es el relativo a la indecidibilidad de la aritmética. La demostración de forma directa de la indecidibilidad de la aritmética es posible por tratarse de una teoría en la que se representan de forma natural las funciones computables. Las ideas básicas proceden de la demostración de Gödel del teorema de incompletitud. La presentación actual suele basarse en una generalización del método de Gödel conocida como lema diagonal o teorema del punto fijo.
En el famoso artículo de Gödel [19] se introduce un procedimiento para codificar numéricamente las fórmulas del lenguaje. También se asocia a cada sucesión de fórmulas un número que dependerá de las fórmulas de la sucesión. En particular, puesto que una demostración es una sucesión de fórmulas verificando ciertas condiciones, se tiene asociada a cada demostración un número. Esta codificación permite expresar numéricamente la metateoría de un sistema formal, es decir, enunciados como "tal fórmula es demostrable", "el sistema es consistente", "el sistema es incompleto", etc. En particular Gödel construye un predicado B(x, y) que expresa que y es el número de una demostración de la fórmula de código x. Entonces el predicado $Bew(x) \equiv \exists y\, B(x, y)$ expresa que hay una demostración de la fórmula de número x. Gödel demostró con la construcción detallada del predicado B(x, y) que dicho predicado es recursivo primitivo. Por tanto Bew(x) es un predicado recursivamente enumerable.

La idea básica de la técnica de Gödel consiste en considerar una fórmula γ de número n verificando

$$\vdash \gamma \leftrightarrow \neg Bew(\mathbf{n})$$

donde hemos denotado por **n** el numeral de n, esto es el término que designa n en el sistema formal
Puesto que la interpretación natural de Bew(**n**) es que la sentencia de número n es derivable, la fórmula γ afirma de sí misma que no es demostrable. Observese que la autorreferencia juega un papel fundamental en la sentencia de Gödel. (cf. [57])

Gödel demostró que si la aritmética es consistente γ no puede ser un teorema aritmético y si es ω-consistente tampoco puede serlo su negación. De donde se deduce la incompletitud de la aritmética.

La demostración de Gödel hace uso de la hipótesis de la ω-consistencia de la teoría. En 1936 Rosser [52] demostró que esta hipótesis se puede reemplazar por la de simple consistencia. La idea subyacente en su demostración es considerar, en lugar de Bew, un predicado de demostrabilidad modificado, a saber :

$$Br(x) \equiv \exists y\, B(x, y) \wedge \forall z\, (z < y \rightarrow \neg Bew(\nu(x), z))$$

donde $\nu(x)$ es el código de la negación de la fórmula de número x.

6.2 Representación de funciones en la aritmética

Una de las partes fundamentales de la técnica de Gödel consiste en considerar la capacidad de una teoría en el lenguaje de la aritmética para expresar funciones y relaciones.

[6-1] Definición

Una función $f : \omega^n \rightarrow \omega$ es representable en una teoría aritmética T si existe una fórmula $\alpha(x_1, \ldots, x_n, y)$ tal que

$$f(a) = b \Rightarrow T \vdash \forall y\, (\alpha(\mathbf{a}, y) \leftrightarrow y = \mathbf{b})$$

[6-2] Definición

Se dice que la relación $R \subset \omega^n$ es representable en una teoría aritmética T si existe una fórmula $\rho(x_1, x_2, \ldots, x_n)$ tal que

$$(a_1, a_2, \ldots, a_n) \in R \Rightarrow T \vdash \rho(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$$
$$(a_1, a_2, \ldots, a_n) \notin R \Rightarrow T \vdash \neg\rho(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$$

El resultado fundamental es

[6-3] Teorema

Las funciones recursivas coinciden con las representables en la aritmética de Robinson.

El teorema es consecuencia de los siguientes lemas:

[6-4] Lema

Las funciones iniciales (cero, sucesor, proyecciones) son representables en **Q**

[6-5] Lema

Si la fórmula α representa f y β_i representa g_i (para cada i = 1, ... ,k) entonces la fórmula $\exists z_1 \ldots \exists z_k(\beta_1(\underline{x}, z_1) \wedge \ldots \wedge \beta_k(\underline{x}, z_k) \wedge \alpha(z_1, \ldots, z_k, y))$ representa la función composición $f(g_1, \ldots, g_k)$

[6-6] Lema

Si g está representada por α y $f(\underline{x}) = \mu y\, (g(\underline{x}, y) = 0)$ entonces la fórmula

$$\beta(\underline{x}, y) = \alpha(\underline{x}, y, 0) \wedge \forall z\, (z < y \rightarrow \neg\alpha(\underline{x}, z, 0)$$

siendo

$$z < y \equiv \exists w\, (sw + z = y)$$

representa f

[6-7] Lema

Si f está definida por recursión a partir de h y g y las funciones h y g son representables en **Q** entonces f es representable en **Q**.

La demostración de estos lemas aparece en muchos manuales. (Cf. p.ej. [4], [14], [35])

En consecuencia :

[6-8] Proposición

Si R es una relación decidible entonces es representable en la aritmética

Demostración

Si R es decidible su función característica c_R es recursiva y por tanto representable por una fórmula $\alpha(x, y)$. Entonces $\alpha(x, \mathbf{1})$ representa R.

6.3 El lema de diagonalización

Dada una fórmula con una variable libre x le corresponderá un número de Gödel n. Podemos considerar la fórmula obtenida al sustituir x por el numeral **n** que designa al número n, o sea, $\alpha(\mathbf{n})$. Esta fórmula tendrá un número de Gödel m. La función d que transforma n en m se suele llamar *función diagonal* y es claramente computable, y por tanto recursiva. Por tanto es representable en la aritmética.

Si γ es una fórmula de número de n el numeral de n se escribirá también $\mathbf{n} = \ulcorner\gamma\urcorner$.

[6-9] Teorema

Sea T una teoría del lenguaje de la aritmética en que la función diagonal sea representable. Sea $\alpha(x)$ una fórmula del lenguaje con la única variable libre x. En estas condiciones existe una sentencia γ tal que

$$T \vdash \gamma \leftrightarrow \alpha(\ulcorner\gamma\urcorner)$$

Demostración

Sea $\delta(x, y)$ la fórmula que representa la función diagonal en T, e.e.

$$d(n) = m \Rightarrow T \vdash \forall y\, (d(\mathbf{n}, y) \leftrightarrow y = \mathbf{m})$$

Construyamos la fórmula

$$\beta(x) \equiv \forall y(d(x, y) \rightarrow \alpha(y))$$

Sea p el número de Gödel de esta fórmula

Al sustituir en β la variable x por **p** se tiene la sentencia

$$\gamma \equiv \forall y(d(\mathbf{p}, y) \rightarrow \alpha(y))$$

Sea q el número de Gödel de esta fórmula. Claramente d(p) = q

Veamos que la fórmula γ verifica la afirmación del teorema.

Como d(p) = q y δ representa d

[1] $T \vdash \forall y(\delta(\mathbf{p}, y) \leftrightarrow y = \mathbf{q})$

y por lo tanto

[2] $T \vdash \delta(\mathbf{p}, \mathbf{q})$

La fórmula $\gamma \rightarrow (\delta(\mathbf{p}, \mathbf{q}) \rightarrow \alpha(\mathbf{p}))$ es lógicamente válida. Obsérvese que $\alpha(\ulcorner\gamma\urcorner)$ es $\alpha(\mathbf{q})$. Por lo tanto

[3] $T \vdash \gamma \rightarrow (\delta(\mathbf{p}, \mathbf{q}) \rightarrow \alpha(\ulcorner\gamma\urcorner))$

que con [2] proporciona

[4] $T \vdash \gamma \rightarrow \alpha(\ulcorner\gamma\urcorner)$

con lo cual tenemos la mitad de lo que pretendíamos

Consideremos ahora la fórmula lógicamente válida

[5] $T \vdash \alpha(\mathbf{q}) \rightarrow (y = \mathbf{q} \rightarrow \alpha(y))$

Por [1] y [5]

[6] $T \vdash \alpha(\mathbf{p}) \rightarrow (\delta(\mathbf{p}, y) \rightarrow \alpha(y))$

Como y no aparece en la fórmula $\alpha(\mathbf{p})$ que es cerrada

[7] $\alpha(\mathbf{p}) \rightarrow \forall y(\delta(\mathbf{p}, y) \rightarrow \alpha(y))$

Es decir, por definición de γ,
[8] $\alpha(\ulcorner\gamma\urcorner) \rightarrow \gamma$
Con lo cual obtenemos la equivalencia buscada

6.4 La indecidibilidad de la aritmética

Como aplicación del teorema del punto fijo se puede demostrar de una manera sencilla la indecidibilidad de la aritmética de Robinson.

[6-10] Teorema

Toda extensión consistente de **Q** es indecidible
Demostración
Sea T una extensión consistente de **Q** y $D = \{\ulcorner\alpha\urcorner : \alpha \in T\}$ el conjunto de números de Gödel de las sentencias de T. Si D fuese decidible existiría una fórmula τ tal que para todo $n \in \omega$

$n \in D \Rightarrow T \vdash \tau(\mathbf{n})$
$n \notin D \Rightarrow T \vdash \neg\tau(\mathbf{n})$

Apliquemos el lema de diagonalización a la fórmula $\neg\tau(x)$: existirá una fórmula γ con $t = \ulcorner\gamma\urcorner$ al que

$T \vdash \gamma \leftrightarrow \neg\tau(\ulcorner\gamma\urcorner)$

De donde se sigue la contradicción :

$t \in D \Rightarrow T \vdash \tau(\mathbf{t}) \Rightarrow T \vdash \neg\gamma \Rightarrow T \nvdash \gamma \Rightarrow \gamma \notin D \Rightarrow t \notin D$
$t \notin D \Rightarrow T \vdash \neg\tau(\mathbf{t}) \Rightarrow T \vdash \gamma \Rightarrow \gamma \in D \Rightarrow t \in D$

6.5 Inseparabilidad de la aritmética

En realidad con el mismo esfuerzo podemos obtener que la aritmética de Robinson (y por tanto también sus extensiones consistentes) es recursivamente inseparable

[6-11] Proposición

Q es recursivamente inseparable
Demostración
Sea $D = \{\ulcorner\alpha\urcorner : \alpha \in \mathbf{Q}\}$ y $R = \{\ulcorner\alpha\urcorner : \neg\alpha \in \mathbf{Q}\}$

Supongamos que existiera un conjunto recursivo C tal que $D \subset C \subset \overline{R}$ Sea α la fórmula que representa C y apliquemos el lema de diagonalización a $\neg\alpha(x)$. Existe una sentencia γ con $t = \ulcorner\gamma\urcorner$ tal que

$$\mathbf{Q} \vdash \gamma \leftrightarrow \neg\alpha(\ulcorner\gamma\urcorner)$$

Entonces se tiene la contradicción

$$t \notin C \Rightarrow \mathbf{Q} \vdash \neg\alpha(\mathbf{t}) \Rightarrow \mathbf{Q} \vdash \gamma \Rightarrow \ulcorner\gamma\urcorner \in D \Rightarrow \ulcorner\gamma\urcorner \in C \Rightarrow t \in C$$

6.6 El teorema de Tarski

A partir del lema de diagonalización puede darse también una prueba muy sencilla del teorema de Tarski relativo a la imposibilidad de expresar dentro de la teoría el concepto de verdad, si consideramos una teoría, como **Q**, que verifique el lema de diagonalización.

[6-12] Definición

El conjunto $B \subset \omega$ es *definible* en N si existe una fórmula $\beta(x)$ con una variable libre tal que $B = \{n \in \omega : N \vDash \beta(\mathbf{n})\}$

[6-13] Teorema

El conjunto $V = \{\ulcorner\alpha\urcorner : N \vDash \alpha\}$ no es definible en N.

Demostración

Si $\beta(x)$ define V en N, aplicando el lema diagonal a $\neg\beta(x)$ existirá γ con $p = \ulcorner\gamma\urcorner$ tal que

$$\mathbf{Q} \vdash \gamma \leftrightarrow \neg\beta(\ulcorner\gamma\urcorner)$$

y por tanto

$$N \vDash \gamma \leftrightarrow \neg\beta(\ulcorner\gamma\urcorner)$$

puesto que $N \vDash \mathbf{Q}$

Pero de ahí se sigue la contradicción

$$p \in V \Leftrightarrow N \vDash \gamma \Leftrightarrow N \vDash \neg\beta(\ulcorner\gamma\urcorner) \Leftrightarrow N \nvDash \beta(\ulcorner\gamma\urcorner) \Leftrightarrow p \notin V$$

6.7 El teorema de Church

Consideremos el conjunto de sentencias lógicamente válidas en el lenguaje de la aritmética

$$L = \{\alpha \in SENT_{L_A} : \vDash \alpha\}$$

La aritmética de Robinson es una extensión finita de esta teoría, pues **Q** es finitamente axiomatizable. La reducción

$$\alpha \in \mathbf{Q} \quad \Leftrightarrow \quad \varepsilon \rightarrow \alpha \in L$$

siendo ε la conjunción de los axiomas de **Q**, muestra que L es indecidible.

[6-14] Teorema

El conjunto de sentencias lógicamente válidas en el lenguaje de la aritmética es indecidible.

Una reducción inmediata proporciona

[6-15] Teorema

El cálculo de predicados total es indecidible

7. LA TÉCNICA DE TARSKI

Exponemos en este capítulo las ideas esenciales de la técnica de Tarski [60] para demostrar la indecidibilidad de la teoría de anillos y la teoría de grupos, así como el resultado de J. Robinson [49] acerca de la indecidibilidad de la teoría de cuerpos. El método de demostración se basa en construir, partiendo de la aritmética de Robinson, interpretaciones de unas teorías en otras. Los teoremas [5-12] y [5-13] de transferencia de indecidibilidad mediante interpretaciones permiten obtener los resultados deseados a partir del resultado básico de la indecidibilidad esencial de la aritmética de Robinson. En nuestra presentación se simplificará algo la exposición de Tarski al elegir una notación más cómoda, junto con un camino que permite ciertas mejoras de índole técnica. Por otra parte, el hecho de poner el énfasis en el aspecto semántico de la definibilidad de unas estructuras en otras, en lugar de la interpretación sintáctica de las teorías, permite, en nuestra opinión, un tratamiento con ventajas considerables.

7.1 Indecidibilidad de la aritmética

El punto de partida de la técnica de Tarski es la indecidibilidad esencial de la aritmética. (Cf. [6-10])

[7-1] Teorema

Q es esencialmente indecidible

Como **Q** es una teoría finitamente axiomatizable, el teorema [4-34] asegura que

[7-2] Teorema

Q es fuertemente indecidible

Puesto que toda teoría compatible con la aritmética completa, Th(N), es compatible con **Q** se tiene

[7-3] Teorema

N es fuertemente indecidible

7.2 Indecidibilidad de la teoría de anillos

Para demostrar la indecidibilidad de la teoría de anillos (unitarios) bastará encontrar un anillo en el que podamos interpretar la aritmética. Dicho anillo tendrá, en consecuencia, una teoría hereditariamente indecidible, de donde se deducirá que la teoría de anillos es hereditariamente indecidible. El candidato natural es el anillo de los números enteros, esto es, la estructura $\mathsf{Z} = (\mathbb{Z}, +^{\mathbb{Z}}, \cdot^{\mathbb{Z}}, 1^{\mathbb{Z}})$. (Por sencillez de la escritura omitiremos los superíndices de dominio, que queda claro por el contexto)
Para determinar la interpretación Γ de N en Z la única dificultad es definir el universo de la interpretación, es decir, caracterizar los números naturales dentro del conjunto de los enteros por una fórmula de primer orden del lenguaje considerado. Para ello podemos utilizar un conocido teorema de teoría de números debido a Lagrange que asegura que todo número natural es suma de cuatro cuadrados. Obviamente la condición es necesaria y suficiente.
Sea pues la fórmula del lenguaje de signatura $\{+, \cdot, 1\}$

$$\gamma(x) \equiv \exists y_1\, \exists y_2\, \exists y_3\, \exists y_4 \;\; x = y_1 \cdot y_1 + y_2 \cdot y_2 + y_3 \cdot y_3 + y_4 \cdot y_4$$

Entonces

$$\mathsf{Z} \models \gamma[n] \qquad \text{syss} \qquad n \in \omega$$

Las restantes fórmulas de la interpretación son , naturalmente,

$$\alpha_{+}(x,y,z) \equiv x + y = z$$
$$\alpha_{\cdot}(x,y,z) \equiv x \cdot y = z$$
$$\alpha_0(x) \equiv x + x = x$$
$$\alpha_s(x,y) \equiv x + 1 = y$$

Es trivial observar que $\mathsf{Z} \models \Phi_\Gamma$, siendo Φ_Γ las condiciones de adecuación de la interpretación, y que $\mathsf{Z}^\Gamma \approx \mathsf{N}$. En consecuencia Γ es una interpretación de N en Z.
Tenemos pues

[7-4] Teorema

La estructura de los enteros Z es fuertemente indecidible

Como la estructura de los enteros es un anillo unitario conmutativo infinito que es dominio de integridad, tenemos como corolario :

[7-5] Teorema

La teoría de anillos (unitarios) es hereditariamente indecidible.
La teoría de anillos conmutativos es hereditariamente indecidible.
La teoría de anillos infinitos es hereditariamente indecidible.
La teoría de los dominios de integridad es hereditariamente indecidible.

Observación

Por el teorema acerca de las extensiones no esenciales [4-41] el teorema anterior vale también si consideramos el lenguaje {+, ·} , sin la constante 1.

La teoría de anillos no es esencialmente indecidible. Es conocido que la teoría de la estructura de los reales es decidible. También lo es la teoría de cualquier anillo finito. Ambas son extensiones de la teoría de anillos.

7.3 Indecidibilidad de la teoría de cuerpos

De forma análoga al apartado anterior, para demostrar la indecidibilidad de la teoría de cuerpos un método natural es interpretar la estructura de los números enteros en la estructura del cuerpo de los números racionales $\mathfrak{Q} = \{\mathbb{Q}, +^{\mathbb{Q}}, \cdot^{\mathbb{Q}}, 1^{\mathbb{Q}}\}$. En este caso, la fórmula adecuada depende de la ecuación diofántica

$$2 + pqa^2 + pz^2 = x^2 + y^2$$

Consideremos el esquema de fórmulas

$$\rho(u, v, w) \equiv \exists x\, \exists y\, \exists z\, (1 + 1 + u \cdot v \cdot w \cdot w + v \cdot z \cdot z = x \cdot x + u \cdot y \cdot y)$$

La fórmula que nos interesa es

$$\gamma(x_0) \equiv \forall u\, \forall v\, (\rho(u, v, 0) \wedge \forall w(\rho(u, v, w) \rightarrow \rho(u, v, sw)\,) \rightarrow \rho(u, v, x_0))$$

(Obsérvese la analogía con el principio de inducción)
Se verifica

$$\mathfrak{Q} \vDash \gamma\,[a] \quad \Leftrightarrow \quad a \in \mathbb{Z}$$

Es inmediato , por inducción, que todo número natural verifica la fórmula. Además, puesto que la variable x_0 sólo aparece al cuadrado, sucede que

$$\mathfrak{Q} \vDash \gamma\,[a] \quad \Leftrightarrow \quad \mathfrak{Q} \vDash \gamma\,[-a]$$

luego la fórmula la verifican también los enteros negativos. Para demostrar que si un número racional verifica dicha fórmula es necesariamente un entero se necesitan

herramientas avanzadas de teoría de números ajenas al propósito de este trabajo. Esta interpretación la obtuvo Julia Robinson bajo la dirección de Tarski en [34]

[7-6] Teorema

La estructura de los números racionales $\mathbb{Q}$ es fuertemente indecidible

Y como antes

[7-7] Teorema

La teoría de cuerpos es hereditariamente indecidible
La teoría de cuerpos infinitos es hereditariamente indecidible
La teoría de espacios vectoriales es hereditariamente indecidible

7.4 Indecidibilidad de la teoría de grupos

Para demostrar la indecidibilidad de la teoría de grupos interpretaremos la estructura $\mathbb{N} = (\omega ; 0, s, +, \cdot)$ en una determinada estructura de grupo. La teoría de tal grupo será hereditariamente indecidible y obtendremos en consecuencia que la teoría de grupos es indecidible. Tarski consideró para ello el grupo de las permutaciones del conjunto de los enteros (e.e. el grupo simétrico $G = S(\mathbb{Z})$, conjunto de biyecciones de $\mathbb{Z}$ en sí mismo con la composición de aplicaciones, $\circ$, como operación del grupo). Por razones técnicas se considera además un elemento distinguido, con lo que la estructura a considerar será $\mathbb{G} = (G; \circ^G, e^G)$, que escribiremos, sencillamente, $(G; \circ, e)$. Obsérvese que $Th(\mathbb{G})$ es una extensión inesencial de la teoría de grupos formulada en la signatura $\sigma_G = \{\circ\}$, por lo que es aplicable el teorema [4-41] sobre indecidibilidad de extensiones inesenciales.
La interpretación de $\mathbb{N} = (\omega; 0, s, +, \cdot)$ en tal grupo se hará construyendo unas interpretaciones intermedias.

En primer lugar observemos que podemos definir el 0 y la aplicación sucesor, mediante la suma, a partir de las equivalencias

$$x = 0 \quad \Leftrightarrow \quad x + x = x$$
$$y = sx \quad \Leftrightarrow \quad y = x + 1$$

Por lo tanto

[7-8] Lema

$(\omega; 0, s, +, \cdot) \hookrightarrow (\omega; 1, +, \cdot)$

Demostración

El universo de la interpretación viene dado, obviamente, por

$$\gamma(x) \equiv x = x$$

Las fórmulas que interpretan 0 y s son, según hemos señalado,

$$\alpha_0(x) \equiv x + x = x$$
$$\alpha_s(x, y) \equiv y = x + 1$$

A continuación observemos que podemos definir el producto en los naturales mediante la operación de un argumento "cuadrado", $k(x) = x^2$. La idea se basa en la fórmula elemental $(x + y)^2 = x^2 + 2xy + y^2$

[7-9] Lema

$(\omega; 1, +, \cdot) \hookrightarrow (\omega; 1, +, k)$

Demostración

El universo de la interpretación viene dado por

$$\gamma(x) \equiv x = x$$

Las fórmulas para interpretar los demás elementos del lenguaje son :

$$\alpha_+(x, y, z) \equiv x + y = z$$
$$\alpha_\cdot(x, y, z) \equiv k(x + y) = k(x) + z + z + k(y)$$
$$\alpha_1(x) \equiv x = 1$$

Veamos ahora que podemos definir el cuadrado a partir del mínimo común múltiplo. Obsérvese que dos números naturales consecutivos son primos entre sí, de forma que, denotando por M la función "mínimo común múltiplo"

$$M(n, n + 1) = n(n + 1) = n^2 + n$$

[7-10] Lema

$(\omega; 1, +, k) \hookrightarrow (\omega; 1, +, M)$

Demostración

Basta considerar

$$\alpha_k(x, y) \equiv Mx(x + 1) = y + x$$

La interpretación del "mínimo común múltiplo" a partir de la relación de divisibilidad es trivial

[7-11] Lema

$(\omega; 1, +, M) \hookrightarrow (\omega; 1, +, |)$

Demostración

$\alpha_M(x, y, z) \equiv \forall w ((x \mid w \wedge y \mid w) \leftrightarrow z \mid w)$

Esta estructura sobre los naturales puede interpretarse sobre una estructura del mismo tipo sobre los enteros de la misma forma que se ha hecho en § 6.3

[7-12] Lema

$(\omega; 1, +, |) \hookrightarrow (\mathbb{Z}; 1, +, |)$

Nos proponemos ahora definir la estructura $(\mathbb{Z}; 1, +, |)$ en el grupo de permutaciones de los enteros. Para ello es útil considerar un lenguaje con un símbolo de constante e que designará la permutación $e(x) = x + 1$. Veamos que podemos construir una interpretación de $(\mathbb{Z}; 1, +, |)$ en $(G; \circ, e)$

El universo de la interpretación estará formado por el subconjunto de G formado por las traslaciones, esto es, las permutaciones de los enteros de la forma $t_a(x) = x + a$ siendo $a \in \mathbb{Z}$. El conjunto de traslaciones forma un subgrupo del grupo de permutaciones y se verifica fácilmente que

$$t_a \circ t_b = t_{a+b}$$

$$t_a \circ t_b^{-1} = t_{a-b}$$

y

$$t_a^{-1} = t_{-a}$$

Por otra parte es inmediato observar que las traslaciones son las potencias de e. En concreto $t_a = e^a$.

En particular es claro que $a \mid b$ syss t_b es una iteración de t_a. Veamos que en este universo podemos representar las operaciones de los enteros.

[7-13] Lema

Sea $p \in G$ una permutación arbitraria de los enteros. Entonces p es una traslación si y sólo si se verifica $p \circ e = e \circ p$

Demostración

[$\Rightarrow$]

Las traslaciones son potencias de e. Por tanto es inmediato que conmutan con e. En efecto, si $t = e^a$ entonces

$$t \circ e = e^a \circ e = e^{a+1} = e^{1+a} = e \circ e^a = e \circ t$$

[$\Leftarrow$]

Sea p una permutación que conmuta con e y sea $p(0) = a$. Veamos que $p(c) = c + a$.
Es fácil por inducción. Para $c = 0$ es claro. Supuesto $p(c) = c + a$ entonces

$$p(c + 1) = p \circ e\,(c) = e \circ p(c) = e(c + a) = c + a + 1 = (c + 1) + a$$

Con lo cual la fórmula vale para los c positivos. Para los negativos es análogo.

Esto permite caracterizar el universo de la interpretación mediante la fórmula de primer orden

$$\gamma(x) \equiv x \circ e = e \circ x$$

[7-14] Lema

La aplicación $h : (\mathbb{Z}; +) \rightarrow (G; \circ)$

$$a \rightarrow t_a$$

es un homomorfismo de grupos

Este lema asegura que la fórmula

$$\alpha_+(x, y, z) \equiv x \circ y = z$$

es adecuada para representar la operación de suma de los enteros, pues $t_a \circ t_b = t_{a+b}$.

[7-15] Lema

Sean $a, b \in \mathbb{Z}$. Entonces son equivalentes

1. $a \mid b$
2. Para toda permutación $p \in G$, si $t_a \circ p = p \circ t_a$, entonces se verifica $t_b \circ p = p \circ t_b$

Demostración

$[1 \Rightarrow 2]$

Supongamos que $b = ad$ y que $t_a \circ p = p \circ t_a$

Demostraremos por inducción sobre d entero que $t_{ad} \circ p = p \circ t_{ad}$

Para $d = 0$ la traslación t_b es t_0 , o sea la identidad y es trivial.

Supongamos que la afirmación es correcta para d , esto es $t_{ad} \circ p = p \circ t_{ad}$ y veamos los casos $d + 1$ y $d - 1$

$$t_{a(d+1)} \circ p = t_{ad+a} \circ p = t_{ad} \circ t_a \circ p = t_{ad} \circ p \circ t_a = p \circ t_{ad} \circ t_a = p \circ t_{a(d+1)}$$

La propiedad queda vista para los múltiplos positivos. Análogo para los negativos.

$[2 \Rightarrow 1]$

Supongamos ahora que para toda permutación $p \in G$ se verifica

$$t_a \circ p = p \circ t_a \Rightarrow t_b \circ p = p \circ t_b$$

y veamos que $a \mid b$

Consideraremos primero el caso $a \neq 0$

Sea la permutación (¡no es una traslación !)

$$p(x) = \begin{cases} x + a & \text{si } a \mid x \\ x & \text{en otro caso} \end{cases}$$

Claramente p es una permutación de $\mathbb{Z}$ (p transforma cada múltiplo de a en el múltiplo siguiente dejando inalterados los demás números)
Además p conmuta con t_a. En efecto, si x no divide a a entonces x+a tampoco y

$t_a \circ p(x) = t_a(x) = x + a$

$p \circ t_a(x) = p(x + a) = x + a$

Y si x divide a a entonces x + a también y

$t_a \circ p(x) = t_a(x + a) = x + a + a$

$p \circ t_a(x) = p(x + a) = x + a + a$

La hipótesis asegura que p conmuta con t_b
Por tanto

$t_b \circ p(0) = p \circ t_b(0)$

$p(0) + b = p(b)$

Y como a | 0 sucede que a + b = p(b)
Al ser $a \neq 0$ y por la definición de p, debe ser a divisor de b (en otro caso sería p(b)=b)

Consideremos ahora el caso a = 0. Tenemos que ver que b = 0.
Como a = 0, t_a es la identidad y por tanto conmuta con cualquier permutación, luego t_b debe conmutar también con cualquier permutación. Si se considera la permutación p(x) = - x (¡no es traslación!) se tiene

$t_b \circ p(x) = p(x) + b = -x + b$

$p \circ t_b(x) = p(x + b) = -x - b$

Luego b = 0

Este lema asegura que la fórmula

$$\alpha_{|}(x, y) \equiv \forall z\, (x \circ z = z \circ x \rightarrow y \circ z = z \circ y)$$

es adecuada para representar la relación divisibilidad en los enteros pues

$$a \mid b \quad \text{syss} \quad (G; \circ, e) \vDash \alpha_{|}\, [t_a, t_b]$$

Por lo tanto la interpretación Γ determinada por

$$\begin{aligned} \gamma(x) &\equiv x \circ e = e \circ x \\ \alpha_{+}(x, y, z) &\equiv x \circ y = z \\ \alpha_{|}(x, y) &\equiv \forall z\, (x \circ z = z \circ x \rightarrow y \circ z = z \circ y) \\ \alpha_{1}(x) &\equiv x = e \end{aligned}$$

verifica

$$(\mathbb{Z}; 1, +, |) \equiv (G; \circ, e)^{\Gamma}$$

Nótese que la construcción realizada permite asegurar que

$$(\mathbb{Z};\ 1,\ +,\ |\ ) \approx (T;\ e,\ \circ,\ \backslash) = (G;\ \circ,\ e)^{\Gamma}$$

siendo T el conjunto de traslaciones, $\circ$ la composición y $\backslash$ la relación

$$t_a \backslash t_b \Leftrightarrow \text{existe } t_c \text{ tal que } t_b = t_{ac}$$

siendo el homomorfismo $a \rightarrow t_a$

[7-16] Proposición

La teoría de la estructura $(G;\ \circ,\ e)$ es fuertemente indecidible

Esta teoría es una extensión no esencial de la teoría del grupo de permutaciones de los enteros con el lenguaje $\{\circ\}$. Por el teorema [4-41]

[7-17] Proposición

La teoría del grupo de permutaciones de los enteros $(G;\ \circ^G)$ es fuertemente indecidible

[7-18] Proposición

La teoría de grupos es hereditariamente indecidible
La teoría de semigrupos es hereditariamente indecidible
La teoría de grupos infinitos es hereditariamente indecidible

Observación

Al tener modelos finitos la teoría de grupos *no* es esencialmente indecidible. Por otra parte, Wanda Szmielew demostró en su tesis de 1950 que la teoría de grupos conmutativos, que es extensión de la teoría de grupos, es decidible. Nótese que en la demostración de la indecidibilidad de la teoría de grupos se ha hecho uso esencial de que el grupo de las permutaciones no es conmutativo: el universo de la interpretación viene caracterizado por la fórmula $x \circ e = e \circ x$, y al representar la relación de divisibilidad hemos utilizado la fórmula $\forall z\ (\ x \circ z = z \circ x \rightarrow y \circ z = z \circ y)$.

7.5 Limitaciones de la técnica de Tarski

La técnica usada por Tarski en la demostración de la indecidibilidad de la teoría de grupos no es adecuada para otras teorías. En [44, pág. 85] ya se señala, por ejemplo, que dicha técnica no vale para la teoría de grupos finitos. Obsérvese que la técnica consiste en obtener una interpretación en una estructura con una teoría fuertemente indecidible. Pero si tratamos de la clase de los grupos finitos, cada grupo finito que consideremos tendrá una teoría decidible.
Utilizar la noción de inseparabilidad finita permite superar esta dificultad. Aplicaremos dicha noción a diversas clases de estructuras en el capítulo 9 obteniendo los deseados resultados de indecidibilidad como corolario inmediato de teoremas más fuertes de inseparabilidad finita. Para ello necesitaremos partir de un primer resultado de inseparabilidad finita y aplicar el método de inmersiones semánticas del § 5.7. En el capítulo 8 se obtiene el primer resultado de partida para la aplicación del método.

8. TEORÍAS INSEPARABLES

La técnica de las interpretaciones permite obtener resultados de inseparabilidad para teorías sin modelos finitos. Ejemplos especialmente importantes de teorías sin modelos finitos son la aritmética y la teoría de conjuntos. Para aplicar el método de las interpretaciones necesitamos partir de una primera teoría inseparable. Demostraremos de forma rápida la inseparabilidad de la aritmética de Robinson siguiendo la idea de J. F. Prida [45] de utilizar un teorema de extensión de las funciones recursivas parciales en la aritmética. A partir de este resultado obtendremos la inseparabilidad de la teoría de conjuntos interpretando la arimética en dicha teoría.

8.1 Inseparabilidad de la aritmética

La técnica de Gödel para demostrar la indecidibilidad de la aritmética se basa en un teorema de representación de las funciones recursivas.(Cf. § 6.2) La demostración del teorema de representación se apoya en unos lemas, la mayor parte de los cuales son sencillos. Pero la demostración del lema [6-7], para tratar el caso de definiciones por recursión, es notablemente más complicado. Esta dificultad puede obviarse considerando un teorema similar referido a la clase más amplia de funciones recursivas parciales. La clase de las funciones recursivas parciales es la menor clase que contiene a la suma, el producto, las funciones proyección, la función característica de la igualdad y es cerrada bajo composición y minimización de una función total. (Cf. [4]).

[8-1] Definición

Diremos que la fórmula aritmética $\alpha(x_1, x_2, \ldots, x_n, x_0)$ *extiende* la función parcial $\varphi : \omega^n \to \omega$ en **Q** si para cada $a_1, a_2, \ldots, a_n, b \in \omega$

$$\varphi(a_1, a_2, \ldots, a_n) = b \Rightarrow \mathbf{Q} \vdash \forall x_0\, (\alpha(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}, x_0) \leftrightarrow x_0 = \mathbf{b})$$

(Si $n \in \omega$ denotamos por **n** el término ss...so , con n veces s)

Se verifica el teorema de extensión siguiente, cuya demostración es notablemente más sencilla que la demostración del teorema de representación de funciones recursivas:

[8-2] Teorema

Toda función recursiva parcial es extensible en **Q** .
Demostración

La prueba es análoga a la bien conocida del teorema de representación de las funciones recursivas.(Cf. p. ej. [4])

[8-3] Teorema

Q es inseparable

Demostración

Sea $D_{\mathbf{Q}} = \{n : \varphi_n \in \mathbf{Q}\}$ y $R_{\mathbf{Q}} = \{n : \neg\varphi_n \in \mathbf{Q}\}$. El enunciado del teorema afirma que $D_{\mathbf{Q}}$ y $R_{\mathbf{Q}}$ son efectivamente inseparables.

Supongamos una enumeración φ_n de las funciones recursivas parciales. Sea ϕ la función recursiva parcial $\phi(n) = \varphi_n(n)$ y sea $\alpha(x, y)$ la fórmula que extiende ϕ en **Q**, es decir :

$$\phi(a) = b \Rightarrow \mathbf{Q} \vdash \forall y\,(\alpha(\mathbf{a}, y) \leftrightarrow y = \mathbf{b})$$

Sea *f* la función recursiva definida por $f(a) = \alpha(a, \mathbf{0})^{\#}$, o sea, *f*(a) es el código de la sentencia obtenida al sustituir x por **a** e y por **0** en la fórmula α.

Por el teorema de recursión existe una función recursiva *h* tal que

$$j_{h(a,b)}(n) = \begin{cases} 0 & \text{si } \exists s\ fh(a,b) \in W_{b,s} - W_{a,s} \\ 1 & \text{si } \exists s\ fh(a,b) \in W_{a,s} - W_{b,s} \\ \uparrow & \text{e.o.c.} \end{cases}$$

Entonces *fh* es una función de separación de $D_{\mathbf{Q}}$ y $R_{\mathbf{Q}}$.

En efecto, supongamos que $D_{\mathbf{Q}} \subset W_a$, $R_{\mathbf{Q}} \subset W_b$ y $W_a \cap W_b = \varnothing$. Entonces

$$\begin{aligned} fh(a, b) \in W_a \;&\Rightarrow\; \varphi_{h(a,b)}(h(a, b)) = 1 \\ &\Rightarrow\; \phi(h(a, b)) = 1 \\ &\Rightarrow \mathbf{Q} \vdash \forall y(\alpha(\boldsymbol{h}\mathbf{(a, b)}, y) \leftrightarrow y = \mathbf{1}) \\ &\Rightarrow \mathbf{Q} \vdash \neg\alpha(\boldsymbol{h}\mathbf{(a, b)}, \mathbf{0}) \\ &\Rightarrow\; f\,h(a, b) \in R_{\mathbf{Q}} \\ &\Rightarrow\; f\,h(a, b) \in W_b \\ &\Rightarrow f\,h(a, b) \notin W_a \end{aligned}$$

$$\begin{aligned} f\,h\,(a, b) \in W_b \;&\Rightarrow\; \varphi_{h(a,b)}(h(a, b)) = 0 \\ &\Rightarrow\; \phi(h(a, b)) = 0 \\ &\Rightarrow \mathbf{Q} \vdash \forall y\,(\alpha(\boldsymbol{h}\mathbf{(a, b)}, y) \leftrightarrow y = \mathbf{0}) \\ &\Rightarrow \mathbf{Q} \vdash \alpha(\boldsymbol{h}\mathbf{(a,b)}, \mathbf{0}) \\ &\Rightarrow f\,h(a, b) \in D_{\mathbf{Q}} \\ &\Rightarrow f\,h(a, b) \in W_a \\ &\Rightarrow f\,h(a, b) \notin W_b \end{aligned}$$

Estas contradicciones indican que $f\,h(a, b) \in \overline{W_a} \cap \overline{W_b}$

Es interesante observar que como consecuencia inmediata de la inseparabilidad de **Q** se obtiene el teorema de incompletitud de Gödel-Rosser [19], [52]

[8-4]Teorema

Toda extensión consistente y axiomatizable de **Q** es incompleta

Demostración

Sea T una extensión axiomatizable consistente de **Q** y consideremos los conjuntos numéricos

$$D_T = \{n \in \omega : \alpha_n \in T\}$$
$$R_T = \{n \in \omega : \neg\alpha_n \in T\}$$

Por ser T axiomatizable ambos son conjuntos r.e.

Sea L_A el conjunto de todas las sentencias aritméticas y consideremos el conjunto numérico

$$S = \{n \in \omega : \alpha_n \in L_A\}$$

Sean

$$D_T = W_d$$
$$R_T \cup \overline{S} = W_r$$

Por ser T extensión de **Q** se tiene

$$D_{\mathbf{Q}} \subset W_d \text{ y } R_{\mathbf{Q}} \subset W_r$$

Por ser T consistente

$$W_d \cap W_r = \varnothing$$

Si *f* es la función de inseparabilidad de $D_{\mathbf{Q}}$ y $R_{\mathbf{Q}}$ se tiene

$$f(d, r) \in \overline{W_d} \cap \overline{W_r} = \overline{D_T} \cap \overline{D_T} \cap S$$

Esto quiere decir que la sentencia de código $f(d, r)$ no es demostrable en T ni tampoco su negación. Así pues T es incompleta.

8.2 Inseparabilidad de la teoría de conjuntos

La indecidibilidad de la aritmética es un resultado fundamental para el matemático –la teoría de números es la "Reina de la Matemática", en frase célebre de Gauss–, pero más significativa aún es la indecidibilidad de la teoría de conjuntos –"el Paraíso que Cantor ha creado para nosotros", en palabras de Hilbert–, pues es idea generalizada que la teoría de conjuntos es capaz de expresar todos los contenidos matemáticos –"sin la teoría de conjuntos y funciones no se puede hacer nada en Matemáticas; con ellas, por el contrario, se puede hacer todo", dice Godement en su *Álgebra*– .

Para demostrar la indecidibilidad de la teoría de conjuntos bastará mostrar que dicha teoría es suficientemente potente para expresar la aritmética, o más concretamente,

que la aritmética de Robinson **Q** es interpretable en la teoría de conjuntos. En 1950, Wanda Szmielew y Alfred Tarski (cf. [60] pág. 34) anunciaron, sin demostración, que **Q** es interpretable en un pequeño fragmento finitamente axiomatizable de una teoría de conjuntos con el lenguaje $\{E, \in\}$, donde E es un símbolo de predicado monario que expresa la propiedad de ser un conjunto y $\in$ denota la relación de pertenencia. Los axiomas utilizados son el axioma de extensionalidad, el axioma del vacío y un axioma que permite formar la unión binaria $x \cup \{y\}$. Con la idea de mantener el sistema finitamente axiomatizable no se usa el axioma de separación. Esta teoría es a su vez fácilmente interpretable en cualquiera de las formalizaciones usuales de la teoría de conjuntos. En 1970, G. E. Collins y J. D. Halpern [8] publicaron una demostración del resultado en el NDJFL. Posteriormente se ha demostrado que esta interpretación se puede hacer en una teoría aún más débil (cf. [1], [38]), consistente únicamente en los axiomas:

N $\quad \forall x \; x \notin \varnothing$

W $\quad \forall x \, \forall y \, \forall z \, (x \in \mathsf{W}yz \leftrightarrow x \in y \vee x = z)$

donde W es un símbolo de función binaria cuyo significado pretendido corresponde a la operación $x \cup \{y\}$ como indica el axioma W. Esta teoría carece incluso del axioma de extensionalidad que sí aparecía en la axiomática de [8].

Al ser la teoría considerada tan restringida la prueba es algo artificiosa. Puesto que **ZF** (o mejor **ZFC**) es el estándar *de facto* de teoría de conjuntos como fundamento de las matemáticas, aquí nos conformaremos con interpretar **Q** en un fragmento de la teoría de conjuntos **ZF** lo suficientemente fuerte para seguir un camino más natural y usual. Puesto que las bases de la construcción son bien conocidas (cf. p.ej. [21], [39], [59]) no seremos excesivamente rígidos en las demostraciones, mezclando argumentos informales con notación lógica de forma que se favorezca la legibilidad. De la consistencia de **ZF** se deduciría así que **ZF** es fuertemente indecidible e inseparable.

La idea básica corresponde a la propuesta de von Neumann de representar cada número natural como el conjunto de los naturales menores :

$$0 \rightharpoonup \varnothing$$
$$1 \rightharpoonup \{0\} = \{\varnothing\}$$
$$2 \rightharpoonup \{0, 1\} = \{\varnothing, \{\varnothing\}\}$$
$$3 \rightharpoonup \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing,\{\varnothing\}\}\}$$
$$\ldots$$

con lo que el concepto de sucesor corresponderá a

$$x \cup \{x\}$$

Esta construcción hace que

$$0 \in 1 \in 2 \in 3 \in \ldots$$

y que

$$0 \subset 1 \subset 2 \subset 3 \subset \ldots$$

La teoría de conjuntos de Zermelo-Fraenkel es una teoría de primer orden con igualdad con un lenguaje de signatura $\{\in\}$, siendo $\in$ un símbolo de relación binario, que escribiremos, como es costumbre, en notación infija. Como es también habitual

se escribirá $x \notin y$ en lugar de $\neg(x \in y)$. Otra notación usual es $x \subset y$ como abreviatura de la fórmula $\forall z\ (z \in x \rightarrow z \in y)$.
Los axiomas de la teoría que utilizaremos son los siguientes :

ZF1. Vacío :
$\exists x\ \forall y\ \ y \notin x$
ZF2. Extensionalidad :
$\forall x \forall y\ (\forall z\ (z \in x \leftrightarrow z \in y) \rightarrow x = y)$
ZF3. Par :
$\forall x\ \forall y\ \exists u\ \forall z\ \ (z \in u \leftrightarrow (z = x \vee z = y))$
ZF4. Unión :
$\forall x\ \exists u\ \forall z\ \ (z \in u \leftrightarrow \exists y\ (z \in y \wedge y \in u))$
ZF5. Partes :
$\forall x\ \exists y\ \forall z\ \ (z \in x \leftrightarrow z \subset x)$
ZF6. Esquema de axiomas de separación :
$\forall x\ \exists y\ \forall z\ \ (z \in y \leftrightarrow z \in x \wedge \varphi(z))$
para cada fórmula φ tal que $z \in lib(\varphi)$, $y \notin var(\varphi)$
ZF7. Infinito :
$\exists x\ (\varnothing \in x\ \wedge \forall z\ (\ z \in x \rightarrow z \cup \{z\} \in x))$

En la anterior formulación de los axiomas de la teoría hemos utilizado abreviaturas usuales cuya legitimidad justificaremos a continuación.

[8-5] Proposición

$\mathbf{ZF} \vdash \exists!x\ \forall z\ \ z \notin x$

Demostración
El axioma del vacío afirma la existencia de x tal que $\forall z\ z \notin x$. Por el axioma de extensionalidad

$\forall x \forall y\ (\forall z\ (z \notin x \leftrightarrow z \notin y) \rightarrow x = y)$

de donde se deduce la unicidad

Esto permite definir el *conjunto vacío*

[8-6] Definición

$x = \varnothing \quad \equiv \ \forall y\ \ y \notin x$

De forma análoga el axioma de extensionalidad permite asegurar la unicidad de los conjuntos cuya existencia aseguran el axioma de par, el axioma de unión y el axioma de partes. Por tanto podemos utilizar las siguientes notaciones

[8-7] Definición

1. $u = \{x, y\} \equiv \forall z\ (z \in u \leftrightarrow z = x \vee z = y)$
2. $\{x\} \equiv \{x, x\}$
3. $u = \mathsf{P}(x) \equiv \forall z(\ z \in u \leftrightarrow z \subset x)$
4. $u = \bigcup x \equiv \forall z\ (z \in u \leftrightarrow \exists y\ (z \in y \wedge y \in u))$
5. $u = x \cup y \equiv u = \bigcup\{x, y\}$

[8-8] Proposición

ZF $\vdash \forall x \forall y \forall z\ (z \in x \cup y \leftrightarrow z \in x \vee z \in y)$

Demostración

$$z \in x \cup y \Leftrightarrow \exists w\ (z \in w \wedge w \in \{x, y\})$$
$$\Leftrightarrow \exists w\ (z \in w \wedge (w \in x \vee w = y))$$
$$\Leftrightarrow z \in x \vee z \in y$$

Por el axioma de extensionalidad el conjunto y cuya existencia se afirma en el axioma de separación es único. Lo que permite utilizar la notación

[8-9] Definición

$$y = \{z \in x: \varphi(x)\} \equiv \forall z\ (z \in y \leftrightarrow z \in x \wedge \varphi(x))$$

Como aplicación inmediata se deduce la existencia de la intersección binaria

[8-10] Definición

$$x \cap y \equiv \{z \in x: x \in y\}$$

Dado un conjunto x el axioma de par permite formar $\{x\} = \{x, x\}$. Nuevamente el axioma de par permite formar el conjunto $\{x, \{x\}\}$. Y el axioma de la unión aplicado a este conjunto asegura la existencia de $\bigcup\{x, \{x\}\} = x \cup \{x\}$. La extensionalidad asegura en todo caso la unicidad. Se tiene por tanto :

[8-11] Proposición

ZF $\vdash \forall x\ \exists! y\ \ y = x \cup \{x\}$

Esto permite la definición deseada para el sucesor

[8-12] Definición

$$x^{+} \equiv x \cup \{x\}$$

Es inmediato observar que, puesto que $x \in x^+$, se tiene :

[8-13] Proposición

$\mathbf{ZF} \vdash \forall x \; x^+ \neq \varnothing$

A continuación usaremos las siguientes abreviaturas de conjunto *inductivo* y conjunto *transitivo* :

[8-14] Definición

1. $\mathrm{Ind}(x) \equiv \varnothing \in x \wedge \forall z (z \in x \rightarrow z^+ \in x)$
2. $\mathrm{Tran}(x) \equiv \forall z (z \in x \rightarrow z \subset x)$

El axioma de infinito afirma la existencia de un conjunto inductivo.

Para construir la interpretación de **Q** en **ZF** lo primero es determinar el universo de la interpretación, esto es determinar el conjunto que represente los números naturales

[8-15] Definición

$\mathrm{Nat}(x) \equiv \forall y (\mathrm{Ind}(y) \rightarrow x \in y)$

[8-16] Proposición

1. $\mathbf{ZF} \vdash \mathrm{Nat}(\varnothing)$
2. $\mathbf{ZF} \vdash \exists x \; \mathrm{Nat}(x)$
3. $\mathbf{ZF} \vdash \forall x (\mathrm{Nat}(x) \rightarrow \mathrm{Nat}(x^+))$

Demostración

1. Ind(x) implica que $\varnothing \in x$
2. Consecuencia inmediata de 1
3. De Nat(x) y Ind(y) se deduce $x \in y$, y por ser y inductivo $x^+ \in y$

[8-17] Definición

$0 \equiv \varnothing$
$1 \equiv \varnothing^+$
$2 \equiv 1^+$
...

[8-18] Proposición

Para todo n se verifica

$$\mathbf{ZF} \vdash \mathrm{Nat}(n)$$

El axioma de infinito permite asegurar la existencia del conjunto de todos los naturales.

[8-19] Proposición

$$\mathbf{ZF} \vdash \exists!u\, \forall x\, (x \in u \leftrightarrow \mathrm{Nat}(x))$$

Demostración

Por el axioma de infinito existe un conjunto inductivo

$$\mathbf{ZF} \vdash \exists y\, \mathrm{Ind}(y)$$

Por el axioma de separación

$$\mathbf{ZF} \vdash \exists w\, \forall x\, (x \in w \leftrightarrow x \in y \wedge \forall z\, (\mathrm{Ind}(z) \rightarrow x \in z))$$

Por tanto

$$\mathbf{ZF} \vdash \exists w\, \forall x\, (x \in w \leftrightarrow \forall z\, (\mathrm{Ind}(z) \rightarrow x \in z))$$

La unicidad se concluye por el axioma de extensionalidad.

[8-20] Definición

Denotaremos ω el conjunto de todos los naturales. Así

$$x \in \omega \equiv \mathrm{Nat}(x) \equiv \forall y\, (\mathrm{Ind}(y) \rightarrow x \in y)$$

[8-21] Proposición

1. $\mathbf{ZF} \vdash \mathrm{Ind}(\omega)$
2. $\mathbf{ZF} \vdash \forall z\, (\mathrm{Ind}(z) \rightarrow \omega \subset z)$
3. $\mathbf{ZF} \vdash \forall z\, (z \subset \omega \wedge \mathrm{Ind}(z) \leftrightarrow z = \omega)$

Demostración

1. Consecuencia de ser $\mathrm{Nat}(\varnothing)$ y $\mathrm{Nat}(x) \rightarrow \mathrm{Nat}(x^+)$.
2. De $x \in \omega$ e $\mathrm{Ind}(z)$ se deduce $x \in z$.
3. Consecuencia de lo anterior.

La parte 3. es el principio de inducción para ω: Todo subconjunto inductivo de ω coincide con ω.

[8-22] Proposición

$$\mathbf{ZF} \vdash \forall x\, ((\mathrm{Nat}(x) \wedge x \neq \varnothing) \rightarrow \exists y\, (\mathrm{Nat}(y) \wedge y^+ = x))$$

Demostración

Sea $v = \{ x \in \omega : x = \varnothing \vee \exists y\, (y \in \omega \wedge x = y^+)\}$

Entonces $\varnothing \in v$ y $x \in v \Rightarrow x^+ \in v$ luego v es un subconjunto inductivo de ω y por el principio de inducción $v = \omega$

[8-23] Proposición

ZF $\vdash \forall y\ (\text{Nat}(y) \rightarrow \text{Tran}(y))$

Demostración

Sea $a = \{y \in \omega : \forall x\ (x \in y \rightarrow x \subset y)\}$. Veamos que a es inductivo. Es trivial que $\varnothing \in a$, pues **ZF** $\vdash \forall x\ (x \in \varnothing \rightarrow x \subset \varnothing)$ ya que por el axioma del vacío el antecedente es falso. Sea ahora $y \in a$. Hay que ver que $y^+ \in a$. En efecto, se verifica

$$x \in y^+ = y \cup \{y\} \Rightarrow x \in y \ \vee x = y \Rightarrow x \subset y.$$

Luego $a = \omega$.

[8-24] Proposición

ZF $\vdash \forall x\ (\text{Nat}(x) \rightarrow x \notin x)$

Demostración

Sea $a = \{x \in \omega : x \notin x\}$. Veamos que a es inductivo. Claramente $\varnothing \notin \varnothing$. Veamos que si $y \in a$ entonces $y^+ \in a$. Sea $y \in a$ y supongamos que $y^+ \notin a$. Entonces debe ser $y^+ \in y^+$, esto es $y \cup \{y\} \in y \cup \{y\}$. Luego $y \cup \{y\} \in y$ o bien $y \cup \{y\} = y$. Como y es transitivo por ser natural, en el primer caso $y \cup \{y\} \subset y$, luego $y \in y$. En el segundo caso también $y \in y$ pues $y \in \{y\}$. En cualquiera de los dos llegamos a una contradicción. Por tanto debe ser $y^+ \notin y^+$ y entonces a es inductivo y coincide con ω.

[8-25] Proposición

ZF $\vdash \forall x\ (\text{Nat}(x) \wedge \text{Nat}(y) \wedge x^+ = y^+ \rightarrow x = y)$

Demostración

De $x \cup \{x\} = y \cup \{y\}$ se deduce $(x \in y \vee x = y) \wedge (y \in x \vee y = x)$

Si fuera $x \neq y$ sería $x \in y$ y también $y \in x$.Como x es transitivo se tendría $x \in x$, contra la proposición anterior.

A continuación nos proponemos mostrar una fórmula que represente adecuadamente la suma. La idea es la siguiente: decir $3 + 4 = 7$ significa que hay una función como la del esquema siguiente :

$$\begin{aligned} 0 &\rightarrow 3 \\ 1 &\rightarrow 4 \\ 2 &\rightarrow 5 \\ 3 &\rightarrow 6 \\ 4 &\rightarrow 7 \end{aligned}$$

Expresaremos esta idea intuitiva en el lenguaje de la teoría de conjuntios.
El axioma de las partes permite construir la noción de par ordenado, de producto cartesiano y de función. La definición de par ordenado (históricamente importante por reducir la teoría de relaciones a la teoría de conjuntos) se debe a Kuratowski.

[8-26] Definición

$$\langle x, y\rangle \equiv \{\{x\}, \{x, y\}\}$$

La siguiente proposición muestra que esta definición es adecuada para obtener el comportamiento deseado de los pares ordenados.

[8-27] Proposición

$$\mathbf{ZF} \vdash \forall x \forall y \forall u \forall v \ (\langle x, y\rangle = \langle u, v\rangle \rightarrow x = u \wedge y = v)$$

Demostración
Basta considerar en un razonamiento por casos las diferentes alternativas posibles consecuencia de la igualdad $\{\{x\}, \{x, y\}\}=\{\{u\}, \{u, v\}\}$.

Aplicando el axioma de separación y el axioma de las partes se asegura la existencia del producto cartesiano.

[8-28 Definición

$$u \times v \equiv \{z \in \mathcal{P}\,\mathcal{P}\,(u \cup v) : \exists x \exists y \ (x \in u \wedge y \in v \wedge z = \langle x, y\rangle)\}$$

La siguiente definición expresa que w es una función de u en v

[8-29] Definición

$$Fun(w, u, v) \equiv w \subset u \times v \wedge \forall x \ (x \in u \rightarrow \exists! y \ (y \in v \wedge \langle x, y\rangle \in w))$$

Con esto estamos en disposición de considerar la fórmula que expresa la suma :

[8-30] Definición

$$\begin{aligned} Sum(x, y, z) \equiv\ & Nat(x) \wedge Nat(y) \wedge Nat(z) \wedge \exists w \ (Fun(w, y^+, z^+) \wedge \\ & \wedge \langle 0, x\rangle \in w \wedge \\ & \wedge \forall u \ \forall v \ (\langle u, v\rangle \in w \wedge u \in y \rightarrow \langle u^+, v^+\rangle \in w) \wedge \\ & \wedge \langle y, z\rangle \in w \end{aligned}$$

[8-31] Proposición

ZF$\vdash \forall x(Nat(x) \rightarrow Sum(x, 0, x))$

Demostración

Basta observar que w={<0, x>} cumple trivialmente todas las condiciones

[8-32] Proposición

ZF$\vdash \forall x \forall y \forall z \forall z' (Sum(x, y, z) \wedge Sum(x, y, z') \rightarrow z = z')$

Demostración

De $Sum(x, y, z) \wedge Sum(x, y, z')$ se deduce la existencia de funciones w y w'. Es inmediato ver que w''= w $\cap$ w' es una función que verifica las condiciones necesarias en ambos casos. De $<y, z> \in w''$ y $<y, z'> \in w''$ se deduce z = z' por la condición de función.

[8-33] Proposición

ZF$\vdash \forall x \forall y \forall z (Nat(x) \wedge Nat(y) \wedge Nat(z) \wedge Sum(x, y, z) \rightarrow Sum(x, y^+, z^+))$

Demostración

Sea w la función que existe por Sum(x, y, z). Entonces w'= w $\cup$ $\{<y^+, z^+>\}$ es la función adecuada para $Sum(x, y^+, z^+)$

Obsérvese que

1. De Nat(y) y Nat(z) se deduce $Nat(y^+)$ y $Nat(z^+)$ por [8-16]
2. De $<0, x> \in w$ se deduce $<0, x> \in w'$
3. Si $<u, v> \in w' \wedge u \in y^+$ entonces se verifica una de las dos situaciones siguientes: o bien, $<u, v> \in w \wedge u \in y$ en cuyo caso $<u^+, v^+> \in w$ y por tanto $<u^+, v^+> \in w'$,o bien, $u = y^+$ $v = z^+$

[8-34] Proposición

ZF$\vdash \forall x \forall y (Nat(x) \wedge Nat(y) \rightarrow \exists! z (Nat(z) \wedge Sum(x, y, z)))$

Demostración

Por inducción sobre $\varphi(y) = \exists z \ Nat(z) \wedge Sum(x, y, z)$. Pues $\varphi(\varnothing)$ es consecuencia de Sum(x, 0, x). Y de $\varphi(y)$ se deduce $\varphi(y^+)$ viendo que $Sum(x, y, z) \rightarrow Sum(x, y^+, z^+)$

La unicidad es consecuencia de [8-32]

Un tratamiento análogo permite interpretar el producto

[8-35] Definición

$Prod(x, y, z) \equiv Nat(x) \wedge Nat(y) \wedge Nat(z) \wedge \exists w (Fun(w, y^+, z^+) \wedge$

$\wedge$ <0, 0> $\in$ w $\wedge$
$\wedge$ $\forall u \forall v \forall v'$ (<u, v> $\in$ w $\wedge$ u $\in$ y $\wedge$ Sum(v , x, v') $\rightarrow$ <u^{+},$v^{'}$> $\in$ w) $\wedge$
$\wedge$ <y, z> $\in$ w

[8-36] Proposición

ZF $\vdash$ $\forall x$ (Nat(x) $\rightarrow$ Prod(x, 0, 0))

Demostración
Tomar w = {<x, 0, 0>}.

[8-37] Proposición

ZF $\vdash \forall x \forall y \forall z \forall z'$ (Prod(x, y ,z) $\wedge$ Prod(x, y, z') $\rightarrow$ z = z')

Demostración
Idéntica a [8-32]

[8-38] Proposición

ZF $\vdash$ $\forall x \forall y \forall z \forall z'$ (Nat(x) $\wedge$ Nat(y) $\wedge$ Nat(z) $\wedge$ Prod(x, y , z) $\wedge$ Sum(z, x , z') $\rightarrow$

$\rightarrow$ Prod(x, y^{+}, z'))

Demostración
Idéntica a [8-33].

[8-39] Proposición

ZF $\vdash$ $\forall x \, \forall y$ (Nat(x) $\wedge$ Nat(y) $\rightarrow \exists !z$ (Nat(z) $\wedge$ Prod(x, y, z))

Demostración
Idéntica a [8-34].

Nuestro propósito es construir una interpretación $\Gamma = (\gamma, g)$ de la aritmética de Robinson **Q** en la teoría de conjuntos **ZF** .
La fórmula γ que define el universo de la interpretación es :

$\gamma(x) \equiv \text{Nat}(x) \equiv \forall y$ (Ind(y) $\rightarrow x \in y$)

Para cada símbolo del lenguaje de **Q** necesitamos una fórmula adecuada del lenguaje de **ZF** que lo represente.
Obviamente las fórmulas adecuadas son

$\alpha_0(x) \equiv \forall z \, z \notin x \equiv x = \varnothing$

$\alpha_s(x,y) \equiv y = x^+ \equiv \forall z(z \in y \leftrightarrow z \in x \vee z = x)$
$\alpha_+(x,y,z) \equiv \text{Sum}(x , y, z)$
$\alpha_\cdot(x,y,z) \equiv \text{Prod}(x, y, z)$

Las condiciones de adecuación de la interpretación son

$\delta_0 \equiv \exists x\, \text{Nat}(x)$
$\delta_1 \equiv \exists!\, x\, \forall z\ z \notin x$
$\delta_2 \equiv \forall x\, (\text{Nat}(x) \rightarrow \exists! y\, (\text{Nat}(y) \wedge y = x^+)$
$\delta_3 \equiv \forall x\, \forall y\, (\text{Nat}(x) \wedge \text{Nat}(y) \rightarrow \exists! z\, (\text{Nat}(z) \wedge \text{Sum}(x , y, z))$
$\delta_4 \equiv \forall x\, \forall y\, (\text{Nat}(x) \wedge \text{Nat}(y) \rightarrow \exists! z\, (\text{Nat}(z) \wedge \text{Prod}(x, y, z))$

Todas se verifican en **ZF** : δ_0 por la proposición [8-16], δ_1 por la proposición [8-5], δ_2 es consecuencia de [8-25], δ_3 por [8-34] y δ_4 por [8-39]

Tenemos ahora que ver que los axiomas de **Q** se transforman en teoremas de **ZF** .
La traducción de la fórmula sx = 0 por Γ es (Véase § 5.2)

$\exists w_0\, \exists w_1\, (\, \alpha_0(w_0) \wedge (w_1 = x) \wedge \alpha_s(w_1, w_0)$

que es lógicamente equivalente en **ZF** a

$x^+ = \varnothing$

Por tanto la traducción del axioma Q1 : $\forall x\ sx \neq 0$ es equivalente a

$\forall x\, (\text{Nat}(x) \rightarrow x^+ \neq \varnothing)$

que es un teorema de **ZF** por verificarse **ZF** $\vdash \forall x\ x^+ \neq \varnothing$ (Prop. [8-13])
De forma análoga la traducción de Q2 : $\forall x\, (x \neq 0 \rightarrow \exists y\ sy = x)$ es equivalente a

$\forall x\, (\text{Nat}(x) \wedge x \neq \varnothing \rightarrow \exists y\, (\, \text{Nat}(y) \wedge y^+ = x)$

que es un teorema de **ZF** (Prop. [8-22])
La traducción de Q3 : $\forall x \forall y\, (sx = sy \rightarrow x = y)$ es equivalente a

$\forall x \forall y\, (\text{Nat}(x) \wedge \text{Nat}(y) \wedge x^+ = y^+ \rightarrow x = y)$

que es un teorema de **ZF** como hemos demostrado en [8-25]
La traducción de Q4 : $\forall x\, (x + 0 = x)$ es equivalente a

$\forall x\, (\, \text{Nat}(x) \rightarrow \text{Sum}(x, 0, x)\,)$

que es un teorema de **ZF** como hemos señalado en [8-31]
La traducción de Q5 : $\forall x \forall y\, (x + sy) = s(x + y)$ es equivalente a

$\forall x \forall y \forall z\, (\text{Nat}(x) \wedge \text{Nat}(y) \wedge \text{Nat}(z) \wedge \text{Sum}(x, y, z) \rightarrow \text{Sum}(x, y^+, z^+)$

que es un teorema de **ZF** como hemos señalado en [8-33]
La traducción de Q4 : $\forall x\ x \cdot 0 = 0$ es equivalente a

$\forall x(\, \text{Nat}(x) \rightarrow \text{Prod}(x, 0, 0)\,)$

que es un teorema de **ZF** como hemos visto en [8-36]
La traducción de Q5 : $\forall x \forall y\ x \cdot sy = x \cdot y + x$ es equivalente a

$\forall x \forall y \forall z\, (\text{Nat}(x) \wedge \text{Nat}(y) \wedge \text{Nat}(z) \wedge \text{Prod}(x, y, z) \wedge \text{Sum}(z, x, z') \rightarrow \text{Prod}(x, y^+, z')$

que es un teorema de **ZF** como hemos señalado en [8-38]

Hemos construido así una interpretación de **Q** en **ZF** . (O más precisamente, en una extensión por definiciones de una subteoría de **ZF**). Lo que asegura, si aceptamos que **ZF** es consistente, el siguiente

[8-40] Teorema

ZF es inseparable

Observación

La axiomatización empleada *no* es una axiomatización finita ; el esquema de axiomas de separación consta de infinitas instancias. La utilización de un fragmento de la teoría de conjuntos finitamente axiomatizable (por ejemplo NW) tiene la ventaja añadida de ser una extensión finita de la teoría de una relación binaria, esto es, la teoría $\mathrm{Con}_{\sigma}(\varnothing)$ siendo $\sigma = \{R\}$ con R un símbolo de predicado binario. Por el teorema de las extensiones finitas [4-33], de la indecidibilidad de la teoría de conjuntos se deduciría como corolario inmediato que la teoría de una relación binaria es indecidible. (Véase un resultado más fuerte en § 10.1)

Nota

La teoría **ZF** no tiene modelos finitos. Si n y m son las representaciones conjuntistas de dos naturales distintos n y m, no es complicado demostrar por inducción metamatemática que $\mathsf{n} \neq \mathsf{m}$.

Sin embargo si consideramos la fórmula $k_{=1} \equiv \forall x \forall y\ (x = y)$, cuyos modelos constan de un único elemento, y formamos la teoría Con({N, $k_{=1}$}), obtenemos una teoría consistente y completa, pues sus modelos, $\mathsf{A} = (A; E)$, constan de un dominio con un único elemento $A = \{p\}$ y donde E es la relación vacía, pues, como consecuencia del axioma N, se verifica que $p \notin p$ (más precisamente: (p, p) no está en la relación E). Es decir, la teoría tiene, salvo isomorfismos, un único modelo. Esta teoría es, por tanto, decidible.

También la teoría Con({W, $k_{=1}$ }) es consistente y completa. Sus modelos constan de un único elemento p tal que $p \in p$. Es por tanto también decidible.

Incluso si debilitamos el axioma W y consideramos

W1 $\quad \forall x\ \forall y\ \forall z\ (x \in \mathsf{W}yz \rightarrow x \in y \vee x = z)$

W2 $\quad \forall x\ \forall y\ \forall z\ (x \in y \vee x = z \rightarrow x \in \mathsf{W}yz)$

la situación es similar.

Los modelos de la teoría Con({N, W1, $k_{=1}$}) tienen un único elemento p tal que $p \notin p$. La teoría es consistente y completa y por tanto decidible.

Si consideramos

$$\beta \equiv \forall x \forall y\ (x \neq \varnothing \wedge y \neq \varnothing \rightarrow x = y)$$

entonces la teoría Con({N, W2, β}) es consistente y completa y por tanto decidible. Sus modelos constan de dos elementos {p, q} tales que $p \notin p$, $q \notin p$, $p \in q$, $q \in q$ y $p \cup \{q\} = q \cup \{p\} = q$.

En consecuencia, **Q** no es interpretable en estas teorías más débiles (pues en tal caso serían esencialmente indecidibles). Por tanto la teoría NW es mínima en este sentido.
Obsérvese que si añadimos a NW el axioma $k_{=1}$ obtenemos una teoría inconsistente, pues el axioma N asegura la existencia de un conjunto sin elementos, y el axioma W asegura la existencia de $\varnothing \cup \{\varnothing\}$ que verifica $\varnothing \in \varnothing \cup \{\varnothing\}$. Por consiguiente, sería $\varnothing \neq \varnothing \cup \{\varnothing\}$, en contradicción con $k_{=1}$.

9. INSEPARABILIDAD FINITA DEL CÁLCULO DE PREDICADOS DE PRIMER ORDEN

9.1 Indecidibilidad e inseparabilidad finita del cálculo de predicados

La indecidibilidad del cálculo de predicados de primer orden fue demostrada en primer lugar por Church en 1936 [6] como consecuencia de la indecidibilidad de una teoría aritmética finitamente axiomatizable. Poco después Turing [62] obtuvo el resultado reduciendo un problema indecidible sobre máquinas "de Turing" al problema de decisión del cálculo de predicados. La demostración de Turing utilizaba una representación de la semántica del programa de una máquina mediante una fórmula del cálculo de predicados. Esta idea fue utilizada por Büchi [3] para obtener de forma más sencilla una prueba de la indecidibilidad del cálculo de predicados de primer orden. En este apartado simplificamos algo más la prueba, según sugerencia de J. F. Prida, utilizando máquinas de registros y aprovechando un teorema de Minsky [36] que asegura la existencia de una máquina de *dos* registros que simula el comportamiento de máquinas con cualquier número de registros. Al tratarse de una máquina con únicamente dos registros la codificación del comportamiento de la máquina mediante fórmulas del cálculo de predicados se simplifica notablemente. La técnica permite obtener no sólo un resultado de indecidibilidad sino el más fuerte de inseparabilidad finita.

Consideraremos la clase de máquinas que, comenzando con los registros vacíos, paran, y la clase de máquinas que finalmente tienen un comportamiento cíclico, y que por lo tanto no pararán nunca. Mediante una codificación usual estos dos conjuntos de máquinas se corresponden con dos conjuntos de números naturales. Denominaremos a estos dos conjuntos de índices PARA y CICLA. El resultado básico es que los conjuntos PARA y CICLA son efectivamente inseparables

A continuación asociaremos a cada máquina de dos registros M de código n una fórmula α_M del lenguaje de predicados de primer orden sin identidad, verificando

$$n \in \text{PARA} \quad \Rightarrow \quad \alpha_M \text{ insatisfactible}$$
$$n \in \text{CICLA} \quad \Rightarrow \quad \alpha_M \text{ finitamente satisfactible}$$

Esta asociación será efectiva lo que permite asegurar la existencia de una función computable que represente dicha transformación. La proposición [3-11] nos permite concluir que el conjunto de fórmulas insatisfactibles y el conjunto de fórmulas finitamente satisfactibles son efectivamente inseparables. En consecuencia, las fórmulas insatisfactibles, las lógicamente válidas, las satisfactibles y las finitamente satisfactibles forman conjuntos indecidibles.

9.2 Máquinas de registros

La formalización del concepto intuitivo de algoritmo o procedimiento efectivo es condición previa a cualquier resultado negativo al problema de decisión. Una de las definiciones formales utiliza la noción de *máquina de registros*, establecida por Sheperdson y Sturgis en 1963.
A continuación se establece rápidamente una versión de estas máquinas. Un estudio más detallado puede encontrarse en el manual de Cutland [9] o en el de Ebbinghaus *et al*. [13] . En Minsky [36] se demuestra la equivalencia de este formalismo con el de las máquinas de Turing. Aceptaremos (Tesis de Church) que toda función computable puede ser calculada por una máquina de registros.
Las máquinas de registros presentan la ventaja de ser un modelo más parecido al de los computadores reales por lo que quizá su programación es más intuitiva que en las máquinas de Turing. Por otra parte, la codificación de la información de la máquina es algo más sencilla.

Instrucciones y programas

Una máquina de registros consta de una cantidad finita de posiciones de memoria R_1, ... , R_n , llamadas *registros*. En cada momento, el registro R_i contiene un número natural que denotamos r_i.
El comportamiento de la máquina viene determinado por un programa. Un programa es una secuencia finita numerada de instrucciones : I_1 ; ... ; I_k .
Cada instrucción pertenece a alguna de las clases siguientes :

I. $R_i \leftarrow R_i + 1$
II. IF R_i>0 THEN $R_i \leftarrow R_i$ - 1 ELSE GOTO I_j
III. GOTO I_j
IV. STOP

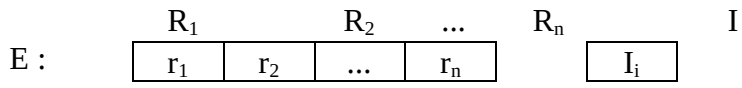
donde $i \in \{1, ..., n\}$ y $j \in \{1, ..., k\}$.

El significado de las anteriores instrucciones es, respectivamente.

I. Aumentar una unidad el contenido del registro R_i y pasar el control a la instrucción siguiente del programa
II. Si el contenido del registro R_i no es nulo disminuirlo en una unidad y pasar a la siguiente instrucción. Si el contenido del registro R_i es nulo dejarlo inalterado y pasar el control a la instrucción etiquetada I_j.
III. Saltar a la instrucción I_j.
IV. Parar la ejecución del programa.

Convendremos (sin pérdida de generalidad) que el programa empieza ejecutando la instrucción I_1, y que tiene una única instrucción STOP que es precisamente la última, esto es, I_k.

En cada momento el comportamiento de la máquina viene determinado por el estado de los registros y la instrucción a ejecutar, es decir por la *configuración*



Formalmente una configuración es una tupla de n + 1 elementos $<i, r_1, r_2, ..., r_k>$

Máquinas que paran y máquinas que ciclan

Si partimos de una configuración $E_1 = <1, r_1, r_2, ..., r_k>$ el programa determina una evolución de las configuraciones

$$E_1 \rightarrow E_2 \rightarrow E_3 \rightarrow ...$$

Indicaremos por $M : E \rightarrow E'$ la evolución de la máquina de la configuración E a la configuración E' en un único paso, y por $M : E \Rightarrow E'$ el cambio de la configuración E a la E' al cabo de un número indeterminado de pasos.

Puede ocurrir que el programa M al partir de una configuración E_1 pare al alcanzar cierta configuración E_t , (esto ocurre si se ha alcanzado la instrucción I_k : `STOP`), lo que indicamos por

$$M : E_1 \Rightarrow E_t \text{ para}$$

o bien

$$M : E_1 \Rightarrow \text{para}$$

si no se necesita especificar la configuración final.

Puede ocurrir que el programa no pare nunca, lo que indicamos por

$$M : E_1 \Rightarrow \infty$$

Un caso particular de esta situación se da cuando tras alcanzar cierta configuración el programa vuelve a alcanzarla, con lo que hay un número finito de configuraciones que se repiten cíclicamente. Indicamos esta situación por

$$M : E_1 \Rightarrow \text{cicla}$$

Para una máquina M de dos registros que parte de la configuración inicial $<1, 0, 0>$ utilizaremos las notaciones

$$M : <1, 0, 0> \Rightarrow \text{para}$$
$$M : <1, 0, 0> \Rightarrow \infty$$
$$M : <1, 0, 0> \Rightarrow \text{cicla}$$

Diremos que una máquina de registros M calcula la función $f : \omega \rightarrow \omega$ si partiendo de la configuración $<1, x, 0,...>$ para en la configuración $<k, x, f(x), ... >$, esto es si

$$M : <1, x, 0,...> \Rightarrow <k, x, f(x), ... > \text{ para}$$

Codificación de máquinas de registros

Por un procedimiento estándar de gödelización podemos asociar a una máquina de registros un único número natural. Para ello podemos asociar a cada instrucción del programa un número según la tabla

Instrucción	*Código*
$R_i \leftarrow R_i + 1$	2^i
IF R_i>0 THEN $R_i \leftarrow R_i$-1 ELSE GOTO I_j	$2^i \cdot 3^j$
GOTO I_j	5^j
STOP	7

y al programa M de instrucciones

$$I_1 ; ... ; I_k$$

podemos asociarle el número

$$\prod_{i=1}^{k} p_i^{\#I_i}$$

siendo p_i el i-ésimo número primo, o sea, $p_1 = 2$, $p_2 = 3$, ... , y $\#I_i$ el código de la instrucción I_i.

Por ejemplo, el código del programa

I_1 : IF R_1 > 0 THEN $R_1 \leftarrow R_1$ - 1 ELSE GOTO I_4
I_2 : $R_2 \leftarrow R_2$ + 1
I_3 : GOTO I_1
I_4 : STOP

es el número $2^{2\cdot 3^4} \cdot 3^{2^2} \cdot 5^5 \cdot 7^7$

La obtención del programa a partir de su código es posible en virtud del teorema fundamental de la aritmética que afirma la descomposición de un número entero mayor que 1 en sus factores primos de forma única.
Es fácil observar que la aplicación es inyectiva (nótese que la primera instrucción es la numerada como I_1) y que tanto la codificación como la decodificación se realizan efectivamente.
Podemos considerar así efectivamente enumeradas las máquinas de registros y referirnos a la máquina de código n como M_n.

9.3 Teorema de Minsky

Las máquinas consideradas tienen un número indeterminado de registros. Veamos que la potencia de cálculo de la máquina no se reduce si reducimos el número de registros a dos. Concretamente veremos que el comportamiento de una máquina de registros

arbitraria puede simularse mediante una máquina con sólo dos registros, en el sentido que se indica a continuación (cf. [36]).

En primer lugar nótese que un programa para una máquina de registros es un objeto finito : únicamente hace referencia a una cantidad finita de registros. El contenido de un cierto estado de tales registros

R_1	R_2		R_k
r_1	r_2	...	r_k

puede codificarse por el número

$$s_E = \prod_{i=1}^{k} p_i^{r_i}$$

donde p_i es el *i*-ésimo número primo. Obsérvese que tanto la codificación como la decodificación pueden realizarse de forma efectiva.

Consideremos ahora un programa M de una máquina de n registros. A partir de M construiremos, de forma efectiva, un programa P para una máquina de dos registros verificando :

1º) Si el programa M parte del estado

E :

r_1	r_2	...	r_k

de código $s_E = \prod_{i=1}^{k} p_i^{r_i}$, y al cabo de uno o más pasos llega a un estado

E' :

r'_1	r'_2	...	r'_k

de código $s_{E'} = \prod_{i=1}^{k} p_i^{r'_i}$

entonces el programa P partiendo del estado

s_E	0

al cabo de cierto número de pasos alcanza el estado

$s_{E'}$	0

2º) Si la máquina de partida M no para, cuando parte de un estado

E :

r_1	r_2	...	r_k

de código s_E, entonces la máquina de dos registros construida P, cuando parte del estado

s_E	0

tampoco para.

3º) Si el programa M parte de un estado

E :

r_1	r_2	...	r_k

de código $s_E = \prod_{i=1}^{k} p_i^{r_i}$, y al cabo de cierto número de pasos para en el estado

E' :

r'_1	r'_2	...	r'_k

de código $s_{E'} = \prod_{i=1}^{k} p_i^{r'_i}$

entonces el programa P partiendo de

s_E	0

al cabo de cierto número de pasos para en el estado

$s_{E'}$	0

Intuitivamente se utiliza el primer registro para guardar la codificación del estado de la máquina M y el segundo registro se utiliza como registro de trabajo.

Para construir la máquina de dos registros P que simula M basta determinar segmentos de programa de P que simulen las operaciones elementales de M. La "compilación" del programa de M consistirá en la "compilación" de cada instrucción de M. Es decir se realiza una simulación "paso a paso".
Basta estudiar, por lo tanto, cómo simular las instrucciones elementales de tipo I y II.

I) La instrucción $R_i \leftarrow R_i + 1$ tiene como efecto pasar del estado

...	r_i	...	r_k

al estado

...	$r_i + 1$	...	r_k

La máquina de dos registros que simula esta instrucción pasará del estado

$p_1^{r_1} \cdot \ldots\ p_i^{r_i} \ldots$	0

al estado

$p_1^{r_1} \cdot \ldots\ p_i^{r_i+1} \ldots$	0

El efecto obtenido es por tanto multiplicar el primer registro por p_i.

El programa deseado realizará las siguientes acciones :

- trasladar el contenido de R_1 a R_2
- devolver a R_1 p_i unidades por cada una de las que hay en R_2

El segmento de programa deseado es :

I_1 : IF $R_1 > 0$ THEN $R_1 \leftarrow R_1 - 1$ ELSE GOTO I_4
I_2 : $R_2 \leftarrow R_2 + 1$
I_3 : GOTO I_1
I_4 : IF $R_2 > 0$ THEN $R_2 \leftarrow R_2 - 1$ ELSE GOTO I_{6+p_i}
I_5 : $R_1 \leftarrow R_1 + 1$
I_6 : $R_1 \leftarrow R_1 + 1$
...
I_{4+p_i} : $R_1 \leftarrow R_1 + 1$
} p_i veces $R_1 \leftarrow R_1 + 1$
I_{5+p_i} : GOTO I_4

La instrucción I_{6+p_i} transfiere el control al inicio del segmento que traduce la instrucción siguiente del programa original.
Es inmediato comprobar que el anterior segmento de programa efectúa la transformación deseada.

II) A continuación debemos simular la instrucción

IF $R_i > 0$ THEN $R_i \leftarrow R_i - 1$ ELSE GOTO I_j

cuyo efecto sobre una configuración

...	r_i+1	...	r_k

es pasar a la configuración

...	r_i	...	r_k

mientras que si el contenido de R_i es nulo la configuración queda inalterada pasándose a la instrucción I_j
La máquina de dos registros deberá pasar, en el primer caso, del estado

$p_1^{r_1} \cdot \ldots p_i^{r_i+1} \ldots$	0

al estado

$p_1^{r_1} \cdot \ldots p_i^{r_i} \ldots$	0

Para ello basta dividir el primer registro entre p_i.
En el caso de ser R_i vacío el contenido del primer registro de P no será múltiplo de p_i y deberá quedar inalterado.
El segmento de programa que codifique este comportamiento deberá identificar si el contenido del primer registro es múltiplo de p_i, dividiendo, en su caso, entre p_i.
Por legibilidad consideraremos el caso $p_i = 3$. (En otros casos no hay diferencias significativas). Para desarrollar el programa basta tener en cuenta que todos los números pertenecen a una de las categorías 3m , 3m+1 , 3m+2
El programa actúa de la siguiente forma :

- Quitar una unidad del primer registro. Si se ha acabado no es múltiplo de 3
- Quitar otra unidad del primer registro. Si se ha acabado no es múltiplo de 3
- Quitar otra unidad del primer registro. Si se ha acabado era múltiplo de 3
- Al acabar el ciclo de tres aumentar una unidad en el segundo registro.
- Rehacer el contenido del primer registro copiando el segundo en el caso de ser múltiplo de 3, con lo que habremos dividido entre 3, o rehaciendo el contenido original en los otros dos casos

```
I1 : IF R1>0 THEN R1 ← R1 - 1 ELSE GOTO I14
I2 : IF R1>0 THEN R1 ← R1 - 1 ELSE GOTO I6
I3 : IF R1>0 THEN R1 ← R1 - 1 ELSE GOTO I12
I4 : R2 ← R2 + 1
I5 : GOTO I1
I6 : R1 ← R1 + 1
I7 : IF R2>0 THEN R2 ← R2 - 1 ELSE GOTO I18
I8 : R1 ← R1 + 1
I9 : R1 ← R1 + 1
I10 : R1 ← R1 + 1
I11 : GOTO I7
I12 : R1 ← R1 + 1
I13 : GOTO I6
I14 : IF R2>0 THEN R2 ← R2 - 1 ELSE GOTO I17
I15 : R1 ← R1 + 1
I16 : GOTO I14
```

La instrucción I_{17} transfiere el control a la instrucción del programa P donde empieza el código que traduce la instrucción siguiente. La instrucción I_{18} transfiere el control a la instrucción del programa P donde empieza el código que traduce la instrucción I_j.

Es fundamental observar que la construcción realizada es totalmente efectiva de forma que existe una función computable

$$h : \omega \rightarrow \omega$$

tal que dada una máquina M_x la máquina $M_{h(x)}$ es una máquina de dos registros que simula el comportamiento de M_x en el sentido descrito
Tenemos por tanto :

[9-1] Teorema

A toda máquina de registros M se le puede asociar de forma efectiva una máquina de dos registros P que simula las computaciones de M en el sentido siguiente :

- $M : E \rightarrow E'$ $\Rightarrow$ $P : (S_E, 0) \Rrightarrow (S_{E'}, 0)$
- $M : E \Rrightarrow E'$ para $\Rightarrow$ $P : (S_E, 0) \Rrightarrow (S_{E'}, 0)$ para
- $M : E \Rrightarrow \infty$ $\Rightarrow$ $P : (S_E, 0) \Rrightarrow \infty$

9.4 PARA y CICLA son efectivamente inseparables

Supondremos una enumeración de las funciones recursivas parciales con un argumento, esto es una biyección por la cual hacemos corresponder a cada $n \in \omega$, una función recursiva parcial de un argumento φ_n.

Los dos conjuntos efectivamente inseparables más sencillos son (ver [3-9]) :

$A_0 = \{x : \varphi_x(x) = 0\}$
$A_1 = \{x : \varphi_x(x) = 1\}$

Veremos a continuación que otros dos conjuntos, que denominaremos PARA y CICLA son efectivamente inseparables.
Para ello consideraremos una enumeración de los programas de máquinas de dos registros. Denotaremos por M_n el programa de número n.
Los conjuntos PARA y CICLA son conjuntos de índices de máquinas de dos registros que partiendo de la configuración inicial vacía, paran o bien repiten una configuración de forma cíclica, respectivamente, esto es,

$$PARA = \{x : M_x : <1, 0, 0> \Rrightarrow \text{para}\}$$
$$CICLA = \{x : M_x : <1, 0, 0> \Rrightarrow \text{cicla}\}$$

Por ejemplo el índice del programa

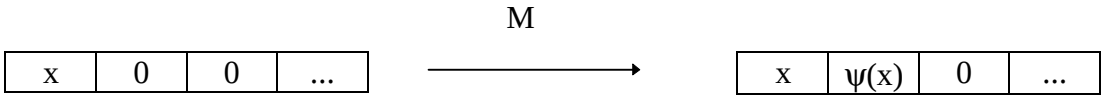
I_1 : $R_2 \leftarrow R_2 + 1$
I_2 : STOP

que es $2^{2^2}\cdot 3^7$, pertenece al conjunto PARA, mientras que el índice del programa

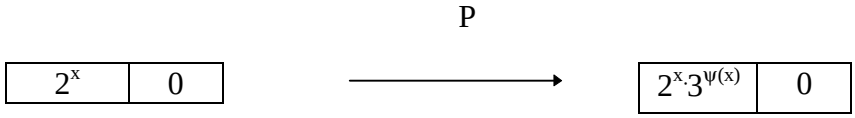
I_1 : $R_2 \leftarrow R_2 + 1$
I_2 : IF R_2>0 THEN $R_2 \leftarrow R_2$ - 1 ELSE GOTO I_4
I_3 : GOTO I_1
I_4 : STOP

que es $2^{2^2}\cdot 3^{2^{2\cdot 3^4}}\cdot 5^5\cdot 7^7$, pertenece a CICLA

Consideremos la función $\psi(x) = \varphi_x(x)$, que es claramente computable. Será por tanto una cierta φ_p. Esta función estará computada por un programa de una máquina de registros M



Por el teorema de Minsky hay una máquina de dos registros P que simula M, y se ha obtenido efectivamente a partir de M



A partir de P construiremos de forma efectiva una máquina de dos registros Q verificando :

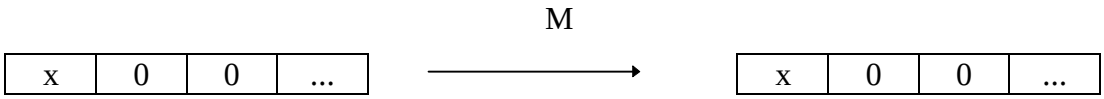
$x \in A_0 \Rightarrow Q : \langle 1, 0, 0\rangle \Rightarrow$ para
$x \in A_1 \Rightarrow Q : \langle 1, 0, 0\rangle \Rightarrow$ cicla

Debido a que la construcción realizada es efectiva el índice de esta máquina se obtiene a partir de x mediante una función computable.
Tendremos por tanto una función computable $f : \omega \rightarrow \omega$ tal que

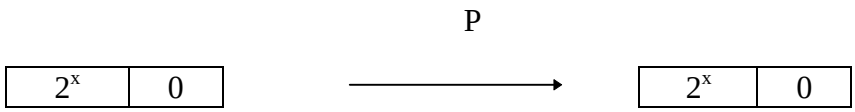
$x \in A_0 \Rightarrow f(x) \in$ PARA
$x \in A_1 \Rightarrow f(x) \in$ CICLA

La construcción de Q es sencilla.

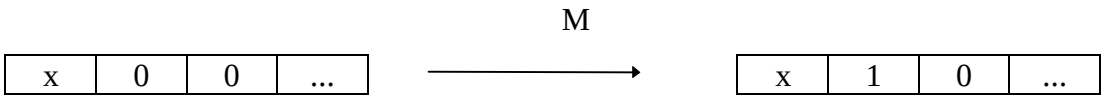
- Si $x \in A_0$ será $\psi(x) = \varphi_x(x) = 0$ luego



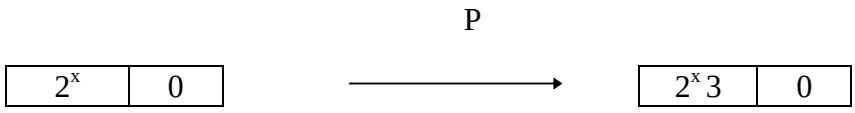
y por tanto



- Si $x \in A_1$ será $\psi(x) = \varphi_x(x) = 1$ luego



y por tanto

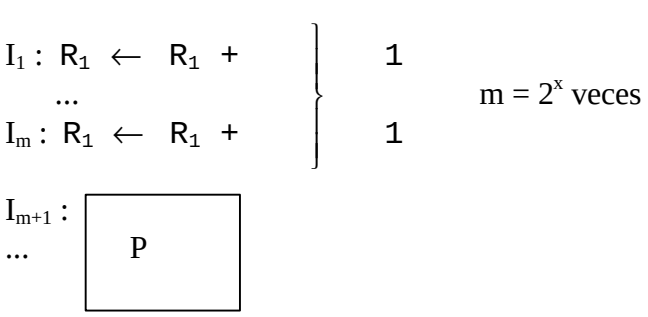


El comportamiento deseado de Q es que cicle cuando $x \in A_1$. Esto se conseguirá comprobando si el primer registro es múltiplo de 3 tras la ejecución de P partiendo de la configuración señalada.

El programa para Q realizará esencialmente las siguientes acciones :

- Introducir 2^x en el primer registro
- Ejecutar el programa de P (salvo la instrucción `STOP`)
- Si el contenido del primer registro es múltiplo de 3 ciclar, en caso contrario parar.

Es fácil comprobar que el programa adecuado es



I_{m+r} :

I_{m+r+1} : IF R_1>0 THEN $R_1 \leftarrow R_1$ - 1 ELSE GOTO I_{m+r+5}
I_{m+r+2} : IF R1>0 THEN $R_1 \leftarrow R_1$ - 1 ELSE GOTO I_{m+r+6}
I_{m+r+3} : IF R1>0 THEN $R_1 \leftarrow R_1$ - 1 ELSE GOTO I_{m+r+6}
I_{m+r+4} : GOTO I_{m+r+1}
I_{m+r+5} : GOTO I_{m+r+5}
I_{m+r+6} : STOP

De la construcción efectuada se deduce, por los teoremas [3-9] y [3-11] que

[9-2] Proposición

PARA y CICLA son efectivamente inseparables.

9.5 Inseparabilidad finita del cálculo de predicados

Sea M el programa de una máquina de dos registros. Asociaremos a M de forma constructiva una fórmula cerrada α_M del lenguaje de primer orden sin identidad de signatura σ = <0, s, K>, donde 0 es una constante, s un símbolo de función unitaria y K es un símbolo de predicado ternario.
La fórmula construida verificará :

M : <1, 0, 0> $\Rrightarrow$ ∞ $\Rightarrow$ α_M tiene modelo
M : <1, 0, 0> $\Rrightarrow$ cicla $\Rightarrow$ α_M tiene modelo finito
M : <1, 0, 0> $\Rrightarrow$ para $\Rightarrow$ α_M no tiene modelo

La idea es describir la semántica del programa mostrando la evolución de las configuraciones de la máquina. La configuración de una máquina de dos registros en un momento determinado de la ejecución del programa puede describirse como una terna de naturales <i, r_1, r_2> siendo i el número de instrucción a ejecutar, y r_1 y r_2 el contenido de los dos registros de la máquina.

Para cada $i \in \omega$ designaremos por $\underline{i}$ el término s...s0 (i veces s), con lo que $s\underline{i}$ designará ss...s0 (i+1 veces s)

Asignaremos a cada instrucción del programa una fórmula con dos variables libres x e y según la tabla siguiente :

instrucción	*fórmula*
I_i : $R_1 \leftarrow R_1 + 1$	$K\underline{i}xy \rightarrow Ks\underline{i}sxy$
I_i : $R_2 \leftarrow R_2 + 1$	$K\underline{i}xy \rightarrow Ks\underline{i}xsy$
I_i : IF R_1>0 THEN $R_1 \leftarrow R_1 - 1$ ELSE GOTO I_j	$(K\underline{i}0y \rightarrow K\underline{j}0y) \wedge (K\underline{i}sxy \rightarrow Ks\underline{i}xy)$
I_i : IF R_2>0 THEN $R_2 \leftarrow R_2 - 1$ ELSE GOTO I_j	$(K\underline{i}x0 \rightarrow K\underline{j}x0) \wedge (K\underline{i}xsy \rightarrow Ks\underline{i}xy)$
I_i : GOTO I_j	$K\underline{i}xy \rightarrow K\underline{j}xy$
I_i : STOP	$\neg K\underline{i}xy$

Así, por ejemplo, la fórmula asociada a la instrucción

$I_3 : R_2 \leftarrow R_2 + 1$

es

$Ksss0xy \rightarrow Kssss0xsy$

Es fácil observar que cada fórmula expresa satisfactoriamente la evolución de la configuración determinada por la correspondiente instrucción. En el caso de la instrucción STOP, la fórmula asociada indica que no se alcanza dicha configuración. (Recuérdese que se ha convenido que la instrucción STOP aparece una única vez en el programa como I_k)

Si el programa M consta de las instrucciones

$I_1; \ ... ; I_k$

mediante la tabla anterior se le asocian las fórmulas

$\alpha_1 ; ... ; \alpha_k$

En particular, la fórmula α_k será $\neg K\underline{k}xy$

Al programa M le asociaremos la fórmula cerrada

$\alpha_M \equiv \forall x \forall y(\alpha_0 \wedge \alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_k)$

siendo α_0 la fórmula $K\underline{1}00$

Veamos que la fórmula construida es adecuada a nuestros intereses.

[9-3] Lema

Si el programa M no para cuando parte de la configuración <1, 0, 0> entonces la fórmula α_M tiene un modelo

Demostración

Supongamos que el programa M no para tras partir de la configuración <1, 0, 0>. Veamos que la fórmula asociada tiene un modelo.
Sea $\mathsf{A} = (\omega\,;\, 0^{\omega},\, s^{\omega},\, K^{\omega})$ la estructura de universo los números naturales, con la constante cero, la función sucesor y la relación constituida por el conjunto de ternas de naturales

$$K^{\omega} = \{(i, a, b) \in \omega^3 : M : <1, 0, 0> \Rrightarrow <i, a, b>\}$$

Es fácil probar que $\mathsf{A} \vDash \alpha_M$:

Claramente $\mathsf{A} \vDash \alpha_0$, es decir, $\mathsf{A} \vDash K\underline{1}00$, pues $(1, 0, 0) \in K^{\omega}$.

También podemos probar, por distinción de casos que, para todo $i<k$, $\mathsf{A} \vDash \forall x \forall y\, \alpha_i$.

Lo veremos en el caso de que la instrucción sea $I_i : R_1 \leftarrow R_1 + 1$ (siendo análogo en los demás casos). En este caso la fórmula asociada es $\alpha_i \equiv Kixy \rightarrow Ksisxy$.
Basta ver que si para una interpretación de las variables x e y como los números a y b se verifica $\mathsf{A} \vDash K\underline{i}xy\ [a,b]$ entonces $\mathsf{A} \vDash Ks\underline{i}sxy\ [a,b]$.

Si $\mathsf{A} \vDash K\underline{i}xy\ [a,b]$ es que $(i, a, b) \in K^{\omega}$, o sea, la máquina alcanza la configuración <i, a, b>, con lo cual, al ser la instrucción $I_i : R_1 \leftarrow R_1 + 1$, la siguiente configuración es <i + 1, a + 1, b>, y por tanto $\mathsf{A} \vDash Ks\underline{i}sxy\ [a,b]$.

Finalmente $\mathsf{A} \vDash \forall x \forall y\, \alpha_k$, es decir, $\mathsf{A} \vDash \forall x \forall y \neg K\underline{k}xy$. En efecto, puesto que por hipótesis M no para cuando parte de la configuración <1, 0, 0>, no existen $a,b \in \omega$ tales que $M : <1, 0, 0> \Rrightarrow <k, a, b>$, esto es, no existen $a,b \in \omega$ tales que $(k, a, b) \in K^{\omega}$.
Por lo tanto, $\mathsf{A} \vDash \forall x \forall y \neg K\underline{k}xy$

Ejemplo
El siguiente programa no para (y no cicla).
Sea M el programa

I_1 : $R_2 \leftarrow R_2 + 1$
I_2 : IF R_1>0 THEN $R_1 \leftarrow R_1$ - 1 ELSE GOTO I_1
I_3 : STOP

La fórmula asociada al programa es
$\alpha_M \equiv \forall x \forall y\, (K\underline{1}00 \wedge (K\underline{1}xy \rightarrow K\underline{2}xsy) \wedge (K\underline{2}0y \rightarrow K\underline{1}0y) \wedge (K\underline{2}sxy \rightarrow K\underline{3}xy) \wedge \neg K\underline{3}xy)$

Es inmediato observar que partiendo de la configuración <1, 0, 0> este programa determina las siguientes configuraciones :

paso	I	R_1	R_2
1	1	0	0
2	2	0	1

3	1	0	1
4	2	0	2
5	1	0	2
6	2	0	3
7	1	0	3
8	2	0	4
9	1	0	4
	...	...	...

Puede comprobarse fácilmente que la fórmula asociada al programa, $\alpha_{M,}$ es válida en la estructura $\mathsf{A} = (\omega; 0^{\omega}, s^{\omega}, K^{\omega})$ siendo

$$K^{\omega} = \{(1, 0, j) / j \in \omega\} \cup \{(2, 0, j) / j \in \omega \backslash \{0\}\}$$

[9-4] Lema

Si el programa M cicla cuando parte de la configuración <1, 0, 0> entonces la fórmula α_M tiene un modelo finito

Demostración

Supongamos que el programa cicla tras partir de un estado. La máquina habrá evolucionado con las configuraciones

<1, 0, 0>
...
<t, a, b>
...
<t, a, b>
...

Hay una cantidad finita de configuraciones y luego se repiten periódicamente algunas de ellas. Sea $S = \{E_1, ..., E_d\}$ el conjunto finito da tales configuraciones. Esto es (i, a, b)$\in$ S syss M : <1, 0, 0> $\Rightarrow$ <i, a, b>. Nótese que al recorrerse únicamente d configuraciones el contenido de los registros es menor que d. Sea m el máximo entre k (número de la instrucción final) y d.

Podemos construir un modelo de α como la estructura

$$\mathsf{A} = (A ; 0^{A}, s^{A}, K^{A})$$

donde A = {0, 1, 2, ..., m} es un conjunto de naturales, 0^A el número cero, s^A es la función s^A = {(0, 1), (1, 2), (2, 3) , ... , (m, 0)} y K^A es el conjunto S de ternas de naturales.

Para ver que A es modelo de α basta ver que para cualquier asignación de variables v(x) = a v(y) = b, la interpretación (A ; v) satisface cada una de las fórmulas α_i

En efecto, supongamos que la instrucción i es

$$I_i : R_1 \leftarrow R_1 + 1$$

y la fórmula asociada

$$\alpha_i \equiv K\underline{i}xy \rightarrow Ks\underline{i}sxy$$

Si $(\mathfrak{A} ; v) \models K\underline{i}xy$ quiere decir que $<i, a, b> \in K^{\mathfrak{A}}$, con lo cual tras ejecutarse la instrucción I_i se obtiene la configuración $<i + 1, a + 1, b>$, lo que significa que se verifica $(\mathfrak{A} ; v) \models Ksisxy$

Análogo si fuera cualquiera de las demás instrucciones. Nos detendremos un momento en el caso de la instrucción STOP. Supongamos que se tiene la instrucción

I_k: STOP

Es claro que tal instrucción no se alcanza en ningún momento, pues estamos suponiendo que el programa cicla, y en tal caso pararía.

Por lo tanto, cualesquiera que sean $a, b \in \omega$, la terna $<k, a, b>$ no pertenece a S. Luego

$$(\mathfrak{A} ; v) \models \neg K\underline{k}xy$$

Ejemplo

El siguiente programa cicla

Sea M el programa

I_1 : $R_1 \leftarrow R_1 + 1$

I_2 : $R_2 \leftarrow R_2 + 1$

I_3 : IF R_2>0 THEN $R_2 \leftarrow R_2$ - 1 ELSE GOTO I_6

I_4 : $R_2 \leftarrow R_2 + 1$

I_5 : GOTO I_3

I_6 : STOP

Al partir de la configuración $<1, 0, 0>$ el programa evoluciona como indica la tabla siguiente :

paso	I	R_1	R_2
1	1	0	0
2	2	1	0
3	3	1	1
4	4	1	0
5	5	1	1
6	3	1	1
7	4	1	0
	...	...	...

Al alcanzar en el paso 6 una configuración igual a la alcanzada en el paso 3 el programa cicla. En este caso d = 5 y m = 6.

Es fácil ver que el modelo deseado tiene como universo A = {0, 1, 2, 3, 4, 5, 6}, la constante 0 designa el cero la función s el sucesor restringida a A y modificada en el valor 6 (con un valor irrelevante), y el predicado ternario K el conjunto

$K = \{(1, 0, 0), (2, 1, 0), (3, 1, 1,), (4, 1, 0), (5, 1, 1)\}$

Nótese que como el programa cicla en el paso 6, los únicos números que intervienen en las configuraciones son los índices de las instrucciones y números menores que 6.

[9-5] Lema

Si el programa M para cuando parte de la configuración $<1, 0, 0>$ entonces la fórmula α_M no tiene modelo

Demostración

Supongamos que, tras partir de la configuración $<1, 0, 0>$ el programa para. La máquina habrá evolucionado con las configuraciones

$<1, 0, 0>$

...

$<k, a, b>$

llegando tras un número finito de pasos a la instrucción I_k : STOP. Veamos que la fórmula α_M no tiene modelo.

En efecto, supongamos que una estructura $\mathsf{A} = (A ; 0^A, s^A, K^A)$ es un modelo de α_M.

Denotemos, para cada $i \in \omega$, por **i** el elemento $s^A...s^A0^A$ (i veces s^A). Así, por ejemplo, $\mathbf{0} \equiv 0^A$ y $\mathbf{1} \equiv s^A0^A$. Nótese que el término $\underline{i}$ viene designado por **i**.

La demostración consistirá en probar por inducción sobre n que si M alcanza la configuración $E_n = <i, a, b>$ entonces $(\mathbf{i, a, b}) \in K^A$. De aquí se concluye fácilmente que A no puede ser modelo de α_M pues, si M para, quiere decir que al cabo de cierto número de pasos se alcanza la configuración $<k, a, b>$ para ciertos $a, b \in \omega$ con lo cual $(\mathbf{k}, \mathbf{a}, \mathbf{b}) \in K^A$, luego sería $\mathsf{A} \vDash K\underline{k}\underline{x}y$ [**a, b**] en contradicción con que si A fuera modelo de α_M se deduciría $\mathsf{A} \vDash \forall x \forall y \neg K\underline{k}xy$

Sean pues $E_1, ... , E_d$ las configuraciones que alcanza M cuando parte de la configuración $E_1 = <1, 0, 0>$.

Para n = 1 es obvio pues $\mathsf{A} \vDash \alpha_M \Rightarrow \mathsf{A} \vDash \alpha_0 \Rightarrow \mathsf{A} \vDash K\underline{1}00 \Rightarrow (\mathbf{1}, \mathbf{0}, \mathbf{0}) \in K^A$.

Supongamos que para $n<d$ si $E_n = <i, a, b>$ entonces $(\mathbf{i}, \mathbf{a}, \mathbf{b}) \in K^A$ (hipótesis de inducción).

Demostraremos que lo mismo sucede para n + 1 por distinción de casos.

Consideremos el caso en que la instrucción I_i es $R_1 \leftarrow R_1 + 1$. La siguiente configuración es $E_{n+1} = <i + 1, a + 1, b>$.

Como $\mathsf{A} \vDash \forall x \forall y (K\underline{i}xy \rightarrow Ks\underline{i}sxy)$ y por hipótesis de inducción $(\mathbf{i}, \mathbf{a}, \mathbf{b}) \in K^A$, se sigue que $(\mathbf{i + 1}, \mathbf{a + 1}, \mathbf{b}) \in K^A$, que es lo que se quería demostrar.

Los demás casos son análogos (Obsérvese que si $n<d$ la instrucción I_n no puede ser la instrucción STOP).

Hemos obtenido el siguiente resultado :

[9-6] Proposición

Existe un procedimiento efectivo que asocia a cada máquina de dos registros M una fórmula α_M del lenguaje del cálculo de predicados de primer orden sin identidad de forma que :

a) M : <1, 0, 0> $\rightarrow$ para $\Rightarrow$ α_M no tiene modelo
b) M : <1, 0, 0> $\rightarrow$ cicla $\Rightarrow$ α_M tiene modelo finito
c) M : <1, 0, 0> $\rightarrow$ no para $\Rightarrow$ α_M tiene modelo

Si consideramos los conjuntos de números naturales

SAT = {n : α_n tiene modelo}
FINSAT = {n : α_n tiene modelo finito}
INSAT = {n : α_n no tiene modelo}

se tiene :

[9-7] Teorema

INSAT y FINSAT son efectivamente inseparables

Demostración

La construcción realizada, al ser efectiva asegura la existencia de una función computable

$f : \omega \rightarrow \omega$

tal que

$f(PARA) \subset INSAT$
$f(CICL) \subset FINSAT$

Como PARA y CICLA son efectivamente inseparables y f es computable entonces INSAT y FINSAT son efectivamente inseparables (Por [3-11])

[9-8] Corolario

INSAT no es recursivo

[9-9] Corolario

El conjunto de fórmulas satisfactibles del lenguaje de primer orden sin identidad es indecidible

[9-10] Corolario

El conjunto de sentencias lógicamente válidas de la lógica de primer orden es indecidible

Demostración

α es lógicamente válida syss $\neg\alpha$ es insatisfactible

Obsérvese que las fórmulas asociadas a las máquinas de registros por la construcción realizada son fórmulas del lenguaje sobre la signatura $\sigma_0 = \{0, s, K\}$. Consideremos la clase K_0 de todas las σ_0-estructuras y sea $Th(K_0)$ la teoría de dicha clase. Hemos demostrado que el conjunto de las sentencias insatisfactibles y el conjunto de las fórmulas finitamente satisfactibles son inseparables. Como para cada sentencia del lenguaje sobre σ se tiene

α insatisfactible $\Leftrightarrow$ $\neg\alpha \in Th(K_0)$

α finitamente satisfactible $\Leftrightarrow$ $\neg\alpha$ finitamente refutable

tenemos como consecuencia que los conjuntos $D_{Th(K_0)}$ y $FR_{Th(K_0)}$ son inseparables, o sea :

[9-11] Teorema

La clase K_0 es finitamente inseparable

Este resultado será el punto de partida para obtener la inseparabilidad finita de las teorías matemáticas usuales que se estudiarán en el siguiente capítulo

10. INSEPARABILIDAD FINITA DE DIVERSAS TEORÍAS

10.1 Inseparabilidad finita de la teoría de una relación binaria

Consideremos un lenguaje con un único símbolo de predicado binario P. Nos proponemos ver que la teoría formada por las sentencias lógicamente válidas en dicho lenguaje es finitamente inseparable. Esta teoría es la teoría de la clase de todas las estructuras de signatura {P}.

Sea K_0 la clase de todas las estructuras de la signatura $\sigma_0 = \{0, s, K\}$ siendo 0 un símbolo de constante, s una función monaria y K un símbolo de predicado ternario. La técnica de Büchi ha permitido demostrar que la teoría de la clase K_0 en un lenguaje sin igualdad es finitamente inseparable. No es difícil ahora codificar esta clase en una clase relacional de estructuras, esto es en una clase sobre una signatura en que únicamente aparezcan símbolos de predicado.
Sea $\sigma_1 = \{C, S, K\}$ una signatura formada por un símbolo de relación unitario $C \in \mathrm{PRED}^{(1)}$, un símbolo de relación binario $S \in \mathrm{PRED}^{(2)}$ y un símbolo de relación ternario $K \in \mathrm{PRED}^{(3)}$. Sea K_1 la clase de todas las σ_1-estructuras.
A cada σ_0-estructura $\mathsf{A} = (A; 0^A, s^A, K^A) \in \mathsf{K}_0$ podemos hacer corresponder de forma totalmente natural una σ_2-estructura $\mathsf{B} = (B ; C^B, S^B, K^B) \in \mathsf{K}_1$, siendo

$$B = A$$
$$C^B = \{0^A\}$$
$$S^B = \{(a, b) \in A \times A : s^A(a) = b\}$$
$$K^B = K^A$$

Así, podemos considerar la interpretación $\Gamma = (\gamma, g)$ con

$$\gamma(x_0) \equiv C(x_0) \vee \neg C(x_0)$$
$$\alpha_0(x_0) \equiv C(x_0)$$
$$\alpha_s(x_0, x_1) \equiv S\, x_0\, x_1$$
$$\alpha_K(x_0, x_1, x_2) \equiv R\, x_0\, x_1\, x_2$$

Es absolutamente trivial observar que $\mathsf{B}^\Gamma \approx \mathsf{A}$.
Tenemos pues una codificación fuerte de la clase K_0 en la clase K_1, El teorema [5-15] asegura que :

[10-1] Teorema

La teoría de la clase K_1 con igualdad es finitamente inseparable

Observación

Para expresar las condiciones de adecuación de la interpretación en este caso necesitamos que el lenguaje incluya la igualdad.

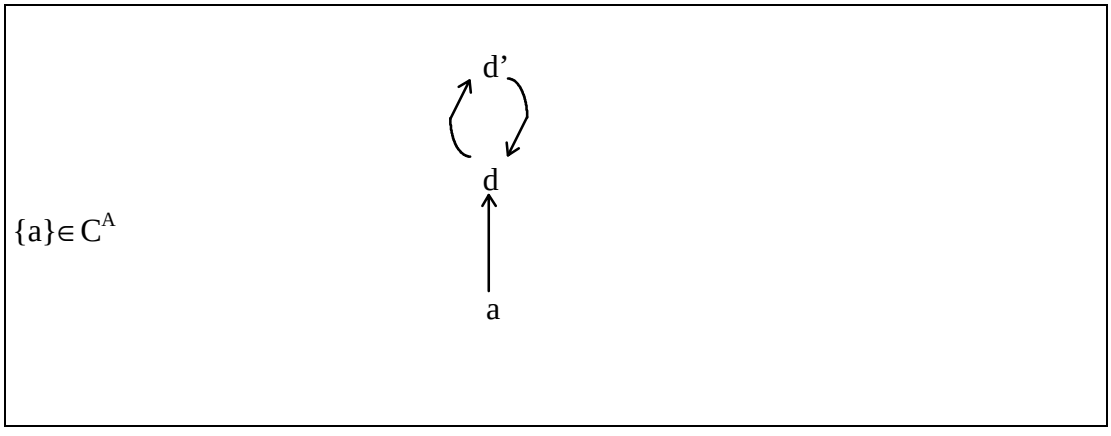
Habiendo visto que la clase K_1 de todas las σ_1-estructuras es finitamente inseparable codificaremos esta clase en la clase K_2 de todas las σ_2-estructuras, siendo $\sigma_2 = \{P\}$, con P un símbolo de predicado binario. Para ello, siguiendo la técnica del teorema [5-15], bastará asociar a cada σ_1-estructura A una σ_2-estructura B, de la cual podamos recuperar, mediante fórmulas de primer orden adecuadas, la estructura A, y de forma que si A es finita entonces B también sea finita.

El universo de la estructura B constará de una copia de los elementos del universo de A y unos nuevos elementos que describimos a continuación. A la vez determinaremos los pares de elementos relacionados en la relación P^B .

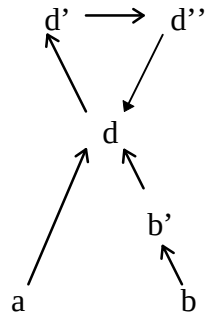
- Para cada elemento a del universo de A tal que $\{a\} \in C^A$ añadiremos dos nuevos elementos d y d' al universo de B y añadiremos los pares (a, d), (d, d') y (d', d) a la relación P^B.
- Para cada par de elementos $(a, b) \in S^A$ añadiremos cuatro nuevos elementos b', d, d' y d'' al universo de B y añadiremos los pares (a, d), (b, b'), (b', d), (d, d'), (d', d'') y (d'', d) a la relación P^B.
- Para cada terna $(a, b, c) \in K^A$ añadiremos siete nuevos elementos b', c', c'', d, d', d'', d''' al universo de B y los pares (a, d), (b, b'), (b', d), (c, c'), (c', c''), (c'', d), (d, d'), (d', d''), (d'', d''') y (d''', d) a la relación P^B.

(Se entiende que en cada momento los elementos introducidos son elementos nuevos distintos)

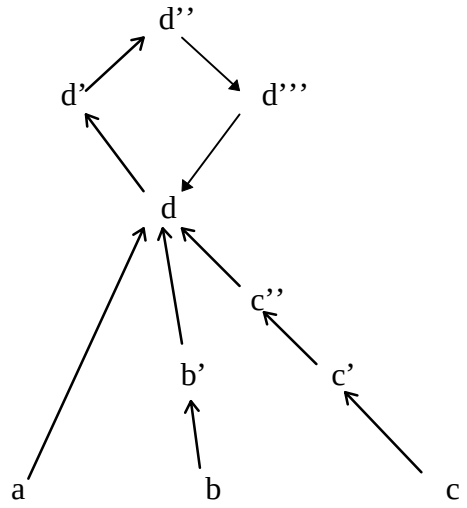
El significado de la construcción se pone de manifiesto claramente al ilustrarse con un gráfico.



$\{a, b\} \in R^A$



$\{a, b, c\} \in K^A$



Para caracterizar los elementos que son copia de elementos de A basta considerar la fórmula

$$\gamma(x) \equiv \neg\, \exists z\, Pzx$$

Se verifica

$$B \models \gamma\,[a] \;\Leftrightarrow a \in A$$

A continuación caracterizaremos los elementos que verifican las relaciones C^A, R^A y K^A. Para ello obsérvese, por ejemplo, que si $(a, b) \in R^A$, hay un circuito de tres elementos al que accede a directamente y b por medio de un elemento interpuesto. Análogas consideraciones en los otros casos. Las fórmulas adecuadas son, pues

$$\alpha_C(x) \equiv \exists v_1\, \exists v_2\, (Pxv_1 \wedge Pv_1v_2 \wedge Pv_2v_1)$$

$$\alpha_R(x, y) \equiv \exists v_1 \exists v_2 \exists v_3 \exists w\ (Pxv_1 \wedge Pv_1v_2 \wedge Pv_2v_3 \wedge Pv_3v_1 \wedge Pyw \wedge Pwv_1)$$

$$\alpha_K(x, y, z) \equiv \exists v_1\, \exists v_2\, \exists v_3\, \exists v_4\, \exists w\, \exists u_1\, \exists u_2\, (Pxv_1 \wedge Pv_1v_2 \wedge Pv_2v_3 \wedge Pv_3v_4 \wedge Pv_3v_1 \wedge \wedge Pyw \wedge Pwv_1 \wedge Pzu_1 \wedge Pu_1u_2 \wedge Pu_2v_1)$$

Se verifica que $B^\Gamma \approx A$

Tenemos pues que

[10-2] Teorema

La teoría de una relación binaria con igualdad es finitamente inseparable

Eliminación de la igualdad

En un momento ulterior será interesante considerar teorías sin el símbolo de igualdad. Veamos que podemos eliminar el signo de igualdad sin alterar significativamente para nuestras intenciones el poder expresivo del lenguaje. La idea básica es considerar un símbolo de predicado diádico E y reemplazar cada expresión del tipo x = y por la expresión Exy. De esta forma a cada fórmula α del lenguaje de la signatura $\sigma_2 = \{P\}$ con igualdad le asociamos una fórmula α^* del lenguaje de signatura $\sigma_3 = \{P, E\}$ sin igualdad. Naturalmente tendremos que imponer condiciones para que el comportamiento de la relación designada por E sea adecuado para referirse a la igualdad : esencialmente que E se comporte como una relación de equivalencia y que sea compatible con los predicados de la signatura. Interesará, pues, considerar la fórmula

$$\rho \equiv \forall x\, Exx \ \wedge \forall x \forall y\, (Exy \rightarrow Eyx) \wedge \forall x \forall y \forall z\, (Exy \wedge Eyz \rightarrow Eyz) \wedge$$
$$\wedge \forall x \forall y \forall u \forall v\, (Exu \wedge Eyv \wedge Pxy \rightarrow Puv)$$

Consideraremos la clase K_3 de σ_3-estructuras $\mathsf{B} = (B ; P^B, E^B)$ que son modelos de ρ, es decir, E^B es una relación de equivalencia congruente con P^B. Nos proponemos demostrar que la teoría de esta clase en un lenguaje sin igualdad, $Th(\mathsf{K}_3)^0$ es finitamente inseparable. Para ello basta observar el siguiente

[10-3] Lema

Para toda sentencia α de L_{σ_2} se verifica

α es satisfactible syss α^* es satisfactible.

Demostración

Claramente si $(A ; P^A)$ es un modelo de α, entonces la estructura $(A ; P^A, E^A)$ siendo $E^A = \{(a, a) : a \in A\}$ es modelo de α^*.

Recíprocamente, si $\mathsf{B} = (B ; P^B ; E^B)$ es un modelo de α^*, al ser E^B una relación de equivalencia congruente con P^B, podemos considerar el conjunto cociente $A = B/E$. Denotaremos por [b] la clase de un elemento $b \in B$. Podemos definir la σ_2-estructura $\mathsf{A} = (A, P^A)$ dada por

$$([b], [c]) \in P^A \quad \text{syss} \quad (b, c) \in P^B$$

Esta definición es independiente de los representantes, por ser $B \vDash \rho$.
Es inmediato ver que $B \vDash \alpha^* \Rightarrow A \vDash \alpha$

En consecuencia

[10-4] Lema

Para toda sentencia $\alpha \in L_{\sigma_2}$ se tiene

$$\alpha \in Th(K_2) \Rightarrow \alpha^* \in Th(K_3)^0$$
$$\alpha \in Fr(K_2) \Rightarrow \alpha^* \in Fr(K_3)^0$$

Demostración
Si $\alpha^* \notin Th(K_3)^0$ existe $B \in K_3$ tal que $B \vDash \neg\alpha^*$. (Obsérvese que $(\neg\alpha)^* = \neg(\alpha^*)$)
Por tanto existe $A \in K_2$ tal que $A \vDash \neg\alpha$, y así, $\alpha \notin Th(K_2)$. La otra implicación es análoga.

Esta reducción permite afirmar, por el teorema [3-11]

[10-5] Proposición

La teoría de la clase de estructuras con una relación binaria y una relación de equivalencia congruente con ella en un lenguaje sin igualdad es finitamente inseparable.

Esta teoría es una extensión finita (con el axioma ρ) de la teoría de la clase de estructuras con dos relaciones binarias. Por el teorema [4-46] se tiene

[10-6] Proposición

La teoría de la clase de estructuras con dos relaciones binarias sin igualdad es finitamente inseparable

Con una técnica idéntica a la utilizada anteriormente podemos codificar cada estructura de la clase de estructuras con dos relaciones binarias en una estructura de la clase K_2 de estructuras con una única relación binaria. Se tiene así :

[10-7] Teorema

La teoría de una relación binaria sin igualdad es finitamente inseparable

La inseparabilidad finita de la teoría de una relación binaria *sin igualdad* será el punto de partida básico para las demostraciones posteriores. Nótese que la técnica de eliminar la igualdad permite un tratamiento mucho más sencillo que el uso de Ershov de las funciones espectralmente representables (cf [13], [35])

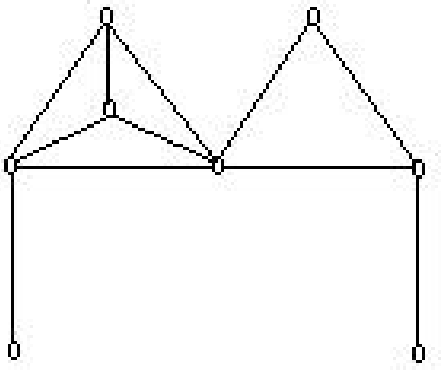
10.2 Inseparabilidad finita de la teoría de grafos

Consideremos el lenguaje con un único símbolo de predicado binario $\sigma_4 = \{R\}$ y los axiomas que expresan que R es una relación simétrica y antirreflexiva (ver § 4.4). La teoría resultante es la teoría de grafos. Consideraremos K_4 la clase de los modelos de dicha teoría. Veamos que la teoría sin igualdad de la clase K_4 es finitamente inseparable. Para ello bastará codificar cada σ_2-estructura en un grafo.
La interpretación se hará en la teoría de grafos sin igualdad, siguiendo una sugerencia de J. F. Prida. La utilidad de la construcción se observará en una posterior codificación. (Ver § 9.4)

[10-8]Teorema

La teoría de grafos sin igualdad es finitamente inseparable
Demostración
Aplicaremos el teorema de Rabin-Ershov construyendo una codificación de la clase de las estructuras con una relación binaria en la clase de los grafos. Haremos corresponder a cada estructura $\mathsf{A} = (A ; P^A)$ una estructura $\mathsf{B} = (B ; R^B)$ de la siguiente manera. El universo B constará de una copia de los elementos de A y otros nuevos elementos. A la vez que describimos estos nuevos elementos determinaremos los pares en la relación R^B. Para cada par $(a, b) \in P^A$ añadiremos seis nuevos elementos distintos $t^{ab}_1, \ldots, t^{ab}_6$, verificándose la relación P^B para los pares (a, t^{ab}_1), (t^{ab}_1, t^{ab}_2), (t^{ab}_1, t^{ab}_4), (t^{ab}_1, t^{ab}_5), (t^{ab}_2, t^{ab}_3),(t^{ab}_2, t^{ab}_4), (t^{ab}_2, t^{ab}_5), (t^{ab}_2, t^{ab}_6), (t^{ab}_3, t^{ab}_6), (t^{ab}_4, t^{ab}_5), (b, t^{ab}_3) y los pares inversos (para que la relación sea simétrica)

El significado de esta construcción se ilustra en la representación gráfica siguiente



a b

Sea S el conjunto de todos los nuevos elementos así introducidos. El universo B será $B = A \cup S$, y la relación R^B el conjunto de todos los pares introducidos.
Obsérvese que si la estructura de partida es finita también lo es el grafo construido.

En el grafo construido los elementos de A se caracterizan por no estar en un "triángulo". Los pares $(a, b) \in P^A$ pueden caracterizarse observando que el elemento a está conectado con el vértice de un "tetraedro"
Consideremos pues las fórmulas

$\tau_3 (x) \equiv \exists u \exists v (Rxu \wedge Ruv \wedge Rvx)$
"x es el vértice de un triángulo"
$\tau_4 (x) \equiv \exists u \exists v \exists w (Rxu \wedge Rxv \wedge Rxw \wedge Ruv \wedge Ruw \wedge Rvw)$
"x es el vértice de un tetraedro"

La interpretación $\Gamma = (\gamma, g)$ deseada viene dada por las fórmulas :

$\gamma(x_0) \equiv \neg\tau_3 (x)$
$\alpha_P(x_1, x_2) \equiv \exists x \exists y \exists z (Rx_1x \wedge Rxy \wedge Ryz \wedge Rzx_2 \wedge \tau_4(x))$

Es claro que

$B \vDash \gamma [m] \Leftrightarrow m \in A$
$B \vDash \gamma(x_1) \wedge \gamma(x_2) \wedge \alpha(x_1,x_2)\ [m, n] \Leftrightarrow (m, n) \in P^A$

Por lo tanto $B^\Gamma \approx A$, lo que completa la prueba.

10.3 Inseparabilidad finita de la teoría de retículos

Sea K_4 la clase de todos los retículos. Demostraremos la inseparabilidad finita de la teoría de retículos, Th(K_4), construyendo una interpretación de la clase K_3 de las estructuras con una relación binaria simétrica antirreflexiva (e.e. la clase de los grafos) en la clase K_4.

Sea A = (A, R) un grafo. Asociaremos al grafo A un retículo B = (B, $\leq^B$) y determinaremos una interpretación $\Gamma = (\gamma, g)$ de A en B de forma que la estructura inducida B^Γ sea isomorfa al grafo A. Para cada par de elementos (a, b) $\in R^A$ sea t_{ab} un nuevo elemento. (Consideramos $t_{ab} \equiv t_{ba}$). Sea $S = \{t_{ab} : (a, b) \in R^A\}$. El universo del retículo B será el conjunto $B = M \cup S \cup \{0,1\}$, siendo 0 y 1 nuevos elementos. En B definimos un orden parcial mediante :

i. $a \leq t_{ab}$
ii. $b \leq t_{ab}$
iii. $0 \leq x$, para todo $x \in B$
iv. $x \leq 1$, para todo $x \in B$

Claramente este orden parcial determina una estructura de retículo. Los átomos de este retículo son los elementos de M. Estos elementos pueden caracterizarse por la fórmula de primer orden :

$$\gamma(x) \equiv x \neq 0 \wedge \forall y\, (y \leq x \rightarrow (y = 0 \vee y = x))$$

Por otra parte la fórmula

$$\alpha_R(x, y) \equiv \exists u\, \exists v\, (x \neq y \wedge x \leq u \wedge y \leq u \wedge u \leq v \wedge u \neq v)$$

verifica claramente

$$\mathsf{B} \models \alpha_R [a, b] \Leftrightarrow (a, b) \in R^A$$

Así la interpretación Γ determinada por las fórmulas γ y α_R verifica que $\mathsf{A} \approx \mathsf{B}^\Gamma$. De esto se sigue que :

[10-9] Teorema

La teoría de retículos es finitamente inseparable

Nota

En la tabla final del artículo de Ershov *et al.* [15] se señala que la teoría de retículos distributivos atómicos finitos es decidible, resultado atribuido a Skolem (cf. [54]).

Modificando algo la demostración anterior podemos conseguir que el retículo asociado al grafo de partida sea un retículo distributivo atómico, de donde se deducirá que la clase de los retículos distributivos atómicos es finitamente inseparable, siendo por tanto la teoría finita de dicha clase una teoría indecidible, *en contra* de la indicación de Ershov .

[10-10]Teorema

La clase de los retículos distributivos atómicos es finitamente inseparable

Demostración

Sea K_3 la clase de todos los grafos. Asociaremos a cada $\mathsf{A} \in \mathsf{K}_3$ con más de un elemento, un retículo distributivo atómico. Para cada $(a, b) \in R^A$ sea $t_{ab} \equiv t_{ba}$ un nuevo elemento. Sea $s_{ab} = \{a, b, t_{ab}\}$. Al ser R^A una relación antirreflexiva y simétrica, el conjunto s_{ab} siempre tiene tres elementos distintos. Sea $S = \{s_{ab} / (a, b) \in R^A\}$ y B el cierre bajo uniones e intersecciones de $\mathsf{P}(A) \cup S$, donde $\mathsf{P}(A)$ es la familia de subconjuntos de A.

Claramente $\mathsf{B} = (B, \leq^B)$, donde la relación de orden es la inclusión, es un retículo distributivo atómico, siendo el cero $\varnothing$, y los átomos los conjuntos unitarios $\{a\}$ con $a \in A$. Nótese que no tenemos que procuparnos de demostrar la propiedad distributiva, por ser cierta para todo subconjunto de un retículo de conjuntos cerrado bajo unión e intersección.

Los átomos quedan caracterizados por la fórmula

$$\gamma(x) \equiv x \neq 0 \wedge \forall y\, (y \leq x \rightarrow (y = 0 \vee y = x))$$

Por tanto

$$\mathsf{B} \models \gamma\ [m] \Leftrightarrow m = \{a\}\ ,\ \text{con } a \in A$$

Consideremos ahora las fórmulas

$$\mathrm{Irr}(x) \equiv \neg\, \exists u\, \exists v\, (u \neq v \wedge u \cup v = z)$$

$$\mathrm{Cub}(x, y, z) \equiv x \cup y \leq z \wedge \neg \exists w\, (x \cup y \leq w \wedge w \leq z \wedge w \neq z)$$

donde hemos usado $\cup$ con el significado usual en teoría de retículos, para expresar la cota superior mínima. La fórmula Irr(x) expresa que el elemento es $\cup$-irreducible. La fórmula Cub(x, y, z) expresa que z cubre directamente a $x \cup y$.

Sea

$$\alpha_R(x, y) \equiv \exists z\, (\mathrm{Irr}(z) \wedge \mathrm{Cub}(x, y, z))$$

Los únicos elementos irreducibles de B son los conjuntos unitarios, $\varnothing$, y los elementos de S. Así

$$\mathsf{B} \models \alpha_R\ [m , n] \Leftrightarrow m = \{a\}, n = \{b\}\ (a, b) \in R^A$$

Se sigue que la correspondencia $a \rightarrow \{a\}$ es un isomorfismo de A en B^Γ. q.e.d.

Nota

La clase de los retículos relativamente pseudocomplementarios es decidible (cf. [15]). Por tanto la clase de los retículos relativamente pseudocomplementarios atómicos también es decidible. Es bien conocido que un retículo distributivo finito es relativamente pseudocomplementario y que cada retículo relativamente pseudocomplementario es distributivo. Así pues la clase de los retículos relativamente pseudocomplementarios atómicos es decidible pero la clase finita, que coincide con la clase de los retículos distributivos atómicos finitos, es indecidible.

Tenemos así un ejemplo de teoría decidible cuya teoría finita es indecidible.

10.4 Inseparabilidad finita de la teoría de anillos

Demostraremos a continuación la inseparabilidad finita de la teoría de anillos. Para ello aplicaremos el teorema de Rabin-Ershov partiendo de la clase de los grafos con más de un elemento y realizando una inmersión en cierta clase de anillos. Esta inmersión verificará las condiciones del teorema por lo que podremos concluir la inseparabilidad finita de la clase considerada. Se hará uso esencial del hecho de que la teoría de grafos *sin identidad* es finitamente inseparable. Los resultados presentados aquí fueron obtenidos por Mal'cev, Taitslin y Ershov (cfr. [15], [29], [31])

Recordemos alguna terminología y resultados relativos a la teoría de anillos. Consideremos un anillo unitario A con universo A y sea 1^A la unidad del anillo.

- Si a es un elemento del anillo y n un entero se define na como
  $na = a + a + ... + a$ si n es positivo (n veces a)
  $0a = 0$
  $na = -(a + a + ... + a)$ si n es negativo (|n| veces a)

Claramente $(mn)a = (ma)(na)$ y $na = (n1^A)a$

- Si la aplicación $f : Z \to A$ definida por $f(n) = n1^A$ es inyectiva, hay un único entero verificando $n1^A = 0$ y es n = 0. En tal caso f(Z) es un anillo isomorfo a Z

Si la aplicación $f : Z \to A$ definida por $f(n) = n1^A$ no es inyectiva, existe un menor entero p tal que $p1^A = 0$. En tal caso f(Z) es un anillo isomorfo a Z/pZ

- Si existe un entero positivo p tal que $p1^A = 0$ entonces el menor entero verificando tal condición se llama la *característica* del anillo

En tal caso para todo elemento $a \in A$ del anillo $pa=0$
Si no existe tal entero se dice que el anillo es de *característica cero*.

- Si el anillo no tiene divisores de cero (por ejemplo, si se trata de un cuerpo) la característica del anillo es cero o un número primo.
- Un subconjunto no vacío $I \subset A$ de un anillo conmutativo es un *ideal* si se verifica :
  1. $\forall a \in I \ \forall x \in A \ \ ax \in I$
  2. $\forall a, b \in I \ \ a - b \in I$
- Claramente la intersección de toda familia de ideales de un anillo es un ideal del anillo. Por lo que, dado un subconjunto cualquiera de elementos del anillo $M \subset A$, podemos considerar la familia de ideales que contienen a M. La intersección de dicha familia es el mínimo ideal que contiene a M. Se denomina el *ideal generado* por M. El ideal generado por un conjunto $M \subset A$ está formado por el conjunto de combinaciones lineales de elementos de M con coeficientes en A, es decir, expresiones de la forma $x_1m_1 + ... + x_km_k$ con $x_i \in A$, $m_i \in M$, $k \in \omega$
- Un ideal I de un anillo determina una relación de equivalencia en el anillo
  $a \equiv_I b \Leftrightarrow a - b \in I$
- Esta relación de equivalencia determina por tanto un conjunto cociente $A/\equiv_I$ que escribimos también A/I, al que se dota de estructura de anillo definiendo de forma natural la suma y producto de clases. El anillo cociente se denota por A/I
- Se llama *anulador* de un anillo A al conjunto $K = \{k \in A : \forall a \in A \ \ ka = 0\}$. El anulador de un anillo es un ideal del anillo.

Consideraremos en primer lugar la clase de anillos de característica p = 2.

Sea G = (G, R^G) un grafo con más de un elemento. Consideremos para cada elemento $a \in G$ un nuevo símbolo m_a y llamemos $M = \{m_a : a \in G\}$ y $T = G \cup M$
Sea P el conjunto de expresiones polinómicas finitas con coeficientes sobre el cuerpo {0, 1} engendrado por los elementos de T. Sus elementos son expresiones finitas de la forma

$$\Sigma\, d_{e_1, \dots, e_r, f_1, \dots, f_s}\, a_1^{e_1} \dots a_r^{e_r}\, m_1^{f_1} \dots m_s^{f_s}$$

donde $d_{e_1, \dots, e_r, f_1, \dots, f_s} \in \{0, 1\}$, $a_i \in G$, $m_j \in M$, y e_i, f_j naturales no todos nulos
Sea P la estructura de anillo sobre dicho conjunto definida de forma natural.
Consideremos los siguientes subconjuntos de P :

$A_1 = \{ u \cdot v \cdot w : u, v, w \in T\}$
$A_2 = \{u \cdot v - v \cdot u : u, v \in T\}$
$A_3 = \{u^2 : u \in G\}$
$A_4 = \{u \cdot v : (u, v) \in R^G\}$
$A_5 = \{u \cdot m_u : u \in G\}$

Sea I el ideal generado por $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$. Este ideal genera un conjunto cociente **B** = P/I con una estructura de anillo inducida que denotamos $\mathsf{G}^\star$ = P/I . Denotaremos por **u** la clase correspondiente al elemento $u \in P$, esto es, **u** = u + I $\in$ P/I.
Obsérvese que la construcción realizada asegura entre otras cosas que el anillo $\mathsf{G}^\star$ es unitario y conmutativo, que es de característica 2 y que el producto de tres elementos es cero. Además si el grafo G de partida es finito el anillo asociado $\mathsf{G}^\star$ también es finito.
Será útil considerar el conjunto de anuladores del anillo $\mathbf{K} = \{\mathbf{k} \in B : \forall y \in \mathbf{B} \quad \mathbf{k} \cdot y = \mathbf{0}\}$
Es claro que los elementos de **B** son de la forma **g** + **m** + **k** donde **g** es una suma de clases de elementos de G, **m** una suma de clases de elementos de M y $\mathbf{k} \in \mathbf{K}$.
El universo de la interpretación lo constituirán los elementos del conjunto

$\mathbf{D} = \{ \mathbf{a} + \mathbf{k} : a \in G , \mathbf{k} \in K\}$

Tenemos por tanto que caracterizar entre los elementos de **B** dichos elementos de **D** por una fórmula de primer orden. Para ello observemos que los elementos de la forma **g** + **k** con **g** suma de clases de elementos de G vienen caracterizados por la condición

$[U_1] \quad x \cdot x = 0$

La construcción realizada asegura que los elementos de A_5 pertenecen al ideal I. Por tanto, dado $a \in G$ se verifica que $\mathbf{a} \cdot \mathbf{m_a} = \mathbf{0}$ y $\mathbf{m_a}^2 \neq \mathbf{0}$; luego los elementos de D verifican la condición

$[U_2] \quad \exists y \, (x \cdot y = 0 \ \wedge \ y \cdot y \neq 0)$

Ahora bien, esta condición la verifican también los elementos de **K**. Para excluirlos basta imponer también la condición

$[U_3] \quad \exists y \ x \cdot y \neq 0$

Así pues, considerando la fórmula

$$\gamma(x) \equiv x \cdot x = 0 \wedge \exists y \, (x \cdot y = 0 \ \wedge \ y \cdot y \neq 0) \wedge (\exists y \ x \cdot y \neq 0)$$

se tiene

$$\mathbf{u} \in \mathbf{D} \quad \Leftrightarrow \quad \mathsf{G}^\star \vDash \gamma [\mathbf{u}]$$

A continuación caracterizaremos los pares $(\mathbf{a} + \mathbf{k}, \mathbf{b} + \mathbf{k'}) \in \mathbf{D}^2$ que representen elementos relacionados en el grafo, es decir el conjunto

$$\mathbf{H} = \{(\mathbf{a} + \mathbf{k}\ ,\ \mathbf{b} + \mathbf{k'}\ ) \in \mathbf{D}^2 : (a, b) \in R^G\}$$

Para ello observemos que dados a, b∈G, **k**, **k'**∈**K** si (a, b)∈R^G , como $A_4 \subset I$, se verifica que **a** · **b** = **0** y por tanto (**a** + **k**)(**b** + **k'**) = **0**. Tales pares verifican, pues, la condición

$[R_1]$ $x \cdot y = 0$

Ahora bien los pares del tipo (**a** + **k** , **a** + **k'**) también verifican $[R_1]$. Para eliminarlos observemos que **a** + **k** + **a** + **k'** ∈ **K** pero **a** + **k** + **b** + **k'**∉ **K.** Por lo tanto sólo los elementos de **H** verifican

$[R_2]$ $\exists z\ (x + y)\ z \neq 0$

Definiremos por tanto

$$\alpha_R\ (x, y) \equiv x \cdot y = 0 \wedge \exists z\ (x + y)\ z \neq 0$$

y se verificará

$$(\mathbf{u}, \mathbf{w}) \in \mathbf{H} \Leftrightarrow\ G^\star \vDash \alpha_R\ [\mathbf{u}, \mathbf{w}]$$

Hemos determinado la interpretación $\Gamma = (\varphi, \alpha_R)$ verificando $G^{\star\ \Gamma} = (\mathbf{D}, \mathbf{H})$

Además **K** define en **D** una relación de equivalencia **u** ~ **v** ⇔ **u** - **v** ∈**K** y determina un conjunto cociente **D**/**K** = {**a** : a∈G}. Análogamente en **H** tendremos **H**/**K** ={(**a** ,**b**) : (a , b) ∈ R^G}. Por lo que (**D**/**K**, **H**/**K**) ≈ G

La relación de equivalencia definida por **K** en **D** es una congruencia respecto **H**.

En efecto supongamos **a** ~ **a**' , **b** ~ **b**' y (a, b)∈R. Entonces

ab = **0**

a - **a**' = **k** ∈**K**

b - **b**' = **l** ∈**K**

Por tanto **a**' **b**' = (**a** - **k**)(**b** - **l**) = **ab** = **0**. Luego (a', b') ∈ R

Una fórmula sin identidad es válida en (**D**, **H**) si y solo si es válida en el cociente (**D**/**K**, **H**/**K**) por lo que para toda fórmula δ se verifica

$$G^{\star\ \Gamma} \vDash \delta \ \Leftrightarrow\ G \vDash \delta$$

es decir, G y $G^{\star\ \Gamma}$ son elementalmente equivalentes

Nota

Obsérvese aquí la importancia de la formulación fuerte del teorema de Rabin-Ershov utilizando la equivalencia elemental en vez de la isomorfía.

Tenemos por tanto :

[10-11] Teorema

La clase de los anillos conmutativos de característica 2 en los que el producto de tres elementos cualesquiera es cero es finitamente inseparable

Consideraremos ahora el caso de los anillos de característica p primo mayor que 2

Todo sigue un camino análogo. Asociaremos a cada grafo con más de un elemento un anillo conmutativo de característica p. Sea $\mathsf{G} = (G, R^G)$ un grafo con más de un elemento. Consideraremos para cada elemento $a \in G$ un nuevo símbolo m_a y llamaremos $M = \{m_a : a \in G\}$ y $T = G \cup M$

Sea P el conjunto de expresiones polinómicas finitas con coeficientes sobre el cuerpo {0, 1, ... , p-1} engendrado por los elementos de T. Sus elementos son expresiones finitas de la forma

$$\Sigma\, d_{e_1, \dots, e_r, f_1, \dots, f_s}\, a_1^{e_1} \dots a_r^{e_r}\, m_1^{f_1} \dots m_s^{f_s}$$

donde $d_{e_1, \dots, e_r, f_1, \dots, f_s} \in \{0,1,\dots, p-1\}$, $a_i \in G$, $m_j \in M$, y e_i, f_j naturales no todos nulos

Sea P la estructura de anillo sobre dicho conjunto definida de forma natural.

Consideremos los siguientes subconjuntos de P :

$A_1 = \{ u \cdot v \cdot w : u, v, w \in T\}$

$A_2 = \{u \cdot v - v \cdot u : u, v \in T\}$

$A_3 = \{u^2 : u \in G\}$

$A_4 = \{m_u \cdot m_v : (u, v) \in R^G\}$

$A_5 = \{u \cdot m_u : u \in G\}$

Sea I el ideal generado por $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$. y $\mathsf{G}^\star = \mathsf{P}/I$ el anillo cociente con la relación de equivalencia determinada por el ideal y **B** su universo. Sea el conjunto de anuladores del anillo $\mathbf{K} = \{\mathbf{k} \in B : \forall y \in \mathbf{B} \quad \mathbf{k} \cdot y = \mathbf{0}\}$.

Los elementos de **B** son de la forma **g** + **m** + **k** con **g** combinación de clases de elementos de G con coeficientes en {0,1,... , p-1}, **m** combinación de clases de elementos de M con coeficientes en {0,1,... , p-1}, y **k** un elemento de **K**.

Si **w** es un elemento de **B** de la forma d**a** + **k** con $a \in G$ verificará

[U1] $\mathbf{w}^2 = (d\mathbf{g} + \mathbf{k})^2 = 0$

[U2] $w \cdot \mathbf{m_b} \neq 0$ si $a \neq b$

Además es fácil observar que estas dos condiciones caracterizan a los elementos de la forma d**a** + **k** con $a \in G$, $\mathbf{u} \in \mathbf{K}$, $d \in \{0,1,\dots , p-1\}$,

Consideremos, pues, la fórmula

$$\gamma(x) \equiv\ x \cdot x = 0 \wedge \exists z\ \ x \cdot z = 0$$

De esta forma, los elementos del conjunto $D = \{d\mathbf{a} + \mathbf{k} : a \in G, d \in \{1, ..., p-1\}, \mathbf{k} \in \mathbf{K}\}$ verifican

$$u \in D \Leftrightarrow \mathsf{G}^\star \vDash \gamma\,[\mathbf{u}]$$

Caracterizaremos ahora los pares de la forma (d**a** + **k**, d'**b** + **k**') con $(a, b) \in R^G$. Sea $\mathbf{H} = \{ (d\mathbf{a} + \mathbf{k}, d'\mathbf{b} + \mathbf{k}') \in B / (a, b) \in R^G\}$, $d , d' \in \{1, ... p-1\}$

Se tendrá :

$\mathbf{m_a}^2 \neq 0$

$\mathbf{m_b}^2 \neq 0$

$\mathbf{m_a} \cdot \mathbf{m_b} = 0$

$(d\,\mathbf{a} + \mathbf{u}) \cdot \mathbf{m_a} = 0$

$(d'\mathbf{b} + \mathbf{k'}) \cdot \mathbf{m_b} = 0$

Tomemos pues

$$\alpha_R(x, y) \equiv \exists u\, \exists v\, (u \cdot u \neq 0 \wedge v \cdot v \neq 0 \wedge u \cdot v = 0 \wedge x \cdot u = 0 \wedge y \cdot v = 0)$$

Se verifica

$$(a, b) \in R \Rightarrow \mathsf{G}^\star \vDash \alpha_R\,[\mathbf{a}, \mathbf{b}]$$

Reciprocamente, supongamos que $\mathbf{a}, \mathbf{b} \in \mathbf{D}$, siendo $\mathbf{a} = d_1 \mathbf{c_1} + \mathbf{k_1}$, $\mathbf{b} = d_2 \mathbf{c_2} + \mathbf{k_2}$, con $d_1, d_2 \in \{1, \ldots, p-1\}$, $c_1, c_2 \in G$, $\mathbf{k_1}, \mathbf{k_2} \in \mathbf{K}$, y verifican $G^\star \vDash \alpha_R [\mathbf{a}, \mathbf{b}]$. Entonces existirán $\mathbf{u}, \mathbf{v} \in \mathbf{B}$, tales que

[1] $\mathbf{u}^2 = 0$
[2] $\mathbf{v}^2 = 0$
[3] $\mathbf{u} \cdot \mathbf{v} = 0$
[4] $(d_1 \mathbf{c_1} + \mathbf{k_1}) \cdot \mathbf{u} = 0$
[5] $(d_2 \mathbf{c_2} + \mathbf{k_2}) \cdot \mathbf{v} = 0$

De [4] y [5] se sigue que **u** y **v** son de la forma

$$\mathbf{u} = d_3 \mathbf{c_1} + d_4 \mathbf{m}_{\mathbf{c_1}} + d_5 \mathbf{k_3}$$
$$\mathbf{v} = d_6 \mathbf{c_2} + d_7 \mathbf{m}_{\mathbf{c_2}} + d_8 \mathbf{k_4}$$

Por [1] y [2] se deduce que

$$d_3 \neq 0$$
$$d_6 \neq 0$$

De [3] se deduce que

$$d_3 d_6 \mathbf{m}_{\mathbf{c_1}} \cdot \mathbf{m}_{\mathbf{c_2}} = 0$$

luego debe ser

$$\mathbf{m}_{\mathbf{c_1}} \cdot \mathbf{m}_{\mathbf{c_2}} = 0$$

y por lo tanto $(c_1, c_2) \in R^G$, $(\mathbf{a}, \mathbf{b}) \in H$ y $(a, b) \in R^G$.

Así pues hemos construido una interpretación

$$\gamma = \{\gamma(x) , \alpha_R(x , y)\})$$

de forma que

$$(G^\star)^\Gamma = (\mathbf{D}, \mathbf{H})$$

Sea ~ la relación de equivalencia definida en **D** mediante

$$\mathbf{w} \sim \mathbf{w}' \text{ syss existen } d \in \{1,..., p-1\} \ \ \mathbf{k} \in \mathbf{K} \text{ tales que } \mathbf{w}' = d\mathbf{w} + k$$

Esta relación es una congruencia respecto a **H**. En efecto, supongamos $(\mathbf{a}, \mathbf{b}) \in \mathbf{H}$. Entonces existen **u**, **v** tales que

$$\mathbf{u}^2 \neq 0$$
$$\mathbf{v}^2 \neq 0$$
$$\mathbf{u} \cdot \mathbf{v} = 0$$
$$\mathbf{a} \cdot \mathbf{u} = 0$$
$$\mathbf{b} \cdot \mathbf{v} = 0$$

Si suponemos

$$\mathbf{a} \sim \mathbf{a}'$$
$$\mathbf{b} \sim \mathbf{b}'$$

será

$$\mathbf{a}' = d_1 \mathbf{a} + \mathbf{k_1} \qquad \mathbf{k_1} \in \mathbf{K},\ d_1 \in \{1, \ldots, p-1\}$$
$$\mathbf{b}' = d_2 \mathbf{b} + \mathbf{k_2} \qquad \mathbf{k_2} \in \mathbf{K},\ d_2 \in \{1, \ldots, p-1\}$$

y por tanto

$$\mathbf{a}' \cdot \mathbf{u} = 0$$
$$\mathbf{b}' \cdot \mathbf{v} = 0$$

luego $(\mathbf{a}', \mathbf{b}') \in \mathbf{H}$

En consecuencia la estructura cociente (**D**/~, **H**/~) es isomorfa a G.
Igual que antes G^{Γ} y G serán elementalmente equivalentes y tenemos

[10-12] Teorema

La teoría de la clase de anillos de característica p primo en que el producto de tres elementos es nulo es finitamente indecidible.

Demostraremos ahora un resultado análogo para la clase de los anillos conmutativos unitarios.

[10-13] Teorema

La clase K_{ACUp} de los anillos conmutativos unitarios de característica p (p primo) es finitamente inseparable
Demostración
Asociaremos a cada anillo $\mathsf{A} = (A ; + , \cdot)$ conmutativo de característica p en el que el producto de tres elementos es cero un anillo conmutativo unitario $\mathsf{A}^{\star}$. Para ello consideraremos un nuevo elemento $e \notin A$ y haremos $e \cdot m = m \cdot e = m$ para $m \in A \cup \{e\}$.
El universo del anillo A será el conjunto de expresiones $\lambda_1 m_1 + ... + \lambda_n m_n \quad m_i \in A \cup \{e\}$, $\lambda_i \in \{0, 1, ... , p-1\}$.
Es inmediato que hemos construido un anillo unitario conmutativo en el que

$$u \in A \Leftrightarrow u^3 = 0$$

luego en este anillo los elementos de A están caracterizados por la fórmula

$$\gamma(x) \equiv x \cdot x \cdot x = 0$$

verificándose

$$\mathsf{A}^{\star} \vDash \gamma [u] \Leftrightarrow u \in A$$

De aquí se deduce inmediatamente el teorema.

Como corolario inmediato tenemos

[10-14] Teorema

La teoría de anillos es finitamente inseparable

10.5 Inseparabilidad finita de la teoría de grupos

Para demostrar la inseparabilidad finita de la teoría de grupos construiremos una inmersión de la clase de los anillos unitarios en la clase de los grupos. Para ello seguiremos una construcción, debida a Mal'cev (cf. [30], [31] y [32]), que permite construir, a partir de un anillo A, un grupo $\mathsf{A}^\star$, que llamaremos *grupo de Mal'cev asociado a* A. Veremos que a partir de un grupo con ciertas características podremos recuperar la estructura de anillo.

El grupo de Mal'cev asociado a un anillo

Sea $\mathsf{A} = (A; +^A, \cdot^A, 0^A, 1^A)$ un anillo unitario (abreviadamente (A; +, ·, 0, 1)).
Construiremos un grupo con la operación ∘, (suprimida a veces en la escritura, como es costumbre en la notación multiplicativa) y dos elementos distinguidos u_1, u_2 . Un grupo con tales elementos distinguidos puede llamarse *grupo enriquecido*. Denotaremos tal estructura $\mathsf{A}^\star = (M; \circ^M, u_1{}^M, u_2{}^M)$ (abreviadamente (M; ∘ , u_1, u_2)). Obsérvese que al considerar diferentes pares de elementos distinguidos en un grupo dado podemos tener grupos enriquecidos no isomorfos, con la definición natural de isomorfía.
El conjunto base serán las ternas de elementos de A, esto es, $M = A^3$. La operación del grupo es

$$(a, b, c) \circ (i, j, k) = (a + i, b + j, b \cdot i + c + k)$$

Los elementos distinguidos son $u_1 = (1, 0, 0)$ y $u_2 = (0, 1, 0)$

[10-15] Lema

(M, ∘) tiene estructura de grupo

Demostración
Confirmar la propiedad asociativa consiste en una mera comprobación . El elemento neutro es (0, 0, 0). El inverso de m = (a, b, c) es $m^{-1} = (-a, -b, b \cdot a - c)$.

Utilizaremos también $\mathsf{A}^\star$ para designar dicha estructura de grupo. Nótese que los inversos de los dos elementos distinguidos son $u_1^{-1} = (-1, 0, 0)$ y $u_2^{-1} = (0, -1, 0)$. Es claro que el grupo obtenido no es abeliano. Obsérvese que si m = (a, b, c) y n = (i, j, k) son dos elementos de M se verifica

$$m \circ n = n \circ m \iff b \cdot i = j \cdot a$$

(Es interesante recordar que la teoría de grupos abelianos es decidible)
Se llama *centro* de un grupo al conjunto de elementos del mismo que conmutan con cualquier elemento del grupo

[10-16] Lema

El centro del grupo $A^\star$ es $Z = \{(0, 0, k)/\ k \in A\}$

Demostración

Es inmediato ver que los elementos de la forma (0, 0, k) conmutan con cualquier elemento de M. Por otra parte, si (i, j, k) es un elemento central debe verificarse, para cualquier $(a,b,c) \in M$, que $(a + i, b + j, b \cdot i + c + k) = (i + a, j + b, j \cdot a + k + c)$, de donde se deduce que $b \cdot i = j \cdot a$. Considerando a = 1 y b = 0 se deduce j = 0. Haciendo a = 0 y b = 1 se deduce i = 0.

Observación

El producto de elementos del centro reproduce la suma del anillo, pues

$$(0, 0, k) \circ (0, 0, k') = (0, 0, k + k')$$

El elemento $q = u_2\ u_1\ u_2^{-1}\ u_1^{-1} = (0, 0, 1)$ reproduce la unidad del anillo. Su inverso es el elemento $q^{-1} = u_1\ u_2\ u_1^{-1}\ u_2^{-1} = (0, 0, -1)$.

En un grupo, los elementos de la forma $u\ v\ u^{-1}\ v^{-1}$ se denominan *conmutadores*. Si consideramos un conmutador $u\ v\ u^{-1}\ v^{-1}$, el elemento inverso, $u^{-1}\ v^{-1}\ u\ v$, es también un conmutador. El producto de dos conmutadores no es necesariamente un conmutador. El conjunto de todos los conmutadores de un grupo genera un subgrupo del mismo, llamado *subgrupo conmutador* o *grupo derivado*. Obsérvese que si el grupo es abeliano el único conmutador es el elemento neutro, por lo que el grupo derivado es trivial.

[10-17] Lema

i. Si m = (a, b, c) y n = (i, j, k) son dos elementos de M se verifica

$$m \circ n \circ m^{-1} \circ n^{-1} = (0, 0, b \cdot i - j \cdot a)$$

ii. Todo conmutador de $A^\star$ es central

Demostración

Es una mera comprobación:

$$(a, b, c) \circ (i, j, k) \circ (a, b, c)^{-1} \circ (i, j, k)^{-1} =$$

$$= (a, b, c) \circ (i, j, k) \circ (-a, -b, b \cdot a - c) \circ (-i, -j, j \cdot i - k) =$$

$$= (a + i, b + j, b \cdot i + c + k) \circ (-(a + i), -(b + j), b \cdot i + b \cdot a - c + j \cdot i - k) =$$

$$= (0, 0, b \cdot i - j \cdot a)$$

Nota

En la literatura algebraica rusa de los años sesenta un grupo en el que su subgrupo derivado es central se denominaba *metabeliano*. En la actualidad el término “grupo metabeliano” suele designar a un grupo resoluble de longitud dos, esto es un grupo cuyo subgrupo conmutador es abeliano. (Para detalles sobre teoría de grupos puede consultarse, por ejemplo, [2] o [49])

[10-18] Lema

Sean $G_1 = \{m \in M / m \circ u_2 = u_2 \circ m\}$ y $G_2 = \{m \in M / m \circ u_1 = u_1 \circ m\}$. Se verifica

i. $u_1 \in G_2$ y $u_2 \in G_1$

ii. $G_1 = \{(0, b, c) / b, c \in A\}$ y $G_2 = \{(a, 0, c) / a, c \in A\}$

iii. G_1 y G_2 son subgrupos abelianos de $A^\star$

iv. $G_1 \cap G_2 = Z$

Demostración

i. trivial

ii. $(a, b, c) \in G_1 \Leftrightarrow (a, b, c)\,(0, 1, 0) = (0, 1, 0)\,(a, b, c) \Leftrightarrow$

$\Leftrightarrow (a, b + 1, c) = (a, 1 + b, a + c) \Leftrightarrow a = 0$

$(a, b, c) \in G_2 \Leftrightarrow (a, b, c)\,(1, 0, 0) = (1, 0, 0)\,(a, b, c) \Leftrightarrow$

$\Leftrightarrow (a + 1, b, b + c) = (1 + a, b, c) \Leftrightarrow b = 0$

iii. $(a, b, c)\,(0, b', c')^{-1} = (0, b, c)\,(0, -b', -c') = (0, b - b', c - c') \in G_1$

$(a, b, c)\,(a', 0, c')^{-1} = (a, 0, c)\,(-a', 0, -c') = (a - a', 0, c - c') \in G_2$

iv. $(a, b, c) \in Z \Leftrightarrow a = 0 \;\&\; b = 0 \Leftrightarrow (a, b, c) \in G_1 \cap G_2$

[10-19] Lema

Para cada elemento central $m \in Z$ existen $g_1 \in G_1$ y $g_2 \in G_2$ tales que

$$m = u_1 g_1 u_1^{-1} g_1^{-1} = u_2 g_2 u_2^{-1} g_2^{-1}$$

Demostración.

Sea $m = (0, 0, k)$. Basta tomar elementos $g_1 = (0, -k, c)$ y $g_2 = (k, 0, c)$ con $c \in A$, por ejemplo, $c = 0$ ó $c = 1$.

Observación

Dados dos elementos centrales, $m_1 = (0, 0, k)$ y $m_2 = (0, 0, k')$ por el lema existe

$g_1 = (0, -k, 0) \in G_1$ tal que $m_1 = u_1 g_1 u_1^{-1} g_1^{-1}$

y existe

$g_2 = (k', 0, 0) \in G_2$ tal que $m_2 = u_2 g_2 u_2^{-1} g_2^{-1}$.

Entonces

$g_2 g_1 g_2^{-1} g_1^{-1} = (k', 0, 0)\,(0, -k, 0)\,(-k', 0, 0)\,(0, k, 0) = (0, 0, k \cdot k')$.

Observamos que se reproduce aquí la multiplicación del anillo.

Anillo asociado a un grupo de Malcev

La construcción realizada proporciona un grupo enriquecido $(M; \circ, u_1, u_2)$ verificando

M1. Todo conmutador es central

M2. Los conjuntos G_1 y G_2 de elementos que conmutan con u_2 y u_1 respectivamente son subgrupos abelianos de M

M3. La intersección $G_1 \cap G_2$ coincide con el centro del grupo

M4. Para cada elemento central $m \in Z$ existen elementos $g_1 \in G_1$ y $g_2 \in G_2$ tales que

$$m = u_1\, g_1\, u_1^{-1}\, g_1^{-1} = u_2\, g_2\, u_2^{-1}\, g_2^{-1}$$

Llamaremos *grupo de Malcev* a un grupo enriqucido verificando las condiciones M1, M2, M3 y M4.

Obsérvese que todas estas condiciones pueden expresarse por fórmulas de primer orden del lenguaje de la teoría de grupos. En efecto, observando que

$$z = x \circ y^{-1} \Leftrightarrow z \circ y = x$$

y considerando los siguientes esquemas de fórmulas

$\tau(u,v,w) \equiv u \circ w \circ v = v \circ w$ ("u es el conmutador de v y w")

$\theta(u, v) \equiv v \circ u = u \circ v$ ("u y v conmutan")

$\delta(u) \equiv \forall v\ \theta(u,v)$ ("u es central")

$\rho(u) \equiv \exists v \exists w\ \tau(u,v,w)$ ("u es un conmutador")

el enunciado de M1 es

$$\mu_1 \equiv \forall x\, (\rho(x) \rightarrow \delta(x))$$

Llamando

$\pi_1(v) \equiv \theta(u_2, v)$ ("$u \in G_1$")

$\pi_2(v) \equiv \theta(u_1, v)$ ("$u \in G_2$")

el enunciado de M2 es

$$\mu_2 \equiv \forall x \forall y\, (\, (\pi_1(x) \wedge \pi_1(y) \rightarrow \exists z\, (\pi_1(z) \wedge z \circ y = x) \wedge$$
$$\wedge\, (\pi_2(x) \wedge \pi_2(y) \rightarrow \exists z\, (\pi_2(z) \wedge z \circ y = x) \wedge \theta(x, y))$$

Para expresar que $G_1 \cap G_2 = Z$ podemos utilizar la fórmula

$$\mu_3 \equiv \forall x\, (\delta(x) \leftrightarrow \pi_1(x) \wedge \pi_2(x))$$

La propiedad M4 se expresa por

$$\mu_4 \equiv \forall x\, (\delta(x) \rightarrow \exists y \exists z\, (\tau(x, u_1, y) \wedge \tau(x, u_2, z))$$

Veamos que, dado un grupo de Malcev, esto es, un grupo G de la variedad determinada por $\mu_1 \wedge \mu_2 \wedge \mu_3 \wedge \mu_4$ podemos recuperar la estructura del anillo de partida.

Para ello a partir del grupo $\mathsf{G} = \{G\ ;\ \circ,\ u_1,\ u_2)$ obtendremos un anillo ${}^{\star}\mathsf{G} = (B\ ;\ +,\ \cdot,\ 0,\ 1)$ de forma que si partimos de un anillo A y componemos las dos transformaciones obtenemos la isomorfía $\mathsf{A} \approx {}^{\star}(\mathsf{A}^{\star})$

El universo del anillo estará constituido por el conjunto de elementos centrales del grupo

$$B=\{x \in G / \forall y \in G\ \ x \circ y = y \circ x\}$$

Según la observación realizada al principio definiremos la suma naturalmente como

$$m_1 + m_2 = m_1 \circ m_2$$

Para definir el producto hacemos uso de la observación tras el lema [10.19] y definimos por lo tanto el producto mediante

$$m_1 \cdot m_2 = g_2\, g_1\, g_2^{-1}\, g_1^{-1}$$

siendo

$$m_1 = u_1\, g_1\, u_1^{-1}\, g_1^{-1}$$
$$m_2 = u_2\, g_1\, u_2^{-1}\, g_2^{-1}$$
$$g_1 \in G_1$$
$$g_2 \in G_2$$

Naturalmente, hay que comprobar que el producto está bien definido. En efecto, supongamos que para ciertos $g_1, h_1 \in G_1$ y ciertos $g_2, h_2 \in G_2$ se verifica

$$m_1 = u_1\, g_1\, u_1^{-1}\, g_1^{-1} = u_1\, h_1\, u_1^{-1}\, h_1^{-1}$$
$$m_2 = u_2\, g_2\, u_2^{-1}\, g_2^{-1} = u_2\, h_2\, u_2^{-1}\, h_2^{-1}$$

Entonces de $u_1\, g_1\, u_1^{-1}\, g_1^{-1} = u_1\, h_1\, u_1^{-1}\, h_1^{-1}$
se deduce $u_1\, g_1 = u_1\, h_1\, u_1^{-1}\, h_1^{-1}\, g_1\, u_1$
o sea $g_1 = h_1\, u_1^{-1}\, h_1^{-1}\, g_1\, u_1$
luego $u_1\, h_1^{-1}\, g_1 = h_1^{-1}\, g_1\, u_1$

Por tanto $h_1^{-1}\, g_1 \in G_2$ por conmutar con u_1. Puesto que tanto h_1 como g_1 están en G_1 también $h_1^{-1}\, g_1 \in G_1$ y por tanto $h_1^{-1}\, g_1$ está en el centro Z. Análogamente se vería que $g_2^{-1}\, h_2 \in Z$. En consecuencia, podemos escribir

$$g_2\, g_1\, g_2^{-1}\, h_2 = g_2\, g_2^{-1}\, h_2\, g_1 = h_2\, g_1 = h_2\, h_1\, h_1^{-1}\, g_1$$

y por tanto

$$g_2\, g_1\, g_2^{-1} = h_2\, h_1\, h_1^{-1}\, g_1\, h_2^{-1} = h_2\, h_1\, h_2^{-1}\, h_1^{-1}\, g_1$$

de donde obtenemos, al fin :

$$g_2\, g_1\, g_2^{-1} g_1^{-1} = h_2\, h_1\, h_2^{-1}\, h_1^{-1}$$

Estas operaciones dotan al conjunto de estructura de anillo unitario.
La adición es la operación del grupo restringida al centro; por tanto hereda las propiedades necesarias para dotar al centro de la estructura de grupo conmutativo.
Comprobemos la propiedad distributiva. Tomemos

$m = u_1\, g_1\, u_1^{-1}\, g_1^{-1}$ con $g_1 \in G_1$
$n = u_1\, h_1\, u_1^{-1}\, h_1^{-1}$ con $h_1 \in G_1$
$p = u_2\, k_2\, u_2^{-1}\, k_2^{-1}$ con $k_2 \in G_2$

Por hipótesis todo conmutador es central. Luego

$$g_1^{-1}\, u_1\, h_1\, u_1^{-1}\, h_1^{-1} = u_1\, h_1\, u_1^{-1}\, h_1^{-1}\, g_1^{-1}$$
$$g_1^{-1}\, k_2\, h_1\, k_2^{-1}\, h_1^{-1} = k_2\, h_1\, k_2^{-1}\, h_1^{-1}\, g_1^{-1}$$

Por tanto se tiene

$$\begin{aligned} m + n &= u_1\, g_1\, u_1^{-1}\, g_1^{-1}\, u_1\, h_1\, u_1^{-1}\, h_1^{-1} = \\ &= u_1\, g_1\, u_1^{-1}\, u_1\, h_1\, u_1^{-1}\, h_1^{-1}\, g_1^{-1} = \\ &= u_1\, g_1\, h_1\, u_1^{-1}\, h_1^{-1} g_1^{-1} = \\ &= u_1\, (g_1\, h_1)\, u_1^{-1}\, (g_1\, h_1)^{-1} \end{aligned}$$

$$m \cdot p = k_2 g_1 k_2^{-1} g_2^{-1}$$
$$n \cdot p = k_2 h_1 k_2^{-1} h_2^{-1}$$

$$\begin{aligned} m \cdot p + n \cdot p &= k_2\, g_1\, k_2^{-1} g_1^{-1}\, k_2\, h_1\, k_2^{-1}\, h_1^{-1} = \\ &= k_2\, g_1\, k_2^{-1}\, k_2\, h_1\, k_2^{-1} h_1^{-1}\, g_1^{-1} = \\ &= k_2\, g_1\, h_1\, k_2^{-1}\, h_1^{-1}\, g_1^{-1} = \\ &= k_2\, (g_1\, h_1)\, k_2^{-1} (g_1\, h_1)^{-1} = \\ &= (m + n) \cdot p \end{aligned}$$

(No comprobaremos aquí que el producto es asociativo; de la asociatividad del anillo de partida se deduce la asociatividad en esta estructura como consecuencia de la isomorfía que veremos más adelante. También se deducirá que $q = u_2\, u_1\, u_2^{-1}\, u_1^{-1}$ es la unidad del anillo. Obsérvese que, si $m = u_1\, g_1\, u_1^{-1}\, g_1^{-1}$, se tiene trivialmente que $m \cdot q = m$)

La interpretación

Las consideraciones anteriores, por las que asociamos a cada anillo unitario su grupo de Mal'cev, permiten definir una interpretación $\Gamma = (\gamma, g)$ de la clase de los anillos unitarios K_{ANU} en la clase K_{GRE} de grupos de Malcev (grupos enriquecidos verificando las condiciones M1, M2, M3, M4). La interpretación viene determinada por las fórmulas :

$\gamma(x) \equiv \delta(x) \equiv \forall y\ (x \circ y = y \circ x)$

$\alpha_+(x, y, z) \equiv x \circ y = z$

$\alpha_\cdot(x, y, z) \equiv \exists w_1 \exists w_2\ (\pi_1(w_1) \wedge \pi_2(w_2) \wedge \tau(x, u_1, w_1) \wedge \tau(y, u_2, w_2) \wedge \tau(z, w_2, w_1))$

$\alpha_0(x) \equiv \forall y\ (y \circ x = y)$

$\alpha_1(x) \equiv x \circ u_1 \circ u_2 = u_2 \circ u_1$

Nótese que se verifican las condiciones de adecuación de la interpretación: el universo es no vacío; está claro que α_+ tiene carácter funcional y hemos comentado ya que $\alpha_\cdot$ es una buena definición del producto; la fórmula α_0 está satisfecha por un único elemento, el elemento neutro del grupo y, finalmente, la fórmula α_1 está satisfecha por un único elemento, a saber, $x = u_1 u_2 u_1^{-1} u_2^{-1}$

Mediante esta interpretación asociados a cada anillo $A \in \mathsf{K}_{ANU}$ un grupo enriquecido $A^\star \in \mathsf{K}_{GRE}$.

Veamos ahora que la estructura inducida por esta interpretación a partir de $A^\star$, o sea, la estructura $(A^\star)^\Gamma = (B\ ;\ +^B\ ,\ 0^B\ ,\ 1^B)$ es isomorfa al anillo de partida A.

El lema [10.16] permite construir de forma natural una biyección entre los universos de dichas estructuras

$$\begin{aligned} f : A &\to B \\ k &\mapsto (0, 0, k) \end{aligned}$$

pues

$$k \in A \Leftrightarrow A^\star \vDash \gamma\,[f(k)] \Leftrightarrow f(k) \in B$$

Esta biyección es además un isomorfismo entre ambas estructuras de anillo. En efecto :

i. $(i, j, k) \in +^A \Leftrightarrow A^\star \vDash \alpha_+\,[f(i), f(j), f(k)] \Leftrightarrow f(i) +^B f(j) = f(k)$

Ver la observación que sigue al lema [8.2].

ii. $(i, j, k) \in \cdot^A \Leftrightarrow A^\star \vDash \alpha_\cdot\,[f(i), f(j), f(k)] \Leftrightarrow f(i) \cdot^B f(k) = f(k)$

Hemos comprobado que si $i \cdot^A j = k$ entonces $f(i) \cdot^B f(j) = f(k)$

Para la implicación inversa basta observar que si $A^\star \vDash \alpha_\cdot\,[f(i), f(j), f(k)]$ entonces se verifican las ecuaciones

$$(a_1, b_1, c_1)\ (0, 1, 0) = (0, 1, 0)\ (a_1, b_1, c_1)$$
$$(a_2, b_2, c_2)\ (1, 0, 0) = (1, 0, 0)\ (a_2, b_2, c_2)$$
$$(0, 0, k)\ (a_1, b_1, c_1)\ (a_2, b_2, c_2) = (a_2, b_2, c_2)\ (a_1, b_1, c_1)$$
$$(0, 0, i)\ (a_1, b_1, c_1)\ (1, 0, 0) = (1, 0, 0)\ (a_1, b_1, c_1)$$
$$(0, 0, j)\ (a_2, b_2, c_2)\ (0, 1, 0) = (0, 1, 0)\ (a_2, b_2, c_2)$$

de las que se deduce

$$a_1 = 0$$
$$b_2 = 0$$
$$b_1 \cdot^A a_2 +^A k = 0$$

$b_1 +^A i = 0$
$j = a_2$
y en consecuencia $i \cdot^A j = k$
De igual forma,
iii. $m = 0^B \Leftrightarrow A^\star \vDash \alpha_0[m] \Leftrightarrow m = (0, 0, 0) = f(0^A)$
iv. $m = 1^B \Leftrightarrow A^\star \vDash \alpha_1[m] \Leftrightarrow m = u_1 u_2 u_1^{-1} u_2^{-1} = (0, 0, 1) = f(1^A)$
Esto muestra que A y $(A^\star)^\Gamma$ son isomorfas.
Estamos, pues, en las hipótesis del teorema de Rabin-Ershov, pues la clase de los anillos unitarios es finitamente axiomatizable y hemos mostrado que es fuertemente codificable en la clase K_{GRE}. De la inseparabilidad finita de la clase de los anillos concluimos por tanto que

[10-20] Teorema

La clase K_{GRE} es finitamente inseparable.

Como $Th(K_{GRE})$ es una extensión finita de la teoría de grupos enriquecidos con dos constantes concluimos

[10-21] Teorema

La clase de los grupos enriquecidos con dos constantes es finitamente inseparable

Por el teorema de las extensiones inesenciales llegamos a

[10-22] Teorema

La clase de los grupos es finitamente inseparable

Y en consecuencia

[10-23] Teorema

La teoría de grupos es indecidible.
La teoría de grupos finitos es indecidible

Como la teoría de grupos es una extensión finita de la teoría de semigrupos tenemos también

[10-24] Teorema

La teoría de semigrupos es finitamente inseparable

11. CONCLUSIONES

En este trabajo se han refinado algunos teoremas necesarios para la demostración de indecidibilidad de teorías matemáticas, lo que ha permitido simplificar algunas demostraciones. Además se han expuesto diversas técnicas y se han analizado sus posibilidades de aplicación y sus dificultades.

Tras obtener resultados de indecidibilidad e inseparabilidad para diversas teorías podemos reflexionar sobre los estilos de demostración empleados. Se observa que hay tres tipos de situaciones y pruebas distintas, a saber :

a) Teorías inseparables
En el caso de teorías sin modelos finitos se obtienen resultados de inseparabilidad. Tal es el caso de la aritmética y de la teoría de conjuntos. En el caso de la aritmética la demostración es directa por representación y diagonalización. Obtenido el resultado de inseparabilidad se transmite por interpretación a la teoría de conjuntos.

b) Estructuras fuertemente indecidibles
Partiendo de la estructura fuertemente indecidible de los números naturales sucesivas inmersiones semánticas nos permiten obtener diversas estructuras fuertemente indecidibles : la estructura de los enteros, el grupo de permutaciones de los enteros, la estructura de los racionales. Todas estas estructuras, al ser fuertemente indecidibles, tienen teorías hereditariamente indecidibles. Como estas estructuras son ejemplos de, respectivamente, anillos, grupos y cuerpos, se obtiene en consecuencia que las teorías de anillos, grupos y cuerpos son indecidibles, incluso hereditariamente indecidibles.

c)Teorías finitamente inseparables
En el caso de teorías con modelos finitos los resultados interesantes son los de inseparabilidad finita. El punto de partida es la inseparabilidad de las máquinas que paran y las máquinas que ciclan. Sucesivas inmersiones semánticas permiten codificar la clase de dichas máquinas en la teoría de una relación binaria, la teoría de grafos, la teoría de anillos y la teoría de grupos. En algunos casos la codificación no es complicada, pero en otros como en el caso de la codificación en anillos, la técnica es ciertamente sofisticada. ¿Habrá alguna forma más sencilla de codificar, por ejemplo, la clase de los grafos en la clase de los anillos que permita un tratamiento más asequible?

Las teorías indecidibles encontradas son o bien esencialmente indecidibles o bien hereditariamente indecidibles. La razón de no encontrar teorías escuetamente indecidibles

se ve clara por los métodos de prueba empleados. Las teorías inseparables son esencialmente indecidibles. En el caso de la técnica de Tarski se obtienen estructuras fuertemente indecidibles y por tanto teorías hereditariamente indecidibles. Los resultados de inseparabilidad finita proporcionados por la técnica de Rabin-Ershov proporcionan teorías hereditariamente indecidibles.

BIBLIOGRAFÍA

[1] BELLÈ, D. & PARLAMENTO, F.. Undecidability in Weak Membership Theories. En Ursini, Aldo & Paolo Agliano (eds.) *Logic and Algebra.* Marcel Dekker. New York. 1996.

[2] BHATTACHARYA, P. B. , JAIN, S. K. & NAGPAUL S. R. *Basic Abstract Algebra.* Cambridge University Press. Cambridge. (2nd ed.) 1994

[3] BÜCHI, J. R.. Turing Machines and the Entscheidungsproblem. *Math. Annalen* 148 , pp. 201-213. 1962

[4] BOOLOS, G. JEFFREY, R. *Computability and Logic*. Cambridge University Press. Cambridge. 1974

[5] CHANG, C.C., KEISLER, H. J. *Model theory*. North-Holland. Amsterdam. 1974

[6] CHURCH, A. . A note on the Entscheidungsproblem. *Journal of Symbolic Logic.* Vol. 1, pp. 40-41; A correction, *ibid*., pp. 101-102. 1936 (reimpreso en M. Davis. *The Undecidable*)

[7] CHURCH, A. & QUINE, W. V. Some Theorems on definability and decidability. *Journal of Symbolic Logic.* Vol. 17, n. 3. 1952

[8] COLLINS, G.E. & HALPERN, J. D. On the interpretability of arithmetic in set theory. *Notre Dame Journal of Formal Logic*, Vol. 11, pp. 477-483. 1970

[9] CUTLAND, N. *Computability.* Cambridge University Press. Cambridge. 1980

[10] DAVIS, M. *Computability and Unsolvability.* McGraw- Hill . New York. 1958 (2º ed. Dover 1982)

[11] DAVIS, M (ed.) *The Undecidable. Basic papers on undecidable propositions, unsolvable problems and computable functions.* Raven Press. New York. 1965 (Correcciones a la traducción en Bauer-Mengelberg, Stefan *Journal of Symbolic Logic* vol 31, pp. 484-494.1966)

[12] DAVIS, M**.** Unsolvable problems. En J. Barwise (ed). *Handbook of mathematical logic*. North-Holland. Amsterdam. 1977.

[13] EBBINGHAUS, H.-D., FLUM, J & THOMAS, W.. *Mathematical Logic.* Springer-Verlag. New York. 1984.

[14] EPSTEIN, R. L. & CARNIELLI, W. A. *Computability. Computable Functions, Logic and the Foundations of Mathematics.* Wadsworth & Brooks. Pacific Grove. 1989.

[15] ERSHOV, YU. L., LAVROV I. A., TAIMANOV A. D., TAISTSLIN M. A. Elementary Theories. *Russian Mathematical Surveys* , vol 20, pp. 35-105. 1965

[16] ERSHOV, YU. L. *Definability and computability*. Consultants Bureau. New York. 1996

[17] FEFERMAN , S**.** Arithmetization of metamathematics in a general setting. *Fundamenta Mathematicae*. Vol. 49, 35-92. 1960

[18] FEFERMAN , S**.** Deciding the Undecidable: Wrestling with Hilbert's Problems. En *In the light of logic*. Oxford University Press. New York. 1998

[19] GÖDEL, K. Über formal unentsheidbare Sätze der Principia Mathematica und verwandter Systeme. I. *Monatshefte für Mathematik und Physik,* vol 38, pp. 173-198. 1931 (Traducción inglesa en Davis, *The Undecidable*, Raven Press. New York pp 39-74)

[20] GRZEGORCZYK, A. Undecidability of Some Topological Theories. *Fundamenta Mathematicae.* Vol 38, pp. 137-151. 1951

[21] HRBACEK, K & JECH, T. *Introduction to Set Theory.* M. Dekker. New York.(2ª ed.) 1984

[22] HUBER DYSON, V. On the decision problem for theories of finite models. *Israel Journal of Mathematics.* 1, pp 55-70. 1964

[23] HUBER DYSON, V. On the decision problem for extensions of a decidable theory. *Fundameta Mathematicae,* 64, pp 7-70. 1979

[24] JANICZAK, A. Undecidability of Some Simple Formalized Theories *Fundamenta Mathematicae.* Vol. 40, pp. 131-139. 1953

[25] KLEENE, S. C. A symmetric form of Gödel's theorem. *Indagationes mathematicae.* Vol. 12. pp 244-246. 1950

[26] KLEENE, S. C. *Introduction to Metamathematics.* North Holland. Amsterdam. 1952

[27] KREISEL, G. Models, Translations and Interpretations. En *Mathematical Interpretation of Formal Systems* L. E. J. Brouwer, E. W. Beth & A. Heyting (eds.) North-Holland. Amsterdam. 1955

[28] KULIKOV N. A. Definability of graphs by congruence lattices. *Algebra i Logica.* Vol. 24. 1, pp 13-25. 1985

[29] MAL'CEV A. I. Effective inseparability of the set of identically true from the set of finitely refutable formulas of certain elementary theories. *Amer. Math. Soc. Trans.* 2, 45, pp. 1005-1008. 1965. (*Soviet Math.* 2 1961)

[30] MAL'CEV A. I. On a correspondence between rings and groups. *Amer. Math. Soc. Trans*. 2, 45. 1965

[31] MAL'CEV, A. I. *The metamathematics of algebraic systems (Collected papers:1936-1967)* North-Holand. Amsterdam. 1971

[32] MAL'CEV, A. I. Undecidability of the elementary theory of finite groups. *Soviet Math.* 2, pp 714-717. 1961

[33] MARCJA , A., PREST, M & TOFFALORI, C. On the Undecidability of some classes of abelian-by-finite groups. *Annals of Pure and Applied Logic* 62, pp. 167-173. 1993

[34] MEL'NICHUK I. L. Unsolvability of problems of equality and divisibility in certain varieties of semigroups. *Algebra i Logica* Vol. 23, 4, pp 430-438. 1984

[35] MENDELSON, E. *Introduction to Mathematical Logic.* Chapman & Hall, Englewood Cliffs, New Jersey. (fourth ed.)1997

[36] MINSKY, M. L. *Computation : Finite and Infinite Machines.* Prentice-Hall. London. 1967

[37] MONK, J. D. *Mathematical Logic.* Springer-Verlag. New York. 1976

[38] MONTAGNA F & MANCINI, A. A Minimal Predicative Set Theory. *Notre Dame Journal of Formal Logic.* Vol. 35, 2, pp 186-203. 1994

[39] MOSCHOVAKIS Y. N. *Notes on Set Theory.* Springer-Verlag. New York. 1994

[40] MYHILL, J. Creative Sets. *Zeitschr. f. math. Logik und Grundlagen d. Math.* Bd I S. pp. 97-108. 1955

[41] MUZALEWSKI, M. Restricted Problems in Some Classes of Algebraic Systems. *Zeitschr. f. math. Logik und Grundlagen d. Math*. Bd. 24, S, pp. 279-287, 1978

[42] ODIFREDDI, P. *Classical Recursion Theory*. North-Holland. Amsterdam. 1989.
[43] PAL'CHUNOV, D.E. Undecidability of theories of Boolean algebras with selected ideals . *Algebra i logica.* Vol. 25, n. 3, pp. 326-346. 1986.
[44] PRIDA, J. F. Una caracterización topológica de las clases Δ-elementales. En J. Echeverría, J. de Lorenzo, L. Peña (eds.) *Calculemos... Matemáticas y libertad* Trotta.Valladolid. 1996
[45] PRIDA, J. F. A Nonstandard Approach to Arithmetic. *Rev. R. Acad. Cienc. Exact. Fís. Nat.* Vol. 93, n. 2. pp. 227-229. 1999
[46] RABIN, M. O. On recursively enumerable and arithmetic models of set theory. *Journal of Symbolic Logic*. Vol. 23, n. 4. 1958
[47] RABIN, M. O. A simple method for undecidability proofs and some applications. *Logic, Methodology and Philosophy of Science (Proc. 1964 Internat. l Congr.)* North-Holland. Amsterdam. pp. 58-68. 1965
[48] ROBINSON, J.. Definability and Decision Problems in Arithmetic. *Journal of Symbolic Logic.* Vol. 14, n. 2. 1949
[49] ROBINSON, D. J. S. *A Course in the Theory of Groups.* Spinger-Verlag. New York. 1993
[50] ROGERS, H.. Certain Logical Reduction and Decision Problems. *Annals of Mathematics.* Vol. 64, n. 2. 1956
[51] ROGERS, H. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill. New York. 1967
[52] ROSSER, J. B. Extensions of some theorems of Gödel and Church. *Journal of Symbolic Logic*. Vol. 1, pp. 87-91. 1936 (También en Davis, *The Undecidable*, pp. 231-235)
[53] SHOENFIELD, J. *Mathematical Logic*. Addison-Wesley. Reading. 1967
[54] SKOLEM, TH. *Selected Works in Logic*. Universitetsforlaget. Oslo. 1970
[55] SMORYNSKI, C.. Review of [Ershov 1965] *Journal of Symbolic Logic.* Vol. 39, n. 3. 1974.
[56] SMULLYAN R. M. *Theory of Formal Systems.* Princeton University Press. Princeton 1961
[57] SMULLYAN R. M. *Diagonalization and Self-Reference.* Clarendon Press. Oxford. 1994
[58] SPREEN, D. Effective inseparability in a topological setting. *Annals of pure and Applied Logic.* Vol. 80, pp. 257-275. 1996
[59] SUPPES, P. *Axiomatic Set Theory.* Dover. New York 1972
[60] TARSKI A, MOSTOWSKI A., ROBINSON R. M. *Undecidable theories*. North-Holland. Amsterdam. 1953
[61] TOFFALORI, C.. An undecidability theorem for lattices over group rings. *Annals of Pure and Applied Logic.* Vol. 88, pp. 241-262. 1997
[62] TURING, A. M. On Computable Numbers, with an Application to the Entscheidungsproblem, *Proceedings of the London Mathematical Society,* ser 2 , vol. 42, pp 230-265, 1936-37; Correction, *ibid.* vol 43, pp. 544-546, 1937. (Reimpreso en Davis, *The Undecidable*, pp. 115-153)
[63] URSINI, A. & AGLIANO, P. (eds.) *Logic and Algebra*. (Lecture Notes in Pure and Applied Mathematics, 180) Marcel Dekker. New York. 1996.

[64] VAUGHT R. On a theorem of Cobham concerning undecidable theories. *Proc. Logic, methodology and Philosophy of Science 1960. Intern. Congress*. Stanford University Press. Stanford. 1962

[65] WILLARD, R. Hereditary Undecidability of Some Theories of Finite Structures. *Journal of Symbolic Logic*. Vol. 59, n. 4. 1994