Computabilidad y Teoría de Modelos

Unidad 0.
Conceptos.

La Lógica Proposicional

Es consistente: No existe una fbf A tal que A y la negación de A sean teoremas.

Es semánticamente completa: Una fbf A es teorema sii es tautología.

Es sintácticamente completa: No puede agregarse un esquema axioma que no sea demostrable sin perder la consistencia.

Es decidible: existe un procedimiento efectivo para establecer si una fbf es o no teorema.

No es completa respecto de la negación: existe una fbf A tal que ni A ni la negación de A son teoremas.

La Lógica de Primer Orden

Es consistente: No existe una fbf A tal que A y la negación de A sean teoremas.

Es semánticamente completa: Una fbf A es teorema sii es lógicamente válida.

No es sintácticamente completa: Puede agregarse un esquema axioma que no sea demostrable sin perder la consistencia.

No es decidible: no existe un procedimiento efectivo para establecer si una fbf es o no teorema.

No es completa respecto de la negación: existe una fbf A tal que ni A ni la negación de A son teoremas.

Las Teorías de Primer Orden

Son semánticamente completas: Una fbf A es teorema sii es verdadera en todos los modelos.

Son Compactas: Una teoría tiene modelo sii cada parte finita de la teoría tiene modelo.

No son categóricas: Si una teoría tiene modelo infinito lo tiene de otras cardinalidades.

Casos Especiales: La aritmética de Peano y la teoría de Conjuntos de Zermelo Fraenkel.
El axioma de elección. La hipótesis del continuo.

Son decidibles: grupos abelianos, aritmética con una sola operación, álgebra de números reales con suma y producto pero sin la noción general de número natural, geometría elemental.

Son indecidibles: grupos, anillos, campos, semigrupos, PA, ZF.

Definiciones y Teoremas Básicos.

El lenguaje Q.
Variables, constantes, símbolos funcionales, símbolos predicativos, conectivas, cuantificadores, auxiliares.

Semántica para Q.
Interpretaciones. 3 niveles de verdad.

El sistema formal SQ.
Axiomas.
SQ 1. $((A \supset (B \supset A))$
SQ 2. $((A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$
SQ 3. $((\neg A \supset \neg B) \supset (B \supset A))$
SQ 4. $(\forall x)A \supset A(x/t)$ si t está libre para x en A.
SQ 5. $A \supset (\forall x)A$ si x no aparece libre en A.
SQ 6. $((\forall x)(A \supset B)) \supset ((\forall x)A \supset (\forall x)B)$
SQ 7. Si A es un axioma entonces $(\forall x)A$ también.

Reglas de Inferencia.
Modus Ponens.
A, $A \supset B$ se deduce B.

Teorías de primer orden.
Extensiones. Modelos.

La lógica de primer orden con igualdad.
Axiomas. Completitud semántica.

Teorema [Soundness Theorem].
Si A es un teorema de SQ entonces es lógicamente válida.

Teorema [Consistencia de SQ]
SQ es consistente.

Teorema [Completitud respecto de la negación]
SQ no es completo respecto de la negación.

Teorema [Extensiones con no-teoremas]
Sea K una teoría de primer orden consistente. Si A es una fbf cerrada de K que no es teorema entonces K + {¬A} es consistente.

Teorema [Lema de Lindenbaum. Extensiones completas]
Si K es una teoría de primer orden consistente entonces existe una teoría K' que es una extensión de K que es consistente y completa respecto a la negación.

Teorema [Extensiones cerradas]
Si K es una teoría de primer orden consistente entonces existe una teoría K' que es una extensión de K que es consistente, cerrada y completa respecto a la negación.

Teorema [Löwenheim-Skolem. Modelos numerables]
Si K es una teoría de primer orden consistente entonces K tiene un modelo numerable.

Teorema [Gödel. Completud semántica]
Si K es una teoría de primer orden y A una fbf que es verdadera en todos los modelos de K entonces A es teorema de K.

Teorema [Compacidad]
Si K es una teoría de primer orden tal que todo subconjunto finito de axiomas tiene modelo entonces K tiene modelo.

Práctica 0.

1. Demostrar que los axiomas de SQ son lógicamente válidos y que el modus ponens preserva la verdad.

2. Analizar la restricción de SQ 4. Ver la fórmula $(\forall x)\neg(\forall y)F(x,y) \supset \neg(\forall y)F(y,y)$

3. Analizar la restricción de SQ 5. Ver la fórmula $F(x) \supset (\forall x)F(x)$

4. Demostrar que SQ no es sintácticamente completa. Ver la fórmula $\neg(\forall x)\neg A \supset (\forall x)A$.

5. Demostrar que SQ no es completa respecto a la negación.

6. Si K es una teoría de primer orden consistente la teoría K', que es una extensión de K con el agregado de un conjunto numerable de constantes nuevas con su numeración efectiva, es consistente.

7. Si K es una teoría de primer orden consistente la teoría K', que es una extensión de K con el agregado de un conjunto numerable de axiomas nuevos de la forma $A(x/c) \supset (\forall x)A$ donde $(\forall x)A$ es cerrada y *c* una constante que no aparece en ningún axioma específico de K, es consistente.

8. El teorema de Lowenheim Skolem no vale para fórmulas abiertas. Ver el conjunto $\{F(x),\neg F(y)\}$ que es consistente y no tiene modelo.

9. Si K es una teoría de primer orden consistente con igualdad entonces K tiene un modelo normal.

10. Si una fbf A es verdadero en todos los modelos normales entonces es teorema de $SQ^{=}$.

Unidad 1.

La Historia: El programa de Hilbert y la escuela de Viena.
Isomorfismo de modelos.
Teorema de Vaught. Aplicaciones.
Sistemas Formales.
Interpretaciones. Teoría de Modelos.
Mecanismos Deductivos. Teoría de la Demostración.
La Metateoría de los Sistemas Formales.
Sistemas Formales Finitistas.
La incompletud informal de la Teoría de los Números Naturales.
La decibilidad de las demostraciones.
Si las demostraciones son decidibles los teoremas son recursivamente enumerables.
Si las demostraciones son decidibles y el sistema es consistente y completo respecto a la negación entonces los teoremas son decidibles.

Lecturas.
Formal Systems and Machines: An Isomorphism. Peter Suber.
A Crash Course in The MathematicsOf Infinite Sets. Peter Suber.

Práctica 1.

El Sistema Formal S.
Definiciones.

Alfabeto:

{ !, #, &, *, (,) }

Construcción de fórmulas:

1. * es a fbf.
2. ! es a fbf.
3. () y)(son fbfs.
4. Si A es una fbf, entonces A!, (A), *A, AA, y AAA son fbfs.
5. Si (A) es una fbf, entonces A, #A, y A# son fbfs.
6. Si A y B son fbfs, entonces A&B es una fbf.
7. Ninguna otra cosa es una fbf.

El mecanismo deductivo
Reglas de inferencia:

1. Si A y B son teoremas, entonces *AB es teorema.
2. Si **A y A son teoremas, entonces !A es teorema.
3. Si (A) es teorema, entonces A es teorema.
4. Si ABC es teorema, entonces C es teorema.

Axiomas:

1. (***)
2. !!!

Metateoría:

Consistencia absoluta: Un sistema formal es absolutamente consistente sii al menos una fbf de su lenguaje no es teorema.

Completud respecto de la exclamación: Un sistema formal es completo respecto de la exclamación sii para cada fbf A se cumple que A es teorema o bien !A es teorema.

Exclamatividad: Un sistema formal es exclamativo sii cada string de !'s es un teorema.

Ejercicios.
1. Demostrar los siguientes teoremas.
   a. !
   b. !!
   c. !!!!

2. Demostrar que S es absolutamente consistente.

3. Es S completo respecto de la exclamación?

4. Demostrar que S es exclamativo.

5. Dificil. Es S decidible?

Unidad 2.

K-validez y Lógica Monádica.

La definición de k-validez.
El análisis de los dominios de interpretación.
La k-validez es decidible.
La lógica de predicados monádicos de primer órden.
Propiedades (consistencia, adecuación etc)
Lema 1: Incremento de dominios.
Lema 2: Partición de dominios en clases.
La lógica de predicados monádicos de primer órden es decidible.

Práctica 2.

K-validez y Lógica Monádica.

1. Calcular el número de relaciones n-arias en un dominio de k elementos.
2. Analizar la 1-validez de la fbf $\neg(\forall x)\neg F(x) \supset (\forall x)F(x)$.
3. Analizar la 2-validez de la fbf $\neg(\forall x)\neg F(x) \supset (\forall x)F(x)$.
4. Demostrar por inducción el Lema 1.
5. Analizar si el Lema 1 implica la existencia de interpretaciones en un dominio infinito.
6. Demostrar el Lema 1 para SQ.
7. Demostrar por inducción el Lema 2.

Unidad 3.

Los cuerpos de característica cero. La imposibilidad de una axiomatización finita.
La teoría de grupos. Axiomas y resultados.

La aritmética de Peano (PA).
Axiomatización en primer orden.
Casos especiales: sin definición de operaciones y sólo con suma (Presburger).
La formalización original de Peano. La determinación unívoca de N.
La categoricidad de PA axiomatizada en segundo orden.
El modelo standard de PA en ZF.
Puede ZF probar teoremas de PA que PA no puede?
La extensión Finita del Teorema de Ramsey y The Goodstein´s Amazing Secuence.
Un modelo no clásico de PA.

Práctica 3.

1. Sea A una fbf de la teoría de cuerpos verdadera en los cuerpos de caractrística cero. Probar que para todo p mayor que un cierto n, A es verdadera en los cuerpos de característica p. ¿Vale la recíproca?

2. Analizar qué ocurre cuando los axiomas de la teoría de grupos se interpretan de la siguiente manera:
El conjunto: los números enteros.
La operación: la suma.
El inverso de x: -x.
La igualdad: la congruencia módulo m.
a. Es esta interpretación un modelo?
b. Es esta interpretación un grupo?
c. Explicar el resultado.

3. Describir una teoría de primer orden cuyos modelos normales sean todos los grupos infinitos. Es posible hacer lo mismo para todos los grupos finitos?

4. Demostrar la existencia de un modelo no clásico de la Aritmética de Peano.

Unidad 4.

Los axiomas de Peano con igualdad.
Numerales. Metateoremas que involucran numerales.
El lema de la desigualdad y el lema de la suma.
Definición de relaciones en PA.
La representabilidad en una teoría con el lenguaje de PA.
La representabilidad de la suma y el producto en PA.
Otras definiciones de representabilidad.

Práctica 4.

La Aritmética de Peano y la representabilidad.

1. Definir en PA las relaciones usuales entre 2 números naturales de tener algún factor común y de ser coprimos.

2. Demostrar la expresabilidad de las siguientes funciones:

a. cero: $N \to N$
   cero $(x) = 0$

b. sucesor: $N \to N$
   sucesor $(x) = x + 1$

c. $Proy_j : N \times N \times \ldots \times N \to N$
   $Proy_j (X_1, X_2, \ldots, X_j, \ldots, X_n) = X_j$

3. Demostrar que si en una teoría con el lenguaje de PA la igualdad está representada por la fórmula $x = y$ entonces la segunda condición de la definición de representabilidad es superflua.

Unidad 5.

La clase de funciones primitivas recursivas.
La clase de funciones recursivas totales.
La clase de funciones recursivas parciales.
Esquemas alternativos de recursión.
La función de Ackermann.
El crecimiento de la función de Ackermann.
La función de Ackermann crece más rápido que cualquier función primitiva recursiva.
La función de Ackermann no es primitiva recursiva.

Práctica 5.

La función de Ackermann.

1. Demostrar las siguientes propiedades de la función de Ackermann.
a. $A(x, y) > y$
b. $A(x, y + 1) > A(x, y)$
c. Si $y_2 > y_1$ entonces $A(x, y_2) > A(x, y_1)$
d. $A(x + 1, y) \geq A(x, y + 1)$
e. $A(x, y) > x$
f. Si $x_2 > x_1$ entonces $A(x_2, y) > A(x_1, y)$
g. $A(x + 2, y) > A(x, 2y)$

2. Demostrar que A tiene un crecimiento mayor que cualquier función primitiva recursiva.

3. Sea $f: N \to N$ una función primitiva recursiva en cuya derivación la mayor función constante usada toma el valor k. Calcular m tal que $A(m, x) > f(x)$ para todo x.

Unidad 6.

La recursividad de la función de Ackermann.
El método de la traza.

Práctica 6.

El método de la traza.

1. Sea la siguiente función f: N x N $\rightarrow$ N

f (0, y) = y + 1
f (x + 1, 0) = f (x, 1)
f (x + 1, y + 1) = f (x, f (x, f (x + 1, y)))

Demostrar que f es recursiva.

2. Sea la función n: N x N $\rightarrow$ N

n(x, y) = el número de pasos para evaluar A(x, y).

Demostrar:
a. n(x + 1, y) > y
b. n(x, y) > y
c. n(x + 1, y + 1) > A(x, y)

Demostrar que n no es primitiva recursiva.

Unidad 7.

El teorema fundamental de la representabilidad.

Práctica 7.

El teorema fundamental de la representabilidad.

1. La regla C (Choice)
La regla C permite la eliminación de cuantificadores existenciales por especialización (es decir pasar de $(\exists x)A(x)$ a $A(c)$) Para introducir la regla C es necesario modificar la definición de demostración de la siguiente manera:

Una demostración de una fbf B es una secuencia finita de fbf $D_1,D_2,D_3,\ldots,D_n = B$ tal que:
1.
a. D_i es axioma.
b. D_i se obtiene por MP de dos fbf anteriores en la secuencia.
c. D_i se obtiene de una fbf $(\exists x)C(x)$ anterior en la secuencia aplicando la regla C donde $D_i = C(d)$ y d es una constante nueva.

2. Los axiomas de 1.a pueden usar las constantes nuevas que aparezcan en aplicaciones de la regla C.

3. B no puede contener ocurrencias de las constantes nuevas que aparezcan en aplicaciones de la regla C.

Ver que si una fbf B puede derivarse a usando la regla C también puede derivarse sin usarla.
(Mendelson Pag 81 y 82)

2. Completar las demostraciones de representabilidad de las funciones derivadas por composición, recursión y minimización.

Unidad 8.

La aritmetización de los formalismos.

Esquema de aritmetización para símbolos, expresiones y secuencias.
Alfabetos primitivos recursivos.
Teoremas particulares para teorías con numerales.
Axiomas primitivos recursivos.
Sobre la decidibilidad de las demostraciones.

Práctica 8.

Demostrar que si K es una teoría con alfabeto primitivo recursivo (recursivo) las siguientes funciones y relaciones son primitivas recursivas (recursivas).

1. EVbl(x): x es el número de Gödel de una expresión que es una variable.
   EIC(x): x es el número de Gödel de una expresión que es una constante.
   EFL(x): x es el número de Gödel de una expresión que es un símbolo de función.
   EPL(x): x es el número de Gödel de una expresión que es un símbolo de predicado.

2. ArgF(x) = n si x es el número de Gödel de una expresión que es un símbolo funcional de aridad n.
   ArgP(x) = n si x es el número de Gödel de una expresión que es un símbolo de predicado de aridad n.

3. Gd(x): x es el número de Gödel de una expresión (secuencia de símbolos).

4. MP(x,y,z): z es el número de Gödel de una expresión que resulta de la aplicación de modus ponens a expresiones de números de Gödel x e y.

5. Gen(x,y): y es el número de Gödel de una expresión que resulta de la aplicación de generalización a una expresión de número de Gödel x.

6. Trm(x): x es el número de Gödel de un término.

7. Atfml(x): x es el número de Gödel de una fbf atómica.

8. Fml(x): x es el número de Gödel de una fbf.

9. Subst(x,y,u,v): x es el número de Gödel de una expresión que resulta de reemplazar en la expresión de

número de Gödel y las ocurrencias de la variable libre de número v por el termino de número u.

10. Sub(y,u,v) = n si Subst(n,y,u,v)

11. Fr(y,v): y es el número de Gödel de una fbf o un término que contiene apariciones libres de la variable de número v.

12. Ff(u,v,w): u es el número de Gödel de un término que esta libre para la variable con número v en la fbf con número w.

13. LAx(x): x es el número de Gödel de un axioma lógico.

14. Neg(x) = n si n es el número de Gödel de ¬A siendo x el número de A.

15. Cond(x,y) = n si n es el número de Gödel de (A ⊃ B) siendo x el número de A e y el número de B.

16. Clos(x) = n si n es el número de Gödel de la clausura de una fbf de número x.

17. Num(y) = n si n es el número de Gödel del numeral s(s(s(…0…))) (n veces)

18. Nu(x): x es el número de Gödel de un numeral.

19. D(u) = n si n es el número de Gödel de B(s(s(s(…0…)))) (u veces) y u es el número de Gödel B(x_1).

20. Ax(y): y es el número de Gödel de un axioma.

21. Prf(y): y es el número de Gödel de una demostración.

22. Pf(y,x): y es el número de Gödel de una demostración de la fbf de número x.

Bibliografía.

Computability and Logic, 3rd ed.
Jeffrey, Richard C. Boolos, George S. / 1997

Metalogic : An Introduction to the Metatheory of Standard First Order Logic
Geoffrey Hunter / 1996

Model Theory (Studies in Logic and the Foundations of Mathematics, Vol 73)
Chen Chung Chang, H. Jerome Keisler / 1990

A Shorter Model Theory
Wilfrid Hodges / 1997

Basic Model Theory (Studies in Logic, Language and Information)
Kees Doets / 1996

New Directions in the Philosophy of Mathematics : An Anthology
Thomas Tymoczko(Editor) / 1998

Mathematical Logic : An Introduction to Model Theory
A.H. Lightstone / 1978

Introducción a la Teoría de Modelos
Gonzalez Asenjo / 1977

The Limits of Mathematics : A Course on Information Theory and Limits of Formal Reasoning
Gregory J. Chaitin / 1998

Metamatematica
Paul Lorenzen / 1970

Logic for Mathematicians
A. Hamilton / 1985

Lógica de Primer Orden
Smullyan, Raymond M . / 1990

American Psycho : A Novel (Vintage Contemporaries)
Bret Easton Ellis / 1991

Symbolic Logic
Peter Suber / 1996
http://www.earlham.edu/~peters/courses/log/loghome.htm

Logical Systems
Peter Suber / 1996
http://www.earlham.edu/~peters/courses/logsys/lshome.htm

Formalized Mathematics
John Harrison / 1996
http://www.cybercom.net/users/rbjones/rbjpub/logic/jrh0100.htm

Trabajo Final

1. *La Teoría Q.*
Sea *Q* la teoría que tiene los mismos axiomas que PA a excepción del esquema axioma de inducción.
Sean *f1*, *f2* y *f3* las siguientes fórmulas bien formadas cerradas:
f1: $(\forall x)((0 + x) = x)$
f2: $(\forall x)(\forall y)((x + y) = (y + x))$
f3: $(\forall x)((0.x) = 0)$

Demostrar que ninguna de las fórmulas precedentes es teorema de *Q*.

2. *Teoremas de PA.*
Demostrar que las fórmulas *f1*, *f2* y *f3* del punto 1 son teoremas de PA.

3. *El Principio de Inducción*.
Demostrar que el esquema axioma de inducción es independiente de los demás axiomas de PA.

4. *La Fórmula de Gödel*.
Sea *G* la fórmula de Gödel y sea PAG la extensión de PA obtenida agregando $\neg G$ como axioma.
Demostrar que si PA es consistente PAG es consistente pero no ω-consistente.

5. *Decidibilidad de PA Sin Cuantificacion*.
a. Demostrar que para cada término cerrado *t* de PA existe un número natural *n* tal que $\vdash_{PA} (t = \overline{n})$.
b. Demostrar que para cada fórmula atómica de PA $(t = s)$ vale $\vdash_{PA} (t = s)$ o $\vdash_{PA} \neg(t = s)$.
c. Demostrar que el subconjunto de fórmulas cerradas de PA sin cuantificadores es decidible.

6. *Teorías Completas*.
Demostrar que una teoría K es completa si y solo si, para todas las fórmulas bien formadas cerradas B y C de K, si $\vdash_{K} B \vee C$ entonces $\vdash_{K} B$ o $\vdash_{K} C$.

7. *Independencia*.
Demostrar que para toda teoría K existe una teoría K', que tiene los mismos teoremas que K, cuyos axiomas son independientes.

8. *Teorías Finitamente Axiomatizables*.
Sean K_1 y K_2 dos teorías sobre el mismo lenguaje L tal que cualquier interpretación M de L es modelo de K_1 si y solo si no es modelo de K_2.

a. Demostrar que $K_1 \cup K_2$ es inconsistente.
b. Demostrar que K_1 y K_2 son finitamente axiomatizables.

9. *Extensiones e Indecidibilidad*.
Sean K y K' dos teorías sobre el mismo lenguaje L tal que K' tiene los axiomas de K más un número finito de axiomas propios.
Demostrar que si K' es indecidible también lo es K.

10. *Isomorfismos y Modelos Finitos*.
Sea K una teoría, M_1 y M_2 dos modelos normales finitos de K.
Demostrar que si M_1 y M_2 tienen el mismo conjunto de sentencias verdaderas entonces son isomorfos.

Teorema de las extensiones con no-teoremas

Sea K una teoría consistente de primer orden y sea A una fbf cerrada.

Si A no es teorema entonces K + {¬A} es consistente.

Dem:

Supongamos que K + {¬A} es inconsistente. Luego existe una fbf B tal que

$$\vdash_{K+\{\neg A\}} B \quad \text{y} \quad \vdash_{K+\{\neg A\}} \neg B$$

Pero

$$\vdash_{K+\{\neg A\}} (\neg B \supset (B \supset A)) \text{ por tautología}$$

Aplicando MP

$$\vdash_{K+\{\neg A\}} B \supset A$$

Aplicando MP nuevamente

$$\vdash_{K+\{\neg A\}} A$$

luego vale

$$\neg A \vdash_{K} A \quad \text{y usando el teorema de la deducción,}$$

$$\vdash_{K} \neg A \supset A \quad \text{y como} \quad \vdash_{K} (((\neg A) \supset A) \supset A)$$

aplicando MP

$$\vdash_{K} A \quad \text{lo cual contradice el enunciado.}$$

Teorema

SQ es consistente.

Dem:

Supongamos que existe una fbf A tal que

$$\vdash_{SQ} A \quad \text{y} \quad \vdash_{SQ} \neg A$$

Por Soundness theorem, A y ¬A son lógicamente válidas. absurdo.

Lema de Lindenbaum

Sea K una teoría de primer orden consistente. Existe una extensión de K que es consistente y completa respecto a la negación.

Dem:

Sea $A_1, A_2, \ldots, A_n, \ldots$ una numeración de las fbf cerradas de K.

Se construye una secuencia de extensiones K_i

$K_0 = K$

para cada $n \in N$

si $\vdash_{K_{n-1}} A_n$

entonces $K_n = K_{n-1}$

si no $K_n = K_{n-1} + \{\neg A_n\}$

Por el teorema de los no-teoremas, cada K_i es consistente.

Sea K_∞ la teoría de primer orden que tiene como axiomas a todos aquellos que son axiomas de alguna extensión K_i.

K_∞ es consistente y completa.

<u>Consistente</u>

Supongamos que K_∞ no sea consistente.

Existe una fbf B tal que

$$\vdash_{K_\infty} B \quad \text{y} \quad \vdash_{K_\infty} \neg B$$

Como las demostraciones son *finitas* existe un $n \in N$ tal que

$$\vdash_{K_n} B \quad \text{y} \quad \vdash_{K_n} \neg B$$

absurdo.

<u>Completa respecto a la negación</u>

Sea A_n la n-ésima fórmula cerrada, luego

$$\vdash_{K_n} A_n \quad \text{ó} \quad \vdash_{K_n} \neg A_n$$

luego

$$\vdash_{K_\infty} A_n \quad \text{ó} \quad \vdash_{K_\infty} \neg A_n$$

Teorías Cerradas

Sea K una teoría de primer orden que tiene al menos un término cerrado. K es **cerrada** si y solo si para cada fórmula A con una variable libre x, si la fórmula obtenida por la sustitución de la variable x por cualquier término cerrado es teorema de K entonces $\forall x$ A es teorema de K.

{informalmente: si algo es verdadero en todo elemento del dominio que tenga un nombre entonces es verdadero en todo elemento del dominio}

Teorema {extensiones cerradas}

Sea K una teoría de primer orden consistente. Existe una teoría K’ extensión de K que es consistente, cerrada y completa respecto a la negación.

Dem:

Sea K_0 la teoría resultante de agregar a K un conjunto enumerable de nuevas constantes con una numeración efectiva.

K_0 es consistente (dem: ejercicio[1])

Sea $\langle A_1, A_2, A_3, \ldots \rangle$ una enumeración de las fbf de K_0 con una única variable libre

y $\langle b_1, b_2, b_3, \ldots \rangle$ una enumeración de las constantes nuevas.

Sea S_1 la fbf

$$A_1(x_1/b) \supset \forall x_1\ A_1$$

donde x_1 es la variable libre de A_1 y b es la primer constante nueva que no aparece en A_1.

Sea S_n la fbf

$$A_n(x_n/b) \supset \forall x_n\ A_1$$

[1] Hunter, 45.11

donde x_n es la variable libre de A_n y b es la primer constante nueva que no aparece en $S_1, S_2, \ldots, S_{n-1}, A_n$.

Sea K_{n+1} la teoría que resulta de añadir S_{n+1} a K_n. Sea K_∞ la teoría que resulta de añadir todos los S_i a K_0.

K_∞ es una extensión de K.

<u>Consistente y cerrada</u>

1. K_i es consistente. (dem: ejercicio[2])

2. K_∞ es consistente.

<u>dem</u>:

Supongamos que no. Existe una fbf A tal que en K_∞ vale

$$\vdash_{K_\infty} A \quad \text{y} \quad \vdash_{K_\infty} \neg A$$

pero esas demostraciones involucrarían una cantidad finita de fórmulas, luego serían demostraciones en K_n para algún n. absurdo.

3. K_∞ es cerrada.

<u>dem</u>:

Sea A_k una fórmula con una variable libre x_k.

Supongamos que $A_k(x_k/c)$ es teorema de K_∞ para todo término cerrado c.

Sea b la nueva constante asociada a A_k en S_k, luego $A_k(x_k/b)$ es un teorema ya que b es un término cerrado.

Pero $(A_k(x_k/b) \supset \forall x_k\, A_k)$ es un axioma de K_∞. Aplicando modus ponens,

$$\vdash_{K_\infty} \forall x_k\, A_k$$

Luego, de suponer que una fórmula es teorema para cualquier término cerrado se llegó a que la fórmula cuantificada es teorema. Luego K_∞ es cerrada.

[2] Hunter, 45.12

Completa respecto a la negación

Por el lema de Lindenbaum existe K′ extensión de K_∞ que es consistente y completa respecto a la negación. Sólo falta ver que K′ sigue siendo cerrada.

La demostración es idéntica a la demostración de que K_∞ es cerrada ya que K′ no tiene nuevas fórmulas y se puede usar la enumeración de K_∞.

El teorema de Löwenheim – Skolem {para teorías cerradas}

Sea T una teoría de primer orden consistente, cerrada y completa respecto a la negación. T tiene un modelo numerable.

Dem:

Sea I una interpretación de T cuyo dominio D es el conjunto de términos cerrados de T.

D es numerable.

Reglas de asignación

1. A cada constante c_i se la interpreta con la constante c_i.
2. A cada símbolo funcional f_i^n se le asigna la función $f_i^n: D^n \to D$

   $f_i^n(t_1,\dots,t_n)= f_i^n(t_1,\dots,t_n)$
3. A cada símbolo relacional F_i^n se le asigna la relación $F_i^n \subseteq D^n$ tal que

   $(t_1,\dots,t_n)\in F_i^n$ sii $\vdash_T F_i^n(t_1,\dots,t_n)$

Ahora hay que ver que una fbf A es verdadera en la interpretación I si y sólo si $\vdash_T$ A (A es teorema) con lo cual I es modelo de T.

Demostración

Inducción sobre el número de cuantificadores y conectivos.

base n = 0

$A = R_i^n(t_1, t_2, \ldots, t_n)$

es verdadero en I sii es teorema de T por definición de I.

paso inductivo [veradero $\Leftrightarrow$ teorema]

1. $A = \neg B$
2. $A = B \supset C$
3. $A = \forall x\ B$

Caso 1: $A = \neg B$

$\Rightarrow$) Si A es verdadero en I, B no es verdadero en I entonces por HI B no es teorema de T y como T es completa respecto a la negación $\vdash_T \neg B$ o sea $\vdash_T A$.

$\Leftarrow$) Si A es teorema de T, $\neg B$ es teorema de T. Como T es consistente B no es teorema de T. Por HI B no es verdadero en I, luego como B es cerrada $\neg B$ es verdadero en I, luego A es verdadero en I.

Caso 2: $A = B \supset C$

Hint: como A es cerrada, B y C son cerradas y conviene demostrar [no verdadero $\Leftrightarrow$ no teorema].

$\Rightarrow$)Si A no es verdadero para I por tabla de verdad de la implicación B es verdadero para I y C es falso para I. Luego por HI

$$\vdash_T B$$

y como además T es completa respecto a la negación

$$\vdash_T \neg C$$

Además $B \supset (\neg C \supset \neg(B \supset C))$ es una tautología del cálculo proposicional con lo cual es teorema de T. Aplicando dos veces MP

$$\vdash_T \neg(B \supset C) \quad \text{luego} \quad \vdash_T \neg A$$

Como T es consistente A no es teorema.

$\Leftarrow$)Si A no es teorema de T como T es completo respecto a la negación

$\vdash_T \neg A$ es decir $\vdash_T \neg(B \supset C)$

Pero por instancias de tautologías

$\vdash_T \neg(B \supset C) \supset B$ y $\vdash_T \neg(B \supset C) \supset \neg C$

Luego aplicando MP

$\vdash_T B$ y $\vdash_T \neg C$

luego por HI y consistencia B es verdadero en I y C es falso en I. Con lo cual $B \supset C$ es falso en I que es lo mismo que A es falso en I.

Lemas necesarios

Lema 1

A es verdadero para I sii $\forall x$ A es verdadero para I.

Lema 2

$\vdash_K A$ sii $\vdash_K \forall x\ A$

Lema 3

Sea I una interpretación con dominio D.

Sea A una fbf con una única variable libre x.

Si I asigna cada elemento de D a un término cerrado y A(x/t) es verdadero para I para cada término cerrado t entonces $\forall x$ A es verdadero para I.

Lema 4

Sea I una interpretación.

Sea A una fbf con una única variable libre x.

Si A es verdadero para I entonces A(x/t), siendo t un término cerrado, es verdadero para I.

Caso 3: A = $\forall x$ B [verdadero $\Leftrightarrow$ teorema]

Dos posibiladades

1. B es cerrada
2. B es abierta

1. <u>B es cerrada</u>

$\Leftarrow$)Supongamos $\vdash_T A$ luego $\vdash_T \forall x\ B$

pero vale $\vdash_T \forall x\ B \supset B$ (por SQ4)

Por Modus Ponens $\vdash_T B$ luego por HI B es verdadero para I con lo cual (por **Lema 1**) $(\forall x)B$ es verdadero para I con lo que A es verdadero para I.

$\Rightarrow$) Supongamos que A es verdadero para I luego (por **Lema 1**) B es verdadero para I y por HI $\vdash_T B$ y (por **Lema 2**)

$\vdash_T \forall x\ B$ luego $\vdash_T A$

2. <u>B es abierta</u>

Como A es cerrado la única variable libre en B es x.

$\Leftarrow$) Supongamos $\vdash_T A$ luego $\vdash_T \forall x\ B$ luego por SQ4

$\vdash_T B(x/t)$ para cada término cerrado de T

por HI B(x/t) es verdadero en I luego (por **Lema 3**) $(\forall x)B$ es verdadero en I luego A es verdadero en I.

$\Rightarrow$) Supongamos que A es verdadero para I luego $(\forall x)B$ es verdadero para I, (por **Lema 1**) B es verdadero para I y (por **Lema 4**) B(x/t) con t cerrado es verdadero para I, luego por HI $\vdash_T B(x/t)$ luego como T es cerrado, $\vdash_T \forall x\ B$

o sea $\vdash_T A$

Teorema {completud}

Si una fórmula de SQ es lógicamente válida entonces es teorema.

Dem:

Sea C una fbf tal que no es teorema.

Luego SQ + $\{\neg C\}$ es consistente.

Luego SQ + $\{\neg C\}$ tiene modelo.

Luego $\neg C$ es verdadero, luego C no es lógicamente válida.

Teorema de Compacidad

Sea K una teoría de primer orden tal que todo subconjunto finito de axiomas tiene modelo. Entonces K tiene modelo.

Dem:

Supongamos que K no tiene modelo. Luego K es inconsistente. Luego existe una fbf B tal que

$$\vdash_K B \qquad \text{y} \qquad \vdash_K \neg B$$

pero ambas demostraciones son finitas luego involucran un número finito de axiomas.

Sea K′ la teoría que tiene como axiomas los que aparecen en las demostraciones de B y $\neg$B.

$$\vdash_{K'} B \qquad \text{y} \qquad \vdash_{K'} \neg B$$

luego K′ es inconsistente. Luego K′ no tiene modelo, lo cual es absurdo.

El conjunto de todos los conjuntos de números naturales

Supongamos que los conjuntos de números naturales son numerables. Luego forman una sucesión $C_0, C_1, \ldots, C_n, \ldots$

	0	1	2	3	4	5	6	…
C_0	si	si	no	no	si	no	si	…
C_1	no	si	no	si	si	…		
C_2	no	no	no	…				
C_3	…							

Sea C el siguiente conjunto de números naturales:

$$i \in C \quad \text{sii} \quad i \notin C_i$$

luego C es un conjunto de números naturales y no es ninguno en la numeración.

Absurdo de suponer que eran numerables.

Teorema ascendente de Löwenheim – Skolem

Si una teoría de primer orden tiene un modelo infinito entonces tiene un modelo de una cardinalidad infinita cualquiera.

Isomorfismo de Modelos

Sea K una teoría de primer orden y sean M y M′ dos modelos de K con dominios D y D′.

M y M′ son isomorfos sii existe una función biyectiva

$I: M \to M'$ tal que

- si en D $c \to d$

  en D′ $c \to I(d)$

  o sea $I(c^M) = c^{M'}$
- si en D $f(d_1,\ldots,d_n) \to d$

  en D′ $f(I(d_1),\ldots,I(d_n)) \to I(d)$

  o sea $I(f^M(d_1,\ldots,d_n)) = f^{M'}(I(d_1),\ldots,I(d_n))$
- $(d_1,\ldots,d_n) \in F^M$ sii $(I(d_1),\ldots,I(d_n)) \in F^{M'}$

Teorema

Sea K una teoría de primer orden y A una fbf cerrada. Sean M y M′ modelos isomorfos de K, entonces A es verdadero para M sii A es verdadero para M′.

α-categoricidad

Sea T una teoría consistente.

T es α–categórica para algún cardinal α sii todos los modelos de cardinal α son isomorfos.

Teorema de Vaught

Sea T una teoría consistente.

Si T es α-categórica para algún cardinal α infinito entonces es completa respecto a la negación.

Dem:

Supongamos que T no tiene modelos finitos, es α-categórica y no es completa.

Luego existe una fbf A tal que

$$\not\vdash_T A \qquad \text{y} \qquad \not\vdash_T \neg A$$

Por el lema de los no-teoremas T + {A} y T + {¬A} son consistentes.

Sean M_1 y M_2 dos modelos respectivos. Luego existen modelos del cardinal α que da la α-categoricidad y deben ser isomorfos lo cual es absurdo.

Teorías de primer orden con igualdad ($SQ^=$)

Se nota F_1^2 con =

E1) $x_i = x_i$

E2) $t_k = U \supset f_i^n(t_1,\ldots,t_k,\ldots,t_n) = f_i^n(t_1,\ldots,U,\ldots,t_n)$

E3) $t_k = U \supset f_i^n(t_1,\ldots,t_k,\ldots,t_n) \supset f_i^n(t_1,\ldots,U,\ldots,t_n)$

Teoremas:

- Consistencia: $SQ^=$ es consistente.
- Completitud:

Si una fbf A es verdadera en todo modelo normal de $SQ^=$ entonces es teorema de $SQ^=$. (dem: ejercicio)

Sistema formal

Un sistema formal S es un lenguaje formal L junto con un mecanismo deductivo que viene dado por

1. El establecimiento de ciertas fbf llamadas AXIOMAS.
2. El establecimiento de ciertas reglas de transformación o inferencia entre fbf. $\left(\frac{\text{premisa}_1, \text{premisa}_2, \ldots}{\text{conclusion}}\right)$

La teoría de la demostración

Consiste en las derivaciones sintácticas a partir del sistema formal.

La semántica o teoría de modelos

Consiste en la interpretación de las construcciones sintácticas de un sistema formal.

La metateoría

Considera los sistemas formales, los mecanismos deductivos y sus interpretaciones como objetos de estudio.
Los teoremas de consistencia, completitud, etc. pertenecen a la metateoría.

Sistemas formales finitistas

- alfabeto finito.
- fórmulas de longitud finita.
- reglas de inferencia con un número finito de premisas.

Teoremas

- un SFF tiene una cantidad numerable de fbf.
- un SFF tiene una cantidad numerable de teoremas.
- en un SFF las demostraciones tienen longitud finita.

Teorema

Si el conjunto de fórmulas de un SF S es decidible y existe un método efectivo para establecer si una cadena de fbf es una demostración entonces el conjunto de teoremas de S es efectivamente enumerable.

Teorema

Si S es un SFF cuyo conjunto de axiomas es decidible entonces el conjunto de teoremas es efectivamente enumerable.

Para teorías de primer orden

Si una teoría de primer orden tiene un conjunto de axiomas decidible y es completa respecto a la negación entonces es decidible.

k-validez

Una fbf A de SQ es k-válida sii es verdadera para toda interpretación de k elementos.

El análisis de los dominios de interpretación

Sea I una interpretación de dominio D de k elementos.

Cuántas relaciones n-arias son posibles en un dominio de k elementos?

Sea R una relación

$R \subseteq D^n$

$R \in \wp(D^n)$

Basta ver cuantos elementos tiene $\wp(D^n)$.

Como D^n tiene k^n elementos, $\wp(D^n)$ tiene $2^{(k^n)}$ elementos.

Luego existen $2^{(k^n)}$ relaciones n-arias en un dominio D de k elementos.

Teorema

La k-validez de una fbf A de SQ es decidible.

Dem:

Inducción sobre la complejidad de A.

Ejemplos[3]

1. La fórmula A: $F(x) \supset \forall x\ F(x)$ es 1-válida.

Dem:

Sea $D = \{d\}$ $k=1$, $n=1$

2 casos: hay que investigar $2^{(1^1)}$ relaciones.

a. $d \in F^I$ y   b. $d \notin F^I$

a. $d \in F^I$

Vale $F(x)$ para d, también vale $\forall x\ F(x)$, luego vale $F(x) \supset \forall x\ F(x)$

b. $d \notin F^I$

No vale $F(x)$ para d, y no vale $\forall x\ F(x)$, luego vale $F(x) \supset \forall x\ F(x)$

Conclusión: A es 1-válida.

2. La fórmula A: $F(x) \supset \forall x\ F(x)$ no es 2-válida.

Dem:

Sea $D = \{d_1, d_2\}$ $k=2$, $n=1$

Hay que analizar $2^{(2^1)}$ relaciones.

1. $F^I = \{d_1, d_2\}$
2. $F^I = \{d_1\}$
3. $F^I = \{d_2\}$
4. $F^I = \varnothing$

Caso 1:

$F(x)$ vale para d_1 y d_2 y $\forall x\ F(x)$ vale para d_1 y d_2, luego $F(x) \supset \forall x\ F(x)$ vale para d_1 y d_2.

Caso 2:

$F(x)$ vale para d_1

$F(x)$ no vale para d_2

$\forall x\ F(x)$ no vale

luego cuando x vale d_1 queda $V \supset F$ lo que es falso.

[3] Ejercicios: Hunter, pág 191.

La lógica de predicados monádicos de primer orden

Definición

Es igual a SQ salvo que no tiene símbolos funcionales y sus únicos símbolos relacionales son monádicos.

Semántica

Igual que SQ.

Teoría de la demostración

Igual que SQ.

Teorema {completud semántica}

- Sea A una fbf cerrada de SQ^M.
  A es lógicamente válida sii A es teorema.
- SQ^M no es completo respecto a la negación.
- SQ^M no es sintácticamente completo.

Lema 1

Si una fbf cerrada A de SQ^M es falsa en una interpretación I de k elementos entonces es falsa para una interpretación I′ de k+1 elementos.

Nota: Vale para SQ.

Dem:

Sea A una fbf cerrada con n símbolos relacionales distintos $F_1,\dots,F_n$ y sea I una interpretación con dominio D de k elementos.

$D = \{d_1,d_2,\dots,d_k\}$

Sea I′ una nueva interpretación con dominio D′ tal que

$D = \{d_1,d_2,\dots,d_k,b\}$

La idea es que b se comporte como algún $d \in D$.

I´ hace las mismas interpretaciones de constantes (no hay símbolos funcionales) y las relaciones son las siguientes:

$F_j^{I'}(d_i)$ sii $F_j^{I}(d_i)$

$F_j^{I'}(b)$ sii $F_j^{I}(d)$

Se demuestra por inducción sobre la complejidad de A.

Lema 2

Si una fbf cerrada C de SQ^M con k símbolos relacionales distintos es falso para una interpretación I entonces es falso para una interpretación I' con un dominio de a lo sumo 2^k elementos.

Dem:

Sea C una fbf cerrada de k símbolos predicativos.

Sean $F_1,\ldots,F_k$ dichos símbolos.

Sea I una interpretación donde C es falso con dominio D.

Se parte el dominio en las siguientes clases:

$C_1 = \{d \in D \;/\; F_1^I(d) \wedge \neg F_2^I(d) \wedge \ldots \wedge \neg F_k^I(d)\}$

$C_2 = \{d \in D \;/\; \neg F_1^I(d) \wedge F_2^I(d) \wedge \ldots \wedge \neg F_k^I(d)\}$

…

Hay a lo sumo 2^k clases (algunas pueden ser vacías) (se piensan como números binarios de longitud k).

Se define I' donde el dominio son las clases anteriores.

Es fácil ver que todos los elementos de una clase cumplen las mismas propiedades.

Falta interpretar los símbolos relacionales de I'.

Se define

$F_i^{I'}(C)$ sii $F_i^{I}(d)$ para todo $d \in C$

donde C es una clase de D.

Luego se aplica inducción.

Teorema de la decidibilidad de SQ^M

Una fbf cerrada A de SQ^M con k símbolos relacionales distintos es lógicamente válida sii es 2^k-válida.

Dem:

$\Rightarrow$) A es lógicamente válida entonces es 2^k-válida.

$\Leftarrow$) Sup A no es lógicamente válida.

Luego es falso para alguna interpretación I.

Luego por **Lema 2** es falso para alguna I′ de a lo sumo 2^k elementos.

Luego iterando el **Lema 1** es falso para exactamente 2^k elementos luego no es 2^k-válida.

Pero la 2^k validez es decidible.

Los cuerpos de característica cero

Un cuerpo de característica p tiene p axiomas del tipo

A_1: $1 \neq 0$

A_2: $1 + 1 \neq 0$

A_3: $1 + 1 + 1 \neq 0$

…

A_p: $1 + 1 + 1 + \ldots + 1 \neq 0$ (p veces)

A_{p+1}: $1 + 1 + 1 + \ldots + 1 = 0$ (p+1 veces)

Los de característica cero tienen numerables axiomas.

Existe alguna axiomatización finita?

Lema

Sea A una fbf tal que $\vdash_{CC_0}$ A luego $\vdash_{CC_n}$ A para algún $n > n_0$.

Dem:

$\vdash_{CC_0}$ A usa un número finito de axiomas.

Teorema

No existe axiomatización finita de CC_0.

Dem:

Supongamos que existe. Sean $B_1,\ldots,B_k$ los axiomas.

Sea $A = B_1 \wedge B_2 \wedge \ldots \wedge B_k$

luego $\vdash_{CC_0}$ A y por teorema anterior $\vdash_{CC_n}$ A $n > n_0$

pero de A se deducen todos los teoremas de CC_0.

En particular $1 + 1 + \ldots + 1 \neq 0$ (n+1 veces) que no es cierto en CC_n.

La teoría de grupos

El lenguaje

Variables: $x_1, x_2, \ldots, x_n, \ldots$

Constante: a_1 {identidad}

Funciones: f_1^1 {inversa} f_1^2 {producto}.

Relaciones: =

Axiomas

- Los de SQ
- Los de igualdad
- G1: $f_1^2(f_1^2(x_1,x_2),x_3)= f_1^2(x_1,f_1^2(x_2,x_3))$ {asoc}
- G2: $f_1^2(a_1,x_1)= x_1$ {ident}
- G3: $f_1^2(f_1^1(x_1),x_1)= a_1$ {inverso}
- La teoría de grupos no es decidible.
- La de abelianos sí lo es.

La aritmética de Peano

El lenguaje

Variables: $x_1, x_2, x_3, \ldots, x_n, \ldots$

Constante: 0

Símbolos funcionales: S, +, .

Símbolos predicativos: =

Los axiomas

Los usuales de teorías con igualdad y además G axiomas y 1 axioma esquema.

PA1: $\forall x_1 \neg(S(x_1) = 0)$

PA2: $\forall x_1 \forall x_2 (S(x_1) = S(x_2) \supset x_1 = x_2)$

PA3: $\forall x_1 (x_1 + 0 = x_1)$

PA4: $\forall x_1 \forall x_2 (x_1 + S(x_2) = S(x_1 + x_2))$

PA5: $\forall x_1 (x_1 . 0 = 0)$

PA6: $\forall x_1 \forall x_2 (x_1 . S(x_2) = (x_1 . x_2) + x_1))$

PA7: Para toda fbf A de PA en la cual x_1 está libre, $A(0) \supset (\forall x_1 (A(x_1) \supset A(S(x_1))) \supset \forall x_1 A(x_1)$

<u>Notas</u>

- PA1 + PA2 + PA7 definen los números naturales. No ocurre como en la aritmética de segundo orden que sus modelos sean isomorfos.
- En PA1 + PA2 + PA7 no se puede expresar la relación <.
- PA1 + PA2 + PA3 + PA4 + PA7 forman la aritmética de Presburguer que es consistente y decidible pero no puede expresar la potencia.

  Es decidible en tiempo $O(2^{(2^n)})$ para una fbf de n símbolos[4].

Los axiomas originales de Peano

Los axiomas originales pretenden definir el conjunto de números naturales N.

1. $0 \in N$
2. $n \in N$ entonces $n' \in N$
3. no existe $n \in N$ tal que $n' = 0$
4. si $m,n \in N$ y $m' = n'$ entonces $m = n$
5. $A \subseteq N$. Si $0 \in A$ y $n \in A \supset n' \in A$ entonces $N = A$.

Teorema

Los axiomas originales de Peano determinan N unívocamente.

(4) Fisher & Rabin 1974

Dem:

Sup. N y M satisfacen los axiomas de Peano.

por 1, $0 \in N$ y $0 \in M$

Sea $A = N \cap M$.

$0 \in A$ y si $n \in A$ entonces $n \in N$ y $n \in M$ luego por 2, $n' \in N$ y $n' \in M$ luego $n' \in A$ por 5, $A = N$ y $A = M$, con lo cual $N = M$.

Nota

Estos axiomas se pueden formalizar en lógica de segundo orden y obtener el siguiente teorema.

Teorema de categoricidad de PA de segundo orden

Los modelos de PA de segundo orden son isomorfos.

El modelo Standard de PA en ZF

$0 = \emptyset$

$1 = \{\emptyset, \{\emptyset\}\}$

$2 = \{\emptyset, \{\emptyset\},\{\emptyset, \{\emptyset\}\}\}$

$3 = \{\emptyset, \{\emptyset\},\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\},\{\emptyset, \{\emptyset\}\}\}\}$

…

$s(x) = x \cup \{x\}$

Pregunta

¿Se pueden demostrar propiedades de la aritmética en ZF que no se pueden demostrar en PA?

Si. Hay una extensión finita del teorema de Ramsey que puede ser expresado en PA y puede ser probado en ZFC pero no en PA (suponiendo PA consistente)[5].

---

[5] Paris and Kirby 1977

Goodstein’s Amazing Sequence

Dado un entero positivo n, otro entero $P_x(n)$ puede ser construido de la siguiente manera:

Escribiendo n en base x (x > 1), o sea,

$n = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$

donde $0 \le a_i < x$ para $i = 0,1,\ldots,k$. Luego, se escribe cada exponente de x en su expresión en base x, y así sucesivamente hasta que todos los exponentes, exponentes de exponentes, ect. estén escritos en base x.

Ahora definimos $P_x(n)$ retando uno y reemplazando cada aparición de x en esa expresión por x+1.

Por ejemplo, si n=529 y x=2 entonces

$529 = 2^9+2^4+1 = 2^{2^3+1}+2^{2^2}+1 = 2^{2^{2+1}+1}+2^{2^2}+1,$

y $P_2(529) = 3^{3^{3+1}+1}+3^{3^3} \approx 1.33 \times 10^{39}$.

La sucesión n, $P_x(n)$, $P_{x+1}(P_x(n))$, $P_{x+2}(P_{x+1}(P_x(n)))$,… es una *Goodstein sequence*.

Restricted ordinal theorem

Para todo par de enteros positivos n y x (x>1), la sucesión

n, $P_x(n)$, $P_{x+1}(P_x(n))$, $P_{x+2}(P_{x+1}(P_x(n)))$,…

llega a cero en un número finito de pasos.

Este resultado es análogo al hecho de que toda secuencia estrictamente decreciente de ordinales transfinitos es finita. Goodstein lo demostró usando inducción tranfinita, y en 1982 Kirby y Paris demostraron que esta propiedad que es estrictamente de teoría de números, no se puede probar en aritmética de primer orden.

Un modelo de PA no isomorfo al standard {no clásico}

Sea PA′ como PA con los siguientes axiomas nuevos:

$c \neq 0$

$c \neq S(0)$

$c \neq S(S(0))$

…

todo subconjunto finito de PA′ tiene modelo interpretando a c como el mayor número que aparece en los axiomas nuevos más uno.

Por el teorema de compacidad PA′ tiene modelo y por lo tanto también tiene un modelo normal M′ (que es modelo de PA).

Si C es el modelo clásico, se tiene que

Teorema

M′ no es isomorfo a C.

Dem:

ejercicio. Se usa el siguiente lema:

Lema

Sea T una teoría de primer orden. M y M′ modelos isomorfos de T, $I: M \to M'$.

Para todo término cerrado t se cumple

$$I(t^M) = t^{M'}$$

Dem:

Inducción

- $t = c$

  $I(t^M) = I(c^M) =^{(6)} c^{M'} = t^{M'}$

- $t = f(t_1,\ldots,t_k)$

  $I(t^M) = I(f(t_1,\ldots,t_k)^M) = I(f^M(t_1{}^M,\ldots,t_k{}^M)) =^{(6)}$

(6) Def. de isomorfismo

$= f^{M'}(I(t_1^M),\ldots,I(t_k^M)) =^{(7)} f^{M'}(t_1^{M'},\ldots,t_k^{M'}) = f(t_1,\ldots,t_k)^{M'} =$
$= t^{M'}$

Axiomas de Peano con igualdad

$PA^{=}1.\ x_1 = x_2 \Rightarrow (x_1 = x_3 \Rightarrow x_2 = x_3)$

$PA^{=}2.\ x_1 = x_2 \Rightarrow S(x_1) = S(x_2)$

Estos axiomas pueden reemplazar para el caso particular de PA los axiomas usuales de teorías con igualdad. (Los 7 axiomas usuales más estos 2 forman una teoría con igualdad[8]).

Numerales

Los términos 0,S(0),S(S(0)),… son llamados numerales y se notan $\overline{0}, \overline{1}, \overline{2}, \ldots$ En general si $n \in N$, $\overline{n}$ denota el término en el lenguaje de PA compuesto por n aplicaciones del símbolo funcional S a la constante 0.

Teoremas que involucran numerales

1. $(\forall x)\ \ x + \overline{1} = s(x)$
2. $(\forall x)\ \ x\ .\ \overline{1} = x$
3. $(\forall x)\ \ x\ .\ \overline{2} = x + x$

Metateoremas que involucran numerales

$n, m \in N$

1. $n = m$ entonces $\vdash_{PA} \overline{n} = \overline{m}$
2. $n \neq m$ entonces $\vdash_{PA} \overline{n} \neq \overline{m}$

---

[7] Hip. inductiva
[8] Mendelson – pag. 159

Lema de la desigualdad

$m \neq n$ entonces $\vdash_{PA} \neg(\overline{m} = \overline{n})$

Dem:

2 casos: $m > n$ y $m < n$. Se demuestra para $m > n$.

Luego existe $k > 0$ tal que $n = m + k$.

1. $\vdash_{PA} \overline{m} = \overline{m+k} \supset \overline{m-1} = \overline{m+k-1}$ instancia de PA2

2. $\vdash_{PA} \overline{m-1} = \overline{m+k-1} \supset \overline{m-2} = \overline{m+k-2}$ instancia de PA2

3. $\vdash_{PA} \overline{m} = \overline{m+k} \supset \overline{m-2} = \overline{m+k-2}$ HS[9] a 1 y 2

Iterando 1, 2 y 3 se tiene

4. $\vdash_{PA} \overline{m} = \overline{m+k} \supset \overline{0} = \overline{k}$

Como $k > 0$

5. $\vdash_{PA} \overline{k} = S(\overline{k-1})$ por igualdad

6. $\vdash_{PA} \overline{m} = \overline{m+k} \supset \overline{0} = S(\overline{k-1})$ reemp. en 4

Pero por contrarrecíproco (caso de tautología)

7. $\vdash_{PA} \neg(\overline{0} = S(\overline{k-1})) \supset \neg(\overline{m} = \overline{m+k})$

8. $\vdash_{PA} \neg(\overline{0} = S(\overline{k-1}))$ PA1

Por MP entre 7 y 8

$\vdash_{PA} \neg(\overline{m} = \overline{m+k})$

finalmente

$\vdash_{PA} \neg(\overline{m} = \overline{n})$

Lema de la suma

$\vdash_{PA} \overline{m} + \overline{n} = \overline{m+n}$

Dem:

Si $n = 0$ queda $\overline{m} + \overline{0} = \overline{m+0}$ que es un caso de PA3.

Si $n > 0$ entonces $\overline{n} = S(\overline{n-1})$ luego

---

[9] HS: $\dfrac{A \supset B \quad B \supset C}{A \supset C}$

1. $\vdash_{PA} \overline{m} + \overline{n} = \overline{m} + S(\overline{n-1})$ igualdad

2. $\vdash_{PA} \overline{m} + S(\overline{n-1}) = S(\overline{m} + \overline{n-1})$ PA4

3. $\vdash_{PA} \overline{m} + \overline{n} = S(\overline{m} + \overline{n-1})$ $PA^{=}1$ de 1 y 2.

se repite el proceso hasta llegar a

4. $\vdash_{PA} \overline{m} + \overline{n} = S(S(\ldots S(\overline{m} + \overline{0})\ldots))$ (n veces)

5. $\vdash_{PA} \overline{m} + \overline{0} = \overline{m}$ PA3

6. $\vdash_{PA} \overline{m} + \overline{n} = S(S(\ldots S(\overline{m})\ldots))$ (n veces) por igualdad

7. $\vdash_{PA} \overline{m} + \overline{n} = \overline{m+n}$ por def. de numeral

Definición de relaciones en PA

Sean t y s términos de PA y w una variable que no está en t ni en s.

$t < s$ es una abreviatura para

$$\exists w\ (w \neq 0 \wedge w + t = s)$$

$t \leq s$ para $t < s \vee t = s$

$t > s$ para $s < t$

$t \geq s$ para $s \leq t$

Notación: Cuantificador existencial único

$(\exists! x)A(x)$ es una abreviatura para

$(\exists x)(A(x) \wedge \forall y(A(y) \supset x = y))$

Representabilidad

Expresable

Sea K una teoría con el lenguaje de PA.

$R \subseteq N^n$ es expresable en K si y solo si existe una fbf $\beta(x_1,\ldots,x_n)$ con variables libres $x_1,\ldots,x_n$ tal que para $k_1,k_2,\ldots,k_n \in N$ se verifica

1. si $(k_1,k_2,\ldots,k_n) \in R$ entonces $\vdash_{K} \beta(\overline{k_1}, \overline{k_2}, \ldots, \overline{k_n})$
2. si $(k_1,k_2,\ldots,k_n) \notin R$ entonces $\vdash_{K} \neg\beta(\overline{k_1}, \overline{k_2}, \ldots, \overline{k_n})$

Representable

Sea K una teoría con el lenguaje de PA.

f: $N^n \to N$ es representable en K si y solo si existe una fbf $\beta(x_1,\dots,x_n,y)$ con variables libres $x_1,\dots,x_n,y$ tal que para $k_1,k_2,\dots,k_n,m \in N$ se verifica

1. si $f(k_1,k_2,\dots,k_n)= m$ entonces $\vdash_K \beta(\overline{k_1},\overline{k_2},\dots,\overline{k_n},\overline{m})$
2. si $f(k_1,k_2,\dots,k_n)\neq m$ entonces $\vdash_K \neg\beta(\overline{k_1},\overline{k_2},\dots,\overline{k_n},\overline{m})$
3. $\vdash_K (\exists! y)\beta(\overline{k_1},\overline{k_2},\dots,\overline{k_n},y)$ para todo $k_1,k_2,\dots,k_n \in N$

Teorema

Sea f: $N^2 \to N$,

$m,n \,\alpha\, m+n$

f es representable en PA.

Dem:

Sea $A(x_1,x_2,x_3)$ la fbf $x_3 = x_1 + x_2$.

Para ver que A representa a f hay que probar:

i. $p = m + n$ entonces $\vdash_{PA} \overline{p} = \overline{m} + \overline{n}$

ii. $p \neq m + n$ entonces $\vdash_{PA} \neg(\overline{p} = \overline{m} + \overline{n})$

iii. $\vdash_{PA} (\exists! x_3)(x_3 = \overline{m} + \overline{n})$

Por lema de la suma en PA vale

$\vdash_{PA} \overline{m} + \overline{n} = \overline{m+n}$

luego

i. $p = m + n$ entonces $\vdash_{PA} \overline{p} = \overline{m+n}$ por igualdad

$\vdash_{PA} \overline{p} = \overline{m} + \overline{n}$ por lema de la suma

ii. $p \neq m + n$ por lema de la desigualdad

$\vdash_{PA} \neg\, \overline{p} = \overline{m+n}$

luego por igualdad

$\vdash_{PA} \neg\, \overline{p} = \overline{m} + \overline{n}$

iii. Hay que demostrar

$\vdash_{PA} (\exists x_3)(x_3 = \overline{m} + \overline{n} \wedge (\forall x)\, x = \overline{m} + \overline{n} \supset x = x_3)$

Para demostrar el existencial basta ver un caso.

$\vdash_{PA} \overline{m+n} = \overline{m} + \overline{n} \wedge (\forall x)\ x = \overline{m} + \overline{n} \supset x = \overline{m+n}$

La primera parte de la conjunción está probada

Faltaría ver que

$\vdash_{PA} (\forall x)\ x = \overline{m} + \overline{n} \supset x = \overline{m+n}$

(queda como ejercicio)

Teorema

Sea f: $\quad N \rightarrow N$

$\qquad n \ \alpha\ 2.n$

f es representable en PA.

Dem:

La fbf propuesta es $A(x_1,x_2) \quad x_2 = x_1 . \overline{2}$

Hay que ver

i. $n = 2\ m$ entonces $\vdash_{PA} \overline{n} = \overline{m}.\overline{2}$

ii. $n \neq 2\ m$ entonces $\vdash_{PA} \neg\ \overline{n} = \overline{m}.\overline{2}$

iii. $\vdash_{PA} (\exists! x_2)\ x_2 = \overline{m}.\overline{2}$

i. $n = 2\ m$

$\overline{m}.\overline{2} = \overline{m}.s(s(0))$	notación
$= (\overline{m}.s(0)) + \overline{m}$	PA6
$= (\overline{m}.\overline{0} + \overline{m}) + \overline{m}$	PA6
$= (\overline{0} + \overline{m}) + \overline{m}$	PA5
$= \overline{m} + \overline{m}$	PA3
$= \overline{m+m}$	lema de la suma
$= \overline{2\ m}$	notación
$= \overline{n}$	

ii. $n \neq 2\ m$

$\vdash_{PA} \neg\ \overline{n} = \overline{2\ m}$	lema de la desigualdad
$\vdash_{PA} \overline{2\ m} = \overline{m}.\overline{2}$	item 1

luego

$\vdash_{PA} \neg\ \overline{n} = \overline{m}\,.\,\overline{2}$ por igualdad

iii. ejercicio

Teorema

Sea S una teoría de primer orden con el lenguaje PA tal que la relación de identidad está representada por la fbf x = y luego para probar representabilidad no es necesario probar la condición ii.

Dem:

Sea $f\colon N^n \to N$ que satisface las condiciones i y iii de representabilidad usando la fbf A.

i. Si $f(k_1,\ldots,k_n) = m$ entonces $\vdash_S A(\overline{k}_1, \overline{k}_2, \ldots, \overline{k}_n, \overline{m})$

iii. $\vdash_S (\exists! y)\ A(\overline{k}_1, \ldots, \overline{k}_n, y)$

Habría que demostrar

ii. Si $f(k_1,\ldots,k_n) \neq m$ entonces $\vdash_S \neg\ A(\overline{k}_1, \overline{k}_2, \ldots, \overline{k}_n, \overline{m})$

Sup $f(k_1,\ldots,k_n) \neq m$

Como la identidad está representada en S por x = y

1. $\vdash_S \neg\ \overline{f(k_1,\ldots,k_n)} = \overline{m}$

y por iii

2. $\vdash_S (\exists! y)\ A(\overline{k}_1, \ldots, \overline{k}_n, y)$ que es lo mismo que

3. $\vdash_S \exists y\ A(\overline{k}_1, \ldots, \overline{k}_n, y) \wedge \forall x (A(\overline{k}_1, \ldots, \overline{k}_n, x) \supset y = x)$

Como el existencial abarca toda la fórmula, se puede demostrar que de 3 instanciando

$y = \overline{f(k_1,\ldots,k_n)}$ y

$x = \overline{m}$

4. $\vdash_S A(\overline{k}_1, \ldots, \overline{k}_n, \overline{m}) \supset \overline{f(k_1,\ldots,k_n)} = \overline{m}$

Aplicando contrarrecíproco

5. $\vdash_S \neg\ \overline{f(k_1,\ldots,k_n)} = \overline{m} \supset \neg\ A(\overline{k}_1, \ldots, \overline{k}_n, \overline{m})$

Por MP 1 y 5

6. $\vdash_S \neg\ A(\overline{k}_1, \ldots, \overline{k}_n, \overline{m})$

La μ-recursividad de la función de Ackermann

Regla 1 $A(0,y) = y^+$

Regla 2 $A(x^+,0) = A(x,1)$

Regla 3 $A(x^+,y^+) = A(x,A(x^+,y))$

Ejemplo:

PASO	EVALUACION	TUPLA	cant. elementos	ψ	
0	A(2,1)	(2,1)	$2^2.3^2.5^1$	180	$\psi(2,1,0)$
1	A(1,A(2,0))	(1,2,0)	$2^3.3^1.5^2.7^0$	600	$\psi(2,1,1)$
2	A(1,A(1,1))	(1,1,1)	$2^3.3^1.5^1.7^1$	840	$\psi(2,1,2)$
3	A(1,A(0,A(1,0)))	(1,0,1,0)	$2^4.3^1.5^0.7^1.11^0$	336	$\psi(2,1,3)$
4	A(1,A(0,A(0,1)))	(1,0,0,1)	$2^4.3^1.5^0.7^0.11^1$	528	$\psi(2,1,4)$
5	A(1,A(0,2))	(1,0,2)	$2^3.3^1.5^0.7^2$	1176	$\psi(2,1,5)$
6	A(1,3)	(1,3)	$2^2.3^1.5^3$	1500	$\psi(2,1,6)$
7	A(0,A(1,2))	(0,1,2)	$2^3.3^0.5^1.7^2$	1960	$\psi(2,1,7)$
8	A(0,A(0,A(1,1)))	(0,0,1,1)	$2^4.3^0.5^0.7^1.11^1$	1232	$\psi(2,1,8)$
9	A(0,A(0,A(0,A(1,0)))	(0,0,0,1,0)	$2^5.3^0.5^0.7^0.11^1.13^0$	352	$\psi(2,1,9)$
10	A(0,A(0,A(0,A(0,1)))	(0,0,0,0,1)	$2^5.3^0.5^0.7^0.11^0.13^1$	416	$\psi(2,1,10)$
11	A(0,A(0,A(0,2)))	(0,0,0,2)	$2^4.3^0.5^0.7^0.11^2$	1936	$\psi(2,1,11)$
12	A(0,A(0,3))	(0,0,3)	$2^3.3^0.5^0.7^3$	2744	$\psi(2,1,12)$
13	A(0,4)	(0,4)	$2^2.3^0.5^4$	2500	$\psi(2,1,13)$
14	5	5	$2^1.3^5$	486	$\psi(2,1,14)$

$\psi: N^3 \to N$

$\psi(2,1,14) = 486$

$\psi(2,1,15) = 486$

$\psi(2,1,16) = 486$

…

Se define $\psi: N^3 \to N$

$\psi(x,y,z)$= número de Gödel del n-ésimo paso en la evaluación de A(x,y) y luego se completa con el último valor (cuando <u>n</u> supera el número de pasos).

ψ se denomina la **traza** de la evaluación de A. Se quiere ver que ψ es una PRF.

Para esto se necesita ver a cada natural como el nº de Gödel de una tupla. Para esto se IGNORAN los exponentes adicionales, y se trata $2^k.3^{w1}.5^{w2}.\ldots.p_k^{wk}.p_{k+1}^{wk+1}.\ldots.p_m^{wm}$ como si fuera $2^k.3^{w1}.5^{w2}.\ldots.p_k^{wk}$

Luego se definen las funciones de SELECCIÓN

$$Q_i(z) = \begin{cases} 1 & \text{z es el nº de Gödel de una tupla a la que se le aplicó la regla i.} \\ 0 & \text{si no.} \end{cases}$$

$i=1,2,3$

Se puede ver en el ejemplo a cada tupla qué regla se le aplica.

PASO	EVALUACION	TUPLA	REGLA
0	A(2,1)	(2,1)	3
1	A(1,A(2,0))	(1,2,0)	2
2	A(1,A(1,1))	(1,1,1)	3
3	A(1,A(0,A(1,0)))	(1,0,1,0)	2
4	A(1,A(0,A(0,1)))	(1,0,0,1)	1
5	A(1,A(0,2))	(1,0,2)	1

Hay que ver que Q_i son PR.

$Q_1(z)= 1$ sii el anteúltimo elemento de la tupla asociada a z es igual a cero,

luego

$Q_1(z)= 1$ sii $E(0,z) > 1 \wedge E(E(0,z) \dot{-} 1,z) = 0$

luego

$Q_1(z)= sg(E(0,z) \dot{-} 2).\overline{sg}(E(E(0,z) \dot{-} 1,z))$

donde son funciones primitivas recursivas las siguientes:

$$sg(x) = \begin{cases} 1 & x > 0 \\ 0 & x = 0 \end{cases}$$

$$\overline{sg}(x) = \begin{cases} 0 & x > 0 \\ 1 & x = 0 \end{cases}$$

$$x \dot{-} y = \begin{cases} x-y & x \geq y \\ 0 & x < y \end{cases}$$

$E(n,z)$= el exponente del $\underline{n}$-ésimo primo en la descomposición en primos de $\underline{z}$.

Ej: $E(0,40) = 3$ ya que $40 = 2^3.3^0.5^1$

$Q_2(z)= 1$ sii el último elemento de la tupla asociada a z es igual a cero,

luego

$Q_2(z)= 1$ sii $E(0,z) > 1 \wedge E(E(0,z)\dot{-}1,z)\neq 0 \wedge E(E(0,z),z)=0$

y de la misma manera

$Q_3(z)= 1$ sii $E(0,z) > 1 \wedge E(E(0,z)\dot{-}1,z)\neq 0 \wedge E(E(0,z),z)\neq 0$

Finalmente,

Q_i es una función primitiva recursiva $i=1,2,3$.

Sea $h_i(z)$= número de Gödel de la tupla que resulta cuando la regla i se aplica a la tupla representada por z (si z no corresponde a una tupla a la cual se puede aplicar la regla i el valor de h_i no tiene importancia).

Veamos h_1

Supongamos z tiene asociada una tupla a la cual se le puede aplicar la regla 1.

$z = 2^k.3^{w1}.5^{w2}\ldots.\ p_{k-1}{}^0.p_k{}^{wk}$

luego

$h_1(z)= 2^{k-1}.3^{w1}\ldots.\ p_{k-1}{}^{wk+1}$

luego

$$h_1(z)= 2^{E(0,z)\dot{-}1}.\prod_{i=1}^{E(0,z)\dot{-}2} pn(i)^{E(i,z)}.pn(E(0,z)\dot{-}1)^{E(E(0,z),z)+1}$$

donde $p_n(i)$ es el i-ésimo primo.

Luego h_1 es una función primitiva recursiva

de la misma forma se ve que h_2 y h_3 son FPR.

Con Q_i y h_i se puede definir ψ

$\psi(x,y,0)= 2^2.3^x.5^y$

$$\psi(x,y,n^+)= \begin{cases} h_1(\psi(x,y,n)) & \text{si } Q_1(\psi(x,y,n))=1 \\ h_2(\psi(x,y,n)) & \text{si } Q_2(\psi(x,y,n))=1 \\ h_3(\psi(x,y,n)) & \text{si } Q_3(\psi(x,y,n))=1 \\ \psi(x,y,n) & \text{en otro caso.} \end{cases}$$

$\Rightarrow$ ψ es una función primitiva recursiva.

Sea η: $N^2 \rightarrow N$

$\eta(x,y)$= nº de pasos para evaluar A(x,y)

$\eta(x,y)= \mu_z\ [E(0,\psi(x,y,z)) = 1]$

η es una función RECURSIVA

Sea

$A(x,y)= E(1,\psi(x,y,\eta(x,y)))$

A es RECURSIVA.

Ejercicio

Ver

1. $\eta(x^+,y) > y$
2. $\eta(x,y) > x$
3. $\eta(x^+,y^+) > A(x,y)$
4. η NO es una FRP.

La función de codificación β

$\beta(x_1,x_2,x_3)= rm(1+(x_3+1).x_2,x_1)$

β es una función primitiva recursiva y representable por Bt.

Lema

Para cada secuencia finita de números naturales $k_0,k_1,\ldots,k_n$ existen números naturales b y c tales que

$\beta(b,c,i)= k_i \quad 0 \leq i \leq n$

Dem:

Sea $j = máx(n,k_0,k_1,\ldots,k_n)$

Sea $c = j!$

Sea $u_i = 1 + (i+1).c \quad 0 \leq i \leq n$

Los u_i son COPRIMOS (ejercicio)

Además

$k_i \leq j \leq j! = c < 1 + (i+1).c = u_i$

con lo cual

$k_i < u_i$

luego por el teorema Chino del resto existe un número b

$b < u_0.u_1.\ldots.u_n$

tal que $rm(u_i,b) = k_i$

pero $\beta(b,c,i)= rm(1 + (1+i).c, b) = rm(u_i,b) = k_i$

Conclusión

Las secuencias finitas de números naturales se pueden codificar con un par de números b y c y funciones P.R.

Teorema de la representabilidad

Cada función recursiva es representable en PA.

Dem:

Inducción sobre las reglas de derivación.

base

+ $z: N \rightarrow N$

  $z(n) = 0$

  z es representable en PA por la fbf $x_1 = x_1 \wedge y = 0$

+ $s: N \rightarrow N$

  $s(n) = n+1$

  s es representable en PA por la fbf $y = s(x_1)$

+ $U_n^j: N^n \rightarrow N$

  $U_n^j(x_1,\ldots,x_n) = x_j$

  U_n^j es representable en PA por la fbf

  $x_1 = x_1 \wedge x_2 = x_2 \wedge \ldots \wedge x_n = x_n \wedge y = x_j$

Inducción

Composición.

g: $N^m \to N$ es representable por $C(x_1,\ldots,x_m,z)$

h_i: $N^n \to N$ es representable por $B_i(x_1,\ldots,x_n,y)$

Sea f: $N^n \to N$

$$f(x_1,\ldots,x_n) = g(h_1(x_1,\ldots,x_n),h_2(x_1,\ldots,x_n),\ldots,h_m(x_1,\ldots,x_n))$$

f es representable por la fbf

$$\exists y_1 \; \exists y_2 \; \ldots \; \exists y_m \; (B_1(x_1,\ldots,x_n,y_1) \wedge B_2(x_1,\ldots,x_n,y_2) \wedge \ldots \wedge B_m(x_1,\ldots,x_n,y_m) \wedge C(y_1,\ldots,y_m,z))$$

Recursión.

g: $N^n \to N$ es representable por $B(x_1,\ldots,x_{n+1})$

h: $N^{n+2} \to N$ es representable por $C(x_1,\ldots,x_{n+3})$

Sea f: $N^{n+1} \to N$ def. por recursión

$$f(x_1,\ldots,x_n,0) = g(x_1,\ldots,x_n)$$

$$f(x_1,\ldots,x_n,y+1) = h(x_1,\ldots,x_n,y,f(x_1,\ldots,x_n,y))$$

f es representable en S por $D(x_1,\ldots,x_{n+2})$

$$\exists u \; \exists v \; [(\exists w \; Bt(u,v,0,w) \wedge B(x_1,\ldots,x_n,w)) \wedge Bt(u,v,x_{n+1},x_{n+2}) \wedge \forall w \; (w < x_{n+1} \Rightarrow \exists y \; \exists z \; Bt(u,v,w,y) \wedge Bt(u,v,s(w),z) \wedge \wedge \; C(x_1,\ldots,x_n,w,y,z))]$$

donde β es una función de codificación de tuplas

$\beta(x_1,x_2,x_3)= rm(1 + (x_3 + 1).x_2, \; x_1)$ [10]

es una función primitiva recursiva representada por la fbf

$Bt(x_1,x_2,x_3,y)$

$$\exists w \; (x_1 = (1 + (x_3 + 1).x_2).w + y \wedge y < (1 + (x_3 + 1).x_2))$$

Minimización.

Sea g: $N^{n+1} \to N$ con una raíz representable por $E(x_1,\ldots,x_{n+2})$

y sea f: $N^n \to N$

$f(x_1,\ldots,x_n)= \mu_y \; (g(x_1,\ldots,x_n,y)= 0)$

entonces f es representable por la fbf $F(x_1,\ldots,x_{n+1})$

$$E(x_1,\ldots,x_{n+1},0) \wedge \forall y \; (y < x_{n+1} \Rightarrow \neg E(x_1,\ldots,x_n,y,0))$$

---

[10] rm(x,y): resto de la división de y por x

La representabilidad de la composición.

$f(x_1,\dots,x_n) = g(h_1(x_1,\dots,x_n),h_2(x_1,\dots,x_n),\dots,h_m(x_1,\dots,x_n))$

g representada por $C(x_1,\dots,x_m,z)$

h_i representada por $B_i(x_1,\dots,x_n,y_i)$

luego f estará representada por $D(x_1,\dots,x_n,z)$:

$\exists y_1\dots\exists y_m\ (B_1(x_1,\dots,x_n,y_1)\wedge \dots \wedge B_m(x_1,\dots,x_n,y_m)\wedge C(y_1,\dots,y_m,z))$

Cond 1

$f(k_1,\dots,k_n)= p$

Sea $h_j(k_1,\dots,k_n)= r_j$ luego $\vdash B_j(\overline{k}_1,\dots,\overline{k}_n,\overline{r}_j)$

Sea $g(r_1,\dots,r_m)= p$ luego $\vdash C(\overline{r}_1,\dots,\overline{r}_m,\overline{p})$

haciendo la conjunción

$\vdash B_1(\overline{k}_1,\dots,\overline{k}_n,\overline{r}_1)\wedge\dots\wedge B_m(\overline{k}_1,\dots,\overline{k}_n,\overline{r}_m)\wedge C(\overline{r}_1,\dots,\overline{r}_m,\overline{p})$

luego por regla E4 que permite cambiar términos cerrados por existenciales,

$\vdash \exists y_1\dots\exists y_m\ (B_1(\overline{k}_1,\dots,\overline{k}_n,y_1) \wedge \dots \wedge B_m(\overline{k}_1,\dots,\overline{k}_n,y_m) \wedge$
$\wedge\ C(y_1,\dots,y_m,\overline{p})$

que es lo que se quería probar.

Cond 2

$\vdash \exists! z\ D(\overline{k}_1,\dots,\overline{k}_n,z)$ o sea

$\vdash \exists z\ D(\overline{k}_1,\dots,\overline{k}_n,z) \wedge$
$\wedge\ (\forall u\ \forall v\ D(\overline{k}_1,\dots,\overline{k}_n,u) \wedge D(\overline{k}_1,\dots,\overline{k}_n,v) \Rightarrow u = v)$

La primera parte sale tomando $z = \overline{p}$.

Basta ver la segunda

$D(\overline{k}_1,\dots,\overline{k}_n,u)$ y $D(\overline{k}_1,\dots,\overline{k}_n,v)$ como premisa y se aplica el metateorema de la deducción.

$\vdash D(\overline{k}_1,\dots,\overline{k}_n,u)$

$\vdash \exists y_1\dots\exists y_m\ (B_1(\overline{k}_1,\dots,\overline{k}_n,y_1) \wedge \dots \wedge B_m(\overline{k}_1,\dots,\overline{k}_n,y_m) \wedge$
$\wedge\ C(y_1,\dots,y_m,u))$

$\vdash B_1(\overline{k}_1,\dots,\overline{k}_n,b_1)\wedge \dots \wedge B_m(\overline{k}_1,\dots,\overline{k}_n,b_m)\wedge C(b_1,\dots,b_m,u)$

$\vdash D(\overline{k}_1,\dots,\overline{k}_n,v)$

$\vdash \exists y_1 \ldots \exists y_m\ (B_1(\overline{k}_1, \ldots, \overline{k}_n, y_1) \wedge \ldots \wedge B_m(\overline{k}_1, \ldots, \overline{k}_n, y_m) \wedge$

$\wedge\ C(y_1, \ldots, y_m, v))$

$\vdash B_1(\overline{k}_1, \ldots, \overline{k}_n, c_1) \wedge \ldots \wedge B_m(\overline{k}_1, \ldots, \overline{k}_n, c_m) \wedge C(c_1, \ldots, c_m, v)^{(*)}$

por la unicidad de B_i

$c_i = b_i \quad 1 \leq i \leq m$

y reemplazando en $^{(*)}$

$C(b_1, \ldots, b_m, v)$

luego por unicidad de C

$u = v$.

<u>La representabilidad de las funciones obtenidas por recursión</u>.

$g: N^n \to N$ es representable por $B(x_1, \ldots, x_{n+1})$

$h: N^{n+2} \to N$ es representable por $C(x_1, \ldots, x_{n+3})$

y sea $f: N^{n+1} \to N$

$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$

$f(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))$

entonces f es representable

Dem:

$f(x_1, \ldots, x_n, y) = z$ si y solo si existe una secuencia finita de números $b_0, b_1, \ldots, b_y$ tales que

$b_0 = g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, 0)$

$b_1 = h(x_1, \ldots, x_n, 0, b_0) = f(x_1, \ldots, x_n, 1)$

…

$b_{w+1} = h(x_1, \ldots, x_n, w, b_w) = f(x_1, \ldots, x_n, w+1)$

con $w + 1 \leq y$, y $b_y = z$.

La idea es usar la función β para representar la secuencia de evaluaciones.

Con lo cual f será representable por la fbf

$D(x_1, \ldots, x_{n+2})$:

$\exists u\ \exists v\ [(\exists w\ Bt(u, v, 0, w) \wedge B(x_1, \ldots, x_n, w)) \wedge$

$\wedge$ $Bt(u,v,x_{n+1},x_{n+2})$ $\wedge$

$\forall w\ (w < x_{n+1} \Rightarrow \exists y\ \exists z\ Bt(u,v,w,y) \wedge Bt(u,v,s(w),z) \wedge$

$\wedge\ C(x_1,\ldots,x_n,w,y,z))]$

Se arma la siguiente secuencia

$$S = <\overset{\substack{0\\ \downarrow}}{f(x_1,\ldots,x_n,0)},\ldots,\overset{\substack{w\\ \downarrow}}{f(x_1,\ldots,x_n,w)},\ldots,\overset{\substack{y\\ \downarrow}}{f(x_1,\ldots,x_n,y)}>$$

y la fbf D se lee

$$D(\overbrace{x_1,\ldots,x_n}^{\text{parámetros}},\underset{\substack{\uparrow\\ \text{variable de iteración}}}{x_{n+1}},\overset{\substack{\text{resultado}\\ \downarrow}}{x_{n+2}})$$

- $\boxed{\text{Interpretación de u y v.}}$

existen u y v que codifican la secuencia S de manera tal que $Bt(u,v,i,w)$ vale si el i-ésimo elemento de S es w.

- $\boxed{\text{Base.}}$

el elemento 0 de S es w y $B(x_1,\ldots,x_n,w)$ o sea $g(x_1,\ldots,x_n)= w$ o sea $f(x_1,\ldots,x_n,0)= g(x_1,\ldots,x_n)$

- $\boxed{\text{Relación entre D y la secuencia.}}$

el elemento x_{n+1} de la secuencia es x_{n+2} donde x_{n+1} y x_{n+2} son las dos últimas variables libres de D.

Sup $D(x_1,\ldots,x_n,x_{n+1},x_{n+2})$ luego $f(x_1,\ldots,x_n,x_{n+1})= x_{n+2}$ y $f(x_1,\ldots,x_n,x_{n+1})$ es un término de la secuencia, el término x_{n+1}.

- $\boxed{\text{Paso inductivo.}}$

Para todo w anterior al elemento a calcular existen s y t tal que el elemento w-ésimo de la secuencia es s y el w+1-ésimo es t y $C(x_1,\ldots,x_n,w,s,t)$ o sea

$s = f(x_1,\ldots,x_n,w)$, $t = f(x_1,\ldots,x_n,w+1)$ y $t = h(x_1,\ldots,x_n,w,s)$

$\Rightarrow f(x_1,\ldots,x_n,w+1)= h(x_1,\ldots,x_n,w,\ f(x_1,\ldots,x_n,w))$

Demostración de la representabilidad.

Primera condición:

$$\vdash$$

$f(k_1,\ldots,k_n,p)= m$ ent $D(\overline{k}_1,\ldots,\overline{k}_n,\overline{p},\overline{m})$

2 casos: $p = 0$ y $p > 0$

Primer caso: $p = 0$

$f(k_1,\ldots,k_n,0)= m$ sii $g(k_1,\ldots,k_n)= m$

Si se considera la secuencia de un solo elemento m, es decir $< m >$ se tiene que existen b y c tal que

$\beta(b,c,0)= m$

luego como β es representable por Bt

1. $\vdash Bt(\overline{b},\overline{c},0,\overline{m})$

Como g es representable por B

2. $\vdash B(\overline{k}_1,\ldots,\overline{k}_n,\overline{m})$

De 1 y 2 aplicando la regla que dice que de la validez para un término se deriva la condición existencial (E4) se tiene

3. $\vdash \exists w\ (Bt(\overline{b},\overline{c},0,w) \wedge B(\overline{k}_1,\ldots,\overline{k}_n,w))$

Como es teorema

4. $\vdash \neg\ (w < 0)$

Aplicando (muchas cosas) se tiene

5. $\vdash \forall w\ (w < 0 \Rightarrow \exists y\exists z\ Bt(\overline{b},\overline{c},w,y) \wedge Bt(\overline{b},\overline{c},s(w),z)$
$\wedge\ C(\overline{k}_1,\ldots,\overline{k}_n,w,y,z))$

de 1, 3 y 5 aplicando E4 se obtiene

$\vdash D(\overline{k}_1,\ldots,\overline{k}_n,\overline{p},\overline{m})$

Segundo caso: $p > 0$

$f(k_1,\ldots,k_n,p)$ es calculado con las ecuaciones de recursión en p+1 pasos.

Sea $r_i = f(k_1,\ldots,k_n,i)$ y sea $< r_0,r_1,\ldots,r_p >$ la secuencia de valores calculados por recursión.

Existen b y c tal que

$\beta(b,c,i)= r_i \qquad 0 \leq i \leq p$

luego

1. $\vdash Bt(\overline{b},\overline{c},\overline{i},\overline{r}_i)$

Volvemos a separar en casos, primer elemento de la secuencia

$\beta(b,c,0)= r_0 = f(k_1,\ldots,k_n,0)= g(k_1,\ldots,k_n)$

luego

2. $\vdash \mathrm{Bt}(\overline{b},\overline{c},0,\overline{r}_0) \wedge \mathrm{B}(\overline{k}_1,\ldots,\overline{k}_n,\overline{r}_0)$

y aplicando E4

3. $\vdash \exists w\ (\mathrm{Bt}(\overline{b},\overline{c},0,w) \wedge \mathrm{B}(\overline{k}_1,\ldots,\overline{k}_n,w))$

Para el último elemento de la secuencia

$r_p = f(k_1,\ldots,k_n,p)= m$

luego $\beta(b,c,p)= m$ con lo cual

4. $\vdash \mathrm{Bt}(\overline{b},\overline{c},\overline{p},\overline{m})$

Para los valores intermedios de la secuencia

$0 < i \leq p - 1$

$\beta(b,c,i)= r_i = f(k_1,\ldots,k_n,i)$

$\beta(b,c,i+1)= r_{i+1} = f(k_1,\ldots,k_n,i+1)= h(k_1,\ldots,k_n,i,r_i)$

luego se puede deducir

5. $\vdash \mathrm{Bt}(\overline{b},\overline{c},\overline{i},\overline{r}_i) \wedge \mathrm{Bt}(\overline{b},\overline{c},\overline{s(i)},\overline{r}_{i+1}) \wedge \mathrm{C}(\overline{k}_1,\ldots,\overline{k}_n,\overline{i},\overline{r}_i,\overline{r}_{i+1})$

Luego por E4

6. $\vdash \exists y\ \exists z\ (\mathrm{Bt}(\overline{b},\overline{c},\overline{i},y) \wedge \mathrm{Bt}(\overline{b},\overline{c},\overline{s(i)},z) \wedge \mathrm{C}(\overline{k}_1,\ldots,\overline{k}_n,\overline{i},y,z))$

Luego para cada i se puede deducir un teorema como éste y hay una propiedad que dice:

$\vdash \mathrm{A}(\overline{0}) \wedge \mathrm{A}(\overline{1}) \wedge \ldots \wedge \mathrm{A}(\overline{k}) \Leftrightarrow \forall x\ (x \leq \overline{k} \Rightarrow \mathrm{A}(x))$

Aplicando a 6

7. $\vdash \forall w\ (w < \overline{p} \Rightarrow \exists y \exists z\ \mathrm{Bt}(\overline{b},\overline{c},w,y) \wedge \mathrm{Bt}(\overline{b},\overline{c},s(w),z) \wedge \mathrm{C}(\overline{k}_1,\ldots,\overline{k}_n,w,y,z))$

Finalmente juntando la última fórmula de cada caso se obtiene

$\vdash \mathrm{D}(\overline{k}_1,\ldots,\overline{k}_n,\overline{p},\overline{m})$

La aritmetización de los formalismos

Aritmetización

Sea K una teoría de primer orden. Se asigna a cada símbolo u de K un número impar g(u) de la siguiente manera:

$g(()= 3$

$g())= 5$

$g(,)= 7$

$g(\neg)= 9$

$g(\Rightarrow)= 11$

$g(\forall)= 13$

$g(x_k)= 13 + 8k$

$g(a_k)= 7 + 8k$

$g(f^n_k)= 1 + 8(2^n.3^k)$

$g(A^n_k)= 3 + 8(2^n.3^k)$

Para asignar números a las secuencias de símbolos (expresiones) se utiliza la función de codificación de Gödel.

$g(u_0u_1\ldots u_r)= 2^{g(u0)}3^{g(u1)}\ldots p_r^{g(ur)}$

Las expresiones tienen números pares. De la misma forma se asignan números a las secuencias de expresiones que se distinguen por ser par el exponente de 2.

Alfabetos primitivos recursivos

Una teoría K tiene un alfabeto primitivo recursivo (recursivo) si las siguientes propiedades son primitivas recursivas (recursivas).

a. IC(x): x es el número de Gödel de una constante individual de K.
b. IV(x): x es el número de Gödel de una variable individual de K.
c. FL(x): x es el número de Gödel de un símbolo de función de K.
d. PC(x): x es el número de Gödel de un símbolo de predicado de K.

Teorema

Si K es una teoría con alfabeto primitivo recursivo (recursivo) las siguientes funciones y relaciones son primitivas recursivas (recursivas).

1. EVbl(x): x es el número de Gödel de una expresión que es una variable.

   EIC(x): x es el número de Gödel de una expresión que es una constante.

   EFL(x): x es el número de Gödel de una expresión que es un símbolo de función.

   EPL(x): x es el número de Gödel de una expresión que es un símbolo de predicado.
2. ArgF(x) = n si x es el número de Gödel de una expresión que es un símbolo funcional de aridad n.

   ArgP(x) = n si x es el número de Gödel de una expresión que es un símbolo de predicado de aridad n.
3. Gd(x): x es el número de Gödel de una expresión (secuencia de símbolos).
4. MP(x,y,z): z es el número de Gödel de una expresión que resulta de la aplicación de modus ponens a expresiones de números de Gödel x e y.
5. Gen(x,y): y es el número de Gödel de una expresión que resulta de la aplicación de generalización a una expresión de número de Gödel x.
6. Trm(x): x es el número de Gödel de un término.
7. Atfml(x): x es el número de Gödel de una fbf atómica.
8. Fml(x): x es el número de Gödel de una fbf.
9. Subst(x,y,u,v): x es el número de Gödel de una expresión que resulta de reemplazar en la expresión de número de Gödel y las ocurrencias de la variable libre de número v por el termino de número u.
10. Sub(y,u,v) = n si Subst(n,y,u,v)
11. Fr(y,v): y es el número de Gödel de una fbf o un término que contiene apariciones libres de la variable de número v.

12. $Ff(u,v,w)$: u es el número de Gödel de un término que esta libre para la variable con número v en la fbf con número w.
13. $LAx(x)$: x es el número de Gödel de un axioma lógico.
14. $Neg(x)= n$ si n es el número de Gödel de $\neg A$ siendo x el número de A.
15. $Cond(x,y)= n$ si n es el número de Gödel de $(A \supset B)$ siendo x el número de A e y el número de B.
16. $Clos(x)= n$ si n es el número de Gödel de la clausura de una fbf de número x.
17. $Num(y)= n$ si n es el número de Gödel del numeral $s(s(s(\ldots 0 \ldots)))$ (n veces)
18. $Nu(x)$: x es el número de Gödel de un numeral.
19. $D(u)= n$ si n es el número de Gödel de $B(s(s(s(\ldots 0 \ldots))))$ (u veces) y u es el número de Gödel $B(x_1)$.
20. $Ax(y)$: y es el número de Gödel de un axioma.
21. $Prf(y)$: y es el número de Gödel de una demostración.
22. $Pf(y,x)$: y es el número de Gödel de una demostración de la fbf de número x.

La representabilidad y la recursión en teorías recursivas

Teorema

Sea K una teoría de primer orden con igualdad cuyo lenguaje contiene la constante 0 y el símbolo de función S y tal que K tiene un lenguaje y un sistema de axiomas primitivo recursivo (recursivo).

Si para cada $r,s \in N$

si $\vdash_K \overline{r} = \overline{s}$ entonces $r = s$

entonces toda función representable en K es recursiva.

Dem:

Sea $f: N^n \rightarrow N$ representable en K por la fbf $B(x_1,\ldots,x_{n+1})$

Sea $P_B(u_1,\ldots,u_n,u_{n+1},y)$ una relación $P_B \subseteq N^{n+2}$ tal que

$P_B(u_1,\ldots,u_n,u_{n+1},y)$: y es el número de Gödel de una prueba en K de $B(\bar{u}_1,\ldots,\bar{u}_{n+1})$

<u>1º</u> P_B es primitiva recursiva

Se puede ver que obteniendo el número de Gödel de B al que llamaremos m, se puede obtener el número de Gödel de $B(\bar{u}_1,\ldots,\bar{u}_{n+1})$ al que llamaremos b y

$$P_B(u_1,\ldots,u_n,u_{n+1},y) \Leftrightarrow Pf(y,b)$$

<u>2º</u> $P_B(u_1,\ldots,u_{n+1},y)$ entonces $f(u_1,\ldots,u_n)= u_{n+1}$

Supongamos que vale $P_B(u_1,\ldots,u_{n+1},y)$

y que $f(u_1,\ldots,u_n)= r$ y veamos que $u_{n+1} = r$

Como B representa a f en K y $f(u_1,\ldots,u_n)= r$ por hipótesis entonces

1. $\vdash_K B(\bar{u}_1,\ldots,\bar{u}_n,\bar{r})$ y
2. $\vdash_K \exists! y\, B(\bar{u}_1,\ldots,\bar{u}_n,y)$

Además por hipótesis

$$P_B(u_1,\ldots,u_{n+1},y)$$

luego por def. de P_B

3. $\vdash_K B(\bar{u}_1,\ldots,\bar{u}_n,\bar{u}_{n+1})$

De 1, 2 y 3 se tiene

4. $\vdash_K \bar{r} = \bar{u}_{n+1}$

y por hipótesis $\vdash_K \bar{r} = \bar{s}$ ent $r = s$

finalmente $r = u_{n+1}$

<u>3º</u> Como se evalúa f

Sean $k_1,\ldots,k_n \in N$ tal que $f(k_1,\ldots,k_n)= r$

luego $\vdash_K B(\bar{k}_1,\ldots,\bar{k}_n,\bar{r})$

Sea j el número de Gödel de una prueba en K de $B(\bar{k}_1,\ldots,\bar{k}_n,\bar{r})$ luego $P_B(k_1,\ldots,k_n,r,j)$.

Luego para cada $x_1,\ldots,x_n$ hay algún y que codifica al par ordenado (r,j) tal que

$P_B(x_1,\ldots,x_n,\sigma_1(y),\sigma_2(y))$ luego

$\mu_y\, P_B(x_1,\ldots,x_n,\sigma_1(y),\sigma_2(y))$ es recursiva y

$f(x_1,\ldots,x_n)= \sigma_1(\mu_y\, P_B(x_1,\ldots,x_n,\sigma_1(y),\sigma_2(y)))$

Expresabilidad de relaciones

Sea K una teoría de primer orden con el lenguaje de PA.

Sea $R \subseteq N^n$. R es **expresable** en K si existe una fbf $B(x_1,\dots,x_n)$ tal que

1. Si $k_1,\dots,k_n \in R$ ent $\vdash_K B(\overline{k}_1,\dots,\overline{k}_n)$
2. Si $k_1,\dots,k_n \notin R$ ent $\vdash_K \neg B(\overline{k}_1,\dots,\overline{k}_n)$

Teorema: Expresibilidad y Representabilidad

Sea K una teoría de primer orden con el lenguaje de PA tal que $\vdash_K 0 \neq 1$

$R \subseteq N^n$ es expresable en K si y solo si C_R es representable en K.

Dem:

$\Rightarrow$) R es expresable en K por $B(x_1,\dots,x_n)$

es fácil ver que C_R es representable por la fbf

$$(B(x_1,\dots,x_n) \wedge y = 0) \vee (\neg B(x_1,\dots,x_n) \wedge y = \overline{1})$$

$\Leftarrow$) C_R es representable en K por $C(x_1,\dots,x_n,y)$

es fácil ver (usando $\vdash_K 0 \neq \overline{1}$) que R es representable por

$$C(x_1,\dots,x_n,0)$$

ω-consistencia

Sea T una teoría de primer orden con el lenguaje de PA.

T es ω-consistente si no existe una fbf $A(x_1)$ con x_1 libre tal que $A(\overline{n})$ es teorema de T para todo $n \in N$ y $\sim(\forall x_1)\, A(x_1)$ también es teorema de T o sea

$$\vdash_T A(\overline{n}) \text{ y } \vdash_T \sim\forall x_1\, A(x_1)$$

<u>Nota</u>

No es cierto que de

$$\vdash_T A(\overline{n}) \text{ para todo } n \in N$$

pueda deducirse

$$\vdash_T (\forall x_1)\ A(x_1)$$

Teorema

Sea T una teoría de primer orden con el lenguaje de PA tal que T es ω-consistente entonces T es consistente.

Dem:

Sea $A(x_1)$ una fbf que es teorema para todos los numerales por ejemplo $A(x_1)$: $x_1 = x_1$

Luego como T es ω-consistente $\sim(\forall x_1)\ A(x_1)$ no es teorema luego T es consistente.

La fórmula U

Sea $W \leq N \times N$

$W(m,n)$: m es el número de Gödel de una fbf $A(x_1)$ con x_1 libre y n es el número de Gödel de una demostración de $A(\overline{m})$.

Como W es representable en PA por la fbf W.

Si $W(m,n)$ entonces $\vdash_{PA}\ W\ (\overline{m},\overline{n})$

Si no $W(m,n)$ entonces $\vdash_{PA}\ \sim W\ (\overline{m},\overline{n})$

Sea la fbf $F(x_1)$: $\forall x_2 \sim W\ (x_1,x_2)$

y sea p el número de Gödel de dicha fbf.

Finalmente sea U la siguiente fbf.

U: $(\forall x_2) \sim W\ (\overline{p},x_2)$ luego U es $F(\overline{p})$

Qué dice U en la interpretación usual?

para cada $n \in N$ no se verifica $W(p,n)$

o sea

para cada $n \in N$ no es cierto que p es el número de Gödel de una fbf $A(x_1)$ con x_1 libre y n el número de Gödel de una demostración en PA de $A(\overline{p})$.

pero la fbf con número de Gödel p es F

o sea

para cada n $\in$ N no es cierto que n es el número de Gödel de una demostración en PA de F($\bar{p}$)

o sea

para cada n $\in$ N no es cierto que n es el número de Gödel de una demostración en PA de U.

<u>Finalmente</u>

U afirma su propia improbabilidad.

Teorema

Si PA es ω-consistente no es completo respecto a la negación.

Dem:

Se verá que tanto U como ~U no son teoremas.

Supongamos que U es teorema $\vdash_{PA} U$.

Sea q el número de Gödel de una prueba en PA de U.

Sea p el número de Gödel de $F(x_1)$: $\forall x_2 \sim(W(x_1,x_2))$.

luego se verifica

$W(p,q)$ con lo cual $\vdash_{PA} W(\bar{p},\bar{q})$ (1)

Como por hipótesis

$\vdash_{PA}$ U entonces $\vdash_{PA} (\forall x_2) \sim W(\bar{p},x_2)$

luego vale (por especialización)

$\vdash_{PA} \sim W(\bar{p},\bar{q})$ (2)

Pero (1) + (2) contradicen la consistencia de PA luego no es cierto $\vdash_{PA}$ U.

Como U no es teorema de PA no existe q $\in$ N que sea el número de Gödel de una prueba en PA de U

o sea no existe q $\in$ N tal que sea el número de Gödel de una prueba de PA de $(x_2)\sim W(\overline{p},x_2)$ luego (!) no vale W(p,q) para ningún q $\in$ N.

Luego por representabilidad

$\vdash_{PA}$ $\sim W(\overline{p},\overline{q})$ para todo q $\in$ N

y por ω-consistencia

$\sim(\forall x_2)\sim W(\overline{p},x_2)$

no es teorema de PA

con lo cual

~U no es teorema de PA.

Finalmente ni U ni ~U son teoremas de PA con lo cual PA no es completo con respecto a la negación.

Las hipótesis del teorema de Gödel

Sea K una teoría de primer orden con el lenguaje de PA tal que

1. K tiene un conjunto recursivo de axiomas.
2. $\vdash_{K}$ $0 \neq \overline{1}$
3. Cada función recursiva es representable en PA.

entonces

a. Si K es consistente U no es teorema.

b. Si K es ω-consistente ~U no es teorema.

Nota

Con 1 se obtiene la recursividad de U.

Con 2 y 3 se obtiene que las relaciones recursivas son expresables con lo cual U es expresable.

Otra demostración del teorema de Gödel

El punto fijo

La función diagonal

$D(u)$= el número de Gödel de $B(\overline{u})$ donde u es el número de Gödel de $B(x_1)$.

Notación

Se denota el número de Gödel de una expresión C por $\ulcorner C \urcorner$

Lema de la diagonalización

Sea K una teoría de primer orden con el lenguaje de PA en la que la función diagonal es representable.

Entonces para cada fbf $E(x_1)$ con x_1 libre existe una fbf C tal que

$$\vdash_K C \Leftrightarrow E(\ulcorner C \urcorner)$$

Dem:

Sea $D(x_1,x_2)$ la fbf que representa a la función diagonal en K.

Sea $F(x_1)$: $(\forall x_2)(D(x_1,x_2)\Rightarrow E(x_2))$

Sea m el número de Gödel de $F(x_1)$

Sea C: $F(\overline{m})$

o sea C: $(\forall x_2)(D(\overline{m},x_2)\Rightarrow E(x_2))$

Sea q el número de Gödel de C $\{q = \ulcorner C \urcorner\}$

Cuánto vale $D(m)$?

$D(m)$: el número de Gödel de $F(\overline{m})$

el número de Gödel de C

$\ulcorner C \urcorner$

Hay que probar $\vdash_K C \Leftrightarrow E(\ulcorner C \urcorner)$

$\Rightarrow$) en realidad $C \vdash_K E(\ulcorner C \urcorner)$

1. C hipótesis

2. $(\forall x_2)(D(\overline{m},x_2) \Rightarrow E(x_2))$ reescritura de 1

3. $D(\overline{m},\overline{q}) \Rightarrow E(\overline{q})$ A4 a 2

4. $D(\overline{m},\overline{q})$ D representa a la diagonal y $D(m)= q$

5. $E(\overline{q})$ MP 3 y 4

6. $\vdash_K C \Rightarrow E(\overline{q})$ metateorema de la deducción

7. $\vdash_K C \Rightarrow E(\ulcorner C \urcorner)$

$\Leftarrow$) en realidad $E(\ulcorner C \urcorner), D(\overline{m},x_2) \vdash_K C$

1. $E(\overline{q})$ hipótesis

2. $D(\overline{m},x_2)$ hipótesis

3. $\exists! x_2\ D(\overline{m},x_2)$ D representa a D

4. $D(\overline{m},\overline{q})$ $D(m)= q$

5. $x_2 = \overline{q}$ 2, 3 y 4

6. $E(x_2)$ sustitución en 1

7. $E(\overline{q}) \vdash_K D(\overline{m},x_2) \Rightarrow E(x_2)$ metateorema de la deducción

8. $E(\overline{q}) \vdash_K \forall x_2(D(\overline{m},x_2) \Rightarrow E(x_2))$ generalización

9. $\vdash_K E(\overline{q}) \Rightarrow \forall x_2(D(\overline{m},x_2) \Rightarrow E(x_2))$ m. de la deducción

10. $\vdash_K E(\overline{q}) \Rightarrow C$

Teorema del punto fijo

Sea K una teoría de primer orden con el lenguaje de PA tal que todas las funciones recursivas son representables. Entonces para cada fbf $E(x_1)$ existe una fbf cerrada C tal que

$$\vdash_K C \Leftrightarrow E(\ulcorner C \urcorner)$$

Dem:

Como D es recursiva, es representable y se aplica el lema anterior.

El teorema de incompletitud (segunda versión)

Sea K una teoría de primer orden con el lenguaje de PA tal que

1. K tiene un conjunto recursivo de axiomas.
2. $\vdash_K 0 \neq \overline{1}$
3. Cada función recursiva es representable en K.

entonces

a. si K es consistente no es el caso que $\vdash_K G$

b. si K es ω-consistente no es el caso que $\vdash_K \sim G$

Dem:

Sea Pf(x,y): y es el número de Gödel de una prueba en K de la fbf de número de Gödel x.

Sea Pf la fbf que representa a Pf.

Sea $E(x_1)$: $\forall x_2\ \neg Pf(x_1,x_2)$

Luego por el teorema del punto fijo debe existir G cerrada tal que

$$(G)\ \vdash_K G \Leftrightarrow \forall x_2\ \neg Pf(x_2,\ulcorner G \urcorner)$$

que se puede interpretar de la siguiente manera.

$\forall x_2\ \neg Pf(x_2,\ulcorner G \urcorner)$: no hay una demostración en K de G.

Luego:

Sea $q = \ulcorner G \urcorner$

a. Supongamos que $\vdash_K G$

Sea r el número de Gödel de una prueba en K de G.

Luego Pf(r,q) luego por representatividad

$\vdash_K Pf(\overline{r},\overline{q})$ y por (G) $\vdash_K \forall x_2\ \neg Pf(x_2,\ulcorner G \urcorner)$ y por especialización $\vdash_K \neg Pf(\overline{r},\ulcorner G \urcorner)$

con lo cual K sería inconsistente.

b. Supongamos que K es ω-consistente y que $\vdash_K \neg G$.

Luego por el contrarrecíproco de G

$$\vdash_K \neg\forall x_2\ \neg Pf(x_2,\ulcorner G \urcorner) \text{ o sea } \vdash_K \exists x_2\ Pf(x_2,\ulcorner G \urcorner)\ (1)$$

Además con k es ω-consistente, es consistente o sea no es el caso de $\vdash_K G$ luego Pf(n,q) es falso para todo natural n, con lo cual por representabilidad

$\vdash_K \neg Pf(\overline{n}, \overline{q})$ para todo natural n y

finalmente por ω-consistencia

no es el caso $\vdash_K \exists x_2\, Pf(x_2, \ulcorner G \urcorner)$ que se contradice con (1).

El teorema de Gödel – Rosser (1936)

Cambia ω-consistencia por consistencia haciendo más compleja la sentencia indecidible.

Sea Neg: $N \rightarrow N$

Neg(x)= nº de Gödel de la fbf ~F siendo x el número de Gödel de la fbf F.

Como Neg es primitiva recursiva, es representable por la fbf $Neg(x_1,x_2)$.

Sea la siguiente fbf

$E(x_1):\forall x_2(Pf(x_2,x_1)\Rightarrow \forall x_3(Neg(x_1,x_3)\Rightarrow\exists x_4(x_4 \leq x_2 \wedge Pf(x_4,x_3))))$

Cuál es la interpretación usual de E?

La fbf de número de Gödel x_1 cumple que para cualquier demostración de x_1 (de número de Gödel x_2) existe una demostración (de número de Gödel x_4) de número de Gödel menor que demuestra la fbf que es la negación de la fbf de número de Gödel x_1.

Por el teorema del punto fijo existe una fbf cerrada R tal que

$$\vdash_K R \Leftrightarrow E(\ulcorner R \urcorner)$$

Luego R afirma que si se puede demostrar entonces también se puede demostrar su negación, $\neg R$ y con una demostración de número de Gödel menor.

Teorema (de Gödel – Rosser)

Sea K una teoría de primer orden con igualdad con el lenguaje de la aritmética entonces si

1. K tiene un conjunto recursivo de axiomas.
2. $\vdash_K 0 \neq \overline{1}$
3. Cada función recursiva es representable.
4. $\vdash_K x \leq \overline{n} \Rightarrow x=0 \vee x=\overline{1} \vee \ldots \vee x=\overline{n}$ para todo $n\in N$.
5. $\vdash_K x \leq \overline{n} \vee \overline{n} \leq x$ para todo $n\in N$.

Si K es consistente entonces no es completo respecto de la negación.

Dem:

Sea p el número de Gödel de R y j el de $\neg R$

a. Supongamos que $\vdash_K R$

luego por el teorema del punto fijo $\vdash_K R \Leftrightarrow E(\ulcorner R \urcorner)$ con lo cual $\vdash_K E(\ulcorner R \urcorner)$ que es lo mismo que

I. $\vdash_K \forall x_2 \; Pf(x_2,\overline{p}) \Rightarrow \; \forall x_3 \; Neg(\overline{p},x_3) \Rightarrow \; \exists x_4 \; (x_4 \leq x_2 \wedge Pf(x_4,x_3))$

Sea k el número de Gödel de una demostración en K de R, luego Pf(k,p) y $\vdash_K Pf(\overline{k},\overline{p})$

Aplicando especialización a I $(x_2/\overline{k})$

$\vdash_K Pf(\overline{k},\overline{p}) \Rightarrow \forall x_3 \; Neg(\overline{p},x_3) \Rightarrow \exists x_4 \; (x_4 \leq \overline{k} \wedge Pf(x_4,x_3))$

y aplicando modus ponens

% $\vdash_K \forall x_3 \; Neg(\overline{p},x_3) \Rightarrow \exists x_4 \; (x_4 \leq \overline{k} \wedge Pf(x_4,x_3))$

Como j es el número de Gödel de $\neg R$ vale

Neg(p,j) y $\vdash_K Neg(\overline{p},\overline{j})$

Aplicando especialización a % $(x_3/\overline{j})$

$\vdash_K Neg(\overline{p},\overline{j}) \Rightarrow \exists x_4 \; (x_4 \leq \overline{k} \wedge Pf(x_4,\overline{j}))$

luego por modus ponens

$\vdash_K \exists x_4 \; (x_4 \leq \overline{k} \wedge Pf(x_4,\overline{j}))$

que es lo mismo que

$\vdash_K \neg\forall x_4 \; \neg(x_4 \leq \overline{k} \wedge Pf(x_4,\overline{j}))$

Como supusimos $\vdash_K$ R y que K es consistente entonces no es el caso de $\vdash_K \neg R$ luego Pf(n,j) es falso para todo n luego $\vdash_K \neg Pf(\overline{n},\overline{j})$ para todo $n \in N$.

Como K es una teoría con igualdad vale

$* \vdash_K x_4 = \overline{n} \Rightarrow \neg Pf(x_4,\overline{j})$ para todo $n \in N$.

pero por la condición 4

$** \vdash_K x_4 \leq \overline{k} \Rightarrow x_4 = 0 \vee \ldots \vee x_4 = \overline{k}$

de * y ** se tiene

$\vdash_K x_4 \leq \overline{k} \Rightarrow \neg Pf(x_4,\overline{j})$ o sea

$\vdash_K \neg(x_4 \leq \overline{k} \wedge Pf(x_4,\overline{j}))$

y por generalización

$\vdash_K \forall x_4 \neg(x_4 \leq \overline{k} \wedge Pf(x_4,\overline{j}))$

que junto con # contradice la consistencia.

b. Supongamos que $\vdash_K \neg R$ (vamos a llegar a $\vdash_K$ R lo cual contradice la consistencia)

Sea m el número de Gödel de una demostración en K de $\neg R$.

Luego Pf(m,j) y también $\vdash_K Pf(\overline{m},\overline{j})$

Reemplazando $\overline{m}$ por un existencial y usando propiedades del $\leq$

$\vdash_K \overline{m} \leq x_2 \Rightarrow \exists x_4 (x_4 \leq x_2 \wedge Pf(x_4,\overline{j}))$ (α)

Además por consistencia de K no es el caso que $\vdash_K$ R

luego Pf(n,p) es falso para todo $n \in N$ luego

$\vdash_K \neg Pf(\overline{n},\overline{p})$ para todo $n \in N$.

Aplicando la condición 4 de las hipótesis

$\vdash_K x_2 \leq \overline{m} \Rightarrow x_2 = 0 \vee \ldots \vee x_2 = \overline{m}$

luego

$\vdash_K x_2 \leq \overline{m} \Rightarrow \neg Pf(x_2,\overline{p})$ (β)

Ahora se puede hacer un derivación sintáctica

1. $Pf(x_2,\overline{p})$	hip.
2. $Neg(\overline{p},x_3)$	hip.
3. $x_2 \leq \overline{m} \vee \overline{m} \leq x_2$	cond 5.

4. $\overline{m} \leq x_2 \Rightarrow \exists x_4 \ (x_4 \leq x_2 \wedge Pf(x_4, \overline{j}))$ (α)

5. $x_2 \leq \overline{m} \Rightarrow \neg Pf(x_2, \overline{p})$ (β)

6. $\neg Pf(x_2, \overline{p}) \vee \exists x_4 \ (x_4 \leq x_2 \wedge Pf(x_4, \overline{j}))$ 3+4+5+ tautología

7. $\exists x_4 \ (x_4 \leq x_2 \wedge Pf(x_4, \overline{j}))$ 1+6+ reglas de disjuntos

8. $Neg(\overline{p}, \overline{j})$ probado en la parte a. de este teorema

9. $\exists! x_3 \ Neg(\overline{p}, x_3)$ representabilidad de Neg

10. $x_3 = \overline{j}$ 2+8+9

11. $\exists x_4 \ (x_4 \leq x_2 \wedge Pf(x_4, x_3))$ 7+10

12. $Pf(x_2, \overline{p}), Neg(\overline{p}, x_3) \vdash_K \exists x_4(x_4 \leq x_2 \wedge Pf(x_4, x_3))$

13. $Pf(x_2, \overline{p}) \vdash_K Neg(\overline{p}, x_3) \Rightarrow \exists x_4(x_4 \leq x_2 \wedge Pf(x_4, x_3))$
metateorema de la deducción

14. $Pf(x_2, \overline{p}) \vdash_K \forall x_3(Neg(\overline{p}, x_3) \Rightarrow \exists x_4(x_4 \leq x_2 \wedge Pf(x_4, x_3)))$
generalización

15. $\vdash_K Pf(x_2, \overline{p}) \Rightarrow \forall x_3(Neg(\overline{p}, x_3) \Rightarrow \exists x_4(x_4 \leq x_2 \wedge Pf(x_4, x_3)))$
metateorema de la deducción

16. $\vdash_K \forall x_2(Pf(x_2, \overline{p}) \Rightarrow \forall x_3 \ Neg(\overline{p}, x_3) \Rightarrow \exists x_4 \ x_4 \leq x_2 \wedge Pf(x_4, x_3))$
generalización

17. $\vdash_K R$

Luego de suponer $\vdash_K \neg R$ se deduce $\vdash_K R$ absurdo.

El segundo teorema de Gödel

Sea K una teoría de primer orden con igualdad con el lenguaje de PA y un conjunto recursivo de axiomas propios. Sea Con_K la siguiente fbf cerrada:

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4 \sim(Pf(x_1, x_3) \wedge Pf(x_2, x_4) \wedge Neg(x_3, x_4))$$

que en la interpretación usual afirma que no hay en K una fbf tal que son demostrables ella y su negación, o sea que K es consistente.

El segundo teorema de Gödel dice que si K es consistente entonces no es el caso $\vdash_K$ Con_K (1931).

El teorema puede interpretarse diciendo que una eventual prueba de la consistencia de K debe usar ideas que escapan a K. Ideas más complejas.

Pruebas de consistencia de PA han sido dadas por Gentzen (1936) y Schütte (1951) pero ambos emplean nociones de cardinalidad que <u>aparentemente</u> no son formalizables en PA.

La demostración usando el teorema de incompletitud de Gödel.

Sea G la fbf cerrada usada para la demostración del teorema de incompletitud.

Sea G la fbf cerrada.

$$Con_K \Rightarrow G.$$

G es el primer teorema de Gödel y su razonamiento metamatemático puede expresarse en K con lo cual

$$\vdash_K Con_K \Rightarrow G \qquad \{\text{ver Fegerman 1960}\}$$

Si fuera cierto,

$$\vdash_K Con_K$$

Aplicando modus ponens

$$\vdash_K G$$

lo cual es absurdo. Con lo cual no es el caso $\vdash_K Con_K$.

La demostración completa que se verá solo vale en PA !

Las condiciones de derivabilidad de Hilbert – Bernays

Sea $Bew(x_1)$ la fbf de una variable libre

$$\exists x_2 \, (Pf(x_2,x_1))$$

que en la interpretación usual afirma que la fbf de número de Gödel x_1 es demostrable.

En PA se verifican las siguientes condiciones para fbf cerradas C y D.

<u>HB1.</u> si $\vdash_{PA}$ C entonces $\vdash_{PA}$ $Bew(\ulcorner C \urcorner)$

<u>HB2.</u> $\vdash_{PA} Bew(\ulcorner C \Rightarrow D \urcorner) \Rightarrow (Bew(\ulcorner C \urcorner) \Rightarrow Bew(\ulcorner D \urcorner))$

HB3. $\vdash_{PA}$ Bew(⌜C⌝)⇒Bew(⌜Bew(⌜C⌝)⌝)

HB1 y HB2 salen por propiedades de Pf (ejercicio).

HB3 es dificil, usa propiedades de PA.

Se puede leer en Boolos 1993 o Shoenfield 1967.

Teorema de Lob

Sea C una fbf cerrada de PA. Entonces

si $\vdash_{PA}$ Bew(⌜C⌝)⇒ C entonces $\vdash_{PA}$ C.

Dem:

Sea la fbf Bew(x_1)⇒ C, dicha fbf tiene una única variable libre x_1 y se le puede aplicar el teorema del punto fijo. Luego existe una fbf cerrada L tal que

$\vdash_{PA}$ L ⇔ (Bew(⌜L⌝)⇒C)

y de aquí se procede a una derivación.

1. $\vdash_{PA}$ L ⇔ (Bew(⌜L⌝)⇒ C) teorema del punto fijo
2. $\vdash_{PA}$ L ⇒ (Bew(⌜L⌝)⇒ C) si y solo si
3. $\vdash_{PA}$ Bew(⌜L ⇒(Bew(⌜L⌝)⇒ C)⌝) HB1 aplicado a 2.
4. $\vdash_{PA}$ Bew(⌜L ⇒ (Bew(⌜L⌝)⇒ C)⌝)⇒ (Bew(⌜L⌝)⇒ Bew(⌜Bew(⌜L⌝)⇒ C⌝)) HB2

4'. $\vdash_{PA}$ Bew(⌜L⌝)⇒ Bew(⌜Bew(⌜L⌝)⇒ C⌝) MP 3 y 4

5. $\vdash_{PA}$ Bew(⌜Bew(⌜L⌝)⇒C⌝)⇒(Bew(⌜Bew(⌜L⌝)⌝)⇒ Bew(⌜C⌝)) HB2
6. $\vdash_{PA}$ Bew(⌜L⌝)⇒ (Bew(⌜Bew(⌜L⌝)⌝)⇒ Bew(⌜C⌝)) 4'+5+transit
7. $\vdash_{PA}$ Bew(⌜L⌝)⇒ Bew(⌜Bew(⌜L⌝)⌝) HB3
8. $\vdash_{PA}$ Bew(⌜L⌝)⇒ Bew(⌜C⌝) 7+8+tautología
9. $\vdash_{PA}$ Bew(⌜C⌝)⇒ C hipótesis
10. $\vdash_{PA}$ Bew(⌜L⌝)⇒ C 8+9+transit
11. $\vdash_{PA}$ L 1+10+si y solo si
12. $\vdash_{PA}$ Bew(⌜L⌝) HB1
13. $\vdash_{PA}$ C MP 10 y 12

El segundo teorema de Gödel

Si PA es consistente entonces $\nvdash_{PA} \mathrm{Con}_{PA}$

Dem:

Supongamos PA consistente.

En PA se puede probar $\vdash_{PA} 0 \neq \overline{1}$ con lo cual

no es el caso $\vdash_{PA} 0 = \overline{1}$

Por el contrarrecíproco del teorema de Lob,

no es el caso $\vdash_{PA} \mathrm{Bew}(\ulcorner 0 = \overline{1} \urcorner) \Rightarrow (0 = \overline{1})$ (1)

Usando la tautología $\sim A \Rightarrow (A \Rightarrow B)$ se tiene

$\vdash_{PA} \sim\mathrm{Bew}(\underbrace{\ulcorner 0 = \overline{1} \urcorner}_{A}) \Rightarrow (\mathrm{Bew}(\ulcorner 0 = \overline{1} \urcorner) \Rightarrow (\underbrace{0 = \overline{1}}_{B}))$

si $\vdash_{PA} \sim\mathrm{Bew}(\ulcorner 0 = \overline{1} \urcorner)$ se aplica MP y

$\vdash_{PA} \mathrm{Bew}(\ulcorner 0 = \overline{1} \urcorner) \Rightarrow (0 = \overline{1})$ lo que contradice (1)

con lo cual no es el caso de $\vdash_{PA} \sim\mathrm{Bew}(\ulcorner 0 = \overline{1} \urcorner)$ (*)

Como vale $\vdash_{PA} 0 \neq \overline{1}$ por HB1 $\vdash_{PA} \mathrm{Bew}(\ulcorner 0 \neq \overline{1} \urcorner)$ y

es fácil ver que

$\vdash_{PA} \mathrm{Con}_{PA} \Rightarrow \sim\mathrm{Bew}(\ulcorner 0 = \overline{1} \urcorner)$

y aplicando (*)

no es el caso de $\vdash_{PA} \mathrm{Con}_{PA}$.