UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

EL TEOREMA DE HERBRAND Y LA CONSISTENCIA DE LA ARITMÉTICA DE PEANO

T E S I S

QUE PARA OBTENER EL TÍTULO DE

M A T E M Á T I C O

P R E S E N T A

CAMILO CAMHAJI GARCÍA

TUTOR: DR. CARLOS TORRES ALCARAZ

A mi Madre (Cucurucho)

(q.e.p.d.)

A mi Tío Toño
(q.e.p.d)

“Dejar una gran duda suele ser más importante que muchas respuestas”

Martín Cañas

(Profesor de matemáticas)

Agradecimientos

Quisiera agradecer en primer lugar a mis padres, que con su confianza y empeño en que acabara esta tesis al fin lo pude lograr, y aquí se las presento. A mi mamá por ser una fuente de buenos deseos para su hijo y por hacer las correcciones ortográficas para que quedara presentable. Por dedicar su vida entera a forjar un buen hombre y lograr que así fuera, con mucho cariño le dedico a esa enorme entrega este trabajo. Se que le hubiera gustado ver su conclusión pero también se que desde donde esta observa en todo momento. Con esta dedicatoria quiero agradecerle por todo lo que me dio y sigue dando gracias mamá, todo mi cariño.

A mi papá por tener siempre la ilusión de que acabaría este trabajo y no dejar de preguntar ¿Y esa tesis para cuándo?

En segundo lugar a mis Tías Cris y Helen por haber estado siempre ahí para ofrecerme su apoyo, son el motivo de que la familia siga unida. A Danny por ser mi prima consentida. A mis abuelos por que de niño fueron mis padres también y porque de grande los sigo queriendo como tales.

En tercer lugar quiero agradecer a todas aquella personas que han estado conmigo en las buenas y en las malas, mis amigos. De la facultad a Lilia y Alf quisiera agradecerles por haber compartido conmigo la carrera con esas largas sesiones de estudio y por haberme motivado siempre que los necesité durante este periodo. Fue muy importante haber compartido con ustedes la experiencia de ser ayudante pues quien sabe que sería de las calificaciones de cientos de alumnos sin su ayuda y porque esos momentos que compartimos afianzaron la amistad. A mis amigos más queridos que intento mencionarlos a todos aunque se me pueda olvidar alguno, saben que los llevo en mi corazón desde hace mucho tiempo, a toda la bandera del Héroes: Toño, Iván, Felipe, Fabo, Pocholo, Ana, Valeria, Raúl, Armando, Gerónimo, Nayar, y a todos los demás asociados.

A mi profesor Carlos Torres pues sé que esperar tantos años no es sencillo, pero este trabajo ayudo a no sólo tener un director de tesis sino un amigo verdadero, a él todo mi aprecio y gracias por la espera.

A Dora por ayudarme con su perseverancia y sus conocimientos sobre computación para ver terminado este trabajo y por ofrecerme su cariño y comprensión al empezar una nueva etapa de nuestras vidas.

A mis hermanos Sara, Elías y Olivia porque sin ustedes seguro sería una persona muy diferente, gracias por el apoyo y por los buenos sentimientos.

A todos los que por alguna u otra razón se me olvida agradecerles pero sepan que si han estado ahí con buenas intenciones estarán en mi corazón, los quiero.

Camilo.

INDICE

Introducción

Los últimos años del siglo XIX fueron escenario de un acalorado debate en torno a la naturaleza y fundamentos de las matemáticas, el cual se habría de intensificar en el primer cuarto del siglo XX con la intervención de matemáticos de la talla de Russell, Whitehead, Hilbert y Poincaré. Uno de los principales intentos por darles un fundamento seguro a las matemáticas en este periodo es el de Hilbert, quien con su programa en los años veinte intento alcanzar una solución satisfactoria. (Sobre este tema habremos de hablar en el capítulo 3 de este trabajo) Es en este entorno cuando aparecen los trabajos de Herbrand. Este periodo de discusión finalizó con la publicación por parte de Gödel de sus famosos teoremas de incompletud. Si bien las investigaciones en torno a la fundamentación de las matemáticas se vieron afectados por tales teoremas, la teoría de la demostración de Hilbert abrió un campo de investigación muy extenso dentro de la lógica matemática.

Cuando Herbrand presentó su tesis de doctorado, Hilbert y sus seguidores habían edificado el poderoso aparato de la metamatemática a fin de lograr un fundamento para las matemáticas con base en el programa mencionado. El trabajo de Herbrand se centró en apoyar las tesis de Hilbert, en la búsqueda de una construcción sintáctica de la matemática, dentro de los trabajos que Herbrand realizó los métodos semánticos no tenían cabida, por lo cual Herbrand no cesó de criticar y disentir del trabajo realizado dentro del programa, sobre todo por darle cabida al sentido semántico. Para algunos de los estudiosos cercanos a Hilbert, las ideas encontradas en los trabajos de Herbrand ayudaron a generar nuevas propuestas que modificaban la dirección original.

Una de las preocupaciones centrales del programa era hallar una prueba de la consistencia de la aritmética basada en los métodos finitistas que Hilbert había impulsado, la solución a este problema se vio frustrada básicamente por la aparición del segundo teorema de Gödel. En esta tesis exponemos una demostración de la consistencia de la aritmética de Peano siguiendo como idea central al teorema de Herbrand. El trabajo inicia con la explicación de la importancia que tiene dicho teorema, introduciendo de esta manera las ideas que hallaremos en la demostración. En una segunda parte nos ocupamos de ciertas cuestiones semánticas y de su manejo dentro de la demostración. Con todo lo anterior sentamos las bases para desarrollar la prueba de consistencia inspirada en los métodos introducidos por Herbrand.

El texto está pensado como un apoyo para los cursos de lógica matemática, dirigido a estudiantes de séptimo u octavo semestre. En un capítulo especial, el capítulo cero, presentamos las nociones básicas para seguir el texto, aclarando al lector el sentido que se les da dentro de este trabajo. Para ello introducimos los conceptos y la notación básica, la cual difiere de la que usó Herbrand. Este cambio se realiza en beneficio de la claridad, dejando de lado el sentido de las ideas propuestas.

Al buscar las ideas iníciales que animaron los trabajos de Herbrand, notamos que se hallaban dispersas en algunos artículos escritos por Jean Van Heijenoort. Por ejemplo, es con la notación de este autor que damos a conocer las ideas de la forma funcional y la expansión de una fórmula. Con ello tenemos una notación más sencilla que la original, lo cual permite una mejor comprensión al momento de presentar el teorema central y su demostración. El primer capítulo termina con algunas de las consecuencias directas del teorema de Herbrand y con su estudio sobre las funciones analizadoras. Exponemos cómo cometió un error al considerar que éstas podían proveer una cota superior para la búsqueda de las expansiones de una fórmula; no obstante, Dreben y Denton lo notan y dan la corrección [en Dreben 1963] explicando como este no devalúa el trabajo de Herbrand sólo lo revisa.

En el segundo capítulo tratamos la consistencia de la aritmética. Comenzamos revisando los cambios principales que Dreben y Denton le dan a las ideas originales, haciendo a un lado los prejuicios semánticos de Herbrand. Además examinamos cómo este cambio, con relación a la semántica, hace posible presentar una versión de la prueba de la consistencia de la aritmética vía el teorema de Herbrand. Como veremos, en la prueba el uso semántico del teorema permite verificar la consistencia de la aritmética mediante la generación de una serie de fórmulas, de las cuales se hace su expansión de satisfacción y entonces se puede concluir que la aritmética es consistente hasta la última fórmula de cada teorema que ha sido agregado. Como veremos esta solución no cumple con el finitismo de Hilbert, pero no por esto deja de ser un trabajo de interés. Pudiéndose comparar en su importancia con la demostración de la consistencia realizada por Gentzen.

En el capítulo 3 hacemos una reseña del contexto histórico en que Herbrand desarrolla sus ideas, es decir pasamos lista de algunos autores que influenciaron su obra, tratando de precisar cómo es que le sugirieron algunas preguntas detonantes que Herbrand responde dentro de su obra. En particular, nos interesó ver cómo a pesar de su aislamiento logró desarrollar lo que Bernays llama “el teorema central de la lógica de predicados”. Así mismo, nos interesó saber cómo generó una de las primeras propuestas de lo que hoy conocemos como funciones recursivas primitivas, tema con el que cerramos este capítulo.

Antes de finalizar esta introducción queremos decir algunas palabras acerca de su vida, si bien se vio cortada de tajo al caer de un risco con tan sólo veintitrés años de edad en 1931, Herbrand dejó un legado de ideas tan ricas que su obra ha sido una fuente de inspiración hasta nuestros días, donde se utilizan en áreas semánticas, como los lenguajes de programación o dentro de la teoría de la demostración y en la demostración automática de teoremas. No podemos sino lamentar la muerte prematura de un pensador que sin lugar a duda nos habría seguido enriqueciendo con un sinnúmero de ideas y resultados que nos habrían maravillado y sorprendido tanto como el teorema que aquí exploramos.

Capítulo 0
Notación y conceptos básicos

En este capítulo introducimos algunas nociones básicas de la lógica matemática necesarias para la comprensión del Teorema de Herbrand. Éstas incluyen algunos conceptos básicos de la lógica proposicional, así como del lenguaje de la lógica de predicados. En el desarrollo del tema enumeramos los símbolos a utilizar y las reglas que nos permiten manejar y construir las fórmulas. Asimismo, hacemos uso de algunos símbolos que, sin pertenecer formalmente al lenguaje, sirven como abreviaturas prácticas de expresiones del lenguaje. Hacia el final mostramos la necesidad de utilizar fórmulas prenexadas y explicamos qué información nos proporcionan las fórmulas de este tipo.
Dado el carácter panorámico de este capítulo, en general los conceptos y los resultados se presentan en un lenguaje un tanto inexacto, casi coloquial.

0.1 Nociones de Lógica Proposicional

En primer lugar veamos qué es una fórmula de la lógica proposicional.
En general, se trata de una fórmula en la que sólo aparecen variables proposicionales, conectivos y símbolos de agrupación.
Para ser más precisos, consideremos los siguientes símbolos y reglas con que se construye la lógica proposicional.

Conectivos: $\neg$ (no), $\wedge$ (y), $\vee$ (o) Los demás conectivos ($\rightarrow$, implica y $\leftrightarrow$, sí y sólo sí) se toman como abreviaturas.
Variables proposicionales: Un conjunto $VP = \{P_1, P_2, ..., P_n, ...\}$ de variables proposicionales.
Paréntesis: (,) como símbolos de agrupación o para denotar la prioridad de un conectivo en la fórmula.

A las letras $P_1, P_2, ..., P_n, ...$ se las llama *fórmulas atómicas* y a las fórmulas que estén formadas con una sola aplicación de un conectivo les llamaremos *moléculas*, es decir, $(P_1 \vee P_2)$, $(P_1 \wedge P_2)$ y $\neg P_1$ son moléculas. Todas las expresiones que se pueden formar mediante el uso repetido de fórmulas atómicas o moléculas y el uso de conectivos y paréntesis se consideran fórmulas de la lógica proposicional. [1]

[1] Al respecto véase Mendelson pp. 29–37 o Kleene pp. 4-12.

Semántica.- una *asignación* (A) es una función A: *VP* ⇨ {0,1}. A los valores 0 y 1 se les llama *valores de verdad* (1 = verdadero, 0 = falso). Toda asignación A se extiende a las fórmulas de *L* mediante las siguientes reglas:

$A(X \wedge Y) = 1 \Leftrightarrow A(X) = A(Y) = 1 \qquad A(X \vee Y) = 0 \Leftrightarrow A(X) = A(Y) = 0 \qquad A(\neg X) = 1 \Leftrightarrow A(X) = 0$

En lo siguiente y cuando sea conveniente usaremos el símbolo ⇔ para abreviar la frase sí y sólo sí

En relación al teorema de Herbrand las siguientes nociones y proposiciones son de importancia.

Definición 0.1.1: Una fórmula *X* es una *tautología* sí y sólo sí para toda asignación A, A(*X*) = 1, es decir, si su valor de verdad es siempre 1 sin importar cual sea el valor de verdad que se le asigne a cada una de las variables de la fórmula. Esto último se puede corroborar mediante diferentes técnicas, dos de las cuales son bien conocidas: las tablas de verdad y el método de los árboles de verdad.

EJEMPLOS:

a) $P \vee \neg P$ b) $((P_1 \leftrightarrow ((\neg P_2) \vee P_3)) \rightarrow ((\neg P_1) \rightarrow P_2))$

Haremos la tabla de verdad de a) para comprobar que es una tautología.

P	$\neg P$	$P \vee \neg P$
0	1	1
1	0	1

Definición 0.1.2: Una fórmula que es falsa bajo cualquier asignación de verdad a sus variables proposicionales se dice que es *una contradicción o no satisfacible*. Es claro que la negación de una tautología es una contradicción y viceversa.

Proposición 0.1.1

Si una fórmula *Y* se obtiene al reemplazar las variables proposicionales de una tautología *X* por fórmulas del lenguaje, (haciéndose la misma sustitución para todas las presencias de las variables sustituidas), entonces la fórmula *Y* es una *instancia de tautología*.

EJEMPLOS:

Tomemos la tautología del inciso a) en el ejemplo anterior y reemplacemos la variable *P* con la nueva fórmula $P_1 \rightarrow P_2$. Tras la sustitución lo que resulta es una fórmula *X* ´ que es una tautología. En efecto, el resultado de la substitución es la fórmula $(P_1 \rightarrow P_2) \vee \neg(P_1 \rightarrow P_2)$ cuya tabla de verdad es la siguiente:

P_1	P_2	$P_1 \rightarrow P_2$	$\neg(P_2 \rightarrow P_2)$	$(P_1 \rightarrow P_2) \vee \neg(P_1 \rightarrow P_2)$
0	0	1	0	1
0	1	1	0	1
1	0	0	1	1
1	1	1	0	1

Ergo se trata de una tautología.

0.2 Nociones relativas al Cálculo de Predicados

Los lenguajes de primer orden tienen sus raíces en el lenguaje introducido por Russell y Whitehead en P*rincipia Mathematica.* En éstos, además de utilizarse los conectivos lógicos, se hace uso de constantes y variables individuales, así como de predicados, símbolos de función y los cuantificadores universal y existencial.

El lenguaje que emplearemos es el siguiente:

Conectivos: $\neg$ (*no*), $\wedge$ (*y*), $\vee$ (*o*).
Cuantificadores: $\exists$ (*existencial*) y $\forall$ (*universal*).
Variables individuales: $x_1, x_2, x_3, \ldots, x_n, \ldots$
Constantes: $c_1, c_2, c_3, \ldots., c_n, \ldots$
Paréntesis: (,) como símbolos de agrupación o para denotar la prioridad de una operación en la fórmula.
Símbolos funcionales: para cada $n \in \mathbb{N}^+$ y $k \in \mathbb{N}$ un símbolo f_k^n
Símbolos de relación (predicados): para cada $n \in \mathbb{N}^+$ y $k \in \mathbb{N}$ un símbolo R_k^n

Términos.-
Los *términos* del cálculo de predicados se forman con los símbolos funcionales, junto con las constantes y variables individuales. La definición formal es la siguiente:

1) Las constantes y variables individuales son *términos*.
2) Si f_k^n es un símbolo funcional y $t_1,t_2,.t_3,\ldots,t_n$ son *términos*, entonces $f_k^n(t_1,t_2,t_3,\ldots,t_n)$ es un *término*.
3) El conjunto mínimo que cumpla las anteriores condiciones es el conjunto de términos.

Fórmulas.-
1) Si R_k^n es un símbolo de relación y $t_1,t_2,.t_3,\ldots,t_n$ son términos, entonces $R_k^n(t_1,t_2,.t_3,\ldots,t_n)$ es una *fórmula atómica*.
2) Si P es una variable proposicional entonces P es una *fórmula atómica.*

A las fórmulas hechas con un solo conectivo del lenguaje o un solo cuantificador les llamaremos *moléculas,* es decir, $R_1(\bar{x}) \vee R_2(\bar{x})$, $R_1(\bar{x}) \wedge R_2(\bar{x})$, $\neg R(\bar{x})$, $\forall x R(x)$ y $\exists R(x)$ son moléculas (donde $\bar{x}$ denota a todos los términos que figuran en R). Las fórmulas que se pueden formar usando repetidas veces conectivos, moléculas, átomos y paréntesis hacen una fórmula del cálculo de predicados. [2]

Definición 0.2.1: Estableciendo el concepto de alcance de los símbolos $\exists$ (*existencial*) y $\forall$ (*universal*) que serán como ya los mencionamos los cuantificadores. Definimos alcance de un cuantificador de la siguiente manera. Si A es una formula y tenemos $\exists x A$ o $\forall x A$ entonces a la fórmula A le llamaremos el alcance del cuantificador.

[2] Al respecto véase Mendelson pp. 56-59 o Kleene pp. 74-83.

Definición 0.2.2: Se dice que la presencia de una *variable está acotada* en una fórmula cuando sucede que un cuantificador, ya sea existencial o universal, le de alcance. Lo anterior ocurre cuando la variable está inmediatamente después del cuantificador y si está dentro de la fórmula que éste cuantifica. De lo contrario se dice que la presencia de la *variable es libre*.

EJEMPLOS:

1) $R_1^2(x_1, x_2)$

2) $R_1^2(x_1, x_2) \to (\forall x_1) R_1^1(x_1)$

3) $(\forall x_1) R_1^2(x_1, x_2) \to (\forall x_1) R_1^1(x_1)$

4) $(\exists x_1) R_1^2(x_1, x_2)$

En el ejemplo 1) vemos que la única presencia de x_1 es libre. En el ejemplo 2) la primera presencia de x_1 es libre, más no así las presencias segunda y tercera de esta misma variable, que son acotadas. En los ejemplos 3) y 4) todas las presencias de x_1 son acotadas. Las presencias de x_2 en todos los ejemplos son libres.
Vemos que una misma variable puede figurar libre y acotada en una misma fórmula del lenguaje. También hacemos la siguiente observación: una variable puede aparecer acotada en una fórmula X del lenguaje, mientras puede figurar libre en una subfórmula de la fórmula X. [3]

Debido a que una variable puede figurar libre y acotada en una misma fórmula procedemos a hacer la siguiente definición.

Definición 0.2.3: Si F es una fórmula del lenguaje y t un término, entonces decimos que t es libre para x_i en F, si no hay una presencia libre de x_i que esté dentro del alcance de algún cuantificador Qx_j,, (con Q denotamos cualquiera de los cuantificadores existencial o universal), donde x_j es una variable en t. Este concepto tiene ciertas aplicaciones técnicas y será de uso común en el texto. Significa que si todas las presencias libres de x_i en F son substituidas por t, entonces no sucede que una variable de t quede acotada en alguna de las sustituciones.

EJEMPLOS:
En la fórmula $R_1^1(x_1)$ el término x_2 es libre para x_1, más no lo es en la fórmula $(\forall x_2) R_1^1(x_1)$.
Ahora si consideramos $(\forall x_2) R_1^2(x_1, x_2) \to R_1^1(x_1)$, el término $f_1^2(x_1, x_3)$ es libre para x_1, pero no lo es para la misma variable x_1 en la fórmula $(\exists x_3)(\forall x_2) R_1^2(x_1, x_2) \to R_1^1(x_1)$.

Definición 0.2.4: Otra noción que utilizamos es la de *fórmula rectificada.* Una fórmula es rectificada cuando cumple las siguientes condiciones:

i) No contiene *cuantificadores ociosos*, es decir, cuantificadores que no ligan variable alguna, o que tienen una variable que no está presente en ningún otro lugar en la fórmula, o que acotan una variable de manera redundante (como, por ejemplo, en $(\forall y)(\forall x) R_1^1(x)$).

ii) No contiene dos cuantificadores en una misma variable.

iii) Ninguna variable figura libre y acotada en la fórmula.

[3] Al respecto véase Mendelson pp. 82-85 o Kleene pp. 93-101.

Un hecho importante es que toda fórmula del lenguaje del cálculo de predicados es equivalente a una fórmula rectificada con las mismas variables libres.

Definición 0.2.5: Una fórmula *X* del lenguaje es un *enunciado* (*E*) si en ella ninguna variable figura libre. Lo que significa que todas sus variables están acotadas. Una fórmula es *abierta* si no contiene ningún cuantificador.

Definición 0.2.6: Si { $x_1, x_2,...,x_k$ } es el conjunto de variables que figuran libres en una fórmula *F*, con *C* (*F*) denotamos a la fórmula $\forall x_1 \forall x_2 \forall x_3 ... \forall x_k F$, llamada *cerradura* de *F*. En *C* (*F*) se ha puesto un cuantificador universal para cada una de las variables libres, tomando en cuenta el orden ascendente de los subíndices de las variables. Obteniendo de esta manera un *enunciado* ***E*** del lenguaje.

EJEMPLO:
Tomemos la fórmula: $R_1^2(x_2, x_5) \rightarrow \neg(\exists x_4) R_1^3(x_1, x_4, x_3)$; su cerradura y fórmula rectificada será $(\forall x_1)(\forall x_2)(\forall x_3)(\forall x_5)\left[R_1^2(x_2, x_5) \rightarrow \neg(\exists x_4) R_1^3(x_1, x_4, x_3)\right]$, donde ésta última fórmula es un enunciado del lenguaje.

Interpretaciones: Una noción muy importante en nuestro estudio es la de *interpretación* de una fórmula en una estructura.

Una interpretación *M* consiste en un conjunto no vacío *D*, llamado el *dominio* de la interpretación, donde:
1) A cada símbolo relacional R_k^n se le asigna una relación $(R_k^n)^M$ de grado *n* en el dominio.
2) A cada símbolo funcional f_k^n se le asigna una operación $(f_k^n)^M$ en *D* de *n* argumentos.
3) A cada constante individual *c* un elemento distinguido c^M en *D*.

En cada interpretación las variables individuales sólo pueden tomar como valores a elementos del dominio. Como veremos, en la aritmética de Peano a los conectivos y cuantificadores se les da su significado usual.

Se tiene una *asignación* cuando a cada variable se le hace corresponder un elemento específico en *D*.

Una fórmula *F* es satisfacible en una interpretación *A* si existe una asignación de valores a sus variables libres que la hacen "verdadera" para esos valores. Una fórmula *F* es *verdadera* en una interpretación *A* cuando todas las asignaciones posibles la satisfacen. En tal caso se escribe $A \vDash F$ ó como una opción de notación podemos escribir $\vDash_A F$.

En una interpretación una fórmula con variables libres puede no tener un valor de verdad fijo (pues su satisfacción depende de los valores asignados a sus variables). Para evitar este problema hacemos uso de la cerradura de la fórmula, pues las fórmulas en las que sólo figuran variables acotadas tienen un valor de verdad que no depende de los valores asignados a las variables, es decir, de las interpretaciones.

Si una fórmula F es verdadera en todas las interpretaciones posibles, decimos que es *válida* ó *universalmente válida* y escribimos $\vDash F$. Decimos que F es *contradictoria ó no satisfacible* si y solo si la negación de F es universalmente válida.

Debido al siguiente metateorema sólo consideraremos enunciados del lenguaje.

Proposición 0.2.1

Una fórmula es válida sí y sólo sí su cerradura es válida. En símbolos: Para toda fórmula F, $\vDash F$ sí y sólo sí $\vDash C(F)$ de hecho para toda fórmula F y para toda interpretación A, sucede que $\vDash_A F$ si y solo si $\vDash_A C(F)$.

Como un concepto preliminar para definir las nociones de verdad y satisfacibilidad hacemos claro el uso que se dará a una sucesión (s).

Definición 0.2.7: Sea s la secuencia función de un argumento que va de los términos usados en las fórmulas a valores dados de D el dominio de interpretación, ésta debe cumplir con las siguientes condiciones.

1) si el término t está compuesto por x_1 entonces $s(t)$ es b_1 un nombre dentro de D para dicha variable.
2) si el término t es una constante entonces $s(t)$ es la interpretación de dicha constante.
3) si f es una letra funcional debe existir g una operación correspondiente a f dentro del dominio D. Si además $t_1, \ \ ,t_n$ son términos entonces $s(f(t_1, \ \ ,t_n))$ es $g(s(t_1), s(t_2) \ \ ,s(t_n))$.

EJEMPLO: Sea el siguiente término $f_2^2(x_2, f_1^2(x_1, a_1))$ su interpretación en la aritmética es decir el conjunto de los números naturales con las operaciones suma y multiplicación ordinarias, ahora interpretamos a f_2^2 y f_1^2 respectivamente con estas operaciones y para la constante a_1 su interpretación es el numero dos (2) entonces mediante la sucesión s que define la interpretación del término, obtenemos $b_2 \, x \, (b_1 + 2)$ donde b_1 y b_2 son variables dentro de la aritmética.

Ahora definimos formalmente las nociones de verdad y satisfacibilidad de una fórmula (Mendelson(1987), según Tarski (1936)).

Definición 0.2.8: La noción de *satisfacibilidad* para las fórmulas del cálculo de predicados, que también denotaremos algunas veces como $L_{M,}$, se define inductivamente como sigue:

1.Si X es una fórmula atómica $R_k^n(t_1,t_2,.t_3,...,t_n)$ y $(R_k^n)^M$ es la relación correspondiente en la interpretación, entonces una sucesión $s = (s_1,s_2,s_3,...,s_n,...)$ satisface a X sí y sólo sí $R_k^n(s(t_1), s(t_2), s(t_3),..., s(t_n))$, esto es, sí y sólo sí $(s(t_1), s(t_2), s(t_3),..., s(t_n)) \in (R_k^n)^M$.
Sean X, Y dos fórmulas para las cuales ya está definida la noción de satisfacción por una sucesión S.
2. S satisface a $\neg X$ sí y sólo sí S no satisface a X.
3. S satisface a $X \wedge Y$ sí y sólo sí S satisface a X y S satisface a Y.
4 .S satisface a $X \vee Y$ sí y sólo sí S satisface a X o S satisface a Y.
5 .S satisface a $X \rightarrow Y$ sí y sólo sí S satisface a Y o S no satisface a X.

6. S satisface a $\forall(x_i)X$ sí y sólo sí toda sucesión que difiere de S en a lo más la i-ésima componente, satisface a X. Como notación de que una fórmula es satisfacible por una asignación en un modelo usamos $M \vDash X\langle S\rangle$ o también lo denotamos como $\vDash_{\mathrm{M}} \mathrm{X}\,\langle S\rangle$.

Definición 0.2.9: Una fórmula F es *verdadera* bajo una interpretación sí y sólo sí toda sucesión en el dominio la satisface. Esta relación se denota con $M \vDash F$. Se dice que F es *falsa* para sí y sólo sí no hay sucesión alguna que satisfaga a F. Como notación tomamos $M \nvDash F$.

Definición 0.2.10: Una interpretación se dice que es un *modelo* de un conjunto Γ de fórmulas sí y sólo sí cada fórmula de Γ es verdadera bajo la interpretación.

Definición 0.2.11: Se dice que X *implica lógicamente a* Y (donde X e Y son fórmulas), si cada vez que X es satisfecha por una asignación S en una interpretación, Y también es satisfecha por la misma asignación y en la misma interpretación. Extendiendo el concepto, se dice que Y es *consecuencia lógica* de Γ, si cada vez que todos los elementos de Γ son satisfechos por una asignación S en una interpretación, entonces también lo es Y. Dos fórmulas X e Y son *lógicamente equivalentes* sí y sólo sí una implica a la otra y viceversa. Se escribe $X \equiv Y$.

Proposición 0.2.2
Toda instancia de tautología es universalmente válida. En otras palabras, si una fórmula se obtiene a partir de una tautología substituyendo las variables proposicionales de ésta ultima por fórmulas, el resultado será una fórmula universalmente valida.

0.3 Teorías de primer orden

En el caso del cálculo proposicional, las tablas de verdad proporcionan un método efectivo para saber si una fórmula es una tautología o no. Por contraste, en el cálculo de predicados no tenemos un procedimiento semejante para saber si una fórmula es universalmente válida. Esto se debe a que, en general, para verificar si la fórmula es verdadera, hay que tratar con una *infinidad* de dominios de cardinalidad arbitraria. Por lo anterior, el uso del método axiomático se hace necesario en el estudio de teorías que implican el uso de cuantificadores. Otra de las razones para recurrir a la axiomática formal es que ésta permite reconstruir la noción de validez universal sin recurrir a nociones semánticas, pues sólo requiere de nociones sintácticas, es decir, nociones que sólo se refieren a relaciones entre signos.

Sean X, Y y Z fórmulas cualesquiera de L_{M}. Los axiomas lógicos del cálculo de predicados son los siguientes:
1) $X \to (Y \to X)$
2) $(X \to (Y \to Z)) \to ((X \to Y) \to (X \to Z))$
3) $(\neg Y \to \neg X) \to ((\neg Y \to X) \to Y)$
4) $\forall x_i X(x_i) \to X(t)$
5) $\forall x_i (X \to Y) \to (X \to \forall x_i Y)$

En 4) t es un término y se pide que t sea libre para x_i en $X(x_i)$. En el caso particular cuando t es una variable x_i tenemos $\forall x_i X(x_i) \to X(x_i)$
En 5) X no contiene presencias libres de x_i.

Las reglas de inferencia del lenguaje son dos:

Modus ponens: De X y de $X \to Y$ se sigue Y. Indicaremos el uso de esta regla con la expresión *MP*.
Generalización: De X se sigue $\forall x_i(X)$. Indicaremos el uso de esta regla con la expresión *Gen*.

Definición 0.3.1: Una *prueba* es una sucesión $X_1, X_2, \ldots X_n$ de fórmulas, en donde cada una de ellas es un axioma o una consecuencia lógica de las anteriores en virtud de alguna de las reglas de inferencia.

Definición 0.3.2: Un t*eorema* es cualquier fórmula X, que figura al final de una prueba. Si X es un teorema, se escribe $\vdash_{\text{cp}} X$.

Si además de los axiomas lógicos, en la derivación de una fórmula X se incluyen algunas fórmulas tomadas de un conjunto Γ de fórmulas, lo que se tiene es una *deducción* de X a partir de Γ y se escribe $\Gamma \vdash_{\text{cp}} X$.

Debemos mencionar que en las pruebas se tendrán en cuenta las siguientes reglas lógicas:

Regla de elección ó regla E. El uso de esta regla se basa en el siguiente metateorema:
Si $\Gamma,\ \exists x Z(c) \vdash W$ donde el símbolo constante c no aparece ni en Z ni en Γ ni en W entonces, $\Gamma,\ \exists x Z(x) \vdash W$. Para encontrar una demostración de esta regla consultar [Amor 2006]

Bajo tales circunstancias $\Gamma \vdash W$, de hecho el uso de la regla E permite abreviar la demostración metamatemática de que $\Gamma, \exists x Z(x) \vdash W$, además existe una deducción de W a partir de Γ y $\exists x Z(x)$ en la cual no aparece $\exists x Z(c)$.

Como una variante al uso de esta regla tenemos lo siguiente.
Sea Γ un conjunto de fórmulas. Supongamos que las siguientes condiciones son satisfechas.

1) $\Gamma \vdash \exists x Z(x)$.
2) $\Gamma,\ Z(x) \vdash W$.
3) x no figura libre en W.
4) x no figura libre en Γ.

En este trabajo veremos ejemplos del uso de esta regla en las demostraciones que haremos en la sección siguiente sobre la forma prenexada de una fórmula, además la segunda versión de la regla la usaremos en el capitulo siguiente al demostrar el uso de la forma funcional de Herbrand.

Haremos también uso del siguiente metateorema, cuya aplicación se conoce como *demostración por reducción al absurdo*.

Proposición 0.3.1

Si $\Gamma, X \vdash Z \wedge \neg Z$ entonces $\Gamma \vdash \neg X$.
En otras palabras, si de $\Gamma \cup \{X\}$ se deduce una contradicción, entonces la negación de *X* se deduce a partir de Γ.

0.4 Forma prenexada de una fórmula

Una fórmula está prenexada cuando es de la forma:
$Q_1x_1Q_2x_2...Q_nx_n(X)$, donde *X* es una fórmula abierta y cada Q_i es un cuantificador universal o existencial.

EJEMPLOS:

a) $(\forall x)(\forall y)(\exists z)(R_1^1(x) \to (R_2^2(x,y) \to \neg R_3^2(y,z)))$

b) $(\forall x)(\exists y)(R_1^2(x,y) \to R_2^2(y,z))$

Para prenexar una fórmula *X* que no se encuentra en esta forma, es decir, en la cual no todos los cuantificadores preceden al resto de toda la fórmula, es suficiente con aplicar ciertas reglas simples. Con su ayuda se puede obtener una fórmula prenexada *X´*, tal que $X \equiv X'$. Las reglas se hallan implícitas en la siguiente proposición.[4]

Proposición 0.4.1

En lo siguiente *x* es una variable que no figura libre en una fórmula *D* y *C*(*x*) es una fórmula, entonces se cumple lo siguiente:

i) $\vdash ((\forall x)C(x) \to D) \equiv (Ex)(C(x) \to D)$

ii) $\vdash ((\exists x)C(x) \to D) \equiv (\forall x)(C(x) \to D)$

iii) $\vdash (D \to (\forall x)C(x)) \equiv (\forall x)(D \to C(x))$

iv) $\vdash (D \to (\exists x)C(x)) \equiv (\exists x)(D \to C(x))$

v) $\vdash \neg((\forall x)C(x)) \equiv (\exists x)(\neg C(x))$

vi) $\vdash \neg((\exists x)C(x)) \equiv (\forall x)(\neg C(x))$

Demostración del inciso *ii*: tomemos la fórmula $((\exists x)C(x) \to D)$ y demostremos que es lógicamente equivalente a $(\forall x)(C(x) \to D)$:

Primero procedemos a demostrar que $\vdash ((\exists x)C(x) \to D) \to (\forall x)(C(x) \to D)$. Con base en la proposición 0.3.1 procedemos como sigue:

1.- $((\exists x)C(x) \to D)$ Hipótesis.

[4] Al respecto véase Mendelson pp. 85-90 o Kleene pp. 125-134.

2.- $\neg(\forall x)(C(x) \to D)$ Hipótesis.
3.- $(\exists x)\neg(C(x) \to D)$ Por introducción del $\neg$ no a la fórmula.
4.- $(\exists x)(C(x) \wedge \neg D)$ Abreviatura de → y distribución del $\neg$ no en la fórmula.
5.- $(\exists x)C(x) \wedge (\exists x)\neg D$ Distribución del existe $\exists$.
6.- $(\exists x)C(x) \wedge \neg D$ Eliminación de cuantificador ocioso.
7.- $(\exists x)C(x)$ Separación de la conjunción en 6.
8.- $\neg D$ Separación de la conjunción en 6.
9.- D Por *MP* de 1 y 7.

Tenemos así que de { $((\exists x)C(x) \to D)$, $\neg(\forall x)(C(x) \to D)$ } se deduce una contradicción, por lo cual la fórmula $(\forall x)(C(x) \to D)$ se deduce mediante el uso de la proposición 0.3.1.

Ahora demostraremos que $\vdash$ $(\forall x)(C(x) \to D) \to ((\exists x)C(x) \to D)$ tenemos lo siguiente:

1.- $(\forall x)(C(x) \to D)$ Hipótesis.
2.- $C(b)$ Hipótesis.
3.- $C(b) \to D$ De 1 por la regla $\forall(x)Y(x) \to Y(b)$.
4.- D Por *MP* de 2 y 3.
5.- $(\forall x)(C(x) \to D)$, $(\exists x)C(x) \vdash D$ Deducimos esta fórmula de 1-4 y por la regla E.
6.- $\vdash (\forall x)(C(x) \to D) \to ((\exists x)C(x) \to D)$ Por la regla de la deducción aplicada 2 veces.

Con lo cual tenemos que $\vdash$ $((\exists x)C(x) \to D) \equiv (\forall x)(C(x) \to D)$ quedando así demostrado el inciso *ii)* ▣

EJEMPLOS:
Consideremos la fórmula $(\forall x)(R_1^1(x) \to (\forall y)(R_2^2(x,y) \to \neg(\forall z)R_3^2(y,z)))$ y siguiendo los pasos antes indicados la convertimos en una fórmula prenexada.
1.- $(\forall x)(R_1^1(x) \to (\forall y)(R_2^2(x,y) \to (\exists z)\neg R_3^2(y,z)))$ Por el inciso (*v)*.
2.- $(\forall x)(R_1^1(x) \to (\forall y)(\exists z)(R_2^2(x,y) \to \neg R_3^2(y,z)))$ Por el inciso (*iv)*.
3.- $(\forall x)(\forall y)(R_1^1(x) \to (\exists z)(R_2^2(x,y) \to \neg R_3^2(y,z)))$. Por el inciso (*iii)*.
4.- $(\forall x)(\forall y)(\exists z)(R_1^1(x) \to (R_2^2(x,y) \to \neg R_3^2(y,z)))$ Por el inciso (*iv)*.
Esta última es una fórmula prenexada.

Consideremos ahora la formula $(\neg(\exists x)R_1^1(x) \vee (\forall y)R_2^1(y)) \wedge (R_3^1(z) \to (\forall w)R_4^1(w))$
1.- $(\neg(\exists x)R_1^1(x) \vee (\forall y)R_2^1(y)) \wedge (\forall w)(R_3^1(z) \to R_4^1(w))$ Por el inciso (*iii)*.
2.- $(\forall x)(\neg R_1^1(x) \vee (\forall y)R_2^1(y)) \wedge (\forall w)(R_3^1(z) \to R_4^1(w))$ Por el inciso (*vi)*.
3.- $(\forall x)(\forall y)(\forall w)(\neg R_1^1(x) \vee R_2^1(y)) \wedge (R_3^1(z) \to R_4^1(w))$

En este último paso usamos una regla que no hicimos explicita: en relación a los conectivos *y* ($\wedge$) y *o* ($\vee$), los cuantificadores pueden pasar al inicio de la fórmula sin cambiar su tipo.

Proposición 0.4.2
Si X es una fórmula del lenguaje, entonces hay una fórmula prenexada, denotada con $P(X)$, tal que:
a) X y $P(X)$ tienen las mismas variables libres.
b) X es lógicamente equivalente a $\mathrm{P}(X)$.

En virtud de las proposiciones anteriores, en los lenguajes de primer orden podemos considerar únicamente fórmulas prenexadas rectificadas.

Capítulo 1
Teorema de Herbrand

En este capítulo veremos el método de Herbrand para la eliminación de cuantificadores de fórmulas prenexadas y aclararemos la necesidad de la “forma funcional de Herbrand”; además, expondremos la noción de la “expansión de Herbrand de una fórmula” y veremos el uso que les da en su teorema y el tipo de problemas que presenta este proceso de eliminación de cuantificadores.
Asimismo, enunciaremos el teorema de Herbrand y explicaremos su uso en forma directa, y examinaremos las dificultades prácticas para determinar la validez de una fórmula.
También veremos qué es lo que pretende Herbrand al aplicar su teorema y analizaremos las razones por las que el teorema no tiene el alcance que él desea.
Daremos una idea de cómo se construyen funciones analizadoras. Estas fueron planteadas por otros autores que siguieron a Herbrand en el desarrollo de su demostración y notaron un error al querer acotar la búsqueda.
Finalmente daremos un avance sobre las implicaciones del teorema de Gödel sobre el resultado que busca Herbrand.

1.1 Forma funcional de Herbrand

Exponemos en esta sección como obtener la forma funcional de Herbrand, para dar curso temporal a las ideas, en esta sección sólo planteamos como obtener la forma funcional cerrada de validez, pero en el capitulo siguiente exponemos que también se puede generar de manera dual la forma funcional cerrada de satisfacción.

Dada una fórmula X del lenguaje de predicados, la *forma funcional cerrada de validez de X*, denotada con Xcv, es una fórmula prenexada sin cuantificadores universales que satisface la siguiente condición:

Versión semántica: $\vDash X$ si y solo si $\vDash$ Xcv.

Versión sintáctica: $\vdash X$ si y solo si $\vdash$ Xcv.

Veamos como se obtiene la forma funcional de Herbrand, es este caso la forma cerrada de validez de una fórmula.

Sin pérdida de generalidad podemos suponer que X es una fórmula rectificada prenexada (la cual, como hemos visto, siempre se puede hallar).

Definición 1.1.1: Se dice que un cuantificador universal es *existencialmente libre* si no lo preceden en la forma prenexada de la fórmula cuantificadores existenciales. De lo contrario se dice que es *existencialmente ligado*.

Debemos hacer notar que el orden de los cuantificadores en fórmulas prenexadas puede cambiar, pero haremos uso de la convención siguiente, los cuantificadores obtenidos en la forma prenexada no podrán alternar su orden contra el dado por su posición original en la fórmula, si la fórmula ya aparecía prenexada entonces simplemente se conserva el orden de los cuantificadores.

Definición 1.1.2: Se dice que una *variable de X* es *existencialmente libre* si no está dentro del alcance de un cuantificador existencial en X, o está dentro del alcance de un cuantificador existencial en X pero la precede un cuantificador universal existencialmente libre, sino sucede ninguno de los dos casos anteriores se dice que la *variable es existencialmente ligada*.

EJEMPLO: Consideremos la fórmula $\forall x \exists y \forall z A(x, y, z)$. En este caso x es una variable existencialmente libre, puesto que esta dentro del alcance de un cuantificador existencial pero la liga un cuantificador existencialmente libre, mientras y y z son variables existencialmente ligadas, la primera esta cuantificada a un cuantificador existencial, mientras que la segunda esta cuantificada por un cuantificador universal existencialmente ligado.

Sean $x_1, x_2, x_3 ... x_n$ las variables universales existencialmente ligadas en X, es decir, que están cuantificadas universalmente pero dentro del alcance de un cuantificador existencial.

Sea e_i el número de cuantificadores existenciales que hacen a la variable x_i existencialmente ligada y sean $y_1, y_2, y_3, ... y_n$ las variables existencialmente cuantificadas de tales cuantificadores en el orden en que aparecen en X. Sean $f_1, f_2, f_3, ... f_n$ símbolos funcionales que no figuran en X, con f_i de aridad e_i . Con x_i queda asociado el término funcional de Herbrand $f_i(x_{i1}, x_{i2}, x_{i3}, ... x_{iei})$.

Ahora Xcv se obtiene como sigue:
En la fórmula X se eliminan todos los cuantificadores universales, a la vez que todas las presencias de las variables x_i se reemplazan por $f_i(x_{i1}, x_{i2}, x_{i3}, ... x_{iei})$. Obviamente en Xcv pueden figurar otras variables libres, a saber, aquellas que son existencialmente libres en X.

EJEMPLOS:
Consideremos la fórmula $\exists x \forall y_1 \forall y_2 R(x, g(y_1, y_2))$. En la cual las variables y_1 y y_2 son existencialmente ligadas. En este caso $e_1 = e_2 = 1$. Tomemos dos símbolos funcionales de Herbrand f_1 y f_2 de aridad 1. La fórmula Xcv es $\exists x R(x, g(f_1(x), f_2(x)))$. Cabe señalar que g no es término funcional de Herbrand

Tomemos como segundo caso la fórmula:
$\forall y_1 \exists x_1 \forall y_2 \exists x_2 \forall y_3 (R_1^2(y_1, x_1) \wedge R_2^2(x_1, y_2) \wedge R_3^3(y_1, x_2, y_3))$; en esta, las variables y_2 y y_3 son existencialmente acotadas, mientras que y_1 es existencialmente libre.
Ahora $e_2 = 1$ y $e_3 = 2$. Tomemos dos símbolos funcionales de Herbrand f_2 de aridad 1 y f_3 de aridad 2.

Xcv es la fórmula $\exists x_1 \exists x_2 (R_1^2(y_1, x_1) \wedge R_2^2(x_1, f_2(x_1)) \wedge R_3^3(y_1, x_2, f_3(x_1, x_2)))$. En Xcv y_1 figura libre, ya que en *X* esta variable es existencialmente libre.

Para demostrar que una fórmula *X* es un teorema del cálculo de predicados si y solo si Xcv lo es, basta con demostrar que esto sucede cuando se elimina el primer cuantificador universal que se encuentra en la fórmula al recorrerla de izquierda a derecha, pues en tal caso la fórmula Xcv, se obtiene al llevar a cabo un número finito de veces este procedimiento.

Si X es de la forma $\forall x Yx$, entonces la variable *x* es existencialmente libre y la fórmula Xcv en cuestión es simplemente *Yx*. Es inmediato que una de ellas es teorema si y solo si la otra lo es.

Otra manera en la que el cuantificador universal puede aparecer es existencialmente acotado, es decir, de la manera siguiente: $\exists \bar{x} \forall y_1 Y(\bar{x}, y_1)$.
En este caso, con el símbolo $\exists \bar{x}$ nos referimos a la cadena de cuantificadores existenciales $\exists x_{i1} \exists x_{i2} \exists_{i3} ... \exists x_{in}$ que preceden al cuantificador $\forall y_1$ en la fórmula, es decir, todos los cuantificadores que hacen a la variable y_1 existencialmente acotada. En donde a la variable y_1 le corresponde un símbolo funcional f_1 de aridad *n* y $\bar{x}$ representa a la eneada $(x_1, x_2, x_3, ..., x_n)$.

Al eliminar el cuantificador existencialmente acotado de la fórmula $\exists \bar{x} \forall y_1 Y(\bar{x}, y_1)$ nos queda una fórmula de la forma: $\exists \bar{x} Y(\bar{x}, f_1(\bar{x}))$.

Demostraremos ahora que las fórmulas anteriores son equivalentes, es decir, una se deduce de la otra.
Primero supongamos que $\vdash \exists \bar{x} \forall y_1 Y(\bar{x}, y_1)$ y demostremos entonces que $\vdash \exists \bar{x} Y(\bar{x}, f_1(\bar{x}))$

1.- $\exists \bar{x} \forall y_1 Y(\bar{x}, y_1)$ Teorema.
2.- $\forall y_1 Y(\bar{x}, y_1)$ Hipótesis.
3.- $\forall y_1 Y(\bar{x}, y_1) \rightarrow Y(\bar{x}, f_1(\bar{x}))$ Teorema de *Lcp*, pues $f_1(x)$ es libre para y_1 en $Y(x, y_1)$.
4.- $Y(\bar{x}, f_1(\bar{x}))$ Por *MP* de 2 y 3.
5.- $\exists \bar{x} Y(\bar{x}, f_1(\bar{x}))$ Por la regla de cuantificación existencial aplicada las veces necesarias.

Como las hipótesis para emplear la regla E se cumplen tenemos entonces que $\vdash \exists \bar{x} Y(\bar{x}, f_1(\bar{x}))$.

Para demostrar que si $\vdash \exists \bar{x} Y(\bar{x}, f_1(\bar{x}))$, entonces $\vdash \exists \bar{x} \forall y_1 Y(\bar{x}, y_1)$, haremos lo siguiente;
Demostraremos que $CP \cup \{\neg(\exists \bar{x} \forall y_1 (\bar{x}, y_1))\}$ es inconsistente cuando $\vdash_{cp} \exists \bar{x} Y(\bar{x}, f_1(\bar{x}))$.

1.- $\neg(\exists \bar{x} \forall y_1 Y(\bar{x}, y_1))$ Hipótesis.
2.- $\forall \bar{x} \exists y_1 \neg(Y(\bar{x}, y_1))$ Equivalente a 1 en *Lcp*, por reglas de prenexación.
3.- $\forall \bar{x} \exists y_1 \neg(Y(\bar{x}, y_1)) \rightarrow \exists y_1 \neg Y(\bar{x}, y_1)$ Teorema de *Lcp*.
4.- $\exists y_1 \neg Y(\bar{x}, y_1)$ Por *MP* de 2 y 3.

Con esta deducción vemos que $\neg(\exists \bar{x} \forall y_1 Y(\bar{x}, y_1)) \vdash \exists y_1 \neg Y(\bar{x}, y_1)$

1b.- $\neg Y(\bar{x}, y_1)$ Hipótesis.
2b.- $\neg(\exists\bar{x}\forall y_1 Y(\bar{x}, y_1))$ Hipótesis.
3b.- $\exists\bar{x}Y(\bar{x}, f_1(\bar{x}))$ Teorema.
4b.- $\forall y_1 \neg Y(\bar{x}, y_1)$ Por *Gen* de 1b.
5b.- $\forall y_1 \neg Y(\bar{x}, y_1) \to \neg Y(\bar{x}, f_1(\bar{x}))$ Teorema de *Lcp*, pues f_1(x) es libre para y_1 en $\neg Y(x, y_1)$.
6b.- $\neg(Y(\bar{x}, f_1(\bar{x})))$ Por *MP* de 4b y 5b.
7b.- $\forall\bar{x}\neg(Y(\bar{x}, f_1(\bar{x})))$ Por *Gen* de 6b.
8b.- $\neg(\exists\bar{x}Y(\bar{x}, f_1(\bar{x})))$ Equivalente a 7b por reglas de prenexación.
9b.- $\exists\bar{x}Y(\bar{x}, f_1(\bar{x}) \wedge \neg(\exists\bar{x}Y(\bar{x}, f_1(\bar{x})))$ Conjunción explicita de 2b y 8b

En esta demostración tenemos que de $\neg Y(\bar{x}, y_1)$, $\neg(\exists\bar{x}\forall y_1 Y(\bar{x}, y_1)) \vdash$ $\exists\bar{x}Y(\bar{x}, f_1(\bar{x}) \wedge \neg(\exists\bar{x}Y(\bar{x}, f_1(\bar{x})))$ que es el paso 9b, en el cual tenemos una contradicción, es decir una fórmula de la forma $Z \vee \neg Z$.
Como las hipótesis necesarias para emplear la regla E se cumplen, hemos llegado a lo siguiente: $\neg(\exists\bar{x}\forall y_1 Y(\bar{x}, y_1)) \vdash_{cp} Z \vee \neg Z$. Ahora, como de $\neg(\exists\bar{x}\forall y_1 Y(\bar{x}, y_1))$ se deduce una contradicción, por la proposición 0.3.1 sabemos que $\vdash_{cp} \exists\bar{x}\forall y_1 Y(\bar{x}, y_1)$. ■

1.2 Expansión de Herbrand de una fórmula

El teorema de Herbrand enuncia una condición necesaria y suficiente para que una fórmula de *Lcp* (con esto denotamos al lenguaje del cálculo de predicados) sea válida o demostrable en el *CP* (con esto denotamos al cálculo proposicional). Se trata de una fórmula del cálculo proposicional asociado a ella. Dicha caracterización se basa en un procedimiento introducido por Herbrand, que a continuación explicamos.

El conjunto *T* de términos de *Lcp* es numerable. Debido a ello cualquier subconjunto de términos, digamos *T´*, también es numerable. Consideremos la siguiente familia $C_i(X)$ de conjuntos finitos de términos del lenguaje asociados a una fórmula *X*.

1) $C_0(X)$ contiene las constantes individuales, las variables libres y aquellas variables universales existencialmente libres de *X*. Cuando en *X* no hay ninguno de estos elementos, C_0 está formada por una constante arbitraria c_0.

2) $C_{i+1}(X)$ contiene a todos los elementos de $C_i(X)$ y a todas las instancias de los términos funcionales de Xcv que se obtienen cuando en éstos se reemplazan las variables por elementos de $C_i(X)$.

Sea *T´* el conjunto $\bigcup_{i=0}^{\infty} C_i(X)$, el cual consiste de términos de *Lcp*. Los términos de *T´* se pueden ordenar de modo que formen una sucesión $t_1, t_2, t_3, ..., t_n, ...$ El modo de llevar a cabo tal ordenación es irrelevante, aunque cabe mencionar que ésta se puede hacer de un modo efectivo (por ejemplo, con la numeración de Gödel). En consecuencia, cada $C_i(X)$ se puede considerar como una sucesión finita S_i de términos de *Lcp*.

EJEMPLOS:
Consideremos la fórmula $\forall x_1 \exists x_2 \forall x_3 R(x_1, x_2, x_3)$, donde Xcv es $\exists x_2 R(x_1, x_2, f(x_2))$. En este caso tenemos:

$C_0(X) = \{x_1\}$
$C_1(X) = \{x_1, f(x_1)\}$
$C_2(X) = \{x_1, f(x_1), f(f(x_1))\}$

y así sucesivamente, con esto podemos considerar que llegaremos a

$C_n(X) = \{x_1, f(x_1), f(f(x_1)), \ldots, f(f(\ldots f(x_1)\ldots)\}$ donde hemos puesto en el último término funcional *n* veces el símbolo *f* y sus respectivos paréntesis.

Tomemos ahora la fórmula $\forall x_1 \exists x_2 \exists x_3 \forall x_4 R(x_1, x_2, x_3, x_4, c)$, Xcv es $\exists x_2 \exists x_3 R(x_1, x_2, x_3, f(x_2, x_3), c)$. En este caso obtenemos:

$C_0(X) = \{x_1, c\}$
$C_1(X) = \{x_1, c, f(x_1,x_1), f(x_1,c), f(c,x_1), f(c,c)\}$
$C_2(X) = \{x_1, c, f(x_1,x_1), f(x_1,c), f(c,x_1), f(c,c), f(x_1,f(x_1,x_1)), f(x_1,f(x_1,c)), f(x_1,f(c,x_1)), f(x_1,f(c,c)), f(c,f(x_1,x_1)), f(c,f(x_1,c)), f(c,f(c,x_1)), f(c,f(c,c)), f(f(x_1,x_1),x_1), f(f(x_1,c),x_1), f(f(c,x_1),x_1), f(f(c,c),x_1), f(f(x_1,x_1),c), f(f(x_1,c),c), f(f(c,x_1),c), f(f(c,c),c), f(f(x_1,x_1),f(x_1,x_1)), f(f(x_1,x_1),f(x_1,c)), f(f(x_1,x_1),f(c,x_1)), f(f(x_1,x_1),f(c,c)), f(f(x_1,c),f(x_1,x_1),), f(f(c,x_1),f(x_1,x_1),), f(f(c,c),f(x_1,x_1)), f(f(x_1,c),f(x_1,c)), f(f(x_1,c),f(c,x_1)), f(f(x_1,c),f(c,c)), f(f(c,x_1),f(x_1,c)), f(f(c,c),f(x_1,c)), f(f(c,x_1),f(c,x_1)), f(f(c,x_1),f(c,c)), f(f(c,c),f(c,x_1)), f(f(c,c),f(c,c))\}$

El término $f(f(x_1,x_1), f(f(x_1,x_1), f(x_1,x_1)))$ aparecerá en $C_3(X)$ y cada C_i de orden superior tendrá términos en los cuales las funciones serán cada vez más complicadas, en ellos figuran todos los términos que aparecen en el conjunto anterior C_{i-1}.

Cabe señalar que cada C_i es una sucesión finita y que el conjunto $\{C_i \mid i \in \mathrm{N}\}$ es una cadena de series contenidas unas en otras de la siguiente forma $C_0 \subset C_1 \subset C_2 \subset ... \subset C_n$
.

Definición 1.2.1: Definimos recursivamente la *Expansión de X sobre Ci,*, como sigue:
1) Si *X* es atómica, $\overline{\mathrm{X}}^{C_i}$ es *X*
2) Si *X* es $\neg Y$, $\overline{\mathrm{X}}^{C_i}$ es $\neg(\overline{Y}^{C_i})$
3) Si *X* es $Y \vee Z$, $\overline{\mathrm{X}}^{C_i}$ es $\overline{Y}^{C_i} \vee \overline{Z}^{C_i}$

4) Si X es $Y \wedge Z$, $\overline{X}^{C_i}$ es $\overline{Y}^{C_i} \wedge \overline{Z}^{C_i}$

5) Si X es $\exists x Y(x)$, $\overline{X}^{C_i}$ es $\underset{k \le n}{\vee} \overline{Y(x/t_k)}^{C_i}$

6) Si X es $\forall x Y(x)$, $\overline{X}^{C_i}$ es $\underset{k \le n}{\wedge} \overline{Y(x/t_k)}^{C_i}$

Si X es una fórmula de *Lcp*. La *expansión de Herbrand de X sobre C_i*, la denotaremos indistintamente con Exp(X,C_i) o con $\overline{X}_{cv}^{C_i}$.

La expansión de una fórmula nos permite tratar la noción de validez, a través de la lógica proposicional, pues con ella los cuantificadores existenciales se convierten en disyunciones finitas y los cuantificadores universales en conjunciones finitas.

EJEMPLOS:

Tomemos la fórmula $\forall x \exists y(\neg R(x,x) \vee R(x,y))$. La Xcv que se obtiene es: $\exists y(\neg R(x,x) \vee R(x,y))$.

Sea $C_0 = \{x\}$; la expansión de Herbrand, Exp(Xcv,C_0), será:

Exp(Xcv,C_0) $\equiv \overline{\exists y(\neg R(x,x) \vee R(x,y))}^{C_0} \equiv \vee \overline{(\neg R(x,x) \vee R(x,y))\left(y/x\right)}^{C_0} \equiv \neg R(x,x) \vee R(x,x)$

Se puede ver que la fórmula $\neg R(x,x) \vee R(x,x)$ es una instancia de sustitución de la fórmula $P \vee \neg P$, la cual es una tautología.

Tomemos ahora la fórmula $\forall x \exists y \forall z(R(x,y) \vee \neg R(x,z))$ La fórmula Xcv es en este caso: $\exists y(R(x,y) \vee \neg R(x,f(y)))$.

Sea $C_0 = \{x\}$; la expansión de Herbrand Exp(Xcv,C_0), es:

$\overline{\exists y(R(x,y) \vee \neg R(x,f(y)))}^{C_0} \equiv \vee \overline{(R(x,y) \vee \neg R(x,f(y)))\left(y/x\right)}^{C_0} \equiv R(x,x) \vee \neg R(x,f(x))$

La pareja (x, x) no es igual a la pareja (x, $f(x)$) por lo que no podemos decir que se trate de una instancia de sustitución en una tautología.

Sea $C_1 = \{x, f(x)\}$. En este caso t_1 es x y t_2 es $f(x)$, de donde resulta que:

Exp(Xcv,C_1) $\equiv \overline{\exists y(R(x,y) \vee \neg R(x,f(y)))}^{C_1} \equiv \vee_{k \le 2} \overline{(R(x,y) \vee \neg R(x,f(y)))\left(y/t_k\right)}^{C_1} \equiv$

$(R(x,x) \vee \neg R(x,f(x))) \vee (R(x,f(x)) \vee \neg R(x,f(f(x))))$

Esta última fórmula es instancia de la tautología $(P_1 \vee \neg P_2) \vee (P_2 \vee \neg P_3)$, por lo cual tenemos que la expansión sobre C_1 da como resultado una tautología.

En general, la fórmula Exp(X,C_i) es una fórmula abierta que se puede considerar instancia de una fórmula del cálculo proposicional. Siguiendo las ideas que aparecen en la sección 0.1 capitulo anterior, tenemos dos alternativas:

1) Hay una n tal que $\text{Exp}(X,C_n)$ es instancia de tautología.
2) Para toda n, $\text{Exp}(X,C_n)$ no es instancia de tautología.

Estas dos posibilidades tienen consecuencias que en su conjunto constituyen el Teorema de Herbrand, tales consecuencias son las siguientes:

Proposición 1.2.1

Si para alguna n, $\text{Exp}(X,C_n)$ es instancia de tautología, entonces $\vdash_{\text{cp}} X$.

Proposición 1.2.2

Si para toda n, $\text{Exp}(X,C_n)$ no es instancia de tautología, entonces $\nvdash_{\text{cp}} X$.

Ahora después de haber explicado lo que es la forma funcional y la expansión de Herbrand de una fórmula, podemos enunciar el teorema de Herbrand, que no es otra cosa que el enunciado de esta equivalencia.

1.3 Teorema de Herbrand (1930)

Una fórmula X del lenguaje de la lógica de predicados es teorema del cálculo de predicados sí y sólo sí existe una $n \in \mathrm{N}$ tal que $\text{Exp}(X,C_n)$ es instancia de tautología. En símbolos:

Para toda $X \in Lcp$, $\vdash_{\text{cp}} X$ sí y sólo sí existe $n \in \mathrm{N}$ tal que $\vDash_{\mathrm{T}} \text{Exp}(X,C_n)$.

En la demostración de la proposición 1.2.2 Herbrand procede por inducción siguiendo un procedimiento enteramente sintáctico. Para ello introduce lo que llama el *orden de una fórmula*. Se trata del menor número natural p tal que $\text{Exp}(X,C_p)$ es instancia de tautología. En símbolos:
$O(X) = min\{p | Exp(X,Sp)$ es instancia de tautología.$\}$

Herbrand lleva a cabo la demostración como sigue:

Primero, demuestra que todos los axiomas del cálculo de predicados son de orden finito.
Segundo, demuestra que cada regla de inferencia del cálculo de predicados cumple lo siguiente: Si las premisas son de orden finito, la conclusión también es de orden finito. La conclusión a la que llega es que todo teorema del cálculo de predicados es de orden finito, lo cual equivale a la proposición 1.2.2.

La demostración de Herbrand es difícil de seguir, además de que contiene un error. En este texto demostraremos las proposiciones 1.2.1 y 1.2.2 recién mencionadas, siguiendo otro camino. Para ello, requerimos de la proposición siguiente:

Proposición 1.2.3
Si para toda n, $\text{Exp}(X,C_n)$ no es instancia de sustitución de una tautología, entonces X no es universalmente válida.

Como sabemos, toda fórmula X que es teorema de *Lcp* es válida. En símbolos: Si $\vdash X$, entonces $\models X$.

Por contraposición: Para toda fórmula X de *Lcp*,. Si $\not\models X$, entonces $\nvdash X$. De esta manera podemos demostrar la proposición 1.2.3 y de ésta se sigue la proposición 1.2.2.

Demostración de la proposición 1.2.3.
La expansión de Herbrand de una fórmula X se obtiene a partir de la fórmula Xcv que carece de cuantificadores universales (es decir, Xcv es una fórmula existencial). Debido a ello toda expansión de Herbrand es una disyunción de instancias de la matriz M de la fórmula Xcv. Tomando en cuenta las leyes asociativa y conmutativa para la disyunción, tenemos lo siguiente:

1) Si $C_n = \{t_1,...,t_k\}$ y Xcv es $\exists x_1...\exists x_m M(x_1,...,x_m)$, entonces la expansión de Herbrand de la fórmula es Exp(X,C_n) = $\vee_{i_1 \leq k} (\vee_{i_2 \leq k} ...(\vee_{i_m \leq k} M(t_i,...,t_{i_m})...))$ por otra parte, las disyunciones de instancias de la matriz se pueden agrupar como se deseé.
2) Para toda $n,h \in \mathrm{N}$, Exp(X,C_n) es subfórmula de Exp(X,C_{n+h}), para lo cual basta agrupar adecuadamente Exp(X,C_{n+h}).

Ahora supongamos que ninguna expansión de Herbrand de una fórmula X es instancia de tautología. En tal caso se puede demostrar que la fórmula X no es universalmente válida construyendo una estructura A sobre el dominio de los números naturales, en la cual X es falsa. Para ello es de utilidad dar a las fórmulas de *CP* una forma más precisa.

Sea Exp(X,C_n) una expansión de Herbrand. A partir de ella podremos obtener una fórmula E_n del cálculo proposicional reemplazando las fórmulas atómicas de Exp(X,C_n) por variables proposicionales. El modo de llevar a cabo este reemplazo es importante, y, para ello, hay que ordenar al conjunto T' de los términos de *Lcp* que aparecen en alguna de las C_n. (Un ordenamiento posible es el siguiente: Las primeras componentes de la sucesión son los elementos de C_0 del orden de C_0. Después, ordenando C_1-C_0, se extiende la sucesión de modo que todos los elementos de C_1 figuren en ella. La aplicación reiterada de este procedimiento proporciona el orden deseado.)

Sea $t_1,t_2,...,t_n,...$ un ordenamiento de T'. Toda fórmula atómica de Exp(X,C_n) es de la forma $R(t_{i1},...,t_{ik})$ donde R es un símbolo relacional de *Lcp* y $t_{i1},...,t_{ik}$ son términos de T'(donde el índice ij señala el lugar que ocupa el término t_{ij} en la sucesión recién formada). E_n, que es enunciado, se obtiene al reemplazar en Exp(X,C_n) cada fórmula atómica $R(t_{i1},...,t_{ik})$ por la variable proposicional $P_{(i1,...ik)}$ en todas sus presencias.
Cabe aclarar aquí que para cada formula atómica $R(t_{i1},...,t_{ik})$ se usara una variable proposicional distinta y se considera la misma variable proposicional para las fórmulas atómicas que sean idénticas.

Ahora nuestra hipótesis se ha transformado en la siguiente: Para toda n, E_n no es tautología. En conformidad, dada n existe una asignación $\mathcal{A}_n : VP \Rightarrow \{0,1\}$, donde VP es el conjunto de variables proposicionales de la fórmula E_n, tal que $\mathcal{A}_n(E_n) = 0$.
Sea $q_1,q_2,...,q_h,...$ un ordenamiento de VP. Vamos a definir una asignación $\mathcal{A}$ con la propiedad de que $\mathcal{A}(E_n) = 0$ para toda $n \in \mathrm{N}$. $\mathcal{A}$ se define de manera recursiva como sigue:

1) $\mathcal{A}\ (q_1) = \begin{cases} 0 \text{ si } A_1 \text{ es finito} \\ 1 \text{ si } A_1 = \{n \in N \mid \mathcal{A}_n(q_1) = 1\} \text{ es infinito} \end{cases}$

2) $\mathcal{A}\ (q_{h+1}) = \begin{cases} 0 \text{ si } A_{h+1} \text{ es finito} \\ 1 \text{ si } A_{h+1} = \{n \in N \mid \mathcal{A}_n(q_1) = \mathcal{A}(q_1),..., \mathcal{A}_n(q_h) = \mathcal{A}(q_h) \text{ y } \mathcal{A}_n(q_{h+1}) = 1\} \text{ es infinito} \end{cases}$

Consideremos una E_m arbitraria. Sea h el mayor índice de las variables proposicionales de E_m. Sabemos que para una infinidad de números N se cumple que $\mathcal{A}_n(q_1) = \mathcal{A}(q_1),...,\ \mathcal{A}_n(q_h) = \mathcal{A}(q_h)$, de modo que podemos escoger una $n \geq m$ con esta propiedad. Como $\mathcal{A}_n(E_n) = 0$ y E_m es subfórmula de E_n, por necesidad $\mathcal{A}_n(E_m) = 0$, pero $\mathcal{A}_n$ y $\mathcal{A}$ coinciden en las variables proposicionales de E_m debido a lo cual $\mathcal{A}\ (E_m) = 0$.

Definamos ahora una interpretación sobre el dominio de los números naturales. Sea f^k un símbolo funcional de Xcv y sean $t_{i1},...,t_{ik}$ términos de T' y supongamos que el término $f^k\ (t_{i1},...,t_{ik})$ es t_{ij}. Se define la función $A(f^k)$:$N^k \rightarrow N$ como $A(f^k)(i1,...,ik) = j$.

Sea R^k un símbolo relacional de Xcv. Se define la relación $A(R^k) \subseteq N^k$ como sigue: $(i1,...,ik) \in A(R^k)$ sí y sólo sí $\mathcal{A}\ (R_{i1,...,ik}) = 1$.

Para demostrar que X no es universalmente válida basta con demostrar que Xcv es falsa en A.
Recordemos que la validez universal de Xcv implica la validez universal de $\exists \bar{z}(Xcv)$.
Donde $\bar{z} = (z_1, z_2,..., z_m)$ es la sucesión de variables libres de Xcv. Por tanto, si $\exists \bar{z}(Xcv)$ es falsa en A, Xcv no es universalmente válida.

Ahora escribimos $\exists \bar{z}(Xcv)$ como $\exists \bar{z} \exists \bar{x} M(\bar{z}, \bar{x})$ con $M(\bar{z}, \bar{x})$ abierta y en su forma normal disyuntiva.

$A \vDash \exists \bar{z} \exists \bar{x} M(\bar{z}, \bar{x})$ sí y sólo sí existen $a_{11},...,a_{1m},a_{i1},...,a_{im}$ tales que, $A \vDash$ $M(\bar{z}, \bar{x})(a_{11},...,a_{1m},a_{i1},...,a_{im})$ y esto último sucede sí y sólo sí $A \vDash M_j(\bar{z}, \bar{x})\ (a_{11},...,a_{1m},a_{i1},...,a_{im})$ para algún disyunto M_j de M.

Si consideramos los números $a_{11},...,a_{im}$ y efectuamos las operaciones pertinentes con ellos, veremos que ciertas eneadas de números están o no en ciertas relaciones.
Por ejemplo, si R^k aparece sin negación en Mj, entonces se tendrá $(i_1,...,i_k) \in A(R^k)$.

En tal caso, tendremos que $\mathcal{A}\ (R^k_{i1,...,ik}) = 1$, respecto a la asignación $\mathcal{A}$. Procediendo de esta manera con las fórmulas atómicas tendremos una conjunción de variables o de negaciones de variables de *VP* que es verdadera bajo $\mathcal{A}$. Este conjunto es un disyunto de E_m para alguna m, lo cual contradice la hipótesis de que $\mathcal{A}\ (E_m) = 0$. ▣

Con esto concluimos la demostración de la proposición 1.2.3 y también de 1.2.2 que como mencionamos se sigue de la proposición recién demostrada.

Demostración de la proposición 1.2.1.

Demostremos ahora que, en general, Exp(X,C_n) $\vdash_{\mathrm{cp}}$ Xcv. Si en particular $\vdash_{\mathrm{cp}}$ Exp(X,C_n) para alguna n, entonces $\vdash_{\mathrm{cp}}$ Xcv. Sea $C_n = (t_1,t_2,...,t_k)$ y $M\,(x_1,x_2,...,x_n)$ la matriz de Xcv. Haremos la demostración de manera sintáctica indicando a la izquierda el número de cada paso y a la derecha la razón por la que es válido.

1.- $\bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} M(t_{i1},t_{i2},...,t_{ik}) \vee ... \vee \bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} M(t_{k1},t_{i2},...,t_{in})$ Hipótesis.

2.- $\exists x_1 \bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} M(x_{i1},t_{i2},...,t_{ik}) \vee ... \vee \bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} M(t_{k1},t_{i2},...,t_{in})$ De 1 por la regla $\dfrac{Y\left(x_1/t_1\right)}{\exists x_1 Y(x_1)}$.

3.- $\bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} (\exists x_1) M(x_{i1},t_{i2},...,t_{ik}) \vee ... \vee \bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} M(t_{k1},t_{i2},...,t_{in})$ De 2 por la regla

$\dfrac{\exists x_i (Y(x_i) \vee Z)}{(\exists x_i Y(x_i)) \vee Z}$.

Aplicando repetidas veces lo hecho en 2 y 3 para los disyuntos sucesivos tenemos lo siguiente:

2k+1.- $\bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} (\exists x_1) M(x_{i1},t_{i2},...,t_{ik}) \vee ... \vee \bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} (\exists x_1) M(x_{i1},t_{i2},...,t_{ik})$.

2k+2.- $\bigvee_{\substack{i2\,\le\,k \\ \vdots \\ in\,\le\,k}} (\exists x_1) M(x_{i1},t_{i2},...,t_{ik})$ De 2k+1 por la regla $\dfrac{Y \vee Y}{Y}$ aplicada reiterada veces.

$\vdots$

n(2k+1)+1.- $\exists x_n \exists x_{n-1} ... \exists x_1 \, M(x_1, x_2, ... x_n)$ Repitiendo lo hecho de 2 a (2k+2), (n-1) veces.

$n(2k+1)+2$.- $\exists x_1 \exists x_2 ... \exists x_n\, M(x_1, x_2, ... x_n)$ Permutando cuantificadores con la regla $\dfrac{\exists x_i \exists x_j Y}{\exists x_j \exists x_i Y}$

y la fórmula deducida es Xcv. ▣

Para pasar de Exp(X,C_n) a Xcv se puede aplicar una sola regla de inferencia que, como acabamos de ver, preserva la propiedad de ser una fórmula universalmente válida. La regla, que llamaremos *Regla de cuantificación existencial* es la siguiente:

Si $X(t_{11},...,t_{im}),..., X(t_{p1},...,t_{pm})$ son instancias de sustitución de $X(x_1,...,x_m)$ con $(t_{11},...,t_{im})$ términos libres para x_i en X, entonces, de $X_1 \vee X_2 \vee,...,\vee X_p$ se infiere $\exists x_1 \exists x_2,..., \exists x_p X$.

En símbolos: $\dfrac{X_1 \vee X_2 \vee ... \vee X_n}{\exists x_1 \exists x_2 ... \exists x_n X}$

Otra regla de inferencia que también preserva la validez universal de las fórmulas, misma que llamaremos *Regla de Herbrand*, es la siguiente:

Si Xcv es una fórmula cerrada de validez para X, entonces de Xcv se infiere X.

En símbolos: $\dfrac{Xcv}{X}$

Hemos probado el teorema de Herbrand mediante las proposiciones 1.2.1 y 1.2.2. En éstas figuran nociones semánticas y sintácticas. Al respecto cabe aclarar ciertas cuestiones que tomaron lugar en la demostración del teorema de Herbrand.
En primer lugar, para Herbrand el uso de nociones semánticas era inadmisible en la metamatemática. De hecho, Herbrand adopta un punto de vista constructivista tal como el propuesto por Hilbert en su programa (mas adelante en este trabajo habremos de retomar este punto).

La segunda cuestión es que la postura de Herbrand le impidió ver las implicaciones semánticas de su teorema, mismas que incluyen el teorema de completud de Gödel para el cálculo de predicados. De estas cuestiones nos ocuparemos en la siguiente sección.

1.4 Algunas implicaciones del Teorema de Herbrand

Como hemos demostrado, de $\vdash$ Xcv se sigue que para alguna n, Exp(X,C_n) es instancia de tautología. Recíprocamente, si Exp(X,C_n) es una instancia de tautología, entonces $\vdash_{\text{cp}}$ Exp(X,C_n) y en la prueba de ésta fórmula sólo se utilizan los axiomas y reglas de inferencia del cálculo proposicional (*CP*). Combinando estos resultados con la proposición 1.2.1 obtenemos lo siguiente:

1)Si $\vDash X$, entonces $\vdash_{cp} X$.
2)Si $\vdash_{cp} X$, entonces $\vDash X$. Esto último en virtud de que el cálculo de predicados es correcto.

Si combinamos los incisos anteriores tenemos el teorema de completud de Gödel (1930) para el cálculo de predicados: Para toda $X \in Lcp$, $\vDash X$ sí y sólo sí $\vdash X$.

Herbrand no dedujo esta equivalencia de su teorema de (1930), debido a que, como ya lo hemos mencionando, rechazaba los métodos semánticos, por lo que sólo pudo concluir lo siguiente:

$\vdash_{cp} X$ sí y sólo sí existe una $n \in \mathrm{N}$ tal que $\mathrm{Exp}(X,S_n)$ es instancia de tautología.

Lo anterior proporciona un criterio alternativo para la noción de *ser un teorema del cálculo de predicados* (*CP*), pero no establece nexo alguno entre la noción semántica de *validez* y la noción sintáctica de “ser derivable en el cálculo de predicados”.

Por otra parte, el teorema de Herbrand puede presentarse en una versión semántica como sigue:

Para toda $X \in Lcp$, $\vDash X$ si y solo si existe $n \in \mathrm{N}$ tal que $\mathrm{Exp}(X,C_n)$ es instancia de tautología.

De hecho la versión semántica del teorema de Herbrand implica al teorema de Gödel de 1930. Es más, se puede obtener un cálculo de predicados completo para las fórmulas universalmente válidas de la siguiente manera:

Sistema del cálculo de predicados con reglas de Herbrand (CP_H)

Axiomas: Si Y es una fórmula abierta, las fórmulas $Y_1,Y_2,...,Y_n$ son instancias de sustitución de Y y $Y_1 \vee Y_2 \vee ... \vee Y_n$ es instancia de tautología, entonces $Y_1 \vee Y_2 \vee ... \vee Y_n$ es un axioma.

Reglas de inferencia: Regla de cuantificación existencial y regla de Herbrand.

Con respecto a las deficiencias en la demostración de Herbrand sobre su teorema, en 1943 Gödel llegó a la conclusión de que hay una laguna en el argumento. En [Dreben 1963] Dreben, Andrews y Aanderaa publicaron contraejemplos que refutan algunos lemas sobre los que descansa la demostración de Herbrand. Desde entonces la demostración ha sido modificada. Asimismo, cabe aclarar que el teorema se ha extendido más allá de la versión puramente constructivista de Herbrand y se le ha dado distintas pruebas y connotaciones de tipo semántico, como la recién expuesta.

1.5 Funciones Analizadoras

Aclaremos cuál fue el error de Herbrand en su demostración; con lo siguiente, dado el orden de una fórmula X, Herbrand pensó que las reglas de prenexación, (como las expuestas en la sección 0.4), preservan el orden de una fórmula, e intentó demostrarlo. Lo que en realidad sucede es que en ocasiones la aplicación de las reglas de prenexación aumenta el orden de la fórmula.

En su trabajo, Herbrand demostró que para cada axioma *A* existe un número *r* tal que Exp(X,C_r) es válida; luego habría de establecer, para cada regla de inferencia, que la conclusión de la regla es de orden *s* para algún número *s*, bajo la suposición de que las premisas de la regla son de ciertos ordenes dados.

Por ejemplo, para el modus ponens supuso que si la fórmula *X* es de orden *p*, y la fórmula $X \rightarrow Y$ es de orden *q*, entonces el máximo entre *p* y *q* es una cota superior del orden de la conclusión *Y*.
Ahora, si *j* es el número de cuantificadores de *X* y *k* el número de cuantificadores de *Y*, Dreben y Aanderaa establecen, con ciertos contraejemplos, que el orden de *H* no se puede acotar con una función de *p* y *q*, ni con una función de *k*, *p* y *q*, o con una función de *j*, *p* y *q*. No obstante, demuestran que hay una función recursiva primitiva de los cuatro argumentos *j*, *k*, *p* y *q* que da una cota superior. La llamaron *función analizadora* de la regla de modus ponens. Para las demás reglas de inferencia hay por lo menos una función analizadora que es recursiva primitiva. Por lo cual dada una prueba de la fórmula *X*, podemos determinar, siguiendo la demostración, un número *p* tal que la Exp(X,C_p) es válida y la determinación de *p* es recursiva primitiva. Si empezamos con la fórmula *X*, sin usar ninguna prueba de *X*, podemos encontrar, construyendo expansiones sucesivas, un número *q* tal que Exp(X,C_q) es válida; pero la determinación de *q* desde *X* es recursiva, no recursiva primitiva.

Como hemos dicho, las funciones analizadoras dependen de las reglas de inferencia consideradas. Su papel es acotar superiormente los dominios C_n en donde se intentara hacer validas las expansiones de Herbrand de la fórmula.

En el sistema de Dreben y Denton, hay 5 reglas de inferencia y 2 axiomas. Lo primero que haremos es ver cuáles de estas reglas y axiomas coinciden con las reglas y axiomas que hemos utilizado. Como veremos, las demás reglas y axiomas corresponden a tautologías. En segundo lugar veremos que la regla de modus ponens es un caso especial de la regla de corte. En vista de que ambos lenguajes tienen el mismo poder expresivo, en lo que sigue utilizaremos el lenguaje de Dreben y Denton para seguir las ideas de estos autores en la demostración de la consistencia de la aritmética.

Las reglas de inferencia propuestas por Dreben y Denton son las siguientes:
1.- Regla de expansión: de *X* se sigue $X \vee Y$.
2.- Regla de contracción: de $X \vee X$ se sigue *X*.
3.- Regla asociativa para el conectivo $\vee$: de $(X \vee Y) \vee Z$ se sigue $X \vee (Y \vee Z)$.
4.- Regla de introducción existencial: de $Z \rightarrow Y$ se infiere $\exists xZ \rightarrow Y$, donde *x* es una variable que no figura libre en *Y*.
5.- Regla de corte: de $X \vee Y$ y $\neg X \vee Z$ se sigue $Y \vee Z$

Los axiomas son los siguientes:
1) $X \vee \neg X$

2) $Y[a] \rightarrow \exists xY$, en donde a es una constante que sustituye en Y(x) todas las presencias de la variable x.

La regla 1 es equivalente al axioma 1 de nuestro sistema y las reglas 2 a 4 son tautologías.

Consideraremos para la siguiente prueba la forma de árbol usada por Gentzen, en la que haremos ver que la regla de corte y las demás reglas de inferencia del sistema de Dreben y Denton hacen del modus ponens una regla de inferencia derivada. Veamos la prueba de esta regla.

$X \rightarrow Y$ hipótesis — X hipótesis

| quitando la abreviatura — | por expansión

$\neg X \vee Y$ — $X \vee Y$

＼ por conjunción ／

$(\neg X \vee Y) \wedge (X \vee Y)$

| por regla de corte

$Y \vee Y$

| por contracción

Y

Con lo cual vemos que modus ponens es un caso especial de la regla de corte donde la fórmula Z es la misma que Y.

Ahora veamos cómo son las funciones analizadoras de estas reglas. Como veremos las funciones no son la misma en todos los casos y dependen de cada regla.

Para la regla de corte la función analizadora va como sigue. Si i es el número de cuantificadores de la fórmula X, j el numero de cuantificadores de la fórmula Y y k el numero de cuantificadores de la fórmula Z, y si las fórmulas $X \vee Y$ y $\neg X \vee Z$ tienen órdenes p y q respectivamente, (es decir, si dichas fórmulas se pudieron hacer validas en dominios C_p y C_q, respectivamente), entonces hay una función recursiva primitiva $f(i, j, k, p, q) = n$, con $i, j, k, p, q \geq 1$ tal que $f(i, j, k, p, q)$ da una cota superior para el orden que la fórmula $Y \vee Z$ tiene una expansión de validez que es tautología.
Para las demás reglas de inferencia la función identidad es suficiente, es decir, si X tiene una expansión de validez de orden p y la formula Y se sigue de X al aplicar una sola vez alguna de las reglas de inferencia (contracción, expansión, asociatividad de la conjunción, o introducción existencial), entonces la fórmula Y también tiene una expansión de validez de orden p.

Finalmente si $j \geq 1$ y para cada término t del conjunto C_h, donde $h \geq 0$ y h es la altura máxima del término y si la fórmula X contiene j cuantificadores, entonces la fórmula $X \vee \neg X$ tiene una expansión de validez de orden j y la fórmula $Y[a] \rightarrow \exists xY$ tiene una expansión de validez sobre un dominio de orden $j+h$. [1]

---

[1] Para un estudio mas amplio sobre funciones analizadoras ver Dreben y Denton en False Lemas in Herbrand, Bulletin of the American Mathematical Society 69 pp. 699-706 y también Herbrand's Analysing Functions, sic, 70 pp. 697-698.

Para aclarar el punto anterior veamos el siguiente ejemplo.

Consideramos a *X y* $X \to Y$ como las siguientes fórmulas $\exists x \forall y(R(x,y))$ y
$\exists x \forall y(R(x,y)) \to \forall y \exists x(R(x,y))$

La primera fórmula veamos de que orden es $\exists x(R(x, f(x)))$ tenemos así que su primera expansión es $(R(c, f(c)))$ su segunda expansión será $R(c, f(c)) \vee R(f(c), f(f(c)))$.

Consideremos ahora la segunda fórmula y hagamos los pasos para verificar su orden

$\exists x \forall y(R(x,y)) \to \forall y \exists x(R(x,y))$

$\exists x \forall y(R(x,y)) \to \forall z \exists w(R(w,z))$

$\forall x \exists y \forall z \exists w(R(x,y) \to R(w,z))$

$\exists y \exists w(R(x,y) \to R(w, f(y)))$

$\neg R(x,x) \vee R(x, f(x))$

$\neg R(x,x) \vee R(x, f(x)) \vee \neg R(x, f(x)) \vee R(x, f(f(x)))$

Como podemos ver en esta última fórmula hay una tautología que encontramos en la disyunción de los términos 2 y 3 esta tautología hace que toda la disyunción sea tautología, pues de la disyunción de algo verdadero con lo que sea siempre se obtiene algo verdadero. Como se puede ver cada uno de estos términos proviene de distintas partes de la fórmula es decir una del antecedente y otra del consecuente por lo cual no se puede decir que la formula Y tenga el mismo orden que la fórmula $X \to Y$ pues ni la fórmula X ni la Y hacen por su aportación que aparezca la tautología, más bien esta aparece por la disyunción entre de las fórmulas.

Buscando en la literatura más información sobre las funciones analizadoras no pudimos encontrar una construcción de la función analizadora de la regla de corte o de modus ponens, sino solo referencias de que debe ser una función recursiva y no recursiva primitiva.
Mi asesor y yo trabajamos sobre este tema con la información obtenida y creemos que la conclusión de que debe haber una función analizadora que sea recursiva, tiene que ver con la idea de minimalización, es decir, la función *f(i, j, k, p, q)* debe de estar dada por una función que sea calculable solo si hay ciertos parámetros que se pueden minimalizar.
La existencia de esta función analizadora de la regla de corte (o de modus ponens) debe tener un argumento indirecto es decir vía la reducción al absurdo, pero tampoco encontramos textos que nos dijeran, mas información sobre como probaron su existencia.

1.6 Problema de la Decisión

El problema de la decisión y la búsqueda de una solución para éste es uno de los motivos de Herbrand para hacer el estudio que lo lleva a su teorema.

El teorema de Herbrand nos ofrece una caracterización alternativa de las fórmulas válidas. Otra caracterización diferente es la que corresponde al teorema de completud de Gödel de 1930. En ambos casos no se logra una respuesta para el problema de la decisión del conjunto de fórmulas válidas. Históricamente, este problema tomó importancia a partir del constructivismo, el cual intento resolver la validez de fórmulas con métodos sintácticos, es decir, sin tener que recurrir a sus interpretaciones. En este sentido los teoremas recién señalados no resuelven más que parcialmente el problema.

Veamos cómo es que el teorema de Herbrand trata este problema. En su versión sintáctica, dicho teorema proporciona un método parcial para decidir la validez de las fórmulas, pero no un procedimiento efectivo de decisión para todas las fórmulas de *Lcp*. De hecho, si una fórmula *X* no es válida, dicho criterio nunca lleva a una decisión respecto de su validez, pues el examen de un número finito de expansiones de Herbrand no es suficiente para negar la validez de la fórmula. Lo único que garantiza es la enumeración recursiva de las fórmulas válidas. Cabe señalar que tal enumerabilidad recursiva también es consecuencia del teorema de Gödel de 1930, y se puede desarrollar mediante su técnica de aritmetización.

Solucionar el problema de la validez sólo con métodos sintácticos fue uno de los principales propósitos de la investigación de Herbrand.

El teorema de Herbrand permite reducir el problema de la validez de una fórmula, al de construir una tautología en la lógica proposicional. En este sentido, el uso de las funciones analizadoras no permite determinar una cota para tal búsqueda. De hecho, es posible que tal cota esté más allá de ω_0 (omega cero), en cuyo caso para decidir la validez de la fórmula no tendremos un límite para el espacio de búsqueda, por lo cual la solución a la que llega Herbrand no tiene la magnitud que deseaba darle.

Capítulo 2
Demostración tipo Herbrand de la consistencia de la aritmética

En este capítulo veremos cómo probar la consistencia de la aritmética con base en las nociones que Herbrand utiliza en su teorema. Veremos primero dos variantes de las nociones presentadas en su teorema, comenzando con la introducción de la forma cerrada de satisfacción de una fórmula. Veremos también que la noción de orden permite eliminar la hipótesis de que la fórmula está prenexada. Seguiremos con la introducción del concepto de “altura” de una fórmula, noción de importancia al probar la consistencia de la aritmética. Continuamos con un análisis de los conceptos más importantes presentes en la prueba de consistencia siguiendo las ideas de Herbrand. Estos se relacionan, sobre todo, con la semántica que el mismo Herbrand rechazaba, pero que después tomo importancia en el estudio de la lógica matemática. Es importante aclarar que ninguna prueba de este tipo fue hecha por Herbrand, más bien, es una técnica desarrollada por otros matemáticos que decidieron darle un seguimiento a las ideas por él propuestas. El acercamiento que Herbrand hace a la consistencia de la aritmética se entiende mejor cuando se le ve como una reformulación de las ideas de Hilbert y de su método de evaluación.

2.1 Variantes a las nociones usadas en el Teorema de Herbrand

La primera variante que veremos es la de forma cerrada de satisfacción para poder usarla en la expansión de una fórmula. Esta fórmula surge de la forma cerrada de validez considerada en el capítulo anterior al hacer la expansión de Herbrand.

En la forma funcional de Herbrand de una fórmula hemos considerado aquellas que provienen de un enunciado prenexado. En tal caso, quitábamos los cuantificadores universales y sustituyéndolos por formas funcionales de Herbrand, para después, al hacer la expansión de Herbrand, quitar los cuantificadores existenciales de la fórmula dejando así una fórmula libre de cuantificadores.
Por último, mediante una cadena de sustituciones buscábamos una tautología, constituida por una disyunción de instancias de sustitución de una matriz. A esta matriz le llamamos expansión de la forma cerrada de validez y la denotamos con $Exp(Xcv,C_n)$.

Para hacer la *expansión de la forma cerrada de satisfacción* haremos ahora una matriz de conjunciones, como a continuación se indica.
Supongamos que la fórmula *X* es un enunciado rectificado prenex. *X* se transforma en su forma cerrada de satisfacción haciendo lo siguiente:

Llamemos a los cuantificadores que están dentro del alcance de un cuantificador universal, *universalmente ligados*. Quitemos de la fórmula estos cuantificadores sustituyendo en lugar de las variables acotadas por cuantificadores universalmente ligados términos funcionales de Herbrand de la aridad correspondiente, en la misma forma en que se hace para la forma cerrada de validez.
Denotaremos a la forma cerrada de satisfacción indistintamente como Xcs o como $\overline{\mathrm{X}}^{S_i}$.

EJEMPLOS:
Retomemos los ejemplos del capítulo anterior.

Consideremos la fórmula $\forall y_1 \exists x_1 \forall y_2 \exists x_2 \forall y_3 (R_1^2(y_1, x_1) \wedge R_2^2(x_1, y_2) \wedge R_3^3(y_1, x_2, y_3))$; en ésta, las variables x_1 y x_2 son universalmente ligadas.
Ahora $e_1 = 1$ y $e_2 = 2$. Tomemos dos símbolos funcionales de Herbrand f_1 de aridad 1 y f_2 de aridad 2.
Xcs es la fórmula $\forall y_1 \forall y_2 \forall y_3 (R_1^2(y_1, f(y_1)) \wedge R_2^2(f(y_1), y_2) \wedge R_3^3(y_1, f(y_1, y_2), y_3))$, mientras que la forma cerrada de validez (Xcv) es $\exists x_1 \exists x_2 (R_1^2(y_1, x_1) \wedge R_2^2(x_1, f_2(x_1)) \wedge R_3^3(y_1, x_2, f_3(x_1, x_2)))$.

Tomemos como segundo caso la fórmula: $\exists x \forall y_1 \forall y_2 R(x, g(y_1, y_2))$; en ella, ninguna variable es universalmente ligada. En este caso dejaremos la variable *x* tal como está y quitaremos el cuantificador existencial, obteniendo así la fórmula Xcs $\forall y_1 \forall y_2 R(x, g(y_1, y_2))$, mientras que Xcv es $\exists x R(x, g(f_1(x), f_2(x)))$. Cabe señalar que *g* no es término funcional de Herbrand en ninguna de las dos fórmulas Xcv y Xcs. En Xcs pueden figurar libres, aquellas variables que sean universalmente libres en *X*. (como en nuestro caso lo fue la variable *x*.)

Ahora de la definición (1.2.1) del capítulo anterior para la expansión de Herbrand tenemos lo siguiente:
Si *X* es una fórmula de la forma $\forall x Y(x)$, $\overline{\mathrm{X}}^{S_i}$ es $\bigwedge_{k \leq n} \overline{Y(x/t_k)}^{S_i}$ lo cual cumple Xcs, de modo que la expansión de la forma cerrada de satisfacción es una matriz de conjunciones, en la cual se pueden sustituir conjuntos C_n de términos del lenguaje. Estos conjuntos están definidos de igual modo que para la expansión de validez. Ahora, a través de una cadena sucesiva de substituciones, lo que buscaremos es satisfacer la fórmula en una interpretación, en este caso la aritmética, o hallar una instancia de tautología.

Veamos la relación existente entre las fórmulas en sus formas Xcs y $\neg((\neg X)cv)$.

Proposición 2.1.1
Si negamos la fórmula X, obtenemos la forma cerrada de validez de la negación y después volvemos a negar la fórmula, el resultado será una fórmula que es equivalente a la forma cerrada de satisfacción, aunque cabe aclarar que no tiene por qué ser la misma fórmula. En símbolos: $Xcs \equiv \neg((\neg X)cv)$

La demostración de esta proposición es como sigue:

Por construcción, Xcv es una fórmula en la que solo aparecen cuantificadores existenciales o no tiene y denotaremos con P(X) a la forma prenexada de la fórmula X , con lo cual tenemos lo siguiente:

$P(X) \equiv X$ y $\neg P(X) \equiv \neg X$ como $\neg X \equiv P(\neg X)$ resulta que $\neg P(X) \equiv P(\neg X)$.

De lo anterior se sigue que $P(\neg X) \equiv \neg X$ y $\neg P(\neg X) \equiv \neg\neg X$ y como $\neg\neg X \equiv X$ y $X \equiv P(X)$, tenemos que $\neg P(\neg X) \equiv P(X)$.

Así, para obtener Xcv no es necesario construir la forma prenexada de $\neg X$, sino obtener $P(\neg P(X))$ a partir de $\neg P(X)$, y luego construir $(\neg X)$cv, negar la fórmula obtenida y finalmente prenexar, lo cual equivale a introducir la negación para así obtener Xcs.

Denotaremos como Exp(Xcs, C_n) a la expansión de Herbrand de la forma cerrada de satisfacción de una fórmula sobre un conjunto C_n de términos del lenguaje. Llamaremos *expansión de satisfacción* a la expansión de Herbrand de la forma cerrada de satisfacción y a la expansión de Herbrand de la forma cerrada de validez la llamaremos *expansión de validez*.

La segunda variante que veremos se debe a las ideas introducidas por Dreben y Denton. Estos autores se dieron cuenta que no es necesario que la fórmula sea un enunciado rectificado prenex; para nuestros fines basta con que sea un enunciado, es decir, una fórmula sin variables libres.
Además, como ya lo hemos mencionado, algunas de las reglas dadas para prenexar fórmulas aumentan el orden de ésta, siguiendo a Dreben y Denton evitaremos este cambio de orden en la fórmula.

Lo que no podemos evitar son las nociones de cuantificador universaloide y existencialoide, necesarias en virtud de que, como mencionamos en el capítulo anterior, al hacer algunos pasos de la prenexación de una fórmula el orden de ésta se altera de una manera impredecible.

Para poder considerar fórmulas que son enunciados cualesquiera haremos lo siguiente:

Los cuantificadores que están dentro de la fórmula los consideramos existencialoides o universaloides según el número de símbolos de negación que les den alcance a éstos.

Definición 2.1.1: Si a un cuantificador existencial le dan alcance un número par de negaciones (que puede ser cero), lo consideramos un cuantificador existencialoide, mientras que si lo preceden un número impar de negaciones lo consideramos un cuantificador universaloide.
Si a un cuantificador universal le dan alcance un número par de negaciones (que puede ser cero), lo consideramos un cuantificador universaloide, mientras que si lo preceden un número impar de negaciones lo consideramos un cuantificador existencialoide.

Cabe hacer la siguiente aclaración. Sí un cuantificador universaloide (existencialoide) es aquél que al pasar la fórmula a su forma prenex se transforma en un cuantificador universal (existencial), en la práctica, no es necesario llevar a cabo el proceso de prenexación, sino sólo tratar a cada cuantificador como si se hubiera hecho el proceso.
Es claro que en una fórmula prenexada los cuantificadores universales son universaloides y los existenciales existencialoides.

Se puede ahora hacer el proceso de encontrar las formas cerradas de validez y satisfacción de una fórmula sin tener que recurrir a la prenexación de fórmulas. Para encontrar Xcv y Xcs haremos los mismos pasos que consideramos para cada una de estas formas de la fórmula, pero sólo debemos considerar a los cuantificadores según sean universaloides o existencialoides.

EJEMPLOS:
Veamos ahora como es que se hacen las expansiones Xcv y Xcs de un enunciado *X*.

Tomemos la fórmula $\forall x \exists y(\neg R(x,x) \vee R(x,y))$. Xcv es $\exists y(\neg R(x,x) \vee R(x,y))$.
Sea $C_0 = \{x\}$; la expansión de Herbrand, Exp(Xcv,C_0), será:

$$\overline{\exists y(\neg R(x,x) \vee R(x,y))}^{C_0} \equiv \overline{\vee (\neg R(x,x) \vee R(x,y))\left(y/x \right)}^{C_0} \equiv \neg R(x,x) \vee R(x,x)$$

Se puede ver que Exp(Xcv,C_0) es una instancia de sustitución de la fórmula $P \vee \neg P$, la cual es una tautología.

Xcs es, $\forall x(\neg R(x,x) \vee R(x, f(x)))$. Tomemos una constante arbitraria c_1 pues en la formula no aparece ninguna variable libre. Sea $C_0 = \{c_1\}$, la expansión de Herbrand de Exp(Xcs, C_0) es:

$$\overline{\forall x(\neg R(x,x) \vee R(x, f(x)))}^{C_0} \equiv \overline{\wedge (\neg R(x,x) \vee R(x, f(x)))\left(x/c_1 \right)}^{C_0} \equiv \neg R(c_1,c_1) \vee R(c_1, f(c_1)).$$

Ahora debemos verificar si esta fórmula es satisfacible en algún dominio. Sean $D = \{0\}$ y $f(0) = 0$. Al sustituir, la fórmula se transforma en $\neg R(0,0) \vee R(0, f(0)) \equiv \neg R(0,0) \vee R(0,0)$, con lo cual se verifica su satisfacción en esta interpretación.

Consideremos ahora un caso en que la fórmula no está prenexada. Tomemos $\forall x(\forall y P(x,y) \rightarrow \forall w P(x,w))$ un enunciado sin prenexar. Bajo las reglas dadas en el capítulo 0, al prenexar lo que resulta es la fórmula $\forall x \exists y \forall w(P(x,y) \rightarrow P(x,w))$. Consideremos la fórmula inicial, quitando la abreviatura "→"; $\forall x(\neg \forall y P(x,y)) \vee \forall w P(x,w))$.

En este caso, los dos cuantificadores $\forall x$ y $\forall w$ son universaloides y $\forall y$ es existencialoide.
La forma cerrada de validez Xcv es $(\neg \forall y P(x,y) \vee P(x,w)$, mientras que la forma cerrada de satisfacción Xcs es $\forall x(\neg P(x, f(x)) \vee \forall w P(x,w)$, que también podemos escribir como $\forall x \forall w(\neg P(x, f(x)) \vee (P(x,w))$ en este ejemplo la forma de Xcs es similar a su forma sin prenexar, por lo cual el uso de estas reglas no afectara su orden, pero en el caso de la forma de Xcv el no prenexar si afectara su orden; veamos.

Al hacer la expansión en Xcv de cada una de las formas, queda lo siguiente:
En el caso de Exp (Xcv,Cn) para Xcv prenexada, la fórmula coincide con el segundo ejemplo dado en el capitulo anterior, por lo cual tenemos, que $C_1 = \{x, f(x)\}$. En este caso t_1 es x y t_2 es f(x), de donde resulta que Exp(Xcv,C_1) es:

$$\overline{\exists y(P(x,y) \vee \neg P(x, f(y)))}^{S_1} \equiv \overline{\vee_{k \leq 2} (P(x,y) \vee \neg P(x, f(y)))\left(y/t_k \right)}^{S_1} \equiv (P(x,x) \vee \neg P(x, f(x))) \vee (P(x, f(x)) \vee \neg P(x, f(f(x))))$$

y esta última fórmula es instancia de tautología, a su vez obtenemos el orden de esta forma es uno pues en C_1 encontramos la tautología.

Ahora, en el caso de Exp (Xcv,C_0) para Xcv sin prenexar tenemos lo siguiente, $C_0 = \{x, w\}$ que son las variables libres de Xcv, tenemos:

$$\overline{\exists y(P(x,y)) \vee \neg P(x,w)}^{S_1} \equiv \overline{\vee_{k\leq 1} (P(x,y) \vee \neg P(x,w))\left(\frac{y}{t_k}\right)}^{S_1} \equiv (P(x,x) \vee \neg P(x,w)) \vee (P(x,w) \vee \neg P(x,w))$$

Verificamos entonces que el orden de la forma sin prenexar es cero pues en C_0, encontramos que la última fórmula obtenida es una tautología. Este ejemplo nos muestra como las reglas de prenexación aumentan el orden de las fórmulas.

Ahora, en el caso de Exp (Xcs,C_0) tenemos lo siguiente:
Como en Xcs no hay variables libres, $C_0 = \{ c_1, c_2 \}$. Estas constantes sustituirán a x y w respectivamente. Ahora Exp (Xcs,C_0) es:

$$\overline{\forall x \forall w(\neg P(x, f(x)) \vee (P(x,w))}^{C_0} \equiv \overline{\wedge (\neg P(x, f(x)) \vee (P(x,w))\left(\frac{x}{c_1}\right)\left(\frac{w}{c_2}\right)}^{C_0} \equiv$$

$\neg P(c_1, f(c_1)) \vee P(c_1, c_2))$. Si D = {0, 1} sea f(0) = 1 y f(1) = 0, entonces la fórmula es satisfacible, pues $\neg P(0, f(0)) \vee P(0,1))$ es una tautología.

Definición 2.1.2: Ahora definimos el concepto de *altura de una fórmula* para lo cual consideraremos los conjuntos de términos definidos como en el capítulo 0. La *altura del término conjunto* T_n se define como sigue:
a) La altura de una constante o una variable es cero.
b) La altura de un término $f(t_1,t_2,...,t_n)$ es 1+ el máximo de las alturas de los términos $t_1,t_2,...,t_n$.
c) La altura de una fórmula es el máximo de las alturas de los términos T_n que figuran en ella.

EJEMPLOS:
Tomemos como un primer ejemplo el término: $f_1(g_1(a_1,a_2), h_1(j_1(a_1,a_3)))$ donde a_1,a_2,a_3 son constantes y f_1, g_1, h_1 y j_1 son símbolos funcionales. Las alturas de las constantes a_1,a_2,a_3 son cero, las de los términos $g_1(a_1,a_2)$ y $j_1(a_1,a_3)$ son 1, la del término $h_1(j_1(a_1,a_3))$ es 2 y la de $f_1(g_1(a_1,a_2),h_1(j_1(a_1,a_3)))$ es 3, así que la altura de todo el término es 3.

Ahora consideremos el término siguiente: $f_2(g_2(a_1), h_2(a_2), j_2(a_2), k_2(a_3))$ donde de nuevo a_1, a_2, a_3 son constantes y su altura es cero, para cada uno de los términos $g_2(a_1)$, $h_2(a_2)$, $j_2(a_2)$, $k_2(a_3)$ la altura es 1 y para $f_2(g_2(a_1), h_2(a_2), j_2(a_2), k_2(a_3))$ la altura es 2 por lo cual la altura del término es 2.

Consideremos como un tercer ejemplo la fórmula que resulta de unir dentro de un símbolo de predicado los términos de los ejemplos anteriores, sea un predicado P entonces la altura sería: $P\,[f_1(g_1(a_1,a_2), h_1(j_1(a_1,a_3)))\,,\, f_2(g_2(a_1), h_2(a_2), j_2(a_2), k_2(a_3))$ sabemos que en el primer término la altura es 3 y el segundo 2, por lo cual la altura de la fórmula es 3, que es el máximo de las alturas de los términos.

Esta noción de altura de un término o de una fórmula es importante pues los conjuntos C_n que dan el orden de una fórmula son conjuntos de términos cuya altura crece con su índice; de hecho, se puede establecer una correspondencia entre el orden y la altura de una fórmula.

Proposición 2.1.2
Una fórmula tiene altura *n* sí y sólo sí el conjunto C_n que le da su orden es de altura *n*.

Esta proposición es obvia. Si construimos C_0 a partir de las variables libres y constantes que aparecen en la fórmula, después construimos C_1 tomando a los elementos de C_0 como entradas de funciones hasta de aridad igual al número de elementos en C_0, por definición en C_1 se ha complicado sólo en uno la altura, si seguimos el proceso para construir los C_n como se indico en el capítulo 1, entonces al llegar a C_n la altura se ha ido complicando de uno a otro C_i en solo una altura más que el anterior pues para C_{i+1} puedo usar los elementos de C_i como entradas en nuevas funciones. Teniendo que la altura de C_n es *n*.

2.2 Conceptos necesarios para la demostración de la consistencia

Antes de ver la prueba de consistencia debemos hacer algunos cambios respecto a los axiomas y las reglas de inferencia, pues seguiremos las ideas de Dreben y Denton. Estos no implican ningún cambio en el alcance de expresividad del lenguaje, como veremos a continuación.

Consideraremos como axiomas lógicos a todas las fórmulas con alguna de las formas siguientes:
1) $\neg P \vee P$.
2) $X\left({}^{y}\!/_{a} \right) \rightarrow \exists y X$.

Tomaremos como reglas de inferencia las siguientes:

1) *Regla de expansión*: de *X* se sigue $X \vee Y$.
2) *Regla de contracción*: de $X \vee X$ se sigue *X*.
3) *Regla de asociatividad de la disyunción*: de $(X \vee Y) \vee Z$ se sigue $X \vee (Y \vee Z)$.
4) *Regla de corte*: de $X \vee Y$ y $\neg X \vee Z$ se sigue $Y \vee Z$.
5) *Regla de introducción del existencial*: sí *x* es una variable que no figura libre en *Y* entonces $\exists x Z \rightarrow Y$ se infiere de $Z \rightarrow Y$.

Los teoremas son todas las fórmulas derivadas mediante una prueba en la que sólo se han utilizado como hipótesis axiomas (lógicos y propios) de la teoría, con base en las cinco reglas de inferencia anteriores. Un *teorema es lógico* si en su prueba no se utilizan axiomas propios. Una teoría *T* es consistente si no todas las fórmulas de su lenguaje son teoremas.

Veremos una variante del Teorema de Herbrand, llamada Teorema de Consistencia de Herbrand:

Teorema de la Consistencia de Herbrand

Una teoría T en la cual todos los axiomas propios son enunciados es consistente sí y sólo sí para toda conjunción finita de axiomas, la expansión de satisfacción es satisfacible con funciones de verdad.

Una reformulación del teorema es: Existe un método uniforme, dada una prueba formal dentro del lenguaje para la fórmula A, con el cual podemos encontrar una expansión de la forma cerrada de validez de tal modo que Exp(Acv,C_n) sea una tautología.

Sobre la demostración de este teorema cabe decir, que los autores de la misma la citan dentro un articulo llamado "The Herbrand theorem and the consistency of arithmetic" pero el articulo no pudo ser revisado para esta tesis pues aunque hicimos una búsqueda exhaustiva nos fue imposible encontrarlo.

Ahora consideremos el caso de una teoría en la cual los axiomas propios son enunciados de la forma $\forall x_1 \forall x_2 ... \forall x_n \exists y A_i$ donde A_i es una fórmula abierta, que contiene solo a las variables $x_1, x_2, \ldots, x_n$. y denotamos a este tipo de axiomas con A_n.
Las correspondientes formas funcionales de satisfacción son fórmulas del tipo $\forall x_1 \forall x_2 ... \forall x_n A_i(f_i(x_1, x_2, ..., x_n))$ denotamos a los axiomas de esta forma con Acs, y la expansión de satisfacción será una fórmula de la siguiente forma $A_i(a_1, ..., a_n, f_i(a_i, ..., a_n))$, las cuales denotamos en el caso de los axiomas, con Exp(Acs,C_n).

Según el teorema de Herbrand, la teoría será consistente sí y sólo sí cada una de las conjunciones finitas de las expansiones de satisfacción es satisfacible.

Desde un punto de vista no constructivista, decir que la conjunción de fórmulas es satisfacible con funciones de verdad es equivalente a decir que la teoría tiene un modelo, es decir, que hay una estructura donde todas las expansiones de satisfacción de la forma anterior son satisfacibles (donde sabemos que éstas son los axiomas propios de la teoría).

Dado que en el caso de la aritmética estas conjunciones son infinitas lo cual es inadmisible, como alternativa debemos construir paulatinamente el modelo en cada caso, es decir, agrupando los axiomas paso a paso. Lo cual es un camino con una visión constructivista.

En otras palabras, en el caso de la aritmética, no hay una forma de construir un modelo de la teoría, es decir, un modelo donde podamos determinar efectivamente todos los valores de verdad de las fórmulas de los axiomas. Sin embargo, lo que podemos hacer es aproximar este modelo para cualquier número finito de conjunciones, dando un método de construcción, es decir, un método uniforme para asignar valores de verdad de modo que las conjunciones sean fórmulas verdaderas.
En este método los valores de verdad ya obtenidos para las primeras fórmulas nos informan acerca de la teoría y de sus teoremas. Lo que quiere decir, con base en la construcción paulatina del modelo, obtenemos información acerca de la teoría que en otros casos no se tiene.

Pongamos un ejemplo para aclarar lo anterior.

Consideremos la fórmula $\forall z \exists w Y$, en la cual Y es una fórmula abierta derivable en una teoría cuyos axiomas no lógicos A_i son de la forma ya mencionada. Por el teorema de la deducción tenemos lo siguiente:

La fórmula $(A_1 \wedge A_2 \wedge ... \wedge A_n) \rightarrow \forall z \exists w Y$ es teorema de una teoría sin axiomas propios, es decir, es una fórmula válida.
En este caso la forma cerrada de satisfacción es de la forma $(A_1cs \wedge A_2cs \wedge ... \wedge A_ncs) \rightarrow \exists w Y(e)$.
Hacemos notar que en A_i un cuantificador es existencialoide sí y solo sí es universaloide en la fórmula $(A_1 \wedge A_2 \wedge ... \wedge A_n) \rightarrow \forall z \exists w Y$
En este caso la expansión de satisfacción de la fórmula es del tipo
$(\mathrm{Exp}\,(A_1cs, C_n) \wedge \mathrm{Exp}\,(A_2cs, C_n) \wedge ... \wedge \mathrm{Exp}\,(A_ncs, C_n)) \rightarrow \mathrm{Exp}\,(\exists w Y(e), C_n)$. Denotemos con *F(1)* esta fórmula.

Se puede ver que sí la expansión de satisfacción de la fórmula es una tautología, entonces tal expansión corresponde a una expansión satisfacible en una interpretación hecha con constantes y símbolos funcionales que figuran en su forma cerrada de satisfacción (dado que al menos una constante figura en su forma funcional). En este ejemplo, suponemos que el dominio C_n tiene como base términos hechos a partir de la constante *e* y los símbolos funcionales que aparecen en los axiomas A_i, junto con los símbolos funcionales de Herbrand f_i. Si tenemos un modelo M para las formas funcionales que figuran en *Acs* y le asignamos un valor cualquiera e_M del modelo al símbolo constante *e*, podemos entonces calcular los valores relativos al modelo de los términos del dominio C_n.

Ahora, como las expansiones de satisfacción de todos los axiomas $\mathrm{Exp}(A_i cs, C_n)$ se satisfacen en M y *F(1)* es una tautología, esto debe ser porque hay un elemento *a* en C_n tal que la fórmula $Y\left(z/e, w/a\right)$ es verdadera en M. Así, para cada elemento e_M que está en el universo de M podemos encontrar efectivamente un elemento a_M con el que $Y\left(z/e, w/a\right)$ se satisface en M, donde e_M y a_M son los elementos denotados por los símbolos *e* y *a*, respectivamente. Con el ejemplo se hace evidente que si Y es una fórmula abierta, entonces todas las fórmulas del tipo $\forall z \exists w Y$ son satisfacibles.

2.3 Demostración tipo Herbrand de la consistencia de la aritmética

Como es de esperarse, el acercamiento "a la Herbrand" a los problemas de consistencia, es mucho más fácil de aplicar cuando tenemos una idea de cómo debe ser el modelo de la teoría cuya consistencia se quiere probar. Un caso sencillo es aquel en que se busca probar la consistencia de la formalización de la aritmética sin inducción, en la cual no figuran símbolos funcionales de Herbrand en las expansiones de satisfacción de los axiomas. Aquí los elementos de la teoría serán los números naturales.

Para especificar una estructura adecuada M, sólo necesitamos asignar de la manera usual números, así como funciones calculables y relaciones decidibles, a los símbolos de relación y función que aparezcan en los axiomas.

Por ejemplo, para 0, *s*, +, *, = y < como símbolos primitivos de la aritmética, asignamos el número 0_M, la función sucesor s_M, la suma $+_M$, el producto $*_M$, la identidad $=_M$ y $<_M$ la relación "ser menor que” y consideramos axiomas propios de la aritmética las siguientes formulas divididas en dos grupos.

Grupo I
Las cerraduras universales de:

1) $x = y \to A_x \equiv A_y$ donde *A* es una fórmula atómica y A_y se obtiene al sustituir una presencia libre de *x* por una presencia libre de *y*.
2) $x = y \to t_x = t_y$ donde *t* es un término y t_y se obtiene al sustituir *y* por *x* de la manera en que se hace en el punto anterior.

Grupo II
Las cerraduras universales para las definiciones recursivas usuales de las operaciones de suma (+) y multiplicación ($\bullet$), además de los axiomas para la relación de orden (<)

$S1.\quad \forall x\, sx \neq 0$

$S2.\quad \forall x \forall y\ (sx \approx sy \to x \approx y)$

$O1.\quad \forall x \forall y\ (x < sy \leftrightarrow x \leq y)$

$O2.\quad \forall x \neg (x < 0)$

$O3.\quad \forall x \forall y\ (x < y \vee x \approx y \vee y \leq x)$

$A1.\quad \forall x\ (x + 0 \approx x)$

$A2.\quad \forall x \forall y\ (x + sy \approx s(x + y))$

$M1.\quad \forall x (x \bullet 0 \approx 0)$

$M2.\quad \forall x \forall y\ (x \bullet sy \approx (x \bullet y) + x)$

En los anteriores axiomas *S* denota a la función Sucesor, *A* a la suma y *M* a la multiplicación, así como *O* a la relación de orden, respectivamente.

Como se puede ver en los axiomas anteriores no aparecen cuantificadores existenciales por lo que claramente se puede construir un modelo M efectivo para los axiomas, y en particular, para las expansiones de satisfacción de cualesquiera conjunciones de los axiomas propios de la teoría, para los cuales el dominio C_n sólo consiste de términos formados con constantes y símbolos funcionales que figuran en las formas cerradas de satisfacción de los axiomas. Se sigue de la explicación al final de la sección 2.2, que sólo tales dominios se necesitan considerar y por el teorema de la consistencia de Herbrand se tiene que la aritmética sin inducción es consistente.

Ahora extendamos la teoría añadiendo el axioma de inducción.
Para ello consideremos el axioma de inducción como sigue: $\forall z((Y(0) \wedge \forall x(Y \to Ysx)) \to \forall xYx$ Donde *Y* es una fórmula abierta en la cual las únicas variables libres son *z* y *x*.

Una forma funcional cerrada de satisfacción para la cerradura de esta fórmula tiene la forma siguiente:
$\forall z((Y(0) \wedge (Y(fz) \to Y(sfz))) \to \forall Yx$, la cual denotamos con *AI*.

En *AI*, *f* es un símbolo funcional de Herbrand correspondiente al cuantificador existencialoide $\forall x$ que aparece en el antecedente del condicional.

En este caso reformulamos el teorema de la consistencia de Herbrand como sigue: Existe un método uniforme, dada una conjunción de *AI* con los demás axiomas de la aritmética (A_n) de manera tal que para la Exp((AI $\wedge$ A_n)cs, C_n), podemos encontrar una asignación de valores de verdad que la hace verdadera.

Con esta extensión de la teoría, iniciamos la prueba de consistencia de la aritmética vía el teorema enunciado en la sección 2.2. Probaremos la consistencia de este sistema como veremos a continuación.

Intuitivamente, queremos que el símbolo *f* corresponda a una función en la aritmética con la propiedad de que si para un número *k*, la fórmula $\forall x Y\left(k/z\right)$ es falsa y la fórmula $Y\left(k/z\; 0/x\right)$ es verdadera, entonces $Y\left(k/z\; fk/x\right)$ es verdadera y $Y\left(k/z\; sfk/x\right)$ es falsa. Por ejemplo, *fk* podría ser el menor número *n* tal que $Y\left(k/z\; sn/x\right)$ es falsa.
No obstante no hay una manera general de decidir dentro de la aritmética si efectivamente $\forall x Y\left(k/z\right)$ es falsa en la teoría de la aritmética, por lo cual, no podemos proceder de la manera en que lo hicimos con el sistema sin inducción.

Es en este punto donde usamos todo el poder que encierra el teorema de la consistencia de Herbrand, pues ahora para probar la consistencia del axioma de inducción con los demás axiomas de la teoría formal de la aritmética, es suficiente con probar que para cada dominio C_n existe una estructura M(C_n) en la cual la expansión de satisfacción Exp(*AI*, C_n), junto con las expansiones de los demás axiomas, son verdaderas. En la estructura M(C_n) no es necesario asegurar que la fórmula $Y[k, fk]$ es verdadera y que $Y[k, sfk]$ es falsa, a menos que para algún término *a* que aparezca en C_n la fórmula $Y[k, a]$ es falsa en M(C_n) y $Y[k, 0]$ es verdadera. En otras palabras, si *n* es el mínimo número para el cual se cumple que $Y[k, sn]$ es falsa, debemos probar que entonces *sn* es “un número demasiado grande” (es decir, no está en el C_n, considerado), y por lo tanto no habríamos de considerar a este número.

En el párrafo anterior, y en lo que sigue, facilitaremos la escritura de las fórmulas al omitir la nomenclatura de división para indicar sustituciones, y sólo pondremos la sustitución hecha.

Ahora, para cada domino C_n se puede obtener desde la estructura M una estructura efectiva M(C_n) que satisfaga las expansiones sobre C_n de todos los demás axiomas, con sólo asignarle alguna función calculable α al símbolo funcional *f*. Desde luego en los distintos dominios C_n se le puede asignar diferentes funciones α.

Después de la propuesta anterior el Teorema de consistencia de Herbrand se reduce a: Dada una instancia de *AI* podemos encontrar efectivamente un mapeo de modo que verifique Exp (*AI*, C_n). Dicho mapeo se determina relacionando una función calculable α dentro de la aritmética para el símbolo funcional de Herbrand f, que aparece en la forma cerrada de satisfacción del Axioma de Inducción al eliminar el cuantificador existencialoide.

Así, nuestra tarea consiste en hallar para cada domino C_n dado, una α tal que $M(C_n)$ también satisface a Exp(AI, C_n). De una manera más precisa, para cada C_n y cada función α, se busca un mapeo m que vaya de los términos de C_n a los números naturales con las funciones sucesor, suma, multiplicación, y la relación de orden, esto lo escribiremos $\langle \mathrm{N}, s, +, \bullet, < \rangle$ y debe cumplir las siguientes condiciones:

1) $m(0) = 0_M$
2) $m(Sa) = S_M m(a)$
3) $m(a+b) = m(a) +_M m(b)$
4) $m(a * b) = m(a) *_M m(b)$
5) $m(fa) = \alpha(m(a))$

Cada uno de estos mapeos (m_i) induce una estructura $M(C_n)$. Que a su vez proporciona un modelo correspondiente a Exp(AI, C_n) procedemos por aproximaciones sucesivas de la manera siguiente:

Empezamos por probar una función α_0 tal que $\alpha_M(k) = 0_A$ para todo número k. Asumiendo que α_i está definida para alguna i, definimos m_i de modo que cumpla las 5 condicionas pedidas para el mapeo, usando α_i en lugar de α. Sea M_i la estructura inducida por m_i.
Si la fórmula Exp(AI, C_n) es verdadera en M_i, entonces claramente tenemos el resultado deseado; en cambio, si esta fórmula es falsa en M_i, se debe a que para algún par de términos a y b pertenecientes a C_n, $Y[a, 0]$ y $Y[a, fa] \rightarrow [Ya, sfa]$ son verdaderas en M_i, pero $Y[a, b]$ es falsa en M_i.

Lo que tenemos ahora es que $m_i(b) \neq 0_M$, por lo que sí $m_i(b) = 0_M$, entonces $Y[a, 0]$ y $Y[a, b]$ deberían tener el mismo valor de verdad en M_i. Este problema se da por el hecho de que no hemos escogido $m_i(fa) = \alpha_i(m(a))$, de tal manera que $Y[a, fa]$ sea verdadera en M_i, y $Y[a, sfa]$ sea falsa en M_i. Remediar este problema es claro: si tenemos que $Y[m_i(a), 0_M]$ es verdadera (sobre el conjunto de los números naturales) y $Y[m_i(a), m_i(b)]$ es falsa, entonces podemos hallar un número $n < m_i(b)$ para el cual $Y[m_i(a), n]$ es verdadera, pero $Y[m_i(a), s_M n]$ es falsa. Para ello, definimos la función α_{i+1} como sigue:

Sea $\alpha_{i+1}(k) = \alpha_i(k)$ para todo número k, excepto $k = m_i(a)$, donde a es un término de la manera ya descrita. En este caso definimos $\alpha_{i+1}(k) = n$, donde n es el número recién descrito.
Definimos entonces m_{i+1} a través de las 5 condiciones propuestas para dar el mapeo, reemplazando α por α_{i+1}, y tenemos que M_{i+1} es la nueva estructura inducida por el mapeo m_{i+1}.

Claramente, tenemos que α_{i+1} es una mejor aproximación a la función deseada, en comparación con α_i; el problema ahora es mostrar que a través de repetir este proceso un número suficiente y finito de veces, debemos hallar una estructura en la cual Exp(AI, C_n) es verdadera.

Debemos notar que para toda i, todos los valores distintos de cero de la función α_i son *correctos*. En otras palabras: sí $\alpha_i(k) \neq 0_M$, entonces $Y[k, \alpha_i(k)]$ es verdadera y $Y[k, s_M\alpha_i(k)]$ es falsa.

La implicación más importante de esto es que podemos *medir el progreso* para llegar al objetivo deseado, con tan solo contar el número de términos a que pertenecen a C_n con la propiedad de que $m_i\ (fa) = 0_M$. Mientras menos de estos términos hallemos, más cerca estaremos de llegar al resultado deseado.

Al calcular la medida de este avance, una de las cosas que debemos hacer es dar prioridad a los términos de menor altura. La razón de esto es que al pasar de la función α_i a α_{i+1} es posible que cambie el valor de $m_i(fa)$. Por ejemplo, puede ser que la altura de a sea relativamente baja, y que este valor cambie haciendo que el valor de $m_i(fb)$ cambie también. Esto sucede cuando a figura en b, en cuyo caso no podemos predecir cómo cambia la altura de b.

No obstante, hay una manera apropiada para medir el progreso. Es la siguiente:
Sea $h(i, p)$ el número de términos a de C_n de altura p tal que $m_i(fa) = 0_M$, y sea i el subíndice de la sucesión $(h(i, 0),..., h(i, p_0))$ en la cual p_0 es la altura de C_n. Para ello, introducimos la siguiente relación:

Sea *subíndice* $(i_1) \prec$ *subíndice* (i_2) sí y sólo sí para alguna $p(0 \leq p \leq p_0)$, tenemos así que $h(i_1,0) = h(i_2,0) = ... = h(i_1, p\text{-}1) = h(i_2, p\text{-}1)$ y también $h(i_1, p) < h(i_2, p)$.

Es fácil mostrar que si $\mathrm{Exp}(AI, C_n)$ es falsa en M_i, entonces se cumple que:
El subíndice $(i+1) \prec$ *subíndice* (i). Esto se debe a que la relación $\prec$ está definida con una función de ordenamiento lineal, y los números $h(i, p)$ están acotados por q, en donde q es el número de términos en C_n.

Se sigue que para alguna $i \leq (1+q)^{p0}$, la fórmula $\mathrm{Exp}(AI, C_n)$ es verdadera en M_i al igual que las expansiones de los demás axiomas de la aritmética. Por tanto para cada dominio C_n existe una estructura $M(C_n)$ para la cual las expansiones de satisfacción de todos los axiomas propios de la teoría son verdaderos.

Con esto hemos concluido la prueba del teorema de consistencia tipo Herbrand y con ello que la teoría aritmética formalizada incluyendo el axioma de inducción es consistente. De hecho, El teorema de la consistencia es un corolario del teorema de Herbrand que se presento en el capítulo 1. Este teorema cobra mucho mayor fuerza al extraerlo del contexto puramente sintáctico que Herbrand le dio, trayendo al contexto semántico un nuevo punto de vista para probar la consistencia de la aritmética.

Esta demostración se debe a Dreben y Denton. Herbrand mismo realizó algo de trabajo en esta dirección, pero los argumentos que usó no se pueden extender a la teoría completa de la aritmética. También cabe señalar que el argumento dado para construir M_i es esencialmente el mismo que se utilizaría para construir una función analizadora para la regla de corte.

2.4 Análisis de las nociones utilizadas en este tipo de demostración

En la prueba de consistencia para la aritmética usamos una misma estructura como modelo para las expansiones de satisfacción de todos los axiomas sobre un dominio C_n. Cuando se añadió el axioma de inducción para fórmulas cerradas ya no pudimos seguir haciendo lo mismo. No obstante, aún fue posible dar un método constructivo a través del cual llegamos al modelo buscado mediante aproximaciones sucesivas. Un obstáculo que tuvimos que superar era lo siguiente: Al usar la función α, si ésta tenía algún valor para el que ya no era verdadera, podíamos construir una nueva función sin tener que retroceder en el proceso. En otras palabras, los valores correctos para α, no era necesario cambiarlos en etapas posteriores al construir la función α.

En la prueba anterior de la consistencia de la aritmética se usaron varios conceptos uqe queremos formalizar en esta sección. Por ello, es que deseamos exponer algunas nociones que formalizan los métodos y por lo tanto, exponemos de manera más detallada las proposiciones que nos parecen de mayor relevancia en la demostración, de este modo, sabremos un poco más al medir el avance hacia el objetivo propuesto. De lo que se trata, es de mostrar que al medir el avance, la meta será alcanzada en un número finito de pasos. Son estos pasos, los que no se puede formalizar en la teoría formal. Al respecto, debemos recordar las limitaciones impuestas por el segundo teorema de incompletud de Gödel. Aún así, la estrategia que hemos seguido en la construcción del modelo no cambia. Es necesario mapear los términos que figuran en las expansiones de satisfacción de los axiomas en elementos de un modelo intuitivamente claro. De ahí surge la estructura apropiada.

Las nociones que deseamos poner más en forma, aun cuando explicamos su funcionamiento dentro de la demostración son las siguientes, algunas de ellas intervinieron implícitamente en la demostración.

Definición 2.4.1: Llamemos una j - subrutina ($1 \leq j \leq p+1$) a la serie de uno o más mapeos consecutivos μ_i, μ_{i+1}, … generados consecutivamente a partir de los dominios $C_0,\ldots, C_{p+1}$ como ya hemos explicado y siguiendo las reglas dadas para generar mapeos en la sección anterior. De modo tal que si el rango de μ_i uno de los mapeos es de rango mayor que j entonces para todos los mapeos que lo preceden de rangos menor que j, la serie es infinita o acaba con un mapeo μ_k, de forma tal que para este existe una función que hace verdaderas a las fórmulas A_1, A_2, …, A_{j-1}. A dicha j - subrutina le llamaremos propia si μ_i si es de rango j y escribiremos $\langle i,\ldots,i+k-1\rangle$ para marcar cuando acabo la j - subrutina $\mu_1,\ldots, \mu_{i+k-1}$.

Como no hay mapeos de orden menor a uno, cualquier 1 - subrutina consiste de un solo mapeo y cualquier mapeo de rango mayor o igual a uno constituye una 1 - subrutina. Para toda j – subrutina tenemos lo siguiente, una (j + i) – subrutina:

1) Está constituida de una sola j – subrutina, lo cual sucede cuando para todos los mapeos mayores que la 1 – subrutina, son de orden menor que j.

2) Está hecha de una serie de j – subrutinas las cuales son propias excepto por a lo más la primera 1 – subrutina.

Para $1 \leq j$, alguna (j +1) – subrutina empezará con un j – subrutina, para la cual tenemos dos opciones es infinita o termina con un mapeo μ_{j+k-1} tal que induce una función α_o que verifica a las formulas $A_1, A_2,\ldots, A_{j-1}$. Si este mapeo también verifica A_j entonces la (j + 1) - subrutina termina en con este mismo mapeo μ_{j+k-1} o si no verifica la fórmula el mapeo μ_{i+k} será de rango j y generará una nueva
j - subrutina propia y este proceso continuará a menos que en alguna j - subrutina terminemos encontrando un mapeo μ_{i+m-1} de modo que induzca una función $\alpha_o(\mu_{i+m-1})$ que verifique a A_j así como a $A_1, A_2, \ldots, A_{j-1}$.

Hemos visto como la series de mapeos $\mu_1,\mu_2,\ldots$ constituyen subrutinas, entonces para probar la última versión enunciada del Teorema de Consistencia de Herbrand, nos bastará con probar el procedimiento de toda j - subrutina es finito. Para lo cual estableceremos algunas propiedades de las subrutinas en los siguientes dos lemas, propiedades relacionadas con las funciones α_{ij} y los mapeos μ_i, los cuales nos dan la base del argumento formal que seguimos.

Definición 2.4.2: Llamemos al buen orden de la aritmética R y definamos R´ como un nuevo orden para los números naturales, del mismo modo como se define R excepto porque en R´ todos los números siguen de cero y damos las propiedades de R´, como sigue:
1) R´ (x, y) si y solo si R(x, y)
2) R´ (x, 0) y no R´ (0, x)

Obviamente R´ es un buen orden definido recursivamente sí y solo sí R lo es. Ahora podemos afirmar lo siguiente, las constantes se pueden ordenar bajo R´, así como los términos que quedan ordenados bajo la nueva relación R´. Si nos es posible ordenar los términos entonces para todas las funciones α_{ij} será posible realizar un cálculo finito para encontrar su valor correspondiente, sobre el cual podremos decidir su orden, esto resulta en una relación de orden que es efectivamente decidible.

Lema 2.4.1: Si r (i + 1) = $j \leq p$ y $\langle \mu_i s_1,\ldots,\mu_i s_n \rangle$ es la eneada critica para del mapeo μ_{i+1} entonces $\varphi_n^{i+1}(\mu_i s_1,\ldots,\mu_i s_n) \leq_{R'} \varphi_n^i \mu_i s_1,\ldots,\mu_i s_n$.
Este lema tiene una demostración por casos de la cual ya hemos hecho una revisión informal en la sección anterior y consideramos que dentro de este texto desviaría la atención del lector, pero si desea hacer una consulta de la demostración puede hacerlo en [Scalon 1963].

Definición 2.4.3: Sea $t_1,\ldots,t_n$ los términos que se pueden formar para algún dominio C_n enlistados de manera que sus alturas van de menor a mayor, es decir, de modo que si t_i es de menor altura que t_j
$i < j$. Para denotar al índice de un mapeo μ_i, escribimos ind(i) y suponemos que es la eneada $\langle \mu_i t_1,\ldots,\mu_i t_c \rangle$. Tenemos de este modo que podemos ordenar los índices de los distintos mapeos como sigue, si el índice de μ_i es menor que el índice de μ_j escribimos ind(i) << ind(j), y en el caso en que para exista $d \leq c$ entonces sabremos que habrá un elemento b talque $\mu_i t_d <_{R'} \mu_j t_d$ con $b < d$ y sucede que $\mu_i t_b = \mu_j t_b$.

Lema 2.4.2: Si $\varphi_j^i \leq_{R'} \varphi_j^k$ para toda j = 1,…, p entonces sucede una de dos opciones ind(i) << ind(k) o ind(i) = ind(k).

Prueba: Si el $ind(i) \neq ind(k)$ entonces sabemos que hay al menos un término en C_n, enlistado en la forma que ya hemos explicado, para el cual μ_i y μ_k son distintos. Sea t_d el primer término dentro del ordenamiento $t_1,\ldots,t_n$, como μ_i y μ_k son mapeos, t_d debe ser de la forma $f_j(s_1,\ldots, s_j)$ y como los términos $s_1,\ldots, s_j$ son de menor altura que t_d sabemos que los mapeos μ_i y μ_j les asignan los mismos valores. Entonces $\mu_i t_d = \varphi_j^i(\mu_i s_1,...,\mu_i s_j) \leq_{R'} \varphi_j^k(\mu_i s_1,...,\mu_i s_j) = \mu_k t_d$, y como t_d es el primer término de C_n en el cual μ_i y μ_k son distintos se sigue que ind(i) << ind(k) y con esto terminamos la demostración del lema anterior pues el caso donde son iguales es trivial.

Ahora si r(i + 1) ≤ r(i) entonces $\varphi_h^{i+1} =_{R'} \varphi_j^i$ para toda h $\neq$ r(i + 1), para j = r(i + 1) φ_h^{i+1} tomara los mismos valores que φ_h^i en todos valores excepto en la eneada critica en la cual por el Lema 2.4.1 $\varphi_h^{i+1}(b_1,...b_j) \leq_{R'} \varphi_j^i(b_1,...b_j)$ por lo cual $\varphi_h^{i+1} \leq_{R'} \varphi_h^i$ para toda h y se sigue por el Lema 2.4.2 que tenemos dos opciones ind(i + 1) << ind(i) o estos índices son iguales. En particular para r(i + 1) ≤ r(i) y r(i + 1) = $j \leq p$ entonces ind(i + 1) << ind(i) y los mapeos μ_{i+1} y μ_i deberán ser diferentes en al menos un término de C_n, a saber el primer término del orden $t_1,\ldots,t_c$ el cual tiene la forma ya mencionada y donde $\langle \mu_i u_1,...,\mu_i u_j \rangle$ es la eneada crítica del mapeo μ_{i+1}. Estos mapeos deben ser distintos en este término dada la forma en que fue escogido pues deben ser iguales en el término $u_1,\ldots u_j$. Con lo cual podemos concluir que los índices de los mapeos en una 2 - subrutina formaran una cadena estrictamente descendente pues la relación de orden (<<) entre los índices forma un buen orden, lo que significa que cada 2 - subrutina puede contener sólo mapeos finitos. Por ahora no lo podemos extender para j - subrutinas mayores a 2 - subrutinas pues la hipótesis de que el rango r(i) < r(i + 1) no incrementa es fundamental en nuestro argumento, pues cuando en la función φ_j^{i1} obtenemos valores no cero para algunas funciones φ_h^{i+1} estos se pueden perder, por consecuencia no podemos esperar que el índice del mapeo μ_{i+1} no sea mayor que el índice del mapeo μ_i.

Lo que si podemos mostrar es que si una j- subrutina está compuesta de otras j - subrutinas finitas éstas no pueden generar una j + 1 - subrutina infinita. Procedemos mostrando que es imposible pues si toda
j - subrutina es finita y suponemos que una serie de estas generarán una (j + 1) - subrutina infinita, todas las j - subrutinas que forman esta serie de ser propias menos las primera. Mostraremos que esto es imposible a través de definir índices para las j - subrutinas y verificando que estos índices forman una cadena estrictamente descendente, ordenándolos bajo un orden bien definido y con esto completaremos la prueba de la última versión que presentamos en la sección anterior sobre el Teorema de Herbrand. Las bases del argumento están dadas por el siguiente teorema.

Teorema 2.4.1: Sean $\langle i,...,i+k-1 \rangle$ y $\langle i+k,...,i+k+m-1 \rangle$ dos j - subrutinas finitas consecutivas para alguna j, ahora si 1 ≤ j ≤ p tal que r(i + k) = j ≤ r(i). Entonces existe d < min(k, m) tal que
a) ind(i + k + d) << ind(i + d) y
b) para toda n $0 \leq n \leq d$, $ind(i+k+n = ind(i+n \ y \ r(i+k+n-1 = r(i+n+1)$.
La prueba del teorema anterior está basada en los siguientes dos lemas.

Lema 2.4.3: Si r(i + k) ≤ r(i) y r(i + a) < r(i + k) para toda a con 1 ≤ a ≤ k entonces $\varphi_h^{i+k} =_{R'} \varphi_j^i$ para j = 1,…,p y resultan dos opciones ind(i + k) << ind(i) o ind(i + k) = ind(i).

La prueba de éste lema es como sigue para toda j < r(i + k) ≤ r(i), $\varphi_j^{i+k} = \varphi_j^0 = \varphi_j^i$ y como no hay mapeos entre μ_i y μ_{i+k} que tengan rango mayor que r(i + k) y $\varphi_j^i = \varphi_j^{i+1} = ... = \varphi_j^{i+k}$, para toda r($i$ + k) < j. Finalmente para j = r(i + k), $\varphi_j^i = ... = \varphi_j^{i+k-1}$ y φ_j^{i+k} toma los mismos valores que φ_j^{i+k-1} para cada eneada de números naturales excepto por los valores de la eneada crítica $\langle b_1,...,b_j \rangle$ de μ_{i+k} la cual por el lema 2.4.1 y $\varphi_j^{i+k}(b_1,...,b_j) \leq \varphi_j^{i+k-1}(b_1,...,b_j)$ y tenemos que $\varphi_j^{i+k} \leq \varphi_j^i$ para j = 1,…,p, por el lema 2.4.2 tenemos dos opciones para los índices o bien ind(i + k) << ind(i) o como segunda opción ind(i + k) = ind(i).

Lema 2.4.4: Sì el ind(i) = ind(k) entonces los mapeos μ_{i+1} y μ_{k+1} deben estar formados a través de hacer el mismo cambio en la función, y nos deja lo siguiente:
a) r(i + 1) = r(k + 1).
b) Si $\langle b_1,...,b_j \rangle$ es la eneada crítica para μ_{i+1} entonces debe serlo también para μ_{k+1} y $\varphi_j^{i+1}(b_1,...,b_j) \leq \varphi_j^{k+1}(b_1,...,b_j)$.

Para probar el lema anterior hacemos lo siguiente. Sí el ind(i) = ind(k) entonces los mapeos μ_i y μ_k deben ser iguales para todos los términos del dominio C_n, Teniendo que $\alpha_0(\mu_i)$ y $\alpha_0(\mu_k)$ deben ser iguales para los todos los disjuntos $K_1,\ldots,K_p$, de modo que μ_{i+1} y μ_{k+1} tendrán el mismo rango y empezaron a formarse con base en el mismo disjunto que se falsifico en el axioma de inducción, es decir, al hacer la expansión de Herbrand hay un disjunto para el cual las funciones alfa del mapeo le relacionan una función que lo hace falso. Ahora para cualquier caso μ_i y μ_k deben ser iguales para $s_1,\ldots,s_j$ y los mapeos μ_{i+1} y μ_{k+1}, tienen la misma eneada crítica $\langle b_1,...,b_j \rangle$. Si 1 < j entonces $\varphi_j^{i+1}(b_1,...,b_j) = \mu_i t = \mu_k t = \varphi_j^{k+1}(b_1,...,b_j)$, para cuando j = 1 entonces $\varphi_j^{i+1}(b_1)\ y\ \varphi_j^{k+1}(b_1)$ deben ser los miembros mínimos bajo R para los cuales los siguiente conjuntos
$\{n \mid\ para\ alguna\ u\ en\ C_1,\ n = \mu_i u\ y\ \alpha_0(\mu_i)\ debe\ verificar\ a\ H_1(s_1,u)\}$ y
$\{n \mid\ para\ alguna\ u\ en\ C_1,\ n = \mu_k u\ y\ \alpha_0(\mu_k)\ debe\ verificar\ a\ H_1(s_1,u)\}$ deben existir, pues los mapeos μ_i y μ_k coinciden en todo C_n y por lo tanto coinciden en C_1 entonces estos conjuntos deben ser el mismo con lo que concluimos que $\varphi_j^{i+1}(b_1) = \varphi_j^{k+1}(b_1)$.

Con estos lemas probados podemos empezar la prueba del Teorema 2.4.1, tenemos que por el Lema 2.4.3 $\varphi_h^{i+k} \leq_{R'} \varphi_h^i$ para h = 1,…,p y sucede alguna de las siguientes ind(i + k) << ind(i) o ind(i + k) = ind(i). Si se da la primera opción entonces tomamos d = 0 y hemos terminado, en cambio si ind(i + k) = ind(i) entonces por el Lema 2.4.4 tenemos que r(i + k + 1) = r(i + 1) y los mapeos μ_{i+k+1} y μ_{i+1} estarán formados de la misma manera, puesto que $\varphi_h^{i+k} \leq_{R'} \varphi_h^i$ para h = 1,…, p y obtenemos lo siguiente $\varphi_h^{i+k+1} \leq_{R'} \varphi_h^{i+1}$ para h = 1,…, p y por el Lema 2.4.2 tenemos ind(i + k + 1) << ind(i + 1) o, por otro lado, ind(i + k + 1) = ind(i+1). Podremos en el siguiente paso inferir como lo hicimos antes que μ_{i+k+2} y μ_{i+2} deben estar formados al hacer el mismo cambio, en el cual r(i + k + 2) = r(i + 2) y que ind(i + k + 2) << ind(i + 2) o ind(i + k +2) = ind(i + 2). Podemos continuar así hasta que no

hallemos alguna d que no satisfaga el teorema, iremos generado de este modo una serie de pares de mapeos $\langle \mu_i, \mu_{+ki} \rangle, \langle \mu_{i+1}, \mu_{i+k+1} \rangle, ...$ modo que para cada par, sus índices ind($i + k + n$) = ind($i + n$) y r($i + k + n + 1$) = r($i + n + 1$) y nos basta con mostrar que esta secuencia de pares de mapeos debe terminar antes de que lleguemos al par $\langle \mu_{i+k-1}, \mu_{i+k+k-1} \rangle$ o el par $\langle \mu_{i+m-1}, \mu_{i+k+m-1} \rangle$, puesto que alguno de estos pares debe pertenecer a la serie que hemos generado sí y sólo sí k = m, entonces los dos pares son el mismo. Si el primer par pertenece a la secuencia entonces por el Lema 2.4.4 tenemos lo siguiente r(i + k + k) = r(i + k) = j, pero el mapeo μ_{i+k+k} será el primer mapeo después de μ_{i+k} para el cual el rango es mayor a j,de manera similar si el segundo par es el que pertenece a la secuencia entonces $j \leq$ r(i + m) = r(i + k + m) y el mapeo μ_{i+m} debe el mapeo μ_{i+k}.
Pero si el par $\langle \mu_{i+k-1}, \mu_{i+k+m-1} \rangle$ pertenece a la secuencia entonces los mapeos μ_{i+k} y μ_{i+k+m} están formados de la misma manera, es decir, al dar ϕ^{i+k-1} y $\phi^{i+k+m-1}$ tendremos el mismo nuevo valor para el mismo sistema de argumentos, más esto es imposible pues los mapeos $\mu_{i+k+1},\ldots,\mu_{i+k+m-1}$ son todos de rango menor que j por lo cual la función $\phi^{i+k+m-1}$ ya tenía asignado el valor que fue introducido en ϕ^{i+k-1} al formar el mapeo μ_{i+k}. Se sigue que debe existir alguna d < min(k,-m) que satisface las condiciones del teorema.

Definición 2.4.4: Si existe W un orden total para un conjunto A, entonces W es el orden de las secuencias finitas que es posible formar con los miembros de A. Dentro de los cuales $\langle a_1,...,a_n \rangle$ precede a $\langle b_1,...,b_m \rangle$ sólo en el caso de que para alguna $d \leq$ min(n, m), a_d precede a b_d en el orden W y para toda x < d, $a_x = b_x$ o bien para n < m y para toda $x \leq m$ $a_x = b_x$.

Definición 2.4.5: El índice de una 1 - subrutina μi es el índ(i), denotando al mapeo μ_i del cual se genero, α y β son los índices de 1 - subrutinas escribimos $\alpha <<_1 \beta$ solo en el caso en el que $\alpha << \beta$.

Ahora el índice de una (j + i) - subrutina finita con $1 \leq j$ es una serie finita $\langle \alpha_1,...,\alpha_k \rangle$ donde $\alpha_1,\ldots,\alpha_k$ son los índices de las distintas j - subrutinas finitas de las cuales se compone la (j + 1) - subrutina tomando el orden de que éstas subrutinas ocurren, sí $\alpha = \langle \alpha_1,...,\alpha_k \rangle$ y $\beta = \langle \beta_1,...,\beta_n \rangle$ son los índices de alguna (j + 1) - subrutina finita entonces escribimos $\alpha <<_{j+1} \beta$ solo en el caso en el que $\langle \alpha_1,...,\alpha_k \rangle$ preceda a $\langle \beta_1,...,\beta_n \rangle$ en el orden dado por la relación $<<_j$.
Sí $\langle i,...,i+k-1 \rangle$ y $\langle i+k,...,i+k+m-1 \rangle$ son dos j - subrutinas consecutivas que forman alguna (j + 1) – subrutina, entonces r($i + k$) = $j \leq$ r(i). Que cumplen las hipótesis del Teorema 2.4.1 y por ello deben tener algún punto en el que difieran a decir d < min(k, m), este punto satisface las condiciones de la definición 2.4.5. Si j = 2 se sigue de inmediato que en la relación de orden $<<_2$, el índice de $\langle i+k,...,i+k+m-1 \rangle$ precede a $\langle i,...,i+k-1 \rangle$ dentro de este ordenamiento. Pero al extender este resultado para 2 < j necesitamos mostrar que el punto de bifurcación para los índices que esta garantizado por el Teorema 2.4.1, esta reflejado en un primer punto donde las (j - 1) - subrutinas, que forman a la j – subrutina, difieren entre si. Establecemos lo anterior con el siguiente lema.

Lema 2.4.5: Sean $\langle i,...,i+k-1 \rangle$ y $\langle m,...,m+q-1 \rangle$ dos j – subrutinas finitas consecutivas con $2 \leq j$ tal que para alguna d < min(k, q) tenemos las opciones ind(m + d) << ind(i + d) y para toda n < d ind(i + n) = ind(m + n) y r(i + n + 1) = r(m + n + 1), entonces el índice de $\langle m,...,m+q-1\rangle$ precede al índice de $\langle i,...,i+k-1\rangle$ dentro del ordenamiento $<<_j$

Este lema es meramente computacional y nos indica como podemos ordenar los índices de las distintas j – subrutinas, que forman a alguna (j + 1) – subrutina. La prueba es por inducción sobre j, pero completarla distraería nuestra atención de la meta principal de esta expocision, por lo cual si el lector desea verificarla puede consultar el texto original [Scanlon 1963]. Con base en este lema podemos concluir que si hay una (j + 1) - subrutina infinita debe contener series infinitas de j - subrutinas finitas y los índices de éstas j - subrutinas forman una serie infinita estrictamente descendiente ordenada bajo el ordenamiento $<<_j$.

Para concluir la formalización de conceptos utilizados en la prueba de la ultima versión del Teorema de Herbrand que enunciamos asi en la sección anterior. Dada una instancia de *AI* podemos encontrar efectivamente un mapeo de modo que verifique Exp (*AI*, C_n). Dicho mapeo se determina relacionando una función calculable α dentro de la aritmética para el símbolo funcional de Herbrand f, que aparece en la forma cerrada de satisfacción del Axioma de Inducción al eliminar el cuantificador existencialoide.

De este modo solo falta hacer claro para teorema que basta con mostrar que todo grupo de j - subrutinas finitas no puede generar una (j + 1) - subrutina infinita y para hacer esto basta con probar el siguiente lema.

Lema 2.4.6: Cada uno de los ordenes $<<_j$ está bien fundamentados, puesto que para cualquier serie estrictamente descendiente a1 $<<_j$ a2 $<<_j$…. esta contiene una cantidad finita de miembros.

La prueba es por inducción sobre j. El paso inicial es obvio pues el $<<_1$ es el buen orden <<. Ahora para cada j $<<_{j+1}$ es el ordenamiento de secuencias finita basado en $<<_j$ será suficiente para los pasos de inducción establecer el hecho general de que si *A* es un conjunto bien ordenado por la relación $\prec$ y denotamos a dicha secuencia finita A como SF(A) la cual es el conjunto de todas las secuencias finitas $\langle a_1,...,a_k\rangle$ de los miembros de *A* de modo que $a_k \prec \ldots, a_2 \prec a_1$ entonces esta serie SF(A) está bien ordenado por la relación $\prec_{SF}$ el ordenamiento basado en $\prec$.

Como $\prec_{SF}$ es un orden total para SF(A) será suficiente mostrar que no hay una cadena infinitamente descendiente de miembros que pertencen a SF(A) bajo $\prec_{SF}$, supongamos que $\alpha_1, \alpha_2, \ldots$ sea la cadena infinita de miembros. Cada α_i será de la forma $\langle a_1^i,...,a_{pi}^i\rangle$ para alguna p_i y para algunos $a_1^i,...,a_{pi}^i$ que pertenecen a *A*. Como no puede haber una cadena una cadena infinita descendiente de miembros de *A* bajo $\prec$, entonces existe un α_{i1} que pertenece a la serie $\alpha_1, \alpha_2, \ldots$ tal que si $i_1 < j$ y $a_1^j = a_1^i$. Por la definición de la relación $\prec_{SF}$, $a_{ij} \prec_{SF} \langle a_1^i, b_2,...,b_k\rangle$ para todas $b_2,\ldots,b_k$ que están en *A*. De los cual se sigue por la hipótesis de inducción que α_1, $\alpha_2, \ldots$ es una serie descendiente infinita y que para toda $i_1 < j$ la secuencia α_j tiene al menos dos miembros. Repitiendo el mismo razonamiento veremos que debe haber alguna $i_1 \leq i_2$ de modo que para toda $i_2 \leq j$ la secuencia α_j debe contener al menos tres miembros, procedimiento de esta manera podemos generar la serie $a_1^i, a_2^i, a_3^i,...$ de los miembros de A, pero como $a_1^i = a_2^i$ y $a_1^i \prec a_2^i$ tenemos que $a_1^i \prec a_2^i$ y en general para cada k $a_1^{ik} \prec a_2^{ik}$ y entonces…$\prec a_2^i \prec a_1^i$ contrario a la hipótesis de que $\prec$ era un buen orden para *A*.

Capítulo 3
Contexto histórico de la obra de Herbrand

En 1929 a los 21 años de edad, Herbrand publicó su tesis doctoral; en ella, expuso el teorema central presentado en el capítulo 1 de este trabajo. Este teorema es muy importante en la teoría de la cuantificación. En este capítulo hablaremos del estado en que se hallaba la lógica matemática en ese momento y señalaremos algunas de las corrientes que influenciaron a Herbrand. En particular, veremos cómo el programa de Hilbert marcó la dirección de sus trabajos. Al respecto, haremos un análisis de la postura de Herbrand y de las razones que lo llevaron a abrazar el intuicionismo cómo única herramienta metamatemática para fundamentar las matemáticas. Además, analizaremos cómo los trabajos de Skolem y Löwenheim influyeron en el teorema de Herbrand. Por último, cerramos el capitulo mostrando cómo la demostración que da Gödel del concepto de "funciones recursivas" se apoya en los trabajos de Herbrand.

3.1 Situación a finales del siglo XIX

Un hecho relevante del siglo XIX fue la aparición de las geometrías no euclidianas, la introducción de la teoría de conjuntos, y la conclusión del sistema de los números reales con base en la noción de infinito actual. Estas cuestiones otorgaron a las matemáticas una mayor generalidad y abstracción, dando lugar con ello a un debate sobre la naturaleza de esta disciplina. Esto llevo a la introducción de nuevos criterios para entender las matemáticas, en específico para comprender las pruebas matemáticas. En este sentido, la lógica prometía suministrar las herramientas indispensables para aclarar esta situación.

En 1879 Frege redujo la demostración matemática a la teoría de la cuantificación. En esta teoría se utiliza un conjunto finito de axiomas lógicos para generar con base en ellos todos los teoremas de una teoría. Con ello, Frege abrió una nueva visión del estudio de la lógica, introduciendo el concepto de función proposicional con argumentos, en vez del concepto sujeto-predicado impuesto por Aristóteles. Frege propuso a la lógica como el fundamento de la matemática y sostuvo que todos los conceptos matemáticos se pueden definir en términos lógicos, pudiéndose deducir todos los teoremas a partir de estos principios lógicos. Para ser más precisos, sostuvo que la aritmética y el análisis se fundamentan en la lógica, distinguiéndolos así de la geometría euclidiana. Afirma que la geometría no está basada en conceptos lógicos sino en la intuición *a priori* del espacio, a diferencia de la aritmética que no apela a tal intuición, sino en las leyes más generales del pensamiento.

Para operar este cambio Frege necesitaba explicar dos cuestiones: primero, el funcionamiento de la nueva lógica, y explicar las bases de su funcionamiento; segundo, llevar a detalle la derivación de la matemática clásica a partir de la lógica.

En sus obras Frege trabajó con las reglas que gobernarían el uso de conceptos tales como variable, función, relación, expresión formal, definición, cuantificador y prueba, justo en el momento en que la matemática requería de una clara caracterización de estos conceptos. Las ideas de Frege influyeron años después en Russell y Whitehead, quienes intentaron continuar su obra entorno a los fundamentos de las matemáticas. Esta necesidad se agudizó con la aparición de las paradojas en la teoría de conjuntos descubiertas por Cantor, Burali-Forti y Russell.

El comienzo del siglo XX se caracterizó por la variedad de explicaciones sobre los conceptos fundamentales de las matemáticas; sobre estas diferencias se perfilaron distintos grupos de matemáticos que creyeron en una u otra explicación.

Un ejemplo importante para nuestro caso es la discusión en torno a la noción de infinito. Para muchos matemáticos, esta noción debía ser rechazada, pues se decía que el razonamiento sobre ella conducía a las paradojas. Esto trajo a colación la distinción Aristotélica entre infinito potencial e infinito actual. En el primer caso el infinito se ve como un ideal, es decir, como algo a lo que se tiende sin poderlo alcanzar. El constructivismo nace de esta forma de ver a las matemáticas. Por el contrario, en el segundo caso el infinito se ve como algo completo, algo que "está ahí" o como algo que es legítimo pensar así. La defensa de esta última forma de pensar está relacionada con el formalismo.

Los seguidores del constructivismo decidieron investigar hasta qué punto es posible construir las teorías matemáticas sin el recurso del infinito actual. Herbrand adoptó este punto de vista como instrumento en el manejo de los fundamentos de las matemáticas, es decir, como herramienta de la metamatemática (aunque no se le considera un partidario incondicional de esta escuela) pues se sirvió de algunas nociones que esta tendencia ve como prohibidas. Herbrand es considerado un formalista, aunque las ideas de este grupo de matemáticos tampoco coinciden plenamente con el trabajo y las ideas que desarrolló.

En sus escritos, Herbrand no menciona a Frege y todo parece indicar que su trabajo sólo lo conoció a través de Russell y Hilbert.

3.2 Situación a principios del siglo XX

3.2.1 Lectura de Russell por parte de Herbrand

Hacia 1903 Russell descubrió la paradoja que lleva su nombre. Esta la presentó ante Frege para indicarle que su sistema permitía la existencia de este tipo de entidades anómalas, haciéndolo inconsistente. A partir de entonces, Russell se avocó a encontrar una solución para fundamentar las matemáticas en la lógica, siguiendo las ideas de Frege.

Para ello, propuso una estratificación del alcance de los cuantificadores en la que se podían generar niveles superiores indefinidamente. Esta solución tiene la característica de introducir cierto relativismo en el sistema. Lo que busca Russell con su teoría de tipos es darle un sentido preciso a los cuantificadores y construir un sistema universal como marco del conjunto de las matemáticas. Esta construcción busca rehacer con un sentido lógico el universo de los fundamentos de las matemáticas. Con ella, Russell logra solucionar las paradojas conocidas, pero no garantiza la coherencia de la teoría resultante. Los objetos de un estrato no se distinguen de los de otro más que por la jerarquía relativa que se les da dentro de la teoría de tipos. Esto representó para algunos matemáticos un sistema demasiado complicado para anular las paradojas, además de presentar ciertas cuestiones como básicas cuando no lo son. La teoría de tipos fue vista como un sistema poco elegante frente a otros planteamientos. La mayor diferencia entre el tratamiento de Russell y el de Frege es que dentro de la teoría de tipos, los objetos se estratifican, sin tener que estar todos en un mismo nivel como en la teoría de Frege. En la obra de Russell y Whitehead la obtención de teoremas es más importante que el estudio de las propiedades del sistema mismo.

En 1927 Herbrand leyó *Principia Mathematica* de Russell y Whitehead; también leyó con cuidado a Hilbert y Ackermann. Para entonces Herbrand se encontraba trabajando en la teoría de la cuantificación. Una consecuencia de tales lecturas son sus resultados más importantes. Es aquí donde surgen las interrogantes: ¿Cuáles eran las motivaciones de Herbrand? ¿Sería acaso cierta desconfianza filosófica acerca de la Teoría de tipos? ¿Cómo interpretó los trabajos de Hilbert acerca de los fundamentos de las matemáticas?

En *Principia Mathematica* encontramos la inspiración de Herbrand para tratar con ciertas nociones fundamentales. Por ejemplo, en el capitulo llamado "Extensión de la teoría de la deducción de un tipo inferior a un tipo superior de proposiciones" se establece un teorema que explica cómo los valores de verdad aplicados a fórmulas sin cuantificadores tienen un uso diferente a cómo se aplican a las fórmulas con cuantificadores, lo cual induce una estratificación de los valores de verdad.

Herbrand en su tesis tiende un puente entre la teoría de la cuantificación y la lógica proposicional cuando enuncia y demuestra el siguiente teorema:

"Si dentro de una fórmula demostrable en lógica proposicional se reemplazan las variables por fórmulas de la teoría de la cuantificación, lo que resulta es una fórmula demostrable en la teoría de la cuantificación."

Este resultado lo interpretamos de la siguiente manera: "Sí dentro de una tautología se cambian las variables proposicionales por fórmulas con cuantificadores, la nueva fórmula será demostrable en la teoría de la cuantificación". Este resultado es de hecho el reciproco de su teorema, y nos da una idea de cómo logra Herbrand darle forma a un teorema como el que plantea al final de su tesis.

El aporte de este teorema es que los axiomas que consideraba admisibles son fórmulas sin cuantificadores. En la demostración de su teorema, Herbrand usa lo que él llama una "identidad normal". La transformación de una fórmula en una identidad normal le permite buscar una tautología dentro de las expansiones de Herbrand de dicha fórmula. Como hemos visto, cuando el proceso concluye con el hallazgo de una tautología, la fórmula en cuestión es válida en la teoría de la cuantificación. Este tratamiento lo hemos expuesto con todo detalle en el capítulo 1; Herbrand expone en este teorema la idea inicial de lo que llamo “el uso de una identidad normal” (usage de une identité normale).

La consideración de identidades normales está relacionada con la regla de existencialización, en virtud de la cual podemos pasar de $R(x,x) \vee \neg R(x,x)$ a $\exists y(R(x,y) \vee \neg R(x,y))$, en donde ciertas presencias de *x* en la primera fórmula se reemplazan por *y*. Si se intenta dar marcha atrás hay que suprimir el cuantificador existencial ($\exists y$) y reemplazar la variable *y* por *x*, de tal modo que sí la primera fórmula es demostrable, la segunda lo debe ser también. Tenemos aquí la semilla de una idea que aparece a lo largo de la obra de Herbrand: poder “revertir” las demostraciones. Esto indica la importancia que Herbrand le da a los teoremas de la forma “si y solo si” frente a los teoremas que sólo tienen un sentido. Sobre todo dentro de la metamatemática.

El problema planteado por Russell al que responde Herbrand con esta técnica, consiste en poder recuperar las fórmulas demostrables en teoría de la cuantificación usando sólo esquemas en que los axiomas utilizados no sean más que fórmulas sin cuantificadores.

Como ya hemos visto, a través de la identificación de las distintas variables se obtiene una fórmula proposicionalmente válida. Es aquí donde Herbrand introduce la noción de “campo finito”, es decir, de conjuntos que se generan a partir de las variables libres y constantes que tenga la fórmula. Esta noción la introdujo para soslayar las nociones semánticas en la demostración del teorema de Löwenheim, como pronto veremos. Esta cuestión central en su trabajo, ya la hemos expuesto en esta tesis.

Se puede decir entonces que las ideas presentes en el teorema de Herbrand se encontraban en *Principia Mathematica* y el teorema de Löwenheim.

3.2.2 Influencia de Hilbert en los trabajos de Herbrand

Si bien *Pricipia Mathematica* marcó el camino de la investigación de Herbrand, en su opinión la visión de Russell no es suficiente. Herbrand ve a la teoría de tipos tan sólo como un sistema de la teoría de la cuantificación con una jerarquía de clases. Esto genera problemas y dificultades que la desvían de su planteamiento inicial, a saber resolver la paradoja de Russell. No obstante, la estratificación infinita, la ramificación y en general, los problemas que provienen del axioma de infinito, no facilitan una solución. Herbrand rechaza la concepción de Russell, adoptando en cambio el punto de vista de Hilbert para tratar lo relacionado con la lógica matemática.

Herbrand llegó a Alemania a finales de 1930, tras ganar la beca Rockefeller por el trabajo realizado en su tesis. El año que pasó en Alemania fue el último de su vida. En este periodo Herbrand se volvió más productivo, pues dejó su aislamiento de París y conoció a von Neumann, Ackermann y Emmy Noeter. Esto le permitió profundizar en el trabajo de la escuela formalista y estudiar los escritos que Hilbert dedicó a los fundamentos de las matemáticas. Es ahí donde tomó contacto con los problemas de la no contradicción, de la completud y de la decisión, los cuales no aparecen en la obra de Russell. De este modo, Herbrand adoptó el punto de vista que Hilbert propone para tratar tales cuestiones desde la metamatemática. En la obra de este periodo utilizó términos propios de los textos de Hilbert; un ejemplo claro es el título de su tesis de doctorado "Investigaciones sobre la teoría de la demostración" (Recherches sur la théorie de la démonstration).

En los escritos de este periodo Herbrand explica las insuficiencias que ve en el trabajo de Russell. Ve que su trabajo sólo se concentra en hacer una sustitución del lenguaje ordinario por otro más cómodo para estudiar los fundamentos de las matemáticas, sin que este hecho asegure la resolución de los problemas. Herbrand le atribuye al aporte de Russell dos meritos. Primero, "el habernos dado la 'certeza experimental' en cuanto a la posibilidad de formalizar las matemáticas." (Herbrand 1930b); segundo, el haber expuesto las ideas iníciales que le dieron forma al trabajo de Hilbert. Sin embargo, es en los escritos de este último que Herbrand encuentra el método a seguir para tratar con los problemas de fundamentos de la matemática.

Aunque Herbrand se nutre de las ideas de Hilbert, podemos decir que su adhesión a éstas tampoco era incondicional. En una nota escrita en 1931 acerca de su tesis doctoral dice Herbrand: "Para concluir, queremos insistir nuevamente en el hecho de que [la metamatemática] es independiente de cualquier opinión filosófica. Los resultados obtenidos son positivos, y así como un matemático que estudia las ecuaciones de Einstein no tiene porque compartir sus ideas, tampoco quién estudia estas teorías tiene porque adherirse a los principios filosóficos de Hilbert." (Herbrand 1931) Con esto pone en relieve el hecho de que lo importante en el trabajo de Hilbert es el método, no sus ideas filosóficas con relación a los fundamentos de la matemática.

En palabras de Herbrand: "La esencia de esta teoría, que Hilbert denomina metamatemática, es el intento de resolver problemas de la filosofía de las matemáticas no mediante la discusión verbal, sino resolviendo cuestiones precisas. No es este el lugar para discutir que tan a fondo penetra esta teoría en la base de los problemas; no obstante, con base en el análisis que hacemos de ella veremos que se halla en acuerdo con el más estricto positivismo y el rigor más perfecto. Sin embargo, se rehúsa a considerar ciertas cuestiones relativas a la teoría del conocimiento, quizá en ello se encuentre su insuficiencia" (Herbrand 1930b)

Podemos decir que a finales de los años veinte y principios de los treinta del siglo XX los trabajos en torno a los fundamentos de las matemáticas seguían la dirección metamatemática propuesta por Hilbert. Una de sus motivaciones era soslayar la crítica que Brouwer hizo sobre los métodos no constructivos. Para evitar toda crítica, propuso restringir a los métodos finitistas al momento de investigar los fundamentos de la matemática. Esta limitación se convirtió en uno de los puntos más importantes dentro de los trabajos de Hilbert.

El modo en que Herbrand empieza a trabajar los temas de la metamatemática puede ser confuso. Al ver algunos de sus escritos se pueden ver declaraciones tan dispares como las siguientes:

- Se debe considerar que el papel de las matemáticas es únicamente proveernos con los razonamientos y sus formas, más no el de buscar que se apliquen a tal o cual objeto. (Herbrand 1930)[1]

[1] Esto último concierne según Herbrand a los físicos o a los filósofos más no a los matemáticos.

- Una teoría matemática no puede ser solamente un juego vano de símbolos, por lo cual se debe traducir en algo real, debe aplicarse a objetos reales concebibles por el entendimiento. (Herbrand 1930b)

Parecería que Herbrand no rechaza la idea de que el trabajo matemático debe tener una referencia en el mundo real, pero encuentra una diferencia muy clara entre la matemática y la metamatemática. La primera opinión toma en cuenta los problemas sólo de la metamatemática, mientras en la segunda se refiere al sistema de las matemáticas mismas. Aun cuando a través de la metamatemática se estudia a la matemática, Herbrand las entiende como dos cosas separadas. Acepta, por ejemplo, ciertos usos de la reducción al absurdo en matemáticas, más no así en metamatemáticas.

Herbrand era un matemático con un gran interés en la filosofía de la ciencia. El punto de vista que asume en el estudio de la metamatemática es alcanzar una reconstrucción tan precisa como sea posible de las teorías matemáticas, así como aclarar la naturaleza de las matemáticas puras.

Herbrand acepta la propuesta finitista en la metamatemática. Encontrando en el finitismo la posibilidad de precisar los problemas técnicos planteados. Es la precisión lo que atrae a Herbrand, pues busca así proporcionar una solución efectiva a los problemas que plantea Hilbert.

Por ejemplo, Herbrand introduce los términos con los que harán las expansiones de la fórmula como un resultado análogo y alternativo al cálculo épsilon de Hilbert. No obstante hay una gran diferencia en el tratamiento para eliminar los cuantificadores. En el de Hilbert se considera anular los cuantificadores existenciales, para en una segunda etapa ver a los cuantificadores universales como una abreviatura de existenciales negados, pudiendo de esta manera repetir el procedimiento de eliminación. El resultado es una fórmula en la que se pierde claridad al aplicarle este proceso. Por el contrario, en el método de Herbrand se elimina cada uno de los cuantificadores de manera independiente. Esta manera tan distinta de ver a los cuantificadores hace más claro que el espíritu con que cada autor aborda los problemas es distinto.

Herbrand comienza sus estudios desde la lógica, pasando después a teorías particulares, que en su punto de vista se obtienen al aumentar las hipótesis o axiomas lógicos con axiomas propios. En cambio, el sistema inicial de Hilbert es la aritmética, a la cual le quiere dar una base lógica. Para Hilbert lo esencial es poder abstraerse del sistema de números y considerarlo un sistema arbitrario de cosas. Así, mientras Hilbert pasa de la aritmética a lógica, Herbrand lo hace en sentido inverso, dando el primero cierta importancia a axiomas que para Herbrand no la tienen.

Esta diferencia de enfoques se reflejo más tarde en el programa de Hilbert. Al reconocer que había algo que no permitía el avance del método de Hilbert, uno de sus discípulos (Bernays) cambió el punto de partida de la teoría de la cuantificación estableciendo un nuevo camino al cambiar el modo de eliminar cuantificadores; al introducir las bases de la técnica hace referencia al método de Herbrand. Esto es un indicativo de la influencia de Herbrand en trabajos posteriores.

Algunos seguidores del trabajo de Herbrand, como Dreben y Scanlon, dicen que la prueba de la no contradicción de la aritmética basada en su método es del mismo grado de complejidad que la prueba basada en las ideas de Hilbert.

3.2.3 Base del método seguido por Herbrand, Skolem y Löwenheim

Herbrand indica entre sus textos los medios de los que se sirvió para escribir su tesis. Sin mencionar la influencia de Löwenheim, tampoco hace referencia a su notación. Sin embargo, dentro del artículo en el que Herbrand trata el problema de la reducción para la teoría de la cuantificación usa los mismos símbolos relacionales propuestos por Löwenheim. Podríamos decir que es en este artículo de Löwenheim donde Herbrand encuentra el argumento semántico que le conduce a introducir la noción de “campos finitos”.

Herbrand le recrimina a Löwenheim sobre todo el sentido semántico de algunas nociones, además de encontrar en sus trabajos lagunas para las definiciones y las demostraciones. Estos desacuerdos son principalmente dos: Primero, para Löwenheim la noción de validez tiene un sentido intuitivo, y por consiguiente, su teorema carece de un sentido preciso. Esta deficiencia aparece al no exponer las definiciones para las nociones semánticas que utiliza, aunque puede superarlas en el contexto en que las utiliza. Segundo, la demostración carece de rigor, haciéndola insuficiente. Herbrand, que en un sentido es un rigorista de la sintaxis, al leer la prueba nota un desvío en la introducción de la noción de infinito, dado que el autor llega a considerar fórmulas de longitud infinita, trayendo consigo el uso del axioma de elección. Löwenheim trata de encontrar un modelo infinito para estas fórmulas, sin lograrlo pues cuenta como base sólo con un conjunto de asignaciones finitas. Por tanto, se ve forzado a usar el concepto de conjunción infinita. Es aquí donde Herbrand ve la insuficiencia. En vez de ello, Herbrand recurre a la introducción de un campo infinito potencial que aproxima a través de los “campos finitos”.

Herbrand no sólo pretende explicar las lagunas de Löwenheim (exigiendo por ejemplo las definiciones explícitas de las nociones semánticas), más bien lo que propone es abandonar esas nociones. En otras palabras, en vez de llenar los faltantes en la demostración, lo que propone es probar un teorema diferente con un sentido sintáctico[2].

En los siguientes teoremas de Herbrand cabe señalar que el sentido de la expresión “ser verdadera en un campo finito” es que la expansión conjuntiva de la fórmula sea satisfacible mediante tablas de verdad, es decir, que sea una tautología. Al respecto, el sentido que Löwenheim le atribuye a la expansión de satisfacción de la fórmula es diferente, pudiéndose explicar la adaptación de Herbrand como la conversión de una noción semántica en una noción sintáctica.

- Teorema 1: Si una formula F es demostrable en la teoría de la cuantificación, entonces $\neg F$ no puede ser verdadera para algún campo finito.
- Teorema 2: Si una formula F no es demostrable en teoría de la cuantificación entonces podemos construir algún campo finito en el cual $\neg F$ es verdadera.

[2] En efecto, computar la tabla de verdad de una fórmula es, más que nada, una operación sintáctica que nada tiene que ver con la noción de “verdad”

El resultado de Löwenheim es muy parecido al de Herbrand y lo podemos enunciar de la siguiente manera: Si una fórmula F no es válida, entonces $\neg F$ es satisfacible en un conjunto numerable de elementos.

Podemos ver que cada autor parte de contextos diferentes dentro de la lógica. Löwenheim no trabaja con axiomas, ni reglas de inferencia, por lo que no toma en cuenta la noción de que una fórmula sea demostrable. El uso de nociones semánticas para este autor pertenece tanto a los argumentos, como a los resultados. El valor de estos resultados es que ponen la semilla para que Herbrand lleve a cabo la reducción de una cuestión no numerable en una numerable, estableciendo de este modo un puente entre la teoría de la cuantificación y la lógica proposicional. En Herbrand la semántica siempre es vista como un juego con la noción de validez. Es por este rechazo hacia las nociones semánticas que propone llevar las ideas de Löwenheim al terreno sintáctico, siendo ahí donde les da certeza. Herbrand cree que el trabajo de Löwenheim tiene cabida dentro de las matemáticas, aunque algo le hace falta para estar dentro de la metamatemática, en la cual le ve gran utilidad. Es por esta razón que no desprecia del todo su trabajo; simplemente dentro de su visión el teorema de Löwenheim no puede pertenecer a la metamatemática.

Al pensar que dentro de la matemática caben otros conceptos que en la metamatemática, Herbrand aclara que para él son dos cuestiones totalmente diferentes. Por ejemplo, entre los conceptos a los cuales les da cabida dentro de las matemáticas se hallan los conjuntos de cardinalidad infinita, los cuales no tienen cabida en la metamatemática.

Skolem es otro de los autores que influyeron en el trabajo de Herbrand. El principal elemento que toma de este autor son las reglas para prenexar fórmulas, a las que Herbrand llama "Règles de Passage". Estas reglas se encuentran en los artículos de Herbrand siguiendo los planteamientos hechos por Skolem. Sin embargo, dentro de sus textos no hace referencia a este autor y es posible que no las haya conocido directamente, sino a través de los estudios que hizo con Ackermann.

Como se vio en este trabajo la prenexación de fórmulas es un proceso básico dentro del planteamiento de Herbrand. Al respecto como ya se dijo en la sección de funciones analizadoras, Herbrand hizo una suposición errónea en su demostración sobre la consistencia de la aritmética.

Aun con esta aportación tan importante, dentro del trabajo de Skolem encontramos otra idea que ocupa a ambos autores con similar importancia, pero que debido a sus puntos de vista divergentes, los lleva por caminos distintos. Se trata de la técnica para eliminar cuantificadores y simplificar el estudio de las fórmulas. Skolem enuncia la equivalencia semántica de las fórmulas prenexadas con la forma funcional de satisfacción, técnica mencionada en este trabajo como similar a la de Herbrand para quitar los cuantificadores de las fórmulas, pero en su caso lo que se obtiene es la forma funcional de validez.

Desde el punto de vista de Herbrand el problema de Skolem fue mezclar las nociones semánticas con las sintácticas, perdiendo así el sentido sintáctico estricto que Herbrand demanda de las proposiciones y demostraciones de la metamatemática. Dentro del trabajo de Skolem encontramos una búsqueda por satisfacer las expansiones de la fórmula sin cuantificadores, para así afirmar que la fórmula original es demostrable. Esto exhibe la combinación de ideas semánticas y sintácticas en su trabajo. En cambio Herbrand siempre lleva sus investigaciones por un camino sintáctico, siendo para él lo relevante hallar una fórmula dentro de la lógica proposicional equivalente en validez lógica a la fórmula inicial. Vemos como las reglas para eliminar cuantificadores son de suma importancia en el trabajo de ambos autores. Herbrand busca darles el sentido estricto que necesitan para tener cabida en la metamatemática.

Las ideas semánticas que tienen Löwenheim y Skolem son vistas por Herbrand como algo incompleto, pero que pueden ser útiles para su causa. Sin embargo, desde su punto de vista estas necesitan cambiar al sentido estricto de la sintaxis para tener cabida en la metamatemática. Al encontrarse con estas nociones Herbrand no tiene inconveniente en usar y adaptar la técnica propuesta, aunque cree que no están pensadas para utilizarse dentro de la metamatemática. Estas ideas que en principio aparentaban ser confusas, siempre guardaron claridad para Herbrand. De esta manera Herbrand toma ideas rechazadas por otros matemáticos, dándoles la forma necesaria para trabajar con ellas. Lo que hace Herbrand es mostrar cómo ciertas ideas pueden entrar en el campo de los fundamentos argumentando sólo en el terreno de la sintaxis.

Los reclamos que Herbrand le hace a Löwenheim son los mismos que le imputa a Skolem, pues los trabajos de ambos autores contienen ideas semánticas que Herbrand rechaza en el entorno de la metamatemática. Es por esto que el trabajo de Herbrand tiene una mayor precisión, suministrando una demostración más completa de los teoremas enunciados a través de métodos sintácticos.

3.2.4 Intuicionismo: Marco del trabajo de Herbrand

Herbrand hace claro que para él hay una distinción dentro de los métodos que considera dentro de las matemáticas y de aquellos utilizables dentro de la metamatemática. En el caso de Skolem no hay tal distinción, valiéndose en ambas de los mismos métodos. Así, lleva a la metamatemática los métodos constructivistas, acercándolo al punto de vista de Brouwer.

Por otro lado, Herbrand deja ver en sus trabajos que no tuvo información de primera mano acerca de Brouwer; quizá la información la obtuvo en sus conversaciones con von Neumann. En algunas ocasiones la crítica de Herbrand sobre Brouwer toma un sentido caricaturesco, al atribuirle ideas que este rechazaba tajantemente. Un ejemplo de ideas contradictorias sobre Brouwer es aquel con el que empezamos esta sección, en el que Herbrand le atribuye haber propuesto hacer uso de nociones no finitistas dentro de las demostraciones matemáticas, siempre y cuando éstas no se lleven a conclusiones dentro de la metamatemática.

Herbrand empieza a utilizar el término intuicionismo después de su estancia en Alemania en 1930. Con él denota lo mismo que Hilbert denomino finitismo. Para Herbrand, “intuicionismo” tiene un sentido cercano a los métodos usados por Hilbert. Es bastante común que algunos autores de finales de los años veinte y principios de los treinta que seguían el programa de Hilbert buscaran un límite para los métodos intuicionistas, es por esto que Herbrand dedica algunos escritos a definirlos. En la evaluación que hace Herbrand habla de “métodos intuicionistas extremos”, pero nunca dice cuales considerar como “no extremos”. Lo que propone con esta forma “extrema” coincide con los métodos finitistas de Hilbert. Cuando escribe su teorema fundamental, Herbrand aclara que éste y su demostración pertenecen al orden del intuicionismo. Como hemos visto, su teorema está relacionado con las ideas finitistas, pero él considera su trabajo como una mejora del resultado presentado en el teorema de Löwenheim. Esta mejora es en pocas palabras reemplazar la idea de satisfacción de una fórmula por la idea de encontrar una tautología dentro de las expansiones que se generan de la fórmula.

Dentro del trabajo de Herbrand encontramos contradicciones, una de las más importantes es que les pide a los otros autores precisión al definir las nociones semánticas. Cuando en sus trabajos tenemos las mismas nociones en versiones sintácticas que aparentan ser más fiables, sin embargo no consigue aclararlas más que aquellas ideas semánticas que rechaza.

Herbrand tiene una actitud intolerante frente a las nociones que usan en teoría de conjuntos, lo cual le lleva a tomar una actitud incluso más estricta que el mismo Hilbert sobre ciertas cuestiones. Por ejemplo, limita a métodos finististas los estudios sobre lógica matemática, pero cuando toca temas como el de la decisión o la reducción, no va directo al problema sino que lo reformula en términos de demostrabilidad. Con su teorema pretende eliminar el uso de la teoría de conjuntos al tratar con problemas dentro de la metamatemática. Al ser las nociones conjuntistas tan vanas para Herbrand, el problema de la completud semántica de la teoría de la cuantificación no tiene ninguna importancia para él. Sin embargo, sus seguidores más importantes como Dreben, Denton y Scalon, al no tener los mismos prejuicios que Herbrand, les pueden dar a las nociones conjuntistas el uso que hemos analizado en el capítulo 2 de este trabajo. Por ejemplo, los conjuntos infinitos generados por campos finitos provenientes de una fórmula no refutable permiten obtener una interpretación de la fórmula dentro de un dominio numerable, pero Herbrand deja de lado esta conclusión.

3.3 Tres definiciones alternas para las Funciones Recursivas

Una de las bases del constructivismo se halla en la teoría de números; al respecto, una idea central es que todos los argumentos usados deben estar fundamentados en funciones cuyos valores sean calculables en un conjunto dado. A esto lo llaman ser *efectivamente calculable* y las funciones usadas son las funciones recursivas. Estas funciones se convirtieron hacia finales de los años veinte en el centro de atención de los matemáticos que trabajaban en el área de los fundamentos. Es en esta época cuando Skolem publicó un trabajo sobre funciones calculables que no eran recursivas primitivas dando con esto un ejemplo de que ambas nociones no eran lo mismo, lo cual se creía hasta ese momento.

En este entorno Herbrand propuso tres posibles definiciones a fin de extender la clase de funciones recursivas primitivas a una clase más amplia que abarcara la clase de las funciones calculables, a esta nueva clase le llamarían funciones recursivas. Esto lo plasmó en un artículo a principios de 1931, en donde presentó una idea general pidiendo que las funciones a usar fueran efectivamente calculables y las operaciones definidas con anterioridad. Sobre esta primera definición propuesta por Herbrand cabe aclarar que al respecto plantea la posibilidad de hacer un programa para efectuar las operaciones ahí descritas, sin indicar la lista de operaciones que suponía se debían seguir. Hacemos notar que en estas propuestas alternativas de la noción de función recursiva Herbrand le da el uso acostumbrado al intuicionismo como reconocimiento a Hilbert, mas no en el sentido que hoy tiene este término.

Por esas mismas fechas Herbrand le envió una carta a Gödel, donde por segunda vez propuso una definición alternativa de la noción de función recursiva. La definición propuesta es:
"Si F es una función desconocida y $f_1,f_2,...f_k$ son funciones conocidas, entonces al sustituir las f_j en F de todas las maneras posibles tenemos que las funciones así obtenidas tienen solución única para F, por lo

que *F* es una función recursiva.” (Herbrand 1930b) Gödel retomó esta definición en 1934, completándola con dos cláusulas más. Primero que las ecuaciones deben tener la forma canónica y segundo que la lista de operaciones usada al calcular un valor de la función debe ser explicita.

Herbrand hizo la tercera propuesta en el último artículo que escribió, unos días antes de su muerte, donde propone lo siguiente: Podemos introducir un número cualquiera de funciones f_i de modo tal que cumplan las hipótesis siguientes:

i) Las funciones no contienen variables aparentes
ii) Las funciones permiten hacer efectivamente el cálculo de f_i para todo sistema particular de números
iii) Es posible demostrar de manera intuicionista que siempre se obtiene un resultado bien definido.

En esta definición Herbrand introduce una nota aclarando el uso de la palabra “intuicionista”. Explica que al traducir al lenguaje ordinario las funciones, éstas deben ser consideradas como una propiedad de los enteros y no sólo como un símbolo.

Tenemos así que en las tres definiciones hechas por Herbrand, el cálculo efectivo del valor de la función se menciona en la primera y la tercera. En la primera definición el cálculo depende de la definición previa de operaciones, mientras que en la tercera depende de propiedades intuitivas de los enteros y estas son independientes a las propiedades de las operaciones. Es esta nota el único escrito de Herbrand en donde le da crédito a las nociones semánticas. Lo cual se considera como un indicativo de que a la sazón empezaba a considerar nociones que no estaban permitidas dentro del intuicionismo.

En una carta a van Heijenoort, Gödel explica lo que él piensa de las definiciones de Herbrand. Al respecto dice que aunque nunca lo conoció, cree que la definición propuesta implica la existencia de una demostración constructiva de la unicidad de la solución de *F*. Hacemos notar que si la tesis de Church es correcta, entonces la unicidad de esta solución es un hecho y la fórmula puede ser aceptada por los intuicionistas. Gödel además aclara que no ve ningún desacuerdo entre la segunda y tercera definiciones; más bien, pudo haber sido que Herbrand no tuvo el tiempo de ver cómo llevar a cabo los cálculos, no pudiendo advertir que algunas reglas quedan intactas en todos los casos.

Después de analizar las tres definiciones de Herbrand, la opinión de Gödel sobre la primera, fue que parecía poco fundamentada, siendo insuficientes los estudios realizados. La segunda y tercera proposiciones, resultan de gran importancia para lo que él llamaría en sus posteriores trabajos función recursiva general. Gödel comentó que sería una exageración decir que fue Herbrand el que introdujo la noción, pero lo justo es decir que contribuyó de manera fundamental para llegar a la definición.

Las últimas investigaciones de Herbrand sobre las funciones recursivas se vieron cortadas por su muerte prematura, dejando la duda en torno a cuanto más, una mente tan brillante como la suya habría podido aportar a la lógica y las matemáticas.

Bibliografía

[Amor 2006] AMOR, José Alfredo Montaño, Compacidad en la lógica de primer orden y su relación con el Teorema de Completud, Facultad de Ciencias, U.N.A.M., 2006, México.

[Dreben 1964] DREBEN, Burton, y AANDERAA, Stal,, Herbrand Analyzing Functions, Bulletin of the American Mathematical Society No. 70, 1964, USA, pp. 697-698.

[Dreben 1963] DREBEN, Burton, ANDREWS, Peter y AANDERAA, Stal. False lemmas in Herbrand, Bulletin of the American Mathematical Society No. 69, 1963, USA, pp. 699-706.

[Dreben 1970] DREBEN, Burton y DENTON, John. Herbrand-style consistency proofs, Intuitionism and proof. theory (Myhill, Vesley and Kino, editors), North-Holland, Amsterdam, 1970.

[Dreben 1966] DREBEN, Burton y DENTON, John. A supplement to Herbrand, J. Symb. Logic 31, 1966, USA.

DREBEN, Burton, DENTON, John y SCANLON, T.M., The Herbrand theorem and the consistency of number theory (por aparecer).

[Herbrand 1971] HERBRAND, Jacques. Logical Writings, editado y compilado por Warren D. Goldfarb, Harvard University, Dordrecht, Holland, 1971.

[Herbrand 1930] HERBRAND, Jacques. Recherches sur la théorie de la démonstration en Logical Writings, editado y compilado por Warren D. Goldfarb, Harvard University, Dordrecht, Holland, 1971.

[Herbrand 1930b] HERBRAND, Jacques. Les bases de la logique hillbertienne en Logical Writings, editado y compilado por Warren D. Goldfarb, Harvard University, Dordrecht, Holland, 1971.

[Herbrand 1931] HERBRAND, Jacques. Sur le problème fondamental de la logique mathématique en Logical Writings, editado y compilado por Warren D. Goldfarb, Harvard University, Dordrecht, Holland, 1971.

HERSH, Reuben. Some proposals for reviving the philosophy of mathematics en New directions in the philosophy of mathematics, Part I: Challenging Foundations, Anthology edited by Thomas Tymoczko, Birkhäuser Boston, Inc., 1986, pp.1-27.

KLEENE, Stephen Cole. Introduction to metamathematics, Chapter XIII, Herbrand´s Theorem, Van Nostrand, New York, 1952, pp. 242-255.

MENDELSON, Elliott, Introduction to MATHEMATICAL LOGIC, New York, USA, 1964. Litton Educational Publishing, Inc.

[Scanlon 1963] SCANLON, Thomas M, Consistency of number theory via Herbrand´s Theorem, The journal of Symbolic Logic, volumen 3, número 1, USA, 1973

TORRES Alcaraz, Carlos, traducción de "Una nota escrita por Jacques Herbrand acerca de su tesis doctoral (1931)" y "Los principios de la lógica hilbertiana" en Mathesis, Serie II Vol. 1, No. 1, Ene-Jun 2001, Impreso en México, UNAM.

TORRES Alcaraz, Carlos, "La epistemología matemática de Jacques Herbrand (análisis de dos escritos filosóficos)", en Mathesis, Serie II Vol. 1, No. 1, Ene-Jun 2001, Impreso en México, UNAM.

TORRES Alcaraz, Carlos. Notas y apuntes inéditos.

VAN HEIJENOORT, Jean, editor, From Frege to Gödel: A sourcebook in mathematical logic, Cambridge, Mass, 1967.

VAN HEIJENOORT, Jean. El desarrollo de la teoría de la cuantificación, Instituto de Investigaciones Filosóficas, Universidad Nacional Autónoma de México, Cuaderno 32, pp. 17-27, México, 1976.