Universidad Nacional Autónoma de México

Facultad de Ciencias

Verificación Formal en Lógica Modal

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Licenciada en Ciencias de la Computación

PRESENTA:

Estefanía Prieto Larios

TUTOR

Dr. Favio Ezequiel Miranda Perea

CD.MX., 2018

Hoja de Datos del Jurado

1. Datos del alumno
   Prieto Lario Estefanía
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Ciencias de la Computación
   308219319

2. Datos del Tutor
   Dr.
   Favio Ezequiel
   Miranda
   Perea

3. Datos del sinodal 1
   Dr.
   Francisco
   Hernández
   Quiroz

4. Datos del sinodal 2
   Dra.
   Lourdes del Carmen
   González
   Huesca

5. Datos del sinodal 3
   Dr.
   Miguel
   Carrillo
   Barajas

6. Datos del sinodal 4
   M. en C.
   Araceli Liliana
   Reyes
   Cabello

7. Datos del trabajo escrito
   Verificación formal en lógica modal
   60 p.
   2018

Programa de Apoyo a Proyectos para la Innovación y Mejoramiento de la Enseñanza (papime) de la

Universidad Nacional Autónoma de México, en el marco del proyecto:

"Tópicos en Ciencias de la Computación Teórica"
(UNAM-PAPIME, PE102117)

Índice general

Resumen

El objetivo de este trabajo es dar una formalización y demostración de las propiedades de los sistemas *HK4* y *CS4*; probar la validez del teorema de la deducción y la demostración de la equivalencia entre ambos sistemas, todo esto utilizando el asistente de pruebas COQ [27]. Cabe mencionar que tanto la formalización como la demostración de las propiedades no son una tarea sencilla. En primer lugar se debe de proponer una representación de la lógica modal proposicional en el lenguaje del asistente de pruebas. En segundo lugar hay que construir la demostración de las propiedades de los sistemas deductivos. En particular, demostrar propiedades estructurales como *debilitamiento, contracción e intercambio*, conlleva a verificar propiedades básicas que se dan por hecho en las pruebas a papel, pero que en la formalización en el asistente de pruebas deben ser enunciadas y verificadas. Un ejemplo de estas dificultades consiste en la definición de contextos mediante listas, así como la demostración de distintas propiedades de los mismos.

Este trabajo está organizado de la siguiente forma: en el primer capítulo delineamos los objetivos y estructura de este trabajo. En el segundo capítulo se exponen los sistemas axiomáticos y se aborda la discusión del por qué el teorema de la deducción falla en la lógica modal dando pie a la definición del sistema axiomático *HK4* que Hakli y Negri [15] proponen y que cuenta con una extensión de noción usual de prueba para el manejo de suposiciones. Esto permite demostrar el teorema de la deducción.

En el tercer capítulo se expone el sistema de deducción natural para la lógica modal intuicionista que Frank Pfenning y Rowan Davies [24] proponen, en el que emplean la metodología de Martin-Löf que distingue entre los juicios y proposiciones. Se demuestra que cumple las propiedades estructurales de contracción, debilitamiento e intercambio. Así como la necesitación generalizada y ciertas reglas de transferencia de fórmulas entre contextos.

En el cuarto capítulo, se presenta la equivalencia (traducción) entre los sistemas *HK4* y *CS4*. De cuya demostración se obtiene un algoritmo para transformar las pruebas de un sistema a otro.

En el quinto capítulo, se presenta la formalización en COQ de los sistemas con sus propiedades y se muestran las pruebas de los teoremas de equivalencia de los sistemas y el de deducción para lógica modal.

Para finalizar este trabajo, se presenta un capítulo de conclusiones y trabajo a futuro. En este capítulo se encuentra de forma resumida los resultados obtenidos y los problemas que se tuvieron durante el proceso de este trabajo.

Capítulo 1

Introducción

La lógica modal, concebida como el estudio formal de las modalidades, fue inventada en la filosofía en el siglo pasado, aunque el estudio informal de las modalidades puede remontarse mucho antes, a los antiguos griegos. Los primeros operadores modales fueron introducidos para resolver los problemas de la implicación y para obtener lógicas de necesidad y posibilidad; la figura clave aquí fue Clarence Irving Lewis, quien publicó su trabajo en 1918 [21]. Poniendo su idea en notación moderna: tomamos alguna fórmula lógica ϕ, y prefijando con un $\Box$ o un símbolo $\Diamond$ obtenemos las expresiones:

$$\begin{array}{rc} \Box\phi : & \text{“la proposición } \phi \text{ es necesaria”} \\ \Diamond\phi : & \text{“la proposición } \phi \text{ es posible”} \end{array}$$

Es decir, la notación de la caja y del diamante nos permite afirmar fundamentalmente nuevos modos de verdad sobre la información expresada por ϕ, a saber que ϕ es necesaria o posible.

En 1933 Kurt Gödel [14], impulsado por las preocupaciones en las bases de las matemáticas, utilizó operadores modales para formalizar la noción de demostrabilidad matemática[1]. En particular, su trabajo permitió que la lógica intuicionista se redujera a la lógica clásica extendida con un operador de demostrabilidad, y la lógica resultante, resultó ser el sistema $S4$ de Lewis. Un resultado importante, cuyo punto general era el siguiente: las modalidades se estaban utilizando para expresar fundamentalmente nuevos modos de verdad con respecto a una pieza de información. En particular, ahora $\Box\phi$ significa que “ϕ es demostrable”, y $\Diamond\phi$ significa que “ϕ es consistente”. [7]

Estos primeros ejemplos de aplicar modalidades a fórmulas lógicas presentaban un modo novedoso de la verdad, sin embargo esto sólo es la punta del iceberg. La lógica temporal (o lógica de tiempo) se presenta con las modalidades “eventualmente” ó “anterior”. La lógica deóntica permite modalidades como “se permite ” u “obligatorio es”. En la lógica epistémica se hace uso de modalidades como “se sabe que”, ya sea para un agente o grupos de agentes. Y las lógicas condicionales analizan otras especies de razón condicional mucho más allá de la cuenta original de Lewis. Esta forma de pensar sobre la lógica modal y las modalidades proviene del trabajo de algunos de los pioneros más prominentes del campo, incluyendo a G. H. Von Wright, Arthur Prior, Jaakko Hintikka, Hans Kamp, y David Lewis.

[1] Marca el comienzo de la lógica de prueba, establece la diferencia exacta entre el concepto de ”demostrabilidad en un sistema formal específico” y el “demostrable por significado correcto (semántica)”.

Entonces la estafeta pasó a otras disciplinas. En particular, las lógicas temporales, dinámicas y epistémicas [19] encontraron su camino en la informática, inteligencia artificial y teoría de juegos. Las lógicas temporales, tanto de árboles de cómputo (Computation Tree Logic, CTL) [19] como de tiempo lineal (Linear Temporal Logic, LTL) [19], se utilizan ahora en la industria para la verificación automática de hardware y software. Los operadores epistémicos, temporales y condicionales son el principal ingrediente de la programación basada en el conocimiento. Y las lógicas modales de conocimiento, las creencias y los deseos, forman el pilar de la teoría del cómputo distribuido. Los pioneros de métodos modales en cómputo incluyen a Edmund Clarke, Joe Halpern, Zohar Manna, Robin Milner, Rohit Parikh, Amir Pnueli, Vaughan Pratt y muchos otros. Pero de nuevo, la diversidad reina y la creación de nuevos formalismos modales para propósitos novedosos de razonamiento continúa incesante [7].

De manera más precisa una lógica modal es un sistema formal que intenta capturar el comportamiento deductivo de las expresiones "es necesario que" y "es posible que". Las lógicas modales pertenecen al grupo de las llamadas "extensiones de la lógica clásica" o "lógicas extendidas".

Existen diferentes concepciones formales de la lógica [1] por ejemplo: la sintáctica, la semántica y la estructural. La primera es la que constituye hoy en día lo que se conoce como teoría de la demostración, la segunda conforma la teoría de modelos y la tercera es un enfoque que pretende caracterizar un sistema formal por medio de las reglas estructurales que cumplen. Este último enfoque está inspirado en los trabajos de consecuencia lógica de Tarski y aquellos sobre deducción natural de Gentzen.

El presente trabajo se sitúa en la teoría de la prueba estructural y desde esta perspectiva aborda una lógica modal proposicional minimal a través de un sistema de deducción axiomático, su formulación mediante secuentes y la demostración de sus propiedades. En el articulo de Hakli y Negri [15] se hace énfasis en que el teorema de la deducción en lógica modal clásica falla, puesto de lo contrario se podría deducir la fórmula $A \to \Box A$ que es falsa en la semántica. Esto da pie a una discusión acerca de que la regla de inferencia de *necesitación o necesidad* se le da una mala interpretación. Por lo que Hakli y Negri proponen un sistema axiomático extendido con la noción de suposiciones (*HK4*) para así probar que el teorema de la deducción sí es válido en la lógica modal. También prueban que el sistema *HK4* es equivalente al cálculo de secuentes $G3K$.

Si bien los sistemas de axiomas son los usuales para la definición y la metateoría de las lógicas modales, su uso práctico es casi imposible puesto que las derivaciones a partir axiomas son difíciles de construir. En su lugar preferimos utilizar sistemas de deducción natural, en particular elegimos el sistema de deducción natural que proponen Pfenning y Davies [24] donde emplean la metodología de Martin-Löf que consiste en hacer la distinción entre juicios y proposiciones. Este sistema corresponde a una la lógica modal intuicionista que nombraremos *CS4*. Surge entonces de manera natural la pregunta acerca de la equivalencia entre *CS4* y el correspondiente sistema axiomático obtenido al restringir el sistema *HK4* a la lógica intuicionista.

Capítulo 2

Sistemas Axiomáticos estilo Hilbert

El primer prototipo de un sistema axiomático se puede encontrar en "*Los Elementos de Euclides*" que presentan un desarrollo sistemático de la geometría elemental, basado en varios postulados simples acerca de puntos y líneas. Usando estas propiedades y un razonamiento lógico riguroso es como se construye la geometría euclidiana. Pero el concepto lógico del sistema de axiomas fue introducido y formalizado a comienzos del siglo XX por el matemático alemán David Hilbert (quien también esencialmente reescribió gran parte de los elementos de Euclides en un estilo moderno y riguroso) por lo que estas clases de sistemas lógicos se conocen como sistemas axiomáticos estilo Hilbert.

Un sistema axiomático consta de un conjunto de axiomas particulares, por ejemplo los usados en una teoría matemática, y un conjunto de reglas de inferencia que nos permiten demostrar o derivar más información de dichos a partir de los axiomas, cada información nueva se le conoce como teorema.

2.1. Lógica Proposicional

Presentamos un sistema axiomático para la lógica proposicional *HP* de implicaciones sin negación, los axiomas son los siguientes y la única regla de inferencia es el modus ponens:

K : $A \to (B \to A)$

W : $(A \to (A \to B)) \to (A \to B)$

C : $(A \to (B \to C)) \to (B \to (A \to C))$

B : $(B \to C) \to ((A \to B) \to (A \to C))$

y *modus ponens*: De A y $A \to B$ se infiere B.

Una prueba "axiomática" es una secuencia de fórmulas, donde cada una de estas, es instancia de axiomas o es un teorema o bien se sigue de la aplicación de la regla de inferencia. Una fórmula derivada de esta manera es un teorema del sistema axiomático. Es importante destacar que se debe ser capaz de distinguir si una fórmula es o no un axioma para poder aplicar adecuadamente la regla de inferencia y así generar nuevos teoremas.

Un ejemplo de prueba axiomática es la del llamado axioma I $(A \to A)$.

Lema 2.1 (Ax-I)**.** *El axioma $A \to A$, es derivable.*

Demostración. La derivación es a partir de los axiomas K y W. PD. $A \to A$
1. (A → (A → A)) → (A → A) W
2. A → (A → A) K
3. A → A *MP* (1,2) ■

El axioma I representa una fórmula que es intuitivamente válida. Sin embargo, la prueba es demasiado complicada, este es el problema de los sistemas axiomáticos. Dado que solo tenemos los axiomas para iniciar una derivación, las pruebas resultan muy difíciles de construir. Para simplificar esta situación lo usual es echar mano del llamado teorema de la deducción que afirma que para probar una implicación es suficiente suponer el antecedente y derivar el consecuente.

El teorema de la deducción es un metateorema en lógica matemática que establece: Si una fórmula B puede ser derivada a partir del conjunto de fórmulas $\Gamma \cup \{A\}$, entonces $A \to B$ se puede derivar a partir de Γ. Este teorema se enuncia formalmente de la siguiente manera:

$$\text{Si } (\Gamma, A) \vdash B \text{ entonces } \Gamma \vdash (A \to B)$$

A continuación, incluimos dos ejemplos que muestran la ayuda del teorema de la deducción en la construcción de derivaciones en el sistema *HP*. El primer ejemplo es una derivación del Ax-I en el sistema *HP*.

Demostración. Una prueba en el sistema *HP* que usa el teorema de la deducción. Basta probar que A deriva a partir de A.
1. $A \vdash_{HP} A$ *Hip*
2. $\vdash_{HP} A \to A$ por *Teo.Deducción.*

■

Veamos en ejemplo más elaborado.

Ejemplo 2.1. $A \to B \vdash_{HP} C \to (C \to A) \to B$.

Demostración. Prueba por derivación.
Por Teorema de la deducción2.1 basta probar que, $A \to B, C \vdash_{HP} (C \to A) \to B$
Por Teorema de la deducción, basta probar que $A \to B, C, (C \to A) \vdash_{HP} B$

1. $A \to B,\ C,\ C \to A \vdash_{HP} (C \to A) \to (A \to B) \to (C \to B)$ *trans*
2. $A \to B,\ C,\ C \to A \vdash_{HP} C \to A$ *Hip*
3. $A \to B,\ C,\ C \to A \vdash_{HP} (A \to B) \to (C \to B)$ *MP*(1, 2)
4. $A \to B,\ C,\ C \to A \vdash_{HP} A \to B$ *Hip*
5. $A \to B,\ C,\ C \to A \vdash_{HP} (C \to B)$ *MP*(3, 4)
6. $A \to B,\ C,\ C \to A \vdash_{HP} C$ *Hip*

7. $A \to B,\ C,\ C \to A \vdash_{HP} B$ $MP(5, 6)$

■

Obsérvese la importancia del teorema de la deducción en las derivaciones en la lógica proposicional. Sin embargo, ¿Qué sucedería si este teorema no fuera válido?. Por ejemplo la lógica modal está construida a partir de la lógica proposicional, pero se especula que el teorema de la deducción no es válido en este sistema [2, 12]. Más adelante resolveremos esta especulación, pero primero definimos a la lógica modal.

2.2. Lógica Modal

Los sistemas axiomáticos de la lógica modal se construyen modularmente a partir del sistema de lógica proposicional agregando los operadores modales y distintos axiomas que dicten su comportamiento.

El sistema para la lógica modal *normal* más pequeño es llamado sistema $\mathbb{K}$, en honor de Saul Kripke, quien propuso una semántica formal para la lógica modal y consta de:

a. Tautologías proposicionales.
b. Instancias del axioma $\mathbb{K}$ $(\Box(X \to Y) \to (\Box X \to \Box Y))$.
c. Es cerrado bajo las reglas de inferencia modus ponens:
De $(X \to Y)$ y de X se concluye Y, y
d. necesitación: De X se concluye $\Box X$.

Otros sistemas modales más grandes se conforman del sistema normal agregando algunos esquemas axiomáticos y la regla de inferencia *necesitación o necesidad*: De X se concluye $\Box X$.

Los nombres estándar para otros esquemas son:

Esquemas Axiomáticos

Nombre	Fórmula
K	$\Box(X \to Y) \to (\Box X \to \Box Y)$
T	$\Box X \to X$
4	$\Box X \to \Box\Box X$
5	$\Diamond X \to \Box\Diamond X$
D	$\Box X \to \Diamond X$
B	$X \to \Box\Diamond X$

Además, hay toda una clase de lógicas modales que son más débiles que las lógicas modales normales. Estas lógicas axiomatizan, remplazando la regla de *necesidad o necesitación* por la regla de *regularidad* $((X \to Y) \to (\Box X \to \Box Y))$ [7]. Estas lógicas tienen una semántica y procedimientos propios de derivación para las pruebas [7], pero esto no es parte del trabajo presente.

Como ya se dijo, las pruebas en un sistema axiomático generalmente son difíciles de construir ya que se tiene que hallar una instancia de algún axioma para poder partir de este y así, ir construyendo la prueba. Además estos sistemas son poco viables para las aplicaciones computacionales ya que no corresponden al razonamiento lógico matemático cotidiano.

Algunos ejemplos de derivaciones en el sistema estilo Hilbert son los siguientes.

Ejemplo 2.2. $\vdash_{\mathbb{K}} \Box(A \to B) \to \Box(\Box A \to \Box B)$

Demostración. Una derivación en el sistema $\mathbb{K}$.

1.	$\Box(A \to B)$	
2.	$\Box(A \to B) \to (\Box A \to \Box B)$	$\mathbb{K}$
3.	$\Box A \to \Box B$	$MP(1, 2)$
4.	$\Box(\Box A \to \Box B)$	$Nec\ (3)$

■

Ejemplo 2.3. $\vdash_{\mathbb{T}} \Box(A \to B) \to \Box(B \to C) \to \Box(A \to C)$

Demostración. Una derivación en el sistema $\mathbb{T}$.

1.	$\Box(A \to B)$	
2.	$\Box(B \to C)$	
3.	$\Box(A \to B) \to (A \to B)$	$\mathbb{T}$
4.	$A \to B$	$MP(1, 3)$
5.	$\Box(B \to C) \to (B \to C)$	$\mathbb{T}$
6.	$B \to C$	$MP(2, 5)$
7.	$(B \to C) \to (A \to B) \to (A \to C)$	B
8.	$(A \to B) \to (A \to C)$	$MP\ (6, 7)$
9.	$A \to C$	$MP(8, 4)$
10.	$\Box(A \to C)$	$Nec\ (9)$

■

Si el teorema de la deducción es válido para sistemas normales de la lógica modal, entonces, de las derivaciones de los dos ejemplos anteriores podemos concluir respectivamente que $\vdash_{\mathbb{K}} \Box(A \to B) \to \Box(\Box A \to \Box B)$ y $\vdash_{\mathbb{T}} \Box(A \to B) \to (\Box(B \to C) \to \Box(A \to C))$. Esto ejemplifica la importancia de que el teorema de la deducción sea válido en la lógica modal.

2.3. Teorema de la Deducción en Lógica Modal

Los sistemas estilo Hilbert para lógica modal se conforman por esquemas de axiomas y reglas de inferencia, *modus ponens* y la regla de *necesitación o necesidad*. Se afirman en varias fuentes [2, 8], que el teorema de la deducción en la forma usual que se representa, no es válido en lógicas modales que contienen la regla de necesitación: De A se infiere $\Box A$. Después de analizar los argumentos que afirman la invalidez del teorema de la deducción en lógicas modales, observaremos que el problema con este teorema, en lógica modal, surge de la interpretación de la derivabilidad a partir del conjunto de fórmulas en un sistema axiomático.

La primera interpretación errónea afirma que la regla de necesitación

$$\frac{\text{A}}{\Box A}\text{ Admite la derivación } A \vdash \Box A$$

Sin embargo, $A \to \Box A$ no es un teorema, invalidando así el teorema de la deducción. Pero el significado real de la regla es: Si A es un teorema entonces $\Box A$ también es un teorema. Es decir, $\vdash \Box A$ siempre que $\vdash A$.

Otra interpretación errónea consiste en entender la derivabilidad a partir del conjunto de fórmulas en un sistema axiomático como la adición de éstas al conjunto de axiomas. Supóngase que se quiere demostrar que $A \to \Box A$ en algún sistema estilo Hilbert modal en el que se cumple el teorema de la deducción, a partir de $A \vdash \Box A$.

Por demostrar: $A \to \Box A$ suponiendo que el Teorema de la deducción es válido en K.

Demostración. $A \vdash_{\mathbb{K}} \Box A$

1. A — *supuesto.*
2. $\Box A$ — *Nec*(1)
3. $A \to \Box A$ — *Teo.Deducción.*(2)

■

Si se agrega A a la lista de axiomas, entonces se puede aplicar la regla de necesidad y concluir $\Box A$ a partir de A, es decir $A \to \Box A$. Sin embargo, esto es no válido.

El problema radica en que en los sistemas estilo Hilbert admiten sólo axiomas, tautologías o teoremas como hipótesis, por lo que en las reglas de inferencia garantizan la correctud de la regla de necesidad. De aquí que, si se considera cualquier hipótesis como axioma o teorema y se emplea la regla de necesidad sin restricción, se puede inferir $\Box A$ a partir de A, y la formulación del teorema de la deducción, falla.

Melvin Fitting [10] propone hacer una modificación a la derivabilidad de tal forma que se realice una distinción entre dos tipos de premisas de tal forma que la regla de necesitación se aplique sólo a uno de estos tipos. Se distingue entre *premisas globales* y *premisas locales*: las primeras son los esquemas axiomáticos o bien tautologías. Las segundas refieren a verdades contingentes. La regla de necesitación o necesidad sólo debe ser aplicada a las premisas globales.

2.4. Sistemas de Hilbert con hipótesis

El problema recién discutido se resuelve al dar una definición formal con un sistema de Hilbert con hipótesis como sigue.

Definición 2.1 (Contexto). *Un contexto (de hipótesis) está definido como:*

$$\Gamma ::= \cdot \mid \Gamma,\ A$$

Asumimos las siguientes convenciones para contextos:

- El contexto vacío se denota por $\cdot$
- La operación de agregar al final la fórmula A al contexto Γ, se denota por Γ, A.
- El operador *;* corresponde a la unión de contextos. Obsérvese que esta operación no es conmutativa pero sí asociativa.
- Se entenderá por Γ, A, B a $((\Gamma, A)$, B).
- Se entenderá por $\Gamma; \Delta; \Pi$ a $((\Gamma; \Delta); \Pi)$.
- Se entenderá por $\Gamma, A; \Delta$ a $(\Gamma, A); \Delta$.

Una de las propiedades sobresalientes de los contextos es la descomposición.

Lema 2.2 (Descomposición de contextos). *Si $\Gamma;\ \Delta\ =\ \Pi,\ A$ entonces ($\Delta\ =\ \cdot$ y $\Gamma\ =\ \Pi,\ A$) ó $\exists\Gamma'',\ \Delta\ =\ \Gamma'',\ A$*

Demostración. Análisis de casos sobre Δ.

Caso 1.
Si $\Delta = \cdot$ y $\Gamma; \cdot = \Pi, A$ entonces $\Gamma = \Pi, A$.

Caso 2. Si $\Delta = \Delta', p$ y $\Gamma; (\Delta', p) = \Pi, A$ PD. $\exists\Gamma'$, $\Delta', p = \Pi, A$.

Por hipótesis se tiene que $\Gamma; (\Delta', p) = \Pi, A$ esto es equivalente a $(\Gamma; \Delta'), p = \Pi, A$.

Entonces $(\Gamma; \Delta') = \Pi$ y $p = A$.
Como $p = A$ se tiene que $\Delta', A = \Gamma', A$ entonces $\Delta' = \Gamma'$ y $A = A$.
Por lo tanto, la Γ' que existe es, $\Delta' = \Gamma'$, $p = A$ entonces $\Delta', p = \Delta', A$. ■

Es importante observar que esta definición de contextos es meramente sintáctica, si bien corresponde a listas finitas. La razón de usar esta clase de definiciones facilitan su implementación y verificación en el asistente de pruebas.

Definición 2.2 (Derivación con suposiciones en lógica axiomática). *Una fórmula A es derivable de algún contexto Γ en el sistema S de la lógica axiomática si:*

- *A es una instancia de algún axioma.*

- *A está en el contexto.*

- *$B \to A$ es derivable en HK4 del contexto Δ, B es derivable en S del contexto Θ, y Γ es Δ; Θ*

- *$A = \Box B$ y B es derivable en S a partir del contexto vacío.*

En este sistema de derivación con suposiciones, la regla de modus ponens se escribe de la siguiente forma:

$$\frac{\Delta \vdash (A \to B) \qquad \Theta \vdash A}{\Delta; \Theta \vdash B}\,\text{MP}$$

y la regla *necesitación* es:

$$\frac{\cdot \vdash A}{\Gamma \vdash \Box A}\,\text{Nec}$$

La regla de modus ponens une, en la conclusión, los contextos de las derivaciones de las premisas ($\Gamma = \Delta; \Theta$) [26]. Debido a esto, se dice que esta regla es *"multiplicativa"* [16] y más informativa, porque el contexto Γ exhibe de dónde provienen cada una de las premisas. Se observa que esta regla de *modus ponens* es distinta a la correspondiente en deducción natural, la regla de eliminación de la implicación, que sólo utiliza un contexto:

$$\frac{\Gamma \vdash (A \to B) \qquad \Gamma \vdash A}{\Gamma \vdash B}$$

entonces, ¿Cuál es la diferencia entre entre la regla de modus ponens de un sistema de deducción axiomático con suposiciones y la regla MP de un sistema de deducción natural?. Veamos un ejemplo:

Ejemplo 2.4. $A \to B \vdash C \to (C \to A) \to B$

Modus ponens en un sistema de deducción axiomático con suposiciones
Demostración.

1. $\cdot \vdash (C \to A) \to (A \to B) \to (C \to B)$ *trans*
2. $C \to A \vdash C \to A$ *Hip*
3. $C \to A \vdash (A \to B) \to (C \to B)$ $MP(1, 2)$
4. $A \to B \vdash A \to B$ *Hip*
5. $C \to A,\, A \to B \vdash (C \to B)$ $MP(3, 4)$
6. $C \vdash C$ *Hip*
7. $C \to A,\, A \to B, C \vdash B$ $MP(5, 6)$
8. $A \to B,\, C \vdash (C \to A) \to B$ *Teo.Deducción.* (7)

9. $A \to B \vdash C \to (C \to A) \to B$ *Teo.Deducción.* (8)

■

Veamos ahora la derivación de la misma fórmula en un sistema de deducción natural.

Por Introducción de la implicación, basta probar que, $A \to B, C \vdash (C \to A) \to B$
Por Introducción de la implicación, basta probar que, $A \to B, C, (C \to A) \vdash B$

1. $A \to B,\ C,\ C \to A \vdash (C \to A) \to (A \to B) \to (C \to B)$ *trans*
2. $A \to B,\ C,\ C \to A \vdash C \to A$ *Hip*
3. $A \to B,\ C,\ C \to A \vdash (A \to B) \to (C \to B)$ $(\to E)$(1, 2)
4. $A \to B,\ C,\ C \to A \vdash A \to B$ (*Hip*)
5. $A \to B,\ C,\ C \to A \vdash (C \to B)$ $(\to E)$ (3, 4)
6. $A \to B,\ C,\ C \to A \vdash C$ *Hip*
7. $A \to B,\ C,\ C \to A \vdash B$ $(\to E)$ (5, 6)

■

Como se ve en el paso dos de la prueba, se tienen 2 hipótesis extras, $A \to B$ y C, que no se usan. Por lo tanto la noción multiplicativa del modus ponens, contiene un control más estricto de las hipótesis que se usan.

Ya podemos definir un sistema axiomático con hipótesis para la lógica modal, el cual ayudará a aclarar la controversia del teorema de la deducción.

2.5. Sistema axiomático estilo Hilbert (*HK4*)

Para los objetivos de este trabajo, usamos un sistema estilo Hilbert con hipótesis para la lógica modal, *HK4*, que se define como sigue:

La primera regla es la regla de hipótesis:

$$\frac{A \in \Gamma}{\Gamma \vdash_{HK4} A}\ Hip$$

Esta regla nos dice que si A es una hipótesis en Γ entonces A es derivable a partir de Γ.

La siguiente regla corresponde a los esquemas axiomáticos:

$$\frac{A \in Axioms}{\Gamma \vdash_{HK4} A}\ Ax$$

La regla *axioms* afirma que si A es una instancia de algún axioma entonces se puede derivar bajo cualquier Γ.

La regla *modus ponens*, dado que $A \to B$ es derivable bajo Δ y A bajo Γ, se infiere que B es derivable a partir de Δ y Γ.

$$\frac{\Gamma \vdash_{HK4} A \qquad \Delta \vdash_{HK4} (A \to B)}{\Gamma; \Delta \vdash_{HK4} B}\text{MP}$$

La regla de *necesitación* dice, a partir de A se infiere $\Box A$. Anteriormente se expusieron los problemas con esta regla y el teorema de la deducción. Por ello, Hakli y Negri [15] proponen la modificación de esta como:

$$\frac{\cdot \vdash_{HK4} A}{\Gamma \vdash_{HK4} \Box A}\,Nec$$

Cabe destacar que sólo se puede utilizar esta regla si A es teorema, es decir si A es derivable a partir del contexto vacío. De otra forma, se recurre al error que este trabajo justifica.

Resumiendo las reglas del sistema *HK4* son:

$$\frac{A \in \Gamma}{\Gamma \vdash_{HK4} A} \qquad \frac{A \in Axioms}{\Gamma \vdash_{HK4} A}$$

$$\frac{\Gamma \vdash_{HK4} A \qquad \Delta \vdash_{HK4} (A \to B)}{\Gamma; \Delta \vdash_{HK4} B}\text{MP} \qquad \frac{\cdot \vdash_{HK4} A}{\Gamma \vdash_{HK4} \Box A}\text{Nec}$$

La definición del sistema *HK4* da solución al problema de la interpretación de la regla *Nec* y con ello, se resuelve la controversia del teorema de la deducción.

Teorema 2.1 (Teorema de la Deducción)**.** *Si* $\Gamma, A \vdash_{HK4} B$ *entonces* $\Gamma \vdash_{HK4} (A \to B)$.

Demostración. Inducción sobre la derivación $\Gamma, A \vdash B$.

Caso 1: Si $A_0 \in \Gamma$, A $\quad \Gamma \vdash_{HK4} A \to A_0$

Si $A_0 \in \Gamma$, A entonces $A_0 \in \Gamma$ o $A_0 = A$.

subcaso 1:
PD. Si $A_0 = A$

Como $A_0 = A$ entonces $\Gamma \vdash_{HK4} A \to A$, pero esto es una instancia del Ax-I (2.1).

subcaso 2: Si $A_0 \in \Gamma$
Como $A_0 \in \Gamma$ entonces $\Gamma \vdash_{HK4} A_0$. Se toma una instancia del K y se aplica la regla *modus ponens* y se concluye $A \to A_0$.

1. $\cdot \vdash_{HK4} A_0 \to (A \to A_0)$ *K*
2. $\Gamma \vdash_{HK4} A_0$ *Hip*

3. $\Gamma; \cdot \vdash_{HK4} A \to A_0$ $MP(1, 2)$

4. $\Gamma \vdash_{HK4} A \to A_0$.

Caso 2: Si $A \in Axioms$

subcaso 1:
PD. $\Gamma \vdash_{HK4} A \to (A_0 \to B \to A_0)$

1. $\cdot \vdash_{HK4} (A_0 \to B \to A_0) \to (A \to (A_0 \to (B \to A_0)))$ K

2. $\Gamma \vdash_{HK4} A_0 \to (B \to A_0)$ K

3. $\Gamma; \cdot \vdash_{HK4} (A \to (A_0 \to (B \to A_0))$ $MP(1, 2)$

4. $\Gamma \vdash_{HK4} (A \to A_0 \to B \to A_0)$

subcaso 2:
PD. $\Gamma \vdash_{HK4} (A \to (A_0 \to A_0 \to B) \to (A_0 \to B))$

1. $\Gamma \vdash_{HK4} (A_0 \to (A_0 \to B)) \to (A_0 \to B)$ W

2. $\cdot \vdash_{HK4} (((A_0 \to (A_0 \to B)) \to (A_0 \to B)) \to$
   $A \to ((A_0 \to A_0 \to B) \to (A_0 \to B))$ K

3. $\Gamma; \cdot \vdash_{HK4} A \to (A_0 \to A_0 \to B) \to A_0 \to B)$ $MP(1, 2)$

4. $\Gamma \vdash_{HK4} A \to (A_0 \to A_0 \to B) \to A_0 \to B)$

Los demás casos son análogos. Se toma una instancia del axioma K. Se utiliza el axioma por demostrar para aplicar *modus ponens* y se pueda concluir lo que se quiere.

Caso 3: Si A es derivada a partir de aplicar la regla *MP*.

Hipótesis

1. $\Gamma_0 \vdash_{HK4} A_0$

2. $\Gamma' \vdash_{HK4} A_0 \to B$

3. $\mathrm{H.I}_1 : \Gamma_0 = \Gamma$, A $\to \Gamma \vdash_{HK4} A \to A_0$

4. $\mathrm{H.I}_2 : \Gamma' = \Gamma$, A $\to \Gamma \vdash_{HK4} A \to (A_0 \to B)$

5. $\Gamma'; \Gamma_0 = \Gamma$, A

Por el lema descomposición de contextos en 5, se tiene que ($\Gamma_0 = \cdot$ y $\Gamma' = \Gamma$, A) o $\exists \Gamma''$, $\Gamma_0 = \Gamma''$, A.

subcaso 1: $\Gamma_0 = \cdot$ y $\Gamma' = \Gamma$, A

1. Como $\Gamma' = \Gamma$, A , sustituimos en Hip_2, se tiene $\Gamma', A \vdash_{HK4} A_0 \to B$

2. Por $H.I_2$ en (1) se tiene $\Gamma \vdash_{HK4} A \to (A_0 \to B)$

3. Sea $\cdot \vdash_{HK4} (A \to (A_0 \to B)) \to (A_0 \to (A \to B))$ C

4. $\Gamma \vdash_{HK4} A_0 \to (A \to B))$ $MP(3, 2)$

5. Como $\Gamma_0 = \cdot$, sustituimos en Hip_1 se tiene $\vdash_{HK4} A_0$

6. $\Gamma \vdash_{HK4} A \to B$ $MP(4, 5)$

subcaso 2: $\exists \Gamma''$, $\Gamma_0 = \Gamma''$, A

1. Como $\Gamma_0 = (\Gamma''$, A). Sustituimos Γ_0 en $H.I_1$ se tiene que $\Gamma'' \vdash_{HK4} A \to A_0$

2. Sea $\Gamma'; \Gamma_0 = \Gamma$, A, sustituimos a Γ_0 por Γ'', A, se tiene $\Gamma'; (\Gamma''$, A) $= \Gamma$, A lo que sigue por $\Gamma'; \Gamma'' = \Gamma$.

3. $\cdot \vdash_{HK4} (A_0 \to B) \to ((A \to A_0) \to (A \to B))$ B

4. $\Gamma' \vdash_{HK4} (A \to A_0) \to (A \to B)$ $MP(3, \text{Hip}_2)$

5. $\Gamma'; \Gamma'' \vdash_{HK4} A \to B$ $MP(4, 1)$

6. $\Gamma \vdash_{HK4} A \to B$

El caso delicado que corresponde a la regla de necesitación:

Caso 4: Si A es derivada a partir de aplicar la regla *Nec*.
Si $\cdot \vdash A_0$ PD. $\Gamma \vdash_{HK4} (A \to \Box A_0)$

1. $\cdot \vdash_{HK4} A_0$ *supuesto*

2. $\cdot \vdash_{HK4} (\Box A_0 \to (A \to \Box A_0))$ K

3. $\Gamma \vdash_{HK4} \Box A_0$ *Nec* (1)

4. $\Gamma; \cdot \vdash_{HK4} (A \to \Box A_0)$ *MP* (2, 3)

5. $\Gamma \vdash_{HK4} (A \to \Box A_0)$

■

Con esto se confirma la validez del teorema de la deducción y en adelante los podremos usar como una regla adicional de derivación. Más aun el inverso de este teorema es válido en *HK4*.

Teorema 2.2 (Teorema de la Deducción inverso)**.** *Si* $\Gamma \vdash_{HK4} A \to B$ *entonces* Γ*,* $A \vdash_{HK4} B$

Demostración. Prueba por derivación.

1. A $\vdash_{HK4} A$ *Hip*

2. $\Gamma \vdash_{HK4} A \to B$ *supuesto*

3. Γ, A $\vdash_{HK4} B$ $MP(2, 1)$

■

Obsérvese que como la regla de modus ponens es multiplicativa no fue necesario usar utilizar la regla estructural de debilitamiento.

2.5.1. Propiedades estructurales sobre *HK4*

En esta sección expondremos algunas propiedades estructurales que nos serán de utilidad más adelante.

Proposición 2.1. El sistema *HK4* satisface la ley de debilitamiento por la derecha e izquierda:

$$\textit{Si } \Gamma \vdash_{Hk4} A \textit{ entonces } \Gamma; \Gamma' \vdash_{Hk4} A$$
$$\textit{Si } \Gamma \vdash_{Hk4} A \textit{ entonces } \Gamma'; \Gamma \vdash_{Hk4} A$$

Demostración. Inducción sobre la derivación de A.
Casos Base:

- Si $A \in \Gamma$ PD. $\Gamma; \Gamma' \vdash_{HK4} A$
  Como $A \in \Gamma$ entonces $\Gamma \vdash_{HK4} A$ pero esto es equivalente a $\Gamma; \cdot \vdash_{HK4} A$ por lo que $\cdot = \Gamma'$.

- Si $A \in Axioms$ PD. $\Gamma; \Gamma' \vdash_{HK4} A$
  Como A es un axioma, entonces se cumple para cualquier contexto.

Hipótesis:

1. $\Gamma \vdash A$
2. $\Gamma_0 \vdash A \to B$
3. H.I_1 $\Gamma; \Gamma' \vdash A$
4. H.I_2 $\Gamma_0; \Gamma' \vdash A \to B$

Sea $\Gamma \vdash A$ y $\Gamma_0 \vdash A \to B$ PD. $(\Gamma_0; \Gamma); \Gamma' \vdash B$

1. $\Gamma_0 \vdash A \to B$ *supuesto*
2. $\Gamma_0; (\Gamma; \Gamma') \vdash B$ *MP* (1, H.I_1)
3. $(\Gamma_0; \Gamma); \Gamma' \vdash B$ *asoc.*

■

El otro caso es análogo.

Veamos que la regla de contracción también es admisible.

Proposición 2.2. El sistema satisface la ley de contracción:

$$\text{Si } (\Gamma', \text{A}), \text{A} \vdash_{HK4} B \text{ entonces } \Gamma', \text{A} \vdash_{HK4} B$$

Demostración. Prueba por derivación.

1. $(\Gamma', \text{A}), \text{A} \vdash_{HK4} B$ *supuesto*
2. $\Gamma', \text{A} \vdash_{HK4} A \to B$ *Teo.Deducción.* (1)

3. $\Gamma' \vdash_{HK4} A \to A \to B$ *Teo.Deducción.*(2)

4. $\cdot \vdash_{HK4} (A \to A \to B) \to (A \to B)$ W

5. $\Gamma' \vdash_{HK4} A \to B$ *MP*(4, 3)

6. Γ', A $\vdash_{HK4} B$ *Teo.Ded.Inv.* (5)

■

Dado que el sistema cumple con la ley de contracción con dos proposiciones, entonces surge el siguiente corolario.

Denotamos con A^n al contexto que tiene n presencias de A, es decir $A^n =_{def} (A, A, ..., A)$ con A n-veces.

Corolario 2.1. *Si* Γ*;* $A^n \vdash_{HK4} B$ *entonces* $\Gamma \vdash A \to B$

Demostración. Inducción sobre n.
Caso base:

1. $\Gamma \vdash_{HK4} B$ *supuesto*

2. $\cdot \vdash_{HK4} (B \to (A \to B))$ K

3. $\Gamma \vdash_{HK4} A \to B$ *MP* (1, 2)

H.I : Si $\Gamma; A^n$ entonces $\Gamma \vdash_{HK4} A \to B$

Caso Inductivo:
Sea $\Gamma, A^{n+1} \vdash_{HK4}$ B PD. $\Gamma \vdash_{HK4} A \to B$

1. Γ, A$^{n+1} \vdash_{HK4}$ B *supuesto*

2. Γ, A$^n, A \vdash_{HK4}$ B *equivalencia* (1)

3. $\Gamma, A \vdash_{HK4} A \to B$ *H.I* (2)

4. $\Gamma \vdash_{HK4} A \to A \to B$ *Teo.Deducción.* (3)

5. Sea $\cdot \vdash_{HK4} (A \to A \to B) \to (A \to B)$ W

6. $\Gamma \vdash A \to B$ *MP* (4, 5)

■

A continuación mostramos que la muy importante la regla de corte también es admisible en *HK4*.

Lema 2.3. *Si* $\Gamma \vdash_{HK4} A$ *y* $\Gamma', A \vdash B$ *entonces* Γ*;* $\Gamma' \vdash_{HK4} B$

Demostración. Prueba por derivación.

1. $\Gamma \vdash_{HK4} A$ *supuesto*

2. $\Gamma', A \vdash_{HK4} B$ *supuesto*

3. $\Gamma' \vdash_{HK4} A \rightarrow B$ *Teo.Deducción.*(2)

4. $\Gamma'; \Gamma \vdash_{HK4} B$ *MP* (3, 1)

■

Si bien el teorema de la deducción proporciona una fuerte herramienta para simplificar derivaciones, su aplicación queda restringida debido a que la única hipótesis que es posible descargar, es la que se encuentra al final del contexto. [1] Aparentemente esto es una desventaja del uso de listas, en vez de conjuntos o multiconjuntos para los contextos. A continuación vemos que esto no es así.

Teorema 2.3 (Teorema de la Deducción Generalizado en Premisas)**.** *Si (*Γ*, A); *$\Gamma' \vdash_{HK4} B$ *entonces* Γ *;* $\Gamma' \vdash_{HK4} A \rightarrow B$

Demostración. Inducción sobre Γ'.
Caso base: Si (Γ, A); $\cdot \vdash_{HK4} B$ PD. $\Gamma; \cdot \vdash_{HK4} A \rightarrow B$

1. (Γ, A); $\cdot \vdash_{HK4} B$ *supuesto*

2. $\Gamma, A \vdash_{HK4} B$

3. $\Gamma \vdash_{HK4} A \rightarrow B$ *Teo.Deducción.* (2)

H.I : Si $(\Gamma, A); \Gamma' \vdash_{HK4} B$ entonces $\Gamma; \Gamma \vdash_{HK4} A \rightarrow B$
Caso inductivo:
Sea (Γ, A) ; (Γ', p) $\vdash_{HK4} B$ PD. $(\Gamma; (\Gamma', p)) \vdash_{HK4} A \rightarrow B$

1. (Γ, A) ; (Γ'', p) $\vdash_{HK4} B$ *supuesto*

2. ((Γ, A) ;Γ''), p $\vdash_{HK4} B$

3. (Γ, A); $\Gamma'' \vdash_{HK4} p \rightarrow B$ *Teo.Deducción.* (2)

4. Γ ; $\Gamma'' \vdash_{HK4} A \rightarrow p \rightarrow B$ *H.I* (3)

5. $\cdot \vdash_{HK4} (A \rightarrow p \rightarrow B) \rightarrow (p \rightarrow A \rightarrow B)$ *C*

6. Γ ; $\Gamma'' \vdash_{HK4} p \rightarrow A \rightarrow B$ *MP* (4, 5)

7. Γ ; Γ'', p $\vdash_{HK4} A \rightarrow B$ *Teo.Ded.Inv.* (6)

8. Γ ; (Γ'', p) $\vdash_{HK4} A \rightarrow B$

■

Una aplicación de este teorema corresponde a la siguiente regla estructural de permutación.

Lema 2.4 (Permutación de contextos)**.** *Si* $\Gamma; \Gamma' \vdash_{HK4} A$ *entonces* $\Gamma'; \Gamma \vdash_{HK4} A$

[1] Recuérdese que los contextos son listas, por lo que el orden es las hipótesis es relevante.

Demostración. Inducción sobre Γ.
Caso Base: $\Gamma = \cdot$.
Este caso es claro puesto que $\cdot; \Gamma' = \Gamma'; \cdot$ que es Γ'.

H.I: Si $\Gamma; \Gamma' \vdash_{HK4} A$ entonces $\Gamma'; \Gamma \vdash_{HK4} A$

Caso Inductivo: $\Gamma = (\Delta, p)$.
Sea $(\Delta, p); \Gamma' \vdash_{HK4} A$ PD. $\Gamma'; (\Delta, p) \vdash_{HK4} A$.

1. $(\Delta, p); \Gamma' \vdash_{HK4} A$ *supuesto*
2. $\Delta; \Gamma' \vdash_{HK4} p \to A$ *Teo.Ded.Gen.Prem* (1)
3. $\Gamma'; \Delta \vdash_{HK4} p \to A$ *H.I* (2)
4. $\Gamma'; \Delta, p \vdash_{HK4} A$ *Teo.Ded.Inv.* (3)

■

La permutación de contextos junto con otras propiedades nos permite demostrar la siguiente generalización de la regla de necesitación.

Definición 2.3. *Sea Δ un contexto, digamos $\Delta = B_1, B_2, .., B_k$, entonces definimos $\Delta^{\Box} =_{def} \Box B_1, \Box B_2, \ldots, \Box B_k$.*

Proposición 2.3 (Necesitación generalizada)**.** Si $\Delta^{\Box} \vdash_{HK4} A$ entonces $\Delta^{\Box}; \Gamma \vdash_{HK4} \Box A$.

Demostración. Inducción sobre Δ.
Caso base:
Es claro que $(\cdot)^{\Box} = \cdot$

1. $(\cdot)^{\Box} \vdash_{HK4} A$ *supuesto*
2. $\Delta^{\Box}; \Gamma \vdash_{HK4} \Box A$ *Nec* (2)

H.I: Si $\Delta^{\Box} \vdash_{HK4} A$ entonces $\Delta^{\Box}; \Gamma \vdash_{HK4} \Box A$

Caso inductivo: Sea $(\Delta, \text{p})^{\Box} \vdash_{HK4} A$ PD. $(\Delta, p)^{\Box}; \Gamma \vdash_{HK4} \Box A$

1. $(\Delta, \text{p})^{\Box} \vdash_{HK4} A$ *supuesto*
2. $\Delta^{\Box} \vdash_{HK4} \Box p \to A$ *Teo.Deducción.* (1)
3. $\Delta^{\Box}; \Gamma \vdash_{HK4} \Box(\Box p \to A)$ *H.I* (3)
4. $\cdot \vdash_{HK4} \Box(\Box p \to A) \to (\Box\Box p \to \Box A)$ $\mathbb{K}$
5. $\Delta^{\Box}; \Gamma \vdash_{HK4} (\Box\Box p \to \Box A)$ *MP* (4, 3)
6. $\Delta^{\Box}; \Gamma \vdash_{HK4} \Box p \to \Box\Box p$ 4
7. $\Delta^{\Box}; \Gamma \vdash_{HK4} (\Box p \to \Box A)$ *trans* (6, 5)

8. $\Gamma; \Delta^{\Box} \vdash_{HK4} (\Box p \rightarrow \Box A)$ *Lema* 2.4

9. $\Gamma; \Delta^{\Box}, \Box p \vdash_{HK4} \Box A$ *Teo.Ded.Inv.* (8)

10. $\Gamma; (\Delta^{\Box}, \Box p) \vdash_{HK4} \Box A$

11. $(\Delta^{\Box}, \Box p); \Gamma \vdash_{HK4} \Box A$ *Lema* 2.4 (10)

■

Terminamos esta sección haciendo un resumen de todas las propiedades anteriores utilizándolas como reglas de derivación.

Reglas de derivación del sistema *HK4*

$$\frac{A \in \Gamma}{\Gamma \vdash_{HK4} A}\text{Hip} \qquad \frac{A \in Axioms}{\Gamma \vdash_{HK4} A} \qquad \frac{\Gamma \vdash_{HK4} A \qquad \Delta \vdash_{HK4} (A \rightarrow B)}{\Gamma, \Delta \vdash_{HK4} B}\text{MP}$$

$$\frac{\cdot \vdash_{HK4} A}{\Gamma \vdash_{HK4} \Box A}\text{Nec} \qquad \frac{\Gamma, A \vdash_{HK4} B}{\Gamma \vdash_{HK4} A \rightarrow B}\text{Teo.Dec}$$

$$\frac{\Gamma \vdash_{HK4} A \rightarrow B}{\Gamma, A \vdash_{HK4} B}\text{Teo.Dec. Inv} \qquad \frac{(\Gamma, A); \Gamma' \vdash_{HK4} B}{\Gamma; \Gamma' \vdash_{HK4} A \rightarrow B}\text{Teo.Dec.Gen.Prem}$$

$$\frac{\Delta^{\Box} \vdash_{HK4} A}{\Delta^{\Box}; \Gamma \vdash_{HK4} \Box A}\text{NecGen} \qquad \frac{\Gamma \vdash_{HK4} A}{\Gamma; \Gamma' \vdash_{HK4} A}\text{Debilitamiento\_R}$$

$$\frac{\Gamma \vdash_{HK4} A}{\Gamma'; \Gamma \vdash_{HK4} A}\text{Debilitamiento\_L} \qquad \frac{\Gamma; \Gamma' \vdash_{HK4} A}{\Gamma'; \Gamma \vdash_{HK4} A}\text{Perm\_ctx}$$

2.6. Derivaciones usando *HK4*

En esta sección se presentarán algunas derivaciones con el sistema *HK4*.

Ejemplo 2.5 (Distributividad de la implicación sobre la implicación)**.** $\cdot \vdash_{HK4} (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

Demostración. Prueba por derivación.
Por el Teorema de la deducción, basta probar que,
$(A \to (B \to C)) \vdash_{HK4} ((A \to B) \to (A \to C))$.
Por el Teorema de la deducción, basta probar que, $(A \to (B \to C)), (A \to B) \vdash_{HK4} (A \to C)$.
Por el Teorema de la deducción, basta probar que, $(A \to (B \to C)), (A \to B), A \vdash_{HK4} C$.

1. $(A \to (B \to C)) \vdash_{HK4} (A \to (B \to C))$ *Hip*
2. $(A \to B) \vdash_{HK4} A \to B$ *Hip*
3. $A \vdash A$ *Hip*
4. $(A \to B), A \vdash_{HK4} B$ *MP* (3, 2)
5. $(A \to (B \to C)), A \vdash_{HK4} B \to C$ *MP* (1, 3)
6. $(A \to (B \to C)), (A \to B), A, A \vdash_{HK4} C$ *MP* (5, 4)
7. $(A \to (B \to C)), (A \to B), A \vdash_{HK4} C$ *contracción (6)*
8. $(A \to (B \to C)), (A \to B) \vdash_{HK4} (A \to C)$ *Teo.Deducción.* (7)
9. $(A \to (B \to C)) \vdash_{HK4} ((A \to B) \to (A \to C))$ *Teo.Deducción.* (8)
10. $\vdash_{HK4} (A \to (B \to C)) \to ((A \to B) \to (A \to C))$ *Teo.Deducción.* (9)

$\blacksquare$

Ejemplo 2.6. $\cdot \vdash_{HK4} \Box(A \to B) \to \Box(B \to C) \to \Box(A \to C)$

Demostración. Prueba por derivación.
Por el Teorema de la deducción, basta probar que, $\Box(A \to B) \vdash_{HK4} \Box(B \to C) \to \Box(A \to C)$.
Por el Teorema de la deducción, basta probar que, $\Box(A \to B), \Box(B \to C) \vdash_{HK4} \Box(A \to C)$.

1. $\Box(A \to B), \Box(B \to C) \vdash_{HK4} \Box(A \to B)$ *Hip*
2. $\Box(A \to B), \Box(B \to C) \vdash_{HK4} \Box(B \to C)$ *Hip*
3. $\cdot \vdash_{HK4} \Box(A \to B) \to (A \to B)$ $\mathbb{T}$
4. $\Box(A \to B), \Box(B \to C) \vdash_{HK4} (A \to B)$ *MP* (3, 1)
5. $\cdot \vdash_{HK4} \Box(B \to C) \to (B \to C)$ $\mathbb{T}$
6. $\Box(A \to B), \Box(B \to C) \vdash_{HK4} (B \to C)$ *MP* (5, 4)
7. $\cdot \vdash_{HK4} (A \to B) \to (B \to C) \to (A \to C)$ *trans*
8. $\Box(A \to B), \Box(B \to C) \vdash_{HK4} (B \to C) \to (A \to C)$ *MP* (7, 4)
9. $(\Box(A \to B), \Box(B \to C)); (\Box(A \to B), \Box(B \to C)) \vdash_{HK4} (A \to C)$ *MP* (8, 6)

10. $\Box(A \to B), \Box(B \to C) \vdash_{HK4} (A \to C)$ *contracción* (9)

11. $(\Box(A \to B), \Box(B \to C)); \cdot \vdash_{HK4} \Box(A \to C)$ *NecGen* (10)

12. $\Box(A \to B) \vdash_{HK4} \Box(B \to C) \to \Box(A \to C)$ *Teo.Deducción.* (11)

13. $\cdot \vdash_{HK4} \Box(A \to B) \to \Box(B \to C) \to \Box(A \to C)$ *Teo.Deducción.* (12)

■

Ejemplo 2.7. $\cdot \vdash_{HK4} \Box(A \to B) \to \Box(\Box A \to \Box B)$

Demostración. Prueba por derivación.
Por el Teorema de la deducción, basta probar que, $\Box(A \to B) \vdash_{HK4} \Box(\Box A \to \Box B)$.

1. $\Box(A \to B) \vdash_{HK4} \Box(A \to B)$ *Hip*

2. $\cdot \vdash_{HK4} \Box(A \to B) \to (\Box A \to \Box B)$ $\mathbb{K}$

3. $\Box(A \to B) \vdash_{HK4} (\Box A \to \Box B)$ *MP* (2, 1)

4. $(\Box(A \to B)); \cdot \vdash_{HK4} \Box(\Box A \to \Box B)$ *NecGen* (3)

5. $\cdot \vdash_{HK4} \Box(A \to B) \to \Box(\Box A \to \Box B)$ *Teo.Deducción.* (4)

■

2.7. Teorema de la Deducción Generalizado

En las secciones anteriores vimos que el teorema de la deducción es una fuerte herramienta para realizar derivaciones. Sin embargo, si se desea descargar más de una premisa, se tiene que utilizar el teorema de la deducción tantas veces como premisas a descargar, lo cual resulta inconveniente. Proporcionamos aquí una solución a este problema mediante la definición de la implicación iterada.
La idea de implicación iterada consiste en representar una implicación de la forma $A_0 \to A_1 \to ... \to A_n \to B$ mediante una implicación entre un contexto y una fórmula, denotada con $(A_n, A_{n-1}, ..., A_0) \hookrightarrow B$. Por ejemplo: $(C, B, A) \hookrightarrow X$ significa $A \to (B \to (C \to X))$.

Definición 2.4 (Implicación Iterada)**.** *Sean A B proposiciones, Δ un contexto. Definimos la implicación iterada de forma recursiva como sigue:*

- $\cdot \hookrightarrow B =_{def} B$
- $(\Delta, A) \hookrightarrow B =_{def} A \to (\Delta \hookrightarrow B)$

A continuación presentamos unas propiedades de la implicación iterada.

Lema 2.5 (Intercambio entre fórmula y contexto)**.** *Si* $\Gamma \vdash_{HK4} \Gamma' \hookrightarrow (A \to B)$ *entonces* $\Gamma \vdash_{HK4} A \to (\Gamma' \hookrightarrow B)$

Demostración. Inducción sobre Γ'.

Caso Base: $\Gamma' = \cdot$
Si $\Gamma \vdash_{HK4} \cdot \hookrightarrow (A \to B)$ PD. $\Gamma \vdash_{HK4} A \to (\cdot \hookrightarrow B)$.

1. $\Gamma \vdash_{HK4} \cdot \hookrightarrow (A \to B)$ — *supuesto*
2. $\Gamma \vdash_{HK4} (A \to B)$ — *Def Imp.Iter.*
3. $\Gamma \vdash_{HK4} A \to (\cdot \hookrightarrow B)$ — *Def. Imp.Iter.*

H.I: Si $\Gamma \vdash_{HK4} \Gamma' \hookrightarrow (A \to B)$ entonces $\Gamma \vdash_{HK4} A \to (\Gamma' \hookrightarrow B)$.

Paso Inductivo: $\Gamma' = (\Delta, P)$.
$\Gamma \vdash_{HK4} (\Delta, P) \hookrightarrow (A \to B)$ PD. $\Gamma \vdash_{HK4} A \to ((\Delta, P) \hookrightarrow B)$.

1. $\Gamma \vdash_{HK4} (\Delta, P) \hookrightarrow (A \to B)$ — *supuesto*
2. $\Gamma \vdash_{HK4} P \to \Delta \hookrightarrow (A \to B)$ — *Def. Imp.Iter.*
3. $\Gamma, P \vdash_{HK4} \Delta \hookrightarrow (A \to B)$ — *Teo.Ded.Inv.* (2)
4. $\Gamma, P \vdash_{HK4} A \to (\Delta \hookrightarrow B)$ — *H.I* (3)
5. $\Gamma \vdash_{HK4} P \to A \to (\Delta \hookrightarrow B)$ — *Teo.Deducción.* (4)
6. $\cdot \vdash_{HK4} (P \to A \to (\Delta \hookrightarrow B)) \to (A \to P \to (\Delta \hookrightarrow B))$ — C
7. $\Gamma \vdash_{HK4} A \to P \to (\Delta \hookrightarrow B)$ — *MP* (6, 5)
8. $\Gamma \vdash_{HK4} A \to ((\Delta, P) \hookrightarrow B)$ — *Def. Imp.Iter.*

■

Esta propiedad corresponde a una generalización del axioma C que permite intercambiar una premisa y un contexto, lo cual implica que el lugar particular de una hipótesis en una implicación iterada, es irrelevante. A continuación generalizamos este lema sustituyendo dicha hipótesis por un contexto.

Lema 2.6 (Intercambio de contextos)**.** *Si* $\Gamma \vdash_{HK4} \Delta \hookrightarrow (\Pi \hookrightarrow B)$ *entonces* $\Gamma \vdash_{HK4} \Pi \hookrightarrow (\Delta \hookrightarrow B)$.

Demostración. Inducción sobre Δ.

Caso Base: $\Delta = \cdot$
$\Gamma \vdash_{HK4} \cdot \hookrightarrow (\Pi \hookrightarrow B)$ PD. $\Gamma \vdash_{HK4} \Pi \hookrightarrow (\cdot \hookrightarrow B)$.

1. $\Gamma \vdash_{HK4} \cdot \hookrightarrow (\Pi \hookrightarrow B)$ *supuesto*

2. $\Gamma \vdash_{HK4} (\Pi \hookrightarrow B)$ *Def. Imp.Iter.*

3. $\Gamma \vdash_{HK4} \Pi \hookrightarrow (\cdot \hookrightarrow B)$ *Def. Imp.Iter.*

H.I: Si $\Gamma \vdash_{HK4} \Delta \hookrightarrow (\Pi \hookrightarrow B)$ entonces $\Gamma \vdash_{HK4} \Pi \hookrightarrow (\Delta \hookrightarrow B)$

Paso Inductivo: $\Delta = (\Delta, A)$.
$\Gamma \vdash_{HK4} (\Delta, A) \hookrightarrow (\Pi \hookrightarrow B)$ PD. $\Gamma \vdash_{HK4} \Pi \hookrightarrow ((\Delta, A) \hookrightarrow B)$.

1. $\Gamma \vdash_{HK4} (\Delta, A) \hookrightarrow (\Pi \hookrightarrow B)$ *supuesto*

2. $\Gamma \vdash_{HK4} A \to \Delta \hookrightarrow (\Pi \hookrightarrow B)$ *Def. Imp.Iter.*

3. $\Gamma, A \vdash_{HK4} \Delta \hookrightarrow (\Pi \hookrightarrow B)$ *Teo.Ded.Inv.* (2)

4. $\Gamma, A \vdash_{HK4} \Pi \hookrightarrow (\Delta \hookrightarrow B)$ *H.I* (3)

5. $\Gamma \vdash_{HK4} A \to \Pi \hookrightarrow (\Delta \hookrightarrow B)$ *Teo.Deducción.* (4)

6. $\cdot \vdash_{HK4} (A \to \Pi \hookrightarrow (\Delta \hookrightarrow B)) \to (\Pi \hookrightarrow A \to (\Delta \hookrightarrow B))$ C

7. $\Gamma \vdash_{HK4} \Pi \hookrightarrow A \to (\Delta \hookrightarrow B)$ *MP* (5,6)

8. $\Gamma \vdash_{HK4} \Pi \hookrightarrow ((\Delta, A) \hookrightarrow B)$ *Def. Imp.Iter.*

■

Juntos los dos lemas anteriores permiten concluir la propiedad intuitiva acerca que el orden de las premisas en un contexto es irrelevante para realizar derivaciones.

A continuación la demostración de la generalización del teorema de la deducción para la implicación iterada.

Teorema 2.4 (Teorema de la Deducción Generalizado). *Si* $\Gamma; \Gamma' \vdash_{HK4} B$ *entonces* $\Gamma \vdash \Gamma' \hookrightarrow B$.

Demostración. Inducción sobre Γ'.

Caso Base:
Puesto que $\cdot \hookrightarrow B$ es B, esto es claro.

H.I: Si $\Gamma; \Gamma' \vdash_{HK4} B$ entonces $\Gamma \vdash_{HK4} \Gamma' \hookrightarrow B$

Paso Inductivo: $\Gamma' = (\Gamma', p)$
$\Gamma; (\Gamma', p) \vdash_{HK4} B$ PD. $\Gamma \vdash_{HK4} (\Gamma', p) \hookrightarrow B$.

1. $\Gamma; (\Gamma', p) \vdash_{HK4} B$ *supuesto*

2. $(\Gamma;\Gamma'), p \vdash_{HK4} B$

3. $\Gamma;\Gamma' \vdash_{HK4} p \to B$ *Teo.Deducción.* (2)

4. $\Gamma \vdash_{HK4} \Gamma' \hookrightarrow p \to B$ *H.I* (3)

5. $\Gamma \vdash_{HK4} p \to \Gamma' \hookrightarrow B$ *Lema* 2.5

6. $\Gamma \vdash_{HK4} (\Gamma', p) \hookrightarrow B$ *Def. Imp.Iter.*

■

Corolario 2.2. *Si* $\Gamma \vdash_{HK4} A$ *entonces* $\cdot \vdash_{HK4} \Gamma \hookrightarrow A$.

Demostración. Sea $\Gamma \vdash_{HK4} A$, esto es equivalente a $\cdot;\Gamma \vdash_{HK4} A$. Por el *Teo.Ded.Gen.* se tiene $\cdot \vdash_{HK4} \Gamma \hookrightarrow A$. ■

En este capítulo se presentaron los sistemas axiomáticos y se discutió y resolvió la controversia del teorema de la deducción en lógica modal con ayuda del sistema *HK4*. En el siguiente capítulo se expone el sistema de deducción natural que proponen Frank Pfenning y Rowan Davies.

Capítulo 3

Sistema de Deducción Natural *CS4*

En este capítulo se presenta el sistema de deducción natural que proponen Frank Pfenning y Rowan Davies [24] para la lógica modal intuicionista $S4$.

El sistema de deducción natural que estos autores proponen utiliza la metodología de Martin-Löf que consiste en distinguir los juicios y proposiciones. A partir de esta noción se formula la construcción de las modalidades de necesidad y posibilidad que dan pauta al sistema de deducción natural.

Martin-Löf proporciona fundamentos para la lógica basados en una distinción entre juicios y proposiciones. Establece que juzgar es conocer y un juicio evidente es un objeto de conocimiento, de tal forma que una prueba o demostración es lo que hace a un juicio evidente.

Se trabaja principalmente con juicios de la forma A es una proposición o A es verdadera, para éste último suponiendo que A es una proposición. Bajo esta idea, se interpreta que el hecho de saber que A es una proposición, significa que se conoce aquello que verifica a A. Por otro lado, saber que A es verdadera significa que se sabe cómo verificar A.

En la caracterización de la lógica por medio de juicios, se utilizan dos reglas por cada conectivo u operador; estas reglas son conocidas como de introducción y de eliminación en los sistemas de Deducción Natural introducidos por Gentzen en 1935. El significado de una proposición está dado por aquello que cuenta como una verificación de la misma, es decir, se obtiene de los objetos que son utilizados para demostrarla, lo cual se refleja en las reglas de introducción que permiten concluir cuándo una proposición es verdadera; estas reglas de introducción se complementan con las reglas de eliminación que proporcionan una forma de obtener información al descomponer una proposición.

Hasta ahora hemos mencionado los juicios de la forma A *es una proposición* y A *es verdadera*. Sin embargo, estos no son suficientes para demostrar el esquema correspondiente a la implicación, puesto que nos gustaría afirmar que $A \to B$ es verdadera si siempre que A es verdadera B también lo es. Para esto se introducen a continuación, los juicios y pruebas hipotéticas. El esquema general de un juicio hipotético es

$$J_1, J_2, ..., J_n \vdash J$$

el cual expresa que se deriva J asumiendo verdaderas cada una de las hipótesis del conjunto $\{J_1, J_2, ..., J_n\}$, es decir tenemos que J a partir de las hipótesis J_1 hasta J_n. En una prueba hipotética del juicio anterior, podemos utilizar cada una de las hipótesis J_i dándolas por hecho; en consecuencia podemos sustituir una derivación arbitraria de J_i para obtener un juicio que no depende de J_i . La forma particular del juicio hipotético que necesitamos es

$$A_1 \textit{ verdadera}, \dots , A_n \textit{ verdadera} \vdash A \textit{ verdadera}$$

Por otra parte, existen juicios que no dependen de hipótesis que afirman la verdad de proposiciones, es decir, juicios que son ciertos independientemente de cualquier conjunto de hipótesis verdaderas, a éstos les llamaremos juicios categóricos. A continuación se introduce el juicio de que A es válida, que se denota por A *válida*, presuponiendo que A es una proposición. La evidencia para la validez de A es la evidencia incondicional de A, lo cual se refleja en la siguiente definición:

Definición de validez:
Una proposición A es válida si:

1. Si $\cdot \vdash A$ entonces $\Gamma \vdash A$
2. Si A es válida entonces $\Gamma \vdash$ A

es decir, A es derivable a partir del conjunto vacío de hipótesis y si A es válida entonces es verdadera para cualquier contexto.
Lo anterior es importante para incorporar hipótesis de la forma A válida en los juicios hipotéticos, dado que el orden es irrelevante, se separan hipótesis verdaderas de válidas, obteniendo el siguiente esquema

$$\mathrm{B}_1 \textit{ válida}, \dots , \mathrm{B}_m \textit{ válida} \mid A_1 \textit{ verdadera}, \dots , \mathrm{A}_n \textit{ verdadera} \vdash \mathrm{A} \textit{ verdadera}$$

Se empleará Δ para representar el conjunto de suposiciones válidas y Γ el conjunto de suposiciones verdaderas.

La sintaxis es:

Variables Proposicionales	$VarP ::= P_0 \mid P_1 \mid \dots \mid P_n$
Proposiciones	$\mathrm{A} ::= VarP \mid A \to A \mid \Box A$
Hipótesis verdaderas	$\Gamma ::= \cdot \mid \Gamma, \mathrm{A}$
Hipótesis válidas	$\Delta ::= \cdot \mid \Delta, \mathrm{A}$

Las reglas de inferencia del sistema de deducción natural de Pfenning y Davies *CS4* son:

$$\frac{}{\Delta \mid (\Gamma, \mathrm{A} ; \Gamma') \vdash_{CS4} A}\, tHip \qquad \frac{}{(\Delta, \mathrm{B}; \Delta') \mid \Gamma \vdash_{CS4} B}\, vHip$$

$$\frac{\Delta \mid (\Gamma, \mathrm{A}) \vdash_{CS4} \mathrm{B}}{\Delta \mid \Gamma \vdash_{CS4} (A \to B)} \to I \qquad \frac{\Delta \mid \cdot \vdash_{CS4} A}{\Delta \mid \Gamma \vdash_{CS4} \Box A}\, \Box I$$

$$\frac{\Delta \mid \ \Gamma \vdash_{CS4} \Box A \qquad (\Delta,\text{A}) \ \mid \Gamma \vdash_{CS4} C}{\Delta \mid \ \Gamma \vdash_{CS4} C} \Box E$$

$$\frac{\Delta \mid \ \Gamma \vdash_{CS4} (A \to B) \qquad \Delta \mid \ \Gamma \vdash_{CS4} A}{\Delta \mid \ \Gamma \vdash_{CS4} B} \to E$$

A continuación damos la definición de derivación del sistema *CS4*.

Definición 3.1. *Una prueba o derivación* Π *es un juicio* $J =_{def} \Delta \mid \Gamma \vdash_{CS4} A$ *es una secuencia finita de juicios* $\Pi = \{J_1, ..., J_k\}$ *tal que* $J_k = J$ *y para cada* $1 \leq i \leq k$ *cumple las siguientes condiciones:*

- J_i *es una instancia de la regla (tHip)*
- J_i *es una instancia de la regla (vHip)*
- J_i *es la conclusión de una instancia de algunas de las reglas de inferencia cuyas premisas son* $J_{l_1}, ..., J_{l_n}$ *con* $l_1, \ldots, l_n \leq i$

Decimos que un juicio J es derivable (demostrable) si existe una derivación de J.

Veamos algunos ejemplos de derivaciones correspondientes a los axiomas de la lógica modal.

Ejemplo 3.1. El juicio $\cdot \mid \cdot \vdash_{CS4} \Box A \to A$ es derivable (Esquema T).

1. $\cdot \mid \Box A \vdash_{CS4} \Box A$ *(tHip)*
2. $A \mid \Box A \vdash_{CS4} \Box A$ *(vHip)*
3. $\cdot \mid \Box A \vdash_{CS4} A$ $(\Box E)$ (1,2)
4. $\cdot \mid \cdot \vdash_{CS4} \Box A \to A$ $(\to I)$ (3)

■

Donde la secuencia de juicios enumerados del 1 al 4, son una prueba o derivación del juicio $\cdot \mid \cdot \vdash_{CS4} \Box A \to A$, por lo que se afirma que es derivable.

Ejemplo 3.2. El juicio $\cdot \mid \cdot \vdash_{CS4} \Box A \to \Box\Box A$ es derivable (Esquema 4).

1. $A \mid \cdot \vdash_{CS4} A$ *(vHip)*
2. $A \mid \cdot \vdash_{CS4} \Box A$ $(\Box I)$ (1)
3. $A \mid \Box A \vdash_{CS4} \Box\Box A$ $(\Box I)$ (2)
4. $\cdot \mid \Box A \vdash_{CS4} \Box A$ *(vHip)*
5. $\cdot \mid \Box A \vdash_{CS4} \Box\Box A$ $(\Box E)$ (4, 3)

6. $\cdot \mid \cdot \vdash_{CS4} \Box A \to \Box\Box A$ $(\to I)$ (5)

■

Donde la secuencia de juicios enumerados del 1 al 6, son una prueba o derivación del juicio $\cdot \mid \cdot \vdash_{CS4} \Box A \to \Box\Box A$, de aquí que el juicio es derivable.

Ejemplo 3.3. El juicio $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to (\Box A \to \Box B)$ es derivable (Esquema K).

1. A, A $\to$ B $\mid \cdot \vdash_{CS4} A$ *(vHip)*
2. A, A $\to$ B $\mid \cdot \vdash_{CS4} A \to B$ *(vHip)*
3. A, A $\to$ B $\mid \cdot \vdash_{CS4} B$ $(\to E)$ (1, 2)
4. A, A $\to$ B $\mid \Box(A \to B), \Box A \vdash_{CS4} B$ $(\Box I)$ (3)
5. A $\mid \Box(A \to B), \Box A \vdash_{CS4} \Box(A \to B)$ *(tHip)*
6. A $\mid \Box(A \to B), \Box A \vdash_{CS4} \Box B)$ $(\Box E)$ (5, 4)
7. $\cdot \mid \Box(A \to B), \Box A \vdash_{CS4} \Box A$ *(vHip)*
8. $\cdot \mid \Box(A \to B), \Box A \vdash_{CS4} \Box B$ $(\Box E)$ (7, 6)
9. $\cdot \mid \Box(A \to B) \vdash_{CS4} \Box A \to \Box B$ $(\to I)$ (8)
10. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box A \to \Box B$ $(\to I)$ (9)

■

Donde la secuencia de juicios enumerados del 1 al 10, son una prueba o derivación del juicio $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to (\Box A \to \Box B)$, por lo que es derivable.

A continuación mostramos las derivaciones en *CS4* de dos teoremas que ya fueron presentados en *HK4*.

Ejemplo 3.4. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box(B \to C) \to \Box(A \to C)$

Demostración. Prueba por derivación.

1. $A \to B, B \to C \mid A \vdash_{CS4} A \to B$ *(vHip)*
2. $A \to B, B \to C \mid A \vdash_{CS4} A$ *(tHip)*
3. $A \to B, B \to C \mid A \vdash_{CS4} B$ $(\to E)$ (1, 2)
4. $A \to B, B \to C \mid A \vdash_{CS4} B \to C$ *(vHip)*
5. $A \to B, B \to C \mid A \vdash_{CS4} C$ $(\to E)$ (3, 4)
6. $A \to B, B \to C \mid \cdot \vdash_{CS4} A \to C$ $(\to I)$ (5)
7. $A \to B, B \to C \mid \Box(A \to B), \Box(B \to C) \vdash_{CS4} \Box(A \to C)$ $(\Box I)$ (6)

8. $B \to C \mid \Box(A \to B), \Box(B \to C) \vdash_{CS4} \Box(A \to B)$ *(tHip)*

9. $B \to C \mid \Box(A \to B), \Box(B \to C) \vdash_{CS4} \Box(A \to C)$ $(\Box E)$ (7, 8)

10. $\cdot \mid \Box(A \to B), \Box(B \to C) \vdash_{CS4} \Box(B \to C)$ *(tHip)*

11. $\cdot \mid \Box(A \to B), \Box(B \to C) \vdash_{CS4} \Box(A \to C)$ $(\Box E)$ (9, 10)

12. $\cdot \mid \Box(A \to B) \vdash_{CS4} \Box(B \to C) \to \Box(A \to C)$ $(\to I)$ (11)

13. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box(B \to C) \to \Box(A \to C)$ $(\to I)$ (12)

■

Ejemplo 3.5. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box(\Box A \to \Box B)$

Demostración. Prueba por derivación.

1. $A \to B \mid \cdot \vdash_{CS4} A \to B$ *(vHip)*

2. $A \to B \mid \cdot \vdash_{CS4} \Box(A \to B)$ $(\Box I)$ (1)

3. $A \to B \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box A \to \Box B$ $\mathbb{K}$

4. $A \to B \mid \cdot \vdash_{CS4} \Box A \to \Box B$ $(\Box E)$ (3,2)

5. $A \to B \mid \Box(A \to B) \vdash_{CS4} \Box(\Box A \to \Box B)$ $(\Box I)$ (4)

6. $\cdot \mid \Box(A \to B) \vdash_{CS4} \Box(A \to B)$ *(tHip)*

7. $\cdot \mid \Box(A \to B) \vdash_{CS4} \Box(\Box A \to \Box B)$ $(\Box E)$ (5,6)

8. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box(\Box A \to \Box B)$ $(\to I)$ (7)

■

Obsérvese que si bien es correcto, el ejemplo 3.5 va en contra del espíritu de la deducción natural porque utiliza el axioma $\mathbb{K}$. Veamos ahora la derivación del mismo utilizando la regla $(\Box E)$ en lugar de $\mathbb{K}$.

Ejemplo 3.6. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box(\Box A \to \Box B)$

Demostración. Prueba por derivación.

1. $A \to B, A \mid \cdot \vdash_{CS4} A \to B$ *(vHip)*

2. $A \to B, A \mid \cdot \vdash_{CS4} A$ *(vHip)*

3. $A \to B, A \mid \cdot \vdash_{CS4} B$ $(\to E)$ (1, 2)

4. $A \to B, A \mid \Box A \vdash_{CS4} \Box B$ $(\Box I)$ (3)

5. $A \to B \mid \Box A \vdash_{CS4} \Box A$ *(tHip)*

6. $A \to B \mid \Box A \vdash_{CS4} \Box B$ $(\Box E)$ (4,5)

7. $A \to B \mid \cdot \vdash_{CS4} \Box A \to \Box B$ $(\to I)$ (6)

8. $A \to B \mid \Box(A \to B) \vdash_{CS4} \Box(\Box A \to \Box B)$ $(\Box I)$ (7)

9. $\cdot \mid \Box(A \to B) \vdash_{CS4} \Box(A \to B)$ *(tHip)*

10. $\cdot \mid \Box(A \to B) \vdash_{CS4} \Box(\Box A \to \Box B)$ $(\Box E)$ (8, 9)

11. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box(\Box A \to \Box B)$ $(\to I)$ (10)

■

Ya vistos algunos ejemplos de derivaciones en *CS4*, veamos las propiedades del sistema.

3.1. Propiedades estructurales en *CS4*

En esta sección se muestran las propiedades estructurales del sistema *CS4*, el cual no maneja una regla de hipótesis. Por ello, el siguiente lema.

Lema 3.1 (CS4_Hip)**.** *Si* $A \in \Gamma$ *entonces* $\Delta \mid \Gamma \vdash_{CS4} A$.

Demostración. Si A $\in \Gamma$ entonces es posible demostrar que existen Γ_1 y Γ_2 tales que $\Gamma = (\Gamma_1, A); \Gamma_2$ de donde, por la regla *(tHip)* se sigue que $\Delta \mid \Gamma \vdash_{CS4} A$. ■

El sistema cumple las propiedades estructurales usuales.

Proposición 3.1. Si Δ | Γ, A, B, $\Gamma' \vdash_{CS4} C$ entonces Δ | Γ, B, A, $\Gamma' \vdash_{CS4} C$

Demostración. Por inducción sobre la estructura de la derivación del juicio Δ | Γ , A, B, $\Gamma' \vdash_{CS4} C$
La prueba se encuentra en [23]. ■

Proposición 3.2. El sistema de inferencia *CS4* satisface la ley de contracción:

Si Δ | Γ, A, A, $\Gamma' \vdash_{CS4} C$ entonces Δ | Γ, A, $\Gamma' \vdash_{CS4} C$

Demostración. Por inducción sobre la estructura de la derivación del juicio Δ | Γ , A, A, $\Gamma' \vdash_{CS4} C$
La prueba se encuentra en [23]. ■

Proposición 3.3. El sistema de inferencia *CS4* satisface la ley de debilitamiento:

Si Δ | Γ, $\Gamma' \vdash_{CS4} C$ entonces Δ | Γ, B, $\Gamma' \vdash_{CS4} C$

Demostración. Por inducción sobre la estructura de la derivación del juicio Δ | Γ, $\Gamma' \vdash_{CS4} C$
La prueba se encuentra en [23]. ■

Proposición 3.4. El sistema de inferencia *CS4* satisface las leyes estructurales análogas, sobre para los contextos de fórmulas válidas:

- Si Δ, A, B, Δ' | $\Gamma \vdash_{CS4} C$ entonces Δ, B, A, Δ' | $\Gamma \vdash_{CS4} C$
- Si Δ, A, A, Δ' | $\Gamma \vdash_{CS4} C$ entonces Δ, A | $\Gamma \vdash_{CS4} C$

- Si Δ, $\Delta' \mid \Gamma \vdash_{CS4} C$ entonces Δ, B, $\Delta' \mid \Gamma \vdash_{CS4} C$

Las demostraciones de dichas propiedades y más información sobre el sistema *CS4* se encuentra en [23].

3.2. Las Fórmulas válidas son verdades necesarias

El trabajo de Pfenning y Davies [24] no refleja en la práctica el hecho de que las fórmulas válidas son fórmulas necesariamente verdaderas, en el sentido de que si asumimos que una fórmula A es válida, es decir $A \in \Delta$, podemos considerarla como una verdad necesaria, lo que operacionalmente significa que se elimine A en Δ mientras se agrega $\Box A$ a Γ.

Proposición 3.5 (Fórmulas válidas son verdades necesarias)**.** Sean Δ, Γ contextos y A, B proposiciones. Si $\Delta, A \mid \Gamma \vdash_{CS4} B$ entonces $\Delta \mid \Gamma, \Box A \vdash_{CS4} B$

Demostración. Inducción sobre $\Delta, A \mid \Gamma \vdash_{CS4} B$.

Casos Base:
Caso 1:

$\Delta \mid ((\Gamma, A_0); \Gamma'), \Box A \vdash_{CS4} A_0$ *CS4_Hip.*

Caso 2: Si $(\Delta', B); \Delta'' = \Delta, A$. PD. $\Delta \mid \Gamma, \Box A \vdash_{CS4} B$

Sea $(\Delta', B); \Delta'' = \Delta, A$ por el lema descomposición de contextos se tiene que $\Delta'' = \cdot$ y $\Delta'', B = \Delta, A$ ó $\exists \Gamma'', \Delta'' = \Gamma'', A$.

subcaso 1: Si $\Delta'' = \cdot$ y $\Delta', B = \Delta, A$.

- Como $\Delta'' = \cdot$ entonces $\Delta', B \mid \Gamma, \Box A \vdash_{CS4} B$
- $\Delta', B = \Delta, A$ entonces $\Delta' = \Delta$ y B = A.
- Por lo que $\Delta \mid \Gamma, \Box A \vdash_{CS4} \Box A$ por *(tHip)*, por el $\mathbb{T}$ y $(\to E)$ se tiene que $\Delta \mid \Gamma, \Box A \vdash_{CS4} A$, pero A = B, entonces $\Delta \mid \Gamma, \Box A \vdash_{CS4} B$.

subcaso 2: $\exists \Gamma'', \Delta'' = \Gamma'', A$.

- Sea $(\Delta', B); \Delta'' \mid \Gamma, \Box A \vdash_{CS4} B$, sustituimos a Δ'' en $((\Delta', B); \Delta'') = \Delta, A$
- Por lo que resulta, $((\Delta', B); (\Gamma'', A)) = \Delta, A$
- Pero es equivalente a $((\Delta', B); \Gamma''), A = \Delta, A$
- y resulta $(\Delta', B); \Gamma'' = \Delta$ y B = A
- Por lo que, $\Delta \mid \Gamma, \Box A \vdash_{CS4} B$.

Casos Inductivos:
H.I $\Delta \mid \Gamma, A_0, \Box A \vdash_{CS4} B$

Sea $\Delta, A \mid \Gamma, A_0 \vdash_{CS4} B$, por H.I se tiene $\Delta \mid \Gamma, A_0, \Box A \vdash_{CS4} B$, permutamos $\Delta \mid \Gamma, \Box A, A_0 \vdash_{CS4} B$ y por $(\to I)$ se tiene $\Delta \mid \Gamma, \Box A \vdash_{CS4} A_0 \to B$.

Caso 4: Si $\Delta, A \mid \Gamma \vdash_{CS4} A_0 \to B$, $\Delta, A \mid \Gamma \vdash_{CS4} A_0$ PD. $\Delta \mid \Gamma, \Box A \vdash_{CS4} B$.
H.I$_1$: $\Delta \mid \Gamma, \Box A \vdash_{CS4} A_0 \to B$
H.I$_2$: $\Delta \mid \Gamma, \Box A \vdash_{CS4} A_0$

1. Sea $\Delta, A \mid \Gamma \vdash_{CS4} A_0 \to B$, por H.I$_1$ se tiene que Si $\Delta \mid \Gamma, \Box A \vdash_{CS4} A_0 \to B$.
2. Sea $\Delta, A \mid \Gamma \vdash_{CS4} A_0$ y por H.I$_2$ se tiene que $\Delta \mid \Gamma, \Box A \vdash_{CS4} A_0$
3. $\Delta \mid \Gamma, \Box A \vdash_{CS4} B$ $\qquad (\to E)$ (1,2)

Caso 5: Si $\Delta, A \mid \cdot \vdash_{CS4} A_0$ PD. $\Delta \mid \Gamma, \Box A \vdash_{CS4} \Box A_0$.
H.I: $\Delta \mid (\cdot, \Box A) \vdash_{CS4} A_0$

1. $\Delta \mid \Gamma, \Box A \vdash_{CS4} \Box A$ $\qquad$ *(tHip)*
2. $\Delta, A \mid \cdot \vdash_{CS4} A_0$ $\qquad$ *supuesto*
3. $\Delta, A \mid \Gamma, \Box A \vdash_{CS4} \Box A_0$ $\qquad (\to I)$ (2)
4. $\Delta \mid \Gamma, \Box A \vdash_{CS4} \Box A_0$ $\qquad (\Box E)$ (3,1)

Caso 6: Si $\Delta, A \mid \Gamma \vdash_{CS4} \Box A_0$ y $\Delta, A, A_0 \mid \Gamma \vdash_{CS4} C$ PD. $\Delta \mid \Gamma, \Box A \vdash_{CS4} C$.
H.I$_1$: $\Delta \mid \Gamma, \Box A \vdash_{CS4} \Box A_0$
H.I$_2$: $\Delta, A_0 \mid \Gamma, \Box A \vdash_{CS4} C$

1. $\Delta, A \mid \Gamma \vdash_{CS4} \Box A_0$ por H.I$_1$ se tiene que $\Delta \mid \Gamma, \Box A \vdash_{CS4} \Box A_0$
2. $\Delta, A, A_0 \mid \Gamma \vdash_{CS4} C$ por H.I$_2$ se tiene que $\Delta, A_0 \mid \Gamma, \Box A \vdash_{CS4} C$
3. $\Delta \mid \Gamma, \Box A \vdash_{CS4} C$ $\qquad (\Box E)$ (1,2)

■

Una consecuencia inmediata de este teorema es la introducción de hipótesis válidas.

Corolario 3.1 (Intro_válidas). *$\Delta, A \mid \Gamma \vdash_{CS4} B$ entonces $\Delta \mid \Gamma \vdash_{CS4} \Box A \to B$*

Demostración.
1. $\Delta, A \mid \Gamma \vdash_{CS4} B$ $\qquad$ *supuesto*
2. $\Delta \mid \Gamma, \Box A \vdash_{CS4} B$ $\qquad$ *Prop* 3.5
3. $\Delta \mid \Gamma \vdash_{CS4} \Box A \to B$ $\qquad (\to I)$ (2)

■

El siguiente corolario generaliza la proposición 3.5.

Corolario 3.2. *Si* $\Delta \mid \Gamma \vdash_{CS4} A$ *entonces* $\cdot \mid \Delta^{\Box}; \Gamma \vdash_{CS4} A$

Demostración. Inducción sobre Δ.

Caso Base:
$\Delta = \cdot$
$\cdot \mid \Gamma \vdash_{CS4} A$ PD. $\cdot \mid \cdot^{\Box}; \Gamma \vdash_{CS4} A$

Sea $\cdot \mid \Gamma \vdash_{CS4} A$, pero esto es equivalente a $\cdot \mid \cdot; \Gamma \vdash_{CS4} A$ pero esto es $\cdot^{\Box}; \Gamma \vdash_{CS4} A$.

H.I: $\Delta \mid \Gamma \vdash_{CS4} A \Rightarrow \cdot \mid \Delta^{\Box}; \Gamma \vdash_{CS4} A$
Paso Inductivo:

Sea $(\Delta', p) \mid \Gamma \vdash_{CS4} A$ PD. $\cdot \mid (\Delta', p)^{\Box}; \Gamma \vdash_{CS4} A$.

1. $(\Delta', p) \mid \Gamma \vdash_{CS4} A$ *supuesto*
2. $\Delta' \mid \Gamma, \Box p \vdash_{CS4} A$ *Prop* 3.5
3. $\Delta' \mid \Gamma \vdash_{CS4} \Box p \to A$ $(\to I)$ (2)
4. $\cdot \mid \Delta'^{\Box}; \Gamma \vdash_{CS4} \Box p \to A$ *H.I* (3)
5. $\cdot \mid \Delta'^{\Box}; \Gamma, \Box p \vdash_{CS4} A$ *Teo.Deducción.* (4)
6. $\cdot \mid \Delta'^{\Box}, \Box p; \Gamma \vdash_{CS4} A$ *perm. y asoc. contexto* (5)
7. $\cdot \mid (\Delta', p)^{\Box}; \Gamma \vdash_{CS4} A$

■

La siguiente proposición es la recíproca de la proposición 3.5 y permite transferir fórmulas modales del contexto de verdaderas al contexto de válidas.

Proposición 3.6 (Verdades necesarias son válidas)**.** Sean Δ, Γ contextos, y A, B *proposiciones.* Entonces, si $\Delta \mid \Gamma, \Box A \vdash_{CS4} B$ entonces $\Delta, A \mid \Gamma \vdash_{CS4} B$

Demostración. .

1. $\Delta, \Box A \mid \Gamma \vdash_{CS4} B$ *supuesto*
2. $\Delta \mid \Gamma \vdash_{CS4} \Box A \to B$ $(\to I)$ (1)
3. Esto pasa $\Delta, A \mid \Gamma \vdash_{CS4} B$ si y sólo si *Corolario* 3.1 (2)

■

El siguiente corolario es la generalización de la proposición 3.6.

Corolario 3.3. *Sean* Δ, Γ *contextos, y* A*,* B *proposiciones. Si* $\cdot \mid \Delta^{\Box}; \Gamma \vdash_{CS4} A$ *entonces* $\Delta \mid \Gamma \vdash_{CS4} A$

Demostración. Inducción sobre Δ.
Caso Base: $\Delta = \cdot$
Si $\cdot \mid \cdot^{\Box}; \Gamma \vdash_{CS4} A$ PD. $\cdot \mid \Gamma \vdash_{CS4} A$.

Puesto que $\cdot^{\Box} = \cdot$, es claro que $\cdot \mid \Gamma \vdash_{CS4} A$.

H.I. $\cdot \mid \Delta^{\Box}; \Gamma \vdash_{CS4} A \Rightarrow \Delta \mid \Gamma \vdash_{CS4} A$

Paso Inductivo: $\Delta = \Delta', p$

1. $\cdot \mid (\Delta', p)^{\Box}; \Gamma \vdash_{CS4} A$ *supuesto*
2. $\cdot \mid \Delta'^{\Box}, \Box p; \Gamma \vdash_{CS4} A$
3. $\cdot \mid \Delta'^{\Box}; \Gamma \vdash_{CS4} \Box p \to A$ $(\to I)$ (2)
4. $\Delta' \mid \Gamma \vdash_{CS4} \Box p \to A$ *H.I* (3)
5. $\Delta', p \mid \Gamma \vdash_{CS4} A$ *Corolario* 3.1 (4)

■

Juntas las proposiciones 3.5 y 3.6 proporcionan un proceso de transferencia entre ambos contextos que constituye una poderosa herramienta de derivación en el sistema *CS4*. Veámoslo en el siguiente ejemplo.

Ejemplo 3.7. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box(B \to C) \to \Box(A \to C)$

Demostración. Prueba por derivación.

1. $A \to B, B \to C \mid A \vdash_{CS4} A \to B$ *(vHip)*
2. $A \to B, B \to C \mid A \vdash_{CS4} A$ *(tHip)*
3. $A \to B, B \to C \mid A \vdash_{CS4} B$ $(\to E)$ (1, 2)
4. $A \to B, B \to C \mid A \vdash_{CS4} B \to C$ *(vHip)*
5. $A \to B, B \to C \mid A \vdash_{CS4} C$ $(\to E)$ (3, 4)
6. $A \to B, B \to C \mid \cdot \vdash_{CS4} A \to C$ $(\to I)$ (5)
7. $A \to B, B \to C \mid \cdot \vdash_{CS4} \Box(A \to C)$ $(\Box I)$ (6)

8. $A \to B \mid \Box(B \to C) \vdash_{CS4} \Box(A \to C)$ *Prop* 3.5 (7)

9. $A \to B \mid \cdot \vdash_{CS4} \Box(B \to C) \to \Box(A \to C)$ $(\to I)$ (8)

10. $\cdot \mid \Box(A \to B) \vdash_{CS4} \Box(B \to C) \to \Box(A \to C)$ *Prop* 3.5 (9)

11. $\cdot \mid \cdot \vdash_{CS4} \Box(A \to B) \to \Box(B \to C) \to \Box(A \to C)$ $(\to I)$ (10)

■

Terminamos el capítulo resumiendo las propiedades anteriores consideradas como reglas admisibles en el sistema *CS4*.

Reglas de derivación del sistema *CS4*

$$\frac{}{\Delta \mid \ (\Gamma, \text{A} ; \Gamma\text{'}) \vdash_{CS4} A}\, tHip \qquad \frac{}{(\Delta, B; \Delta') \mid \Gamma \vdash_{CS4} B}\, vHip$$

$$\frac{\Delta \mid (\Gamma, A) \vdash_{CS4} B}{\Delta \mid \Gamma \vdash_{CS4} (A \to B)} \to I \qquad \frac{\Delta \mid \cdot \vdash_{CS4} A}{\Delta \mid \Gamma \vdash_{CS4} \Box A}\, \Box I$$

$$\frac{\Delta \mid \Gamma \vdash_{CS4} \Box A \qquad (\Delta, A) \mid \Gamma \vdash_{CS4} C}{\Delta \mid \Gamma \vdash_{CS4} C}\, \Box E$$

$$\frac{\Delta \mid \Gamma \vdash_{CS4} (A \to B) \qquad \Delta \mid \Gamma \vdash_{CS4} A}{\Delta \mid \Gamma \vdash_{CS4} B} \to E$$

$$\frac{\Delta, A \mid \Gamma \vdash_{CS4} B}{\Delta \mid \Gamma, \Box A \vdash_{CS4} B}\, \text{Val\_VNec} \qquad \frac{\Delta, A \mid \Gamma \vdash_{CS4} B}{\Delta \mid \Gamma \vdash_{CS4} \Box A \to B}\, \text{Intro \_Val}$$

$$\frac{\Delta \mid \Gamma, \Box A \vdash_{CS4} B}{\Delta, A \mid \Gamma \vdash_{CS4} B}\, \text{VNec\_Val}$$

En este capítulo se presentó el sistema *CS4* y se demostraron propiedades que serán de utilidad para la equivalencia de los sistemas. En el siguiente capítulo se mostrarán los teoremas de equivalencia entre los sistemas *HK4* y *CS4*.

Capítulo 4

Equivalencia

En los capítulos anteriores se definieron los sistemas deductivos *HK4* y *CS4*, ambos correspondientes a la lógica modal constructiva $S4$. Si decimos que ambos formalismos representan a la misma lógica es entonces natural preguntarse sobre su equivalencia en el sentido de que toda prueba en alguno de ellos debe de tener su correspondiente en el otro. En este capítulo nos dedicamos a demostrar formalmente esta propiedad.

Convencerse de que toda prueba en *HK4* tiene su correspondiente en *CS4* es relativamente sencillo, solo se tiene que mostrar que los axiomas de *HK4* son derivables en *CS4*; sustituir el uso de un axioma por su correspondiente derivación y el resto de la prueba será el mismo salvo que será necesario agregar un contexto vacío de fórmulas válidas en cada paso. Formalizamos esta idea a continuación.

Teorema 4.1. *Sea* Γ *un contexto y* A *una Proposición*

$$\Gamma \vdash_{HK4} A \quad \textit{entonces} \quad \cdot \mid \Gamma \vdash_{CS4} A$$

Demostración. Inducción sobre la derivación de A
Caso 1: Si A $\in \Gamma$ PD. $\cdot \mid \Gamma \vdash_{CS4} A$

Por hipótesis se tiene que A $\in \Gamma$ entonces $\Gamma \vdash_{CS4}$ A por el lema *CS4_Hip* se tiene que
$\cdot \mid \Gamma \vdash_{CS4}$ A.

Caso 2: PD. $\cdot \mid \Gamma \vdash_{CS4} A \to A$

1. $\cdot \mid (\Gamma, A) \vdash_{CS4} A$ $\quad(\to I)$
2. $\cdot \mid$ (Γ, A); $\cdot \vdash_{CS4} A$
3. $\cdot \mid$ (Γ, A); $\cdot \vdash_{CS4} A$ $\quad$ *(tHip)* (2)

Caso 3: PD. $\cdot \mid \Gamma \vdash_{CS4} A \to (B \to A)$

1. $\cdot \mid (\Gamma, A) \vdash_{CS4} B \to A$ $\quad(\to I)$
2. $\cdot \mid$ (Γ, A), B $\vdash_{CS4} A$ $\quad(\to I)$ (2)
3. $\cdot \mid$ (Γ, A); ($\cdot$, B) $\vdash_{CS4} B \to A$ $\quad$ *equivalencia*

4. $\cdot \mid$ (Γ, A); (·, B) $\vdash_{CS4} A$ *(tHip)*

Caso 4: PD. $\cdot \mid \Gamma \vdash_{CS4} ((A \to A \to B) \to (A \to B))$

1. $\cdot \mid \Gamma, (A \to A \to B) \vdash_{CS4} (A \to B))$ $(\to I)$
2. $\cdot \mid \Gamma, (A \to A \to B), A \vdash_{CS4} B$ $(\to I)$
3. $\cdot \mid \Gamma, (A \to A \to B)$; (·, A) $\vdash_{CS4} (A \to A \to B)$ *(tHip)*
4. $\cdot \mid \Gamma, (A \to A \to B)$; (·, A) $\vdash_{CS4} A$ *(tHip)*
5. $\cdot \mid \Gamma, (A \to A \to B)$; (·, A) $\vdash_{CS4} A \to B$ $(\to E)$ (3,4)
6. $\cdot \mid \Gamma, (A \to A \to B)$; (·, A) $\vdash_{CS4} B$ $(\to E)$ (4,5)

Caso 5: PD. $\cdot \mid \Gamma \vdash_{CS4} ((A \to (B \to C)) \to (B \to (A \to C)))$

1. $\cdot \mid (\Gamma, (A \to (B \to C))) \vdash_{CS4} (B \to (A \to C))$ $(\to I)$
2. $\cdot \mid (\Gamma, (A \to (B \to C))), B \vdash_{CS4} (A \to C)$ $(\to I)$
3. $\cdot \mid (\Gamma, (A \to B \to C)), B, A \vdash_{CS4} C$ $(\to I)$
4. $\cdot \mid (\Gamma, (A \to (B \to C))), B, A \vdash_{CS4} (A \to (B \to C))$ $(\to I)$
5. $\cdot \mid (\Gamma, (A \to B \to C)), B, A \vdash_{CS4} A$ *(tHip)*
6. $\cdot \mid (\Gamma, (A \to B \to C)), B, A \vdash_{CS4} B \to C$ $(\to E)$ (4,5)
7. $\cdot \mid (\Gamma, (A \to B \to C)), B, A \vdash_{CS4} B$ *(tHip)*
8. $\cdot \mid (\Gamma, (A \to B \to C)), B, A \vdash_{CS4} C$ $(\to E)$ (6,7)

El resto de los axiomas, es análogo.

Caso MP: PD. $\cdot \mid \Gamma \vdash_{CS4} B$ Hipótesis:
H.I$_1$: $\cdot \mid \Gamma \vdash_{CS4} A$
H.I$_2$: $\cdot \mid \Gamma' \vdash_{CS4} A \to B$

1. $\cdot \mid \Gamma'; \Gamma \vdash_{CS4} A$ *debilitamiento en H.I$_1$*
2. $\cdot \mid \Gamma'; \Gamma \vdash_{CS4} A \to B$ *debilitamiento en H.I$_2$*
3. $\cdot \mid \Gamma'; \Gamma \vdash_{CS4} B$ $(\to E)$ (1,2)

Último caso: Si $\cdot \mid \cdot \vdash_{CS4} A$ PD. $\cdot \mid \Gamma \vdash_{CS4} \Box A$

1. $\cdot \mid \cdot \vdash_{CS4} A$ *supuesto*
2. $\cdot \mid \Gamma \vdash_{CS4} \Box A$ $(\Box I)$ (1)

■

Ahora bien para probar la dirección contraria tenemos que colapsar los dos contextos de una prueba en *CS4* en uno solo para el caso de *HK4*, pero sin perder la distinción existente entre hipótesis válidas y verdaderas. Para esto nos servimos de la proposición 3.5 y en particular el corolario 3.3, el cual permite transferir todas las formulas válidas del contexto Δ al contexto de hipótesis verdaderas, no si antes prefijar un operador $\Box$ a cada uno de sus elementos.

Teorema 4.2. *Sean A una Proposición y Δ, Γ contextos.*

$$\textit{Si } \Delta \mid \Gamma \vdash_{CS4} A \quad \textit{entonces} \quad \Delta^{\Box}; \Gamma \vdash_{HK4} A$$

Demostración. Inducción sobre la derivación de A

Caso 1: PD. $\Delta^{\Box}$; $((\Gamma, A); \Gamma') \vdash_{HK4} A$

1. Si A $\in (\Gamma, A); \Gamma'$ entonces A $\in ((\Gamma, A); \Gamma'); \Delta^{\Box}$ entonces $\Delta^{\Box}$; $((\Gamma, A); \Gamma'); \vdash_{HK4} A$

Caso 2: PD. $((\Delta, \mathrm{B}); \Delta')^{\Box}; \Gamma \vdash_{HK4} B$

1. $\cdot \vdash_{HK4} \Box B \to B$ $\mathbb{T}$
2. Como B $\in (\Delta, B); \Delta'$ válidas, entonces B $\in ((\Delta, B)^{\Box}; \Delta')$ verdaderas.
3. $((\Delta, B); \Delta')^{\Box} \vdash_{HK4} \Box B$ *Hip*
4. $((\Delta, B); \Delta')^{\Box} \vdash_{HK4} B$ *MP* (1,3)
5. $((\Delta, B); \Delta')^{\Box}; \Gamma \vdash_{HK4} B$ *debilitamiento* (4)

Caso 3: Si $\Delta^{\Box}$; $(\Gamma, \mathrm{A}) \vdash_{HK4}$ B. PD. $\Delta^{\Box}$; $\Gamma \vdash_{HK4}$ A $\to$ B

1. $\Delta^{\Box}$; $(\Gamma, \mathrm{A}) \vdash_{HK4}$ B *Hip*
2. $(\Delta^{\Box};\Gamma)$, A $\vdash_{HK4}$ B
3. $\Delta^{\Box};\Gamma \vdash_{HK4}$ A $\to$ B *Teo.Deducción.* (2)

Caso 4: Si $\Delta^{\Box}$; $\Gamma \vdash_{HK4}$ A $\to$ B y $\Delta^{\Box}$; $\Gamma \vdash_{HK4}$ A PD. $\Delta^{\Box};\Gamma \vdash_{HK4}$ B

1. $\Delta^{\Box}; \Gamma \vdash_{HK4} A \to B$ *Hip*
2. $\Delta^{\Box}; \Gamma \vdash_{HK4} A$ *Hip*
3. $(\Delta^{\Box}; \Gamma);(\Delta^{\Box}; \Gamma) \vdash_{HK4}$ B *MP* (1,2)
4. $\Delta^{\Box}; \Gamma \vdash_{HK4}$ B *contracción* (3)

Caso 5: Si $\Delta^{\Box}; \cdot \vdash_{HK4} A$ PD. $\Box\Delta; \Gamma \vdash \Box A$

1. $\Delta^{\Box}; \cdot \vdash_{HK4} A$ *Hip*
2. $\Delta^{\Box} \vdash_{HK4} A$
3. $\Delta'^{\Box} \vdash_{HK4} A$ *Hip*

4. $\cdot \vdash_{HK4} \Delta'^{\Box} \to A$ *Teo.Ded.Gen.Prem* (1)

5. $\Gamma;\ \Delta'^{\Box} \vdash_{HK4} \Box A$ *NecGen* (2)

6. $\Gamma;\ \Delta^{\Box} \vdash_{HK4} \Box A$

Último caso: Si $\Delta^{\Box};\ \Gamma \vdash_{HK4} \Box A$ y $(\Delta,\ \mathrm{A})^{\Box};\ \Gamma \vdash_{HK4} C \quad \Delta^{\Box};\ \Gamma \vdash_{HK4} C$

1. $\Delta^{\Box};\ \Gamma \vdash_{HK4} \Box A$ *Hip*

2. $(\Delta,\ \mathrm{A})^{\Box};\ \Gamma \vdash_{HK4} C$ *Hip*

3. $(\Delta,^{\Box}\ \Box\mathrm{A});\ \Gamma \vdash_{HK4} C$

4. $(\Delta^{\Box};\ \Gamma) \vdash_{HK4} \Box A \to C$ *Teo.Ded.Gen.Prem* (3)

5. $(\Delta^{\Box};\ \Gamma);\ (\Delta^{\Box};\ \Gamma) \vdash_{HK4} C$ *MP* (4, 1)

6. $(\Delta^{\Box};\ \Gamma) \vdash_{HK4} C$ *contracción* (5)

■

Juntos los teoremas 4.1 y 4.2, constituyen la equivalencia entre los sistemas *HK4* y *CS4* enunciada en el siguiente corolario.

Corolario 4.1. *Sean A una Proposición y Δ, Γ contextos.*

$$\Delta^{\Box}; \Gamma \vdash_{HK4} A \text{ si y sólo si } \Delta \mid \Gamma \vdash_{CS4} A.$$

Demostración. $\Rightarrow$) Si $\Delta^{\Box}; \Gamma \vdash_{HK4} A$ entonces $\Delta \mid \Gamma \vdash_{CS4} A$.

1. $\Delta^{\Box}; \Gamma \vdash_{HK4} A$ *supuesto*

2. $\cdot \mid \Delta^{\Box}; \Gamma \vdash_{CS4} A$ *Teo.* 4.1

3. $\Delta \mid \Gamma \vdash_{CS4} A$ *Corolario* 3.3.

$\Leftarrow$) Si $\Delta \mid \Gamma \vdash_{CS4} A$ entonces $\Delta^{\Box}; \Gamma \vdash_{HK4} A$.
Es el teorema 4.2. ■

4.1. Traducciones

Los teoremas 4.1 y 4.2 incluyen en su demostración un procedimiento algorítmico para traducir de un sistema a otro. El caso sencillo es de *HK4* a *CS4*: dada una derivación en la lógica axiomática, esta se traduce a deducción natural sustituyendo los pasos correspondientes a instancias de axiomas por la derivación de cada axioma en particular en deducción natural. Por ejemplo los axiomas $\mathbb{K}$, $\mathbb{T}$ y 4 se sustituyen por las derivaciones dadas en los ejemplos 3.3, 3.1 y 3.2 respectivamente. Los pasos restantes correspondientes al modus ponens y necesitación, se resuelven de manera directa mediante la eliminación de la implicación, debilitamiento y eliminación del $\Box$, respectivamente.

4.1.1. Traducción de *CS4* a *HK4*

La traducción del sistema de deducción natural al axiomático se presenta de manera esquemática a continuación, presentando la simulación de *HK4* representando a cada una de las reglas de *CS4*.

- La regla de hipótesis verdaderas:

$$
\begin{array}{lccclll}
 & \vdots & & & & \vdots & \\
j: & \Delta \mid (\Gamma, \mathrm{A}; \Gamma') \vdash_{CS4} A & (tHip) & \longmapsto & k: & \mathrm{A} \in (\Gamma, \mathrm{A}; \Gamma') & \\
 & & & & k{+}1: & \Delta^{\Box}; (\Gamma, \mathrm{A}; \Gamma') \vdash_{HK4} A & (Hip) \\
 & \vdots & & & & \vdots &
\end{array}
$$

- La regla de hipótesis válidas:

$$
\begin{array}{lccclll}
 & \vdots & & & & \vdots & \\
 & & & & k: & \cdot \vdash \Box B \to B & (\mathbb{T}) \\
j: & ((\Delta, \mathrm{B}); \Delta') \mid \Gamma \vdash_{CS4} B & (vHip) & \longmapsto & k+1: & ((\Delta^{\Box}, \Box\, \mathrm{B}); \Delta'^{\,\Box}); \Gamma \vdash_{HK4} \Box B & (Hip) \\
 & & & & k+2: & ((\Delta^{\Box}, \Box\, \mathrm{B}); \Delta'^{\,\Box}); \cdot \vdash_{HK4} B & (MP)\ (\mathrm{j, k}) \\
 & \vdots & & & & \vdots &
\end{array}
$$

- La regla de introducción de la implicación $(\to I)$:

$$
\begin{array}{lccclll}
 & \vdots & & & & \vdots & \\
j: & \Delta \mid \Gamma, \mathrm{A} \vdash_{CS4} B & (Hip) & \longmapsto & k: & \Delta^{\Box}; \Gamma, \mathrm{A} \vdash_{HK4} B & (Hip) \\
j{+}1: & \Delta \mid \Gamma \vdash_{CS4} A \to B & (\to I)\ (\mathrm{j}) & & k+1: & \Delta^{\Box}; \Gamma \vdash_{HK4} A \to B & \textit{Teo.Deducción.}\ (\mathrm{j}) \\
 & \vdots & & & & \vdots &
\end{array}
$$

- La regla de eliminación de la implicación $(\to \mathrm{E})$:

$$
\begin{array}{lcclll}
 & \vdots & & & \vdots & \\
i: & \Delta \mid \Gamma \vdash_{CS4} A & & k: & \Delta^{\Box}; \Gamma \vdash_{HK4} A & \mathrm{H.I}\ i \\
 & \vdots & & & \vdots & \\
j: & \Delta \mid \Gamma \vdash_{CS4} A \to B & \longmapsto & l: & \Delta^{\Box}; \Gamma \vdash_{HK4} A \to B & \mathrm{H.I}\ j \\
 & \vdots & & & \vdots & \\
n: & \Delta \mid \Gamma \vdash_{CS4} B & & m: & (\Delta^{\Box}; \Gamma); (\Delta^{\Box}; \Gamma) \vdash_{HK4} B & (MP\ (k, l)) \\
 & \vdots & & m+1: & \Delta^{\Box}; \Gamma \vdash_{HK4} B & \text{contracción (m)} \\
 & \vdots & & & \vdots &
\end{array}
$$

- La regla de introducción del operador $\Box$:

$$
\begin{array}{lccclll}
 & \vdots & & & & \vdots & \\
i: & \Delta \mid \cdot \vdash_{CS4} A & & \longmapsto & k: & \Delta^{\Box} \vdash_{HK4} A & H.I i \\
 & \vdots & & & & \vdots & \\
j: & \Delta \mid \cdot \vdash_{CS4} \Box A & (\Box I)\ i & & l: & \Delta^{\Box}; \Gamma \vdash_{HK4} \Box A & NecGenk \\
 & \vdots & & & & \vdots &
\end{array}
$$

- La regla de eliminación del operador $\Box$:

$$
\begin{array}{llll|lllr}
 & \vdots & & & & \vdots & & \\
i: & \Delta|\ \Gamma \vdash_{CS4} \Box A & & & k: & \Delta^{\Box}; \Gamma \vdash_{HK4} \Box A & & H.I\,i \\
 & \vdots & & & & \vdots & & \\
j: & \Delta, A|\ \Gamma \vdash_{CS4} C & & \longmapsto & l: & \Delta^{\Box}, \Box A; \Gamma \vdash_{HK4} C & & H.I\,j \\
 & \vdots & & & & \vdots & & \\
n: & \Delta|\ \Gamma \vdash_{CS4} C & (\Box E)(i,j) & & m: & \Delta^{\Box}; \Gamma \vdash_{HK4} \Box A \to C & & (\mathit{Teo.Ded.Gen.Prem})\ l \\
 & & & & m+1: & (\Delta^{\Box}; \Gamma); (\Delta^{\Box}; \Gamma) \vdash_{HK4} C & & (\mathit{MP})\ (k,\ m) \\
 & & & & m+2: & \Delta^{\Box}; \Gamma \vdash_{HK4} C & & (\text{contracción})\ m+1 \\
 & \vdots & & & & \vdots & &
\end{array}
$$

Como ejemplo realizamos el proceso de traducción correspondiente a la derivación del ejemplo 3.6.

Ejemplo 4.1. $\cdot \vdash_{HK4} \Box(A \to B) \to \Box(\Box A \to \Box B)$

Demostración. Prueba por derivación.

1. $\cdot \vdash_{HK4} \Box(A \to B) \to (A \to B)$ $\mathbb{T}$
2. $(\Box(A \to B), \Box A); \cdot \vdash_{HK4} \Box(A \to B)$ *Hip*
3. $(\Box(A \to B), \Box A); \cdot \vdash_{HK4} A \to B$ *MP* (1, 2)
4. $\cdot \vdash_{HK4} \Box A \to A$ $\mathbb{T}$
5. $(\Box(A \to B), \Box A); \cdot \vdash_{HK4} \Box A$ *Hip*
6. $(\Box(A \to B), \Box A); \cdot \vdash_{HK4} A$ *MP* (4, 5)
7. $((\Box(A \to B), \Box A); \cdot); ((\Box(A \to B), \Box A); \cdot) \vdash_{HK4} B$ *MP* (3, 6)
8. $(\Box(A \to B), \Box A); \cdot \vdash_{HK4} B$ *contracción* (7)
9. $(\Box(A \to B), \Box A); \cdot \vdash_{HK4} \Box A$ *Hip*
10. $(\Box(A \to B), \Box A); \Box A \vdash_{HK4} \Box B$ *NecGen* (8)
11. $(\Box(A \to B)); \Box A \vdash_{HK4} \Box A \to \Box B$ *Teo.Ded.Gen.Prem* (10)
12. $((\Box(A \to B)); \Box A); ((\Box(A \to B)); \Box A) \vdash_{HK4} \Box B$ *MP* (11, 9)
13. $(\Box(A \to B)); \Box A \vdash_{HK4} \Box B$ *contracción* (12)
14. $(\Box(A \to B)); \cdot \vdash_{HK4} \Box A \to \Box B$ *Teo.Deducción.* (13)
15. $(\Box(A \to B)); \Box(A \to B) \vdash_{HK4} \Box(\Box A \to \Box B)$ *NecGen* (14)
16. $\cdot; \Box(A \to B) \vdash_{HK4} \Box(A \to B)$ *Hip*
17. $\cdot; \Box(A \to B) \vdash_{HK4} \Box(A \to B) \to \Box(\Box A \to \Box B)$ *Teo.Ded.Gen.Prem* (15)

18. $(\cdot; \Box(A \to B)); (\cdot; \Box(A \to B)) \vdash_{HK4} \Box(\Box A \to \Box B)$ *MP* (16, 17)

19. $\cdot; \Box(A \to B) \vdash_{HK4} \Box(\Box A \to \Box B)$ *contracción* (18)

20. $\cdot; \cdot \vdash_{HK4} \Box(A \to B) \to \Box(\Box A \to \Box B)$ *Teo.Deducción.* (19)

■

En este capítulo se presentaron las demostraciones de las equivalencias de los sistemas. Como las pruebas son constructivas, se dio un "algoritmo" para poder realizar la equivalencia del sistema *CS4* a *HK4*.

Capítulo 5

Verificación Formal en COQ

En este capítulo se presenta la formalización en el asistente de pruebas COQ [27] de los sistemas deductivos *HK4*, *CS4* y sus propiedades, así como el teorema de equivalencia entre ambos sistemas. Asumimos que el lector conoce el funcionamiento de dicho asistente de pruebas y apuntamos para información particular sobre el mismo [5] [4].

El área de la computación conocida como verificación formal surge de querer crear un código libre de errores, Edsger Dijkstra y Tony Hoare establecieron una visión para incorporar pruebas de corrección en la forma en que se escriben los programas. Una especificación formal de un programa es una oración expresada en lenguaje matemático, donde la sintaxis y la semántica son definidas formalmente. Algunas ventajas de emplear un lenguaje formal es entender del comportamiento y diseño del programa, así como corregir errores sintácticos y semánticos. La manera de detectar errores y/o probar la corrección del programa, es por medio de métodos matemáticos, a esto le llamamos verificación formal, que es la forma de probar que el programa cumple la propiedad de la especificación [28].

Veamos un ejemplo de especificación formal.

Ejemplo 5.1. Sean m_1 y m_2, dos matrices de 2 x 2.

$$Si \;\; m_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad y \quad m_2 = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \quad entonces \quad (m_1 + m_2) = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

Este enunciado es una especificación formal de alto nivel, puesto que involucra objetos y operaciones matemáticas sin presentar su implementación. La cual se realiza utilizando un lenguaje de programación y una estructura de datos en particular, digamos `Java` y arreglos bidimensionales:

```
int [][] matriz_suma(){
    int[][] m1 = new int [2][2];
    int[][] m2 = new int [2][2];
    int [][] sumam = new int [2][2];
```

```
        int i, j;

        for (i = 0; i < m1.length; i++){
            for (j = 0; j < m1[i].length; j++){
                sumam[i][j] = m1[i][j] + m2[i][j];
            }
        }
        return this.sumam;
    }
```

Sin embargo aún queda por resolver el problema de que si esta implementación particular cumple la especificación formal anterior. El proceso de verificación formal se encarga de resolver esta clase de problemas.

La especificación y verificación formal de los sistemas *HK4* y *CS4* se dará en el asistente de pruebas COQ. Un asistente de pruebas es una herramienta computacional que nos permite realizar pruebas formales de manera interactiva con el usuario.

El asistente de pruebas COQ [27], es una sofisticada implementación de una lógica de orden superior llamada cálculo de construcciones inductivas. Esto permite definir en el mismo ambiente programas funcionales, así como especificaciones o propiedades acerca de ellos y más aún las demostraciones formales de dichas propiedades. Para esto, COQ implementa un lenguaje matemático de alto nivel para la especificación llamado *GALLINA*.

El proceso de verificación formal en COQ consiste de manera general de las siguientes cuatro etapas.

- Definición de las estructuras de datos.
- Desarrollo de la implementación.
- Especificación formal de propiedades o teoremas.
- Demostraciones de los anteriores.

Algunos ejemplos correspondientes a estas etapas, en nuestra implementación particular, son los siguientes.

- Estructura de Datos: Contextos Γ y derivaciones $\Gamma \vdash A$.
- Implementación: Operación de pertenencia de un elemento a un contexto (`elem A G`), función de concatenación de contextos (;).
- Especificación:
    - La operación ; es asociativa.
    - Propiedad de permutación entre contextos: Si $\Gamma_1; \Gamma_2 \vdash_{HK4} A$ *entonces* $\Gamma_2\,;\,\Gamma_1 \vdash_{HK4}\ A$
    - Teorema de la deducción: Si $\Gamma, A \vdash B$ entonces $\Gamma \vdash A \to B$.

A continuación presentamos más a detalle algunas partes de la implementación, correspondientes a las tres primeras etapas. La cuarta etapa, correspondiente a las demostraciones, se encuentra disponible en los scripts de COQ.

5.1. Contextos

Para nuestros propósitos, un contexto es un lista finita donde los elementos se van agregando al final, lo cual se conoce como una lista `snoc`.

$$\texttt{ctx} =_{def} \texttt{empty} \mid \texttt{Snoc ctx Proposition}$$

La especificación de los contextos, se presenta a continuación.

- `empty` implementa al contexto vacío.
- `Snoc G A` implementa la operación de agregar la proposición A al contexto Γ y se denota como `G, A`.
- ```
  Fixpoint conc (G D : ctx): ctx :=
  match D with
     | empty ⇒ G
     | Snoc D' p ⇒ Snoc (conc G D') p.
  ```

  la función `conc` implementa la concatenación de contextos Γ y Δ y la notación es `G;D`.

En la verificación formal, se tiene que dar la especificación de propiedades básicas que omitimos durante una prueba a papel por ejemplo, las siguientes propiedades de los contextos:

```
ctx_empty_conc: forall (G : ctx) , (empty;G) = G.
ctx_conc_empty: forall (G : ctx) , (G;empty) = G.
ctx_snoc_conc:  forall (G G': ctx) (A B: Proposition),
                (((G, A); G'), B) = ((G, A);(G', B)).
ctx_snoc_concbis: forall (G G': ctx) (A B: Proposition),
                  (((G, A), B); G') = ((G, A);((empty, B); G')).
ctx_conc_conc: forall (G G' G'' : ctx), G; (G'; G'') = (G; G'); G''.
ctx_nempty_split: forall (G: ctx),
              G <> empty → exists (G1 G2:ctx), G = G1; G2.
```

El importante lema de descomposición de contextos, que nos permitió obtener una prueba relativamente directa del teorema de la deducción, se especifica de la siguiente manera.

```
ctx_decomposition: forall (G D P: ctx) (A: Proposition),
(G;D = P, A) → (D = empty ∧ G = P, A) ∨ exists (G'': ctx), D = (G'', A).
```

5.2. *HK4*

La especificación de la sintaxis de *HK4* es:

- `VarP n` implementa a P_n.
- `Impl A B` implementa a $A \to B$ y se denota por `A ==> B`.
```

- Box A implementa a $\Box A$ y se denota por #A.

La noción de derivación del sistema *HK4* está implementado mediante el siguiente predicado inductivo:

```
Inductive Hk4: ctx → prop → Prop:=
| Hip: forall (G: ctx)(A: prop),
elem A G → Hk4 G  A
| AxI: forall (G: ctx) (A: prop),
Hk4 G (A ==> A)
| K: forall (G: ctx) (A B: prop),
Hk4 G (A ==>(B ==>  A))
| W: forall (G: ctx) (A B: prop),
Hk4 G ((A ==> (A ==> B)) ==> (A ==> B))
| C: forall (G': ctx) (A B C: prop),
Hk4 G' ((A ==> (B ==> C)) ==> (B ==>(A ==> C)))
| B: forall (G': ctx) (A B C: prop),
Hk4 G' ((B ==> C) ==> ((A ==> B) ==> (A ==> C)))
| EK: forall (G: ctx) (A B: prop),
Hk4 G (Box(A ==> B) ==> (Box A) ==> (Box B))
| E4: forall (G : ctx) (A : prop),
Hk4 G (Box A ==> Box(Box A))
| ET: forall (G : ctx) (A : prop),
Hk4 G (Box A ==> A)
| MP: forall (G D:ctx) (A B: prop),
Hk4 G A → Hk4 D (A ==> B) → Hk4 (G ; D) B
| Nec: forall (G: ctx) (A: prop),
Hk4 empty A → Hk4  G (Box A).
```

de tal forma que Hk4 G A implementa a $\Gamma \vdash_{HK4} A$, lo cual se refleja con la siguiente notación

```
Notation "G |- A" := (Hk4 G A) (at level 30).
```

La especificación de algunas derivaciones del sistema *HK4* que se probaron anteriormente son:

```
Theorem InverseDeductionTh:
forall (G: ctx) (A B: Proposition), G |- (A ==>  B) → G, A |- B.

Corollary ContractionGen:
forall (n:nat) (G: ctx) (A B: Proposition), G; (replicate A n) |- B → G |- (A ==>  B).

Lemma Cut:
forall (G G': ctx) (A B : Proposition), (G |- A) → (G', A |- B) → (G'; G |- B).

Theorem DeductionTh_Prem:
forall (G' G: ctx) (A B: Proposition), (G, A); G' |- B → G; G' |- (A ==>  B).

Proposition Weakening_R:
forall (G G': ctx) (A : Proposition), G |- A → (G; G') |- A.
```

Teniendo la especificación y verificación formal de propiedades y operaciones sobre el sistema *HK4*, a continuación veremos la especificación el teorema de la deducción en *HK4*.

```
Theorem DeductionTh:
forall (G : ctx) (A B : Proposition), (G, A) |- B → G |- (A ==> B).
```

La prueba del teorema de la deducción en COQ, es similar a la prueba que se presenta en 2.1. Con esto se certifica formalmente que el teorema de la deducción en la lógica modal constructiva $S4$ es válido, por lo que la controversia de la regla de necesitación está resuelta.

5.3. *CS4*

La especificación formal del sistema *CS4*, sus propiedades y operaciones se presentan a continuación.
Los contextos de hipótesis válidas y verdaderas se implementan como:

```
Definition TrueHyps : Set := ctx.
Definition ValHyps : Set := ctx.
```

La noción de derivación del sistema *CS4* está implementado mediante el siguiente predicado inductivo:

```
Inductive Cs4 : ValHyps → TrueHyps → Proposicion → Prop :=
| nd_thyp : forall (D : ValHyps) (G G' : TrueHyps) (A : Proposicion),
Cs4 D ((G,A) ; G') A

| nd_vhyp : forall (D D': ValHyps) (G : TrueHyps) (B : Proposicion),
Cs4 (D,B ; D') G B

| nd_intro : forall (D : ValHyps) (G : TrueHyps) (A B : Proposicion),
Cs4 D (G,A) B → Cs4 D G (A ==> B)

| nd_apply : forall (D : ValHyps) (G : TrueHyps) (A B : Proposicion),
Cs4 D G (A ==> B) → Cs4 D G A → Cs4 D G B

| nd_boxI : forall (D : ValHyps) (G : TrueHyps) (A: Proposicion),
Cs4 D empty A → Cs4 D G (Box A)

| nd_boxE : forall (D : ValHyps) (G : TrueHyps) (A C : Proposicion),
Cs4 D G (Box A) → Cs4 (D,A) G C  → Cs4 D G C.
```

de tal forma que `Cs4 D G A` implementa a $\Delta \mid \Gamma \vdash_{CS4} A$, lo cual se refleja con la siguiente notación

```
Notation "D | G |- A" := (Cs4 D G A) (at level 30).
```

La especificación de unas propiedades del sistema *CS4* que se probaron anteriormente son:

```
Lemma weakening_thyps:
D | (G ; G') |- A → forall (B : Proposition), D | (G, B ; G') |- A.
```

```
Lemma ctx_weak_R:
D | G |- A → forall (G': ctx), D | (G;G') |- A.

Proposition val_to_true:
(D,A) | G |- B → D | (G, *A) |- B.

Corollary intro_val:
(D,A) | G |- B → D | G |- (*A ==> B).

Corollary ctx_val_to_true:
D | G |- A → empty | (boxed D; G) |- A.
```

La función `boxed` se define como:

```
Fixpoint boxed (c:ctx) : ctx :=
match c with
  | empty ⇒ empty
  | snoc G' b ⇒ snoc (boxed G') (Box b)
end.
```

Una vez dada la especificación y verificación formal de propiedades y operaciones del sistema *CS4* damos la especificación de la equivalencia entre los sistemas.

5.4. Equivalencia

A continuación se presenta la especificación de los teorema de equivalencia entre los sistemas *HK4* y *CS4*.

La especificación del teorema que representa la derivación de A en *CS4* a partir de que derivó A en *HK4* 4.1 es:

```
Theorem HK4_to_CS4:
forall (G: ctx) (A: Proposition), (G |- A) → empty | G |- A).
```

donde la prueba es similar a la prueba del teorema 4.1 presentado en el capítulo 4.

Y el teorema de regreso, *CS4* a *HK4*, está especificado como:

```
Theorem CS4_to_HK4:
forall (D: ctx) (G: ctx) (A: Proposition), D | G |- A → boxed D; G |- A.
```

En este capítulo se mostró la especificación y verificación formal de los sistemas *HK4* y *CS4*, sus propiedades y la equivalencia entre los sistemas. Esto justifica formalmente la idea intuitiva de que en la lógica modal $S4$, un sistema axiomático de Hilbert es equivalente a un sistema de deducción natural.

En el siguiente y último capítulo se exhiben las conclusiones y trabajo a futuro, relacionados a nuestra verificación formal.

Conclusiones y Trabajo a futuro

El propósito y el producto final de este trabajo fue desarrollar una verificación formal de los siguientes aspectos deductivos de la lógica modal constructiva $S4$ en el asistente de pruebas COQ.

- Un sistema axiomático de Hilbert con manejo explícito de hipótesis, llamado *HK4*, que resuelve la controversia de la validez del teorema de la deducción en lógica modal.
- La demostración del teorema de la deducción en *HK4*.
- Un sistema de deducción natural, llamado *CS4*, que utiliza dos contextos correspondientes a hipótesis válidas y verdaderas. Esta característica permite un razonamiento más adecuado para la práctica al permitir la transferencia de fórmulas modales entre ambos contextos.
- La equivalencia de los sistemas deductivos *HK4* y *CS4*.

Para lograr las demostraciones de todo lo anterior fue necesario identificar diversos resultados y operaciones auxiliares, así como realizar la especificación y verificación formal de las mismas, todo esto dentro del asistente de pruebas.

Trabajo a Futuro

Para terminar nuestra exposición mencionamos dos líneas de trabajo a futuro, la primera consiste en agregar el operador de posibilidad a la lógica *CS4* tal como se describe en [23] [24].

La introducción del operador $\Diamond$ en *CS4* es:

$$\frac{\Delta \mid \ \Gamma \vdash_{CS4} \text{A } \textit{posible}}{\Delta \mid \ \Gamma \vdash_{CS4} \Diamond A} \Diamond I$$

La eliminación del operador $\Diamond$ en *CS4* es:

$$\frac{\Delta \mid \ \Gamma \vdash_{CS4} \text{A } \textit{verdadera} \qquad \Delta \mid \ A \vdash_{CS4} \text{C } \textit{posible}}{\Delta \mid \ \Gamma \vdash_{CS4} C \textit{ posible}} \Diamond E$$

Al hacer las distinciones con verdad y posibilidad se tienen las reglas:

$$\frac{\Delta \mid \ \Gamma \vdash_{CS4} \Box \text{ A } \textit{verdadera} \qquad \Delta, \text{A} \mid \ \Gamma \vdash_{CS4} \text{C } \textit{posible}}{\Delta \mid \ \Gamma \vdash_{CS4} C \textit{posible}} \Box E_p$$

$$\frac{\Delta \mid \ \Gamma \vdash_{CS4} A \ \mathit{verdadera}}{\Delta \mid \ \Gamma \vdash_{CS4} A \ \mathit{posible}} \, nd\_tp$$

Obsérvese que estas reglas de inferencia requieren, del lado derecho del torniquete, dos clases de juicios correspondientes a verdad y posibilidad, a diferencia a los sistemas deductivos usuales. Para definir un sistema axiomático que corresponda a estas reglas de deducción natural es necesario:

- Distinguir verdad y posibilidad en *HK4*.
- Agregar una regla de inferencia en *HK4* para el operador $\Diamond$.
- Construir derivaciones en *CS4* de los esquemas axiomáticos:
  - $\Diamond K : \Box(A \to B) \to (\Diamond A \to \Diamond B)$
  - $\Diamond T : A \to \Diamond A$ y
  - $\Diamond 4 : \Diamond\Diamond A \to \Diamond A$
- Verificar nuevamente la equivalencia entre *CS4* y *HK4* una vez que se haya agregado el operador $\Diamond$.

La segunda línea de trabajo que queremos mencionar se refiere a la semántica de la lógica modal. Dado que la mayoría de las investigaciones en lógica modal y sus derivadas, como las lógicas temporales, epistémicas o híbridas, se basan en la semántica resulta muy relevante utilizar los métodos de verificación formal para certificar resultados semánticos conocidos y también para desarrollar nuevas conclusiones. A este respecto apuntamos a [20], que propone un método eficiente de razonamiento que combina la semántica con los sistemas axiomáticos de Hilbert. Por otra parte, en [3] se propone una implementación de la semántica de marcos de Kripke en COQ, para lógicas modales de orden superior, la cual utiliza ampliamente el mecanismo de tácticas definidas por el usuario en el asistente de pruebas.

Relacionar estos trabajos con la verificación aquí presentada, representa un reto importante para acercar a las lógicas modales al ámbito de las matemáticas formalizadas.

Bibliografía

[1] Alchourrón Carlos. *Introducción: Concepciones de la lógica.* Enciclopedia Iberoamericana de Filosofía. Vol. 77 (pp 11-47). Editorial Trotta.

[2] Barcan Marcus, R. *Strict implication, deducibility and the deduction theorem. The Journal of Symbolic Logic.* Vol. 18. pag. 234-236. 1953.

[3] Benzmüller Christoph, Woltzenlogel Paleo Bruno, *Interacting with Modal Logic in the COQ Proof Assistant.* Computer Science - Theory and Applications - 10th International Computer Science Symposium in Russia, CSR 2015, Listvyanka, Russia, July pag.13-17, 2015, Proceedings.

[4] Bertot Yves. *Coq in a Hurry.* 3rd cycle. Types Summer School, also used at the University of Goteborg, Nice, Ecole Jeunes Chercheurs en Programmation, Universite de Nice, France. 2016, pp.49.

[5] Bertot Yves, Castéran Pierre. *Interactive Theorem Proving and Program Development: Coq'Art: The Calculus of Inductive Constructions.* Springer. 2004.

[6] Blackburn Patrick, Rijke Maarten, Venema Yde. *Modal Logic.* Cambridge University Press. 2002.

[7] Blackburn Patrick, Van Benthem Johan. *Studies in Logic and practical reasoning: Handbook of Modal Logic.* Vol 3. 2007.

[8] Chagrov A., Zakharyaschev M. *Modal Logic.* Clarendon Press. 1997.

[9] Chellas Brian. *Modal Logic. An introduction.* Cambridge University Press. 1980.

[10] Fitting Melvin, *Modal Proof Theory* in Blackburn P., van Benthem J., Wolter F. (eds) Handbook of Modal Logic, pp. 85- 138. Elsevier, Amsterdam. 2007.

[11] Fitting Melvin, *Proof Methods for Modal and Intuitionistic Logics.* Springer science. 1983.

[12] Ganguli, S., Nerode, A. *Effective completeness theorems for modal logic. Annals of Pure and Applied Logic*, vol. 128, pp. 141–195. (2004).

[13] Garson J.W., *Modal Logic for Philosophers.* Cambridge University Press. 2013.

[14] Gödel Kurt. *An interpretation of the intuitionistic propositional calculus* (1933f). In: Feferman, S., et. al. (eds.) Collected Works, vol. 1. pp. 300-303. Oxford: Oxford University Press.

[15] Hakli Raul, Negri Sara, *Does the deduction theorem fail for modal logic?*. Synthese. Vol 187. pag. 849-867. 2012.

[16] Heine Sorensen Morten, Urzyczyn Pawel. *Lectures on the Curry- Howard Isomorphism.* Elsevier Science. 2006

[17] Herstein. I.N. *Álgebra moderna*. Trillas. 1980.

[18] Hughes, G. Cresswell M. *A new introduction to modal logic*. London. 1968.

[19] Huth Michael, Ryan Mark, *Logic in computer science. Modelling and Reasoning about Systems*. Cambridge University Press. 2004.

[20] Jürgen Ohlbach Hans. *Combining Hilbert Style and Semantic Reasoning in a Resolution Framework*. Dept. of Computing. Imperial College. 180 Queen's Gate, London. pag. 205-219. 1998.

[21] Lewis Clarence I. *A survey of Symbolic Logic*. University of California Press. Berkeley. 1918.

[22] Lewis Clarence I. *Symbolic logic.*. New York: The Century Co. 1932.

[23] Linares Arévalo P. Selene, *Deducción natural en lógica modal: Una implementación en COQ*.Tesis de maestría. 2015.

[24] Pfenning F, Davies R., *A judgmental reconstruction of modal logic*. Department of Computer Science, Carnegie Mellon University, Pittsburgh. 2000.

[25] Popkorn Sally, *First steps in Modal logic*. Cambridge University Press. 1994.

[26] Von Plato Jan. *Elements of Logical Reasoning*. Cambridge University Press. 2013.

[27] The Coq Proof Assistant: `https://coq.inria.fr`

[28] Hartnett Kevin (2016). *Hacker-Proof Code Confirmed*. Quanta Magazine. `www.quantamagazine.org/formal-verification-creates-hacker-proof-code-20160920/`