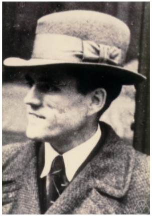
Introducción a la correspondencia entre pruebas y programas:

Eliminación de cortes en el sistema NJ

Alexandre Miquel

marzo de 2021

Introducción



Gerhard **Gentzen** (1909–1945)

1935: *Untersuchungen über das logische Schließen I. & II.*
(Investigaciones sobre las deducciones lógicas I. y II.)

1936: *Die Widerspruchsfreiheit der reinen Zahlentheorie*
(La ausencia de contradicción de la teoría pura de los números)

- El primer artículo introduce:
  - la deducción natural (NJ/NK)
  - el cálculo de secuentes (LJ/LK)
  - la noción de corte (en ambos contextos)
- Teorema de eliminación de cortes en el cálculo de secuentes
  (Teorema adaptado a la deducción natural por Prawitz en 1965)
- El segundo artículo extiende el teorema de eliminación de cortes a la aritmética de Peano, lo que implica su consistencia

$\rightsquigarrow$ Inicio de la interpretación computacional de la lógica

Plan

Plan

Lenguajes de primer orden (recordatorio)

- Un lenguaje de primer orden distingue dos tipos de expresiones:
  - los términos, que sirven para representar objetos
  - las fórmulas, que sirven para representar enunciados
- Cada lenguaje de primer orden está definido a partir de un vocabulario, que consta de:
  - símbolos de función (notación: f, g, h, etc.) con sus aridades
  - símbolos de predicado (notación: p, q, r, etc.) con sus aridades

  La aridad de un símbolo (de función o de predicado) es un entero natural que indica (de modo convencional) el número de argumentos esperado por el símbolo
- Un símbolo de constante es un símbolo de función de aridad 0
- Muchos lenguajes proveen un símbolo de igualdad (i.e. un símbolo de predicado binario escrito $=$)

Términos (recordatorio)

Sea $\mathcal{V}$ un vocabulario. Se considera un conjunto infinito numerable de símbolos de variables (notación: x, y, z, etc.), disjunto de $\mathcal{V}$

Definición (Términos)

Los términos (notación: t, u, v, etc.) inducidos por el vocabulario $\mathcal{V}$ están definidos mediante la gramática:

Términos $\qquad t, u \quad ::= \quad x \quad | \quad f(t_1, \ldots, t_k)$

donde x es cualquier variable y f cualquier símbolo de función de aridad k

Dados términos t, u y una variable x, se escriben:

- $FV(t)$ al conjunto (finito) de las variables libres del término t
- $t[x := u]$ al término obtenido sustituyendo en t cada ocurrencia (libre) de la variable x por el término u

Fórmulas (recordatorio)

Sea $\mathcal{V}$ un vocabulario

Definición (Fórmulas)

Las fórmulas (notación: A, B, C, etc.) inducidas por el vocabulario $\mathcal{V}$ están definidas mediante la gramática:

$$\textbf{Fórmulas} \qquad \begin{array}{rcl} A, B, C & ::= & p(t_1, \ldots, t_k) \;\mid\; \top \;\mid\; \bot \\ & \mid & \neg A \;\mid\; A \wedge B \;\mid\; A \vee B \\ & \mid & A \Rightarrow B \;\mid\; A \Leftrightarrow B \\ & \mid & \forall x\, A \;\mid\; \exists x\, A \end{array}$$

donde p es cualquier símbolo de predicado de aridad k

Dados una fórmula A, un término u y una variable x, se escriben:

- $FV(A)$ al conjunto (finito) de las variables libres de la fórmula A
- $A[x := u]$ a la fórmula obtenida sustituyendo en A cada ocurrencia libre de la variable x por el término u

¡Cuidado a los conflictos entre variables libres y ligadas! $\rightsquigarrow$ α-conversión

¿Cuál sistema de deducción?

- Hay varios métodos equivalentes para presentar las reglas de deducción de la lógica intuicionista (o clásica):

  1. En el estilo de Hilbert (sólo fórmulas, sin secuentes)
  2. En el estilo de Gentzen (reglas izquierdas y derechas)
  3. En el estilo de la deducción natural (con o sin secuentes)

  Como estos sistemas de deducción definen exactamente la misma clase de fórmulas demostrables[1] (para una lógica dada, LJ o LK), la elección de un sistema particular sólo es una cuestión de comodidad

- Los sistemas basados en las fórmulas (sistemas de Hilbert, D. N. sin secuentes) son más fáciles de definir, pero más difíciles de manipular

- En lo siguiente, siempre usaremos sistemas con secuentes

[1] En los sistemas basados en secuentes, las fórmulas están identificadas con los secuentes de la forma $\vdash A$ (con 0 hipótesis y 1 tesis)

Secuentes (recordatorio)

Definición (Secuente) [Gentzen 1934]

Un secuente es un par de listas (finitas) de fórmulas, escrito

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_m \qquad (n, m \geq 0)$$

donde:

- $A_1, \ldots, A_n$ son las hipótesis (que forman el antecedente)
- $B_1, \ldots, B_m$ son las tesis (que forman el consecuente)

- Se usa la notación $\Gamma \vdash \Delta$ (donde Γ, Δ son listas de fórmulas)
- Significado intuitivo: $\bigwedge \Gamma \Rightarrow \bigvee \Delta$
- El secuente vacío "$\vdash$" representa la contradicción
- Las notaciones $FV(A)$ (conjunto de variables libres) y $A[x := u]$ (sustitución) se extienden de modo obvio a las listas de fórmulas $\Gamma \equiv A_1, \ldots, A_n$:

$$\begin{aligned} FV(\Gamma) &:= FV(A_1) \cup \cdots \cup FV(A_n) \\ \Gamma[x := u] &:\equiv A_1[x := u], \ldots, A_n[x := u] \end{aligned}$$

Reglas de inferencia y sistemas de deducción

Se pueden usar las fórmulas y los secuentes como juicios.
Cada sistema de deducción está basado en un conjunto de juicios $\mathscr{J}$ (= un conjunto de expresiones que "asertan algo")

- Dado un conjunto de juicios $\mathscr{J}$:

Definición (Regla de inferencia)

Una regla de inferencia es un par formado por un conjunto finito de juicios $\{J_1, \ldots, J_n\} \subseteq \mathscr{J}$ y un juicio $J \in \mathscr{J}$, escrito típicamente:

$$\frac{J_1 \quad \cdots \quad J_n}{J}$$

- $J_1, \ldots, J_n$ son las premisas de la regla
- J es la conclusión de la regla

Definición (Sistema de deducción)

Un sistema de deducción es un conjunto de reglas de inferencia

Juicios derivables (1/2)

Definición (Derivación)

Sea $\mathscr{S}$ un sistema de deducción basado en un conjunto de juicios $\mathscr{J}$

1. Las derivaciones (de juicios) en $\mathscr{S}$ están definidas inductivamente del modo siguiente:

   Si $d_1, \dots, d_n$ son derivaciones de $J_1, \dots, J_n$ en $\mathscr{S}$, respectivamente, y si $(\{J_1, \dots, J_n\}, J)$ es una regla de $\mathscr{S}$, entonces

   $$d \;=\; \left\{ \dfrac{\begin{array}{c}\vdots\; d_1 \\ J_1\end{array} \quad \cdots \quad \begin{array}{c}\vdots\; d_n \\ J_n\end{array}}{J} \right. \qquad \text{es una derivación de } J \text{ en } \mathscr{S}$$

2. Un juicio J es derivable en $\mathscr{S}$ cuando tiene una derivación en $\mathscr{S}$

- Por definición, el conjunto de los juicios derivables en $\mathscr{S}$ es el mínimo conjunto de juicios cerrado por las reglas en $\mathscr{S}$

Juicios derivables (2/2)

- Dos sistemas de deducción (basados en la misma noción de juicio) son equivalentes cuando inducen los mismos juicios derivables

Definición (Regla admisible)

Una regla $R = (\{J_1, \ldots, J_n\}, J)$ es admisible en un sistema $\mathscr{S}$ cuando: $J_1, \ldots, J_n$ derivables en $\mathscr{S}$ implica que J es derivable en $\mathscr{S}$.

Las reglas admisibles se escriben tradicionalmente:

$$\begin{array}{c} J_1 \quad \cdots \quad J_n \\ \hline\hline J \end{array}$$

- Claramente: R admisible en $\mathscr{S}$ sii $\mathscr{S} \cup \{R\}$ equivalente a $\mathscr{S}$
- **Obs.:** En la práctica, se definen los sistemas de deducción a partir de esquemas de reglas (i.e. familias de reglas), que todavía se llaman reglas. La noción de regla admisible se extiende inmediatamente a los esquemas

Los símbolos de la implicación

En lógica, hay (al menos) tres símbolos para representar la implicación:

- El símbolo de implicación $\Rightarrow$, en las fórmulas. Representa un punto potencial para una deducción, pero no un paso real de deducción
- El símbolo $\vdash$ (« tesis »), en los secuentes. Como $\Rightarrow$, pero en un secuente, que representa una fórmula (parcialmente) descompuesta:

$$\begin{array}{rc} & A_1, \ldots, A_n \vdash B_1, \ldots, B_m \\ \approx & A_1 \wedge \cdots \wedge A_n \Rightarrow B_1 \vee \cdots \vee B_m \end{array}$$

- La raya de inferencia " ——————— ", en las reglas y las derivaciones. Este símbolo representa un paso real de deducción:

$$\frac{P_1 \quad \cdots \quad P_n}{C} \qquad \left(\begin{array}{l}\text{De } P_1,\ldots,P_n \\ \text{deducir } C\end{array}\right)$$

Significado de los secuentes

- Los secuentes no enriquecen la expresividad de un sistema lógico; sólo sirven para representar un estado de demostración, o una fórmula parcialmente descompuesta:

$$\Gamma \vdash \Delta \qquad \approx \qquad \bigwedge \Gamma \Rightarrow \bigvee \Delta$$

(Con las convenciones $\bigwedge \varnothing := \top$ y $\bigvee \varnothing := \bot$)

- En (¿casi?) todos los sistemas de la literatura, tenemos que:

$$\Gamma \vdash \Delta \ \text{ derivable} \qquad \text{sii} \qquad \vdash \left(\bigwedge \Gamma \Rightarrow \bigvee \Delta\right) \ \text{ derivable}$$

Esta equivalencia se cumple, al menos:
  - En el cálculo de secuentes de Gentzen (LK)
  - En el cálculo de secuentes intuicionista (LJ)
  - En deducción natural intuicionista/clásica (NJ/NK)
  - En lógica lineal (LL), remplazando $\wedge$, $\vee$, $\top$, $\bot$, $\Rightarrow$ por $\otimes$, $\parr$, 1, $\bot$, $\multimap$

- **Ejercicio:** Verificarlo para los sistemas NJ/NK presentados más abajo

Plan

Simplificación del lenguaje de fórmulas

En lo siguiente, trabajaremos con un lenguaje de fórmulas simplificado

Fórmulas
$$\begin{array}{rcl} A, B, C & ::= & p(t_1, \ldots, t_k) \quad | \quad \top \quad | \quad \bot \\ & | & A \wedge B \quad | \quad A \vee B \quad | \quad A \Rightarrow B \\ & | & \forall x\, A \quad | \quad \exists x\, A \end{array}$$

en el cual la negación $\neg A$ y la equivalencia lógica $A \Leftrightarrow B$ son construcciones definidas mediante las abreviaturas:

$$\neg A \;:\equiv\; A \Rightarrow \bot \qquad\qquad A \Leftrightarrow B \;:\equiv\; (A \Rightarrow B) \wedge (B \Rightarrow A)$$

Observación: Todas las construcciones restantes son primitivas.
En efecto, en lógica intuicionista, las leyes de De Morgan no son válidas, de tal modo que dichas construcciones no son definibles entre sí[2]

[2] Con la excepción de $\top$, que se puede definir por $\top \;:\equiv\; \bot \Rightarrow \bot$

Deducción natural intuicionista (NJ)

- La deducción natural intuicionista (sistema NJ) es un sistema de deducción basado en secuentes asimétricos de la forma:

$$A_1, \ldots, A_n \vdash A \qquad \text{es decir:} \qquad \Gamma \vdash A$$

  Estos secuentes también se llaman secuentes intuicionistas

- Recordatorio: $\Gamma \vdash A$ tiene el mismo significado que $\bigwedge \Gamma \Rightarrow A$
- El sistema NJ tiene tres tipos de (esquemas de) reglas:
  - Las reglas de introducción, que definen cómo se <u>demuestran</u> las construcciones lógicas
  - Las reglas de eliminación, que definen cómo se <u>usan</u> las construcciones lógicas
  - La regla axioma, que es una regla de conservación
- La Trimūrti de la lógica:

Reglas de introducción	=	Brahmá
Reglas de eliminación	=	Shiva
Regla axioma	=	Vishnú

Reglas de deducción del sistema NJ (1/2)

- Reglas del cálculo proposicional intuicionista:

	Introducción	Eliminación
(Axioma)	$\dfrac{}{\Gamma \vdash A}$ si $A \in \Gamma$	
$(\Rightarrow)$	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$	$\dfrac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$
$(\wedge)$	$\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$	$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$ $\qquad$ $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$
$(\vee)$	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$ $\qquad$ $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$	$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$
$(\top)$	$\dfrac{}{\Gamma \vdash \top}$	(sin regla de eliminación)
$(\bot)$	(sin regla de introducción)	$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}$

Reglas de deducción del sistema NJ (2/2)

- Reglas de introducción y de eliminación de los cuantificadores:

$$(\forall)\qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x\, A}\ \text{si } x \notin FV(\Gamma) \qquad\Big|\qquad \frac{\Gamma \vdash \forall x\, A}{\Gamma \vdash A[x := t]}$$

$$(\exists)\qquad \frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x\, A} \qquad\Big|\qquad \frac{\Gamma \vdash \exists x\, A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \text{si } x \notin FV(\Gamma, B)$$

- Reglas de introducción y de eliminación de la igualdad:

$$(=)\qquad \frac{}{\Gamma \vdash t = t} \qquad\Big|\qquad \frac{\Gamma \vdash t = u \qquad \Gamma \vdash A[x := t]}{\Gamma \vdash A[x := u]}$$

Reglas derivadas

- **Reglas de la negación:**

  Las reglas de la negación $\neg A \ :\equiv\ A \Rightarrow \bot$ aparecen como un caso particular de las reglas de la implicación:

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A} \qquad\qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}$$

- **Reglas de la equivalencia lógica:**

  Similarmente, se pueden derivar las reglas de la equivalencia lógica

$$A \Leftrightarrow B \ :\equiv\ (A \Rightarrow B) \wedge (B \Rightarrow A)$$

  a partir de las reglas de la conjunción y de la implicación:

$$\frac{\Gamma, A \vdash B \qquad \Gamma, B \vdash A}{\Gamma \vdash A \Leftrightarrow B} \qquad \frac{\Gamma \vdash A \Leftrightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B} \qquad \frac{\Gamma \vdash A \Leftrightarrow B \qquad \Gamma \vdash B}{\Gamma \vdash A}$$

Ejercicio: Escribir las derivaciones correspondientes

Ejemplos de derivaciones (1/2)

$$
\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\,(\text{ax})}{A \wedge B \vdash B}\,(\wedge\text{-el}_2) \qquad \dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\,(\text{ax})}{A \wedge B \vdash A}\,(\wedge\text{-el}_1)}{\dfrac{A \wedge B \vdash B \wedge A}{\vdash A \wedge B \Rightarrow B \wedge A}\,(\Rightarrow\text{-in})}\,(\wedge\text{-in})
$$

$$
\dfrac{\dfrac{}{A \vee B \vdash A \vee B}\,(\text{ax}) \qquad \dfrac{\dfrac{}{A \vee B,\ A \vdash A}\,(\text{ax})}{A \vee B,\ A \vdash B \vee A}\,(\vee\text{-in}_2) \qquad \dfrac{\dfrac{}{A \vee B,\ B \vdash B}\,(\text{ax})}{A \vee B,\ B \vdash B \vee A}\,(\vee\text{-in}_1)}{\dfrac{A \vee B \vdash B \vee A}{\vdash A \vee B \Rightarrow B \vee A}\,(\Rightarrow\text{-in})}\,(\vee\text{-el})
$$

Ejemplos de derivaciones (2/2)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x = y \vdash x = y}\,(\text{ax}) \qquad \dfrac{}{x = y \vdash x = x}\,(\text{=-in})}{x = y \vdash y = x}\,(\text{=-el, con } A(z) \equiv z{=}x)}{\vdash x = y \Rightarrow y = x}\,(\Rightarrow\text{-in})}{\vdash \forall y\,(x = y \Rightarrow y = x)}\,(\forall\text{-in})}{\vdash \forall x\,\forall y\,(x = y \Rightarrow y = x)}\,(\forall\text{-in})$$

$$\dfrac{\dfrac{\dfrac{}{\exists y\,\forall x\,A(x,y) \vdash \exists y\,\forall x\,A(x,y)}\,(\textbf{ax}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\exists y\,\forall x\,A(x,y),\ \forall x\,A(x,y_0) \vdash \forall x\,A(x,y_0)}\,(\textbf{ax})}{\exists y\,\forall x\,A(x,y),\ \forall x\,A(x,y_0) \vdash A(x,y_0)}\,(\forall\textbf{-el})}{\exists y\,\forall x\,A(x,y),\ \forall x\,A(x,y_0) \vdash \exists y\,A(x,y)}\,(\exists\textbf{-in})}{\exists y\,\forall x\,A(x,y),\ \forall x\,A(x,y_0) \vdash \forall x\,\exists y\,A(x,y)}\,(\forall\textbf{-in})}{\dfrac{\exists y\,\forall x\,A(x,y) \vdash \forall x\,\exists y\,A(x,y)}{\vdash \exists y\,\forall x\,A(x,y) \Rightarrow \forall x\,\exists y\,A(x,y)}\,(\Rightarrow\textbf{-in})}\,(\exists\textbf{-el})$$

Geometría de las reglas (1/3)

- **Idea fundamental:** Cada construcción (conectiva, cuantificador, igualdad) está definida por sus reglas de introducción & eliminación
- Por ejemplo, para verificar que $A \wedge B$ está definida por las reglas

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad\qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

  basta con introducir una nueva conectiva $A \heartsuit B$ con las reglas

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \heartsuit B} \qquad\qquad \frac{\Gamma \vdash A \heartsuit B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \heartsuit B}{\Gamma \vdash B}$$

  y derivar en el nuevo sistema la equivalencia deseada:

$$\vdash \; A \wedge B \;\Leftrightarrow\; A \heartsuit B$$

- **Ejercicio:** 1. Derivar la equivalencia anterior

  2. Hacer el mismo ejercicio con $\vee$, $\Rightarrow$, $\top$, $\bot$, $\forall$, $\exists$, $=$

Geometría de las reglas (2/3)

- Por analogía con las reglas de la conjunción usual (i.e. binaria)

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad\qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

se puede definir una conjunción de aridad $n \geq 0$ con las reglas:

$$\frac{\Gamma \vdash A_1 \quad \cdots \quad \Gamma \vdash A_n}{\Gamma \vdash A_1 \wedge \cdots \wedge A_n} \qquad \frac{\Gamma \vdash A_1 \wedge \cdots \wedge A_n}{\Gamma \vdash A_1} \quad \cdots \quad \frac{\Gamma \vdash A_1 \wedge \cdots \wedge A_n}{\Gamma \vdash A_n}$$

- Considerando el caso $n = 0$, se obtienen las reglas...

$$\frac{}{\Gamma \vdash \wedge_0} \qquad\qquad \text{(0 regla de eliminación)}$$

... de la conectiva $\top \ \equiv \ \wedge_0$

Geometría de las reglas (3/3)

- Por analogía con las reglas de la disyunción usual (i.e. binaria)

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}$$

se puede definir una disyunción de aridad $n \geq 0$ con las reglas:

$$\frac{\Gamma \vdash A_1}{\Gamma \vdash A_1 \vee \cdots \vee A_n} \quad \cdots \quad \frac{\Gamma \vdash A_n}{\Gamma \vdash A_1 \vee \cdots \vee A_n}$$

$$\frac{\Gamma \vdash A_1 \vee \cdots \vee A_n \qquad \Gamma, A_1 \vdash C \quad \ldots \quad \Gamma, A_n \vdash C}{\Gamma \vdash C}$$

- Considerando el caso $n = 0$, se obtienen las reglas...

(0 regla de introducción) $$\frac{\Gamma \vdash \vee_0}{\Gamma \vdash C}$$

... de la conectiva $\bot \ \equiv \ \vee_0$

Propiedades

Se escribe $\Gamma \subseteq \Gamma'$ cuando cada hipótesis que ocurre en Γ también ocurre en Γ' (sin tener en cuenta ni el orden ni el número de ocurrencias)

Proposición (Debilitamiento generalizado)

La siguiente regla de inferencia es admisible en el sistema NJ:

$$\frac{\Gamma \vdash A}{\Gamma' \vdash A} \ \text{si } \Gamma\subseteq\Gamma'$$

Demostración. Se trata de demostrar que si un secuente $\Gamma \vdash A$ tiene derivación d, entonces para todo $\Gamma' \supseteq \Gamma$, el secuente $\Gamma' \vdash A$ tiene (otra) derivación d' (en NJ).

Formalmente, la derivación $d' : (\Gamma' \vdash A)$ se construye por recurrencia sobre la derivación $d : (\Gamma \vdash A)$, remplazando (en d) cada secuente de la forma $\Gamma, \Delta \vdash C$ por el secuente $\Gamma', \Delta \vdash C$. $\square$

Obs. Las derivaciones d y d' tienen los mismos pasos de deducción (y en el mismo orden); sólo cambian los antecedentes de los secuentes subyacentes

Propiedades (2/3)

La regla (admisible) de debilitamiento generalizado

$$\frac{\Gamma \vdash A}{\Gamma' \vdash A} \text{ si } \Gamma \subseteq \Gamma'$$

implica otras tres reglas admisibles:

(Permutación) $\dfrac{\Gamma \vdash A}{\sigma(\Gamma) \vdash A}$ (σ permutación de Γ)

(Debilitamiento) $\dfrac{\Gamma \vdash A}{\Gamma, B \vdash A}$

(Contracción) $\dfrac{\Gamma, B, B \vdash A}{\Gamma, B \vdash A}$

Propiedades (3/3)

Proposición (Sustitutividad)

La siguiente regla de inferencia es admisible en el sistema NJ:

$$\frac{\Gamma \vdash A}{\Gamma[x := u] \vdash A[x := u]}$$

Demostración. Por recurrencia sobre la derivación d del secuente $\Gamma \vdash A$ se construye una derivación $d[x := u]$ del secuente $\Gamma[x := u] \vdash A[x := u]$, remplazando (en d) cada secuente de la forma $\Gamma, \Delta \vdash C$ por el secuente $\Gamma[x := u], \Delta[x := u] \vdash C[x := u]$. □

Obs. Como anteriormente, las derivaciones d y $d[x := u]$ tienen los mismos pasos de deducción (y en el mismo orden); sólo cambian los secuentes subyacentes

Deducción natural clásica (sistema NK)

- La deducción natural clásica (sistema NK) se define a partir del sistema NJ, remplazando la regla

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ (\textit{ex falso quod libet}) \qquad \text{por} \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (\textit{reductio ad absurdum})$$

- Como en el sistema NJ, la regla de debilitamiento generalizado (que implica las reglas de permutación, debilitamiento y contracción) así como la regla de sustitutividad son admisibles en el sistema NK

- En particular, la regla del "*ex falso quod libet*" es admisible en el sistema NK, y por lo tanto:

Proposición (Inclusión NJ $\subset$ NK)

Todo secuente derivable en NJ también es derivable en NK

El recíproco no se cumple: el secuente $\vdash x = y \lor x \neq y$ es derivable en el sistema NK, pero no es derivable en el sistema NJ (prueba más adelante)

Plan

La noción de corte (1/3)

- Un corte es un trozo de derivación formado por una introducción de cierta construcción X inmediatamente seguida por una eliminación de la misma construcción X:

$$
\dfrac{\dfrac{\begin{matrix}\vdots\, d_1 \\ ?\vdash ?\end{matrix} \quad \dots \quad \begin{matrix}\vdots\, d_n \\ ?\vdash ?\end{matrix}}{\cdots \vdash X(\cdots)}\,(X\text{-in}_i) \qquad \begin{matrix}\vdots\, d'_1 \\ ?\vdash ?\end{matrix} \quad \dots \quad \begin{matrix}\vdots\, d'_m \\ ?\vdash ?\end{matrix}}{?\vdash ?}\,(X\text{-el}_j)
$$

  La formula $X(\cdots)$ introducida y eliminada es la fórmula cortada

- Intuitivamente, un corte representa un «desvío» en una derivación

- **Ejemplo:** corte de implicación:

$$
\dfrac{\dfrac{\begin{matrix}\vdots\, d \\ \Gamma, A\vdash B\end{matrix}}{\Gamma\vdash A\Rightarrow B}\,(\Rightarrow\text{-in}) \qquad \begin{matrix}\vdots\, d' \\ \Gamma\vdash A\end{matrix}}{\Gamma\vdash B}\,(\Rightarrow\text{-el})
$$

La noción de corte (2/3)

- Una construcción lógica (conectiva, cuantificador, igualdad) con n_i reglas de introducción y n_e reglas de eliminación induce $n_i \times n_e$ formas distintas de cortes:

$\Rightarrow$	$1 \times 1 = 1$
$\wedge$	$1 \times 2 = 2$
$\vee$	$2 \times 1 = 2$
$\top$	$1 \times 0 = 0$
$\bot$	$0 \times 1 = 0$
$\forall$	$1 \times 1 = 1$
$\exists$	$1 \times 1 = 1$
$=$	$1 \times 1 = 1$
Total	8

- En total, hay 8 formas distintas de cortes en el sistema NJ

La noción de corte (3/3)

- Cada corte se puede reducir, cancelando la formula cortada (así como el «desvío» correspondiente).

  Veremos más adelante cómo se reducen las 8 formas de corte

- La reducción de un corte puede introducir nuevos cortes en la derivación, o duplicar cortes ya existentes. En muchos casos la reducción de un corte resulta en una derivación más grande (del mismo secuente) y con más cortes

- Sin embargo, Gentzen (1934) y Prawitz (1965) demostraron:

Teorema (Eliminación de cortes en NJ)

El procedimiento de reducción de cortes siempre termina en NJ
(Y esto: independientemente del orden de reducción de los cortes)

Corolario (Derivaciones sin cortes en NJ)

Todo secuente derivable en NJ tiene una derivación sin cortes (en NJ)

Reducción de los cortes

Cortes de $\wedge$:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\, d_1\\ \Gamma \vdash A\end{array} \quad \begin{array}{c}\vdots\, d_2\\ \Gamma \vdash B\end{array}}{\Gamma \vdash \color{red}{A \wedge B}}\,(\wedge\text{-in})}{\Gamma \vdash A}\,(\wedge\text{-el}_\mathbf{1}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\, d_1\\ \Gamma \vdash A\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\, d_1\\ \Gamma \vdash A\end{array} \quad \begin{array}{c}\vdots\, d_2\\ \Gamma \vdash B\end{array}}{\Gamma \vdash \color{red}{A \wedge B}}\,(\wedge\text{-in})}{\Gamma \vdash B}\,(\wedge\text{-el}_\mathbf{2}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\, d_2\\ \Gamma \vdash B\end{array}$$

Sustitución de un axioma

- Se observa que una derivación del secuente $\Gamma, A \vdash B$ sólo contiene secuentes de la forma $\Gamma, A, \Gamma' \vdash B'$ (Γ' y B' cualesquiera)

- Dadas derivaciones $\begin{array}{c} \vdots\ d \\ \Gamma, A \vdash B \end{array}$ y $\begin{array}{c} \vdots\ d' \\ \Gamma \vdash A \end{array}$, se escribe

$$\begin{array}{c} \vdots\ d' \\ \Gamma \vdash A \\ \vdots\ d[\mathrm{ax}(A){:=}d'] \\ \Gamma \vdash B \end{array}$$

  a la derivación del secuente $\Gamma \vdash B$ obtenida a partir de d:

  - eliminando la hipótesis A de todos los secuentes que aparecen en d
  - remplazando cada invocación del axioma A (en un contexto de la forma Γ, A, Γ') por la derivación d' (debilitada en el contexto Γ, Γ')

- **Obs.:** La derivación "sustituida" $d[\mathrm{ax}(A) := d']$ contiene una copia de la derivacíon d' para cada invocación del axioma A en la derivación d

Reducción de los cortes (2/5)

Corte de $\Rightarrow$:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\; d\\ \Gamma, A \vdash B\end{array}}{\Gamma \vdash {\color{red}A \Rightarrow B}}\,(\Rightarrow\text{-in}) \qquad \begin{array}{c}\vdots\; d'\\ \Gamma \vdash A\end{array}}{\Gamma \vdash B}\,(\Rightarrow\text{-el}) \qquad \rightsquigarrow \qquad \begin{array}{l}\quad\vdots\; d'\\ \Gamma \vdash A\\ \quad\vdots\; d[\mathrm{ax}(A){:=}d']\\ \Gamma \vdash B\end{array}$$

Reducción de los cortes

Cortes de $\lor$:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A\end{array}}{\Gamma \vdash A \lor B}\,(\lor\text{-in}_1) \qquad \begin{array}{c}\vdots\ d'_1\\ \Gamma, A \vdash C\end{array} \qquad \begin{array}{c}\vdots\ d'_2\\ \Gamma, B \vdash C\end{array}}{\Gamma \vdash C}\,(\lor\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d\\ \Gamma \vdash A\\ \vdots\ d'_1[\mathrm{ax}(A){:=}d]\\ \Gamma \vdash C\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash B\end{array}}{\Gamma \vdash A \lor B}\,(\lor\text{-in}_2) \qquad \begin{array}{c}\vdots\ d'_1\\ \Gamma, A \vdash C\end{array} \qquad \begin{array}{c}\vdots\ d'_2\\ \Gamma, B \vdash C\end{array}}{\Gamma \vdash C}\,(\lor\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d\\ \Gamma \vdash B\\ \vdots\ d'_2[\mathrm{ax}(B){:=}d]\\ \Gamma \vdash C\end{array}$$

Corte de $\top/\bot$: ninguno

Reducción de los cortes

Corte de $\forall$: $(\text{con} \quad x \notin FV(\Gamma))$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A\end{array}}{\Gamma \vdash \forall x\, A}\ (\forall\text{-in})}{\Gamma \vdash A[x := t]}\ (\forall\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d[x{:=}t]\\ \Gamma \vdash A[x := t]\end{array}$$

Corte de $\exists$: $(\text{con} \quad x \notin FV(\Gamma, B))$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A[x := t]\end{array}}{\Gamma \vdash \exists x\, A}\ (\exists\text{-in}) \qquad \begin{array}{c}\vdots\ d'\\ \Gamma, A \vdash B\end{array}}{\Gamma \vdash B}\ (\exists\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d\\ \Gamma \vdash A[x := t]\\ \vdots\ d'[x{:=}t][\mathrm{ax}(A[x{:=}t]){:=}d]\\ \Gamma \vdash B\end{array}$$

Reducción de los cortes (5/5)

Corte de $=$:

$$\dfrac{\dfrac{}{\Gamma \vdash t = t}\ (=\text{-in}) \qquad \begin{array}{c} \vdots\ d' \\ \Gamma \vdash A[x := t] \end{array}}{\Gamma \vdash A[x := t]}\ (=\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c} \vdots\ d' \\ \Gamma \vdash A[x := t] \end{array}$$

Eliminación de cortes en el sistema NJ

Teorema (Eliminación de cortes en NJ)

El sistema formado por las 8 reglas de reducción anteriores es fuertemente normalizante, en el sentido de que no existe ninguna sucesión infinita de reducciones (entre derivaciones de un mismo secuente):

$$\nexists(d_0 \leadsto d_1 \leadsto d_2 \leadsto \cdots \leadsto d_i \leadsto d_{i+1} \leadsto \cdots)$$

Por lo tanto, toda sucesión de reducciones es finita

Demostración: Postpuesta

Corolario (Derivaciones sin cortes en NJ)

Todo secuente derivable en NJ tiene una derivación sin cortes (en NJ)

Obs.: Las derivaciones sin cortes son en general mucho más largas que las derivaciones con cortes (del mismo secuente)

Alcance filosófico de la eliminación de cortes (1/2)

Intuitivamente, un corte representa la interacción entre:

- la prueba de un lema (que en general se acaba por una introducción) y
- el contexto en que se usa dicho lema (en general: una eliminación)

Reducir los cortes consiste en remplazar cada invocación de un lema por una demostración particular del lema, instanciada con parámetros concretos y adaptada al contexto de invocación. Por ejemplo:

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ P(x)\vdash Q(x)\end{array}}{\vdash P(x)\Rightarrow Q(x)}\,(\Rightarrow\text{-in})}{\vdash \forall x\,(P(x)\Rightarrow Q(x))}\,(\forall\text{-in})}{\vdash P(t)\Rightarrow Q(t)}\,(\forall\text{-el}) \qquad \begin{array}{c}\vdots\ d'\\ \vdash P(t)\end{array}}{\vdash Q(t)}\,(\Rightarrow\text{-el})$$

$$\rightsquigarrow \quad \dfrac{\dfrac{\begin{array}{c}\vdots\ d[x{:=}t]\\ P(t)\vdash Q(t)\end{array}}{\vdash P(t)\Rightarrow Q(t)}\,(\Rightarrow\text{-in}) \qquad \begin{array}{c}\vdots\ d'\\ \vdash P(t)\end{array}}{\vdash Q(t)}\,(\Rightarrow\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d'\\ \vdash P(t)\\ \vdots\ d[x{:=}t][\mathrm{ax}(P(t)){:=}d']\\ \vdash Q(t)\end{array}$$

Alcance filosófico de la eliminación de cortes (2/2)

Se observa que la composición de dos demostraciones de la forma

$$\dfrac{\begin{matrix}\vdots\ d_1\\ A\vdash B\end{matrix}}{\vdash A\Rightarrow B}\,(\Rightarrow\text{-in}) \qquad \text{y} \qquad \dfrac{\begin{matrix}\vdots\ d_2\\ B\vdash C\end{matrix}}{\vdash B\Rightarrow C}\,(\Rightarrow\text{-in})$$

(con o sin cortes) crea naturalmente 2 cortes:

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}\vdots\ d_2\\ B\vdash C\end{matrix}}{\vdash B\Rightarrow C}\,(\Rightarrow\text{-in})}{A\vdash {\color{red}B\Rightarrow C}}\,(\text{Deb.}) \qquad \dfrac{\dfrac{\dfrac{\begin{matrix}\vdots\ d_1\\ A\vdash B\end{matrix}}{\vdash A\Rightarrow B}\,(=\text{-in})}{A\vdash {\color{red}A\Rightarrow B}}\,(\text{Deb.}) \qquad \dfrac{}{A\vdash A}\,(\text{ax})}{A\vdash B}\,(\Rightarrow\text{-el})}{A\vdash C}\,(\Rightarrow\text{-el})}{\vdash A\Rightarrow C}\,(\Rightarrow\text{-in})$$

$\Rightarrow$ Los cortes surgen de la modularidad del razonamiento matemático

Propiedades de las derivaciones sin cortes (1/7)

Proposición (Derivaciones sin cortes de $\vdash A$ en NJ)

En el sistema NJ, toda derivación sin cortes de un secuente de la forma

$$\vdash A \qquad \text{(i.e. con antecedente vacío)}$$

se acaba con una regla de introducción

En particular, una derivación sin cortes...

- ... del secuente $\vdash A \Rightarrow B$ se acaba por la regla $\Rightarrow$-intro
- ... del secuente $\vdash A \wedge B$ se acaba por la regla $\wedge$-intro
- ... del secuente $\vdash A \vee B$ se acaba por la regla $\vee$-intro$_1$ o $\vee$-intro$_2$
- ... del secuente $\vdash \forall x\, A$ se acaba por la regla $\forall$-intro
- ... del secuente $\vdash \exists x\, A$ se acaba por la regla $\exists$-intro

Propiedades de las derivaciones sin cortes (2/7)

Demostración.

Por inducción sobre la estructura de la derivación $d : (\vdash A)$ (sin cortes), distinguiendo los casos en función de la última regla aplicada:

- Regla axioma. Caso imposible, pues el antecedente es vacío.
- Regla de eliminación, por ejemplo: $\Rightarrow$-elim (i.e. *modus ponens*).
  En este caso, la derivación $d : (\vdash A)$ es de la forma

$$d \;\equiv\; \left\{ \begin{array}{c} \dfrac{\begin{array}{c} \vdots\ d_1 \\ \vdash B \Rightarrow A \end{array} \quad \begin{array}{c} \vdots\ d_2 \\ \vdash B \end{array}}{\vdash A} \end{array} \right.$$

  Se observa que la subderivación d_1 del secuente $\vdash B \Rightarrow A$ también es sin cortes. Por hipótesis de inducción, d_1 se acaba con una regla de introducción. Entonces d es un corte, lo que demuestra que este caso es imposible.
- De modo análogo, si d se acaba con otra regla de eliminación, se observa que la subderivación d_1 (sin cortes) de su premisa principal (con antecedente vacío) se acaba por una regla de introducción (por hipótesis de inducción), lo que implica que d es un corte y demuestra que el correspondiente caso es imposible.
- Regla de introducción. Es el único caso posible. $\square$

Propiedades de las derivaciones sin cortes (3/7)

Combinado con el teorema de eliminación de cortes, la proposición anterior implica la consistencia del sistema NJ:

Corolario 1 (Consistencia)

El secuente $\vdash \bot$ no es derivable en el sistema NJ

Demostración.

Si el secuente $\vdash \bot$ fuera derivable en NJ, tendría una derivación sin cortes. Tal derivación acabaría con una regla de intro: imposible pues tal regla no existe. $\square$

Propiedades de las derivaciones sin cortes

Corolario 2 (Propiedad de la disyunción)

Si un secuente de la forma $\vdash A \vee B$ es derivable en el sistema NJ, entonces al menos uno de $\vdash A$ o $\vdash B$ es derivable

Demostración.

Si el secuente $\vdash A \vee B$ es derivable, entonces tiene una derivación sin corte, que se acaba con una regla de introducción. Tal derivación tiene dos formas posibles:

- O bien de la forma $\dfrac{\begin{array}{c}\vdots\, d \\ \vdash A\end{array}}{\vdash A \vee B}\,(\vee\text{-in}_1)$, que contiene una derivación de $\vdash A$.
- O bien de la forma $\dfrac{\begin{array}{c}\vdots\, d \\ \vdash B\end{array}}{\vdash A \vee B}\,(\vee\text{-in}_2)$, que contiene una derivación de $\vdash B$. □

Propiedades de las derivaciones sin cortes (5/7)

Corolario 3 (El tercer excluido no es derivable en NJ)

El secuente $\vdash x = y \lor x \neq y$ no es derivable en el sistema NJ

Demostración.

Supongamos que $\vdash x = y \lor x \neq y$ es derivable en NJ. Por el corolario anterior:

- O bien el secuente $\vdash x = y$ es derivable. Entonces la fórmula $\forall x \forall y\, (x = y)$ es derivable en NJ y (luego) en NK, lo que es absurdo pues dicha fórmula tiene un contramodelo obvio (con dos puntos).
- O bien el secuente $\vdash x \neq y$ es derivable. Entonces la fórmula $\forall x \forall y\, (x \neq y)$ es derivable en NJ y (luego) en NK, lo que es absurdo pues dicha fórmula tiene un contramodelo obvio (con un punto).

Por lo tanto, la hipótesis es absurda. $\square$

Obs.: El argumento anterior viene de que en el sistema NJ (cálculo de predicados intuicionista), la propiedad de la disyunción también se aplica a las fórmulas abiertas. No será más el caso en sistemas como HA (aritmética intuicionista)

Propiedades de las derivaciones sin cortes (6/7)

Corolario 4 (Propiedad de la existencia en NJ)

Si un secuente de la forma $\vdash \exists x\, A(x)$ es derivable en el sistema NJ, entonces el secuente $\vdash A(t)$ es derivable para algún término t

Se dice que el término t es un testigo de la propiedad existencial $\exists x\, A(x)$

Demostración.

Si el secuente $\vdash \exists x\, A(x)$ es derivable, entonces tiene una derivación sin cortes, que se acaba con una regla de introducción. Por lo tanto, tal derivación es de la forma

$$\dfrac{\begin{array}{c}\vdots\ d\\ \vdash A(t)\end{array}}{\vdash \exists x\, A(x)}\ (\exists\text{-in})$$

que contiene una derivación d de un secuente de la forma $\vdash A(t)$. $\square$

Propiedades de las derivaciones sin cortes (7/7)

Corolario 5 (Igualdades derivables en NJ)

Un secuente de la forma $\vdash t = u$ es derivable en NJ si y sólo si $t \equiv u$ (es decir: si y sólo si los términos t y u son idénticos)

Demostración.

Supongamos que el secuente $\vdash t = u$ es derivable en NJ. Entonces tiene una derivación sin cortes, que se acaba con una regla de introducción. Por lo tanto, tal derivación es de la forma

$$\frac{}{\vdash t = t}\ (=\text{-in})$$

lo que implica que $t \equiv u$. El recíproco es obvio. □

Plan

Conclusión

- Corte = introducción + eliminación de la misma construcción

Teorema de eliminación de cortes (en NJ)

Todo secuente derivable en NJ tiene una derivación sin cortes
(en general mucho más larga que una derivación con cortes del mismo secuente)

- El mayor interés de las derivaciones sin cortes (en NJ) viene de la

Proposición (Derivaciones sin cortes de $\vdash A$ en NJ)

Toda derivación sin cortes de $\vdash A$ (contexto vacío) se acaba por una intro

- Por lo tanto, el sistema NJ es consistente y cumple las propiedades de la disyunción y de la existencia (incluso sobre las fórmulas abiertas)
- Sin embargo, la forma de las derivaciones sin cortes no se extiende a los secuentes generales (con contextos no vaciós)
- ¿Cómo extender los resultados anteriores a las teorías axiomáticas?