Introducción a la correspondencia entre pruebas y programas:

Eliminación de cortes en la Aritmética de Heyting (HA)

Alexandre Miquel

marzo de 2021

Plan

Introducción

- El interés del teorema de eliminación de cortes (en NJ) viene de la

Proposición 1 (Derivaciones sin cortes de $\vdash A$ en NJ)

Toda derivación sin cortes de un secuente de la forma $\vdash A$ (sin hipótesis) se acaba con una regla de introducción

- De esta propiedad se deducen la consistencia, la propiedad de la disyunción y la propiedad de la existencia para el sistema NJ
- Sin embargo, la Prop. 1 no se extiende a los secuentes cualesquiera (i.e. con hipótesis). Por lo tanto, no se puede utilizarla para analizar las derivaciones de teoremas en las teorías axiomáticas:

$$\mathscr{T} \vdash A \qquad \text{sii} \qquad \Gamma \vdash A \quad \text{para algún } \Gamma \subseteq \mathrm{Ax}(\mathscr{T})$$

- ¿Cómo extender la eliminación de cortes a las teorías axiomáticas?

  $\Rightarrow$ Caso de la Aritmética de Heyting: sistemas HA y HA$^{\cong}$

El lenguaje de la Aritmética

Vocabulario:

Símbolos de función:	0	(«cero»)
	$s(\_)$	(«sucesor»)
	$\_ + \_$	(«suma»)
	$\_ \times \_$	(«producto»)
Símbolo de predicado:	$\_ = \_$	(«igualdad»)

Términos y fórmulas de la aritmética

Términos $t, u ::= x \mid 0 \mid s(t) \mid t + u \mid t \times u$

Fórmulas $A, B, C ::= t = u \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid A \Rightarrow B \mid \forall x\, A \mid \exists x\, A$

con las abreviaturas $\neg A :\equiv A \Rightarrow \bot$, $A \Leftrightarrow B :\equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$,
$1 :\equiv s(0)$, $2 :\equiv s(1)$, $3 :\equiv s(2)$, etc.

Los axiomas de Peano

Axiomas de cálculo:

(1) $\forall x\,(x + 0 = x)$

(2) $\forall x\,\forall y\,(x + s(y) = s(x + y))$

(3) $\forall x\,(x \times 0 = 0)$

(4) $\forall x\,\forall y\,(x \times s(y) = (x \times y) + x)$

Inyectividad & no confusión:

(5) $\forall x\,\forall y\,(s(x) = s(y) \Rightarrow x = y)$

(6) $\forall x\,(s(x) \neq 0)$ (donde $x \neq y \;:\equiv\; \neg(x = y)$)

Esquema de inducción:

(7) $\forall \vec{z}\,[A(\vec{z}, 0) \wedge \forall x\,(A(\vec{z}, x) \Rightarrow A(\vec{z}, s(x))) \;\Rightarrow\; \forall x\,A(\vec{z}, x)]$

para cada fórmula $A(\vec{z}, x)$ con variables libres $\{\vec{z}, x\}$

Las aritméticas de Peano (PA) y de Heyting (HA)

Se llaman:

- Aritmética de Peano (PA) o aritmética clásica (de 1er orden)
  a la teoría clásica cuyos axiomas son los axiomas de Peano
- Aritmética de Heyting (HA) o aritmética intuicionista (de 1er orden)
  a la teoría intuicionista cuyos axiomas son los axiomas de Peano

Es decir:

$$\mathrm{PA} \vdash A \quad \text{sii} \quad \Gamma \vdash_{\mathrm{NK}} A \quad \text{para algún} \quad \Gamma \subseteq \mathrm{Ax(PA)}$$

$$\mathrm{HA} \vdash A \quad \text{sii} \quad \Gamma \vdash_{\mathrm{NJ}} A \quad \text{para algún} \quad \Gamma \subseteq \mathrm{Ax(PA)}$$

Expresividad de la aritmética de Heyting (1/4)

- La Aritmética de Heyting es una teoría muy expresiva que permite demostrar las propiedades algebraicas básicas de las operaciones elementales en $\mathbb{N}$: asociatividad, conmutatividad, elementos neutros, distributividad, reglas de simplificación, etc. Además, tenemos que:

$$\mathsf{HA} \vdash \forall x \forall y \, (x = y \vee x \neq y)$$

- También se pueden derivar las propiedades básicas del orden amplio (reflexividad, transitividad, antisimetría, totalidad) así como las del orden estricto mediante las abreviaturas:

$$x \leq y \;:\equiv\; \exists z \, (x + z = y) \qquad\qquad x < y \;:\equiv\; s(x) \leq y$$

- Cabe destacar que el principio de inducción fuerte es derivable en HA

$$\mathsf{HA} \vdash \forall x \, (\forall y \, (y < x \Rightarrow A(y)) \Rightarrow A(x)) \;\Rightarrow\; \forall x \, A(x)$$

mientras el principio del buen orden sólo es clásicamente derivable:

$$\mathsf{PA} \vdash \exists x \, A(x) \;\Rightarrow\; \exists x \, (A(x) \wedge \forall y \, (A(y) \Rightarrow x \leq y))$$

Expresividad de la aritmética de Heyting (2/4)

- Se pueden demostrar las propiedades de divisibilidad y de la aritmética modular (división euclidiana, teorema de Bézout, teorema chino del resto, etc.) así como las propiedades de los números primos mediante las abreviaturas:

$$\begin{aligned} (z, z') = x \div y &:\equiv z' < y \ \wedge \ x = zy + z' \\ y|x &:\equiv \exists z\,(x = zy) \\ \mathrm{Prim}(x) &:\equiv x \geq 2 \ \wedge \ \forall y\,(y|x \Rightarrow y = 1 \vee y = x) \end{aligned}$$

- En particular, el teorema de Euclides

  «Existen infinitos números primos»

  se puede expresar y derivar en HA:

$$\mathrm{HA} \ \vdash \ \forall x\, \exists y\,(y > x \wedge \mathrm{Prim}(y))$$

Expresividad de la aritmética de Heyting (3/4)

- Aunque los términos de HA/PA sólo puedan expresar polinomios

$$t, u \quad ::= \quad x \quad | \quad 0 \quad | \quad s(t) \quad | \quad t + u \quad | \quad t \times u$$

las fórmulas de HA/PA permiten expresar mucho más funciones

- Por ejemplo, se puede definir la operación de potencia mediante una fórmula $P(x, y, z)$ "$\approx x^y = z$" (¡muy larga!) tal que:

$$\text{HA} \vdash \forall x \forall z \, (P(x, 0, z) \Leftrightarrow z = 1)$$
$$\text{HA} \vdash \forall x \forall y \forall z \, (P(x, y, z) \Rightarrow \forall z' \, (P(x, s(y), z') \Leftrightarrow z' = zx))$$

Ejercicio (difícil): Construir tal fórmula

- De modo similar, se pueden representar (fuertemente[1]) todas las funciones recursivas primitivas

- Por codificaciones adecuadas, se pueden representar en HA/PA todas las estructuras de datos hereditariamente finitas: tuplas, listas finitas, conjuntos/árboles/grafos finitos, etc.

[1] Es decir: con la teoría ecuacional correspondiente, como en ejemplo anterior

Expresividad de la aritmética de Heyting (4/4)

- Usando la fórmula $P(x, y, z)$ ("$x^y = z$"), se define la relación:

$$y \in x \;:\equiv\; \exists z\, \exists x'\, \exists x''\, (P(2, y, z) \wedge x'' < z \wedge x = 2x'z + z + x'')$$

"el dígito de índice y en la representación binaria de x es 1"

- **Intuición:** Se puede ver cada entero natural como el conjunto de las posiciones de los dígitos 1 en su representación en base 2. En particular:

$$0 = \varnothing, \quad 1 = \{0\} = \{\varnothing\}, \quad 2 = \{1\} = \{\{\varnothing\}\}, \quad 3 = \{0, 1\} = \{\varnothing, \{\varnothing\}\}, \quad \text{etc.}$$

- Con la igualdad $x = y$ usual de la aritmética, la fórmula $y \in x$ permite traducir todas las fórmulas del lenguaje de la teoría de conjuntos adentro del lenguaje de la aritmética

- **Ejercicio:** Verificar que vía esta traducción
  - los axiomas de ZF salvo el infinito,
  - la negación del axioma del infinito,
  - el axioma de elección, y
  - el axioma de fundación

  son todos derivables en HA

HA = teoría intuicionista de los conjuntos hereditariamente finitos

¿Cómo adaptar la eliminación de cortes a HA?

- **Problema:** Debido a la presencia de axiomas, una derivación de $\mathrm{HA} \vdash A$ no se acaba necesariamente con una regla de introducción
- **Solución:** ¡Integrar los axiomas al sistema de deducción!
- **Punto de vista filosófico del logicismo**
  (Gottlob Frege, Bertrand Russell, Alfred North Whitehead, Rudolf Carnap)
  (1) Los conceptos matemáticos se pueden derivar de conceptos lógicos a través de definiciones explícitas
  (2) Los teoremas de las matemáticas se pueden derivar de axiomas lógicos a través de deducciones puramente lógicas
- **Un punto de vista fructífero:**
  - *Principia Mathematica* [Russell & Whitehead, 1910–1913]
  - Eliminación de cortes en HA/PA [Gentzen 1936, Prawitz 1965]
  - Eliminación de cortes en HA2/PA2 [Girard 1969]
  - Teorías de tipos [Martin-Löf 1974]
  - Cálculo de construcciones, Sistema Coq [Coquand 1985, Paulin 1989]
  - Deducción módulo [Dowek, 2000]
  - Sistemas de tipos para IZ, IZF_C [Miquel, 2001–2009]

Los axiomas de Peano (recordatorio)

Axiomas de cálculo:

(1) $\forall x\,(x + 0 = x)$

(2) $\forall x\,\forall y\,(x + s(y) = s(x + y))$

(3) $\forall x\,(x \times 0 = 0)$

(4) $\forall x\,\forall y\,(x \times s(y) = (x \times y) + x)$

Inyectividad & no confusión:

(5) $\forall x\,\forall y\,(s(x) = s(y) \Rightarrow x = y)$

(6) $\forall x\,(s(x) \neq 0)$ (donde $x \neq y \;:\equiv\; \neg(x = y)$)

Esquema de inducción:

(7) $\forall \vec{z}\,[A(\vec{z}, 0) \wedge \forall x\,(A(\vec{z}, x) \Rightarrow A(\vec{z}, s(x))) \;\Rightarrow\; \forall x\,A(\vec{z}, x)]$

para cada fórmula $A(\vec{z}, x)$ con variables libres $\{\vec{z}, x\}$

... ¿Cómo integrar estos axiomas en el sistema de deducción?

Integración de los axiomas (1)–(4) (1/3)

Los axiomas de cálculo

(1) $\forall x\,(x + 0 = x)$

(2) $\forall x\,\forall y\,(x + s(y) = s(x + y))$

(3) $\forall x\,(x \times 0 = 0)$

(4) $\forall x\,\forall y\,(x \times s(y) = (x \times y) + x)$

se pueden remplazar por dos congruencias[2]

$t \cong t'$ ("los términos t y t' son computacionalmente equivalentes")

$A \cong A'$ ("las fórmulas A y A' son computacionalmente equivalentes")

generadas por las reglas:

$$\begin{array}{rcl@{\qquad}rcl} t + 0 & \cong & t & t \times 0 & \cong & 0 \\ t + s(u) & \cong & s(t + u) & t \times s(u) & \cong & (t \times u) + t \end{array}$$

Esto permite luego razonar a menos de la congruencia $A \cong A'$

[2] Es decir: relaciones de equivalencia compatibles con todos los símbolos lógicos:

- símbolos de funciones en los términos,
- símbolos de predicado, conectivas y cuantificadores en las fórmulas

Integración de los axiomas (1)–(4) (2/3)

- Las congruencias $t \cong t'$ y $A \cong A'$ generadas por las reglas

$$\begin{array}{rcl@{\qquad}rcl} t+0 & \cong & t & t\times 0 & \cong & 0 \\ t+s(u) & \cong & s(t+u) & t\times s(u) & \cong & (t\times u)+t \end{array}$$

tienen un sistema de representantes canónico: las formas normales

- La forma normal de un término (de una fórmula) se calcula aplicando las reglas anteriores de la izquierda a la derecha mientras se pueda

- Se demuestra que dos términos (fórmulas) son computacionalmente equivalentes si y sólo si tienen la misma forma normal:

$$\begin{array}{rcl@{\qquad}l@{\qquad}rcl} t & \cong & t' & \text{sii} & \downarrow t & \equiv & \downarrow t' \\ A & \cong & A' & \text{sii} & \downarrow A & \equiv & \downarrow A' \end{array}$$

donde $\downarrow t$ (resp. $\downarrow A$) nota la forma normal de t (resp. de A)

- Por lo tanto, las congruencias $t \cong t'$ y $A \cong A'$ son decidibles

Integración de los axiomas (1)–(4) (3/3)

- Se adaptan las reglas de NJ para razonar "a menos de $\cong$":

$$\text{(Axioma)}\quad \frac{}{\Gamma \vdash A'}\ \text{si}\ A' \cong A \in \Gamma \qquad \text{(=-in)}\quad \frac{}{\Gamma \vdash t = t'}\ \text{si}\ t \cong t' \qquad \text{(etc.)}$$

- Aparece una nueva regla admisible de conversión:

$$\text{(Conv)}\quad \frac{\Gamma \vdash A}{\Gamma \vdash A'}\ \text{si}\ A \cong A'$$

- Estos cambios permiten derivar los axiomas de cálculo, por ejemplo:

$$\text{(1)}\qquad \dfrac{\dfrac{}{\vdash x + 0 = x}\ (=\text{-in})}{\vdash \forall x\,(x + 0 = x)}\ (\forall\text{-in}) \qquad \text{(etc.)}$$

- Más generalmente, este cambio de punto de vista permite agrupar múltiples pasos de cálculo en un única inferencia, por ejemplo:

$$\frac{}{p(6 \times 7) \vdash p(5 \times 8 + 2)}\ (\text{ax})$$

Integración del axioma (5)

- Para integrar en el sistema de deducción el axioma

  (5) $\forall x \forall y\, (s(x) = s(y) \Rightarrow x = y)$

  basta con introducir un nuevo símbolo de función (unario)

Términos $t, u \quad ::= \quad \cdots \quad | \quad \mathrm{pred}(t)$ («predecedor»)

con las equivalencias computacionales:

$$\mathrm{pred}(0) \cong 0 \qquad \mathrm{pred}(s(t)) \cong t$$

Intuición: «pred» es una inversa por la izquierda de «s»

- Luego se deduce que el sucesor es inyectivo:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{s(x) = s(y) \vdash s(x) = s(y)}\,(\text{ax}) \quad \dfrac{}{s(x) = s(y) \vdash \mathrm{pred}(s(x)) = \mathrm{pred}(s(x))}\,(=\text{-in})}{s(x) = s(y) \vdash \mathrm{pred}(s(x)) = \mathrm{pred}(s(y))}\,(=\text{-el})}{s(x) = s(y) \vdash x = y}\,(\text{Conv})}{\vdash s(x) = s(y) \Rightarrow x = y}\,(\Rightarrow\text{-in})}{\vdash \forall x \forall y\, (s(x) = s(y) \Rightarrow x = y)}\,(\forall\text{-in} \times 2)$$

Integración del axioma (6)

- Para integrar en el sistema de deducción el axioma

  (6) $\forall x\,(s(x) \neq 0)$

  basta con introducir un nuevo símbolo de predicado (unario)

Fórmulas $A, B \quad ::= \quad \cdots \quad | \quad \mathrm{null}(t)$ («nulidad»)

con las equivalencias computacionales:

$$\mathrm{null}(0) \cong \top \qquad \mathrm{null}(s(t)) \cong \bot$$

- Luego se deduce que el sucesor nunca alcanza 0:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{s(x)=0 \vdash s(x)=0}\,(\mathrm{ax}) \quad \dfrac{}{s(x)=0 \vdash s(x)=s(x)}\,(=\text{-in})}{s(x)=0 \vdash 0=s(x)}\,(=\text{-el}) \quad \dfrac{\dfrac{}{s(x)=0 \vdash \top}\,(\top\text{-in})}{s(x)=0 \vdash \mathrm{null}(0)}\,(\mathrm{Conv})}{s(x)=0 \vdash \mathrm{null}(s(x))}\,(=\text{-el})}{s(x)=0 \vdash \bot}\,(\mathrm{Conv})}{\vdash s(x) \neq 0}\,(\Rightarrow\text{-in})}{\vdash \forall x\,(s(x) \neq 0)}\,(\forall\text{-in})$$

Integración del esquema de inducción (7)

- **Para resumir:** Se integran los axiomas (1)–(6) en el sistema de deducción, introduciendo una relación de equivalencia computacional $A \cong A'$ y razonando a menos de dicha equivalencia

  Intuición: Los axiomas (1)–(6) hablán más de computación que de deducción

- Sin sorpresa, este método no se extiende al esquema de inducción

  (7) $\forall \vec{z}\,[A(\vec{z},0) \wedge \forall x\,(A(\vec{z},x) \Rightarrow A(\vec{z},s(x))) \;\Rightarrow\; \forall x\,A(\vec{z},x)]$
  para cada fórmula $A(\vec{z},x)$ con variables libres $\{\vec{z},x\}$

  que hay que remplazar por la nueva regla de deducción:

(Nat-el) $$\frac{\Gamma \vdash A[x:=0] \qquad \Gamma, A \vdash A[x:=s(x)]}{\Gamma \vdash A'} \text{ si } \begin{cases} x \notin FV(\Gamma) \\ A' \cong A[x:=t] \end{cases}$$

  Intuición: Esq. de inducción = regla de eliminación de los enteros naturales, opuesta a los constructores de enteros naturales 0 y $s(\_)$ (via el término t)

- Se escribe HA$^{\cong}$ («Aritmética computacional») al sistema obtenido

Plan

Plan

Sintaxis de $\mathrm{HA}^{\cong}$

Se trata de definir el sistema $\mathrm{HA}^{\cong}$ («Aritmética computacional»), cuya sintaxis es la siguiente:

Términos y fórmulas de $\mathrm{HA}^{\cong}$

Términos
$$t, u ::= x \mid 0 \mid s(t) \mid \mathrm{pred}(t) \mid t + u \mid t \times u$$

Fórmulas
$$A, B, C ::= t = u \mid \mathrm{null}(t) \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid A \Rightarrow B \mid \forall x\, A \mid \exists x\, A$$

con las abreviaturas $\neg A :\equiv A \Rightarrow \bot$, $A \Leftrightarrow B :\equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$,
$1 :\equiv s(0)$, $2 :\equiv s(1)$, $3 :\equiv s(2)$, etc.

Los términos y las fórmulas de $\mathrm{HA}^{\cong}$ están equipados con congruencias

$$t \cong t' \quad \text{(sobre los términos)} \quad \text{y} \quad A \cong A' \quad \text{(sobre las fórmulas)}$$

que vamos a definir más adelante

Términos: reducción y equivalencia (1/6)

Definición (Reducción en un paso)

Se equipan los términos de HA$^{\cong}$ con una relación binaria $t \succ t'$ de reducción en un paso, definida inductivamente por las 12 reglas:

$$\frac{}{\mathsf{pred}(0) \succ 0} \qquad \frac{}{\mathsf{pred}(s(t)) \succ t}$$

$$\frac{}{t + 0 \succ t} \qquad \frac{}{t + s(u) \succ s(t + u)}$$

$$\frac{}{t \times 0 \succ 0} \qquad \frac{}{t \times s(u) \succ (t \times u) + t}$$

(casos de base)

$$\frac{t \succ t'}{s(t) \succ s(t')} \qquad \frac{t \succ t'}{\mathsf{pred}(t) \succ \mathsf{pred}(t')}$$

$$\frac{t_1 \succ t_1'}{t_1 + t_2 \succ t_1' + t_2} \qquad \frac{t_2 \succ t_2'}{t_1 + t_2 \succ t_1 + t_2'}$$

$$\frac{t_1 \succ t_1'}{t_1 \times t_2 \succ t_1' \times t_2} \qquad \frac{t_2 \succ t_2'}{t_1 \times t_2 \succ t_1 \times t_2'}$$

(pasos inductivos)

Términos: reducción y equivalencia (2/6)

Lema (Variables libres)

Si $t \succ t'$, entonces $FV(t') \subseteq FV(t)$

Demostración. Por inducción sobre la derivación de $t \succ t'$ □

Obs.: Variables libres pueden desaparecer durante la reducción, por ej.: $z \times 0 \succ 0$

Lema (Sustitutividad)

Si $t \succ t'$, entonces $t[x := u] \succ t'[x := u]$

Demostración. Por inducción sobre la derivación de $t \succ t'$ □

Términos: reducción y equivalencia (3/6)

Definición (Reducción en múltiples pasos)

Se define inductivamente la relación $t \twoheadrightarrow t'$ de reducción en múltiples pasos por las dos reglas:

$$\frac{}{t \twoheadrightarrow t} \qquad \frac{t \twoheadrightarrow t' \quad t' \succ t''}{t \twoheadrightarrow t''}$$

Obs.: La relación $t \twoheadrightarrow t'$ es la clausura reflexiva-transitiva de la relación $t \succ t'$, es decir: la mínima relación reflexiva y transitiva (el mínimo preorden) que contiene la relación $t \succ t'$. De modo equivalente:

$$t \twoheadrightarrow t' \quad \text{sii} \quad \text{existen } n \in \mathbb{N},\ t_0, \ldots, t_n \text{ tales que: } t \equiv t_0 \succ t_1 \succ \cdots \succ t_{n-1} \succ t_n \equiv t'$$

Términos: reducción y equivalencia (4/6)

Proposición (Clausura contextual + Sustitutividad)

0. Si $t \succ t'$, entonces $FV(t') \subseteq FV(t)$
1. Si $t \succ t'$, entonces $\begin{cases} s(t) \succ s(t') \\ \mathrm{pred}(t) \succ \mathrm{pred}(t') \end{cases}$
2. Si $t_1 \succ t_1'$ y $t_2 \succ t_2'$, entonces $\begin{cases} t_1 + t_2 \succ t_1' + t_2' \\ t_1 \times t_2 \succ t_1' \times t_2' \end{cases}$
3. Si $t \succ t'$ y $u \succ u'$, entonces $t[x := u] \succ t'[x := u']$

Demostración. Por inducción sobre las correspondientes derivaciones □

Términos: reducción y equivalencia (5/6)

Definición (Equivalencia computacional)

Se define inductivamente la relación $t \cong t'$ de equivalencia computacional entre términos por las tres reglas:

$$\frac{}{t \cong t} \qquad \frac{t \cong t' \quad t' \succ t''}{t \cong t''} \qquad \frac{t \cong t' \quad t'' \succ t'}{t \cong t''}$$

Obs.: La relación $t \cong t'$ es la clausura reflexiva-simétrica-transitiva de la relación $t \succ t'$, es decir: la mínima relación de equivalencia que contiene la relación $t \succ t'$. De modo equivalente:

$$t \cong t' \quad \text{sii} \quad \text{existen } n \in \mathbb{N},\ t_0, \ldots, t_n \text{ tales que: } t \equiv t_0 \prec\succ t_1 \prec\succ \cdots \prec\succ t_{n-1} \prec\succ t_n \equiv t'$$

escribiendo $t_i \prec\succ t_{i+1}$ cuando $t_i \succ t_{i+1}$ o $t_{i+1} \succ t_i$

Términos: reducción y equivalencia (6/6)

Proposición (Clausura contextual + Sustitutividad)

1. Si $t \cong t'$, entonces $\begin{cases} s(t) \cong s(t') \\ \mathrm{pred}(t) \cong \mathrm{pred}(t') \end{cases}$
2. Si $t_1 \cong t_1'$ y $t_2 \cong t_2'$, entonces $\begin{cases} t_1 + t_2 \cong t_1' + t_2' \\ t_1 \times t_2 \cong t_1' \times t_2' \end{cases}$
3. Si $t \cong t'$ y $u \cong u'$, entonces $t[x := u] \cong t'[x := u']$

Demostración. Por inducción sobre las correspondientes derivaciones □

Términos: formas normales (1/2)

Definición (Formas normales)

Dados términos t y t', se dice que:

- t' es en forma normal cuando $t' \not\succ$ (i.e. t' no se reduce)
- t' es una forma normal de t cuando $t \twoheadrightarrow t'$ y $t' \not\succ$

Problema: Dado un término t:

1. ¿Tiene t una forma normal?
2. Cuando existe, ¿es única?

Términos: formas normales (2/2)

Lema (Normalización fuerte)

La relación $t \succ t'$ es fuertemente normalizante, en el sentido de que no existe ninguna reducción infinita:

$$\nexists(t_0 \succ t_1 \succ t_2 \succ \cdots \succ t_i \succ t_{i+1} \succ \cdots)$$

Demostración. A cada término t se asocia un peso $\mathbf{w}(t) \in \mathbb{N}^*$ definido por:

$$\begin{array}{rclcrcl} \mathbf{w}(x) & := & 1 & & \mathbf{w}(0) & := & 1 \\ \mathbf{w}(s(t)) & := & \mathbf{w}(t)+1 & & \mathbf{w}(\mathrm{pred}(t)) & := & \mathbf{w}(t)+1 \\ \mathbf{w}(t+u) & := & \mathbf{w}(t)+2\mathbf{w}(u) & & \mathbf{w}(t\times u) & := & 3\mathbf{w}(t)\mathbf{w}(u) \end{array}$$

Luego se demuestra que la condición $t \succ t'$ implica que $\mathbf{w}(t) > \mathbf{w}(t')$ (por inducción sobre la derivación de $t \succ t'$) □

Corolario (Existencia de las formas normales)

Todo término t tiene una forma normal

Términos: confluencia (1/3)

Proposición (Confluencia local)

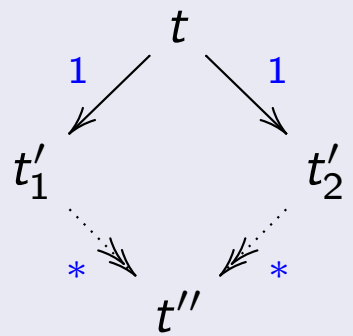
La relación $t \succ t'$ es localmente confluente. Es decir:

Para todos términos t, t'_1, t'_2 tales que:

$$t \succ t'_1 \quad \text{y} \quad t \succ t'_2,$$

existe un término t'' tal que

$$t'_1 \succ\!\!\!\!\!\!* \; t'' \quad \text{y} \quad t'_2 \succ\!\!\!\!\!\!* \; t''$$

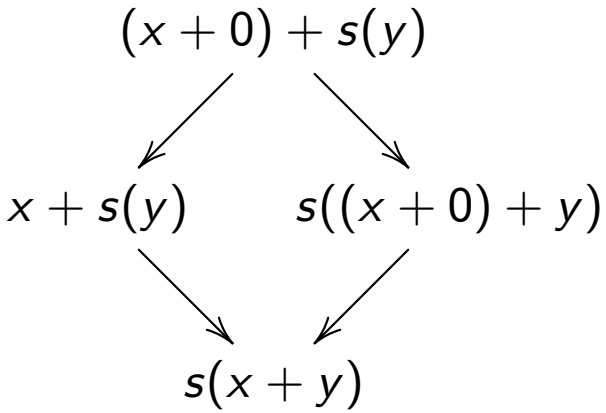


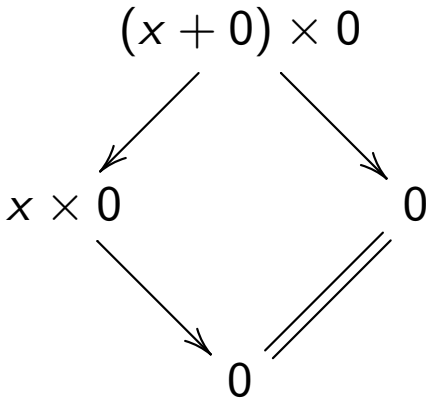
Demostración. Por inducción sobre las derivaciónes de $t \succ t'_1$ y $t \succ t'_2$. □

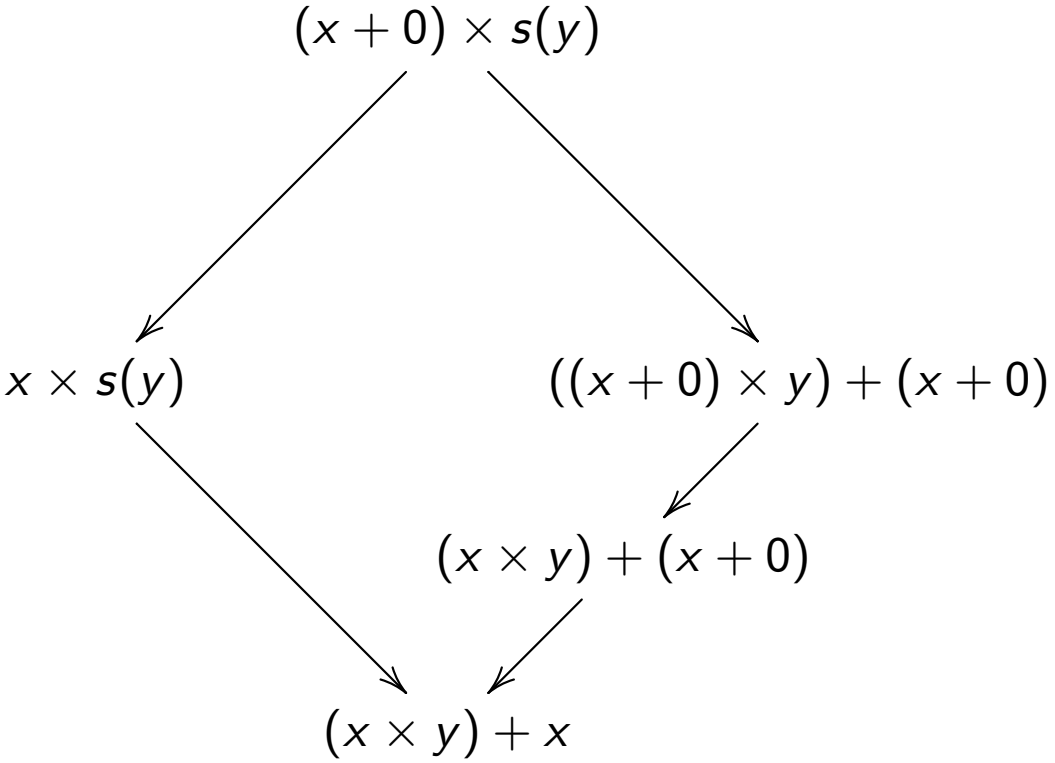
Ejercicio: Escribir la demostración completa

Términos: confluencia (2/3)

Ejemplos de confluencia local:







Términos: confluencia (3/3)

Teorema (Confluencia)

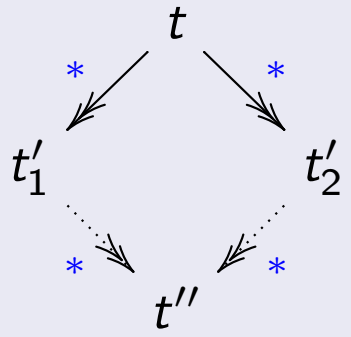
La relación $t \succ t'$ es confluente. Es decir:

Para todos términos t, t'_1, t'_2 tales que:

$$t \succ\!\!\!\!\succ t'_1 \quad \text{y} \quad t \succ\!\!\!\!\succ t'_2,$$

existe un término t'' tal que

$$t'_1 \succ\!\!\!\!\succ t'' \quad \text{y} \quad t'_2 \succ\!\!\!\!\succ t''$$



Demostración. Sigue del lema de Newman, que dice que toda relación fuertemente normalizante y localmente confluente es confluente. □

Corolario (Existencia y unicidad de la formas normal)

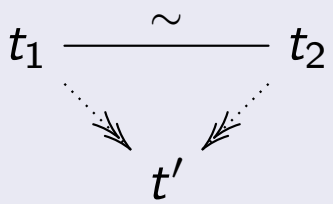
Todo término t tiene una única forma normal. Notación: $\downarrow t$

Términos: propiedad de Church-Rosser

Teorema (Propiedad de Church-Rosser)

La relación $t \succ t'$ cumple la propiedad de Church-Rosser. Es decir:

$$t_1 \cong t_2 \qquad \text{si y sólo si} \qquad t_1 \succ\!\!\succ t' \ \text{ y } \ t_2 \succ\!\!\succ t' \ \text{ para algún } t'$$



Demostración. ($\Rightarrow$) Por inducción sobre la derivación de $t_1 \cong t_2$, usando la propiedad de confluencia. ($\Leftarrow$) Obvio, por def. de $\succ\!\!\succ$ y $\cong$. □

Corolario (Criterio de equivalencia)

Dos términos son equivalentes si y sólo si tienen la misma forma normal:

$$t_1 \cong t_2 \qquad \text{sii} \qquad \downarrow t_1 \equiv \downarrow t_2$$

En particular, la relación $t_1 \cong t_2$ es decidible

Intermezzo: estructura de las formas normales (1/2)

Se consideran las dos formas de términos **neut** ("neutros") y **norm** ("normales") definidas por las gramáticas:

$$\begin{array}{rcl} \mathbf{neut} & ::= & x \mid \mathrm{pred}(\mathbf{neut}) \\ & & \mid \mathbf{norm} + \mathbf{neut} \mid \mathbf{norm} \times \mathbf{neut} \\ \mathbf{norm} & ::= & \mathbf{neut} \mid 0 \mid s(\mathbf{norm}) \end{array}$$

Observaciones:

- Los **neut** son los **norm** que no son ni 0 ni de la forma $s(\_)$
- Todos los **neut** son abiertos (i.e. tienen variable libre)
- Los **norm** cerrados son exactamente los enteros de Peano:

$$t \equiv \underbrace{s(\cdots s}_{n}(0)\cdots)$$

Intermezzo: estructura de las formas normales (2/2)

$$\begin{array}{rcl} \textbf{neut} & ::= & x \mid \mathrm{pred}(\textbf{neut}) \\ & \mid & \textbf{norm} + \textbf{neut} \mid \textbf{norm} \times \textbf{neut} \\ \textbf{norm} & ::= & \textbf{neut} \mid 0 \mid s(\textbf{norm}) \end{array}$$

Proposición (Caracterización de las formas normales)

1. Los términos en forma normal son los términos de la forma **norm**

Y por lo tanto:

2. Los términos cerrados en forma normal son los enteros de Peano
3. La forma normal de un término cerrado t es el valor de t en el modelo estándar: $\downarrow t \equiv [\![t]\!]^{\mathbb{N}}$
4. Dos términos cerrados t_1 y t_2 son computacionalmente equivalentes si y sólo si corresponden al mismo entero de Peano:

$$t_1 \cong t_2 \quad \text{sii} \quad \downarrow t_1 \equiv \downarrow t_2 \quad \text{sii} \quad [\![t_1]\!]^{\mathbb{N}} = [\![t_2]\!]^{\mathbb{N}}$$

Fórmulas: reducción y equivalencia (1/3)

Definición (Reducción en un paso)

Se equipan las fórmulas de HA$^{\cong}$ con una relación binaria $A \succ A'$ de reducción en un paso, definida inductivamente por las 13 reglas:

$$\frac{}{\mathsf{null}(0) \succ \top} \qquad \frac{}{\mathsf{null}(s(t)) \succ \bot} \qquad \frac{t \succ t'}{\mathsf{null}(t) \succ \mathsf{null}(t')}$$

$$\frac{t \succ t'}{t = u \succ t' = u} \qquad \frac{u \succ u'}{t = u \succ t = u'}$$

$$\frac{A \succ A'}{A \Rightarrow B \succ A' \Rightarrow B} \qquad \frac{B \succ B'}{A \Rightarrow B \succ A \Rightarrow B'}$$

$$\frac{A \succ A'}{A \wedge B \succ A' \wedge B} \qquad \frac{B \succ B'}{A \wedge B \succ A \wedge B'}$$

$$\frac{A \succ A'}{A \vee B \succ A' \vee B} \qquad \frac{B \succ B'}{A \vee B \succ A \vee B'}$$

$$\frac{A \succ A'}{\forall x\, A \succ \forall x\, A'} \qquad \frac{A \succ A'}{\exists x\, A \succ \exists x\, A'}$$

Fórmulas: reducción y equivalencia (2/3)

De modo análogo, se definen:

- La relación $A \succcurlyeq A'$ de reducción en múltiples pasos, como la clausura reflexiva-transitiva de la relación $A \succ A'$
- La relación $A \cong A'$ de equivalencia computacional, como la clausura reflexiva-simétrica-transitiva de la relación $A \succ A'$

Estas tres relaciones cumplen las mismas propiedades que las relaciones análogas sobre los términos:

- Sustitutividad y clausura contextual (para $\succcurlyeq$ y $\cong$)
- Normalización fuerte
- Confluencia local y confluencia
- Existencia y unicidad de las formas normales. Notación: $\downarrow A$
- Propiedad de Church-Rosser y criterio de equivalencia

Ejercicio: Enunciar y demostrar estas propiedades

Fórmulas: reducción y equivalencia (3/3)

La relación $A_1 \cong A_2$ de equivalencia computacional es decidible:

$$A_1 \cong A_2 \quad \text{sii} \quad \downarrow A_1 \equiv \downarrow A_2$$

Observación: La relación de equivalencia computacional no permite identificar un $\Rightarrow$ con un $\wedge$, un $\vee$ o un $\forall$:

Lema

Para toda fórmula C:

$$\begin{array}{llll}
C \cong A \Rightarrow B & \text{sii} & C \equiv A' \Rightarrow B', & \text{con } A' \cong A \text{ y } B' \cong B \\
C \cong A \wedge B & \text{sii} & C \equiv A' \wedge B', & \text{con } A' \cong A \text{ y } B' \cong B \\
C \cong A \vee B & \text{sii} & C \equiv A' \vee B', & \text{con } A' \cong A \text{ y } B' \cong B \\
C \cong \forall x\, A & \text{sii} & C \equiv \forall x\, A', & \text{con } A' \cong A \\
C \cong \exists x\, A & \text{sii} & C \equiv \exists x\, A', & \text{con } A' \cong A \\
C \cong t = u & \text{sii} & C \equiv t' = u', & \text{con } t' \cong t \text{ y } u' \cong u
\end{array}$$

Sin embargo: $\top \cong \text{null}(0)$ y $\bot \cong \text{null}(s(t))$ (pero $\top \ncong \bot$)

Plan

Reglas de deducción del sistema $HA^{\cong}$ (1/2)

- Como siempre, usamos secuentes de la forma $\Gamma \vdash A$
- Reglas del cálculo proposicional intuicionista:

(Axioma) $$\frac{}{\Gamma \vdash A'} \text{ si } A' \cong A \in \Gamma$$

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

Reglas de deducción del sistema $HA^{\cong}$ (2/2)

- Reglas de introducción y de eliminación de los cuantificadores:

$$(\forall)\quad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x\, A}\ \text{si}\ x \notin FV(\Gamma) \qquad \frac{\Gamma \vdash \forall x\, A}{\Gamma \vdash A'}\ \text{si}\ A' \cong A[x:=t]$$

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

- Reglas de introducción y de eliminación de la igualdad:

$$(=)\quad \frac{}{\Gamma \vdash t = t'}\ \text{si}\ t \cong t' \qquad \frac{\Gamma \vdash t = u \qquad \Gamma \vdash A[x := t]}{\Gamma \vdash A'}\ \text{si}\ A' \cong A[x:=u]$$

- Regla de eliminación de los enteros naturales (= inducción):

$$(\text{Nat-el})\quad \frac{\Gamma \vdash A[x := 0] \qquad \Gamma, A \vdash A[x := s(x)]}{\Gamma \vdash A'}\ \text{si}\ \begin{cases} x \notin FV(\Gamma) \\ A' \cong A[x:=t] \end{cases}$$

Propiedades (1/3)

Dadas listas de fórmulas $\Gamma \equiv A_1, \ldots, A_n$ y $\Gamma' \equiv A'_1, \ldots A'_m$
se escribe $\Gamma \cong \Gamma'$ cuando $n = m$ y $A_i \cong A'_i$ para todo $i \in [1..n]$

Proposición (Conversión)

La siguiente regla de inferencia es admisible en el sistema HA$^{\cong}$:

$$\frac{\Gamma \vdash A}{\Gamma' \vdash A'} \text{ si } \begin{cases} \Gamma \cong \Gamma' \\ A \cong A' \end{cases}$$

Demostración. Se trata de demostrar que si un secuente $\Gamma \vdash A$ tiene derivación d, entonces para todos $\Gamma' \cong \Gamma$ y $A' \cong A$, el secuente $\Gamma' \vdash A'$ tiene (otra) derivación d'.

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 un secuente de la forma $\Gamma', \Delta' \vdash C'$, con $\Delta' \cong \Delta$ y $C' \cong C$. □

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

Propiedades (2/3)

Recordatorio: 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 $HA^{\cong}$:

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

Demostración. Por inducción sobre la derivación de $\Gamma \vdash A$. □

Corolario (Reglas de permutación, debilitamiento y contracción)

La siguientes reglas son admisibles en el sistema $HA^{\cong}$:

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

donde σ es cualquier permutación de Γ

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

Derivación de los axiomas de Peano en HA$^{\cong}$ (1/4)

- Axioma: $\forall x\,(x + 0 = 0)$

$$\dfrac{\dfrac{}{\Gamma \vdash x + 0 = 0}\ (=\text{-in})}{\Gamma \vdash \forall x\,(x + 0 = 0)}\ (\forall\text{-in})$$

- Axioma: $\forall x\,\forall y\,(x + s(y) = s(x + y))$

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash x + s(y) = s(x + y)}\ (=\text{-in})}{\Gamma \vdash \forall x\,(x + s(y) = s(x + y))}\ (\forall\text{-in})}{\Gamma \vdash \forall x\,\forall x\,(x + s(y) = s(x + y))}\ (\forall\text{-in})$$

- Axiomas de $\times$: Análogo

Derivación de los axiomas de Peano en $HA^{\cong}$ (2/4)

- Inyectividad del sucesor:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{s(x)=s(y)\vdash s(x)=s(y)}\,(\text{ax}) \quad \dfrac{}{s(x)=s(y)\vdash \text{pred}(s(x))=\text{pred}(s(x))}\,(=\text{-in})}{s(x)=s(y)\vdash x=y}\,(*)}{\vdash s(x)=s(y)\Rightarrow x=y}\,(\Rightarrow\text{-in})}{\vdash \forall y\,(s(x)=s(y)\Rightarrow x=y)}\,(\forall\text{-in})}{\vdash \forall x\,\forall y\,(s(x)=s(y)\Rightarrow x=y)}\,(\forall\text{-in})$$

$(*)$ Regla $(=\text{-el})$ con la fórmula $A(z) :\equiv \text{pred}(s(x))=\text{pred}(z)$

Derivación de los axiomas de Peano en $HA^{\cong}$ (3/4)

- No-sobreyectividad del sucesor:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots\ d}{s(x)=0 \vdash 0=s(x)} \quad \dfrac{}{s(x)=0 \vdash \mathsf{null}(0)}\ (\top\text{-in})}{s(x)=0 \vdash \bot}\ (*)}{\vdash s(x)\neq 0}\ (\Rightarrow\text{-in})}{\vdash \forall x\,(s(x)\neq 0)}\ (\forall\text{-in})$$

$$\text{con} \quad d = \left\{ \dfrac{\dfrac{}{s(x)=0 \vdash s(x)=0}\ (=\text{-in}) \quad \dfrac{}{s(x)=0 \vdash s(x)=s(x)}\ (\text{ax})}{s(x)=0 \vdash 0=s(x)}\ (**) \right.$$

$(*)$ Regla $(=\text{-el})$ con la fórmula $A(z) :\equiv \mathsf{null}(z)$

$(**)$ Regla $(=\text{-el})$ con la fórmula $A(z) :\equiv z = s(x)$

Derivación de los axiomas de Peano en HA$^{\cong}$ (4/4)

- Esquema de inducción:

$$\dfrac{\dfrac{\dfrac{}{C \vdash C}\,(\text{ax})}{C \vdash A(\vec{z},0)}\,(\wedge\text{-el}_1) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{C, A(\vec{z},x) \vdash C}\,(\text{ax})}{C, A(\vec{z},x) \vdash \forall x\,(A(\vec{z},x) \Rightarrow A(\vec{z},s(x)))}\,(\wedge\text{-el}_2)}{C, A(\vec{z},x) \vdash A(\vec{z},x) \Rightarrow A(\vec{z},s(x))}\,(\forall\text{-el}) \qquad \dfrac{}{C, A(\vec{z},x) \vdash A(\vec{z},x)}\,(\text{ax})}{C, A(\vec{z},x) \vdash A(\vec{z},s(x))}\,(\Rightarrow\text{-el})}{\dfrac{\dfrac{C \vdash A(\vec{z},x)}{C \vdash \forall x\, A(\vec{z},x)}\,(\forall\text{-in})}{\vdash C \;\Rightarrow\; \forall x\, A(\vec{z},x)}\,(\Rightarrow\text{-in})}{\vdash \forall \vec{z}\,[\underbrace{A(\vec{z},0) \wedge \forall x\,(A(\vec{z},x) \Rightarrow A(\vec{z},s(x)))}_{C} \;\Rightarrow\; \forall x\, A(\vec{z},x)]}\,(\forall\text{intro}\times n)$$

Extensión conservativa (1/2)

Es claro que:

- El lenguaje de HA está incluido en el lenguaje de $HA^{\cong}$
- Los axiomas de HA son derivables en $HA^{\cong}$ (sin hipótesis)
- Las reglas de NJ son casos particulares de las reglas de $HA^{\cong}$

Por lo tanto:

Proposición (Extensión $HA \subseteq HA^{\cong}$)

Si $\mathrm{HA} \vdash A$, entonces $\vdash_{\mathrm{HA}^{\cong}} A$ (sin hipótesis)

Además:

Proposición (Extensión conservativa)

$HA^{\cong}$ es una extensión conservativa de HA, en el sentido de que para toda fórmula cerrada A del lenguaje de HA, tenemos que:

$$\mathrm{HA} \vdash A \quad \text{si y sólo si} \quad \vdash_{\mathrm{HA}^{\cong}} A \quad \text{(sin hipótesis)}$$

Extensión conservativa (2/2)

Arquitectura de la prueba de conservatividad:

Se observa que cualquier formula $A \in \mathscr{L}_{\mathsf{HA}^{\cong}}$ se puede traducir en una fórmula $A^* \in \mathscr{L}_{\mathsf{HA}}$ (i.e. sin los símbolos pred y null) con las mismas variables libres y "el mismo significado"

(La definición de la traducción $A \mapsto A^*$ es muy técnica.)

Luego se verifica que:

(1) Para toda fórmula A de HA: $\quad \mathsf{HA} \vdash A^* \Leftrightarrow A$
(Por recurrencia sobre la fórmula A)

(2) Para todas fórmula $A_1 \cong A_2$ de HA$^{\cong}$: $\quad \mathsf{HA} \vdash A_1^* \Leftrightarrow A_2^*$
(Por inducción sobre la derivación de $A_1 \cong A_2$)

(3) Si un secuente $\Gamma \vdash A$ es derivable en HA$^{\cong}$, entonces existe una lista $\Delta \subset \mathrm{Ax}(\mathsf{HA})$ tal que el secuente $\Gamma^*, \Delta \vdash A^*$ sea derivable en NJ
(Por inducción sobre la derivación de $\Gamma \vdash A$ en HA$^{\cong}$, usando (2))

(4) Se concluye, observando que si $\vdash_{\mathsf{HA}^{\cong}} A$ (con $A \in \mathscr{L}_{\mathsf{HA}}$), entonces $\mathsf{HA} \vdash A^*$ (por (3)), y luego $\mathsf{HA} \vdash A$ (por (1)). □

Plan

La noción de corte (1/?)

En el sistema HA$^{\cong}$, un corte describe la interacción entre:

- una regla de introducción y una regla de eliminación
  (de la misma construcción lógica, como en el sistema NJ)
- un constructor (0 o s) y la regla de inducción
  (inducción = regla de eliminación de los enteros naturales)

Así, tenemos:

- 8 cortes lógicos —los de NJ—, más
- 2 cortes de inducción

Reducción de los cortes lógicos (1/5)

Cortes de $\wedge$:

$$\dfrac{\dfrac{\begin{array}{cc}\vdots\, d_1 & \vdots\, d_2\\ \Gamma \vdash A & \Gamma \vdash B\end{array}}{\Gamma \vdash A \wedge B}\,(\wedge\text{-in})}{\Gamma \vdash A}\,(\wedge\text{-el}_1) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\, d_1\\ \Gamma \vdash A\end{array}$$

$$\dfrac{\dfrac{\begin{array}{cc}\vdots\, d_1 & \vdots\, d_2\\ \Gamma \vdash A & \Gamma \vdash B\end{array}}{\Gamma \vdash A \wedge B}\,(\wedge\text{-in})}{\Gamma \vdash B}\,(\wedge\text{-el}_2) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\, d_2\\ \Gamma \vdash B\end{array}$$

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

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

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

  - eliminando la hipótesis A de todos los secuentes apareciendo en d
  - remplazando cada invocación del axioma A (en un secuente de la forma $\Gamma, A, \Gamma' \vdash A'$, con $A' \cong A$) por la derivación d' (debilitada y convertida al secuente $\Gamma, \Gamma' \vdash A'$)

- **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 lógicos (2/5)

Corte de $\Rightarrow$:

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

Reducción de los cortes lógicos (3/5)

Cortes de $\vee$:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A\end{array}}{\Gamma \vdash A \vee B}\ (\vee\text{-in}_1) \qquad \begin{array}{cc}\vdots\ d_1' & \vdots\ d_2'\\ \Gamma, A \vdash C & \Gamma, B \vdash C\end{array}}{\Gamma \vdash C}\ (\vee\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d\\ \Gamma \vdash A\end{array} \qquad \begin{array}{c}\vdots\ d_1'[\mathsf{ax}(A) := d]\\ \Gamma \vdash C\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash B\end{array}}{\Gamma \vdash A \vee B}\ (\vee\text{-in}_2) \qquad \begin{array}{cc}\vdots\ d_1' & \vdots\ d_2'\\ \Gamma, A \vdash C & \Gamma, B \vdash C\end{array}}{\Gamma \vdash C}\ (\vee\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d\\ \Gamma \vdash B\end{array} \qquad \begin{array}{c}\vdots\ d_2'[\mathsf{ax}(B) := d]\\ \Gamma \vdash C\end{array}$$

Corte de $\top/\bot$: ninguno

Reducción de los cortes lógicos (4/5)

Corte de $\forall$: (con $x \notin FV(\Gamma)$ y $A' \cong A[x := t]$)

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

Corte de $\exists$: (con $x \notin FV(\Gamma, B)$)

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

Reducción de los cortes lógicos (5/5)

Corte de $=$: (con $t \cong t'$ y $A' \cong A[x := t']$)

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

Reducción de los cortes de inducción (1/4)

Intuición 1: El principio de inducción sólo sirve para demostrar una propiedad $P(x)$ hasta un término abierto, por ejemplo $y + 3$:

$$\dfrac{\begin{array}{cc}\vdots\, d_0 & \vdots\, d_s(x) \\ P(0) & P(x) \Rightarrow P(x+1)\end{array}}{P(y+3)}$$

Cuando se trata de alcanzar un entero concreto, por ejemplo 4, siempre se puede "desenrollar" la inducción del modo siguiente:

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{cc}\vdots\, d_0 & \vdots\, d_s(0) \\ P(0) & P(0) \Rightarrow P(1)\end{array}}{P(1)} \quad \vdots\, d_s(1)}{P(2)} \quad \vdots\, d_s(2)}{P(3)} \quad \vdots\, d_s(3)}{P(4)}$$

Reducción de los cortes de inducción (2/4)

Intuición 2: En la Aritmética, los enteros naturales son:

- Introducidos por los símbolos 0 y $s(x)$ ("constructores")

$$t \quad ::= \quad 0 \quad | \quad s(t') \quad | \quad \cdots$$

- Eliminados por el principio de inducción:

$$\frac{\Gamma \vdash A[x := 0] \qquad \Gamma, A \vdash A[x := s(x)]}{\Gamma \vdash A' \quad (\cong A[x := t])}\ \text{(Nat-el)} \qquad (\text{si } x \notin FV(\Gamma))$$

Por lo tanto... La regla de inducción forma un corte cada vez que está usada con un término t de la forma $t \cong 0$ o $t \cong s(t')$

(Cuando t no es de ninguna de las dos formas anteriores, no hay corte)

Reducción de los cortes de inducción (3/4)

Cortes de inducción: (con $x \notin FV(\Gamma)$ y $A' \cong A[x := t]$)

- Corte cuando $t \cong 0$:

$$\dfrac{\begin{array}{cc}\vdots\, d_0 & \vdots\, d_s \\ \Gamma \vdash A[x := 0] & \Gamma, A \vdash A[x := s(x)]\end{array}}{\Gamma \vdash A' \quad (\cong A[x := 0])}\ \text{(Nat-el)} \quad \rightsquigarrow \quad \dfrac{\begin{array}{c}\vdots\, d_0 \\ \Gamma \vdash A[x := 0]\end{array}}{\Gamma \vdash A'}\ \text{(Conv)}$$

- Corte cuando $t \cong s(t')$:

$$\dfrac{\begin{array}{cc}\vdots\, d_0 & \vdots\, d_s \\ \Gamma \vdash A[x := 0] & \Gamma, A \vdash A[x := s(x)]\end{array}}{\Gamma \vdash A' \quad (\cong A[x := s(t')])}\ \text{(Nat-el)} \quad \rightsquigarrow \quad \dfrac{\dfrac{\begin{array}{cc}\vdots\, d_0 & \vdots\, d_s \\ \Gamma \vdash A[x := 0] & \Gamma, A \vdash A[x := s(x)]\end{array}}{\Gamma \vdash A[x := t']}\ \text{(Nat-el)} \\ \vdots\ d_s[x{:=}t'][\mathrm{Ax}(A[x{:=}t']){:=}\ldots] \\ \Gamma \vdash A[x := s(t')]}{\Gamma \vdash A'}\ \text{(Conv)}$$

Reducción de los cortes de inducción (4/4)

Ejemplo de reducción en el caso cerrado:

$$\dfrac{\begin{array}{cc}\vdots\, d_0 & \vdots\, d_s(x) \\ \Gamma \vdash P(0) & \Gamma, P(x) \vdash P(s(x))\end{array}}{\Gamma \vdash P(4)}\ \text{(Nat-el)} \quad \overset{\times 5}{\rightsquigarrow} \quad \begin{array}{l} \vdots\, d_0 \\ \Gamma \vdash P(0) \\ \vdots\, d_s(0)[\mathrm{Ax}(P(0)) := d_0] \\ \Gamma \vdash P(1) \\ \vdots\, d_s(1)[\mathrm{Ax}(P(1)) := \cdots] \\ \Gamma \vdash P(2) \\ \vdots\, d_s(2)[\mathrm{Ax}(P(2)) := \cdots] \\ \Gamma \vdash P(3) \\ \vdots\, d_s(3)[\mathrm{Ax}(P(3)) := \cdots] \\ \Gamma \vdash P(4) \end{array}$$

Eliminación de cortes en el sistema HA$^{\cong}$

Teorema (Eliminación de cortes en HA$^{\cong}$)

El sistema formado por las 10 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):

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

Por lo tanto, toda sucesión de reducciones es finita

Demostración: Postpuesta

Corolario (Derivaciones sin cortes en HA$^{\cong}$)

Todo secuente derivable en HA$^{\cong}$ tiene una derivación sin cortes (en HA$^{\cong}$)

Variables libres de una derivación (1/4)

Definición (Variables libres de una derivación, 1/3)

Dada una derivación $d \equiv \left\{ \dfrac{\begin{array}{ccc} \vdots\, d_1 & & \vdots\, d_n \\ \Gamma_1 \vdash A_1 & \cdots & \Gamma_n \vdash A_n \end{array}}{\Gamma \vdash A}\ (R) \right.$

se define el conjunto $FV(d)$ de las variables libres de d por inducción sobre d, distinguiendo los casos en función de la última regla (R):

- Regla sin premisa (axioma, $\top$-intro, $=$-intro): $FV(d) := FV(\Gamma) \cup FV(A)$
- Otra regla del cálculo proposicional ($\Rightarrow$-intro, $\Rightarrow$-elim, $\wedge$-intro, $\wedge$-elim$_{1,2}$, $\vee$-intro$_{1,2}$, $\vee$-elim, $\bot$-elim): $FV(d) := FV(d_1) \cup \cdots \cup FV(d_n)$
- Regla $=$-elim: $FV(d) := FV(d_1) \cup FV(d_2) \cup FV(A)$

$$d \equiv \left\{ \dfrac{\begin{array}{cc} \vdots\, d_1 & \vdots\, d_1 \\ \Gamma \vdash t = u & \Gamma \vdash B[x := t] \end{array}}{\Gamma \vdash A}\ (=\text{-el}) \right. \qquad (\text{con}\ \ A \cong B[x := u])$$

(...)

Variables libres de una derivación (2/4)

Definición (Variables libres de una derivación, 2/3)

- Regla $\forall$-intro: $FV(d) := FV(d_1) \setminus \{x\}$

$$d \equiv \begin{cases} \vdots\ d_1 \\ \dfrac{\Gamma \vdash B}{\Gamma \vdash \forall x\, B}\ (\forall\text{-in}) \end{cases} \qquad (\text{con}\quad x \notin FV(\Gamma))$$

- Regla $\forall$-elim: $FV(d) := FV(d_1) \cup FV(A) \cup FV(t)$

$$d \equiv \begin{cases} \vdots\ d_1 \\ \dfrac{\Gamma \vdash \forall x\, B}{\Gamma \vdash A}\ (\forall\text{-el}) \end{cases} \qquad (\text{con}\quad A \cong B[x := t])$$

- Regla $\exists$-intro: $FV(d) := FV(d_1) \cup FV(t)$

$$d \equiv \begin{cases} \vdots\ d_1 \\ \dfrac{\Gamma \vdash B[x := t]}{\Gamma \vdash \exists x\, B}\ (\forall\text{-in}) \end{cases}$$

(...)

Variables libres de una derivación (3/4)

Definición (Variables libres de una derivación, 3/3)

- Regla $\exists$-elim: $FV(d) := FV(d_1) \cup (FV(d_2) \setminus \{x\})$

$$d \equiv \left\{ \dfrac{\begin{array}{cc} \vdots\, d_1 & \vdots\, d_2 \\ \Gamma \vdash \exists x\, B & \Gamma, B \vdash A \end{array}}{\Gamma \vdash A}\ (\exists\text{-el}) \right. \qquad (\text{con}\ \ x \notin FV(\Gamma, A))$$

- Regla de inducción: $FV(d) := FV(d_1) \cup (FV(d_2) \setminus \{x\}) \cup FV(A) \cup FV(t)$

$$d \equiv \left\{ \dfrac{\begin{array}{cc} \vdots\, d_1 & \vdots\, d_2 \\ \Gamma \vdash B[x := 0] & \Gamma, B \vdash B[x := s(x)] \end{array}}{\Gamma \vdash A}\ (\text{Nat-el}) \right. \qquad \begin{pmatrix} \text{con}\ \ x \notin FV(\Gamma) \\ \text{y}\ \ A \cong B[x := t] \end{pmatrix}$$

Variables libres de una derivación (4/4)

Lema

Para toda derivación d de un secuente $\Gamma \vdash A$:

(1) $FV(\Gamma) \cup FV(A) \subseteq FV(d)$

(2) Si $d \rightsquigarrow d'$ (reducción de corte), entonces $FV(d') \subseteq FV(d)$

(3) Para toda variable $x \in FV(d)$ y para todo término u:

$$FV(d[x := u]) = (FV(d) \setminus \{x\}) \cup FV(u)$$

Recordatorio: $d[x := u]$ es una derivación de $\Gamma[x := u] \vdash A[x := u]$

- La conclusión de una derivación cerrada es un secuente cerrado, pero un secuente cerrado puede tener un derivación abierta
- Siempre se puede cerrar una derivación d de un secuente $\Gamma \vdash A$ ya cerrado, sustituyendo a cada variable $x \in FV(d)$ cualquier término cerrado (por ejemplo 0). Esto no afecta la conclusión $\Gamma \vdash A$

Propiedades de las derivaciones sin cortes (1/7)

A partir de ahora, sólo se consideran derivaciones cerradas

Proposición (Forma de una derivación cerrada y sin cortes de $\vdash A$)

En HA$^{\cong}$, toda derivación cerrada y sin cortes de un secuente de la forma

$$\vdash A$$ (i.e. con antecedente vacío)

se acaba con una regla de introducción

Obs.: La hipótesis "derivación cerrada" implica que la fórmula A está cerrada

Propiedades de las derivaciones sin cortes (2/7)

Demostración.

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

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

$$d \equiv \left\{ \begin{array}{c} \begin{array}{cc} \vdots\, d_1 & \vdots\, d_2 \\ \vdash B \Rightarrow A & \vdash B \end{array} \\ \hline \vdash A \end{array} \right.$$

  Se observa que la subderivación d_1 del secuente $\vdash B \Rightarrow A$ también es cerrada y 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 lógica, se observa que la subderivación d_1 de su premisa principal (también cerrada y sin cortes) 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. (...)

Propiedades de las derivaciones sin cortes (3/7)

Demostración (continuación).

- Regla de inducción. En este caso, la derivación $d : (\vdash A)$ es de la forma

$$d \equiv \left\{ \dfrac{\begin{array}{cc} \vdots\ d_1 & \vdots\ d_2 \\ \vdash B[x := 0] & B \vdash B[x := s(x)] \end{array}}{\vdash A} \right. \qquad (\text{con } A \cong B[x := t])$$

  Como la derivación d está cerrada, el término t también está cerrado (por def. de $FV(d)$). Por lo tanto, tenemos que $t \cong 0$ o $t \cong s(t')$ para algún t'. Esto implica que d es un corte, y demuestra que este caso también es imposible.

- Regla de introducción. Es el único caso posible. □

Propiedades de las derivaciones sin cortes (4/7)

Combinada con el teorema de eliminación de cortes, la proposición anterior implica la consistencia del sistema HA$^{\cong}$:

Corolario 1 (Consistencia)

El secuente $\vdash \bot$ no es derivable en el sistema HA$^{\cong}$

Demostración.

Si el secuente $\vdash \bot$ fuera derivable en HA$^{\cong}$, tendría una derivación cerrada y sin cortes. Tal derivación acabaría con una regla de intro: imposible pues tal regla no existe. $\square$

Propiedades de las derivaciones sin cortes (5/7)

Corolario 2 (Propiedad de la disyunción)

Si un secuente cerrado de la forma $\vdash A \vee B$ es derivable en el sistema HA$^{\cong}$, entonces al menos uno de $\vdash A$ o $\vdash B$ es derivable

Demostración.

Si el secuente cerrado $\vdash A \vee B$ es derivable en HA$^{\cong}$, entonces tiene una derivación cerrada y sin cortes, 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 (6/7)

Corolario 3 (Propiedad de la existencia en $HA^{\cong}$)

Si un secuente cerrado de la forma $\vdash \exists x\, A(x)$ es derivable en $HA^{\cong}$, entonces el secuente $\vdash A(n)$ es derivable para algún entero de Peano n

Demostración.

Si el secuente cerrado $\vdash \exists x\, A(x)$ es derivable en $HA^{\cong}$, entonces tiene una derivación cerrada y sin cortes, que se acaba con una regla de introducción. Por lo tanto, tal derivación es de la forma

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

donde t es un término cerrado. Escribiendo $n := \downarrow t$, se deduce una derivación:

$$\dfrac{\begin{array}{c}\vdots\ d\\ \vdash A(t)\end{array}}{\vdash A(n)}\ (\text{Conv})$$

□

Propiedades de las derivaciones sin cortes (7/7)

Corolario 4 (Igualdades derivables en HA$^{\cong}$)

Un secuente cerrado de la forma $\vdash t = u$ es derivable en el sistema HA$^{\cong}$ si y sólo si $t \cong u$ (i.e. t y u son computacionalmente equivalentes)

Demostración.

Supongamos que el secuente cerrado $\vdash t = u$ es derivable en HA$^{\cong}$. Entonces tiene una derivación cerrada y sin cortes, que se acaba con una regla de introducción. Por lo tanto, tal derivación es de la forma

$$\dfrac{}{\vdash t = u}\ (=\text{-in}),$$

con $t \cong u$. El recíproco es obvio. □

Extracción de programas

Teorema (Extracción de funciones recursivas)

Si el siguiente secuente cerrado es derivable en $HA^{\cong}$

$$\vdash \ \forall x_1 \cdots \forall x_k \, \exists y \, A(x_1, \ldots, x_k, y)$$

entonces existe una función recursiva total $f : \mathbb{N}^k \to \mathbb{N}$ tal que

$$\vdash \ A(n_1, \ldots, n_k, f(n_1, \ldots, n_k))$$

es derivable en $HA^{\cong}$ para todo $(n_1, \ldots, n_k) \in \mathbb{N}^k$

Demostración.

Dada una derivación cerrada d de $\vdash \forall x_1 \cdots \forall x_k \, \exists y \, A(x_1, \ldots, x_k, y))$, se construye la función recursiva $f : \mathbb{N}^k \to \mathbb{N}$ del modo siguiente:

$f(n_1, \ldots, n_k) :=$

1. Formar la derivación $d\langle n_1, \ldots, n_k \rangle$ de $\vdash \exists y \, A(n_1, \ldots, n_k, y))$
2. Eliminar los cortes de $d\langle n_1, \ldots, n_k \rangle$, y extraer el testigo t
3. Devolver el entero $n := \downarrow t$

□

Ejemplo

- Consideremos una derivación cerrada d del teorema:

$$\mathsf{HA}^{\cong} \vdash \forall x\, \exists y\, (x = 2y \vee x = 2y + 1)$$

- A cada $n \in \mathbb{N}$ se asocia la derivación cerrada

$$d\langle n \rangle \;:\equiv\; \left\{ \dfrac{\begin{array}{c}\vdots\; d \\ \vdash \forall x\, \exists y\, (x = 2y \vee x = 2y + 1)\end{array}}{\vdash \exists y\, (n = 2y \vee n = 2y + 1)}\ (\forall\text{-el}) \right.$$

- Eliminando los cortes en la derivación anterior, se obtiene una derivación d'_n sin cortes que sólo tiene dos formas posibles:

$$\dfrac{\dfrac{\dfrac{}{\vdash n = 2p}\ (=\text{-in})}{\vdash n = 2p \vee n = 2p + 1}\ (\vee\text{-in}_1)}{\vdash \exists y\, (n = 2y \vee n = 2y + 1)}\ (\exists\text{-in}) \quad \text{o} \quad \dfrac{\dfrac{\dfrac{}{\vdash n = 2p + 1}\ (=\text{-in})}{\vdash n = 2p \vee n = 2p + 1}\ (\vee\text{-in}_2)}{\vdash \exists y\, (n = 2y \vee n = 2y + 1)}\ (\exists\text{-in})$$

- En ambos casos, la derivación d'_n contiene el entero $p := \lfloor n/2 \rfloor$

Plan

Conclusión

- El teorema de eliminación de cortes en el sistema HA$^{\cong}$ implica que:

Teorema

El sistema HA$^{\cong}$ es constructivo, en el sentido de que es consistente y cumple las propiedades de la disyunción y de la existencia

- Y como HA$^{\cong}$ es una extensión conservativa de HA, se deduce que:

Teorema

La Aritmética de Heyting (HA) es constructiva (mismo sentido)

- Se observa que la consistencia de HA se deduce de la propiedad de eliminación de cortes por medios puramente aritméticos
- Por lo tanto, el teorema de eliminación de cortes no se puede demostrar en HA/PA (por el segundo teorema de incompletitud)
- Ahora necesitamos más herramientas para demostrar los teoremas de eliminación de cortes: los cálculos lambda (puro y tipados)