Cálculo de Enunciados L

Temas:

- El Sistema formal L: axiomas y regla de inferencia.
- Demostración de teoremas y deducciones en L.
- Corrección, completitud y decidibilidad de L.

Trabajo Práctico: TP 03.

Bibliografía:

- Pons, Rosenfeld, Smith. Lógica para Informática. Capítulo 1
- Hamilton. Lógica para Matemáticos. Capítulo 2

Martes 07 de Septiembre 2021 de 16 a 18hs:
Unirse a la reunión Zoom
https://zoom.us/j/99670397999?pwd=ZmhlUGFIZFBRcWpNSEh4MmxJc1JOZz09

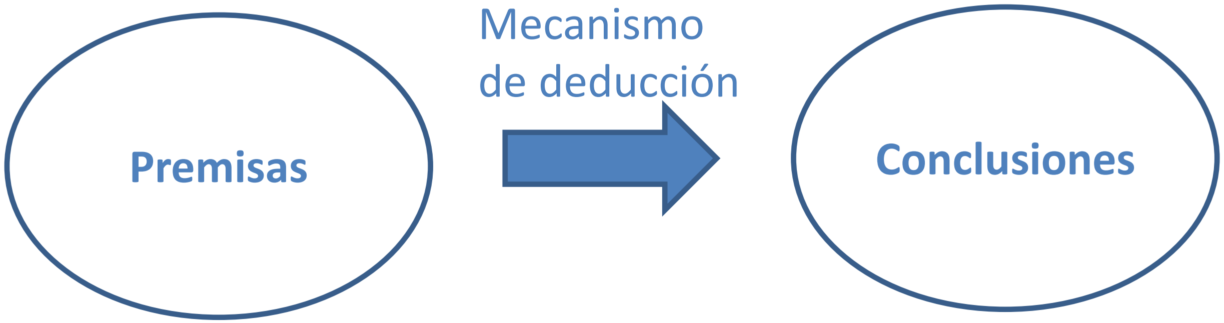
ID de reunión: 996 7039 7999 Código de acceso: LOGICA

Dra. Claudia Pons

Claudia.pons.33@gmail.com

Mecanismos formales de razonamiento

Un mecanismo formal de razonamiento (o de inferencia, deducción, demostración) consiste en una colección de reglas que pueden ser aplicadas sobre cierta información inicial para derivar información adicional, en una forma puramente sintáctica.



A continuación se presentan un *sistema deductivo* llamado L.

El Sistema formal L

Un sistema deductivo axiomático está compuesto por: l. probar lógica.

- **un conjunto de *axiomas* (en realidad esquemas de axiomas)**
- **un conjunto *de reglas de inferencia*.**

Los axiomas son fórmulas bien formadas.
Las reglas determinan qué fórmulas pueden inferirse a partir de qué fórmulas.

Axiomas de L

Los axiomas de un sistema axiomático son un conjunto de fórmulas que se toman como punto de partida para las demostraciones.
Un conjunto de axiomas muy conocido para la lógica proposicional es el que definió J. Lukasiewicz:

$\vdash A$ (equivalente). $\models A$

el teorema con L y ello.

el tautología. Tabla de verdad.

$L_1 : (A \to (B \to A))$

$L_2 : (A \to (B \to C)) \to ((A \to B) \to (A \to C))$

$L_3 : ((\neg A) \to (\neg B)) \to (B \to A)$

Reglas de inferencia de L

El sistema L tiene una única regla de inferencia, el modus ponens:

MP: a partir de A y de $(A \to B)$ se infiere B

Una regla de inferencia es una función que asigna una fórmula (conclusión) a un conjunto de fórmulas (premisas).

Axiomas de L

Veamos como se instancian los axiomas de L

L_1 : $(A \rightarrow (B \rightarrow A))$

$(p \rightarrow (p \rightarrow p))$ con $A=p$ y $B=p$

$((p \rightarrow p) \rightarrow (q \rightarrow (p \rightarrow p)))$ con $A=(p \rightarrow p)$ y $B=q$

L_2 : $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

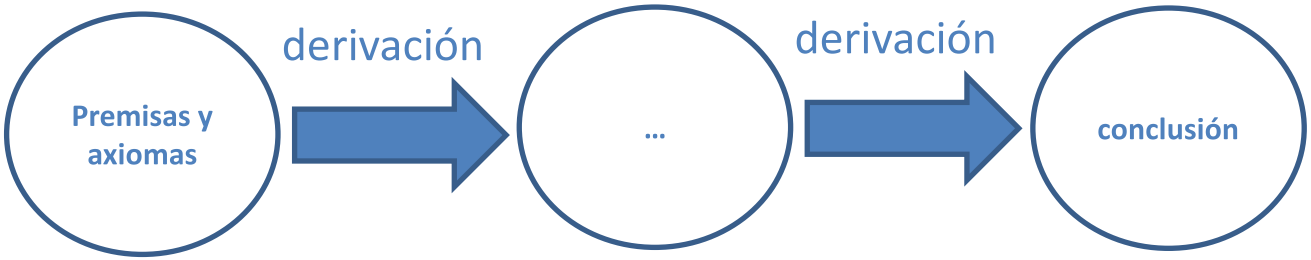
$((p \rightarrow p) \rightarrow (q \rightarrow p)) \rightarrow (((p \rightarrow p) \rightarrow q) \rightarrow ((p \rightarrow p) \rightarrow p))$

con $A=(p \rightarrow p)$, $B=q$ y $C=p$

Demostración o derivación en L

- Una ***demostración*** es una sucesión de aplicaciones de reglas de inferencia que permite llegar a una conclusión a partir de determinadas premisas y axiomas.

- Como la derivación es una relación transitiva, todas las fórmulas que se vayan obteniendo sucesivamente están implicadas por las premisas o axiomas.



Demostración o derivación en L

La notación es la siguiente $\mathbf{\Gamma \mid\!-_L A_n}$

Se lee: "A partir de las premisas contenidas en el conjunto Γ (Gamma) se deduce (o infiere o deriva) la conclusión A_n".

- Γ es un conjunto de premisas (o hipótesis)
- A_n es la conclusión a la que se quiere llegar.

Tanto las premisas como la conclusión son fórmulas bien formadas (fbf), es decir, son sentencias escritas en el lenguaje de la lógica.

- Una **demostración** es una sucesión finita de fórmulas bien formadas

$$A_1, A_2, \ldots, A_n,$$

tal que para todo i, con $1 \leq i \leq n$, A_i es una premisa o es un axioma, o bien se infiere de miembros anteriores de la sucesión como consecuencia directa de la aplicación de una regla de inferencia (MP).

Demostración. Ejemplo

- El esquema general es este: $\Gamma \mid\!-_L A_n$
- Nuestro ejemplo es: $\{ ((p \to q) \to r), q \} \mid\!-_L (p\text{->}r)$

- Para demostrar que la conclusión realmente se deduce de esas premisas hay que armar una demostración.

Recordar:

Una **demostración** es una sucesión finita de fórmulas bien formadas

$A_1, A_2, \ldots, A_n$

tal que para todo i, con $1 \leq i \leq n$,

- A_i es una premisa o es un axioma, o bien

- A_i se infiere de miembros anteriores por Modus Ponens.

Demostración. Ejemplo

El esquema general es este: $\Gamma \mid\!-_L A_n$

Nuestro ejemplo es: $\{ ((p \rightarrow q) \rightarrow r), q \} \mid\!-_L (p\text{->}r)$

Vamos a construir la demostración:

1.	q->(p->q)	instancia de L1
2.	q	hipótesis
3.	(p->q)	aplicación de MP entre 1 y 2
4.	$((p \rightarrow q) \rightarrow r)$	hipótesis
5.	r	aplicación de MP entre 3 y 4
6.	r->(p->r)	instancia de L1
7.	(p->r)	aplicación de MP entre 5 y 6

Se observa que construimos una cadena de 7 pasos, A_1, A_2, A_3, A_4 A_5, $A_{6,}$ A_7 donde el último paso es la fbf que queríamos derivar.

En cada uno de los pasos usamos:

- una premisa (paso 2 y paso 4)
- un axioma (paso 1 y 6),
- la aplicación de la regla de inferencia MP (paso 3, 5 y 7)

Esta cadena **DEMUESTRA que efectivamente a partir de esas 2 premisas , sean** A_2, y A_4 **se deriva la conclusión** A_7 $(p \rightarrow r)$

Que es un teorema de L?

- Cuando una fbf se puede demostrar a partir del conjunto vacío de hipótesis se la llama **TEOREMA de L**.
- Por ejemplo (p->p) es un teorema de L.
- La notación es **$|-_L$ (p->p)**
- Vean que Gamma no aparece (porque está vacío).
- Para demostrar que (p->p) es un teorema de L tenemos que construir la cadena que termine en (p->p), por ejemplo la siguiente cadena es una demostración:

1.	$(p \rightarrow ((p \rightarrow p) \rightarrow p)) \rightarrow ((p \rightarrow (p \rightarrow p)) \rightarrow (p \rightarrow p))$	instanciando el axioma L_2
2.	$p \rightarrow ((p \rightarrow p) \rightarrow p)$	instanciando el axioma L_1
3.	$(p \rightarrow (p \rightarrow p)) \rightarrow (p \rightarrow p)$	MP entre 1 y 2
4.	$p \rightarrow (p \rightarrow p)$	instanciando el axioma L_1
5.	**$(p \rightarrow p)$**	MP entre 3 y 4

Metateorema de la Deducción

Si $\Gamma \cup \{A\} \vdash_L B$ entonces $\Gamma \vdash_L (A \to B)$

Veamos para que sirve.
Hemos demostrado
$\Gamma \vdash_L (p\text{->}p)$ para Γ conjunto vacío.

Nos llevó 5 engorrosos pasos!!

Aplicando el Meta-teorema de la deducción lo podemos resolver mas fácil!

Si demuestro $\Gamma \cup \{p\} \vdash_L p$
entonces por el MT de la Deducción obtengo $\Gamma \vdash_L (p \to p)$

Cuántos pasos tiene la demostración de $\Gamma \cup \{p\} \vdash_L p$ **?**
1 solo. Trivial!

Metateorema de la Deducción. Ejemplo

Premisas:

- Si tenemos una buena especificación entonces obtenemos un diseño correcto.
- Si obtenemos un diseño correcto obtenemos un buen programa, a menos que nuestro programador sea mediocre.
- Nuestro programador no es mediocre.

Se quiere concluir que:

- Si tenemos una buena especificación obtenemos un buen programa.

Metateorema de la Deducción. Ejemplo

Primeramente formalizamos el razonamiento mediante las variables de enunciado p, q, r, s:

p : Tenemos una buena especificación
q : Obtenemos un diseño correcto
r : Obtenemos un buen programa
s : Nuestro programador es mediocre

Premisas:

- Si tenemos una buena especificación entonces obtenemos un diseño correcto. $A_1 :$ $(p \rightarrow q)$
- Si obtenemos un diseño correcto obtenemos un buen programa, a menos que nuestro programador sea mediocre. $A_2 : q \rightarrow ((\neg s) \rightarrow r)$
- Nuestro programador no es mediocre. $A_3 : (\neg s)$

Conclusión:

- Si tenemos una buena especificación obtenemos un buen programa. $A_4 : (p \rightarrow r)$

La argumentación es: $\Gamma \vdash_L (A \rightarrow B)$

Es decir $\{\underbrace{(p \rightarrow q)}_{A_1}, \underbrace{q \rightarrow ((\neg s) \rightarrow r)}_{A_2}, \underbrace{(\neg s)}_{A_3}\} \vdash_L \underbrace{(p \rightarrow r)}_{A_4}$

Metateorema de la Deducción. Ejemplo

Si $\Gamma \cup \{A\} \vdash_L B$ entonces $\Gamma \vdash_L (A \rightarrow B)$

La argumentación que queremos demostrar es: $\Gamma \vdash_L (A \rightarrow B)$
Es decir $\{(p \rightarrow q), q \rightarrow ((\neg s) \rightarrow r), (\neg s)\} \vdash_L (p \rightarrow r)$

Usando el MT de la deducción vamos a demostrar: $\Gamma \cup \{A\} \vdash_L B$
Es decir, $\{(p \rightarrow q), q \rightarrow ((\neg s) \rightarrow r), (\neg s), \mathbf{p}\} \vdash_L \mathbf{r}$

Demostración:

1.	$(p \rightarrow q)$	pertenece a Γ
2.	$\mathbf{p}$	es A
3.	q	MP
4.	$q \rightarrow ((\neg s) \rightarrow r)$	pertenece a Γ
5.	$((\neg s) \rightarrow r)$	MP
6.	$(\neg s)$	pertenece a Γ
7.	r	MP

Metateorema de la Deducción. Ejemplo

Y la misma demostración sin usar el MT de la Deducción quedaría así:

$\{(p \rightarrow q), q \rightarrow ((\neg s) \rightarrow r), (\neg s)\} \vdash_L (p \rightarrow r)$

1.	$(p \rightarrow q)$	pertenece a Γ
2.	$q \rightarrow ((\neg s) \rightarrow r)$	pertenece a Γ
3.	$p \rightarrow ((\neg s) \rightarrow r)$	por S.H. (3 pasos mas)
4.	$(p \rightarrow ((\neg s) \rightarrow r)) \rightarrow ((p \rightarrow (\neg s)) \rightarrow (p \rightarrow r))$	instanciación del axioma L_2
5.	$(p \rightarrow (\neg s)) \rightarrow (p \rightarrow r)$	MP entre 3 y 4
6.	$(\neg s) \rightarrow (p \rightarrow (\neg s))$	instanciación del axioma L_1
7.	$(\neg s)$	pertenece a Γ
8.	$(p \rightarrow (\neg s))$	MP entre 6 y 7
9.	$(p \rightarrow r)$	MP entre 5 y 8

Corrección (Sensatez), Completitud y Consistencia de L

Corrección (Sensatez) y Completitud de un sistema deductivo

De un sistema deductivo se espera naturalmente que:

- sus demostraciones produzcan conclusiones correctas,
- y también en lo posible la propiedad inversa, es decir que sea capaz de demostrar todas y cada una de ellas.

Formalmente ambas propiedades se pueden formular de la siguiente manera:

El sistema deductivo L es ***correcto*** (o ***sensato***)

si $\vdash_L A$ implica $\models A$.

Si A es **teorema**, entonces A es **tautología**.

Recíprocamente, un sistema deductivo L es ***completo***

si $\models A$ implica $\vdash_L A$.

Si A es tautología entonces A es teorema.

Corrección y Completitud de un sistema deductivo

Notemos las diferencias entre $|-_L A$ y $|= A$

$|-_L A$

A es teorema, lo demuestro construyendo su demostración (una secuencia $A_1, A_2, \ldots, A$, tal que para todo i, con $1 \leq i \leq n$, A_i es un axioma, o bien se infiere de miembros anteriores de la sucesión por MP)

Es un procedimiento sintáctico, hago «cuentas» en el cálculo.

$|= A$

A es tautología, lo demuestro construyendo su tabla de verdad y comprobando que da Verdadero en todas las filas.

Es un procedimiento «semántico», aplico las funciones de verdad.

Corrección y Completitud de un sistema deductivo

$L_1 : (A \to (B \to A))$

$L_2 : (A \to (B \to C)) \to ((A \to B) \to (A \to C))$

$L_3 : ((\neg A) \to (\neg B)) \to (B \to A)$

Notemos las diferencias entre $|-_L A$ y $|= A$

$|-_L (p \to p)$

1. $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$ instanciando el axioma L_2
2. $(p \to ((p \to p) \to p))$ instanciando el axioma L_1
3. $(p \to (p \to p)) \to (p \to p)$ MP entre 1 y 2
4. $p \to (p \to p)$ instanciando el axioma L_1
5. **$(p \to p)$** MP entre 3 y 4

Es un procedimiento «**sintáctico**», hago «cuentas» en el cálculo.

$|= (p \to p)$

p	$(p \to p)$
V	V
F	V

Es un procedimiento «**semántico**», aplico las funciones de verdad.

Corrección del sistema deductivo L

La corrección de un sistema deductivo está garantizada si se cuenta con axiomas verdaderos y reglas de inferencia correctas (o sensatas), es decir que preservan la verdad.

Entonces ¿Cómo demostramos que L es correcto?

Debemos demostrar lo siguiente.

- sus axiomas L1, L2 y L3 son tautologías,
- Su regla MP preserva la verdad.

Corrección del sistema deductivo L

Los axiomas de L son tautologías

- $L_1 : A \to (B \to A)$
- $L_2 : (A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- $L_3 : ((\neg A) \to (\neg B)) \to (B \to A)$

Les hacemos la tabla de verdad, por ej:

A	B	$A \to (B \to A)$
V	V	V
V	F	V
F	V	V
F	F	V

Corrección del sistema deductivo L

La regla Modus Ponens preserva la verdad.

Definición de MP: a partir de A y de (A $\rightarrow$ B) se infiere B

Lo demostraremos **por el absurdo**:

Suponemos que MP no preserva la verdad, es decir que a partir de A y de (A $\rightarrow$ B), siendo ambas tautologías, se ha inferido B la cual NO es tautología.

Entonces como B no es tautología, existe una valuación, sea v, para las letras de enunciado que aparecen en B (es decir, una fila en su tabla de verdad) para la cual v(B)=F.

Por otra parte como A es tautología, en esa misma valuación toma el valor Verdadero, o sea v(A)=V.

¿Qué valor toma v(A $\rightarrow$ B) ? Toma el valor F, lo cual contradice la hipótesis que dce que (A $\rightarrow$ B) es tautología. PQD.

Corrección del sistema deductivo L

Hemos demostrado que L es sensato (o correcto)

En símbolos:

Si $\vdash_L A$ entonces $\models A$

En palabras:

Si A es teorema de L entonces A es tautología

Propiedad: Consistencia

Un conjunto de Fbf, sea G, **no es consistente** cuando existe alguna Fbf A tal que:
$G \mid\!-_L A$ y $G \mid\!-_L (\sim A)$
Es decir, G permite deducir un enunciado y su negación.

Esta definición se aplica también a L, considerando a G como su conjunto de axiomas.

PROPIEDAD: L es consistente

Demostración:

Por el absurdo. Suponemos que L no es consistente, entonces por definición de consistencia existe una Fbf A tal que: $\mid\!-_L A$ y $\mid\!-_L (\sim A)$

Es decir, tanto A como (~A) ambas son teoremas de L.

Pero por la propiedad de Corrección de L, sabemos que todos los teoremas de L son tautologías. Por lo tanto A es tautologia (o sea $v(A)=V$ para toda valoración v) y al mismo tiempo (~A) es tautología (o sea $v(\sim A)=V$), lo cual es absurdo pues $v(A) \neq v(\sim A)$. PQD.

Propiedad: Decidibilidad

En la teoría de la computación, se define un problema de decisión como aquél que tiene dos respuestas posibles: “sí” o “no”.

Se dice que un problema de decisión es ***decidible*** si existe un algoritmo (es decir, un procedimiento que siempre termina) que lo resuelve.

En el marco de los sistemas deductivos es muy relevante también la cuestión de la decidibilidad, que se formula de la siguiente manera:

Dados Γ y A, ¿existe algún algoritmo que responda “sí” en el caso de que $\Gamma \models A$ y que responda “no” en el caso de que $\Gamma \not\models A$?

Claramente, en la lógica proposicional esta cuestión tiene una respuesta positiva, utilizando algoritmos basados en las tablas de verdad.

Propiedad: Consistencia

Veamos una propiedad muy interesante de L: Si el conjunto de premisas no es consistente, **todo se vuelve demostrable** a partir de dicho conjunto.

En símbolos, sea G un conjunto no consistente, entonces para cualquier Fbf A ocurre que G $|-_L$ A.

Demostración:

Como G no es consistente, entonces puedo deducir B y $\sim$B para alguna Fbf B. Usando ese resultado vemos como puedo demostrar **cualquier** otra Fbf, sea A:

1.	$\sim B \rightarrow (B \rightarrow A)$	Esto es un teorema ya demostrado (Hamilton)
2.	$\sim B$	
3.	$(B \rightarrow A)$	MP entre 1 y 2
4.	B	
5.	A	MP entre 3 y 4.

Notar que no hemos asumido nada acerca de A, por lo tanto esta demostración sirve para cualquier Fbf A, sea contradicción, tautología o contingencia.

Anexo

Demostración del teorema $\vdash_L (\sim B \rightarrow (B \rightarrow A))$

En cada paso se instancia algún axioma de L o se aplica el MP.

(1)	$(\sim\mathscr{B}\rightarrow(\sim\mathscr{A}\rightarrow\sim\mathscr{B}))$	$(L1)$
(2)	$((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$	$(L3)$
(3)	$((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))\rightarrow(\sim\mathscr{B}\rightarrow((\sim\mathscr{A}\rightarrow\sim\mathscr{B})$ $\rightarrow(\mathscr{B}\rightarrow\mathscr{A})))$	$(L1)$
(4)	$(\sim\mathscr{B}\rightarrow((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A})))$	(2), (3) MP
(5)	$(\sim\mathscr{B}\rightarrow((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A})))\rightarrow((\sim\mathscr{B}\rightarrow(\sim\mathscr{A}\rightarrow\sim\mathscr{B})$ $\rightarrow(\sim\mathscr{B}\rightarrow(\mathscr{B}\rightarrow\mathscr{A})))$	$(L2)$
(6)	$(\sim\mathscr{B}\rightarrow(\sim\mathscr{A}\rightarrow\sim\mathscr{B}))\rightarrow(\sim\mathscr{B}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$	(4), (5) MP
(7)	$(\sim\mathscr{B}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$	(1), (6) MP