Lógica y Teoría Descriptiva de Conjuntos

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Lógica y Teoría Descriptiva de Conjuntos

Los Del DGIIM, losdeldgiim.github.io

José Juan Urrutia Milán

Granada, 2025

Índice general

El presente documento es un resumen del microcredencial de "Lógica y Teoría Descriptiva de Conjuntos", que recoge los principales conceptos que se impartieron en el mismo. Si cursa el microcredencial se recomienda ver los recursos proporcionados por el profesorado. Si está cursando actualmente la asignatura de "Lógica y Métodos Discretos" del grado de Informática, los dos primeros capítulos pueden serle de gran ayuda.

A lo largo del curso trabajaremos en $\mathbb{Z}_2$, por lo que se recomienda al lector repasar los apuntes de Álgebra I en caso de no estar familiarizado con dicho cuerpo.

1. Lógica Proposicional

Consideraremos un conjunto finito de proposiciones atómicas, que serán para nosotros enunciados indivisibles. Nos interesará la veracidad o falsedad de cada una de estas proposiciones. Consideraremos sobre estas las conectivas $\neg$, $\wedge$, $\vee$, $\to$ y $\leftrightarrow$. De esta forma, somos capaces de definir lo que es una proposición en nuestro lenguaje.

Definición 1.1 (Proposición)**.** Definimos las proposiciones de forma recursiva[1]:

1. Las proposiciones atómicas son proposiciones.

2. Si α y β son proposiciones, también lo son:

$$\neg\alpha, \ \alpha \wedge \beta, \ \alpha \vee \beta, \ \alpha \to \beta, \ \alpha \leftrightarrow \beta$$

3. No hay más proposiciones que las que se puedan obtener siguiendo una secuencia finita de pasos a partir de las enunciadas.

1.1. Semántica

Una vez definida lo que es una proposición, pasamos a lo que nos interesa, asignar un valor de verdad o de falsedad a cada una de las proposiciones que nos encontremos. Para ello, consideraremos una aplicación del conjunto de las proposiciones en $\mathbb{Z}_2$, e interpretaremos el valor de 0 como falso y el valor de 1 como verdad.

Definición 1.2 (Interpretación)**.** Sea $\mathcal{P}$ el conjunto de todas las proposiciones de un lenguaje proposicional, una interpretación sobre el mismo es una aplicación $I : \mathcal{P} \to \mathbb{Z}_2$ que verifica:

1. $I(\neg a) = 1 + I(a)$.

2. $I(a \wedge b) = I(a)I(b)$.

3. $I(a \vee b) = I(a) + I(b) + I(a)I(b)$.

4. $I(a \to b) = 1 + I(a) + I(a)I(b)$.

5. $I(a \leftrightarrow b) = 1 + I(a) + I(b)$.

Para cualesquiera proposiciones $a, b \in \mathcal{P}$.

[1] Algo que será habitual en este curso.

Observación. Observemos que, gracias a la naturaleza recursiva de las interpretaciones, basta dar un valor de $\mathbb{Z}_2$ a cada proposición atómica para obtener una interpretación: conocidos los valores de las proposiciones atómicas conocemos el valor de cualquier proposición y viceversa.

Definición 1.3. Sea α y β dos proposiciones de forma que $I(\alpha) = I(\beta)$ para cualquier interpretación I, entonces escribiremos que $\alpha \equiv \beta$ y podemos decir que α y β son semánticamente equivalentes.

Definición 1.4. Sea α una proposición:

- Si existe una interpretación I de forma que $I(\alpha) = 1$, diremos que p es **satisfacible**.
- Si existe una interpretación I de forma que $I(\alpha) = 0$, diremos que p es **refutable**.
- Si $I(\alpha) = 1$ para cualquier interpretación I, diremos que p es una **tautología**.
- Si $I(\alpha) = 0$ para cualquier interpretación I, diremos que p es una **contradicción**.

Definición 1.5 (Consecuencia lógica)**.** Sea $\Gamma \cup \{p\}$ un conjunto de proposiciones, decimos que p es consecuencia lógica de Γ (notado por $\Gamma \vDash p$), si dada una interpretación I, siempre que se tenga que $I(\gamma) = 1$ para cualquier $\gamma \in \Gamma$, entonces se tiene que $I(p) = 1$.

Notación. Por comodidad, si p es una proposición de forma que $\emptyset \vDash p$, entonces notaremos:

$$\vDash p$$

Notemos que en este caso p es una tautología, ya que estamos diciendo que $I(p) = 1$ para cualquier[2] interpretación I.

Proposición 1.1. *Se verifica que* $\Gamma \vDash p$ *si y solo si* $(1 + I(p)) \prod_{\gamma \in \Gamma} I(\gamma) = 0$.

Demostración. Veamos las dos implicaciones:

$\Longrightarrow$) Sea I una interpretación:

- Si existe un $\gamma \in \Gamma$ de forma que $I(\gamma) = 0$, entonces tenemos el resultado.
- En caso contrario, tendremos que $I(\gamma) = 1$ para cualquier $\gamma \in \Gamma$. En dicho caso, como $\Gamma \vDash p$, se tendrá que $I(p) = 1$, por lo que:

$$1 + I(p) = 0 \Longrightarrow (1 + I(p)) \prod_{\gamma \in \Gamma} I(\gamma) = 0$$

$\Longleftarrow$) Sea I una interpretación que verifica $I(\gamma) = 1$ para cualquier $\gamma \in \Gamma$, como $\mathbb{Z}_2$ es un dominio de integridad, de $(1 + I(p)) \prod_{\gamma \in \Gamma} I(\gamma) = 0$ deducimos que $I(p) + 1 = 0$, por lo que $I(p) = 1$ y entonces se tiene que $\Gamma \vDash p$.

[2] Cualquiera que haga ciertos todos los elementos del vacío.

$\square$

Teorema 1.2 (de la deducción)**.** *Sea* $\Gamma \cup \{\alpha, \beta\}$ *un conjunto de proposiciones, equivalen:*

1. $\Gamma \vDash \alpha \to \beta$

2. $\Gamma \cup \{\alpha\} \vDash \beta$

Demostración. Demostramos las dos implicaciones:

1) $\Longrightarrow$ 2) Sea I una interpretación de forma que $I(\alpha) = 1$ y que $I(\gamma) = 1$ para todo $\gamma \in \Gamma$, entonces (por 1) deducimos que $I(\alpha \to \beta) = 1$, luego:

$$1 = I(\alpha \to \beta) = 1 + \cancelto{1}{I(\alpha)} + \cancelto{1}{I(\alpha)} I(\beta) = 1 + 1 + I(\beta) = I(\beta)$$

2) $\Longrightarrow$ 1) Sea I una interpretación de forma que $I(\gamma) = 1$ para todo $\gamma \in \Gamma$:

- Si $I(\alpha) = 0$, entonces:

$$I(\alpha \to \beta) = 1 + I(\alpha) + I(\alpha)I(\beta) = 1$$

  Por lo que se tiene 1.

- Si $I(\alpha) = 1$, como $\Gamma \cup \{\alpha\} \vDash \beta$, entonces $I(\beta) = 1$, por lo que:

$$I(\alpha \to \beta) = 1 + I(\alpha) + I(\alpha)I(\beta) = 1 + 1 + 1 = 1$$

$\square$

Ejemplo. Demostraremos ahora que varias proposiciones son tautologías:

$\vDash \alpha \to \alpha$

Por el Teorema de la deducción (1.2), $\vDash \alpha \to \alpha$ es equivalente a ver que $\{\alpha\} \vDash \alpha$. En efecto, sea I una interpretación de forma que $I(\alpha) = 1$, tenemos que $I(\alpha) = 1$.

$\vDash \alpha \to (\beta \to \alpha)$

Por el Teorema de la deducción, es equivalente ver que $\{\alpha\} \vDash \beta \to \alpha$; que nuevamente por el Teorema de la deducción es equivalente ver que $\{\alpha, \beta\} \vDash \alpha$. En efecto, sea I una interpretación de forma que $I(\alpha) = I(\beta) = 1$, entonces $I(\alpha) = 1$.

$\vDash (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$

Por el Teorema de la deducción aplicado 3 veces, es equivalente ver que:

$$\{\alpha \to (\beta \to \gamma), \alpha \to \beta, \alpha\} \vDash \gamma$$

Sea I una interpretación de forma que:

$$1 = I(\alpha \to (\beta \to \gamma)) = I(\alpha \to \beta) = I(\alpha)$$

Entonces:

$$\begin{aligned} 1 &= I(\alpha \to \beta) = 1 + I(\alpha) + I(\alpha)I(\beta) = 1 + 1 + I(\beta) = I(\beta) \Longrightarrow I(\beta) = 1 \\ 1 &= I(\alpha \to (\beta \to \gamma)) = 1 + I(\alpha) + I(\alpha)I(\beta \to \gamma) \\ &= 1 + I(\alpha) + I(\alpha)(1 + I(\beta) + I(\beta)I(\gamma)) = 1 + 1 + 1(1 + 1 + I(\gamma)) \\ &= I(\gamma) \Longrightarrow \underline{I(\gamma) = 1} \end{aligned}$$

$\models (\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha)$

Por el Teorema de la deducción aplicado 2 veces, es equivalente ver que:

$$\{\neg\alpha \to \neg\beta, \neg\alpha \to \beta\} \models \alpha$$

Sea I una interpretación de forma que:

$$1 = I(\neg\alpha \to \neg\beta) = 1 + I(\neg\alpha) + I(\neg\alpha)I(\neg\beta)$$
$$1 = I(\neg\alpha \to \beta) = 1 + I(\neg\alpha) + I(\neg\alpha)I(\beta)$$

Entonces (sumando):

$$0 = I(\neg\alpha \to \neg\beta) + I(\neg\alpha \to \beta) = I(\neg\alpha)(I(\neg\beta) + I(\beta)) \overset{(*)}{=} I(\neg\alpha)$$

Donde en $(*)$ hemos usado que $I(\neg\beta) = 1 + I(\beta) \Longrightarrow I(\neg\beta) + I(\beta) = 1$.

Como $I(\neg\alpha) = 0$, se tiene que $I(\alpha) = 1$, como queríamos demostrar.

Definición 1.6. Sea Γ un conjunto de proposiciones, decimos que Γ es **inconsistente** si para toda interpretación I existe $\gamma \in \Gamma$ de forma que $I(\gamma) = 0$.

Proposición 1.3. *Sea $\Gamma \cup \{\alpha\}$ un conjunto de proposiciones, equivalen:*

1. $\Gamma \models \alpha$.
2. $\Gamma \cup \{\neg\alpha\}$ *es inconsistente.*

Demostración. Demostramos las dos implicaciones:

1) $\Longrightarrow$ 2) Sea I una interpretación:

- Si existe un $\gamma \in \Gamma$ de forma que $I(\gamma) = 0$, entonces Γ es inconsistente, de donde $\Gamma \cup \{\neg\alpha\}$ también lo es.
- Si $I(\gamma) = 1$ para cualquier $\gamma \in \Gamma$, aplicando que $\Gamma \models \alpha$ deducimos que $I(\alpha) = 1 \Longrightarrow I(\neg\alpha) = 1 + I(\alpha) = 0$, por lo que $\Gamma \cup \{\neg\alpha\}$ es inconsistente.

2) $\Longrightarrow$ 1) Sea I una interpretación de forma que $I(\gamma) = 1$ para cualquier $\gamma \in \Gamma$, como $\Gamma \cup \{\neg\alpha\}$ es inconsistente, deducimos que $I(\neg\alpha) = 0$, luego $I(\alpha) = 1$. $\square$

1.2. Demostraciones

Definición 1.7 (Demostración)**.** Sean $\mathcal{A}$ y $\Gamma \cup \{p\}$ dos conjuntos de proposiciones (nos referiremos al conjunto $\mathcal{A}$ como "conjunto de axiomas" y a Γ como "conjunto de hipótesis"), una demostración de p a partir de Γ (notado por $\Gamma \vdash p$) es una secuencia de proposiciones $\alpha_1, \alpha_2, \ldots, \alpha_n$ de forma que $\alpha_n = p$ y se verifica para todo i menor o igual que n:

- bien $\alpha_i \in \mathcal{A} \cup \Gamma$.
- bien existen j, k naturales con $j < k < i$ siendo $\alpha_k = \alpha_j \to \alpha_i$.

  En este caso, diremos que se tiene α_i por modus ponens de j y k.

Notación. Si p es una proposición de forma que $\emptyset \vdash p$, podremos notar $\vdash p$ y diremos que p es un teorema.

Ejemplo. Como ejemplo de demostración, veamos que $\{\alpha, \alpha \to \beta\} \vdash \beta$ (regla conocida como "Modus ponens"). Para ello, consideramos:

$$\begin{aligned}
\alpha_1 &= \alpha \\
\alpha_2 &= \alpha \to \beta \\
\alpha_3 &= \beta
\end{aligned}$$

Como vemos, es una demostración de β a partir de $\{\alpha, \alpha \to \beta\}$ porque $\alpha_1, \alpha_2, \alpha_3$ son proposiciones, $\alpha_3 = \beta$ y:

- $\alpha_1 \in \Gamma$.
- $\alpha_2 \in \Gamma$.
- $1, 2 < 3$ y $\alpha_2 = \alpha_1 \to \alpha_3$.

Notación. Para abreviar las demostraciones, a partir de ahora no daremos una secuencia numerada de proposiciones $\alpha_1, \ldots, \alpha_n$, sino que numeraremos los pasos de la demostración y entenderemos que para formalizarla totalmente debemos coger como α_i el paso $i-$ésimo de la demostración.

Más aún, para no pararnos a comprobar las condiciones abstractas que han de cumplir cada una de las propiedades de la demostrción, incluiremos junto a los pasos de la demostración un comentario sobre por qué dicho paso es válido.

Con esta notación, la demostración de $\{\alpha, \alpha \to \beta\} \vdash \beta$ quedaría de la forma:

1. α es una hipótesis.
2. $\alpha \to \beta$ es una hipótesis.
3. β por Modus Ponens de 1 y 2.

Finalmente, como conjunto $\mathcal{A}$ de axiomas, consideraremos:

$$\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3$$

Con:

$$\begin{aligned}
\mathcal{A}_1 &= \{\alpha \to (\beta \to \alpha) : \alpha, \beta \text{ son proposiciones}\} \\
\mathcal{A}_2 &= \{(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)) : \alpha, \beta, \gamma \text{ son proposiciones}\} \\
\mathcal{A}_3 &= \{(\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha) : \alpha, \beta \text{ son proposiciones}\}
\end{aligned}$$

Ejemplo. Ejemplos de algunas demostraciones:

- $\{\alpha\} \vdash \beta \to \alpha$
  1. $\alpha \to (\beta \to \alpha) \in \mathcal{A}_1$
  2. α es una hipótesis

3. $\beta \to \alpha$ Modus ponens de 1 y 2.

- $\vdash \alpha \to \alpha$

  1. $(\alpha \to ((\alpha \to \alpha) \to \alpha)) \to ((\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)) \in \mathcal{A}_2$
  2. $\alpha \to ((\alpha \to \alpha) \to \alpha) \in \mathcal{A}_1$
  3. $(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$ Modus ponens de 1 y 2
  4. $\alpha \to (\alpha \to \alpha) \in \mathcal{A}_1$
  5. $\alpha \to \alpha$ Modus ponens de 3 y 4

Teorema 1.4 (de Herbrand o de la deducción)**.** *Sea* $\Gamma \cup \{\alpha, \beta\}$ *un conjunto de proposiciones, equivalen:*

1. $\Gamma \vdash \alpha \to \beta$

2. $\Gamma \cup \{\alpha\} \vdash \beta$

Demostración. Demostramos las dos implicaciones:

1) $\Longrightarrow$ 2) Como $\Gamma \vdash \alpha \to \beta$, podemos construir una demostración de n pasos de la proposición $\alpha \to \beta$ a partir de Γ. En cuyo caso, podemos añadir 2 pasos más a su demostración, de forma que:

1. $\dots$
   $\vdots$

n. $\alpha \to \beta$

$n+1$. α es hipótesis

$n+2$. β por Modus ponens de n y $n+1$

Como en los n primeros pasos solo hemos usado como hipótesis Γ, hemos conseguido demostrar en $n+2$ pasos que $\Gamma \cup \{\alpha\} \vdash \beta$.

2) $\Longrightarrow$ 1) Como $\Gamma \cup \{\alpha\} \vdash \beta$, podemos obtener una demostración β a partir de $\Gamma \cup \{\alpha\}$ de n pasos: $\beta_1, \dots, \beta_n$ (con $\beta_n = \beta$). Por inducción sobre n (el número de pasos de la demostración):

- Si $n = 1$: Como $\Gamma \cup \{\alpha\} \vdash \beta$ gracias a la demostración $\beta_1 = \beta$, distinguimos casos:

  (a) $\beta_1 \in \mathcal{A}$. En dicho caso, podemos considerar la demostración:
     1. $\beta_1 \in \mathcal{A}$
     2. $\beta_1 \to (\alpha \to \beta_1) \in \mathcal{A}_1$
     3. $\alpha \to \beta_1$ por Modus ponens de 1 y 2

     Y con esto tenemos que $\Gamma \vdash \alpha \to \beta$.

  (b) $\beta_1 \in \Gamma$. En dicho caso, podemos considerar una demostración similar al caso anterior:
     1. $\beta_1 \in \Gamma$
     2. $\beta_1 \to (\alpha \to \beta_1) \in \mathcal{A}_1$

3. $\alpha \to \beta_1$ por Modus ponens de 1 y 2

Y con esto también tenemos que $\Gamma \vdash \alpha \to \beta$.

(c) $\beta_1 = \alpha$. En dicho caso, podemos copiar la demostración de $\vdash \beta \to \beta$ del ejemplo anterior, llegando a que $\Gamma \vdash \alpha \to \beta$.

- En el paso de inducción, supuesto que de $\Gamma \cup \{\alpha\} \vdash \beta_m$ podemos deducir que $\Gamma \vdash \alpha \to \beta_m$ para todo $m \leqslant n$, suponemos ahora que $\Gamma \cup \{\alpha\} \vdash \beta_{n+1}$ y queremos ver que $\Gamma \vdash \alpha \to \beta_{n+1}$.

  En dicho caso, supuesto que $\beta_{m+1} \notin \mathcal{A} \cup \Gamma \cup \{\alpha\}$ (ya que si no la demostración es análoga al caso $n = 1$), la única posibilidad es que hayan de existir $i, j < n + 1$ con $\beta_i = \gamma$ y $\beta_j = \gamma \to \beta_{m+1}$.

  Si ahora consideramos los i primeros pasos de la demostración, tenemos que $\Gamma \cup \{\alpha\} \vdash \gamma$ y si consideramos los j primeros pasos, tenemos que $\Gamma \cup \{\alpha\} \vdash \gamma \to \beta_{n+1}$. Por hipótesis de inducción, como $i, j < n + 1$, tenemos que $\Gamma \vdash \alpha \to \gamma$ y que $\Gamma \vdash \alpha \to (\gamma \to \beta_{n+1})$. En este momento, podemos realizar la demostración (con hipótesis Γ):

  1. ...

     $\vdots$

  p. $\alpha \to \gamma$

  $p+1$. ...

     $\vdots$

  q. $\alpha \to (\gamma \to \beta_{n+1})$

  $q+1$. $(\alpha \to (\gamma \to \beta_{n+1})) \to ((\alpha \to \gamma) \to (\alpha \to \beta_{n+1})) \in \mathcal{A}_2$

  $q+2$. $(\alpha \to \gamma) \to (\alpha \to \beta_{n+1})$ por Modus ponens de q y $q+1$.

  $q+3$. $\alpha \to \beta_{n+1}$ por Modus ponens de p y $q+2$.

□

1.2.1. Resultados útiles a la hora de realizar demostraciones

Proposición 1.5 (Regla de reducción al absurdo clásica). *Sea* $\Gamma \cup \{\alpha, \beta\}$ *un conjunto de proposiciones: si* $\Gamma \cup \{\neg\alpha\} \vdash \beta$ *y* $\Gamma \cup \{\neg\alpha\} \vdash \neg\beta$*, entonces* $\Gamma \vdash \alpha$.

Demostración. Supuesto que $\Gamma \cup \{\neg\alpha\} \vdash \beta$ y que $\Gamma \cup \{\neg\alpha\} \vdash \neg\beta$, por el Teorema de Herbrand (1.4), se tiene que $\Gamma \vdash \neg\alpha \to \beta$ y que $\Gamma \vdash \neg\alpha \to \neg\beta$. En dicho caso:

1. ...

   $\vdots$

p. $\neg\alpha \to \neg\beta$

$p+1$. ...

   $\vdots$

q. $\neg\alpha \to \beta$

$q+1$. $(\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha) \in \mathcal{A}_3$

$q+2$. $((\neg\alpha \to \beta) \to \alpha)$ por Modus ponens de $q+1$ y p.

$q+3$. α por Modus ponens de $q+2$ y q.

Como desde el paso 1 hasta el q solo hemos usado como hipótesis Γ, deducimos que $\Gamma \vdash \alpha$. □

Proposición 1.6 (Leyes de silogismo o transitividad de la flecha)**.** *Sean α, β y γ proposiciones, se verifican:*

1. $\vdash (\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))$
2. $\vdash (\beta \to \gamma) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$

Demostración. Demostraremos la primera y dejamos la segunda como ejercicio. Para ello, aplicando el Teorema de Herbrand 3 veces, llegamos a que 1 es equivalente a ver que:

$$\{\alpha \to \beta, \beta \to \gamma, \alpha\} \vdash \gamma$$

Para ello, nos sirve con la demostración:

1. $\alpha \to \beta$ es una hipótesis
2. α es una hipótesis
3. β por Modus ponens de 1 y 2
4. $\beta \to \gamma$ es una hipótesis
5. γ por Modus ponens de 3 y 4

□

Corolario 1.6.1 (Regla del silogismo)**.** *Sea $\Gamma \cup \{\alpha, \beta\}$ un conjunto de proposiciones, si $\Gamma \vdash \alpha \to \beta$ y $\Gamma \vdash \beta \to \gamma$, entonces $\Gamma \vdash \alpha \to \gamma$.*

Proposición 1.7 (Ley de conmutación de premisas)**.** *Sean α, β y γ proposiciones:*

$$\vdash (\alpha \to (\beta \to \gamma)) \to (\beta \to (\alpha \to \gamma))$$

Demostración. Aplicando el Teorema de Herbrand 3 veces, es equivalente a ver que:

$$\{\alpha \to (\beta \to \gamma), \beta, \alpha\} \vdash \gamma$$

Para ello, nos sirve con:

1. $\alpha \to (\beta \to \gamma)$ es una hipótesis
2. α es una hipótesis
3. $\beta \to \gamma$ por Modus ponens de 1 y 2
4. β es una hipótesis
5. γ por Modus ponens de 3 y 4

□

Corolario 1.7.1 (Regla de conmutación de premisas). *Sea* $\Gamma \cup \{\alpha, \beta, \gamma\}$ *un conjunto de proposiciones, si* $\Gamma \vdash \alpha \to (\beta \to \gamma)$*, entonces* $\Gamma \vdash \beta \to (\alpha \to \gamma)$*.*

Proposición 1.8 (Ley de la doble negación). *Sea* α *una proposición:*

$$\vdash \neg\neg\alpha \to \alpha$$

Demostración. Por el Teorema de Herbrand, es equivalente a ver que $\{\neg\neg\alpha\} \vdash \alpha$. Para ello, usamos la regla de la reducción al absurdo clásica, ya que:

1. $\{\neg\neg\alpha, \neg\alpha\} \vdash \neg\neg\alpha$
2. $\{\neg\neg\alpha, \neg\alpha\} \vdash \neg\alpha$

Luego concluimos que $\{\neg\neg\alpha\} \vdash \alpha$. □

Proposición 1.9 (Ley débil de la doble negación). *Sea* α *una proposición:*

$$\vdash \alpha \to \neg\neg\alpha$$

Demostración. Por el Teorema de Herbrand, es equivalente a ver que $\{\alpha\} \vdash \neg\neg\alpha$. Para ello, usamos la regla de la reducción al absurdo clásica, con lo que partimos que $\{\alpha, \neg\neg\neg\alpha\}$ y tenemos que demostrar una proposición y su negación. Para ello:

1. $\neg\neg\neg\alpha \to \neg\alpha$ por la ley de la doble negación
2. $\neg\neg\neg\alpha$ es una hipótesis
3. $\neg\alpha$ por Modus ponens de 1 y 2
4. α es una hipótesis

Concluimos por la regla de la reducción al absurdo que $\{\alpha\} \vdash \neg\neg\alpha$. □

1.3. Teoremas de coherencia y adecuación

A lo largo de este capítulo hemos manejado en los lenguajes proposicionales dos conceptos fundamentales: las tautologías ($\vDash \alpha$), relacionadas con las interpretaciones; y los teorema ($\vdash \alpha$), relacionados con las demostraciones. Las primeras tienen un gran interés en informática y ciencias de la computación, gracias a las consecuencias semánticas que podemos realizar de forma autómatica, tal y como vimos con el Algoritmo de Davis & Putnam. Por otra parte, las segundas tienen un gran interés matemático, por ser la principal herramienta que sustentan todo el conocimiento matemático. Veremos ahora dos teoremas que nos permiten relacionar las tautologías con los teoremas, de gran importancia en los lenguajes de primer orden.

Teorema 1.10 (de coherencia). *Sea* α *una proposición, si* $\vdash \alpha$*, entonces* $\vDash \alpha$*. Es decir, todo teorema es una tautología.*

Demostración. Si α es un teorema, por definición este tendrá una demostración de n pasos $\alpha_1, \ldots, \alpha_n$:

- α_1 será un axioma y anteriormente probamos que todo axioma era una tautología.
- A α_2 le ocurrirá lo mismo.
- α_i para $i \geqslant 3$ podrá ser un axioma, en cuyo caso ya sabemos cómo proceder o resultado de aplicar modus ponens sobre dos pasos anteriores. Sin embargo, anteriormente vimos que si a y $a \to b$ eran tautologías, entonces b era una tautología, por lo que α_i será una tautología.

Finalmente, llegaremos a $\alpha_n = \alpha$, con lo que podemos concluir que α es una tautología. $\square$

Y además la otra implicación también es cierta, aunque su demostración excede los objetivos del curso.

Teorema 1.11 (de adecuación)**.** *Sea α una proposición, si $\models \alpha$, entonces $\vdash \alpha$. Es decir, toda tautología es un teorema.*

2. Lógica de Primer Orden

Es necesario introducir ahora lenguajes en los que podamos cuantificar cosas. Como primer ejemplo, si sabemos que "Todo hombre es mortal" y que "Sócrates es un hombre", nos gustaría deducir que, entonces, "Sócrates es mortal". Sin embargo, para esto hemos de poder cuantificar, cosa que no es posible con los lenguajes proposicionales pero sí con los lenguajes de primer orden.

Los lenguajes de primer orden estarán formados por:

- Constantes: $c_1, c_2, \dots, a, b, c, \dots$
- Variables: $x_1, x_2, \dots, x, y, z, \dots$
- Símbolos de función: $f_1, f_2, \dots, f, g, h, \dots$
- Símbolos de relación: $R_1, R_2, \dots, R, S, T, \dots$
- Conectivas lógicas: $\vee$, $\wedge$, $\neg$, $\rightarrow$, $\leftrightarrow$
- Cuantificadores: $\forall$, $\exists$

A los conjuntos de todas las constantes, de todas la variables y de todos los símbolos de función los notaremos por $Cons(\mathcal{L}), Var(\mathcal{L}), Fun(\mathcal{L})$, si $\mathcal{L}$ es nuestro lenguaje de primer orden.

Notación. En otros libros o contextos, en vez de denotar a los símbolos de función o variables con una letra que pueda llevar o no superíndice, estos las denotan con un superíndice:

- $f_1^{n_1}, f_2^{n_2}, \dots$
- $R_1^{m_1}, R_2^{m_2}, \dots$

En este caso, el superíndice indica la ariedad de la función o relación. Por ejemplo, si consideramos f^3, tenemos un símbolo de función que se aplica a 3 variables.

Definición 2.1 (Término)**.** Un término es:

1. Cualquier constante.
2. Cualquier variable.
3. Si $t_1, t_2, \dots, t_n$ son términos y f es un símbolo de función $n-$ario, entonces $f(t_1, t_2, \dots, t_n)$ es un término.

4. No hay más términos que los que se puedan obtener siguiendo una secuencia finita de pasos a partir de las enunciadas.

Al conjunto de todos los términos de nuestro lenguaje $\mathcal{L}$ lo denotamos por $Term(\mathcal{L})$.

Ejemplo.

- $f(x, f(x, y))$ es un término.
- $f(x, f(x))$ no es un término, ya que usamos un mismo símbolo de función, f, para denotar dos objetos: una función unaria y una función binaria.

Definición 2.2 (Fórmulas atómicas)**.** Si $t_1, \ldots, t_n$ son términos y R es un símbolo de relación $n-$ario, entonces $R(t_1, \ldots, t_n)$ es una fórmula atómica (o simplemente, un átomo).

Definición 2.3 (Fórmulas)**.** Son fórmulas:

1. Las fórmulas atómicas.
2. Si φ y ψ son fórmulas, también lo son:
$$\neg\varphi,\ \varphi \wedge \psi,\ \varphi \vee \psi,\ \varphi \to \psi,\ \varphi \leftrightarrow \psi$$
3. Si x es una variable y φ es una fórmula, también lo son: $\forall x\varphi$, $\exists x\varphi$.
4. No hay más fórmulas que las que se puedan obtener siguiendo una secuencia finita de pasos a partir de las enunciadas.

Al conjunto de todas las fórmulas de nuestro lenguaje $\mathcal{L}$ lo denotamos por $Form(\mathcal{L})$.

Definición 2.4. Una ocurrencia de una variable en una fórmula es una aparición de su escritura.

- En la fórmula $\forall x\varphi$, diremos que φ es el radio de acción de $\forall x$.
- En la fórmula $\exists x\varphi$, diremos que φ es el radio de acción de $\exists x$.

Diremos que x se encuentra cuantificada al ver $\forall x$ o $\exists x$.
Diremos que una ocurrencia de una variable x es ligada si aparece cuantificada o en el radio de acción de $\forall x$ o de $\exists x$.
Finalmente, diremos que una variable es libre si no aparece ligada. Si φ es una fórmula en la que las variables $x_1, \ldots, x_n$ aparecen libres, será usual denotar:
$$\varphi(x_1, \ldots, x_n)$$
Que no debe confundirse con un término de una función o relación $n-$aria, ya que φ no es ni un símbolo de función o relación, sino una fórmula.

Ejemplo. En la siguiente fórmula:
$$\forall x(\exists y R(x, y) \to Q(y))$$

- x aparece cuantificada en su primera ocurrencia.

- y aparece cuantificada en su primera ocurrencia.
- x aparece ligada en su segunda ocurrencia.
- y aparece ligada en su segunda ocurrencia.
- y aparece como variable libre en su tercera ocurrencia.

Definición 2.5 (Sentencia)**.** Una sentencia es una fórmula sin ocurrencias de variables libres.

2.1. Semántica

Trataremos de generalizar el concepto de "interpretación", ya visto para lenguajes proposicionales. Para ello, será necesario primero definir los conceptos de "estructura" y de "asignación".

Definición 2.6 (Estructura)**.** Una estructura ε en un lenguaje $\mathcal{L}$ es una cuádrupla

$$\varepsilon = (D, \{c_i^\varepsilon\}_{n\in\mathbb{N}}, \{f_i^\varepsilon\}_{n\in\mathbb{N}}, \{R_i^\varepsilon\}_{n\in\mathbb{N}})$$

de forma que:

- D es un conjunto no vacío al que llamamos <u>universo</u> o <u>dominio</u>.
- A cada constante c_i de $\mathcal{L}$ le corresponde un elemento c_i^ε de D.
- A cada símbolo de función f_i de $\mathcal{L}$ le corresponde una función $f_i^\varepsilon : D^n \to D$.
- A cada símbolo de relación R_i de $\mathcal{L}$ le corresponde una aplicación $R_i^\varepsilon : D^m \to \mathbb{Z}_2$, de forma que $R_i^\varepsilon(c_1^\varepsilon, c_2^\varepsilon) = 1$ si c_1^ε y c_2^ε están relacionados y 0 en caso contrario.

Definición 2.7 (Asignación)**.** Una asignación v en ε es una aplicación $v : Var(\mathcal{L}) \to D$. Dada una asignación v, podremos extenderla a $v' : Term(\mathcal{L}) \to D$ de la forma:

$$v'(t) = \begin{cases} c^\varepsilon & \text{si } t = c \text{ una constante} \\ v(x) & \text{si } t = x \text{ una variable} \\ f^\varepsilon(v'(t_1), \dots, v'(t_n)) & \text{si } t = f(t_1, \dots, t_n) \end{cases}$$

Definición 2.8 (Interpretación)**.** Una interpretación es una tupla (ε, v) con ε una estructura y v una asignación que tiene asociada una aplicación[1] $I_\varepsilon^v : Form(\mathcal{L}) \to \mathbb{Z}_2$ que cumple para cualesquiera fórmulas φ y ψ:

1. $I^v(\neg\varphi) = 1 + I^v(\varphi)$.
2. $I^v(\varphi \wedge \psi) = I^v(\varphi)I^v(\psi)$.
3. $I^v(\varphi \vee \psi) = I^v(\varphi) + I^v(\psi) + I^v(\varphi)I^v(\psi)$.
4. $I^v(\varphi \to \psi) = 1 + I^v(\varphi) + I^v(\varphi)I^v(\psi)$.

[1] A la que próximamente denotaremos simplemente como I^v, por simplicidad, entendiendo que la estructura ε viene dada por el contexto.

5. $I^v(\varphi \leftrightarrow \psi) = 1 + I^v(\varphi) + I^v(\psi)$.
6. $I^v(R(t_1, \ldots, t_n)) = R^\varepsilon(v(t_1), \ldots, v(t_n))$
   Con R un símbolo de relación $n-$ario y $t_1, \ldots, t_n$ términos.
7. $I^v(\forall x\varphi) = \begin{cases} 1 & \text{si para todo } a \in D,\ I^{v(x|a)}(\varphi) = 1 \\ 0 & \text{en caso contrario} \end{cases}$
8. $I^v(\exists x\varphi) = \begin{cases} 1 & \text{si existe } a \in D \text{ con } I^{v(x|a)}(\varphi) = 1 \\ 0 & \text{en caso contrario} \end{cases}$

Siendo:

$$v(x \mid a)(y) = \begin{cases} v(y) & \text{si } y \neq x \\ a & \text{si } y = x \end{cases}$$

Definición 2.9. Sea $\varphi \in Form(\mathcal{L})$:

- Dada una estructura ε, diremos que φ es válida en ε si $I^v(\varphi) = 1$ para toda asignación v en ε.
- Dada una estructura ε, diremos que φ es satisfacible en ε si $I^v(\varphi) = 1$ para alguna asignación v en ε.
- Diremos que φ es universalmente válida si φ es válida en cualquier estructura.
- Diremos que φ es satisfacible si existe una estructura ε donde φ es satisfacible.
- Diremos que φ es refutable si $\neg\varphi$ es satisfacible.
- Diremos que φ es una contradicción si $\neg\varphi$ es universalmente válida.

Lema 2.1 (de Coincidencia)**.** *Sea $\varphi \in Form(\mathcal{L})$ de forma que $x_1, \ldots, x_n \in Var(\mathcal{L})$ son las variables con ocurrencias libres en φ y sea ε una estructura. Entonces, dada una asignación v en ε:*

$$I^v(\varphi) = I^w(\varphi)$$

para toda asignación w en ε tal que $w(x_i) = v(x_i)$ para todo $i \in \{1, \ldots, n\}$.

Observación. En particular, si φ es una sentencia, entonces $I^v(\varphi)$ no depende de la asignación v. Por tanto, si φ es satisfacible en ε, entonces φ es válida en ε.

Definición 2.10 (Consecuencia lógica)**.** Sea $\Gamma \cup \{\varphi\} \subseteq Form(\mathcal{L})$, diremos que φ es consecuencia lógica de Γ, notado por $\Gamma \vDash \varphi$, si para toda interpretación (ε, v) tal que $I^v(\gamma) = 1$ para toda $\gamma \in \Gamma$, fuerza a que $I^v(\varphi) = 1$.

Teorema 2.2 (de la Deducción)**.** *Sea $\Gamma \cup \{\varphi, \psi\} \subseteq Form(\mathcal{L})$, son equivalentes:*

1. $\Gamma \vDash \varphi \to \psi$.
2. $\Gamma \cup \{\varphi\} \vDash \psi$.

Definición 2.11 (Inconsistencia)**.** Sea $\Gamma \subseteq Form(\mathcal{L})$, diremos que Γ es inconsistente si no existe una interpretación (ε, v) tal que $I^v(\gamma) = 1$ para toda $\gamma \in \Gamma$.

Teorema 2.3. *Sea $\Gamma \cup \{\varphi\} \subseteq Form(\mathcal{L})$, son equivalentes:*

1. $\Gamma \models \varphi$.

2. $\Gamma \cup \{\neg\varphi\}$ *es inconsistente.*

Ejemplo. Demostremos las siguientes fórmulas universalmente válidas:

1. $\models \forall x\varphi(x) \leftrightarrow \forall y\varphi(y)$ con[2] y libre para x en $\varphi(x)$.

   Dada cualquier interpretación (ε, v), queremos ver que:

   $$I^v(\forall x\varphi(x) \leftrightarrow \forall y\varphi(y)) = 1$$

   Y sabemos que eso es equivalente a ver que:

   $$I^v(\forall x\varphi(x)) = I^v(\forall y\varphi(y))$$

   Que se puede ver a partir de su definición:

   $$\begin{aligned} I^v(\forall x\varphi(x)) &= \begin{cases} 1 & \text{si } I^{v(x|a)}(\varphi(x)) = 1 \text{ para todo } a \in D \\ 0 & \text{en caso contrario} \end{cases} \\ &\overset{(*)}{=} \begin{cases} 1 & \text{si } I^{v(y|a)}(\varphi(y)) = 1 \text{ para todo } a \in D \\ 0 & \text{en caso contrario} \end{cases} \\ &= I^v(\forall y\varphi(y)) \end{aligned}$$

   Donde en $(*)$ debemos tener cuidado y usar que y es libre para x en $\varphi(x)$, ya que x aparecía libre en φ y como y es libre para x en $\varphi(x)$, al hacer la sustitución de x por y no estaremos cambiando variables libres en φ, por lo que a partir del Lema de Coincidencia (Lema 2.1), al no cambiar variables libres en φ, no cambiamos su condición de verdad.

2. $\models \forall x\varphi(x) \to \varphi(t)$ con t libre para x en $\varphi(x)$.

   Por el Teorema de la Deducción, probar esto es equivalente a ver que:

   $$\{\forall x\varphi(x)\} \models \varphi(t)$$

   Por tanto, sea (ε, v) una interpretación de forma que $I^v(\forall x\varphi(x)) = 1$, entonces para todo $a \in D$, se tendrá $I^{v(x|a)}(\varphi(x)) = 1$. Si tomamos $a = v(t)$, entonces tendremos que:

   $$I^{v(x|a)}(\varphi(x)) = I^v(\varphi(t))$$

2.2. Demostraciones

Trataremos ahora de generalizar lo que hicimos ya para la demostraciones en el caso de los lenguajes proposicionales, para que cualquier demostración hecha con lenguajes proposicionales siga siendo válida ahora.

2.2.1. Definición de una demostración

En lugar de dar directamente la definición de demostración, daremos primero los axiomas de nuestro sistema y las reglas de inferencia que usaremos, para posteriormente dar la definición de demostración.

[2]Estamos usando una notación que se introduce en la siguiente sección.

Axiomas

Sobre nuestro lenguaje $\mathcal{L}$ consideraremos los 3 primeros conjuntos de axiomas, que son los que ya teníamos en lenguajes proposicionales:

$$\mathcal{A}_1 = \{\varphi \to (\psi \to \varphi) : \varphi, \psi \in Form(\mathcal{L})\}$$
$$\mathcal{A}_2 = \{(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)) : \varphi, \psi, \chi \in Form(\mathcal{L})\}$$
$$\mathcal{A}_3 = \{(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi) : \varphi, \psi \in Form(\mathcal{L})\}$$

Ahora, será necesario considerar nuevos axiomas que nos permitan generalizar lo ya visto para lenguajes proposicionales a lenguajes de primer orden. Como el lector puede deducir, estos axiomas tendrán que contener cuantificadores, ya que es el concepto principal que introducimos en los lenguajes de primer orden. Antes de dar el cuarto axioma[3], introduciremos la siguiente notación:

Notación. Sea $\varphi \in Form(\mathcal{L})$ y $x_1, \ldots, x_n \in Var(\mathcal{L})$, al notar:

$$\varphi(x_1, \ldots, x_n)$$

Estamos diciendo que, si $x_1, \ldots, x_n$ son variables que aparecen en φ, entonces tienen todas sus ocurrencias libres en φ.

Notación. Sea $\varphi \in Form(\mathcal{L})$, $x \in Var(\mathcal{L})$ y $t \in Term(\mathcal{L})$, cuando aparezca:

"t libre para x en $\varphi(x)$"

Y notemos $\varphi(t)$, significará que estamos cambiando las ocurrencias libres de x que había en φ por t. Por ser t un término, este puede depender de otras variables, por lo que en este proceso no se permite que variables de t se queden ligadas, sino que deben aparecer libres.

Podemos dar ya el cuarto axioma:

$$\mathcal{A}_4 = \{\forall x\varphi(x) \to \varphi(t) \mid \varphi \in Form(\mathcal{L}), x \in Var(\mathcal{L}), t \text{ libre para } x \text{ en } \varphi(x)\}$$

Observemos que casos particulares interesantes de este axioma son:

- $\forall x\varphi \to \varphi$
- $\forall x\varphi(x) \to \varphi(x)$

Y podemos finalmente dar el quinto axioma[4]:

$$\mathcal{A}_5 = \{\forall x(\varphi \to \psi) \to (\varphi \to \forall x\psi) \mid \varphi, \psi \in Form(\mathcal{L}), x \text{ no aparece libre en } \varphi\}$$

De esta forma, nuestro conjunto de axiomas vendrá dado por:

$$\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3 \cup \mathcal{A}_4 \cup \mathcal{A}_5$$

Notemos que en estos 5 axiomas no aparecen los conectores $\wedge$, $\vee$, $\leftrightarrow$ ni el cuantificador $\exists$. En caso de querer usarlos:

- Los conectores los expresaremos como fórmulas semánticamente equivalentes pero usando $\neg$ y $\to$.
- Usaremos que $\exists x\varphi$ es semánticamente equivalente a $\neg\forall x\neg\varphi$, siendo $\varphi \in Form(\mathcal{L})$.

[3] Algunos autores dividen este axioma en dos, ya que no consideran la notación que vamos a considerar para poder dar este axioma.

[4] Que en aquellos autores que dividen el cuarto axioma en dos, aparece como el sexto.

Reglas de inferencia

Las reglas de inferencia que consideraremos en nuestro sistema serán las siguientes, las cuales tendremos en cuenta a la hora de realizar la definición de lo que será una demostración:

$$\begin{array}{lcl} \text{Modus ponens} & & \text{Generalización} \\ \varphi \to \psi & & \varphi \\ \underline{\varphi \qquad\qquad\qquad} & & \underline{\qquad\qquad\qquad\quad} \\ \psi & & \forall x \varphi \end{array}$$

Definición 2.12 (Demostración)**.** Si consideramos el conjunto de fórmulas $\mathcal{A}$ previamente definido y sea $\Gamma \cup \{\varphi\} \subseteq Form(\mathcal{L})$, una demostración de p a partir de Γ (notado por $\Gamma \vdash p$) es una secuencia de fórmulas $\alpha_1, \alpha_2, \ldots, \alpha_n$ de forma que $\alpha_n = p$ y se verifica para todo i menor o igual que n alguna de las tres condiciones siguientes:

- $\alpha_i \in \mathcal{A} \cup \Gamma$.
- Existen j, k naturales con $j < k < i$ siendo $\alpha_k = \alpha_j \to \alpha_i$ (Modus ponens).
- Existe un natural j con $j < i$ siendo $\alpha_i = \forall x \alpha_j$ (Generalización).

2.2.2. Primeros resultados

Como primer resultado a destacar, como los lenguajes de primer orden generalizan los lenguajes proposicionales, cualquier demostración para los lenguajes proposicionales seguirán siendo válidas para los lenguajes de primer orden.

Teorema 2.4 (de la Deducción)**.** *Sean $\Gamma \cup \{\varphi, \psi\} \subseteq Form(\mathcal{L})$. Si tenemos que $\Gamma \cup \{\varphi\} \vdash \psi$ y en su demostración no usamos la regla de generalización sobre un paso en que haya intervenido φ con una variable libre en φ, entonces:*

$$\Gamma \vdash \varphi \to \psi$$

Observación. Ha sido necesario introducir la condición extra que no teníamos en lenguajes proposicionales ya que vamos a poder demostrar, por ejemplo, $\{A(x)\} \vdash \forall x A(x)$:

1. $A(x)$ es hipótesis.
2. $\forall x A(x)$ por generalización

Sin embargo, $\nvdash A(x) \to \forall x A(x)$, ya si que si consideramos por ejemplo el dominio $D = \mathbb{Z}_2$ y A es "ser igual a 0", de $A(0)$ no podemos concluir que todo elemento de $\mathbb{Z}_2$ sea 0. Esto se debe a que semánticamente:

$$\{A(x)\} \nvDash \forall x A(x)$$

El lector podría sospechar que la regla de generalización carece de sentido o contradice lo enunciado, pero si somos capaces de demostrar algo para un elemento x arbitrario en un cierto conjunto, entonces seremos capaces de afirmar que $\forall x$ en dicho conjunto, tendremos la proposición conseguida para el elemento arbitrario anterior. Esta es la intuición detrás de la regla de generalización.

Proposición 2.5. *Sean* $\Gamma \cup \{\varphi, \psi\} \subseteq Form(\mathcal{L})$*, si tenemos que* $\Gamma \vdash \varphi \to \psi$*, entonces* $\Gamma \cup \{\varphi\} \vdash \psi$*.*

Teorema 2.6 (Regla de reducción al Absurdo)**.** *Sean* $\Gamma \cup \{\varphi, \psi\} \subseteq Form(\mathcal{L})$ *si tenemos que* $\Gamma \cup \{\neg\varphi\} \vdash \psi$ *y* $\Gamma \cup \{\neg\varphi\} \vdash \neg\psi$ *y en esas demostraciones no usamos la regla de generalización sobre un pasa en el que haya intervenido* $\neg\varphi$ *con una variable libre en* $\neg\varphi$*, entonces:*

$$\Gamma \vdash \varphi$$

Ejemplo. Buscamos demostrar $\vdash (\varphi \to \forall x\psi) \to \forall x(\varphi \to \psi)$ con x no libre en φ.

Buscamos demostrar con precaución[5] que:

$$\{\varphi \to \forall x\psi\} \vdash \forall x(\varphi \to \psi)$$

Para ello:

1. $\varphi \to \forall x\psi$ es una hipótesis.
2. $\forall x\psi \to \psi \in \mathcal{A}_4$
3. $\varphi \to \psi$ por silogismo de 1 y 2.
4. $\forall x(\varphi \to \psi)$ generalización de 3.

Como x no está libre en φ, tampoco lo estará en $\varphi \to \forall x\psi$, por lo que en esta demostración no hemos usado la regla de generalización sobre un paso en el que haya intervenido $\varphi \to \forall x\psi$ con una variable libre en la misma, por lo que podremos aplicar el Teorema de la Deducción, obteniendo lo que queríamos probar.

2.3. Teoremas de adecuación y coherencia

Una parte positiva de los lenguajes de primer orden es que a pesar de ser más generales que los proposicionales, seguimos contando con los teoremas de adecuación y de coherencia:

Teorema 2.7 (de coherencia)**.** *Sea* $\varphi \in Form(\mathcal{L})$*, si* $\vdash \varphi$*, entonces* $\models \varphi$*.*

Demostración. La demostración es similar a la del Teorema de coherencia para lenguajes proposicionales, pero ahora hemos de tener en cuenta más axiomas, así como la regla de generalización. □

Teorema 2.8 (de consistencia)**.** *Nuestro conjunto de axiomas* $\mathcal{A}$ *junto con las reglas de inferencia es consistente, es decir, no existe* $\varphi \in Form(\mathcal{L})$ *de forma que* $\vdash \varphi$ *y* $\nvdash \varphi$*.*

Teorema 2.9 (de adecuación)**.** *Sea* $\varphi \in Form(\mathcal{L})$*, si* $\models \varphi$*, entonces* $\vdash \varphi$*.*

[5] Para poder aplicar luego el Teorema de la Deducción bajo las hipótesis correctas con la limitación extra.

2.4. Sistemas matemáticos

2.4.1. Lenguajes de Primer Orden con Igualdad

Un lenguaje de primer orden con igualdad es un lenguaje de primer orden $\mathcal{L}$ en el que habrá un símbolo de relación destacado A.

Notación. Aceptaremos las siguientes notaciones con el fin de abreviar los enunciados:

1. Si $s, t \in Term(\mathcal{L})$, usaremos con frecuencia:

$$s = t$$

   Para denotar $A(s, t)$.

2. En el caso de tener $\neg(s = t)$, podremos notar: $s \neq t$.

3. Usaremos $\exists_1 x\varphi(x)$ como abreviatura de:

$$\exists x\varphi(x) \land \forall y(\varphi(y) \to x = y)$$

La única diferencia con los lenguajes de primer orden corrientes será que tendremos dos conjuntos de axiomas extras:

$$\mathcal{A}_6 = \{\forall x(x = x) \mid x \in Var(\mathcal{L})\}$$

Y para introducir el último axioma, hace falta introducir más notación:

Notación. Sea $\varphi \in Form(\mathcal{L})$, y $x, y \in Var(\mathcal{L})$, si notamos $\varphi(x, y)$ tras notar $\varphi(x, x)$, significará que estamos reemplazando algunas ocurrencias libres de x por y en la fórmula φ.

El último axioma será:

$$\mathcal{A}_7 = \{(x = y) \to (\varphi(x, x) \to \varphi(x, y)) \mid x, y \in Var(\mathcal{L})\}$$

Observación. Notemos que con dos conjuntos de axiomas que hemos añadido, tenemos que "=" es una relación de equivalencia:

- $\mathcal{A}_6$ nos da la relación reflexiva.
- De $\mathcal{A}_7$ deducimos la simétrica y la transitiva.

Sin embargo, "=" es mucho más que eso, ya que de $\mathcal{A}_7$ no solo deducimos esas propiedades, sino muchas más, tal y como vemos en el siguiente ejemplo.

Ejemplo. Demostraremos que:

$$\vdash (x = y) \to (f(t_1, \ldots, x, \ldots, t_n) = f(t_1, \ldots, y, \ldots, t_n))$$

Para ello, bastará demostrar con cuidado que:

$$\{x = y\} \vdash f(t_1, \ldots, x, \ldots, t_n) = f(t_1, \ldots, y, \ldots, t_n)$$

1. $\forall x(x = x) \in \mathcal{A}_6$
2. $\forall x(x = x) \to f(t_1, \dots, x, \dots, t_n) = f(t_1, \dots, x, \dots, t_n) \in \mathcal{A}_4$
3. $f(t_1, \dots, x, \dots, t_n) = f(t_1, \dots, x, \dots, t_n)$ por modus ponens de 1 y 2.
4. $(x = y) \to ((f(t_1, \dots, x, \dots, t_n) = f(t_1, \dots, x, \dots, t_n)) \to$
   $\to (f(t_1, \dots, x, \dots, t_n) = f(t_1, \dots, y, \dots, t_n))) \in \mathcal{A}_7$
5. $x = y$ es hipótesis.
6. $(f(t_1, \dots, x, \dots, t_n) = f(t_1, \dots, x, \dots, t_n)) \to (f(t_1, \dots, x, \dots, t_n) = f(t_1, \dots, y, \dots, t_n))$
   por modus ponens de 4 y 5.
7. $f(t_1, \dots, x, \dots, t_n) = f(t_1, \dots, y, \dots, t_n)$ por modus ponens de 3 y 6.

Como no hemos usado ningún paso de generalización, podemos aplicar el Teorema de la Deducción, obteniendo lo que queríamos probar.

2.4.2. Aritmética de Primer Orden

En aritmética de primer orden, consideraremos un lenguaje de primer orden $\mathcal{L}$, que tendrá:

- Variables.
- Una sola constante, que denotaremos por 0.
- Tres símbolos de función, que denotaremos por[6] s, $+$ y $\cdot$.
- Un símbolo de relación que denotaremos por $=$.

En aritméticas de primer orden, consideraremos como axiomas $\mathcal{A}_1, \dots, \mathcal{A}_7$, junto con los siguientes:

$$\begin{aligned}
\mathcal{N}_1 &= \{\forall x(s(x) \neq 0) : x \in Var(\mathcal{L})\}\\
\mathcal{N}_2 &= \{\forall x \forall y(s(x) = s(y) \to x = y) : x, y \in Var(\mathcal{L})\}\\
\mathcal{N}_3 &= \{\forall x(x + 0 = x) : x \in Var(\mathcal{L})\}\\
\mathcal{N}_4 &= \{\forall x \forall y(x + s(y) = s(x + y)) : x, y \in Var(\mathcal{L})\}\\
\mathcal{N}_5 &= \{\forall x(x \cdot 0 = 0) : x \in Var(\mathcal{L})\}\\
\mathcal{N}_6 &= \{\forall x \forall y(x \cdot s(y) = x \cdot y + x) : x, y \in Var(\mathcal{L})\}\\
\mathcal{N}_7 &= \{\varphi(0) \to (\forall x(\varphi(x) \to \varphi(s(x))) \to \forall x \varphi(x)) : \varphi(x) \in Form(\mathcal{L})\}
\end{aligned}$$

La aritmética de primer orden funcionará bien cuando pensemos que estamos en un dominio similar a $\mathbb{N}$. Pensando esto, los axiomas $\mathcal{N}_i$ conviene entenderlos como:

1. $\mathcal{N}_1$ y $\mathcal{N}_2$ definen cómo funciona la función s, que podemos entender por "siguiente".

[6] Y entenderemos que $\cdot$ tiene mayor prioridad de $+$.

2. $\mathcal{N}_3$ y $\mathcal{N}_4$ definen de forma inductiva la operación $+$.

3. $\mathcal{N}_5$ y $\mathcal{N}_6$ definen de forma inductiva la operación $\cdot$.

4. $\mathcal{N}_7$ es una versión más débil del principio de inducción.

Decimos que $\mathcal{N}_7$ es una versión más débil del principio de inducción porque el principio de inducción (en matemáticas) es el siguiente:

Proposición 2.10. *Sea $A \subseteq \mathbb{N}$, si $0 \in A$ y siempre que $n \in A \Longrightarrow n+1 \in A$, entonces $A = \mathbb{N}$.*

Donde hacemos una afirmación sobre cualquier subconjunto de $\mathbb{N}$, por lo que estamos considerando elementos dentro de un conjunto no numerable de elementos (el conjunto de todos los subconjuntos de $\mathbb{N}$, que no es numerable). Esta idea no se puede expresar en lenguajes de primer orden, por tener solo un conjunto numerable de fórmulas.

2.4.3. Teoría de conjuntos (de Zermelo-Fraenkel)

La teoría de conjuntos es un lenguaje de primer orden donde:

- No tenemos constantes ni símbolos de función, por lo que los únicos términos que podremos considerar son las variables.
- Como relaciones solo tendremos dos, que denotaremos por $\in$ y $=$ (y usaremos $\notin$ y $\neq$ como sus respectivas negaciones).

Notación. Dados $t, s \in Term(\mathcal{L})$, usaremos $t \subseteq s$ como abreviatura de:

$$\forall x(x \in t \to x \in s)$$

En este contexto, consideraremos como axiomas $\mathcal{A}_1, \ldots, \mathcal{A}_7$, junto con los siguientes (entendiendo que todo lo que sale son variables):

$$\begin{aligned}
ZF_1 &= \{x = y \leftrightarrow \forall z(z \in x \leftrightarrow z \in y)\} \\
ZF_2 &= \{\exists x \forall y(y \notin x)\} \\
ZF_3 &= \{\forall x \forall y \exists z \forall u(u \in z \leftrightarrow (u = x \vee u = y))\} \\
ZF_4 &= \{\forall x \exists y \forall z(z \in y \leftrightarrow \exists u(u \in x \wedge z \in u))\} \\
ZF_5 &= \{\forall x \exists y \forall z(z \in y \leftrightarrow z \subseteq x)\} \\
ZF_6 &= \{\forall x_1 \exists_1 x_2 \varphi(x_1, x_2) \to \forall x_3 \exists x_4 \forall x_5(x_5 \in x_4 \leftrightarrow \exists x_6(x_6 \in x_3 \wedge \varphi(x_6, x_5)))\} \\
ZF_7 &= \{\exists x(\emptyset \in x \wedge \forall y(y \in x \to y \cup \{y\} \in x))\} \\
ZF_8 &= \{\forall x(x \neq \emptyset \to \exists y(y \in x \wedge \neg \exists z(z \in x \wedge z \in y)))\}
\end{aligned}$$

Las variables recibirán usualmente el nombre de "conjuntos" o "elementos" y una forma de entender mejor estos axiomas es la siguiente:

1. ZF_1 recibe el nombre de "extensionalidad" y puede entenderse como una condición de cuándo dos conjuntos son iguales.

2. ZF_2 afirma la existencia de un conjunto sin elementos.

   A partir de ZF_1 y ZF_2 puede demostrarse que aquel conjunto sin elementos es único. Por tanto, a partir de ahora nos referiremos a este único conjunto por $\emptyset$, y le llamaremos "conjunto vacío". De esta forma, ZF_2 recibe el nombre de "existencia del conjunto vacío".

3. ZF_3 recibe el nombre de "emparejamiento", y afirma que dados dos conjuntos x e y, podemos considerar z, el conjunto formado por estos dos elementos: $\{x, y\}$. En el caso $\{x, x\}$, notaremos simplemente $\{x\}$.

4. ZF_4 nos dice que siempre que tengamos un conjunto x, existirá un conjunto y que contendrá todos aquellos elementos que están en algún conjunto de x. De esta forma, podemos pensar en ZF_4 como en la existencia de las uniones arbitrarias de conjuntos. Si consideramos la unión de un conjunto x, podremos denotarlo por:

   $$\bigcup x$$

   Y cuando tengamos dos conjuntos t y s, podremos denotar:

   $$t \cup s = \bigcup \{t, s\}$$

5. ZF_5 recibe el nombre de "conjunto potencia" y afirma que dado un conjunto x, existe un conjunto y que contiene todos aquellos conjuntos que sean subconjuntos de x. Este conjunto y recibirá usualmente el nombre de $\mathcal{P}(x)$.

6. ZF_6 recibe el nombre de "esquema de reemplazo" y nos permite definir funciones mediante la regla $\varphi(x_1, x_2)$: dado cualquier x_1, existirá un único x_2 de forma que se tenga $\varphi(x_1, x_2)$. En cuyo caso, podremos considerar el conjunto imagen de un conjunto por dicha aplicación:

   Si pensamos en x_3 como un subconjunto del dominio de la aplicación, entonces existirá un x_4 (imagen de x_3 por la aplicación), y este verificará que un elemento está en él si y solo si hay un elemento de x_3 que se aplicaba en él.

7. ZF_7 recibe el nombre de "axioma del infinito", y es que afirma la existencia de un conjunto x que contiene a $\emptyset$ y es infinito.

8. ZF_8 recibe el nombre de "axioma de regularidad", y viene a decir que dada conjunto no vacío x contiene un elemento y que es disjunto con el propio x (es decir, que cualquier conjunto no vacío contiene un elemento que no comparte ningún elemento con el propio conjunto no vacío de partida).

   Este axioma nos permite no caer en cadenas infinitas de pertenencias. Por ejemplo, si tuviéramos dos conjuntos x e y de forma que:

   $$x = \{y\} \qquad y = \{x\}$$

   Entonces, tendríamos:

   $$x \ni y \ni x \ni y \ni \ldots$$

   Pero este axioma no lo permite.

Axioma de elección (AE).

Para todo conjunto no vacío x existe un conjunto y que tiene un único elemento en común con cada elemento de x.

Lema de Zorn.

Si toda cadena de un conjunto ordenado tiene cota superior, entonces el conjunto tiene un elemento maximal.

Principio de buena ordenación.

Todo conjunto no vacío admite un buen orden (un elemento mínimo).

Hipótesis del continuo (HC).

Todo subconjunto infinito de $\mathbb{R}$ es numerable o tiene la misma cardinalidad de que $\mathbb{R}$.

(AE) y (HC) no son demostrables con la axiomática de Zermelo-Fraenkel, son independientes entre sí y son consistentes con estos axiomas, así como sus negaciones.