Trabajo Fin de Grado - Curso 2017/ 2018

Teoremas de Decibilidad en Álgebras de Relaciones

Autora: **Adah Díaz Torres**

Tutor: Enric Cosme Llópez

Facultat de Ciències Matemàtiques

Grado en Matemáticas

Dedicado a mi tutor por aceptarme
cuando todo parecía perdido,
a Irene por su inspirador arte,
a mi familia por su apoyo,
a Raúl por su comprensión y ternura.
Especialmente dedicado a mamá
por ser siempre oasis en el desierto.

Resumen

Comenzaremos desarrollando los conceptos matemáticos del álgebra relacional y el álgebra de términos necesarios para probar los tres teoremas de decibilidad para leyes entre relaciones que se presentarán a lo largo del trabajo. La utilidad principal de estos teoremas reside en la automatización de las pruebas formales para ecuaciones relacionales. Para presentar los teoremas repasaremos distintos artículos centrados en cada una de las tres estructuras algebraicas principales que se presentarán a lo largo del trabajo: Álgebras de Kleene, Alegorías y Alegorías de Kleene. Veremos que el conjunto de relaciones sobre un conjunto dado presenta estructura de álgebra, para cualquiera de estas tres signaturas, siempre que se asocien las operaciones adecuadas al conjunto de las relaciones. Introduciremos distintas álgebras, con las tres estructuras mencionadas, para las que ya se han automatizado los procesos de pruebas formales. Los teoremas nos permitirán viajar entre álgebras asegurando la validez de una ecuación en el álgebra de relaciones si y solo si se satisface un procedimiento determinado en la otra álgebra. El teorema de decibilidad para alegorías de Kleene unificará los resultados del teorema de decibilidad para álgebras de Kleene y el teorema de decibilidad para alegorías.

Palabras clave: Álgebra de relaciones, Teoremas de decibilidad, Álgebras de Kleene, Alegorías, Alegorías de Kleene.

Índice general

Introducción

En el marco conceptual del álgebra relacional, nos encontramos con el problema de determinar la validez de ecuaciones e inecuaciones entre relaciones. En el primer capítulo de *Automata for relation algebra and formal proofs* [16], Damien Pous presenta algunos conceptos del cálculo relacional, campo iniciado por De Morgan, Pierce y más adelante Schröder a finales del siglo XIX, y estudiado extensamente por Tarski en la década de 1940. Lo hace con el objetivo, entre otros, de presentar algoritmos para la automatización de los procedimientos de decisión sobre las mencionadas ecuaciones e inecuaciones. En este trabajo, ampliamos ese primer capítulo, desarrollando las bases mátematicas que sustentan la programación de algoritmos para la decibilidad de ecuaciones relacionales. Así, reuniremos resultados de distintos artículos unificando notación, con el objetivo de clarificar la base matemática que sustenta la formalización teórica y así probar de forma clara los teoremas de decibilidad que recoje Damien Pous a partir de los trabajos de Freyd y Scedrov [9], Andréka y Bredikhin [1] con alegorías; Kleene, Conway [7] y Kozen [10, 11] con álgebras de Kleene; y los resultados recientes de Paul Brunet y Damien Pous para alegorías de Kleene [4].

En el primer capítulo haremos una revisión de los conceptos básicos del álgebra de conjuntos así como una introducción al álgebra de relaciones, para ello hemos revisado los *Apuntes de Matemática Básica* (Marta Pla) [15]. En esta introducción se repasarán las propiedades más importantes del álgebra relacional y se definirán las distintas operaciones que se dan entre relaciones.

En el segundo capítulo estudiaremos las bases del álgebra universal, apoyándonos en *A Course in Universal Algebra* (Stanley Burris y H.P. Sankappanavar) [5], que nos permitirán definir el álgebra de términos, basándonos principalemente en el artículo *Eilenberg theorems for many-sorted formations* (J. Climent y E. Cosme) [6].

Los siguientes capítulos presentarán la misma estructura entre sí. En primer lugar definiremos una signatura algebraica con la que construiremos la correspondiente álgebra de términos. En segundo lugar veremos que existe un álgebra definida sobre el conjunto de relaciones junto con algunas operaciones que admite, en cada caso, la estructura de la correspondiente álgebra de términos para la signatura definida. A continuación presentaremos otra álgebra con la misma estructura: la del conjunto de lenguajes en el tercer capítulo, dedicado a álgebras de Kleene, y la del conjunto de grafos en el cuarto capítulo, dedicado a las alegorías. Finalmente, probaremos en cada capítulo el teorema de decibilidad para las álgebras estudiadas. Estos teoremas nos permitirán viajar entre álgebras de forma que probar la validez de una ecuación en relaciones sea equivalente a probar que se satisface un procedimiento en lenguajes o grafos. Y, dado que se pueden automatizar las pruebas de procedimiento en lenguajes o grafos, esto facilitará enormemente las pruebas de ecuaciones relacionales.

Por último, el capítulo quinto pretende agrupar ambos resultados. Para ello se define una nueva signatura algebraica, que reúne las operaciones de las signaturas de los capítulos tercero y cuarto (salvo por la operación constante $\top$ que presenta problemas como se explicará en la introducción al capítulo). Y de la misma forma que en estos, veremos que el conjunto de relaciones admite la estructura del álgebra de términos para la signatura definida, estructura de alegoría de Kleene. A continuación, presentaremos dos álgebras con esta misma estructura: lenguajes de grafos y partes de la $\Sigma^{\mathrm{Al}'}$-álgebra libre. Cerraremos con el tercer teorema de decibilidad: *Teorema de Decibilidad en Alegorías de Kleene*, que recoge los dos resultados anteriores para todas las operaciones salvo $\top$.

A lo largo del trabajo, en lo que se refiere a teoría de conjuntos, adoptaremos la siguiente convención. Un *ordinal* α es un conjunto transitivo bien ordenado para la pertenencia. Es decir, $\alpha = \{\beta \mid \beta \in \alpha\}$. El primer *ordinal transfinito*, ω_0, se denotará por $\mathbb{N}$ que es el conjunto de todos los números naturales. Por esto, para todo $n \in \mathbb{N}$

$$n = \{0, \ldots, n-1\}$$

Así, la tupla $(a_0, \ldots, a_{n-1})$, la escribiremos $((a_i)_{i \in n})$.

Capítulo 1

Relaciones algebraicas

1.1. Conceptos previos

Comenzamos por dar unas nociones básicas de la teoría de conjuntos que nos permitirán definir las relaciones algebraicas y sus propiedades.

Definición 1.1.1. Dado un conjunto C, definimos el *conjunto de las partes de* C, y escribimos $\mathcal{P}(C)$, como el conjunto de todos los subconjuntos de C, es decir, los conjuntos B tales que $B \subseteq C$.

Definición 1.1.2. Sean C_1 y C_2 conjuntos, definimos el *producto cartesiano de* C_1 *con* C_2, y lo denotamos $C_1 \times C_2$, como el conjunto de todos los pares ordenados con primer elemento en C_1 y segundo elemento en C_2. Es decir, el conjunto de elementos (a, b) con $a \in C_1$ y $b \in C_2$.

Ejemplo 1.1.3. Sea $C_1 = \{1, 2, 3\}$ un conjunto. Entonces, el conjunto de las partes de C_1 es:

$$\mathcal{P}(C_1) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, C_1\}.$$

Sea $C_2 = \{a, b\}$ un segundo conjunto, el producto cartesiano de C_1 con C_2 es:

$$C_1 \times C_2 = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Definición 1.1.4. Dado un conjunto C, una *relación binaria* en C es un subconjunto $\mathcal{R} \subseteq C \times C$. Escribiremos

$$a\mathcal{R}b \quad \text{si y solo si} \quad (a, b) \in \mathcal{R}.$$

El conjunto de relaciones en C es el conjunto $\mathcal{P}(C \times C)$.

Notación. A lo largo del trabajo utilizaremos la siguiente notación:

- Letras mayúsculas latinas, $A, B, C, \ldots$, para referirnos a conjuntos.
- Letras minúsculas, $a, b, c, \ldots$, para denotar elementos en los conjuntos.
- Letras mayúsculas caligráficas, $\mathcal{R}, \mathcal{S}, \mathcal{T}, \ldots$, cuando nos refiramos a relaciones.

Definición 1.1.5. Dada una relación binaria $\mathcal{R}$ en un conjunto C, diremos que $\mathcal{R}$ es:

- *Reflexiva* si $\forall a \in C, \quad a\mathcal{R}a.$
- *Irreflexiva* si $\forall a \in C, \quad a\not\mathcal{R}a.$
- *Transitiva* si $\forall a, b, c \in C, \quad a\mathcal{R}b$ y $b\mathcal{R}c \Rightarrow a\mathcal{R}c.$
- *Simétrica* si $\forall a, b \in C, \quad a\mathcal{R}b \Rightarrow b\mathcal{R}a.$
- *Antisimétrica* si $\forall a, b \in C, \quad a\mathcal{R}b$ y $b\mathcal{R}a \Rightarrow a = b.$
- *Asimétrica* si $\forall a, b \in C, \quad a\mathcal{R}b \Rightarrow b\not\mathcal{R}a.$
- *Completa* si $\forall a, b \in C, \quad a\mathcal{R}b$ ó $b\mathcal{R}a.$
- *Acíclica* si para $(a_i)_{i \in n+1} \in C^{n+1}, n \in \mathbb{N}, \forall i \in n, a_i\mathcal{R}a_{i+1} \Rightarrow a_0 \neq a_n.$

Veamos algunos ejemplos.

Ejemplo 1.1.6. Dado el conjunto $C = \{1, 2, 3, 4\}$, definimos las relaciones $\mathcal{R}, \mathcal{S}$ y $\mathcal{T}$ en C y vemos sus propiedades:

$$\mathcal{R} = \{(1, 2), (2, 3)\}$$

$\mathcal{R}$ no es reflexiva, es irreflexiva, no es transitiva, no es simétrica, es antisimétrica, es asimétrica, no es completa y es acíclica.

$$\mathcal{S} = \{(1, 1), (2, 2), (1, 2), (2, 1), (3, 4)\}$$

$\mathcal{S}$ no es reflexiva, no es irreflexiva, es transitiva, no es simétrica, no es antisimétrica, no es asimétrica, no es completa, no es acíclica y no es acíclica.

$$\mathcal{T} = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$$

$\mathcal{T}$ es reflexiva, no es irreflexiva, es transitiva, es simétrica, es antisimétrica, no es asimétrica y no es completa.

Veamos las definiciones de relación de equivalencia y relación de orden.

Definición 1.1.7. Una relación binaria en C es una *relación de equivalencia* si cumple las propiedades *r*eflexiva, transitiva y *s*imétrica.

Definición 1.1.8. Una relación binaria en C es una *relación de orden parcial* si cumple las propiedades *r*eflexiva, transitiva y *a*ntisimétrica.

Además, una relación binaria en C es:

- *orden parcial estricto* si es *i*rreflexiva y *t*ransitiva.
- *orden total* si es un *o*rden parcial y *c*ompleta.
- *orden total estricto* si es un *o*rden parcial estricto y *c*ompleta.

Ejemplo 1.1.9. Retomando el ejemplo anterior, vemos que $\mathcal{R}$ y $\mathcal{S}$ no se ajustan a ninguna de las definiciones, en cambio $\mathcal{T}$ es a la vez una relación de equivalencia y de orden parcial.

Definición 1.1.10. Una relación binaria $\mathcal{R}$ en un conjunto C es un *preorden* en C si es reflexiva y transitiva.

Si $(a, b) \in \mathcal{R}$ preorden, decimos que *a es menor o igual que b*. Normalmente utilizaremos el símbolo $\lhd$ para denotar preórdenes, y escribiremos $a \lhd b$.

Nota. Un *orden parcial* en C, es un preorden $\lhd$ que además cumple la propiedad antisimétrica.

Definición 1.1.11. Dado un preorden $\lhd$ en C y un subconjunto $A \subseteq C$, se define la *clausura descendente* de A como:

$$^{\downarrow\lhd}A = \{c \in C \mid \exists a \in A : c \lhd a\}$$

A lo largo de esta sección hemos introducido nociones básicas sobre las relaciones y sus propiedades. En lo que sigue de capítulo nos centraremos en el conjunto que contiene todas las relaciones sobre un conjuto C cualquiera.

1.2. El conjunto de relaciones

Como hemos visto en la Definición 1.1.4, el conjunto de todas las relaciones sobre un conjunto C, es el conjunto $\mathcal{P}(C \times C)$. Veremos en esta sección algunas de las propiedades y operaciones que admite este conjunto.

El conjunto $\mathcal{P}(C \times C)$ está provisto de un *orden parcial* dado por la inclusión entre relaciones.

Además, este conjunto contiene tres relaciones especiales:

- La *relación vacía*, que denotaremos por 0.
  Se define como $0 = \emptyset$.

- La *relación universal o total*, que denotaremos por $\top$.
  Se define como $\top = C \times C$.

- Y la *relación identidad*, que denotaremos por 1.
  Se define como $1 = \{(a, b) \in C \times C \mid a = b\}$.

Veamos ahora tres *operaciones unarias* que podemos realizar con las relaciones.

- *Complemento:* La relación complementaria a la relación $\mathcal{R}$, denotada $\mathcal{R}^c$, se define como:

$$\mathcal{R}^c := \{(a, b) \in C \times C \mid a \not\mathcal{R} b\}.$$

- *Inversa:* La relación inversa u opuesta de $\mathcal{R}$ se denota por $\mathcal{R}^o$ y se define como:

$$\mathcal{R}^o := \{(a, b) \in C \times C \mid b\mathcal{R}a\}.$$

- *Clausura reflexivo-transitiva:* La clausura reflexivo-transitiva de $\mathcal{R}$, denotada $\mathcal{R}^*$, se define como:

$$\mathcal{R}^* := \{(a, b) \in C \times C \mid \begin{array}{l} \exists c_0, \dots, c_n \in C : \\ : c_0 = a \text{ y } c_n = b \text{ y } \forall i \in n, c_i \mathcal{R} c_{i+1}\} \end{array}.$$

Veamos ahora tres *operaciones binarias* que podemos realizar con los elementos de $\mathcal{P}(C \times C)$.

- *Unión:* La unión de $\mathcal{R}$ y $\mathcal{S}$, denotada $\mathcal{R} \cup \mathcal{S}$, es la relación que contiene todos los elementos que están en $\mathcal{R}$ o $\mathcal{S}$:

$$\mathcal{R} \cup \mathcal{S} := \{(a, b) \in C \times C \mid a\mathcal{R}b \text{ ó } a\mathcal{S}b\}.$$

- *Intersección:* La intersección de $\mathcal{R}$ y $\mathcal{S}$, denotada $\mathcal{R} \cap \mathcal{S}$, es la relación que contiene todos los elementos que están en $\mathcal{R}$ y $\mathcal{S}$:

$$\mathcal{R} \cap \mathcal{S} := \{(a, b) \in C \times C \mid a\mathcal{R}b \text{ y } a\mathcal{S}b\}.$$

- *Composición:* La composición de $\mathcal{R}$ y $\mathcal{S}$, denotada por $\mathcal{R} \cdot \mathcal{S}$, se define como:

$$\mathcal{R} \cdot \mathcal{S} := \{(a, b) \in C \times C \mid \exists c \in C : a\mathcal{R}c \text{ y } c\mathcal{S}b\}.$$

Además, se puede realizar la potencia de una relación.

- *Potencia:* Para $n \in \mathbb{N}$, se define la potencia n-ésima de una relación $\mathcal{R}$ de forma recurrente sobre la composición de relaciones como sigue:

$$\begin{array}{rcl} \mathcal{R}^0 & = & 1, \\ \mathcal{R}^{n+1} & = & \mathcal{R}^n \cdot \mathcal{R}. \end{array}$$

Nota. Sea $\mathcal{R}^n$ la potencia n-ésima de la relación $\mathcal{R}$ y sean $a, b \in C$. Entonces, $a\mathcal{R}^n b$ si y solo si existen $(x_i)_{i \in n+1}$ en C tales que:

$$\begin{array}{l} x_0 = a, \\ x_n = b, \\ x_i \mathcal{R} x_{i+1} \text{ para todo } i \in n+1. \end{array}$$

.

Definición 1.2.1. Diremos que dos relaciones $\mathcal{R}$ y $\mathcal{S}$ *conmutan* si dados tres elementos $a, b, c \in C$ tales que $c\mathcal{R}a$ y $c\mathcal{S}b$, entonces existe un elemento $d \in C$ tal que $b\mathcal{R}d$ y $a\mathcal{S}d$. Es decir, si $\mathcal{R} \cdot \mathcal{S} = \mathcal{S} \cdot \mathcal{R}$.

Nos limitaremos a esta lista de operaciones a pesar de no ser exhaustiva. De estas operaciones derivan distintas propieades. Vemos algunos ejemplos:

Propiedad 1.2.2. *Si $1 \subseteq \mathcal{R}$ entonces $\mathcal{R}$ es reflexiva.*

Demostración. La relación identidad está en $\mathcal{R}$, $1 \subseteq \mathcal{R}$, por tanto se cumple que para cualquier $a \in C, a\mathcal{R}a$ y entonces $\mathcal{R}$ es reflexiva. □

Propiedad 1.2.3. *Si $\mathcal{R} \cdot \mathcal{R} \subseteq \mathcal{R}$ entonces $\mathcal{R}$ es transitiva.*

Demostración. La composición de R con R es el conjunto

$$\mathcal{R} \cdot \mathcal{R} = \{(a, b) \in C \times C \mid \exists\, c \in C : a\mathcal{R}c \text{ y } c\mathcal{R}b\}.$$

Sabemos por hipótesis que este conjunto está contenido en

$$\mathcal{R} = \{(a, b) \in C \times C \mid a\mathcal{R}b\}.$$

Entonces, sea un elemento $(a, b) \in \mathcal{R} \cdot \mathcal{R}$ se cumpirá que existe un $c \in C$ tal que $a\mathcal{R}c$ y $c\mathcal{R}b$, y puesto que $(a, b) \in \mathcal{R} \cdot \mathcal{R} \subseteq \mathcal{R}$, se sigue que $a\mathcal{R}b$.

Es decir, $a\mathcal{R}c$ y $c\mathcal{R}b$ implica $a\mathcal{R}b$ y por tanto $\mathcal{R}$ es transitiva. □

Propiedad 1.2.4. *Si $\mathcal{R} \cdot \mathcal{R}^* \cap 1 = \emptyset$ entonces $\mathcal{R}$ es acíclica.*

Demostración. Veamos en primer lugar cual es la relación $\mathcal{R}\cdot\mathcal{R}^*\cap 1$:

$$\mathcal{R}\cdot\mathcal{R}^* = \{(a,b)\in C\times C \mid \exists c\in C : a\mathcal{R}c \text{ y } c\mathcal{R}^*b\}$$

donde $c\mathcal{R}^*b$ significa que existen $c_2, c_3, \ldots, c_{n-1}\in C$ tales que

$$c\mathcal{R}c_2 \text{ y } c_2\mathcal{R}c_3 \text{ y } \ldots \text{ y } c_{n-1}\mathcal{R}b.$$

Por tanto,

$$\begin{aligned}\mathcal{R}\cdot\mathcal{R}^* = \{(a,b)\in C\times C \mid\ & \exists c, c_2, c_3, \ldots, c_{n-1}\in C :\\ & : a\mathcal{R}c \text{ y } c\mathcal{R}c_2 \text{ y } c_2\mathcal{R}c_3 \text{ y } \ldots \text{ y } c_{n-1}\mathcal{R}b\}.\end{aligned}$$

Así tenemos,

$$\begin{aligned}\mathcal{R}\cdot\mathcal{R}^* = \{(a,b)\in C\times C \mid\ & \exists c_0 = a, c_1, c_2, \ldots, c_{n-1}, c_n = b\in C :\\ & : c_i\mathcal{R}c_{i+1}\ \forall i\in n\}.\end{aligned}$$

Ahora bien,

$$\begin{aligned}\mathcal{R}\cdot\mathcal{R}^*\cap 1 &= \{(a,b)\in C\times C \mid a(\mathcal{R}\cdot\mathcal{R}^*)b \text{ y } a1b\}\\ &= \{(a,b)\in C\times C \mid a(\mathcal{R}\cdot\mathcal{R}^*)b \text{ y } a=b\}\\ &\underset{(*)}{=} \emptyset\end{aligned}$$

donde la igualdad marcada con $(*)$ se da por hipótesis.

Es decir que para cualesquiera $c_0, \ldots, c_n \in C$ tales que $c_i\mathcal{R}c_{i+1}$ para $i\in n$ se cumple que $c_0\neq c_n$ y, por tanto, $\mathcal{R}$ es acíclica. □

Propiedad 1.2.5. *Si $\mathcal{R}^o\cdot\mathcal{S}\subseteq\mathcal{S}\cdot\mathcal{R}^o$ entonces $\mathcal{R}$ y $\mathcal{S}$ conmutan.*

Demostración. Comencemos por ver en que consisten las relaciones $\mathcal{R}^o\cdot\mathcal{S}$ y $\mathcal{S}\cdot\mathcal{R}^o$.

$$\begin{aligned}\mathcal{R}^o\cdot\mathcal{S} &= \{(a,b)\in C\times C \mid \exists\, c\in C : a\mathcal{R}^0c \text{ y } c\mathcal{S}b\}\\ &\underset{(*)}{=} \{(a,b)\in C\times C \mid \exists\, c\in C : c\mathcal{R}a \text{ y } c\mathcal{S}b\}.\end{aligned}$$

$$\begin{aligned}\mathcal{S}\cdot\mathcal{R}^o &= \{(a,b)\in C\times C \mid \exists\, d\in C : a\mathcal{S}d \text{ y } d\mathcal{R}^0b\}\\ &\underset{(*)}{=} \{(a,b)\in C\times C \mid \exists\, d\in C : a\mathcal{S}d \text{ y } b\mathcal{R}d\}.\end{aligned}$$

(*) Recordamos que $\mathcal{R}^o = \{(a,b)\in C\times C \mid b\mathcal{R}a\}$ es la relación inversa de $\mathcal{R}$. Entonces, como $\mathcal{R}^o\cdot\mathcal{S}\subseteq\mathcal{S}\cdot\mathcal{R}^o$ tenemos que dado un elemento $(a,b)\in\mathcal{R}^o\cdot\mathcal{S}$, este cumplirá que existe $c\in C$ tal que $c\mathcal{R}a$ y $c\mathcal{S}b$, y, como por hipótesis $\mathcal{R}^o\cdot\mathcal{S}\subseteq\mathcal{S}\cdot\mathcal{R}^o$, el elemento (a,b) está también en $\mathcal{S}\cdot\mathcal{R}^o$, por lo que cumple que existe $d\in C$ tal que $a\mathcal{S}d$ y $b\mathcal{R}d$.

Así, si se cumple $c\mathcal{R}a$ y $c\mathcal{S}b$, entonces existe $d\in C$ tal que $a\mathcal{S}d$ y $b\mathcal{R}d$ y, por tanto, $\mathcal{R}$ y $\mathcal{S}$ conmutan. □

Además, estas operaciones safisfacen muchas ecuaciones. Algunas de ellas muy sencillas:

- La composición de relaciones es asociativa: $(\mathcal{R}\cdot\mathcal{R}')\cdot\mathcal{R}'' = \mathcal{R}\cdot(\mathcal{R}'\cdot\mathcal{R}'')$.

  Demostración.

  $$\begin{array}{rcl}(\mathcal{R}\cdot\mathcal{R}')\cdot\mathcal{R}'' & = & \{(a,b)\in C\times C \mid \exists\, d\in C : a(\mathcal{R}\cdot\mathcal{R}')d \text{ y } d\mathcal{R}''b\} \\ & = & \{(a,b)\in C\times C \mid \exists\, c,d\in C : a\mathcal{R}c \text{ y } c\mathcal{R}'d \text{ y } d\mathcal{R}''b\} \\ & = & \{(a,b)\in C\times C \mid \exists\, c\in C : a\mathcal{R}c \text{ y } c(\mathcal{R}'\cdot\mathcal{R}'')b\} \\ & = & \mathcal{R}\cdot(\mathcal{R}'\cdot\mathcal{R}'')\end{array}$$

  Con lo que queda probada la propiedad asociativa para la composición de relaciones. □

- La composición de cualquier relación con la relación vacía es la relación vacía: $\mathcal{R}\cdot 0 = 0 = 0\cdot\mathcal{R}$.

- La clausura reflexivo-transitiva es transitiva: $\mathcal{R}^*\cdot\mathcal{R}^* \subseteq \mathcal{R}^*$.

  Demostración. Comenzamos por ver cuál es la relación $\mathcal{R}^*\cdot\mathcal{R}^*$. Recordamos que

  $$\begin{array}{rl}\mathcal{R}^* := & \{(a,b)\in C\times C \mid \exists c_0,\ldots,c_n\in C, c_0=a \text{ y } c_n=b \\ & \text{ y } \forall i\in n, a_i\mathcal{R}a_{i+1}\}\end{array}$$

  es la clausura reflexivo-transitiva de $\mathcal{R}$.

  $$\begin{array}{l}\mathcal{R}^*\cdot\mathcal{R}^* = \\ = \{(a,b)\in C\times C \mid \exists\, c\in C : a\mathcal{R}^*c \text{ y } c\mathcal{R}^*b\} \\ = \{(a,b)\in C\times C \mid \exists\, c_0=a,\ldots,c_m=c\in C : \forall i\in n, c_i\mathcal{R}c_{i+1} \\ \text{ y } \exists c_m=c,\ldots,c_n=b\in C, m<n : \forall i\in n-m, c_i\mathcal{R}c_{i+1}\}.\end{array}$$

  Entonces, dado un elemento $(a,b)\in\mathcal{R}^*\cdot\mathcal{R}^*$, sabemos que existen elementos $c_0=a, c_1,\ldots,c_{n-1},c_n=b\in C$ tales que para $i\in n$ se cumple: $a_i\mathcal{R}a_{i+1}$, por lo que podemos afirmar que $(a,b)\in\mathcal{R}^*$. Es decir, $\mathcal{R}^*\cdot\mathcal{R}^*\subseteq\mathcal{R}^*$. □

Algunas ecuaciones, en cambio, requieren más trabajo para comprobar si se cumplen o no:

$$
\begin{aligned}
1 \cap \mathcal{R} &\subseteq \mathcal{R}\cdot\mathcal{R} \cap \mathcal{R}\cdot\mathcal{R}\cdot\mathcal{R} && (1.1)\\
(\mathcal{R} \cup \mathcal{S})^* &= \mathcal{R}^*\cdot(\mathcal{S}\cdot\mathcal{R}^*)^* && (1.2)\\
(\mathcal{R} \cup \mathcal{S})^* &= ((1 \cup \mathcal{R})\cdot\mathcal{S})^* && (1.3)\\
\mathcal{R}\cdot(\mathcal{S} \cap \mathcal{T}) &= \mathcal{R}\cdot\mathcal{S} \cap \mathcal{R}\cdot\mathcal{T} && (1.4)\\
\mathcal{R}\cdot\mathcal{S} \cap \mathcal{T} &\subseteq \mathcal{R}\cdot(\mathcal{S} \cap \mathcal{R}^o\cdot\mathcal{T}) && (1.5)\\
\mathcal{R}\cdot\mathcal{S} \cap \mathcal{T} &\subseteq (\mathcal{R} \cap \mathcal{T}\cdot\mathcal{S}^o)\cdot(\mathcal{S} \cap \mathcal{R}^o\cdot\mathcal{T}) && (1.6)\\
(\mathcal{R} \cap \mathcal{S}\cdot\top)\cdot\mathcal{T} &= \mathcal{R}\cdot\mathcal{T} \cap \mathcal{S}\cdot\top && (1.7)
\end{aligned}
$$

Vemos a continucación la demostración de un par de estas propiedades como muestra de la dificultad que supone saber si son o no ciertas:

- Propiedad (1.1) $1 \cap \mathcal{R} \subseteq \mathcal{R}\cdot\mathcal{R} \cap \mathcal{R}\cdot\mathcal{R}\cdot\mathcal{R}$.

  Demostración. Para ver que se cumple hemos de comprobar que dado un elemento $(a, b) \in 1 \cap \mathcal{R}$, dicho elemento también se encuentra en $\mathcal{R}\cdot\mathcal{R}\cap\mathcal{R}\cdot\mathcal{R}\cdot\mathcal{R}$, para ello hemos de ver que nuestro elemento (a, b) está tanto en $\mathcal{R}\cdot\mathcal{R}$ como en $\mathcal{R}\cdot\mathcal{R}\cdot\mathcal{R}$.

  Sea $(a, b) \in 1 \cap \mathcal{R}$, entonces $\begin{cases} (a,b) \in 1 & \text{por tanto} \quad a = b \\ y & \\ (a,b) \in \mathcal{R} & \text{por tanto} \quad a\mathcal{R}b. \end{cases}$

  Así $a\mathcal{R}a, a\mathcal{R}b$ y $b\mathcal{R}b$.

  Para ver que $(a, b) \in \mathcal{R} \cdot \mathcal{R} = \{(a, b) \mid \exists c \in C : a\mathcal{R}c \text{ y } c\mathcal{R}b\}$ basta con considerar $c = a$ o $c = b$ y así comprobamos que efectivamente $(a, b) \in \mathcal{R} \cdot \mathcal{R}$.

  Por otro lado, para comprobar que

  $$(a, b) \in \mathcal{R} \cdot \mathcal{R} \cdot \mathcal{R} = \{(a, b) \mid \exists d, e \in C : a\mathcal{R}d \text{ y } d\mathcal{R}e \text{ y } e\mathcal{R}b\},$$

  consideramos $d = a$ y $e = b$ y tenemos que $(a, b) \in \mathcal{R} \cdot \mathcal{R} \cdot \mathcal{R}$.

  Por lo tanto el elemento $(a, b) \in \mathcal{R}\cdot\mathcal{R} \cap \mathcal{R}\cdot\mathcal{R}\cdot\mathcal{R}$, y así:

  $$1 \cap \mathcal{R} \subseteq \mathcal{R}\cdot\mathcal{R} \cap \mathcal{R}\cdot\mathcal{R}\cdot\mathcal{R}.$$

  Y podemos afirmar que la inecuación es universalmente válida en para cualquier relación $\mathcal{R}$. □

- Propiedad (1.4): $\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})=\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}$.

  Demostración. Para ver si son iguales veremos en que consisten las expresiones a cada lado de la igualdad.

  Comenzamos por ver como es la relación $\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})$:

  $$\mathcal{S}\cap\mathcal{T}=\{(c,b)\mid c\mathcal{S}b \text{ y } c\mathcal{T}b\},$$

  entonces:

  $$\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})=\{(a,b)\mid \exists c\in C: a\mathcal{R}c, c\mathcal{S}b \text{ y } c\mathcal{T}b\}.$$

  Por otro lado, veamos como es la relación $\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}$:

  $$\left.\begin{array}{lcl}\mathcal{R}\cdot\mathcal{S} & = & \{(a,b)\mid \exists d\in C: a\mathcal{R}d \text{ y } d\mathcal{S}b\}\\ \mathcal{R}\cdot\mathcal{T} & = & \{(a,b)\mid \exists e\in C: a\mathcal{R}e \text{ y } e\mathcal{T}b\}\end{array}\right\}$$

  por tanto:

  $$\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}=\{(a,b)\mid \exists c,d\in C: a\mathcal{R}c, c\mathcal{S}b, a\mathcal{R}d \text{ y } d\mathcal{T}b\}.$$

  La inclusión $\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})\subseteq\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}$ es evidente, ya que dado $(a,b)\in\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})$, consideramos $c=d=e$ y por tanto existe $c\in C$ tal que $a\mathcal{R}c, c\mathcal{S}b$ y $c\mathcal{T}b$. De esta forma $(a,b)\in\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}$.

  La inclusión contraria, $\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})\supseteq\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}$ no tiene porque cumplirse, veamos un contraejemplo:

  Sobre el conjunto $C=\{1,2,3\}$, consideramos las relaciones $\mathcal{R}=\{(1,2),(1,3)\},\mathcal{S}=\{(2,3)\}$ y $\mathcal{T}=\{(3,3)\}$, entonces:

  $$\left.\begin{array}{lcl}\mathcal{R}\cdot\mathcal{S} & = & \{(1,3)\}\\ \mathcal{R}\cdot\mathcal{T} & = & \{(1,3)\}\end{array}\right\}\text{ entonces } (1,3)\in\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}$$

  Pero $\mathcal{S}\cap\mathcal{T}=\emptyset$ por lo que $\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})=\mathcal{R}\cdot\emptyset=\emptyset$

  Y así, existe un elemento $(1,3)\in\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}$ tal que $(1,3)\notin\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})$

  Por tanto no necesariamente se da la igualdad: $\mathcal{R}\cdot(\mathcal{S}\cap\mathcal{T})=\mathcal{R}\cdot\mathcal{S}\cap\mathcal{R}\cdot\mathcal{T}$ y esta no es una ecuación universalmente válida para relaciones. □

Resulta trabajoso comprobar la validez de estas propiedades. Nos planteamos, en consecuencia, si existe la posibilidad de decidir si una inecuación es válida o no sin necesidad de demostrar cada caso en particular. En este trabajo pretendemos hallar métodos que nos permitan decidir de forma más sencilla si una inecuación es universalmente válida o no en modelos relacionales. Para ello veremos que se pueden dar equivalencias entre la validez de una inecuación en relaciones y una inecuación en lenguajes, y también entre la validez de una inecuación en relaciones y la existencia de un homomorfismo entre grafos. Esto nos permitirá decir que una ecuación es universalmente válida para todo modelo relacional si y solo si los lenguajes o grafos asociados a ella cumplen determinadas hipótesis.

Estudiaremos en el siguiente capítulo algunos conceptos del álgebra de términos para ver que podemos entender las relaciones, los lenguajes y los grafos como determinadas álgebras. Lo que nos permitirá más adelante dar las equivalencias de las que hablamos.

Capítulo 2

Álgebra de términos

2.1. Álgebra universal. Definición y ejemplos.

El álgebra universal tiene por objetivo, entre otros, extraer los elementos comunes de distintos tipos de estructuras algebraicas, cuando esto sea posible. Para lograr este objetivo, se buscan conceptos, construcciones y resultados que generalicen los conocimientos que ya se tienen sobre situaciones especiales. Describiremos en esta sección algunos de estos conceptos generales que nos permitirán comprender, y presentar con mayor facilidad, el álgebra de términos.

Para llegar a la definición de álgebra, comenzaremos por ver algunos conceptos básicos necesarios:

Definición 2.1.1. Dado un conjunto A no vacío y un entero n no negativo, definimos $A^0 = \{\emptyset\}$, y, para $n > 0$, definimos A^n como el conjunto de n-tuplas de elementos de A.

Definición 2.1.2 (Ariedad, operaciones n-arias)**.** Una *operación n-aria* en A es una aplicación σ de A^n en A. Llamamos *ariedad* de σ a n. Una *operación finitaria* es una operación n-aria, para algún n.

Notación. La imagen de $(a_i)_{i\in n}$ por una operación n-aria σ se denota por $\sigma((a_i)_{i\in n})$.

Definición 2.1.3. Una operación σ en A se llama *constante* si su ariedad es cero; está completamente determinada por la imagen de $\sigma(\emptyset)$ en A del único elemento $\emptyset$ de A^0 y, como tal, es conveniente identificarla con el elemento $\sigma(\emptyset)$. Por lo tanto una constante es considerada como un elemento de A.

Una operación σ en A es *unaria, binaria* o *ternaria* si su ariedad es 1, 2 o 3, respectivamente.

Notación. Llamaremos $\mathrm{Hom}(A^n, A)$ al conjunto de todas las aplicaciones $\sigma : A^n \longrightarrow A$.

Definición 2.1.4. Una *signatura algebraica* es un conjunto Σ de símbolos de operaciones tal que a cada elemento σ de Σ se le asigna un entero no negativo n. Este entero se llama ariedad de σ, y se dice que σ es un símbolo de operación n-aria.

El subconjunto de símbolos de operación n-arias de Σ se denota por Σ_n. Así, la *signatura algebraica* puede representarse como $\Sigma = (\Sigma_n)_{n\in\mathbb{N}}$.

Ahora que tenemos claro el concepto de signatura algebraica, podemos dar la definición de Σ-álgebra:

Definición 2.1.5. Dada una signatura algebraica Σ, una Σ-*álgebra* $\mathbf{A}$ es un par ordenado (A, F) donde A es un conjunto no vacío y F es una familia de operaciones finitarias en A indexadas por Σ de manera que a cada símbolo de función n-aria σ en Σ, le corresponde una operación n-aria $\sigma^{\mathbf{A}}$ en $\mathbf{A}$:

$$\begin{array}{rcl} F:\Sigma & \longrightarrow & \bigcup_{n\in\mathbb{N}} \mathrm{Hom}(A^n, A) \\ \sigma & \longmapsto & \sigma^{\mathbf{A}} : A^n \longrightarrow A \end{array}$$

Al conjunto A se le llama *conjunto subyacente* (o universo) de $\mathbf{A} = (A, F)$, y las $\sigma^{\mathbf{A}}$ se llaman *operaciones fundamentales* de $\mathbf{A}$.

Notación. Habitualmente escribiremos σ en lugar de $\sigma^{\mathbf{A}}$.

Dada una signatura algebraica Σ, si el conjunto Σ es finito, es decir, $\Sigma = \{\sigma_1, \dots, \sigma_k\}$, en ocasiones escribiremos $(A, \sigma_1, \dots, \sigma_k)$ en lugar de (A, F), ordenando las operaciones fundamentales de forma que:

$$\textit{ariedad}\ \sigma_1 \geq \textit{ariedad}\ \sigma_2 \geq \cdots \geq \textit{ariedad}\ \sigma_k$$

Definición 2.1.6. Dadas dos Σ-álgebras, $\mathbf{A} = (A, F)$ y $\mathbf{B} = (B, G)$, diremos que $\mathbf{B}$ *es subálgebra de* $\mathbf{A}$ si $B \subseteq A$ y todas las operaciones fundamentales de $\mathbf{B}$ son la restricción de la operación correspondiente de $\mathbf{A}$ a B, es decir, para cada símbolo de función σ, $\sigma^{\mathbf{B}}$ es la restricción de $\sigma^{\mathbf{A}}$ a B.

A continuación veremos como ejemplo algunas de las álgebras más conocidas, como son los grupos, los anillos o los monoides, expresadas de la forma que hemos visto en esta sección. En ningún caso nos encontraremos con operaciones de ariedad mayor o igual a tres.

Ejemplo 2.1.7 (Grupoides)**.** Un grupoide o magma es un álgebra $(G, \cdot)$ que solo tiene una operación binaria; esta operación suele denotarse por $\cdot$. Para la imagen de (a, b) por esta operación, escribiremos $a \cdot b$ (o simplemente ab), y la llamaremos producto de a por b.

Ejemplo 2.1.8 (Semigrupos)**.** Un semigrupo es un grupoide $(G, \cdot)$ con una operación binaria $\cdot$ que satisface la ley:
G1: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Ejemplo 2.1.9 (Monoides)**.** Un monoide $\mathbf{M}$ es un álgebra $(M, \cdot, 1)$, donde $\cdot$ es una operación binaria y 1 es una constante, que satisface la ley (G1) y además:
M1: $x \cdot 1 = 1 \cdot x = x$.

Ejemplo 2.1.10 (Grupos)**.** Un grupo $\mathbf{G}$ es un álgebra $(G, \cdot, ^{-1}, 1)$ con una operación binaria, una operación unaria y una constante, en la que se cumplen las condiciones (G1), (M1) y además:
G2: $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Un grupo $\mathbf{G}$ es *abeliano* (o conmutativo) si, además, cumple:
G3: $x \cdot y = y \cdot x$.

Ejemplo 2.1.11 (Anillos)**.** Un anillo $\mathbf{R}$ es un álgebra $(R, +, \cdot, -, 0)$, donde $+$ y $\cdot$ son operaciones binarias, $-$ es una operación unaria y 0 es una constante, que satisface las siguientes condiciones:
R1: $(R, +, -, 0)$ es un grupo abeliano.
R2: $(R, \cdot)$ es un semigrupo.
R3: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
y $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Un *anillo con identidad* es un álgebra $(R, +, \cdot, -, 0, 1)$ tal que (R1)-(R3) y (M1) se cumplen.

Antes de pasar a la siguiente sección, definimos el concepto de homomorfismo entre Σ-álgebras. Este será necesario para poder dar los distintos procedimientos que proporcionan los tres teoremas de decibilidad que nos premitirán probar, utilizando otras álgebras, si una ecuación es universalmente válida en el álgebra de relaciones.

Definición 2.1.12. Dadas dos Σ-álgebras $\mathbf{A} = (A, F)$ y $\mathbf{B} = (B, G)$, definimos un Σ-*homomorfismo* o simplemente *homomorfismo de* $\mathbf{A}$ *a* $\mathbf{B}$ como una aplicación de A a B, denotada por $f : \mathbf{A} \longrightarrow \mathbf{B}$, tal que, para cada $\sigma \in \Sigma_n$, y para cada $(a_i)_{i \in n} \in A^n$ se satisface la siguiente expresión:

$$f(\sigma^{\mathbf{A}}((a_i)_{i \in n})) = \sigma^{\mathbf{B}}(f((a_i)_{i \in n})).$$

En la siguiente sección definiremos el concepto de álgebra de términos que nos permitirá formar álgebras a partir de una signatura algebraica dada. Estas álgebras harán de intermediarias entre las relaciones y los lenguajes, los grafos, los lenguajes de grafos, etc. Lo harán mediante homomorfismos entre álgebras con la misma signatura algebraica. La existencia de estos homomorfismos viene asegurada por la *propiedad universal del álgebra de términos* que probaremos en la siguiente sección.

2.2. Álgebras de términos

Dada un álgebra **A** generalmente hay muchas aplicaciones además de las operaciones fundamentales que conservan subálgebras de A. Las aplicaciones más obvias de este tipo son las obtenidas por la composición de las operaciones fundamentales. Esto nos lleva a estudiar los términos que consisten precisamente en los elementos obtenidos por la composición de operaciones fundamentales actuando sobre variables de un conjunto X dado. Vemos a continuación la definición formal:

Definición 2.2.1. Sea X un conjunto cuyos elementos llamaremos *variables*. Sea Σ una signatura algebraica. El conjunto de *términos de tipo* Σ *sobre* X se denota por $\mathrm{T}_\Sigma(X)$ y es el conjunto más pequeño tal que:

(I) $X \subseteq \mathrm{T}_\Sigma(X)$.

(II) $\Sigma_0 \subseteq \mathrm{T}_\Sigma(X)$.

(III) Para cualquier $n \in \mathbb{N}$, si $(p_i)_{i \in n} \in \mathrm{T}_\Sigma(X)$ y $\sigma \in \Sigma_n$, entonces la cadena $\sigma((p_i)_{i\in n}) \in \mathrm{T}_\Sigma(X)$.

Notación. Para un símbolo de operación binaria $\cdot$ normalmente escribiremos $p_1 \cdot p_2$ en lugar de $\cdot(p_1, p_2)$.

Para $p \in \mathrm{T}_\Sigma(X)$, escribiremos p como $p((x_i)_{i\in n})$ para indicar que las variables actuando en p están entre $x_0, \dots, x_{n-1} \in X$.

Ejemplo 2.2.2. Veamos algunos ejemplos de términos en distintas Σ-álgebras:

(1) Sea Σ una signatura algebraica con $\Sigma_2 = \{\cdot\}$ y $\Sigma_n = \emptyset$ para $n \neq 2$, y sea $X = \{x, y, z\}$. Entonces algunos de los términos sobre X son los siguientes:

$$x, y, z, x \cdot y, y \cdot z, x \cdot (y \cdot z), (x \cdot y) \cdot z \in \mathrm{T}_\Sigma(X).$$

(2) Sea Σ una signatura algebraica con $\Sigma_1 = \{^{-1}\}, \Sigma_2 = \{+, \cdot\}$ y $\Sigma_n = \emptyset$ para $n \neq 1, 2$, y sea X el conjunto del ejemplo anterior. Entonces:

$$x, y, z, x^{-1}, x \cdot y, x + z, x \cdot (y + z), (x \cdot y) + (x \cdot z)^{-1} \in \mathrm{T}_\Sigma(X).$$

(3) Sea Σ una signatura algebraica con $\Sigma_2 = \{\cup, \cap\}$ y $\Sigma_n = \emptyset$ para $n \neq 2$, y sea $X = \{x, y, z\}$. Entonces, algunos de los términos sobre X son:

$$x, y, z, x \cup y, x \cap y, (y \cap z) \cup (y \cap x) \in \mathrm{T}_\Sigma(X).$$

Llegados a este punto es natural dotar al conjunto $\mathrm{T}_\Sigma(X)$ de estructura de Σ-álgebra. Veámoslo:

Definición 2.2.3. Dada una signatura algebraica Σ y un conjunto de variables X, si $\mathrm{T}_\Sigma(X) \neq \emptyset$ entonces la Σ-álgebra de términos sobre X, escrita como $\mathbf{T}_\Sigma(X)$, tiene como conjunto subyaciente (o universo) al conjunto $\mathrm{T}_\Sigma(X)$, y las operaciones fundamentales satisfacen:

$$\begin{array}{rccc} \sigma^{\mathbf{T}_\Sigma(X)}: & \mathrm{T}_\Sigma(X)^n & \longrightarrow & \mathrm{T}_\Sigma(X) \\ & (p_1, \ldots, p_n) & \longmapsto & \sigma(p_1, \ldots, p_n) \end{array}$$

para $\sigma \in \Sigma_n$ y $p_i \in \mathrm{T}_\Sigma(X)$, para todo $i \in n$.

Nota. $\mathbf{T}_\Sigma(\emptyset)$ existe si y solo si $\Sigma_0 \neq \emptyset$.

Nos referiremos al siguiente resultado como la *propiedad universal del álgebra de términos*. Esta propiedad asegura que, dada una aplicación de un conjunto de variables en un álgebra cualquiera con determinada signatura, siempre existe una extensión de la aplicación que nos lleva del álgebra de términos con la misma signatura en el álgebra dada.

Proposición 2.2.4. *Sea Σ una signatura algebraica, sea X un conjunto de variables y sea $\mathbf{A}$ una Σ-álgebra, entonces, para toda aplicación $f : X \longrightarrow A$, existe un único homomorfismo $f^{\#} : \mathbf{T}_\Sigma(X) \longrightarrow \mathbf{A}$ que extiende a f, esto es $f^{\#} \circ \eta_X = f$.*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "\eta_X"'] & \mathbf{A} \\ & \mathbf{T}_\Sigma(X) \arrow[u, "f^{\#}"'] \end{tikzcd}$$

donde $\eta_X : X \longrightarrow \mathbf{T}_\Sigma(X)$ es la aplicación, conocida como inserción de generadores*, que lleva la variable $x \in X$ al término $x \in \mathbf{T}_\Sigma(X)$.*

Demostración. Veamos en primer lugar la existencia:

Sea $p \in \mathrm{T}_\Sigma(X)$ un término. Por construcción de $\mathrm{T}_\Sigma(X)$ se pueden dar los siguientes casos:

(1) $p = x$ con $x \in X$.

(2) $p = \sigma$ para algún $\sigma \in \Sigma_0$.

(3) $p = \sigma((p_i)_{i\in n})$ para un único $\sigma \in \Sigma_n$ y una familia de términos $(p_i)_{i\in n} \in \mathrm{T}_\Sigma(X)^n$.

Definimos la aplicación $f^\#$ por indución sobre el término p.
Así, en el caso (1) se define $f^\#(x) = f(x)$.
En el caso (2) definimos $f^\#(\sigma^{\mathbf{T}_\Sigma(X)}) = \sigma^{\mathbf{A}}$.
Por último, en el caso (3), se define como

$$f^\#(\sigma^{\mathbf{T}_\Sigma(X)}((p_i)_{i\in n})) = \sigma^{\mathbf{A}}((f^\#(p_i))_{i\in n})$$

Falta probar que $f^\#\colon \mathrm{T}_\Sigma(X) \longrightarrow \mathbf{A}$ es un homomorfismo y que se cumple que $f^\# \circ \eta_X = f$.

Sean $\sigma \in \Sigma_n$ y $(p_i)_{i\in n} \in \mathrm{T}_\Sigma(X)$, $f^\#$ es homomorfismo si conserva las operaciones fundamentales, es decir, si se cumple:

$$f^\#(\sigma^{\mathbf{T}_\Sigma(X)}((p_i)_{i\in n})) = \sigma^{\mathbf{A}}((f^\#(p_i))_{i\in n})$$

y esto es cierto precisamente por la construcción de $f^\#$. Por tanto, $f^\#$ es homomorfismo.

Además, si $x \in X$:

$$f^\# \circ \eta_X(x) = f^\#(x) = f(x), \quad \text{entonces:} \quad f^\# \circ \eta_X = f$$

Probemos ahora la unicidad:

Sea $g\colon \mathbf{T}_\Sigma(X) \longrightarrow \mathbf{A}$ un homomorfismo que extiende a f, esto es $g \circ \eta_X = f$. Sea $p \in \mathrm{T}_\Sigma(X)$ un término, si:

(1) $p = x$ con $x \in X$, entonces $g(x) = f(x) = f^\#(x)$

(2) $p = \sigma$ para algún $\sigma \in \Sigma_0$, entonces $g(\sigma^{\mathbf{T}_\Sigma(X)}) = \sigma^{\mathbf{A}} = f^\#(\sigma^{\mathbf{T}_\Sigma(X)})$

(3) $p = \sigma((p_i)_{i\in n})$ para un único $\sigma \in \Sigma_n$ y una familia de términos $(p_i)_{i\in n} \in \mathrm{T}_\Sigma(X)^n$, entonces:

$$g(\sigma^{\mathbf{T}_\Sigma(X)}((p_i)_{i\in n})) = \sigma^{\mathbf{A}}((f^\#(p_i))_{i\in n}) = f^\#(\sigma^{\mathbf{T}_\Sigma(X)}((p_i)_{i\in n})).$$

Es decir, para todo término $p \in \mathrm{T}_\Sigma(X)$, se cumple que $g(p) = f^\#(p)$. Por lo tanto: $g = f^\#$. $\square$

Este resultado será clave a lo largo del trabajo ya que asegura la existencia de un homomorfismo único entre cualquier álgebra de términos y cualquier álgebra con la misma signatura siempre que exista una aplicación del conjunto de variables en esta álgbra. Es decir, gracias a este resultado, sabemos que dada una aplicación de un conjunto de variables en una Σ-álgebra, existe una única interpretación de las variables en esa álgebra.

En los capítulos que siguen definiremos distintas signaturas algebraicas, Σ, y dotaremos al conjunto de las relaciones de estructura de Σ-álgebra para la signatura definida en cada caso, asociándole determinadas operaciones. En cada capítulo de los que veremos a continuación se definirá al menos otra álgebra con la misma estructura. Gracias a los homomorfismos entre estas Σ-álgebras y la Σ-álgebra de términos asociada, cuya existencia podemos asegurar gracias a la *propiedad universal del álgebra de términos*, podremos probar los distintos teoremas de decibilidad. Serán estos teoremas de decibilidad los que nos den la equivalencia entre la validez inecuaciones en relaciones y diferentes procedimientos en lenguajes, grafos, lenguajes de grafos, etc.

Capítulo 3

Decibilidad en álgebras de Kleene

En este capítulo definiremos la signatura de un álgebra de Kleene. A continuación veremos que se puede construir un álgebra con el conjunto de las relaciones y determinadas operaciones de las estudiadas en el primer capítulo, tal que presente estructura de álgebra de Kleene. En la siguiente sección definiremos los lenguajes y se dotará al conjunto de todos los lenguajes sobre un alfabeto A de estructura de álgebra de Kleene, definiendo las operaciones pertinentes entre lenguajes. Asimismo, definiremos una aplicación del conjunto de variables al conjunto de los lenguajes de forma que, por la propiedad universal del álgebra de términos, podremos extenderla a un homomorfismo. Por último probaremos el Teorema de Decibilidad en Álgebras de Kleene que asegurará la validez de una ley relacional si y solo si se cumple la equivalente inecuación entre lenguajes. Serán el homomorfismo que extiende la aplicación definida en esta capítulo y el homomorfismo que extiende una interpretación relacional cualquiera, $f^{\#}$, los que nos permitan determinar esa equivalencia. Basaremos el contenido de este capítulo en el trabajo realizado por Jean-Éric Pin en *Mathematical Foundations of Automata Theory* [14].

Definición 3.0.1. Definimos la *signatura de Kleene* como la signatura $\Sigma^{\mathrm{Kl}} = (\Sigma_n^{\mathrm{Kl}})_{n\in\mathbb{N}}$ tal que $\Sigma_2^{\mathrm{Kl}} = \{+, \cdot\}, \Sigma_1^{\mathrm{Kl}} = \{^*\}, \Sigma_0^{\mathrm{Kl}} = \{0, 1\}$ y $\Sigma_n^{\mathrm{Kl}} = \emptyset$ para $n > 2$. Llamaremos *álgebra de Kleene* a toda Σ^{Kl}-álgebra.

Notación. A lo largo del trabajo aparecerán unos y ceros como operaciones constantes en distintas álgebras. Cuando esto pueda crear confusión escribiremos a las constantes un superíndice indicando el álgebra en la que están actuando.

3.1. Álgebras de Klenee para relaciones

Sea C un conjunto, consideramos el conjunto $\mathcal{P}(C \times C)$, como hemos visto en el capítulo 1, este es el conjunto que contiene todas las relaciones en C. El conjunto de todas las relaciones sobre un conjunto C es un álgebra de Kleene con las operaciones binarias unión y composición, la operación unaria clausura reflexivo-transitiva y las constantes relación vacía y relación identidad. Es decir,

$$\mathcal{P}(\mathbf{C} \times \mathbf{C}) = (\mathcal{P}(C \times C), \cup, \cdot, ^*, 0, 1)$$

es un álgebra de Kleene.

Recordamos las operaciones sobre relaciones con las que trabajaremos en este capítulo:

- *Unión:* $\mathcal{R} \cup \mathcal{S} = \{(a, b) \in C \times C \mid a\mathcal{R}b$ ó $a\mathcal{S}b\}$.
- *Composición:* $\mathcal{R} \cdot \mathcal{S} = \{(a, b) \in C \times C \mid \exists c \in C : a\mathcal{R}c$ y $c\mathcal{S}b\}$.
- *Clausura reflexivo-transitiva:* $\mathcal{R}^* = \{(a, b) \in C \times C \mid \exists c_0, \ldots, c_n \in C :$ $: c_0 = a, c_n = b$ y $\forall i \in n, c_i\mathcal{R}c_{i+1}\}$.
- *Relación vacía:* $0 = \emptyset$.
- *Relación identidad:* $1 = \{(a, b) \in C \times C \mid a = b\}$.

De este forma, podemos expresar las ecuaciones e inecuaciones que hemos visto al final del capítulo 1 y que planteaban dificultades a la hora de decidir sobre su validez, como ecuaciones e inecuaciones entre términos de un álgebra de Kleene.

En la siguiente sección daremos unas nociones básicas sobre lenguajes que nos permitirán presentar el *Teorema de decibilidad en álgebras de Kleene*. Este teorema asegura la válidez de una inecuación entre relaciones si y solo si se cumple una inecuación entre ciertos lenguajes asociados a esas relaciones. Para poder probarlo necesitaremos, además del contenido de la siguiente sección, el Lema que se da a continuación:

Lema 3.1.1. $(\mathcal{P}(C \times C), \cdot, 1)$ *es un monoide.*

Demostración. Para comprobar que $(\mathcal{P}(C \times C), \cdot, 1)$ es un monoide hemos de ver que la operación binaria composición de relaciones, $\cdot$, cumple la propiedad asociativa y que el elemento relación identidad, 1, es neutro para esta operación.

Dadas las relaciones $\mathcal{R}, \mathcal{R}', \mathcal{R}'' \in A$ se cumple que $\mathcal{R} \cdot (\mathcal{R}' \cdot \mathcal{R}'') = (\mathcal{R} \cdot \mathcal{R}') \cdot \mathcal{R}''$ como ya vimos en el capítulo dedicado a las relaciones en la sección 1.2.

Además, si $\mathcal{R} = \{(a,b) \in C \times C \mid a\mathcal{R}b\}$, entonces:

$$\begin{aligned}
\mathcal{R} \cdot 1 &= \{(a,b) \in C \times C \mid \exists c \in C\colon a\mathcal{R}c \text{ y } c1b\} \\
&= \{(a,b) \in C \times C \mid \exists c \in C\colon a\mathcal{R}c \text{ y } c = b\} \\
&= \{(a,b) \in C \times C \mid a\mathcal{R}b\} \\
&= \mathcal{R}
\end{aligned}$$

Y, por otro lado, $1 \cdot \mathcal{R} = \mathcal{R}$ por un razonamiento similar.

Así $(\mathcal{P}(C \times C), \cdot, 1)$ es un monoide. □

3.2. Lenguajes

En esta sección presentamos los lenguajes. Con el conjunto de lenguajes sobre un alfabeto y ciertas operaciones que definiremos a lo largo de la sección, construiremos un álgebra que también está dotada de estructura de álgebra de Kleene.

Definición 3.2.1. Sea A un conjunto que denominaremos *alfabeto*. El *monoide libre en A*, denotado por $\mathbf{A}^*$, es $(A^*, \curlywedge, \lambda)$ donde:

- A^* es el *conjunto de todas las palabras en A*, esto es, el conjunto de todas las aplicaciones $w : n \longrightarrow A,\ n \in \mathbb{N}$.

$$A^* = \bigcup_{n \in \mathbb{N}} \mathrm{Hom}(n, A)$$

  La aplicación w es una *palabra*. Llamamos a n *longitud de la palabra*.

- $\curlywedge$ es la *concatenación de palabras en A*, es decir, $\curlywedge$ es la operación binaria en A^* que envía un par de palabras (w, v) en A a la palabra $w \curlywedge v : |w| + |v| \longrightarrow A$. Donde $|w|$ y $|v|$ son las *longitudes* (o dominios) de las aplicaciones w y v, respectivamente.

$$\begin{aligned}
w \curlywedge v : |w| + |v| &\longrightarrow A \\
i \quad &\longmapsto \begin{cases} w_i & \text{si } 0 \leq i < |w| \\ v_{i-|w|} & \text{si } |w| \leq i < |w| + |v| \end{cases}
\end{aligned}$$

- λ es la *palabra vacía en A* que se define como la única aplicación de $\emptyset$ en A. Es el elemento neutro para la concatenación de palabras.

Ejemplo 3.2.2. Sea el alfabeto $A = \{c, a, s\}$.

La palabra $w : 4 \longrightarrow A$ tal que $w(0) = c, w(1) = a, w(2) = s$ y $w(3) = a$ se representa normalente como $w = casa$. La longitud de la palabra es $|w| = 4$.

Sea v otra palabra en A, $v : 2 \longrightarrow A$ tal que $v(0) = c$ y $v(1) = a$, es decir $v = ca$, con longitud $|v| = 2$.

Entonces, la concatenación de w con v es la palabra:

$$w \curlywedge v : 6 \longrightarrow A \text{ tal que } w \curlywedge v = casaca.$$

De la misma forma que hicimos con las relaciones, vemos el siguiente lema que nos permitirá utilizar la *Propiedad Universal del Monoide Libre* para hallar la equivalencia de la que venimos hablando entre relaciones y lenguajes.

Lema 3.2.3. $(A^*, \curlywedge, \lambda)$ *es un monoide.*

Demostración. Para comprobar que $(A^*, \curlywedge, \lambda)$ es un monoide hemos de ver que la operación binaria concatenación de palabras, $\curlywedge$, cumple la propiedad asociativa y que el elemento palabra vacía, λ, es neutro para esta operación.

Dadas las palabras $w, v, u \in A^*$, entonces $w\colon |w| \longrightarrow A$, $v\colon |v| \longrightarrow A$ y $u\colon |u| \longrightarrow A$. Veamos que se cumple $w \curlywedge (v \curlywedge u) = (w \curlywedge v) \curlywedge u$:

$$\begin{aligned} w \curlywedge (v \curlywedge u) :&|w| + (|v| + |u|) \longrightarrow A \\ &i \quad \longmapsto \begin{cases} w_i & \text{si } 0 \leq i < |w| \\ (v \curlywedge u)_{i-|w|} & \text{si } |w| \leq i < |w| + (|v| + |u|) \end{cases} \end{aligned}$$

Y, como

$$\begin{aligned} v \curlywedge u :&|v| + |u| \longrightarrow A \\ &j \quad \longmapsto \begin{cases} v_j & \text{si } 0 \leq j < |v| \\ u_{j-|v|} & \text{si } |v| \leq j < |v| + |u| \end{cases} \end{aligned}$$

Entonces:

$$\begin{aligned} w \curlywedge (v \curlywedge u) :&|w| + |v| + |u| \longrightarrow A \\ &i \quad \longmapsto \begin{cases} w_i & \text{si } 0 \leq i < |w| \\ v_{i-|w|} & \text{si } |w| \leq i < |w| + |v| \\ u_{i-(|w|+|v|)} & \text{si } |w| + |v| \leq i < |w| + |v| + |u| \end{cases} \end{aligned}$$

De la misma forma,

$$\begin{aligned}(w \curlywedge v) \curlywedge u :&(|w| + |v|) + |u| \longrightarrow A \\ i \quad &\longmapsto \begin{cases} (w \curlywedge v)_i & \text{si } 0 \leq i < (|w| + |v|) \\ u_{i-(|w|+|v|)} & \text{si } (|w| + |v|) \leq i < (|w| + |v|) + |u| \end{cases}\end{aligned}$$

Y, como

$$\begin{aligned}w \curlywedge v :&|w| + |v| \longrightarrow A \\ j \quad &\longmapsto \begin{cases} w_j & \text{si } 0 \leq j < |w| \\ v_{j-|w|} & \text{si } |w| \leq j < |w| + |v| \end{cases}\end{aligned}$$

Entonces:

$$\begin{aligned}w \curlywedge (v \curlywedge u) :&|w| + |v| + |u| \longrightarrow A \\ i \quad &\longmapsto \begin{cases} w_i & \text{si } 0 \leq i < |w| \\ v_{i-|w|} & \text{si } |w| \leq i < |w| + |v| \\ u_{i-(|w|+|v|)} & \text{si } |w| + |v| \leq i < |w| + |v| + |u| \end{cases}\end{aligned}$$

Y así, vemos que $w \curlywedge (v \curlywedge u) = (w \curlywedge v) \curlywedge u$.

Por otro lado, la palabra vacía, λ, se define como la única aplicación $\lambda \colon 0 \longrightarrow A$. Por tanto la concatenación de w y λ es la palabra:

$$\begin{aligned}w \curlywedge \lambda :&|w| + |0| \longrightarrow A \\ i \quad &\longmapsto \begin{cases} w_i & \text{si } 0 \leq i < |w| \\ \lambda_{i-|w|} & \text{si } |w| \leq i < |w| \end{cases}\end{aligned}$$

Es decir:

$$\begin{aligned}w \curlywedge \lambda :&|w| \longrightarrow A \\ i \quad &\longmapsto w_i \quad \text{si } 0 \leq i < |w|\end{aligned}$$

Así, $w \curlywedge \lambda = w$. De forma equivalente se prueba que $\lambda \curlywedge w = w$. Por tanto, λ es el elemento neutro para la concatenación de palabras.

Así, $(A^*, \curlywedge, \lambda)$ es un monoide. □

Hemos visto que tanto $(\mathcal{P}(C \times C), \cdot, 1)$ como $(A^*, \curlywedge, \lambda)$ son monoides. A continuación probamos la *Propiedad Universal del Monoide Libre* que, de forma similar a la propiedad universal del álgebra de términos, asegura la existencia de un homomorfismo del monoide libre en otro monoide como extensión de una aplicación dada entre el alfabeto A y el segundo monoide.

Utilizaremos esta propiedad para obtener un homomorfismo entre los dos monoides estudiados en este capítulo.

Proposición 3.2.4 (Propiedad Universal del Monoide Libre.)**.** *Sea la aplicación $f : A \longrightarrow \mathbf{M}$ del alfabeto A en el monoide $\mathbf{M} = (M, \cdot, 1)$, entonces existe un único homomorfismo de monoides.*

$$f^{\natural} \colon \mathbf{A}^{*} \longrightarrow \mathbf{M}$$

tal que $f^{\natural} \circ \mu_A = f$. Es decir, tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "\mu_A"'] & \mathbf{M} \\ & \mathbf{A}^{*} \arrow[u, "f^{\natural}"'] \end{tikzcd}$$

donde $\mu_A : A \longrightarrow \mathbf{A}^{*}$ es la aplicación que lleva el elemento $a \in A$ a la palabra $a \in \mathbf{A}^{*}$ de longitud $n = 1$.

Demostración. Veamos en primer lugar la existencia:

Sea $w \in A^{*}$ una palabra, entonces w puede ser $w = \lambda$, donde $\lambda \in A$ es la palabra vacía, o $w = w_0 \dots w_{|w|-1}$.

Definimos la aplicación $f^{\natural}$ como:

(1) $f^{\natural}(\lambda) = 1^{\mathbf{M}}$.

(2) $f^{\natural}(w) = f^{\natural}(w_0 \dots w_{|w|-1}) = f(w_0) \cdot \ldots \cdot f(w_{|w|-1})$.

Falta probar que $f^{\natural} \colon \mathbf{A}^{*} \longrightarrow \mathbf{M}$ es un homomorfismo y que se cumple que $f^{\natural} \circ \mu_A = f$.

Sean las palabras $u, v \in A^{*}$ tales que $u = u_0 \dots u_{|u|-1}$ y $v = v_0 \dots v_{|v|-1}$, $f^{\natural}$ es homomorfismo si conserva las operaciones fundamentales, es decir, si se cumple:

$$f^{\natural}(\lambda) = 1^{\mathbf{M}}.$$
$$f^{\natural}(u \curlywedge v) = f^{\natural}(u) \cdot f^{\natural}(v).$$

Veámoslo:

$f^{\natural}(\lambda) = 1^{\mathbf{M}}$ por la construcción de $f^{\natural}$.

$$
\begin{aligned}
f^{\natural}(u \curlywedge v) &= f^{\natural}(u_0 \ldots u_{|u|-1} v_0 \ldots v_{|v|-1}) \\
&= f(u_0) \cdot \ldots \cdot f(u_{|u|-1}) \cdot f(v_0) \cdot \ldots \cdot f(v_{|v|-1}) \\
&= \Big(f(u_0) \cdot \ldots \cdot f(u_{|u|-1}) \Big) \cdot \Big(f(v_0) \cdot \ldots \cdot f(v_{|v|-1}) \Big) \\
&= f^{\natural}(u) \cdot f^{\natural}(v).
\end{aligned}
$$

Así, $f^{\natural}$ es homomorfismo.

Además, si $a \in A$:

$$f^{\natural} \circ \mu_A(a) = f^{\natural}(a) = f(a), \quad \text{entonces:} \quad f^{\natural} \circ \mu_A = f.$$

Probemos ahora la unicidad:

Sea $g : \mathbf{A}^* \longrightarrow \mathbf{M}$ un homomorfismo que extiende a f, esto es $g \circ \mu_A = f$. Sea $w \in A^*$ una palabra, si:

(1) $w = \lambda$, entonces $g(\lambda) = 1^{\mathbf{M}} = f^{\natural}(\lambda)$.

(2) $w = w_0 \ldots w_{|w|-1}$, entonces:

$$
\begin{aligned}
g(w_0 \ldots w_{|w|-1}) &= g(w_0 \curlywedge \cdots \curlywedge w_{|w|-1}) \\
&= g(w_0) \cdot \ldots \cdot g(w_{|w|-1}) \\
&= g \circ \mu_A(w_0) \cdot \ldots \cdot g \circ \mu_A(w_{|w|-1}) \\
&= f(w_0) \cdot \ldots \cdot f(w_{|w|-1}) \\
&= f^{\natural}(w).
\end{aligned}
$$

Es decir, para toda palabra $w \in A^*$, se cumple que $g(w) = f^{\natural}(w)$. Por lo tanto: $g = f^{\natural}$. Y así, el homomorfismo existe y es único. $\square$

Notación. Siguiendo la tradición en ciencias de la computación llamaremos *lenguajes* a los subconjuntos $L \subseteq A^*$.

En particular, $\emptyset$ y A^* son también lenguajes en A^*.

Veamos algún ejemplo de lenguajes.

Ejemplo 3.2.5. Sea el alfabeto $A = \{m, a, p, q, u, e, s, r, o\}$, los siguientes conjuntos son lenguajes:

(1) $L = \{mapa, peque, pero, seso, queso\} \subseteq \mathbf{A}^*$.

(2) $K = \{pam, ro, sse, uesro\} \subseteq \mathbf{A}^*$.

A continuación definimos las distintas operaciones que se pueden realizar con lenguajes en A^*.

Definición 3.2.6. Sean $L, K \subseteq A^*$ dos lenguajes, se definen las siguientes operaciones:

- *Unión:* $L \cup K = \{w \in A^* \mid w \in L \text{ ó } w \in K\}$.
- *Producto:* $L \cdot K = \{w \in A^* \mid w = v \curlywedge u, v \in L \text{ y } u \in K\}$.
- *Potencia:* Para $n \in \mathbb{N}$ se define la potencia n-ésima de un lenguaje L de forma recurrente como sigue:

$$\begin{array}{lcl} L^0 & = & \{\lambda\}. \\ L^{n+1} & = & L^n \cdot L. \end{array}$$

- *Producto estrella:* $L^* = \bigcup_{n \in \mathbb{N}} L^n$.

Y las operaciones constantes:

- *Cero:* $0 = \emptyset$.
- *Identidad:* $1 = \{\lambda\}$.

Veamos como actúan estas operaciones sobre los lenguajes del ejemplo anterior.

Ejemplo 3.2.7. Sean A, L y K, el alfabeto y los lenguajes, respectivamente, del ejemplo 3.2.5. Entonces:

La *unión de L y K* es:

$$L \cup K = \{mapa, peque, pero, seso, queso, pam, ro, sse, uesro\}.$$

Algunas palabras del *producto de L por K* son:

$$mapapam, pequepam, quesosse, mapauesro \in L \cdot K.$$

Algunas palabras del *producto estrella de L* son:

$$mapapequeseso, quesoperoseso, mapa, quesoquesoquesoqueso \in L^*.$$

El conjunto $\mathcal{P}(A^*)$ es el conjunto de todos los lenguajes en A^*. Notamos que $\mathcal{P}(A^*)$ es también un álgebra de Kleene con las operaciones binarias unión y producto, la operación unaria producto estrella, y las constantes cero y palabra vacía. Es decir,

$$\mathcal{P}(\mathbf{A}^*) = (\mathcal{P}(A^*), \cup, \cdot, ^*, 0, \lambda)$$

es un álgebra de Kleene.

Así, tanto las relaciones sobre un conjunto como los lenguajes sobre un alfabeto, tienen estructura de álgebra de Kleene. En la siguiente sección veremos el teorema que nos permitirá utilizar esto para decidir sobre la validez de una ecuación entre relaciones demostrando que se cumple la ecuación equivalente en lenguajes.

3.3. Teorema de decibilidad en álgebras de Kleene

Hemos hablado con frecuencia, a lo largo del trabajo de ley universalmente válida para relaciones. En la definición que sigue expresamos formalmente este concepto para las relaciones entendidas como términos de un álgebra de Kleene.

Definición 3.3.1. Dados dos términos $p, q \in \mathrm{T}_{\Sigma \mathrm{Kl}}(X)$, diremos que la inecuación $p \subseteq q$ es *universalmente válida para modelos relacionales*, y escribiremos $\mathrm{Rel} \models p \subseteq q$ si y solo si, para todo conjunto C y para toda aplicación $f : X \longrightarrow \mathcal{P}(C \times C)$ se tiene que $f^{\#}(p) \subseteq f^{\#}(q)$.

Veamos ahora como ejemplo la demostración de la validez universal de una ecuación en modelos relacionales. Después del *Teorema de Decibilidad en Álgebras de Kleene* probaremos de nuevo esta ecuación pero utilizando los lenguajes asociados a las relaciones a cada lado de la ecuación.

Ejemplo 3.3.2. Sean $x, y, z \in \mathrm{T}_{\Sigma \mathrm{Kl}}(X)$ términos en un álgebra de Kleene. Queremos probar que la siguiente ecuación entre términos es universalmente váida en modelos relacionales:

$$\mathrm{Rel} \models x \cdot (y \cdot z) = x \cdot y + x \cdot z$$

Consideramos la interpretación relacional $f \colon X \longrightarrow \mathcal{P}(C \times C)$ que lleva, mediante el homomorfismo $f^{\#}$, los términos x, y, z a las relaciones $\mathcal{R}, \mathcal{S}, \mathcal{T}$ sobre un conjunto C cualquiera, respectivamente. Por tanto, podemos expresar la ecuación entre los términos x, y, z como la siguiente ecuación entre relaciones:

$$\mathcal{R} \cdot (\mathcal{S} \cup \mathcal{T}) = \mathcal{R} \cdot \mathcal{S} \cup \mathcal{R} \cdot \mathcal{T}$$

Probemos que se trata de una ecuación universalmente válida para cualquier modelo relacional.

Demostración. Para probar que se cumple la igualdad, probaremos ambas inclusiones. En primer lugar, veamos que dado $(a, b) \in \mathcal{R} \cdot (\mathcal{S} \cup \mathcal{T})$ entonces $(a, b) \in \mathcal{R} \cdot \mathcal{S} \cup \mathcal{R} \cdot \mathcal{T}$.

Consideramos $(a, b) \in \mathcal{R} \cdot (\mathcal{S} \cup \mathcal{T})$, entonces existe $c \in C$ tal que $a\mathcal{R}c$ y $c(\mathcal{S} \cup \mathcal{T})b$, así, $c\mathcal{S}b$ ó $c\mathcal{T}b$. Si $a\mathcal{R}c$ y $c\mathcal{S}b$, entonces $(a, b) \in \mathcal{R} \cdot \mathcal{S}$. Por otro lado, si $a\mathcal{R}c$ y $c\mathcal{T}b$, entonces $(a, b) \in \mathcal{R} \cdot \mathcal{T}$. Por tanto si $(a, b) \in \mathcal{R} \cdot (\mathcal{S} \cup \mathcal{T})$ entonces $(a, b) \in \mathcal{R} \cdot \mathcal{S}$ o $(a, b) \in \mathcal{R} \cdot \mathcal{T}$. Así $(a, b) \in \mathcal{R} \cdot \mathcal{S} \cup \mathcal{R} \cdot \mathcal{T}$.

Por otro lado, veamos que si $(a, b) \in \mathcal{R} \cdot \mathcal{S} \cup \mathcal{R} \cdot \mathcal{T}$ entonces $(a, b) \in \mathcal{R} \cdot (\mathcal{S} \cup \mathcal{T})$.

Sea $(a,b) \in \mathcal{R} \cdot \mathcal{S} \cup \mathcal{R} \cdot \mathcal{T}$, entonces $a(\mathcal{R} \cdot \mathcal{S})b$ ó $a(\mathcal{R} \cdot \mathcal{T})b$. Si $a(\mathcal{R} \cdot \mathcal{S})b$, existe $c \in C$ tal que $a\mathcal{R}c$ y $c\mathcal{S}b$ y entonces $(a,b) \in \mathcal{R} \cdot (\mathcal{S} \cup \mathcal{T})$. Si $a(\mathcal{R} \cdot \mathcal{T})b$, existe $d \in C$ tal que $a\mathcal{R}d$ y $d\mathcal{T}b$ y así $(a,b) \in \mathcal{R} \cdot (\mathcal{S} \cup \mathcal{T})$. Por tanto, en cualquier caso, se da la inclusión.

Puesto que se cumplen ambas inclusiones, queda probada la igualdad. $\square$

Como hemos visto, necesitamos la interpretación relacional f que va del conjunto de variables, X, en el conjunto de relaciones $\mathcal{P}(C \times C)$ para poder trasladar una inecuación entre términos de un álgebra de Kleene a una inecuación entre relaciones. De igual manera, necesitaremos una aplicación que vaya del conjunto de variables en el de lenguajes para poder proceder con ellos. La aplicación de la siguiente definición lleva los elementos $x \in X$ a lenguajes en $\mathcal{P}(X^*)$.

Definición 3.3.3. Definimos la aplicación $[\cdot]$ como sigue:

$$\begin{array}{rcl} [\cdot] : X & \longrightarrow & \mathcal{P}(X^*) \\ x & \longmapsto & \{x\} \end{array}$$

Propiedad 3.3.4. *Sea la aplicación $[\cdot]$ de la definición anterior, como $\mathcal{P}(X^*)$ es un álgebra de Kleene, sabemos, por la propiedad universal del álgebra de términos, que $[\cdot]$ puede extenderse de forma única a un homomorfismo de álgebras de Kleene:*

$$[\cdot]^\# : \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X) \longrightarrow \mathcal{P}(X^*)$$

tal que $[\cdot]^\# \cdot \eta_X = [\cdot]$.

$$\begin{tikzcd} X \arrow[r, "{[\cdot]}"] \arrow[dr, "\eta_X"'] & \mathcal{P}(X^*) \\ & \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X) \arrow[u, "{[\cdot]^\#}"'] \end{tikzcd}$$

Así, mediante los homomorfismos que extienden las aplicaciones f y $[\cdot]$, podemos ir del conjunto de variables X en el álgebra de términos $\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$ y de esta bien a $\mathcal{P}(C \times C)$, bien a $\mathcal{P}(X^*)$.

El *Teorema de Decibilidad en Álgebras de Kleene* asegura que una inecuación entre dos términos de un álgebra de Kleene es universalmente válida para todo modelo relacional si y solo si se cumple la misma inecuación para los lenguajes asociados a esos términos mediante el homomorfismo $[\cdot]^\#$ que extiende a la aplicación $[\cdot]$.

Teorema 3.3.5. *Dados dos términos $p, q \in \mathrm{T}_{\Sigma\mathrm{Kl}}(X)$, se cumple:*

$$\mathrm{Rel} \models p \subseteq q \quad \textit{si y solo si} \quad [p]^{\#} \subseteq [q]^{\#}.$$

Antes de empezar con la prueba veremos dos lemas técnicos.

Lema 3.3.6. *Para todo lenguaje $L \subseteq X^*$ y para todo $n \in \mathbb{N}$ se cumple la siguiente igualdad entre relaciones:*

$$\{(w, wv) \mid w \in X^*, v \in L\}^n = \{(w, wv) \mid w \in X^*, v \in L^n\}.$$

Demostración. Por inducción sobre $n \in \mathbb{N}$.

Para $n = 0$:

$$\begin{array}{rcl} \{(w, wv) \mid w \in X^*, v \in L\}^0 & = & 1 \\ & = & \{(w, w) \mid w \in X^*\} \\ & = & \{(w, wv) \mid w \in X^*, v \in L^0\}. \end{array}$$

Suponemos cierto para n y probamos que para $n + 1$ se cumple:

$$\{(w, wv) \mid w \in X^*, v \in L\}^{n+1} = \{(w, wv) \mid w \in X^*, v \in L^{n+1}\}$$

$$\begin{array}{l} \{(w, wv) \mid w \in X^*, v \in L\}^{n+1} \\ = \{(w, wv) \mid w \in X^*, v \in L\}^n \cdot \{(w, wv) \mid w \in X^*, v \in L\} \\ = \{(w, wv) \mid w \in X^*, v \in L^n\} \cdot \{(w, wv) \mid w \in X^*, v \in L\} \end{array}$$

donde la última igualdad se debe a la hipótesis inductiva.

Esta operación consistente en la composición de dos relaciones da como resultado una nueva relación. Veamos que esta nueva relación es precisamente $\{(w, wv) \mid w \in X^*, v \in L^{n+1}\}$.

Para simplificar llamamos $\mathcal{R}_1 = \{(w, wv) \mid w \in X^*, v \in L^n\}$ y $\mathcal{R}_2 = \{(w, wv) \mid w \in X^*, v \in L\}$. La relación que se obtiene de la composición de estas es la siguiente:

$$\{(w, w') \mid \exists u \in X^* : w\mathcal{R}_1 u \text{ y } u\mathcal{R}_2 w'\}.$$

Por cumplirse $w\mathcal{R}_1 u$, se tiene que $u = wv'$ con $w \in X^*$ y $v' \in L^n$. Así, $u\mathcal{R}_2 w' \equiv wv'\mathcal{R}_2 w'$. Y por tanto $w' = wv'v''$ con $w \in X^*$, $v' \in L^n$ y $v'' \in L$. Podemos reescribir $w' = wv$ con $v = v'v'' \in L^n \cdot L = L^{n+1}$. Y así,

$$\mathcal{R}_1 \cdot \mathcal{R}_2 = \{(w, wv) \mid w \in X^*, v \in L^{n+1}\}.$$

Y por tanto queda demostrado el lema. $\square$

En particular se cumple:

Corolario 3.3.7. $\{(w, wv) |\ w \in X^*, v \in L\}^* = \{(w, wv) |\ w \in X^*, v \in L^*\}$.

Veamos el segundo lema:

Lema 3.3.8. *Sean X y C conjuntos no vacíos y sea $f^\natural \colon X^* \longrightarrow \mathcal{P}(C \times C)$ el único homomorfismo de monoides que extiende a $f \colon X \longrightarrow \mathcal{P}(C \times C)$ tal que $f^\natural \circ \mu_A = f$ (como vimos en el capítulo anterior). Entonces, para todo lenguaje $L \subseteq X^*$ y para todo $n \in \mathbb{N}$ se cumple la siguiente igualdad entre relaciones:*

$$\Big(\bigcup_{v \in L} f^\natural(v)\Big)^n = \bigcup_{v \in L^n} f^\natural(v).$$

Demostración. Sea $\mathcal{R} \in \bigcup_{v \in L^n} f^\natural(v)$, entonces existe $v^\mathcal{R} \in L^n$ tal que $f^\natural(v^\mathcal{R}) = \mathcal{R}$. Como $v^\mathcal{R} \in L^n$, entonces $v^\mathcal{R} = v_0^m \dots v_{n-1}^\mathcal{R}$ con $v_i^\mathcal{R} \in L$ para todo $i \in n$. Así,

$$\mathcal{R} = f^\natural(v^\mathcal{R}) = f^\natural(v_0^\mathcal{R} \dots v_{n-1}^\mathcal{R}) = f^\natural(v_0^\mathcal{R}) \cdot \dots \cdot f^\natural(v_{n-1}^\mathcal{R})$$

Y como $f^\natural(v_i^\mathcal{R}) \in \bigcup_{v \in L} f^\natural(v)$, entonces:

$$\mathcal{R} = f^\natural(v_0^\mathcal{R}) \cdot \dots \cdot f^\natural(v_{n-1}^\mathcal{R}) \in \Big(\bigcup_{v \in L} f^\natural(v)\Big)^n$$

Veamos la otra inclusión.

Sea $\mathcal{R} \in \Big(\bigcup_{v \in L} f^\natural(v)\Big)^n = \bigcup_{v \in L} f^\natural(v) \cdot \dots \cdot \bigcup_{v \in L} f^\natural(v)$. Entonces existen $v_0, \dots, v_{n-1} \in L$ tales que $\mathcal{R} = f^\natural(v_0) \cdot \dots \cdot f^\natural(v_{n-1})$.

Sea $v^\mathcal{R} = v_0 \dots v_{n-1} \in L^n$. Entonces,

$$\mathcal{R} = f^\natural(v_0) \cdot \dots \cdot f^\natural(v_{n-1}) = f^\natural(v^\mathcal{R}) \in \bigcup_{v \in L^n} f^\natural(v)$$

Y, por tanto, queda demostrada la igualdad. □

En particular se cumple:

Corolario 3.3.9. $\Big(\bigcup_{v \in L} f^\natural(v)\Big)^* = \bigcup_{v \in L^*} f^\natural(v)$.

Ahora estamos en condiciones de demostrar el primer teorema de decibilidad: *Teorema de Decibilidad en Álgebras de Kleene.*

Recordemos el teorema:

Teorema 3.3.5 *Dados dos términos $p, q \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, se cumple:*

$$\mathrm{Rel} \models p \subseteq q \quad \textit{si y solo si} \quad [p]^\# \subseteq [q]^\#.$$

Demostración. Supongamos que Rel $\models p \subseteq q$. Entonces, para todo conjunto C y para toda asignación de variables $f : X \longrightarrow \mathcal{P}(C \times C)$ se tiene que $f^{\#}(p) \subseteq f^{\#}(q)$.

Vamos a encontrar un conjunto C y una aplicación $f : X \longrightarrow \mathcal{P}(C \times C)$ tal que si $f^{\#}(p) \subseteq f^{\#}(q)$ entonces se cumpla $[p]^{\#} \subseteq [q]^{\#}$.

Tomamos $C = X^*$ y definimos la siguiente asignación de variables,

$$\begin{array}{rccl} f: & X & \longrightarrow & \mathcal{P}(X^* \times X^*) \\ & x & \longmapsto & \{(w, wx) \in X^* \times X^* \mid w \in X^*\} \end{array}$$

Y, por hipótesis, se cumple que $f^{\#}(p) \subseteq f^{\#}(q)$.

<u>Afirmación 1:</u> Para todo término $r \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$ se tiene que

$$f^{\#}(r) = \{(w, wv) \in X^* \times X^* \mid v \in [r]^{\#}\}$$

Demostración. Demostraremos esta afirmación por inducción sobre la estructura de r. Notamos que el término r puede ser de la forma:

(1) $r = x$ para alguna variable $x \in X$.

(2) $r = 0^{\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)}$.

(3) $r = 1^{\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)}$.

(4) $r = s^*$ para algún $s \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$.

(5) $r = s + t$ para algunos términos $s, t \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$.

(6) $r = s \cdot t$ para algunos términos $s, t \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$.

Comprobaremos caso por caso.

(1) Sea $r = x$ una variable, entonces:

$$\begin{array}{rl} f^{\#}(x) = & f^{\#} \circ \eta_X(x) \\ = & f(x) = \{(w, wx) \in X^* \times X^* \mid w \in X^*\} \end{array}$$

Además, como $[x]^{\#} = \{x\}$, se tiene que $x \in [x]^{\#}$.

(2) Sea r el cero del álgebra de términos de Kleene, $r = 0^{\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)}$, entonces:

$$\begin{array}{rcl} f^{\#}(0^{\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)}) & = & 0^{\mathcal{P}(X^* \times X^*)} \\ & = & \emptyset \\ & = & \{(w, wv) \in X^* \times X^* \mid v \in [0]^{\#}\} \end{array}$$

ya que $[0]^{\#} = \emptyset$.

(3) Sea r el término identidad, $r = 1^{\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)}$, entonces:

$$\begin{aligned} f^{\#}(1^{\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)}) = {} & 1^{\mathcal{P}(X^* \times X^*)} \\ = {} & \{(w,w) \in X^* \times X^* \mid w \in X^*\} \\ = {} & \{(w,w\lambda) \in X^* \times X^* \mid w \in X^*\} \\ = {} & \{(w,wv) \in X^* \times X^* \mid w \in X^*, v \in [\lambda]^{\#}\} \end{aligned}$$

ya que $[\lambda]^{\#} = \{\lambda\}$.

(4) Sea $r = s^*$, el producto estrella de un término $s \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, entonces:

$$\begin{aligned} f^{\#}(s^*) = {} & (f^{\#}(s))^* \\ = {} & \{(w,wv) \in X^* \times X^* \mid v \in [s]^{\#}\}^* \\ \underset{(*_1)}{=} {} & \{(w,wv) \in X^* \times X^* \mid v \in [s^*]^{\#}\}. \end{aligned}$$

$(*_1)$ Aplicando el Corolario 3.3.7 y que $[\cdot]^{\#}$ es homomorfismo.

(5) Sea $r = s + t$ el término resultante de la suma de los términos $s, t \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, entonces:

$$\begin{aligned} & f^{\#}(s+t) = \\ & = f^{\#}(s) \cup f^{\#}(t) \\ & = \{(w,wv) \in X^* \times X^* \mid v \in [s]^{\#}\} \cup \{(w,wv) \in X^* \times X^* \mid v \in [t]^{\#}\} \\ & = \{(w,wv) \in X^* \times X^* \mid v \in [s]^{\#} \text{ ó } v \in [t]^{\#}\}. \end{aligned}$$

Si $v \in [s]^{\#}$ ó $v \in [t]^{\#}$, entonces $v \in [s]^{\#} \cup [t]^{\#}$, y dado que $[\cdot]^{\#}$ es homomorfismo, $[s]^{\#} \cup [t]^{\#} = [s+t]^{\#}$.

Así, $f^{\#}(s+t) = \{(w,wv) \in X^* \times X^* \mid v \in [s+t]^{\#}\}$.

(6) Por último, sea $r = s \cdot t$ el término resultante del producto de los términos $s, t \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, entonces:

$$\begin{aligned} & f^{\#}(s \cdot t) = \\ & = f^{\#}(s) \cdot f^{\#}(t) \\ & = \{(w,wv) \in X^* \times X^* \mid v \in [s]^{\#}\} \cdot \{(w,wv) \in X^* \times X^* \mid v \in [t]^{\#}\}. \end{aligned}$$

Para simplificar llamamos $\mathcal{R}_1 = \{(w,wv) \in X^* \times X^* \mid v \in [s]^{\#}\}$ y $\mathcal{R}_2 = \{(w,wv) \in X^* \times X^* \mid v \in [t]^{\#}\}$.

La relación que se obtiene de la composición de estas es: $\mathcal{R}_1 \cdot \mathcal{R}_2 = \{(w,w') \mid \exists u \in X^* : w\mathcal{R}_1 u \text{ y } u\mathcal{R}_2 w'\}$.

Por cumplirse $w\mathcal{R}_1 u$, se tiene que $u = wv'$ con $w \in X^*$ y $v' \in [s]^\#$. Así, $u\mathcal{R}_2 w' \equiv wv'\mathcal{R}_2 w'$. Y por tanto $w' = wv'v''$ con $w \in X^*$, $v' \in [s]^\#$ y $v'' \in [t]^\#$. Podemos reescribir $w' = wv$ con $v = v'v'' \in [s]^\# \cdot [t]^\# = [s \cdot t]^\#$ ya que $[\cdot]^\#$ es homomorfismo.

Así, $f^\#(s \cdot t) = \{(w, wv) \in X^* \times X^* \mid v \in [s \cdot t]^\#\}$ y queda probada la afirmación. $\square$

En particular se tiene que $v \in [r]^\#$ si y solo si $(\lambda, v) \in f^\#(r)$ para todo término $r \in \mathrm{T}_{\Sigma\mathrm{Kl}}(X)$.

Si $v \in [p]^\#$ entonces $(\lambda, v) \in f^\#(p)$. Así, como $f^\#(p) \subseteq f^\#(q)$ por hipótesis, se tiene que $(\lambda, v) \in f^\#(q)$, y entonces, $v \in [q]^\#$. Por lo tanto $[p]^\# \subseteq [q]^\#$.

Probemos la implicación contraria.

Suponemos ahora que $[p]^\# \subseteq [q]^\#$. Queremos probar que se cumple $\mathrm{Rel} \models p \subseteq q$.

Sea C un conjunto y sea la aplicación $f\colon X \longrightarrow \mathcal{P}(C \times C)$, queremos ver que $f^\#(p) \subseteq f^\#(q)$.

Afirmación 2: Para todo término $r \in \mathrm{T}_{\Sigma\mathrm{Kl}}(X)$ se tiene que

$$f^\#(r) = \bigcup_{v \in [r]^\#} f^\natural(v)$$

Demostración. Demostraremos esta afirmación por inducción sobre la estructura de r. Notamos que el término r puede ser de la forma:

(1) $r = x$ para alguna variable $x \in X$.

(2) $r = 0^{\mathrm{T}_{\Sigma\mathrm{Kl}}(X)}$.

(3) $r = 1^{\mathrm{T}_{\Sigma\mathrm{Kl}}(X)}$.

(4) $r = s^*$ para algún $s \in \mathrm{T}_{\Sigma\mathrm{Kl}}(X)$.

(5) $r = s + t$ para algunos términos $s, t \in \mathrm{T}_{\Sigma\mathrm{Kl}}(X)$.

(6) $r = s \cdot t$ para algunos términos $s, t \in \mathrm{T}_{\Sigma\mathrm{Kl}}(X)$.

Comprobaremos caso por caso.

(1) Sea $r = x$ una variable, entonces:

$$\begin{aligned} f^{\#}(x) = & \ f^{\#} \circ \eta_X(x) \\ = & \ f(x) \\ = & \ f^{\natural}(x) \\ = & \bigcup_{v \in \{x\}} f^{\natural}(v) \\ = & \bigcup_{v \in [x]^{\#}} f^{\natural}(v) \end{aligned}$$

ya que $[x]^{\#} = \{x\}$.

(2) Sea r el cero del álgebra de términos, $r = 0^{\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)}$, entonces:

$$\begin{aligned} f^{\#}(0^{\mathbf{T}_{\Sigma}^{\mathrm{Kl}}}) = & \ 0^{\mathcal{P}(C \times C)} \\ = & \ \emptyset \\ = & \bigcup_{v \in [0]^{\#}} f^{\natural}(v) \end{aligned}$$

ya que $[0]^{\#} = \emptyset$.

(3) Sea r el término identidad, $r = 1^{\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)}$, entonces:

$$\begin{aligned} f^{\#}(1^{\mathbf{T}_{\Sigma}^{\mathrm{Kl}}}) = & \ 1^{\mathcal{P}(C \times C)} \\ = & \ f^{\natural}(\lambda) \\ = & \bigcup_{v \in \{\lambda\}} f^{\natural}(v) \\ = & \bigcup_{v \in [\lambda]^{\#}} f^{\natural}(v) \end{aligned}$$

ya que $[\lambda]^{\#} = \{\lambda\}$.

(4) Sea $r = s^*$, el producto estrella de un término $s \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, entonces:

$$\begin{aligned} f^{\#}(s^*) = & \ (f^{\#}(s))^* \\ = & \ (\bigcup_{v \in [s]^{\#}} f^{\natural}(v))^* \\ \underset{(*_3)}{=} & \bigcup_{v \in [s^*]^{\#}} f^{\natural}(v) \end{aligned}$$

$(*_3)$ Aplicando el Corolario 3.3.9 y que $[\cdot]^{\#}$ es un homomorfismo.

(5) Sea $r = s + t$ el término resultante de la suma de los términos $s, t \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, entonces:

$$\begin{aligned} f^{\#}(s+t) = &\ f^{\#}(s) \cup f^{\#}(t) \\ = &\ (\bigcup_{v \in [s]^{\#}} f^{\natural}(v)) \cup (\bigcup_{v \in [t]^{\#}} f^{\natural}(v)) \\ = &\ \bigcup_{v \in [s]^{\#} \text{ ó } v \in [t]^{\#}} f^{\natural}(v). \end{aligned}$$

Si $v \in [s]^{\#}$ ó $v \in [t]^{\#}$, entonces $v \in [s]^{\#} \cup [t]^{\#}$, y dado que $[\cdot]^{\#}$ es homomorfismo, $[s]^{\#} \cup [t]^{\#} = [s+t]^{\#}$.

Así, $f^{\#}(s+t) = \bigcup_{v \in [s+t]^{\#}} f^{\natural}(v)$.

(6) Sea $r = s \cdot t$ el término resultante del producto de los términos $s, t \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, entonces:

$$\begin{aligned} f^{\#}(s \cdot t) = &\ f^{\#}(s) \cdot f^{\#}(t) \\ = &\ (\bigcup_{v_s \in [s]^{\#}} f^{\natural}(v_s)) \cdot (\bigcup_{v_t \in [t]^{\#}} f^{\natural}(v_t)). \end{aligned}$$

Sea $m \in \bigcup_{v_s \in [s]^{\#}} f^{\natural}(v_s)$, entonces existe $u_s^m \in [s]^{\#}$ tal que $m = f^{\natural}(u_s^m)$ y sea $l \in \bigcup_{v_t \in [t]^{\#}} f^{\natural}(v_t)$, entonces existe $u_t^l \in [t]^{\#}$ tal que $l = f^{\natural}(u_t^l)$. Entonces $m \cdot l \in (\bigcup_{v_s \in [s]^{\#}} f^{\natural}(v_s)) \cdot (\bigcup_{v_t \in [t]^{\#}} f^{\natural}(v_t))$ y, además:

$$m \cdot l = f^{\natural}(u_s^m) \cdot f^{\natural}(u_t^l) = f^{\natural}(u_s^m u_t^l) \in \bigcup_{v \in [s]^{\#} \cdot [t]^{\#}} f^{\natural}(v).$$

Recíprocamente, sea $m \in \bigcup_{v \in [s]^{\#} \cdot [t]^{\#}} f^{\natural}(v)$, entonces existe $v' \in [s]^{\#} \cdot [t]^{\#}$ tal que $m = f^{\natural}(v')$. Y existen $w \in [s]^{\#}$ y $u \in [t]^{\#}$ tales que $v' = wu$. Por tanto:

$$m = f^{\natural}(v') = f^{\natural}(wu) = f^{\natural}(w) \cdot f^{\natural}(u) \in (\bigcup_{v_s \in [s]^{\#}} f^{\natural}(v_s)) \cdot (\bigcup_{v_t \in [t]^{\#}} f^{\natural}(v_t)).$$

Así $(\bigcup_{v_s \in [s]^{\#}} f^{\natural}(v_s)) \cdot (\bigcup_{v_t \in [t]^{\#}} f^{\natural}(v_t)) = \bigcup_{v \in [s]^{\#} \cdot [t]^{\#}} f^{\natural}(v)$. Y dado que $[\cdot]^{\#}$ es homomorfismo: $[s]^{\#} \cdot [t]^{\#} = [s \cdot t]^{\#}$, de lo que sigue:

$$f^{\#}(s \cdot t) = \bigcup_{v \in [s \cdot t]^{\#}} f^{\natural}(v).$$

Dado que se cumple para todo término en $\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, queda probada la Afirmación 2. $\square$

Así, por la Afirmación 2, $f^{\#}(p) = \bigcup_{v \in [p]^{\#}} f^{\natural}(v)$ que está contenido en $\bigcup_{v \in [q]^{\#}} f^{\natural}(v)$ ya que por hipótesis $[p]^{\#} \subseteq [q]^{\#}$. Y, de nuevo por la Afirmación 2, $\bigcup_{v \in [q]^{\#}} f^{\natural}(v) = f^{\#}(q)$. Por lo tanto:

$$f^{\#}(p) = \bigcup_{v \in [p]^{\#}} f^{\natural}(v) \subseteq \bigcup_{v \in [q]^{\#}} f^{\natural}(v) = f^{\#}(q).$$

Y así, $f^{\#}(p) \subseteq f^{\#}(q)$. $\square$

Como consecuencia directa del teorema, se tiene el siguiente resultado:

Corolario 3.3.10. *Dados dos términos $p, q \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$, se cumple:*

$$\mathrm{Rel} \models p = q \quad \textit{si y solo si} \quad [p]^{\#} = [q]^{\#}$$

Retomamos el ejemplo 3.3.2 en el que probabamos la validez universal de una ecuación trabajando con relaciones:

Ejemplo 3.3.11. En el ejemplo 3.3.2 probamos que se cumplía la siguiente ecuación para todo modelo relacional:

$$\mathrm{Rel} \models x \cdot (y \cdot z) = x \cdot y + x \cdot z$$

con $x, y, z \in \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$ términos. Hicimos la prueba utilizando las relaciones asociadas a estos términos mediante una asignación relacional cualquiera f. Sabemos por el teorema que acabamos de ver que una ecuación es válida para cualquier modelo relacional si y solo si se cumple para los lenguajes asociados a los términos que intervienen en la ecuación. Como hemos visto a lo largo del capítulo, la propiedad universal del álgebra de términos asegura que la aplicación $[\cdot]\colon X \longrightarrow \mathcal{P}(X^*)$ se puede extender a un homomorfismo $[\cdot]^{\#}\colon \mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X) \longrightarrow \mathcal{P}(X^*)$. Por tanto podemos interpretar los términos de la ecuación como lenguajes en $\mathcal{P}(X^*)$. Así, la expresión de la ecuación anterior entre lenguajes es de la siguiente forma:

$$[x \cdot (y + z)]^{\#} = [x \cdot y + x \cdot z]^{\#}$$

Probemos que es cierta esta expresión.

Demostración.

$$\begin{aligned}
[x \cdot (y+z)]^{\#} &= [x]^{\#} \cdot [y+z]^{\#} \\
&= [x]^{\#} \cdot ([y]^{\#} \cup [z]^{\#}) \\
&= \{x\} \cdot (\{y\} \cup \{z\}) = \{x\} \cdot \{y, z\} \\
&= \{xy, xz\} = \{xy\} \cup \{xz\} \\
&= [x \cdot y]^{\#} \cup [x \cdot z]^{\#} = [x \cdot y + x \cdot z]^{\#}
\end{aligned}$$

donde hemos utilizado que $[\cdot]^{\#}$ es homomorfismo y que $[x]^{\#} = \{x\}$. □

Mediante estos ejemplos pretendemos evidenciar la simplicidad de trabajar con lenguajes frente a hacerlo con relaciones. No obstante, cuando se trata de ecuaciones más complicadas, la prueba utilizando lenguajes también se puede complicar. Aún así, esta equivalencia resulta ventajosa dado que, como ya se ha explicado, la prueba para lenguajes se puede automatizar mediante el uso de autómatas finitos. De hecho, comprobar la equivalencia entre lenguajes formales con autómatas es un problema clásico en informática, con múltiples aplicaciones. En su trabajo, D.Pous presenta nuevos algoritmos enfocados a la resolución de este problema. (Véase [16].)

En este capítulo hemos definido una signatura algebraica, la signatura de Kleene, y la consiguiente álgebra de términos, $\mathrm{T}_{\Sigma^{\mathrm{Kl}}}(X)$. Hemos visto que el conjunto de las relaciones admite estructura de Σ^{Kl}-álgebra con las operaciones unión, composición, clausura reflexivo-transitiva, relación vacía e identidad. Además, hemos presentado los lenguajes y hemos definido las operaciones unión, producto, producto estrella, cero y uno. Hemos visto que el conjunto de lenguajes junto con estas operaciones admite también estructura de álgebra de Kleene. Finalmente hemos probado varios lemas que nos han permitido demostrar el primer teorema de decibilidad. Este teorema proporciona un procedimiento para determinar la validez de una ecuación relacional mediante la prueba de una equivalencia entre lengujes que, como ya se ha explicado, consituye un problema clásico en el campo de la informática para cuya resolución existen múltiples algoritmos. Con el objeto de mostrar la simplicidad que aporta el teorema a la prueba de una ecuación en relaciones, hemos probado, como ejemplo, la validez de una ecuación utilizando primero las propiedades relacionales y después utilizando el procedimiento entre lenguajes que nos proporciona el Teorema de Decibilidad en Álgebras de Kleene.

Capítulo 4

Decibilidad en alegorías

En este capítulo definiremos la signatura de una alegoría y veremos que se puede construir un álgebra con el conjunto de las relaciones y determinadas operaciones entre ellas, de manera que presente estructura de alegoría. En la segunda sección definiremos los grafos y algunas operaciones entre ellos. Veremos que el álgebra de todos los grafos sobre un alfabeto A admite también estructura de alegoría. A continuación, definiremos una aplicación del conjunto de variables al conjunto de grafos de forma que, por la propiedad universal del álgebra de términos, podremos extender la aplicación a un homomorfismo que parte del álgebra de términos con signatura de alegoría. Finalmente, probaremos el *Teorema de Decibilidad en Alegorías* que asegurará la validez de una inecuación relacional si y solo si existe un homomorfismo entre los grafos asociados a cada término. Serán el homomorfismo de la nueva aplicación junto con el que estudiamos en el primer capítulo, $f^{\#}$, los que nos permitan determinar la correspondencia entre relaciones y grafos. Basaremos el contenido de este capítulo en el trabajo realizado por Enric Cosme y Damien Pous en $\mathsf{K}4$-*free Grafs as a Free Algebra* [8].

Definición 4.0.1. Definimos la *signatura de una alegoría* como la signatura $\Sigma^{\mathrm{Al}} = (\Sigma_n^{\mathrm{Al}})_{n\in\mathbb{N}}$ tal que $\Sigma_2^{\mathrm{Al}} = \{\cdot, \cap\}, \Sigma_1^{\mathrm{Al}} = \{^o\}, \Sigma_0^{\mathrm{Al}} = \{1, \top\}$ y $\Sigma_n^{\mathrm{Al}} = \emptyset$ para $n > 2$. Llamaremos *alegoría* a toda Σ^{Al}-álgebra.

4.1. Alegorías para relaciones

Ya sabemos que $\mathcal{P}(C \times C)$ es el conjunto que contiene todas las relaciones en C. Vimos en el capítulo anterior que este conjunto se puede entender como un álgebra de Kleene, $\mathcal{P}(\mathbf{C} \times \mathbf{C}) = (\mathcal{P}(C \times C), \cup, \cdot, ^*, 0, 1)$. Pero si ahora consideramos las operaciones fundamentales siguientes: las operaciones binarias composición e intersección de relaciones, la operación unaria relación inversa y las constantes relación identidad y relación total; entonces el conjunto de todas las relacione sobre C admite estructura de alegoría con estas operaciones. Es decir,

$$\mathcal{P}(\mathbf{C} \times \mathbf{C}) = (\mathcal{P}(C \times C), \cdot, \cap, ^o, 1, \top)$$

es una alegoría.

Recordamos las operaciones sobre relaciones con las que trabajaremos en este capítulo:

- *Composición:* $\mathcal{R} \cdot \mathcal{S} = \{(a, b) \in C \times C \mid \exists c \in C : a\mathcal{R}c \text{ y } c\mathcal{S}b\}$.
- *Intersección:* $\mathcal{R} \cap \mathcal{S} = \{(a, b) \in C \times C \mid a\mathcal{R}b \text{ y } a\mathcal{S}b\}$.
- *Inversa:* $\mathcal{R}^o = \{(a, b) \in C \times C \mid b\mathcal{R}a\}$.
- *Relación identidad:* $1 = \{(a, b) \in C \times C \mid a = b\}$.
- *Relación total:* $\top = C \times C$.

Ahora, podemos expresar las ecuaciones e inecuaciones que hemos visto al final del capítulo 1 y que planteaban dificultades a la hora de decidir sobre su validez, como ecuaciones e inecuaciones entre términos de un álgebra de Kleene, como vimos en el capítulo 3. En este capítulo veremos como expresarlas como términos de una alegoría. La elección dependerá de las operaciones que intervengan en la ecuación de la cual queramos comprobar su validez.

En la siguiente sección daremos unas nociones básicas sobre grafos que nos permitirán presentar el *Teorema de Decibilidad en Alegorías*. Este teorema asegura la validez de una inecuación entre relaciones si y solo si se da un homomorfismo entre ciertos grafos asociados a los términos que denotan esas relaciones, de forma similar al primer teorema de decibilidad.

4.2. Grafos

A continuación veremos la definición de grafo y las operaciones que se pueden realizar con ellos, también algunos ejemplos. Veremos que el conjunto de todos los grafos sobre un alfabeto junto con las operaciones definidas está dotado de estructura de alegoría. Además daremos la definición de homomorfismo entre grafos, necesaria para poder presentar el segundo teorema de decibilidad.

Definición 4.2.1. Sea A un alfabeto. Un *grafo* sobre A es una tupla $G = (V, E, s, t, l, i, o)$ donde:

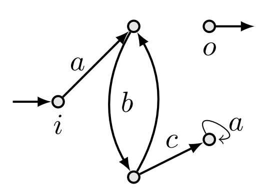
- V es un conjunto finito de *vértices*.
- E es un conjunto finito de *ejes*
- s y t son aplicaciones que van de E en V indicando el *origen* y *destino*, respectivamente, de cada eje.
- l es una aplicación $l\colon E \longrightarrow A$ que a cada eje le asigna una etiqueta en A. La llamamos *aplicación etiquetado*.
- i y o son elementos de V llamados respectivamente *entrada* y *salida*.

Nota. A lo largo del capítulo mostraremos algunos grafos mediante su representación gráfica. Así, los vértices se representaran por círculos: $\circ$ y los ejes se represantarán mediante flechas que van de un vértice a otro: $\circ\!\longrightarrow\!\circ$. Si un eje esta etiquetado mediante l por el elemento $a \in A$ lo representaremos: $\circ\xrightarrow{a}\circ$. Por último, los elementos entrada y salida se representarán por $\longrightarrow\circ$ y $\circ\longrightarrow$, respectivamente.

En ocasiones, representaremos un grafo G de forma simplificada como:

$$\longrightarrow \underset{i}{\circ} \xrightarrow{\quad G \quad} \underset{o}{\circ} \longrightarrow$$

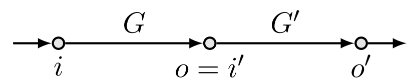
Ejemplo 4.2.2. Sea el alfabeto $A = \{a, b, c\}$. El siguiente es un grafo sobre A:



Veamos ahora las operaciones que se pueden realizar entre grafos:

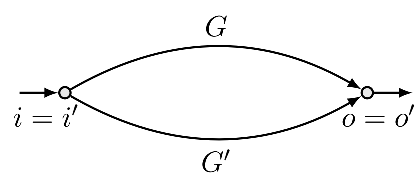
Definición 4.2.3. Sean G y G' dos grafos sobre el alfabeto A, tales que $G = (V, E, s, t, l, i, o)$ y $G' = (V', E', s', t', l', i', o')$, se definen las siguientes operaciones:

- La *composición en serie* de G y G' se denota por $G \cdot G'$ y consiste en el grafo:



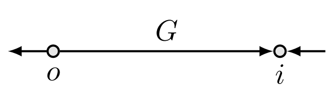
Este grafo tiene por vértices la unión disjunta de los vértices de ambos grafos, donde identificamos o con i'. El conjunto de ejes es la unión de E y E'. Así, las aplicaciones $s., t.$ y $l.$ del grafo composición en serie actúan como s, t y l si lo hacen sobre un eje $e \in E$, y como s', t' y l' si lo hacen sobre un eje $e \in E'$. La entrada del grafo es la entrada de G, i. La salida del grafo es la salida de G', o'.

- La *composición en paralelo* de G y G' se denota por $G \cap G'$ y consiste en el grafo:



que tiene por vértices la unión disjunta de los vértices de G y G', donde identificamos i con i' y o con o'. Los ejes del grafo composición en paralelo son la unión de los ejes de ambos grafos, las funciones $s_\cap, t_\cap$ y $l_\cap$ del grafo composición en paralelo actúan como s, t y l si lo hacen sobre un eje $e \in E$, y como s', t' y l' si lo hacen sobre un eje $e \in E'$. Por último, la entrada, $i_\cap$, es el vértice entrada de G y G', es decir: $i_\cap = i = i'$. Del mismo modo, la salida es $o_\cap = o = o'$.

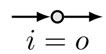
- El grafo *opuesto* de G se denota por G^o y es el grafo:



que coincide con el grafo G, salvo porque se han intercambiado la entrada y la salida, es decir: $i_o = o$ y $o_o = i$.

Además, definimos dos grafos constantes:

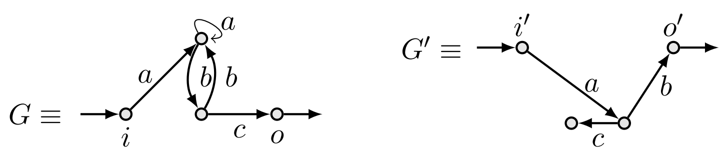
- El *grafo identidad*, que denotaremos por 1 o 1^{G}, es un grafo con un solo nodo que es a la vez entrada y salida:



- El *grafo total*, que denotaremos por $\top$, es el grafo que solo tiene dos vértices disjuntos, uno de entrada y otro de salida:

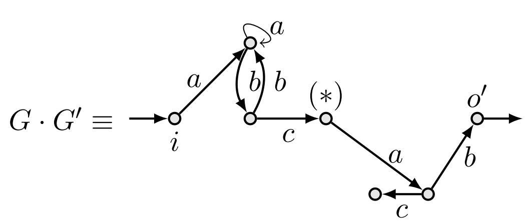
Veamos algún ejemplo de estas operaciones.

Ejemplo 4.2.4. Sean G y G' los siguientes grafos sobre el alfabeto $A = \{a, b, c\}$:



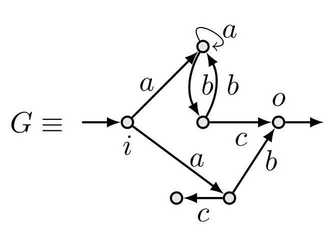
Entonces:

- La composición en serie de G y G' es el grafo:



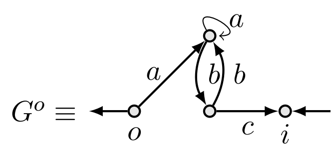
  donde (*) es el vértice en el que hacemos la correspondencia: $o = i'$.

- La composición en paralelo de G y G' es el grafo:



donde $i = i'$ y $o = o'$.

- El grafo opuesto de G es:



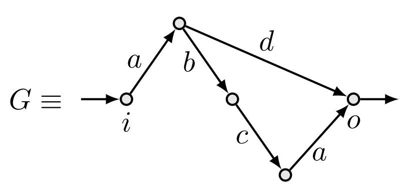
Definición 4.2.5. Definimos el conjunto $\mathsf{G}(A)$ como el conjunto de todos los grafos sobre el alfabeto A.

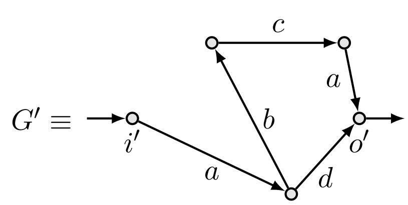
Así, $\mathsf{G}(\mathbf{A}) = (\mathsf{G}(A), \cdot, \cap, ^o, 1, \top)$ tiene estructura de alegoría.

El teorema de decibilidad en alegorías, como ya se anunciaba previamente, asegura la validez de una ecuación entre relaciones si y solo si existe un homomorfismo entre los grafos asociados a las relaciones de la inecuación. Necesitamos pues definir el concepto de *homomorfismo de grafos*.

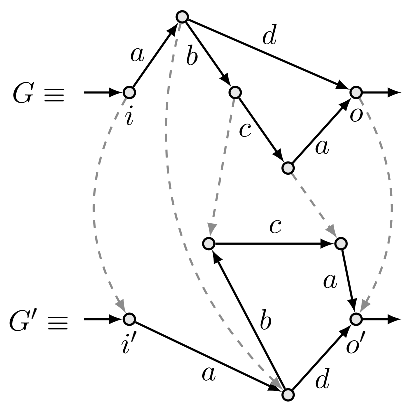
Definición 4.2.6. Sean G y G' dos grafos sobre el alfabeto A, tales que $G = (V, E, s, t, l, i, o)$ y $G' = (V', E', s', t', l', i', o')$. Un homomorfismo de G a G' es un par $h = (f, g)$ de funciones $f : V \longrightarrow V'$ y $g : E \longrightarrow E'$ que respeta los diversos componentes: $i' = f(i)$, $o' = f(o)$, $s' \circ g = f \circ s$, $t' \circ g = f \circ t$ y $l = l' \circ g$. Si existe un homomorfismo de G a G' lo denotamos $G' \blacktriangleleft G$.

Ejemplo 4.2.7. Sea el alfabeto $A = \{a, b, c, d\}$ y sean G y G' los siguientes grafos sobre A:





Veamos gráficamente que existe un homomorfismo de G a G':



Las flechas de la imagen representan la aplicación $f\colon V \longrightarrow V'$ de la definición de homomorfismo. La aplicación $g\colon E \longrightarrow E'$ es la que lleva el eje entre dos vértices de G al eje entre dos vértices de G' con la misma etiqueta en A. Notamos que f lleva el vértice entrada de G, i, al vértice entrada de G', i'. De la misma forma f lleva el vértice salida o de G al vértice salida o' de G'.

4.3. Teorema de decibilidad en alegorías

Veremos en esta sección el segundo teorema de decibilidad que nos dará un método para demostrar la validez de una ecuación en relaciones mediante la existencia de un homomorfismo entre grafos. En primer lugar definimos inecuación universalmente válida para modelos relacionales como hicimos en el capítulo anterior, pero esta vez consideramos términos en una alegoría.

Definición 4.3.1. Dados dos términos $p, q \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$, diremos que la inecuación $p \subseteq q$ es *universalmente válida para modelos relacionales*, y escribiremos $\mathrm{Rel} \models p \subseteq q$ si y solo si, para todo conjunto C y para toda aplicación $f : X \longrightarrow \mathcal{P}(C \times C)$ se tiene que $f^{\#}(p) \subseteq f^{\#}(q)$.

De la misma forma que hicimos en decibilidad en álgebras de Kleene, veamos ahora como ejemplo la demostración de la validez universal de una inecuación en modelos relacionales. Después del *Teorema de Decibilidad en Alegorías* probaremos de nuevo esta inecuación pero utilizando los grafos asociados a las relaciones a cada lado de la inecuación.

Ejemplo 4.3.2. Sean $x, y, z \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$ términos en una alegoría. Queremos probar que la siguiente inecuación entre términos es universalmente váida en modelos relacionales:

$$\mathrm{Rel} \models x \cdot (y \cap z) \subseteq (x \cap (z \cdot y^o)) \cdot y$$

Consideramos la interpretación relacional $f\colon X \longrightarrow \mathcal{P}(C \times C)$ que lleva, mediante el homomorfismo $f^{\#}$, los términos x, y, z a las relaciones $\mathcal{R}, \mathcal{S}, \mathcal{T}$ sobre un conjunto C cualquiera, respectivamente. Por tanto, podemos expresar la inecuación entre los términos x, y, z como la siguiente inecuación entre relaciones:

$$\mathcal{R} \cdot \mathcal{S} \cap \mathcal{T} \subseteq (\mathcal{R} \cap \mathcal{T} \cdot \mathcal{S}^o) \cdot \mathcal{S}$$

Probemos que se trata de una inecuación universalmente válida para modelos relacionales.

Demostración. Para probar que se cumple la inecuación veamos que dado $(a, b) \in \mathcal{R} \cdot \mathcal{S} \cap \mathcal{T}$ entonces $(a, b) \in (\mathcal{R} \cap \mathcal{T} \cdot \mathcal{S}^o) \cdot \mathcal{S}$.

Consideramos $(a, b) \in \mathcal{R} \cdot \mathcal{S} \cap \mathcal{T}$, entonces $a\mathcal{T}b$ y $a(\mathcal{R} \cdot \mathcal{S})b$ así existe $c \in C$ tal que $a\mathcal{R}c$ y $c\mathcal{S}b$.

Veamos en que consiste la relación a la derecha de la inecuación. Sea $(a, b) \in (\mathcal{R} \cap \mathcal{T} \cdot \mathcal{S}^o) \cdot \mathcal{S}$ entonces existe $d \in C$ tal que $a(\mathcal{R} \cap \mathcal{T} \cdot \mathcal{S}^o)d$ y $d\mathcal{S}b$. Entonces $a\mathcal{R}d$ y $a(\mathcal{T} \cdot \mathcal{S}^o)d$. Por tanto, existe $e \in C$ tal que $a\mathcal{T}e$ y $e\mathcal{S}^o d$, así, $d\mathcal{S}e$. Es decir:

$$(\mathcal{R} \cap \mathcal{T} \cdot \mathcal{S}^o) \cdot \mathcal{S} = \{(a, b) \in C \times C \mid \exists d, e \in C : a\mathcal{R}d, d\mathcal{S}b, d\mathcal{S}e \text{ y } a\mathcal{T}e\}$$

Así, dado $(a, b) \in \mathcal{R} \cdot \mathcal{S} \cap \mathcal{T}$ existen $d = c$ y $e = b$ tales que $a\mathcal{R}d, d\mathcal{S}b, d\mathcal{S}e$ y $a\mathcal{T}e$, es decir, $a\mathcal{R}c, c\mathcal{S}b, a\mathcal{T}b$, y por tanto $(a, b) \in (\mathcal{R} \cap \mathcal{T} \cdot \mathcal{S}^o) \cdot \mathcal{S}$. $\square$

Como podemos ver en el ejemplo, necesitamos la interpretación relacional f que va del conjunto de variables, X, en el conjunto de relaciones $\mathcal{P}(C \times C)$ para poder trasladar una inecuación entre términos de una alegoría a una inecuación entre relaciones. De igual manera, necesitaremos una aplicación que vaya del conjunto de variables en el de grafos para poder proceder con ellos. La aplicación de la siguiente definición lleva los elementos $x \in X$ a grafos en $\mathsf{G}(X)$.

Definición 4.3.3. Definimos la aplicación g como sigue:

$$\begin{aligned} \mathsf{g} : X \quad &\longrightarrow \quad \mathsf{G}(X) \\ x \quad &\longmapsto \quad \mathsf{g}(x) \equiv \longrightarrow \overset{i}{\circ} \xrightarrow{\qquad x \qquad} \overset{o}{\circ} \longrightarrow \end{aligned}$$

Propiedad 4.3.4. *Sea la aplicación* g *de la definición anterior, como* $\mathsf{G}(X)$ *es una alegoría, sabemos por la propiedad universal del álgebra de términos que* g *puede extenderse de forma única al homomorfismo:*

$$\mathsf{g}^{\#} : \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X) \longrightarrow \mathsf{G}(X)$$

tal que $\mathsf{g}^{\#} \cdot \eta_X = \mathsf{g}$.

$$\begin{tikzcd} X \arrow[r, "\mathsf{g}"] \arrow[dr, "\eta_X"'] & \mathsf{G}(X) \\ & \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X) \arrow[u, "\mathsf{g}^{\#}"'] \end{tikzcd}$$

Así, mediante los homomorfismos que extienden las aplicaciones f y g, podemos ir del conjunto de variables X en el álgebra de términos $\mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$ y de esta bien a $\mathcal{P}(C \times C)$, bien a $\mathsf{G}(X)$.

El *Teorema de Decibilidad en Alegorías* asegura que una inecuación entre dos términos de una alegoría es universalmente válida para todo modelo relacional si y solo si existe un homomorfismo entre los grafos asociados a esos términos mediante el homomorfismo $\mathsf{g}^{\#}$ que extiende a la aplicación g. Veamos el teorema:

Teorema 4.3.5. *Dados dos términos* $p, q \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$, *se cumple:*

$$Rel \models p \subseteq q \quad \textit{si y solo si} \quad \mathsf{g}^{\#}(p) \blacktriangleleft \mathsf{g}^{\#}(q).$$

Antes de entrar a la demostración del segundo teorema de decibilidad veremos un lema técnico necesario para la prueba.

Lema 4.3.6. *Sea* $p \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$, *sea* $\mathsf{g}^{\#}(p) = (V, E, s, t, l, i, o)$ *el grafo asociado al término* p. *Sea* C *un conjunto y sea* $f : X \longrightarrow \mathcal{P}(C \times C)$ *una asignación de relaciones a las variables en* X. *Entonces, para todo* $a, b \in C$ *se tiene que* $(a, b) \in f^{\#}(p)$ *si y solo si existe una aplicación* $\phi : V \longrightarrow C$ *tal que:*

(I) $\phi(i) = a$

(II) $\phi(o) = b$

(III) *Si* $e \in E$ *es un eje cumpliendo*

$$\left.\begin{array}{l} s(e) = v \\ t(e) = w \\ l(e) = x \end{array}\right\} \textit{ entonces } (\phi(v), \phi(w)) \in f(x).$$

Demostración. Demostraremos esta afirmación por inducción sobre la estructura de p. Notamos que el término p puede ser de la forma:

(1) $p = x$ para alguna variable $x \in X$.

(2) $p = 1^{\mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)}$.

(3) $p = \top^{\mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)}$.

(4) $p = q^o$ para algún $q \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$.

(5) $p = q \cdot r$ para algunos términos $q, r \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$.

(6) $p = q \cap r$ para algunos términos $q, r \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$.

Comprobaremos en cada caso ambas implicaciones.

(1) Sea el término $p = x$ una variable.

($\Rightarrow$) Sean $a, b \in C$ tales que $(a, b) \in f^{\#}(p)$, entonces

$$(a, b) \in f^{\#}(p) = f^{\#}(x) = f^{\#} \circ \eta_X(x) = f(x)$$

Por otro lado, $\mathsf{g}^{\#}(p) = \mathsf{g}^{\#}(x) = \mathsf{g}^{\#} \circ \eta_X(x) = \mathsf{g}(x) \equiv \to \overset{i}{\circ} \xrightarrow{\;x\;} \overset{o}{\circ} \to$

Consideramos la aplicación $\phi\colon V \longrightarrow C$ que asigna a la entrada y la salida del grafo las siguientes imágenes: $\phi(i) = a, \phi(o) = b$. Entonces, por definición, se cumplen (I) y (II). Para (III) notamos que solo hay un eje $e \in E$ con

$$\left.\begin{array}{l} s(e) = i \\ t(e) = o \\ l(e) = x \end{array}\right\} \text{ y se cumple que } (\phi(i), \phi(o)) = (a, b) \in f(x).$$

($\Leftarrow$) Sea ϕ la aplicación de V en C que satisface las hipótesis. Notemos que $\mathsf{g}^{\#}(p) = \mathsf{g}^{\#}(x) = \mathsf{g}^{\#} \circ \eta_X(x) = \mathsf{g}(x) \equiv \to \overset{i}{\circ} \xrightarrow{\;x\;} \overset{o}{\circ} \to$.

La aplicación ϕ satisface:

(I) $\phi(i) = a$

(II) $\phi(o) = b$

(III) Sea e el único eje de $\mathsf{g}^{\#}(x)$, entonces

$$\left.\begin{array}{l} s(e) = i \\ t(e) = o \\ l(e) = x \end{array}\right\} \text{ y se cumple que } (\phi(i), \phi(o)) \in f(x).$$

Entonces, como $(\phi(i), \phi(o)) = (a, b)$, se tiene que

$$(a, b) \in f(x) = f^{\#} \circ \eta_X(x) = f^{\#}(x) = f^{\#}(p)$$

con lo que queda probado el primer caso.

(2) Sea $p = 1^{\mathrm{T}_{\Sigma\mathrm{Al}}(X)}$ la identidad del álgebra de términos.

($\Rightarrow$) Sean $a, b \in C$ tales que $(a, b) \in f^{\#}(p)$, entonces

$$(a, b) \in f^{\#}(p) = f^{\#}(1^{\mathrm{T}_{\Sigma\mathrm{Al}}(X)}) = 1^{\mathcal{P}(C\times C)}.$$

Así $a = b$.

Por otro lado, $\mathsf{g}^{\#}(p) = \mathsf{g}^{\#}(1^{\mathrm{T}_{\Sigma\mathrm{Al}}(X)}) = 1^{\mathsf{G}(X)} \equiv \overset{i\,=\,o}{\longrightarrow\circ\longrightarrow}$.

Consideramos la aplicación $\phi\colon V \longrightarrow C$ que asigna al único vértice $i \in V$ la imagen $a \in C$. Así, por definición se cumple $\phi(i) = a$ y como $i = o$ y $a = b$, se tiene $\phi(o) = \phi(i) = a = b$, es decir, se cumplen (I) y (II). Notamos que el grafo $1^{\mathsf{G}(X)}$ no tiene ningún eje $e \in E$, por tanto queda demostrada la implicación. Veamos el recíproco.

($\Leftarrow$) Sea ϕ la aplicación de V en C que satisface las hipótesis. Notamos que $\mathsf{g}^{\#}(p) = \mathsf{g}^{\#}(1^{\mathrm{T}_{\Sigma\mathrm{Al}}(X)}) = 1^{\mathsf{G}(X)} \equiv \overset{i\,=\,o}{\longrightarrow\circ\longrightarrow}$.

La aplicación ϕ satisface: (I) $\phi(i) = a$ y (II) $\phi(o) = b$. Dado que $g^{\#}(p)$ no tiene ningún eje, no cabe considerar la hipótesis (III).

Como $g^{\#}(p)$ consiste en un único vértice, $a = \phi(i) = \phi(o) = b$. Y así, $(a, b) \in 1^{\mathcal{P}(C\times C)} = f^{\#}(1^{\mathrm{T}_{\Sigma\mathrm{Al}}(X)}) = f^{\#}(p)$.

(3) Sea $p = \top^{\mathrm{T}_{\Sigma\mathrm{Al}}(X)}$ la operación constante total en el álgebra de términos.

($\Rightarrow$) Sean $a, b \in C$ tales que $(a, b) \in f^{\#}(p)$, entonces

$$(a, b) \in f^{\#}(p) = f^{\#}(\top^{\mathrm{T}_{\Sigma\mathrm{Al}}(X)}) = \top^{\mathcal{P}(C\times C)}.$$

Por otro lado, $\mathsf{g}^{\#}(p) = \mathsf{g}^{\#}(\top^{\mathrm{T}_{\Sigma\mathrm{Al}}(X)}) = \top^{\mathsf{G}(X)} \equiv \overset{i}{\longrightarrow\circ} \qquad \overset{o}{\circ\longrightarrow}$.

Consideramos la aplicación $\phi\colon V \longrightarrow C$ que asigna las siguientes imágenes: $\phi(i) = a, \phi(o) = b$. Así, por la definición de ϕ se cumplen (I) y (II). Notamos que el grafo $\top^{\mathsf{G}(X)}$ no tiene ningún eje $e \in E$, por tanto queda demostrada la implicación.

($\Leftarrow$) Sea ϕ la aplicación de V en C que satisface las hipótesis, entonces ϕ satisface: (I) $\phi(i) = a$ y (II) $\phi(o) = b$. Dado que $g^{\#}(p)$ no tiene ningún eje, no cabe considerar la hipótesis (III).

Como $\top^{\mathcal{P}(C\times C)}$ contiene a todas las relaciones en C,

$$(a,b) \in \top^{\mathcal{P}(C\times C)} = f^{\#}(\top^{\mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)}) = f^{\#}(p).$$

(4) Sea $p = q^o$ el opuesto del término $q \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$.

($\Rightarrow$) Sean $a, b \in C$ tales que $(a,b) \in f^{\#}(p)$, entonces

$$(a,b) \in f^{\#}(p) = f^{\#}(q^o) = f^{\#}(q)^o.$$

Así, $(b,a) \in f^{\#}(q)$.

Notamos que $\mathsf{g}^{\#}(p) = \mathsf{g}^{\#}(q^o) = \mathsf{g}^{\#}(q)^o \equiv \longleftarrow \overset{o}{\circ} \xrightarrow{\quad q \quad} \overset{i}{\circ} \longleftarrow$

y $\mathsf{g}^{\#}(q) \equiv \longrightarrow \overset{i_q}{\circ} \xrightarrow{\quad q \quad} \overset{o_q}{\circ} \longrightarrow$.

Fijamos la siguiente notación: $\mathsf{g}^{\#}(q) = (V_q, E_q, s_q, t_q, l_q, i_q, o_q)$.

Por inducción, existe $\phi_q \colon V_q \longrightarrow C$ tal que se cumple:

(I) $\phi_q(i_q) = b$

(II) $\phi_q(o_q) = a$

(III) Si $e \in E_q$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v \\ t(e) = w \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi_q(v), \phi_q(w)) \in f(x).$$

Notamos que el grafo asociado al término p, es $\mathsf{g}^{\#}(p) = (V, E, s, t, l, i, o)$ donde $V = V_q$, excepto por los vértices entrada y salida que cumplen $i = o_q$ y $o = i_q$. El resto de elementos de ambos grafos coinciden: $E = E_q, s = s_q, t = t_q$ y $l = l_q$. Por lo que ϕ coincide con ϕ_q, excepto en los vértices mencionados. Así, ϕ cumple:

(I) $\phi(i) = \phi_q(o_q) = a$

(II) $\phi(o) = \phi_q(i_q) = b$

(III) Si $e \in E = E_q$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v \\ t(e) = w \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi(v), \phi(w)) = (\phi_q(v), \phi_q(w)) \in f(x).$$

Con lo que queda demostrada la implicación a derecha.

($\Leftarrow$) Por hipótesis existe una aplicación $\phi \colon V \longrightarrow C$ que cumple:

(I) $\phi(i) = a$

(II) $\phi(o) = b$

(III) Si $e \in E$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v \\ t(e) = w \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi(v), \phi(w)) \in f(x).$$

Sea $\mathsf{g}^{\#}(q) = (V_q, E_q, s_q, t_q, l_q, i_q, o_q)$ el grafo asociado al término q, como en la implicación anterior. Y sea $\phi_q \colon V_q \longrightarrow C$ tal que se cumple:

(I) $\phi_q(i_q) = b$

(II) $\phi_q(o_q) = a$

(III) Si $e \in E_q$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v \\ t(e) = w \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi_q(v), \phi_q(w)) \in f(x).$$

Así, por inducción, $(b, a) \in f^{\#}(q)$. Por tanto:

$$(a, b) \in f^{\#}(q)^o = f^{\#}(q^o) = f^{\#}(p).$$

Y queda demostrado el caso (4).

(5) Sea $p = q \cdot r$ el término resultante del producto de $q, r \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$ términos.

($\Rightarrow$) Sean $a, b \in C$ tales que $(a, b) \in f^{\#}(p)$, entonces

$$(a, b) \in f^{\#}(p) = f^{\#}(qr) = f^{\#}(q) \cdot f^{\#}(r).$$

Entonces existe $c \in C$ tal que $(a, c) \in f^{\#}(q)$ y $(c, b) \in f^{\#}(r)$.

Fijamos la siguiente notación:

$\mathsf{g}^{\#}(q) = (V_q, E_q, s_q, t_q, l_q, i_q, o_q)$ y $\mathsf{g}^{\#}(r) = (V_r, E_r, s_r, t_r, l_r, i_r, o_r)$.

Por inducción existen $\phi_q \colon V_q \longrightarrow C$ y $\phi_r \colon V_r \longrightarrow C$ tales que se cumple:

(I) $\phi_q(i_q) = a$

(II) $\phi_q(o_q) = c$

(III) Si $e \in E_q$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v_q \\ t(e) = w_q \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi_q(v_q), \phi_q(w_q)) \in f(x).$$

Y para ϕ_r:

(I) $\phi_r(i_r) = c$

(II) $\phi_r(o_r) = b$

(III) Si $e \in E_r$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v_r \\ t(e) = w_r \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi_r(v_r), \phi_r(w_r)) \in f(x).$$

Notamos que $\mathtt{g}^{\#}(p) = \mathtt{g}^{\#}(q) \cdot \mathtt{g}^{\#}(r) \equiv \longrightarrow \overset{i}{\circ} \xrightarrow{\mathtt{g}^{\#}(q)} \circ \xrightarrow{\mathtt{g}^{\#}(r)} \overset{o}{\circ} \longrightarrow$. Así, el conjunto de vértices de $\mathtt{g}^{\#}(p)$ es la unión disjunta de los vértices de $\mathtt{g}^{\#}(q)$ y los vértices de $\mathtt{g}^{\#}(r)$, donde hemos identificado $o_q = i_r$. La aplicación ϕ, será aquella que lleva los vértices de V_q a la imagen por ϕ_q y los de V_r a la imagen por ϕ_r; y que actúa de igual manera con los ejes. En el vértice especial $o_q = i_r$, sabemos que $\phi_q(o_q) = c = \phi_r(i_r)$, por lo que la aplicación ϕ está bien definida y cumple (I), (II) y (III).

($\Leftarrow$) Por hipótesis existe una aplicación $\phi : V \longrightarrow C$ tal que:

(I) $\phi(i) = a$

(II) $\phi(o) = b$

(III) Si $e \in E$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v \\ t(e) = w \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi(v), \phi(w)) \in f(x).$$

Notamos que $\mathtt{g}^{\#}(p) = \mathtt{g}^{\#}(q) \cdot \mathtt{g}^{\#}(r) \equiv \longrightarrow \overset{i}{\circ} \xrightarrow{\mathtt{g}^{\#}(q)} \circ \xrightarrow{\mathtt{g}^{\#}(r)} \overset{o}{\circ} \longrightarrow$.

Notamos que la restricción $\phi_q|_{V_q} : V_q \longrightarrow C$, es una aplicación que cumple (I), (II) y (III). Llamamos $c = \phi_p(o_p)$. Entonces, por inducción, se tiene que $(a, c) \in f^{\#}(q)$.

De la misma forma, la restricción $\phi_r|_{V_r} \colon V_r \longrightarrow C$ cumple (I), (II) y (III); y por la correspondencia entre o_q e i_r, se tiene que $\phi_p|_{V_r}(i_r) = c$. Y por inducción se tiene que $(c, b) \in f^{\#}(r)$.

Y por lo tanto, $(a, b) \in f^{\#}(q) \cdot f^{\#}(r) = f^{\#}(qr) = f^{\#}(p)$.

(6) Sea el término $p = q \cap r$ resultante de la intersección de los términos $q, r \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$.

($\Rightarrow$) Sean $a, b \in C$ tales que $(a, b) \in f^{\#}(p)$, entonces

$$(a, b) \in f^{\#}(p) = f^{\#}(q \cap r) = f^{\#}(q) \cap f^{\#}(r).$$

Fijamos la siguiente notación:

$\mathsf{g}^{\#}(q) = (V_q, E_q, s_q, t_q, l_q, i_q, o_q)$ y $\mathsf{g}^{\#}(r) = (V_r, E_r, s_r, t_r, l_r, i_r, o_r)$.

Por inducción existen $\phi_q \colon V_q \longrightarrow C$ y $\phi_r \colon V_r \longrightarrow C$ tales que se cumple:

(I) $\phi_q(i_q) = a$

(II) $\phi_q(o_q) = b$

(III) Si $e \in E_q$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v_q \\ t(e) = w_q \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi_q(v_q), \phi_q(w_q)) \in f(x).$$

Y para ϕ_r:

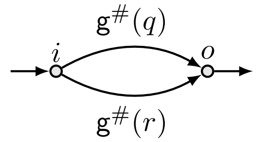
(I) $\phi_r(i_r) = a$

(II) $\phi_r(o_r) = b$

(III) Si $e \in E_r$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v_r \\ t(e) = w_r \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi_r(v_r), \phi_r(w_r)) \in f(x).$$

Notamos que $\mathsf{g}^{\#}(p) = \mathsf{g}^{\#}(q) \cap \mathsf{g}^{\#}(r) \equiv$



.

Así, el conjunto de vértices de $\mathsf{g}^{\#}(p)$ es la unión disjunta de los vértices de $\mathsf{g}^{\#}(q)$ y los vértices de $\mathsf{g}^{\#}(r)$, donde hemos identificado $i = i_q = i_r$ y $o = o_q = o_r$. La aplicación ϕ, será aquella que lleva los vértices de V_q a la imagen por ϕ_q y los de V_r a la imagen por ϕ_r; y que actúa de igual manera con los ejes. En los vértices especiales i y o, sabemos que $\phi(i) = \phi_q(i_q) = \phi_r(i_r) = a$ y $\phi(o) = \phi_q(o_q) = \phi_r(o_r) = b$, por lo que la aplicación ϕ está bien definida y cumple (I), (II) y (III).

Veamos la implicación contraria.

($\Leftarrow$)Por hipótesis existe una aplicación $\phi : V \longrightarrow C$ tal que:

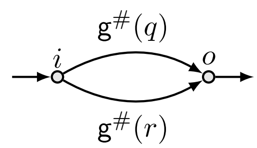
(I) $\phi(i) = a$

(II) $\phi(o) = b$

(III) Si $e \in E$ es un eje que cumple

$$\left.\begin{array}{l} s(e) = v \\ t(e) = w \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi(v), \phi(w)) \in f(x).$$

Notamos que $\mathsf{g}^{\#}(p) = \mathsf{g}^{\#}(q) \cap \mathsf{g}^{\#}(r) \equiv$



.

La restricción $\phi_q|_{V_q} : V_q \longrightarrow C$, es una aplicación que cumple (I), (II) y (III). Por inducción, se tiene que $(a, b) \in f^{\#}(q)$.

De la misma forma, la restricción $\phi_r|_{V_r} : V_r \longrightarrow C$ cumple (I), (II) y (III) y por inducción se tiene que $(a, b) \in f^{\#}(r)$.

Y por lo tanto, $(a, b) \in f^{\#}(q) \cap f^{\#}(r) = f^{\#}(q \cap r) = f^{\#}(p)$.

Así, queda demostrado el lema para todo término $p \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$. □

Estamos ahora en condiciones de probar el segundo teorema de decibilidad. El *Teorema de Decibilidad en Alegorías* asegura la validez de una inecuación entre relaciones si y solo si existe un homomorfismo entre los grafos asociados a las relaciones de la inecuación.

Recordemos el teorema:

Teorema 4.3.5 *Dados dos términos $p, q \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$, se cumple:*

$$\mathit{Rel} \models p \subseteq q \quad \textit{si y solo si} \quad \mathsf{g}^{\#}(p) \blacktriangleleft \mathsf{g}^{\#}(q)$$

Demostración. Suponemos que $Rel \models p \subseteq q$. Hemos de encontrar un homomorfismo de grafos de $\mathsf{g}^{\#}(q)$ a $\mathsf{g}^{\#}(p)$, donde $\mathsf{g}^{\#}(q) = (V_q, E_q, s_q, t_q, l_q, i_q, o_q)$ y $\mathsf{g}^{\#}(p) = (V_p, E_p, s_p, t_p, l_p, i_p, o_p)$.

Sea $C = V_p$, consideramos la siguiente interpretación:

$$\begin{array}{rcl} f\colon X & \longrightarrow & \mathcal{P}(V_p \times V_p) \\ x & \longmapsto & \{(v,w) \mid \exists e \in E_p \text{ tal que } s(e) = v, t(e) = w \text{ y } l(e) = x\} \end{array}$$

Por hipótesis $f^{\#}(p) \subseteq f^{\#}(q)$.

Consideramos $\phi_1\colon V_p \longrightarrow V_p$, tal que $\phi_1 = Id_{V_p}$. Entonces ϕ_1 cumple:

(I) $\phi_1(i_p) = i_p$

(II) $\phi_1(o_p) = o_p$

(III) Si $e \in E_p$ es un eje que cumple

$$\left.\begin{array}{l} s_p(e) = v \\ t_p(e) = w \\ l_p(e) = x \end{array}\right\} \text{ entonces } (\phi_1(v), \phi_1(w)) = (v,w) \in f(x)$$

por la construcción de f.

Así, por el lema 4.3.6, $(i_p, o_p) \in f^{\#}(p) \subseteq f^{\#}(q)$. Y aplicando de nuevo el lema 4.3.6, existe $\phi\colon V_q \longrightarrow V_p$ tal que:

(I) $\phi(i_q) = i_p$

(II) $\phi(o_q) = o_p$

(III) Si $e \in E_q$ con $\left.\begin{array}{l} s_q(e) = v \\ t_q(e) = w \\ l_q(e) = x \end{array}\right\}$ entonces $(\phi(v), \phi(w)) \in f(x)$.

Definimos $\psi\colon E_q \longrightarrow E_p$ como la aplicación que lleva el eje $e \in E_q$ con $s_q(e) = v, t_q(e) = w$ y $l_q(e) = x$ al eje $\psi(e) \in E_p$ con $s_p(\psi(e)) = \phi(v), t_p(\psi(e)) = \phi(w)$ y $l_p(\psi(e)) = x$. Gráficamente, esto es:

$$\begin{tikzcd} v \arrow[r, bend left, "e", "x"'] \arrow[d, dashed] & w \arrow[d, dashed] \\ \phi(v) \arrow[r, bend left, "\psi(e)", "x"'] & \phi(w) \end{tikzcd}$$

Sea $e \in E_q$, entonces el par (ϕ, ψ) cumple:

- $i_p = \phi(i_q)$,
- $o_p = \phi(o_q)$,
- $s_p \circ \psi(e) = s_p(\psi(e)) = \phi(v) = \phi(s_q(e)) = \phi \circ s_q(e)$, así $s_p \circ \psi = \phi \circ s_q$,
- $t_p \circ \psi(e) = t_p(\psi(e)) = \phi(w) = \phi(t_q(e)) = \phi \circ t_q(e)$, así $t_p \circ \psi = \phi \circ t_q$,
- $l_q = x = l_p(\psi(e)) = l_p \circ \psi(e)$, entonces $l_q = l_p \circ \psi$.

Y así, el par (ϕ, ψ) es un homomorfismo de $\mathtt{g}^{\#}(q)$ a $\mathtt{g}^{\#}(p)$.

Veamos ahora la implicación contraria. Suponemos que existe un homomorfismo (φ, ψ) de $\mathtt{g}^{\#}(q)$ a $\mathtt{g}^{\#}(p)$.

Sea C un conjunto y sea $f \colon X \longrightarrow \mathcal{P}(C \times C)$. Queremos comprobar que entonces $f^{\#}(p) \subseteq f^{\#}(q)$.

Sea $(a, b) \in f^{\#}(p)$. Para comprobar que $(a, b) \in f^{\#}(q)$, en virtud del lema 4.3.6, es suficiente comprobar la existencia de una aplicación $\phi_q \colon V_q \longrightarrow C$ cumpliendo las condiciones (I), (II) y (III) del lema.

Como $(a, b) \in f^{\#}(p)$, por el mismo lema 4.3.6, sabemos que existe una aplicación $\phi_p \colon V_p \longrightarrow C$, cumpliendo:

(I) $\phi_p(i_p) = a$

(II) $\phi_p(o_p) = b$

(III) Si $e \in E_p$ con $\left.\begin{array}{l} s_p(e) = v_p \\ t_p(e) = w_p \\ l_p(e) = x \end{array}\right\}$ entonces $(\phi_p(v_p), \phi_p(w_p)) \in f(x)$.

Consideramos la aplicación $\phi_q = \phi_p \circ \varphi \colon V_q \longrightarrow C$

(I) $\phi_q(i_q) = \phi_p \circ \varphi(i_q) = \phi_p(i_p) = a$

(II) $\phi_q(o_q) = \phi_p \circ \varphi(o_q) = \phi_p(o_p) = b$

(III) Si $e \in E_q$ con $\left.\begin{array}{l} s_q(e) = v_q \\ t_q(e) = w_q \\ l_q(e) = x \end{array}\right\}$ entonces
$(\phi_q(v_q), \phi_q(w_q)) = (\phi_p \circ \varphi(v_q), \phi_p \circ \varphi(w_q)) = (\phi_p(v_p), \phi_p(w_p)) \in f(x)$.

Así, existe una función ϕ_q cumpliendo (I), (II) y (III). Entonces, por el lema 4.3.6, $(a, b) \in f^{\#}(q)$. Y por tanto, $f^{\#}(p) \subseteq f^{\#}(q)$. Quedando demostrado el teorema. $\square$

Como consecuencia del teorema se da el siguiente resultado.

Corolario 4.3.7. *Dados dos términos $p, q \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$, se cumple:*

$$Rel \models p = q \quad \textit{si y solo si} \quad \begin{cases} \mathtt{g}^{\#}(p) \blacktriangleleft \mathtt{g}^{\#}(q) \ \textit{y} \\ \mathtt{g}^{\#}(q) \blacktriangleleft \mathtt{g}^{\#}(p) \end{cases}$$

Retomamos ahora el ejemplo 4.3.2:

Ejemplo 4.3.8. En el ejemplo 4.3.2 probamos al comienzo de la sección que se cumple la siguiente expresión:

$$\mathrm{Rel} \models x \cdot (y \cap z) \subseteq (x \cap (y \cdot z^o)) \cdot z$$

para términos $x, y, z \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$.

Para ello, probamos que dadas $\mathcal{R}, \mathcal{S}$ y $\mathcal{T}$ relaciones sobre un conjunto C cualquiera asociadas mediante una asignación relacional f a los términos x, y, z, la inecuación:

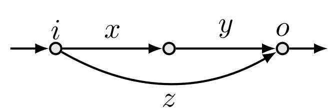
$$\mathcal{R} \cdot \mathcal{S} \cap \mathcal{T} \subseteq (\mathcal{R} \cap \mathcal{T} \cdot \mathcal{S}^o) \cdot \mathcal{S}$$

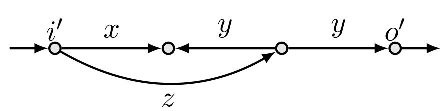
se cumple.

Veamos que, gracias al teorema, podemos probar esta inecuación de forma más sencilla hallando un homomorfismo entre los grafos asociados a los términos de la inecuación mediante el homomorfismo $\mathtt{g}^{\#}$ que extiende a la aplicación $\mathtt{g}$ que definimos en este mismo capítulo.

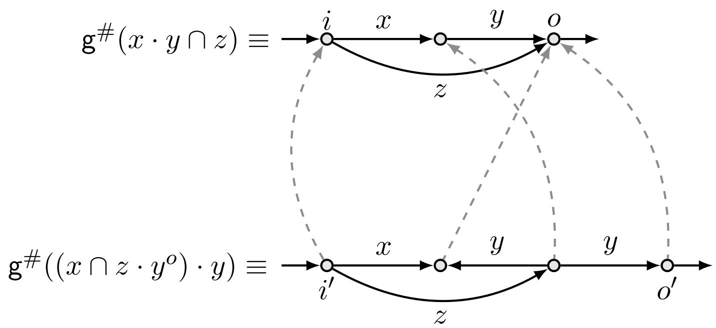
Entonces, para confirmar que la inecuación entre relaciones dada es universalmente válida, basta con probar que existe un homomorfismo de $\mathtt{g}^{\#}((x \cap z \cdot y^o) \cdot y)$ a $\mathtt{g}^{\#}(x \cdot y \cap z)$. Veámoslo:

Demostración. Para probarlo, representaremos gráficamente ambos grafos y veremos que existe el homomorfismo mencionado. Veamos la representación gráfica:

$\mathtt{g}^{\#}(x \cdot y \cap z) \equiv$ 

$\mathtt{g}^{\#}((x \cap z \cdot y^o) \cdot y) \equiv$ 

Veamos graficamente que existe el homomorfismo que buscamos:



Las flechas grises, $\dashrightarrow$, como en el ejemplo de homomorfismo entre grafos (Ejemplo 4.2.7), representan la aplicación $f\colon V' \longrightarrow V$ dónde V' y V son los conjuntos de vértices de $\mathtt{g}^{\#}((x \cap z \cdot y^o) \cdot y)$ y $\mathtt{g}^{\#}(x \cdot y \cap z)$ respectivamente. La aplicación g de la definición de homomorfismo es la que lleva el eje entre dos vértices de un grafo al eje entre dos vértices del otro con la misma etiqueta, ahora las etiquetas de nuestros grafos son los términos $x, y, z \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$ involucrados en la inecuación. Notamos que f lleva el vértice entrada de un grafo, i', al vértice entrada del otro, i. De la misma forma f lleva el vértice salida o' al vértice salida o.

Así, existe un par $h = (f, g)$ de funciones tal que respeta los diversos componentes. Por tanto, $\mathtt{g}^{\#}(x \cdot y \cap z) \blacktriangleleft \mathtt{g}^{\#}((x \cap z \cdot y^o) \cdot y)$. $\square$

Mediante estos ejemplos pretendemos mostrar la sancillez de trabajar con grafos frente a hacerlo directamente con relaciones. No obstante, igual que nos pasaba con los lenguajes, cuando se trata de ecuaciones más complicadas, probar que existe un homomorfismo de grafos puede resultar complejo. Aún así, esta equivalencia resulta ventajosa dado que, aunque el problema del homomorfismo entre grafos es un conocido problema NP-completo en teoría de complejidad computacional, cuando trabajamos con alegorías, este problema se reduce a un caso muy restringido: los grafos de términos tienen un ancho de arbol menor o igual que dos. En concreto, dado un grafo arbitrario G con n vértices y una palabra q de tamaño m, un algoritmo de programación dinámica simple decide si existe un homomorfismo de $\mathtt{g}^{\#}(q)$ a G en $O(n^2 m)$ operaciones. (Véase [16].)

En este capítulo hemos definido una nueva signatura algebraica: la signatura de una alegoría, Σ^{Al}; y la consiguiente álgebra de términos: $\mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$. Hemos visto que el conjunto de las relaciones admite estructura de Σ^{Al}-álgebra con las operaciones composición, intersección, inverso, relación total e identidad. Además, hemos presentado los grafos y hemos definido las operaciones composición en serie, composición en paralelo, opuesto, identidad y grafo total. Hemos visto que el conjunto de grafos junto con estas operaciones admite también estructura de alegoría. Finalmente hemos probado un lema que nos ha permitido demostrar el Teorema de Decibilidad en Alegorías. Este teorema proporciona un procedimiento para determinar la validez de una ecuación relacional mediante la prueba de la existencia de un homomorfismo entre grafos. Como ya hemos explicado, hallar ese homomorfismo es un problema conocido en el campo de la informática para cuya resolución existen ya algoritmos. Con el objeto de hacer patente la utilidad del teorema para probar la validez de una ecuación en relaciones, hemos probado, como ejemplo, la validez de una ecuación utilizando primero las propiedades relacionales y después utilizando el procedimiento entre grafos que nos proporciona el segundo teorema de decibilidad.

Capítulo 5

Decibilidad en alegorías de Kleene

En este capítulo definiremos la signatura de una alegoría de Kleene. En la primera sección veremos que el conjunto de las relaciones con determinadas operaciones admite estructura de alegoría de Kleene. En la siguiente sección definiremos los lenguajes de grafos y las opeRaciones en este conjunto y veremos que el conjunto de todos los lenguajes de grafos sobre el alfabeto A presenta estructura de alegoría de Kleene. Ocurrirá lo mismo con el álgebra que definimos en la tercera sección, el álgebra de las partes de la $\Sigma^{\mathrm{Al}'}$-álgebra libre. Asimismo, definiremos la signatura $\Sigma^{\mathrm{Al}'}$ y las operaciones que se pueden realizan con elementos en $\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)$. Definiremos una aplicación del conjunto de variables X en cada una de estas álgebras, gracias a la propiedad universal del álgebra de términos podremos extenderlas a homomorfismos que parten de $\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$ y van al álgebra respectiva. Por último probaremos dos lemas que relacionan estos homomorfismos entre sí y con el homomorfismo, $f^{\#}$, extensión de una interpretación relacional cualquiera, $f\colon X \longrightarrow \mathcal{P}(C \times C)$; que serán claves para probar el tercer y último teorema de decibilidad: *Teorema de Decibilidad en Alegorías de Kleene*. Basaremos el contenido de este capítulo en el trabajo realizado por Paul Brunet y Damien Pous en *Petri Automata for Kleene Allegories* [4].

Definición 5.0.1. Definimos la *signatura de una alegoría de Kleene* como la signatura $\Sigma^{\mathrm{AK}} = (\Sigma_n^{\mathrm{AK}})_{n\in\mathbb{N}}$ tal que $\Sigma_2^{\mathrm{AK}} = \{\cdot, +, \cap\}, \Sigma_1^{\mathrm{AK}} = \{^*, ^o\}, \Sigma_0^{\mathrm{AK}} = \{0, 1\}$ y $\Sigma_n^{\mathrm{AK}} = \emptyset$ para $n > 2$. Llamaremos *alegoría de Kleene* a toda Σ^{AK}-álgebra.

Notamos que en esta estructura no se considera la operación constante $\top$, esto se debe a que $\top$ tiene distintas interpretaciones según el álgebra en la que trabajemos y este hecho presenta problemas a la hora de demostrar algunos de los lemas que se darán a lo largo del capítulo. Dejando fuera la constante $\top$ podemos, aunque de forma sesgada, generalizar el resultado con el tercer teorema de decibilidad. Este teorema nos aportará dos métodos distintos para probar la validez de una ecuación relacional, uno de ellos será utilizando los lenguajes de grafos, el otro mediante lenguajes sobre el álgebra de términos $\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)$.

5.1. Alegorías de Kleene para relaciones

Como ya sabemos, $\mathcal{P}(C \times C)$ es el conjunto que contiene todas las relaciones en un conjunto C cualquiera. El conjunto $\mathcal{P}(C \times C)$, combinado con distintas operaciones, presenta estructura bien de álgebra de Kleene: $(\mathcal{P}(C \times C), \cup, \cdot, ^*, 0, 1)$, bien de alegoría: $(\mathcal{P}(C \times C), \cdot, \cap, ^o, 1, \top)$, como hemos visto en anteriores capítulos.

Veremos en este capítulo que $\mathcal{P}(C \times C)$, con las operaciones composición, unión e intersección de relaciones, calusura reflexivo-transitiva, relación inversa, relación vacía y relación identidad tiene estructura de Σ^{AK}-álgebra. Es decir,

$$\mathcal{P}(\mathbf{C} \times \mathbf{C}) = (\mathcal{P}(C \times C), \cdot, \cup, \cap, ^*, ^o, 0, 1)$$

es una alegoría de Kleene.

Recordamos las operaciones sobre relaciones con las que trabajaremos en este capítulo:

- *Composición:* $\mathcal{R} \cdot \mathcal{S} = \{(a, b) \in C \times C \mid \exists c \in C : a\mathcal{R}c \text{ y } c\mathcal{S}b\}$
- *Unión:* $\mathcal{R} \cup \mathcal{S} = \{(a, b) \in C \times C \mid a\mathcal{R}b \text{ ó } a\mathcal{S}b\}$
- *Intersección:* $\mathcal{R} \cap \mathcal{S} = \{(a, b) \in C \times C \mid a\mathcal{R}b \text{ y } a\mathcal{S}b\}$
- *Clausura reflexivo-transitiva:* $\mathcal{R}^* = \{(a, b) \in C \times C \mid \exists c_0, \ldots, c_n \in C : : c_0 = a, c_n = b \text{ y } \forall i \in n, c_i\mathcal{R}c_{i+1}\}$
- *Inversa:* $\mathcal{R}^o = \{(a, b) \in C \times C \mid b\mathcal{R}a\}$
- *Relación vacía:* $0 = \emptyset$
- *Relación identidad:* $1^C = \{(a, b) \in C \times C \mid a = b\}$

Ahora podemos expresar las ecuaciones entre relaciones como ecuaciones entre términos de una alegoría de Kleene. Igual que en los capítulos anteriores, necesitamos un álgebra que posea estructura de alegoría de Kleene y que nos permita transladar el problema de la validez universal de una inecuación en relaciones a esta nueva álgebra donde trabajaremos de forma más sencilla. En este caso presentamos dos álgebras distintas con estructura de alegoría de Kleene: los *Lenguajes de grafos* y el conjunto de las *Partes de la* $\Sigma^{\mathrm{Al}'}$*-álgebra libre*. Vemos en las siguientes secciones en que consisten ambas álgebras.

5.2. Lenguajes de grafos

Comenzaremos por definir el conjunto de los lenguajes de grafos. A continuación veremos que este conjunto, con determinadas operaciones, presenta estructura de alegoría de Kleene.

Definición 5.2.1. Dado un alfabeto A, definimos el conjunto de *lenguajes de grafos sobre* A como el conjunto $\mathcal{P}(\mathsf{G}(A))$.

Recordamos que $\mathsf{G}(A)$ es el conjunto de todos los grafos sobre el alfabeto A definido en el capítulo 4. El conjunto $\mathcal{P}(\mathsf{G}(A))$ junto con las operaciones entre lenguajes de grafos que veremos a continuación, presenta la estructura de una alegoría de Kleene.

Definición 5.2.2. Sea A un alfabeto y sean $\mathcal{L}$ y $\mathcal{K} \in \mathcal{P}(\mathsf{G}(A))$ dos lenguajes sobre grafos, se definen las siguientes operaciones:

- *Producto:* $\mathcal{L} \cdot \mathcal{K} = \{G \cdot H \mid G \in \mathcal{L} \text{ y } H \in \mathcal{K}\}$.
- *Suma:* $\mathcal{L} + \mathcal{K} = \mathcal{L} \cup \mathcal{K}$, donde $\cup$ es la unión conjuntista.
- *Intersección:* $\mathcal{L} \cap \mathcal{K} = \{G \cap H \mid G \in \mathcal{L} \text{ y } H \in \mathcal{K}\}$.
- *Inverso:* $\mathcal{L}^o = \{G^o \mid G \in \mathcal{L}\}$.
- *Producto estrella:* $\mathcal{L}^* = \bigcup_{n\in\mathbb{N}} \mathcal{L}^n$.
- *Cero:* $0 = \emptyset$.
- *Identidad:* $1 = \{1^{\mathsf{G}(X)}\} = \{\overset{i=o}{\longrightarrow\circ\longrightarrow}\}$.

Así, $(\mathcal{P}(\mathsf{G}(A)), \cdot, +, \cap, ^*, ^o, 0, 1)$ es una *alegoría de Kleene*.

5.3. Partes de la $\Sigma^{\mathrm{Al}'}$-álgebra libre

A continuación presentamos otra álgebra que posee también estructura de alegoría de Kleene. Para ello, definimos la signatura $\Sigma^{\mathrm{Al}'}$:

Definición 5.3.1. Definimos la *signatura de una alegoría sin* $\top$ como la signatura $\Sigma^{\mathrm{Al}'} = (\Sigma_n^{\mathrm{Al}'})_{n\in\mathbb{N}}$ tal que $\Sigma_2^{\mathrm{Al}'} = \{\cdot, \cap\}, \Sigma_1^{\mathrm{Al}'} = \{^o\}, \Sigma_0^{\mathrm{Al}'} = \{1\}$ y $\Sigma_n^{\mathrm{Al}'} = \emptyset$ para $n > 2$.

Así, el conjunto de las partes del álgebra libre $\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(A)$, con las operaciones que se definen a continuación, es una alegoría de Kleene.

Definición 5.3.2. Sea A un alfabeto y sean $\mathcal{L}$ y $\mathcal{K} \in \mathcal{P}(\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(A))$ dos elementos del conjunto de las partes de la $\Sigma^{\mathrm{Al}'}$-álgebra libre, se definen las siguientes operaciones:

- *Producto:* $\mathcal{L} \cdot \mathcal{K} = \{p \cdot q \mid p \in \mathcal{L} \text{ y } q \in \mathcal{K}\}$.
- *Suma:* $\mathcal{L} + \mathcal{K} = \mathcal{L} \cup \mathcal{K}$, donde $\cup$ es la unión conjuntista.
- *Intersección:* $\mathcal{L} \cap \mathcal{K} = \{p \cap q \mid p \in \mathcal{L} \text{ y } q \in \mathcal{K}\}$.
- *Inverso:* $\mathcal{L}^o = \{p^o \mid p \in \mathcal{L}\}$.
- *Producto estrella:* $\mathcal{L}^* = \bigcup_{n\in\mathbb{N}} \mathcal{L}^n$.
- *Cero:* $0 = \emptyset$.
- *Identidad:* $1 = \{1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}\}$.

Es decir, $(\mathcal{P}(\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(A)), \cdot, +, \cap, ^*, ^o, 0, 1)$ es una *alegoría de Kleene*.

5.4. Teorema de decibilidad en alegorías de Kleene

Veremos en esta sección el tercer teorema de decibilidad que nos dará una doble equivalencia entre la validez de una inecuación entre relaciones, una inecuación entre lenguajes de grafos asociados a las relaciones y una inecuación entre elementos de $\mathcal{P}(\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X))$ asociados también a las relaciones. En primer lugar definimos inecuación universalmente válida para modelos relacionales como hicimos en los capítulos anteriores, pero esta vez consideramos términos en una alegoría de Kleene.

Definición 5.4.1. Dados dos términos $p, q \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$, diremos que la inecuación $p \subseteq q$ es *universalmente válida para modelos relacionales*, y escribiremos $\mathrm{Rel} \models p \subseteq q$ si y solo si, para todo conjunto C y para toda aplicación $f : X \longrightarrow \mathcal{P}(C \times C)$ se tiene que $f^{\#}(p) \subseteq f^{\#}(q)$.

De la misma forma que hicimos en decibilidad en álgebras de Kleene y decibilidad en alegorías, veamos ahora como ejemplo la demostración de la validez universal de una inecuación en modelos relacionales. Después del *Teorema de Decibilidad en Alegorías de Kleene* probaremos de nuevo esta inecuación pero utilizando los dos métodos que nos propone el tercer teorema de decibilidad.

Ejemplo 5.4.2. Sean $x, y \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$ términos en una alegoría de Kleene. Queremos probar que la siguiente inecuación entre términos es universalmente váida en modelos relacionales:

$$\mathrm{Rel} \models 1 \cap x \subseteq (x \cap x^o) + y$$

donde 1 es la identidad en una alegoría de Kleene.

Consideramos la interpretación relacional $f : X \longrightarrow \mathcal{P}(C \times C)$ que lleva, mediante el homomorfismo $f^{\#}$, los términos $1, x, y$ a las relaciones $1, \mathcal{R}, \mathcal{S}$ sobre un conjunto C cualquiera, respectivamente. Por tanto, podemos expresar la inecuación entre los términos $1, x, y$ como la siguiente inecuación entre relaciones:

$$1 \cap \mathcal{R} \subseteq (\mathcal{R} \cap \mathcal{R}^o) \cup \mathcal{S}$$

Probemos que se trata de una inecuación universalmente válida para modelos relacionales.

Demostración. Para probar que se cumple la inecuación veamos que dado $(a, b) \in 1 \cap \mathcal{R}$ entonces $(a, b) \in (\mathcal{R} \cap \mathcal{R}^o) \cup \mathcal{S}$.

Si $(a, b) \in 1 \cap \mathcal{R}$, entonces $a1b$ y $a\mathcal{R}b$, pero si $a1b$ sabemos que $a = b$ por lo que $(a, b) = (a, a)$ y sabemos que $a\mathcal{R}a$.

Por otro lado, si $(a, b) \in (\mathcal{R} \cap \mathcal{R}^o) \cup \mathcal{S}$, entonces $a\mathcal{S}b$ ó $a(\mathcal{R} \cap \mathcal{R}^o)b$, y si $a(\mathcal{R} \cap \mathcal{R}^o)b$, entonces $a\mathcal{R}b$ y $a\mathcal{R}^o b$.

Así, dado $(a, b) \in 1 \cap \mathcal{R}$, sabemos que $(a, b) = (a, a)$ y $a\mathcal{R}a$. De lo que se deduce que $a\mathcal{R}^o a$. Por tanto $a(\mathcal{R} \cap \mathcal{R}^o)a$. Y así $(a, b) = (a, a) \in (\mathcal{R} \cap \mathcal{R}^o) \cup \mathcal{S}$.

Por tanto queda probado que $1 \cap \mathcal{R} \subseteq (\mathcal{R} \cap \mathcal{R}^o) \cup \mathcal{S}$. □

Como podemos ver en el ejemplo, es necesaria la interpretación relacional f que va del conjunto de variables, X, en el conjunto de relaciones, $\mathcal{P}(C \times C)$ para poder trasladar una inecuación entre términos de una alegoría a una inecuación entre relaciones. De igual manera, necesitaremos una aplicación que vaya del conjunto de variables en el de lenguajes de grafos para poder proceder con ellos. La aplicación de la siguiente definición lleva los elementos $x \in X$ a lenguajes de grafos en $\mathcal{P}(\mathsf{G}(X))$.

Definición 5.4.3. Definimos $\mathcal{G}$ como la aplicación:

$$\begin{array}{rcl} \mathcal{G}\colon X & \longrightarrow & \mathcal{P}(\mathsf{G}(X)) \\ x & \longmapsto & \{\to \overset{i}{\circ} \xrightarrow{\quad x \quad} \overset{o}{\circ} \to\} = \{\mathsf{g}(x)\} \end{array}$$

Esta aplicación se puede extender a un homomorfismo.

Propiedad 5.4.4. *Sea la aplicación $\mathcal{G}$ de la definición anterior, como sabemos que $\mathcal{P}(\mathsf{G}(X))$ es una alegoría de Kleene, por la* propiedad universal del álgebra de términos *se puede extender $\mathcal{G}$ de forma única a un homomorfismo:*

$$\mathcal{G}^{\#} : \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X) \longrightarrow \mathcal{P}(\mathsf{G}(X))$$

tal que $\mathcal{G}^{\#} \cdot \eta_X = \mathcal{G}$, es decir, tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} X \arrow[r, "\mathcal{G}"] \arrow[dr, "\eta_X"'] & \mathcal{P}(\mathsf{G}(X)) \\ & \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X) \arrow[u, "\mathcal{G}^{\#}"'] \end{tikzcd}$$

Y necesitaremos también una aplicación que vaya del conjunto de variables en el de lenguajes sobre la $\Sigma^{\mathrm{Al}'}$-álgebra libre para poder proceder con ellos. La aplicación de la siguiente definición lleva los elementos $x \in X$ a conjuntos en $\mathcal{P}(\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X))$.

Definición 5.4.5. Definimos la aplicación $[\![\cdot]\!]$ como sigue:

$$\begin{array}{rcl} [\![\cdot]\!] : X & \longrightarrow & \mathcal{P}(\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)) \\ x & \longmapsto & \{x\} \end{array}$$

Propiedad 5.4.6. *Sea la aplicación $[\![\cdot]\!]$ de la definición anterior, como $\mathcal{P}(\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X))$ es una alegoría de Kleene, sabemos por la* propiedad universal del álgebra de términos *que $[\![\cdot]\!]$se puede extender a un único homomorfismo:*

$$[\![\cdot]\!]^{\#} : \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X) \longrightarrow \mathcal{P}(\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X))$$

tal que $[\![\cdot]\!]^{\#} \cdot \eta_X = [\![\cdot]\!]$.

$$\begin{tikzcd}
X \arrow[r, "[\![\cdot]\!]"] \arrow[dr, "\eta_X"'] & \mathcal{P}(\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)) \\
& \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X) \arrow[u, "[\![\cdot]\!]^{\#}"']
\end{tikzcd}$$

Así, mediante los homomorfismos que extienden las aplicaciones f, $\mathcal{G}$ y $[\![\cdot]\!]$, podemos movernos entre las tres alegorías de Kleene que hemos estudiado en este capítulo.

El *Teorema de Decibilidad en Alegorías de Kleene* nos aporta dos métodos distintos para poder asegurar que una inecuación entre dos términos de una alegoría de Kleene es universalmente válida en todo modelo relacional. Para poder presentar este resultado introducimos la siguiente definición.

Definición 5.4.7. Sean $p', q' \in \mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)$, decimos que p' *es menor o igual que* q' y escribimos $p' \lhd q'$ si y solo si $\mathtt{g}^{\#}(p') \blacktriangleleft \mathtt{g}^{\#}(q')$

Nota. Notamos que si p es un término en $\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$, tiene sentido el conjunto

$$^{\lhd}[\![p]\!]^{\#} = \{q \in \mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X) \mid \exists w \in [\![p]\!]^{\#} : q \lhd w\}$$

Por la definición, $q \lhd w$ si y solo si $\mathtt{g}^{\#}(q) \blacktriangleleft \mathtt{g}^{\#}(w)$, es decir, estamos considerando grafos sobre $\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)$.Como hemos definido los grafos $\mathtt{g}^{\#}(p)$ para términos $p \in \mathrm{T}_{\Sigma^{\mathrm{Al}}}(X)$ en el capítulo 4 y $\Sigma^{\mathrm{Al}'} \subseteq \Sigma^{\mathrm{Al}}$, el conjunto $^{\lhd}[\![p]\!]^{\#}$ está bien definido.

El último teorema de decibilidad da, como se ha dicho, dos métodos distintos para determinar si una inecuación entre términos de una alegoría de Kleene es universalmente válida para todo modelo relacional. Uno de ellos interpreta los términos como lenguajes de grafos mediante el homomorfismo $\mathcal{G}^{\#}$. Para el otro método interpretamos los términos como lenguajes sobre la $\Sigma^{\mathrm{Al}'}$-álgebra libre mediante el homomorfismo $[\![\cdot]\!]^{\#}$. Presentamos el teorema a continuación:

Teorema 5.4.8. *Sean $p, q \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$ términos de una alegoría de Kleene. Entonces son equivalentes:*

1) $Rel \models p \subseteq q$

2) $[\![p]\!]^{\#} \subseteq^{\lhd} [\![q]\!]^{\#}$

3) $\mathcal{G}^{\#}(p) \subseteq^{\blacktriangleleft} \mathcal{G}^{\#}(q)$.

Para poder probar este teorema de decibilidad necesitamos algunos lemas técnicos. El lema al *Teorema de Decibilidad en Alegorías de Kleene* que se da a continuación relaciona las extensiones, $\mathcal{G}^{\#}$ y $[\![\cdot]\!]^{\#}$, de las dos aplicaciones que hemos definido en esta sección.

Lema 5.4.9. *Sea $p \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$ se cumple la siguiente igualdad:*

$$\mathcal{G}^{\#}(p) = \{\mathsf{g}^{\#}(w) \mid w \in [\![p]\!]^{\#}\}$$

Nota. Recordamos que la aplicación $\mathsf{g}^{\#} : \mathrm{T}_{\Sigma^{\mathrm{AI}}}(X) \longrightarrow \mathsf{G}(X)$ es la que extiende a la aplicación:

$$\begin{array}{rcl} \mathsf{g} : X & \longrightarrow & \mathsf{G}(X) \\ x & \longmapsto & \mathsf{g}(x) \equiv \longrightarrow \overset{i}{\circ} \xrightarrow{\quad x \quad} \overset{o}{\circ} \longrightarrow \end{array}$$

Demostración. Probaremos la igualdad por inducción sobre la estructura del término $p \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$. Notamos que p puede ser de la forma:

(1) $p = x$ para alguna variable $x \in X$.

(2) $p = 0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}$.

(3) $p = 1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}$.

(4) $p = q^*$ para algún $q \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$.

(5) $p = q^o$ para algún $q \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$.

(6) $p = q \cdot r$ para algunos términos $q, r \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$.

(7) $p = q + r$ para algunos términos $q, r \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$.

(8) $p = q \cap r$ para algunos términos $q, r \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$.

Comprobaremos la igualdad en cada caso.

(1) Sea $p = x$ una variable en X, entonces:

$$\begin{aligned} \mathcal{G}^{\#}(x) = & \ \{\mathsf{g}(x)\} \\ = & \ \{\mathsf{g}^{\#}(x)\} \\ = & \ \{\mathsf{g}^{\#}(w) \mid w \in \{x\}\} \\ = & \ \{\mathsf{g}^{\#}(w) \mid w \in [\![x]\!]^{\#}\} \end{aligned}$$

ya que $[\![x]\!]^{\#} = \{x\}$.

(2) Sea $p = 0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}$ el cero del álgebra de términos, entonces:

$$\begin{aligned}\mathcal{G}^{\#}(0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}) &= \emptyset \\ &= \{\mathsf{g}^{\#}(w) \mid w \in \emptyset\} \\ &= \{\mathsf{g}^{\#}(w) \mid w \in [\![0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}]\!]^{\#}\}\end{aligned}$$

ya que $[\![0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}]\!]^{\#} = \emptyset$.

(3) Sea $p = 1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}$ el término identidad del álgebra de términos, entonces:

$$\begin{aligned}\mathcal{G}^{\#}(1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}) &= \{1^{\mathsf{G}}\} \\ &= \{\mathsf{g}^{\#}(1^{\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)})\} \\ &= \{\mathsf{g}^{\#}(w) \mid w \in \{1^{\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)}\}\} \\ &= \{\mathsf{g}^{\#}(w) \mid w \in [\![1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}]\!]^{\#}\}\end{aligned}$$

ya que $[\![1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}]\!]^{\#} = \{1^{\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)}\}$.

(4) Si $p = q^*$ es el producto estrella de un término $q \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$, entonces:

$$\begin{aligned}\mathcal{G}^{\#}(q^*) &\overset{\mathcal{G}^{\#}Hom}{=} \mathcal{G}^{\#}(q)^* \\ &\overset{Def}{=} \bigcup_{n\in\mathbb{N}} \mathcal{G}^{\#}(q)^n \\ &\overset{H.I.}{=} \bigcup_{n\in\mathbb{N}} \{\mathsf{g}^{\#}(w) \mid w \in [\![q]\!]^{\#}\}^n \\ &= \bigcup_{n\in\mathbb{N}} \{\mathsf{g}^{\#}(w_0)\dots\mathsf{g}^{\#}(w_{n-1}) \mid w_0,\dots,w_{n-1} \in [\![q]\!]^{\#}\} \\ &\overset{\mathsf{g}^{\#}Hom}{=} \bigcup_{n\in\mathbb{N}} \{\mathsf{g}^{\#}(w_0\dots w_{n-1}) \mid w_0\dots w_{n-1} \in ([\![q]\!]^{\#})^n\} \\ &= \bigcup_{n\in\mathbb{N}} \{\mathsf{g}^{\#}(v) \mid v \in ([\![q]\!]^{\#})^n\} \\ &= \{\mathsf{g}^{\#}(v_0) \mid v_0 \in ([\![q]\!]^{\#})^0\} \cup \dots \\ &\quad \dots \cup \{\mathsf{g}^{\#}(v_{n-1}) \mid v_{n-1} \in ([\![q]\!]^{\#})^{n-1}\} \\ &= \{\mathsf{g}^{\#}(u) \mid u \in \big(([\![q]\!]^{\#})^0 \cup \dots \cup ([\![q]\!]^{\#})^{n-1}\big)\} \\ &\overset{[\![\cdot]\!]^{\#}Hom}{=} \{\mathsf{g}^{\#}(u) \mid u \in \textstyle\bigcup_{n\in\mathbb{N}}([\![q]\!]^{\#})^n\} \\ &\overset{Def}{=} \{\mathsf{g}^{\#}(u) \mid u \in ([\![q]\!]^{\#})^*\} \\ &\overset{[\![\cdot]\!]^{\#}Hom}{=} \{\mathsf{g}^{\#}(u) \mid u \in [\![q^*]\!]^{\#}\}.\end{aligned}$$

(5) Sea $p = q^o$ el término opuesto de $q \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$, entonces:

$$\begin{array}{rcl} \mathcal{G}^{\#}(q^o) & \stackrel{\mathcal{G}^{\#}Hom}{=} & \mathcal{G}^{\#}(q)^o \\ & \stackrel{H.I.}{=} & \{\mathsf{g}^{\#}(w) \mid w \in [\![q]\!]^{\#}\}^o \\ & \stackrel{Def}{=} & \{\mathsf{g}^{\#}(w)^o \mid w \in [\![q]\!]^{\#}\} \\ & = & \{\mathsf{g}^{\#}(w^o) \mid w \in [\![q]\!]^{\#}\} \\ & = & \{\mathsf{g}^{\#}(w) \mid w \in [\![q^o]\!]^{\#}\}. \end{array}$$

(6) Sea el término $p = q \cdot r$ resultado del producto de los dos términos $q, r \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$. Entonces:

$$\begin{array}{rcl} \mathcal{G}^{\#}(q \cdot r) & \stackrel{\mathcal{G}^{\#}Hom}{=} & \mathcal{G}^{\#}(q) \cdot \mathcal{G}^{\#}(r) \\ & \stackrel{H.I.}{=} & \{\mathsf{g}^{\#}(w) \mid w \in [\![q]\!]^{\#}\} \cdot \{\mathsf{g}^{\#}(v) \mid v \in [\![r]\!]^{\#}\} \\ & \stackrel{Def}{=} & \{\mathsf{g}^{\#}(w) \cdot \mathsf{g}^{\#}(v) \mid w \in [\![]\!]^{\#}, v \in [\![r]\!]^{\#}\} \\ & \stackrel{\mathsf{g}^{\#}Hom}{=} & \{\mathsf{g}^{\#}(w \cdot v) \mid w \cdot v \in [\![q]\!]^{\#} \cdot [\![r]\!]^{\#}\} \\ & \stackrel{[\![\cdot]\!]^{\#}Hom}{=} & \{\mathsf{g}^{\#}(u) \mid u \in [\![q \cdot r]\!]^{\#}\}. \end{array}$$

(7) Si $p = q+r$ es el término suma de los términos $q, r \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$. Entonces:

$$\begin{array}{rcl} \mathcal{G}^{\#}(q + r) & \stackrel{\mathcal{G}^{\#}Hom}{=} & \mathcal{G}^{\#}(q) + \mathcal{G}^{\#}(r) \\ & \stackrel{Def}{=} & \mathcal{G}^{\#}(q) \cup \mathcal{G}^{\#}(r) \\ & \stackrel{H.I.}{=} & \{\mathsf{g}^{\#}(w) \mid w \in [\![q]\!]^{\#}\} \cup \{\mathsf{g}^{\#}(v) \mid v \in [\![r]\!]^{\#}\} \\ & \stackrel{Def}{=} & \{\mathsf{g}^{\#}(u) \mid u \in [\![q]\!]^{\#} \cup [\![r]\!]^{\#}\} \\ & \stackrel{[\![\cdot]\!]^{\#}Hom}{=} & \{\mathsf{g}^{\#}(u) \mid u \in [\![q + r]\!]^{\#}\}. \end{array}$$

(8) Sea $p = q \cap r$ la intersección de los términos $q, r \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$. Entonces:

$$\begin{array}{rcl} \mathcal{G}^{\#}(q \cap r) & \stackrel{\mathcal{G}^{\#}Hom}{=} & \mathcal{G}^{\#}(q) \cap \mathcal{G}^{\#}(r) \\ & \stackrel{H.I.}{=} & \{\mathsf{g}^{\#}(w) \mid w \in [\![q]\!]^{\#}\} \cap \{\mathsf{g}^{\#}(v) \mid v \in [\![r]\!]^{\#}\} \\ & \stackrel{Def}{=} & \{\mathsf{g}^{\#}(w) \cap \mathsf{g}^{\#}(v) \mid w \in [\![q]\!]^{\#}, v \in [\![r]\!]^{\#}\} \\ & \stackrel{\mathsf{g}^{\#}Hom}{=} & \{\mathsf{g}^{\#}(w \cap v) \mid w \cap v \in [\![q]\!]^{\#} \cap [\![r]\!]^{\#}\} \\ & \stackrel{[\![\cdot]\!]^{\#}Hom}{=} & \{\mathsf{g}^{\#}(u) \mid u \in [\![q \cap r]\!]^{\#}\}. \end{array}$$

Así queda probado que $\mathcal{G}^{\#}(p) = \{\mathsf{g}^{\#}(w) \mid w \in [\![p]\!]^{\#}\}$, para todo término $p \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$. □

A continuación veremos el segundo lema al *Teorema de Decibilidad en Alegorías de Kleene*. Este resultado relaciona la extensión $f^{\#}\colon \mathrm{T}_{\Sigma\mathrm{AK}}(X) \longrightarrow \mathcal{P}(C{\times}C)$ de una interpretación relacional cualquiera, $f\colon X \longrightarrow \mathcal{P}(C{\times}C)$, con la extensión $[\![\cdot]\!]^{\#}\colon \mathrm{T}_{\Sigma\mathrm{AK}}(X) \longrightarrow \mathcal{P}(\mathrm{T}_{\Sigma\mathrm{Al}'}(X))$ de la aplicación $[\![\cdot]\!]$ definida en la sección anterior. Es en este lema donde surge el problema con la operación constante $\top$, ya que hay distintas formas de interpretarla en lenguajes de grafos. Veamos el lema:

Lema 5.4.10. *Para todo término $p \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$ y toda interpretación relacional $f\colon X \longrightarrow \mathcal{P}(C \times C)$, se tiene:*

$$f^{\#}(p) = \bigcup_{w \in [\![p]\!]^{\#}} f^{\#}(w).$$

Demostración. Probaremos la igualdad por inducción sobre la estructura del término $p \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$. Recordamos que p puede ser de la forma:

(1) $p = x$ para alguna variable $x \in X$.

(2) $p = 0^{\mathrm{T}_{\Sigma\mathrm{AK}}(X)}$.

(3) $p = 1^{\mathrm{T}_{\Sigma\mathrm{AK}}(X)}$.

(4) $p = q^*$ para algún $q \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$.

(5) $p = q^o$ para algún $q \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$.

(6) $p = q \cdot r$ para algunos términos $q, r \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$.

(7) $p = q + r$ para algunos términos $q, r \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$.

(8) $p = q \cap r$ para algunos términos $q, r \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$.

Comprobaremos la igualdad en cada caso.

(1) Sea $p = x$ una variable en X, entonces:

$$\begin{aligned} f^{\#}(x) &= \bigcup_{w \in \{x\}} f^{\#}(w) \\ &= \bigcup_{w \in [\![x]\!]^{\#}} f^{\#}(w) \end{aligned}$$

ya que $[\![x]\!]^{\#} = \{x\}$.

(2) Sea $p = 0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}$ el cero del álgebra de términos, entonces:

$$\begin{aligned} f^{\#}(0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}) &= \emptyset \\ &= \bigcup_{w \in \emptyset} f^{\#}(w) \\ &= \bigcup_{w \in [\![0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}]\!]^{\#}} f^{\#}(w) \end{aligned}$$

ya que $[\![0^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}]\!]^{\#} = \emptyset$.

(3) Sea $p = 1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}$ el término identidad del álgebra de términos, entonces:

$$\begin{aligned} f^{\#}(1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}) &= \bigcup_{w \in \{1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}\}} f^{\#}(w) \\ &= \bigcup_{w \in [\![1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}]\!]^{\#}} f^{\#}(w) \end{aligned}$$

ya que $[\![1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}]\!]^{\#} = 1^{\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)} = \{1^{\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)}\}$.

(4) Si $p = q^*$ es el producto estrella de un término $q \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$, entonces: Probamos primero que para todo $n \in \mathbb{N}$ se cumple:

$$f^{\#}(q^n) = \bigcup_{w \in [\![q^n]\!]^{\#}} f^{\#}(w).$$

Consideramos $w = w_0 \dots w_{n-1} \in ([\![q]\!]^{\#})^n = [\![q^n]\!]^{\#}$

$$\begin{aligned} f^{\#}(q^n) &\overset{f^{\#} Hom}{=} f^{\#}(q)^n \\ &= f^{\#}(q) \overset{n)}{\dots} f^{\#}(q) \\ &\overset{H.I.}{=} \Big(\bigcup_{w_0 \in [\![q]\!]^{\#}} f^{\#}(w_0) \Big) \dots \Big(\bigcup_{w_{n-1} \in [\![q]\!]^{\#}} f^{\#}(w_{n-1}) \Big) \\ &= \bigcup_{\substack{w_0 \in [\![q]\!]^{\#} \\ \dots \\ w_{n-1} \in [\![q]\!]^{\#}}} \Big(f^{\#}(w_0) \dots f^{\#}(w_{n-1}) \Big) \\ &\overset{f^{\#} Hom}{=} \bigcup_{w_0 \dots w_{n-1} \in ([\![q]\!]^{\#})^n} f^{\#}(w_0 \dots w_{n-1}) \\ &\overset{[\![\cdot]\!]^{\#} Hom}{=} \bigcup_{w \in [\![q^n]\!]^{\#}} f^{\#}(w). \end{aligned}$$

Y por tanto

$$
\begin{array}{rcl}
f^{\#}(q^*) & \overset{f^{\#}Hom}{=} & (f^{\#}(q))^* \\
& \overset{Def}{=} & \bigcup\limits_{n\in\mathbb{N}} (f^{\#}(q))^n \\
& \overset{H.I.}{=} & \bigcup\limits_{n\in\mathbb{N}} \Big(\bigcup\limits_{w\in[\![q]\!]^{\#}} f^{\#}(w) \Big)^n \\
& = & \bigcup\limits_{n\in\mathbb{N}} \Big(\bigcup\limits_{w\in[\![q^n]\!]^{\#}} f^{\#}(w) \Big) \\
& = & \bigcup\limits_{w\in \bigcup\limits_{n\in\mathbb{N}} [\![q^n]\!]^{\#}} f^{\#}(w) \\
& = & \bigcup\limits_{w\in[\![q^*]\!]^{\#}} f^{\#}(w).
\end{array}
$$

(5) Sea $p = q^o$ el término opuesto de $q \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$, entonces:

$$
\begin{array}{rcl}
f^{\#}(q^o) & \overset{f^{\#}Hom}{=} & f^{\#}(q)^o \\
& \overset{H.I.}{=} & \Big(\bigcup\limits_{w\in[\![q]\!]^{\#}} f^{\#}(w) \Big)^o \\
& = & \bigcup\limits_{w\in[\![q]\!]^{\#}} \Big(f^{\#}(w) \Big)^o \\
& = & (*)
\end{array}
$$

Si $(a,b) \in f^{\#}(q^o)$, existe $w \in [\![q]\!]^{\#}$ tal que $(a,b) \in (f^{\#}(w))^o$. Entonces $(b,a) \in f^{\#}(w)$ y por tanto $(a,b) \in f^{\#}(w^o)$. Así:

$$
\begin{array}{rcl}
(*) & = & \bigcup\limits_{w\in[\![q]\!]^{\#}} f^{\#}(w^o) \\
& = & \bigcup\limits_{w\in[\![q^o]\!]^{\#}} f^{\#}(w)
\end{array}
$$

ya que $[\![q^o]\!]^{\#} \overset{[\![\cdot]\!]^{\#}Hom}{=} ([\![q]\!]^{\#})^o = \{w^o \mid w \in [\![q]\!]^{\#}\}$.

(6) Sea el término $p = q \cdot r$ resultado del producto de los dos términos

$q, r \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$. Entonces:

$$\begin{aligned}
f^{\#}(q \cdot r) &\overset{f^{\#}Hom}{=} f^{\#}(q) \cdot f^{\#}(r) \\
&\overset{H.I.}{=} \Big(\bigcup_{v \in [\![q]\!]^{\#}} f^{\#}(v)\Big) \cdot \Big(\bigcup_{u \in [\![r]\!]^{\#}} f^{\#}(u)\Big) \\
&= \bigcup_{\substack{v \in [\![q]\!]^{\#} \\ u \in [\![r]\!]^{\#}}} f^{\#}(v) \cdot f^{\#}(u) \\
&\overset{f^{\#}Hom}{=} \bigcup_{\substack{v \in [\![q]\!]^{\#} \\ u \in [\![r]\!]^{\#}}} f^{\#}(v \cdot u) \\
&= \bigcup_{w \in [\![q \cdot r]\!]^{\#}} f^{\#}(w)
\end{aligned}$$

ya que $[\![q \cdot r]\!]^{\#} = \{v \cdot u \mid v \in [\![q]\!]^{\#}, u \in [\![r]\!]^{\#}\}$.

(7) Si $p = q + r$ es el término suma de los términos $q, r \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$. Entonces:

$$\begin{aligned}
f^{\#}(q + r) &\overset{f^{\#}Hom}{=} f^{\#}(q) \cup f^{\#}(r) \\
&\overset{H.I.}{=} \Big(\bigcup_{v \in [\![q]\!]^{\#}} f^{\#}(v)\Big) \cup \Big(\bigcup_{u \in [\![r]\!]^{\#}} f^{\#}(u)\Big) \\
&= \bigcup_{w \in [\![q]\!]^{\#} \cup [\![r]\!]^{\#}} f^{\#}(w) \\
&\overset{[\![\cdot]\!]^{\#}Hom}{=} \bigcup_{w \in [\![q+r]\!]^{\#}} f^{\#}(w).
\end{aligned}$$

(8) Sea $p = q \cap r$ la intersección de los términos $q, r \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$. Entonces:

$$\begin{aligned}
f^{\#}(q \cap r) &\overset{f^{\#}Hom}{=} f^{\#}(q) \cap f^{\#}(r) \\
&\overset{H.I.}{=} \Big(\bigcup_{v \in [\![q]\!]^{\#}} f^{\#}(v)\Big) \cap \Big(\bigcup_{u \in [\![r]\!]^{\#}} f^{\#}(u)\Big) \\
&= \bigcup_{\substack{v \in [\![q]\!]^{\#} \\ u \in [\![r]\!]^{\#}}} f^{\#}(v) \cap f^{\#}(u) \\
&\overset{f^{\#}Hom}{=} \bigcup_{\substack{v \in [\![q]\!]^{\#} \\ u \in [\![r]\!]^{\#}}} f^{\#}(v \cap u) \\
&= \bigcup_{w \in [\![q \cap r]\!]^{\#}} f^{\#}(w)
\end{aligned}$$

ya que $[\![q \cap r]\!]^{\#} = \{v \cap u \mid v \in [\![q]\!]^{\#}, u \in [\![r]\!]^{\#}\}$.

De esta forma queda probado que para todo término $p \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$ se cumple el resultado. $\square$

Como extensión al lema anterior, Lema 5.4.10, se da el siguiente resultado:

Corolario 5.4.11. *Para todo término $p \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$ y toda interpretación relacional $f\colon X \longrightarrow \mathcal{P}(C \times C)$, se tiene:*

$$f^{\#}(p) = \bigcup_{v \in^{\triangleleft} [\![p]\!]^{\#}} f^{\#}(v)$$

Demostración. Sea $v \in^{\triangleleft} [\![p]\!]^{\#}$, entonces existe $w \in [\![p]\!]^{\#}$ tal que $v \triangleleft w$, es decir, $\mathtt{g}(v) \blacktriangleleft \mathtt{g}(w)$. Entonces, por el *Teorema de Decibilidad en Alegorías Rel* $\models v \subseteq w$ y, en particular, $f^{\#}(v) \subseteq f^{\#}(w)$. A su vez, $f^{\#}(w) \subseteq \bigcup_{u \in [\![p]\!]^{\#}} f^{\#}(u)$ que, por el lema 5.4.10, es $f^{\#}(p)$. Es decir,

$$f^{\#}(v) \subseteq f^{\#}(w) \subseteq \bigcup_{u \in [\![p]\!]^{\#}} f^{\#}(u) = f^{\#}(p).$$

Y, por tanto

$$\bigcup_{v \in^{\triangleleft} [\![p]\!]^{\#}} f^{\#}(v) \subseteq f^{\#}(p).$$

Veamos la otra inclusión para comprobar que se da la igualdad.

Por el lema 5.4.10, $f^{\#}(p) = \bigcup_{w \in [\![p]\!]^{\#}} f^{\#}(w)$. Notemos que para todo $w \in [\![p]\!]^{\#}$, $w \triangleleft w$ ya que $\mathtt{g}(w) \blacktriangleleft \mathtt{g}(w)$. Entonces $w \in^{\triangleleft} [\![p]\!]^{\#}$. Así, $f^{\#}(w) \subseteq \bigcup_{v \in^{\triangleleft} [\![p]\!]^{\#}} f^{\#}(v)$. Y, por tanto:

$$f^{\#}(p) = \bigcup_{w \in [\![p]\!]^{\#}} f^{\#}(w) \subseteq \bigcup_{v \in^{\triangleleft} [\![p]\!]^{\#}} f^{\#}(v)$$

Con lo que queda probado el corolario. $\square$

A lo largo de la demostracion del tercer teorema de decibilidad utilizaremos, además de los dos lemas de esta sección, el lema 4.3.6 que probamos en el Capítulo 4, Decibilidad en Alegorías, y que es válido también en $\mathrm{T}_{\Sigma^{\mathrm{AI}'}}(X)$ ya que no aparece ninguna operación nueva.

Recordemos el lema.

Lema 4.3.6. *Sea $p \in \mathrm{T}_{\Sigma^{\mathrm{AI}}}(X)$, sea $\mathtt{g}^{\#}(p) = (V, E, s, t, l, i, o)$ el grafo asociado al término p. Sea C un conjunto y sea $f\colon X \longrightarrow \mathcal{P}(C \times C)$ una* *asignación de relaciones a las variables en* X*. Entonces, para todo* $a, b \in C$ *se tiene que* $(a, b) \in f^{\#}(p)$ *si y solo si existe una aplicación* $\phi : V \longrightarrow C$ *tal que:*

(I) $\phi(i) = a$

(II) $\phi(o) = b$

(III) *Si* $e \in E$ *es un eje cumpliendo*

$$\left.\begin{array}{l} s(e) = v \\ t(e) = w \\ l(e) = x \end{array}\right\} \text{ entonces } (\phi(v), \phi(w)) \in f(x).$$

Ahora sí nos encontramos en condiciones de probar el último teorema de decibilidad: *Teorema de Decibilidad en Alegorías de Kleene.*

Recordemos el teorema:

Teorema 5.4.8 *Sean* $p, q \in \mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$ *términos de una alegoría de Kleene. Entonces son equivalentes:*

1) $Rel \models p \subseteq q$

2) $[\![p]\!]^{\#} \subseteq^{\triangleleft} [\![q]\!]^{\#}$

3) $\mathcal{G}^{\#}(p) \subseteq^{\blacktriangleleft} \mathcal{G}^{\#}(q)$.

Demostración. *1)* $\Rightarrow$ *3)* Sea $\mathsf{g}(w) \in \mathcal{G}^{\#}(p)$ con $w \in [\![p]\!]^{\#}$. Fijamos la notación $\mathsf{g}(w) = (V_w, E_w, s_w, t_w, l_w, i_w, o_w)$. Consideramos la aplicación:

$$\begin{array}{rcl} f \colon X & \longrightarrow & \mathcal{P}(V_w \times V_w) \\ x & \longmapsto & \{(v, v') \in V_w \times V_w \mid \exists e \in E_w : \\ & & : s_w(e) = v, t_w(e) = v' \text{ y } l_w(e) = x\} \end{array}$$

Por el lema 4.3.6 $(i_w, o_w) \in f^{\#}(w) \subseteq \bigcup_{w \in [\![p]\!]^{\#}} f^{\#}(w) = f^{\#}(p)$, donde la última igualdad se da por el lema 5.4.10. Y por hipótesis $f^{\#}(p) \subseteq f^{\#}(q)$. De nuevo por el lema 5.4.10 $f^{\#}(q) = \bigcup_{v \in [\![q]\!]^{\#}} f^{\#}(v)$. Entonces existe $v \in [\![q]\!]^{\#}$ tal que $(i_w, o_w) \in f^{\#}(v)$. Aplicando de nuevo el lema 4.3.6 existe una aplicación $\phi \colon V_v \longrightarrow V_w$ tal que, como vimos en la demostración del segundo teorema de decibilidad, asegura la existencia de un homomorfismo de $\mathsf{g}(v)$ en $\mathsf{g}(w)$. Así $\mathsf{g}(w) \blacktriangleleft \mathsf{g}(v)$ y por tanto $\mathcal{G}^{\#}(p) \subseteq^{\blacktriangleleft} \mathcal{G}^{\#}(q)$.

3) ⇒ 2) Sea $w \in [\![p]\!]^{\#}$, por el lema 5.4.9 $\mathtt{g}(w) \in \mathcal{G}^{\#}(p)$. Por hipótesis existe $\mathtt{g} \in \mathcal{G}^{\#}(q)$ tal que $\mathtt{g}(w) \blacktriangleleft \mathtt{g}$. Ahora bien, como $\mathtt{g} \in \mathcal{G}^{\#}(q)$, por el lema 5.4.10, entonces $\mathtt{g} = \mathtt{g}(u)$ con $u \in [\![q]\!]^{\#}$. Así $\mathtt{g}(w) \blacktriangleleft \mathtt{g}(u)$ con $u \in [\![q]\!]^{\#}$, lo que implica que $w \triangleleft u$, y por tanto, $w \in^{\triangleleft} [\![q]\!]^{\#}$. Y así: $[\![p]\!]^{\#} \subseteq^{\triangleleft} [\![q]\!]^{\#}$.

2) ⇒ 1) Sea f una interpretación relacional, $f\colon X \longrightarrow \mathcal{P}(C \times C)$. Queremos probar que $f^{\#}(p) \subseteq f^{\#}(q)$. Por el lema 5.4.10 $f^{\#}(p) = \bigcup_{w \in [\![p]\!]^{\#}} f^{\#}(w)$. Por hipótesis $\bigcup_{w \in [\![p]\!]^{\#}} f^{\#}(w) \subseteq \bigcup_{u \in^{\triangleleft} [\![q]\!]^{\#}} f^{\#}(u)$. Ahora bien, por el corolario 5.4.11 $\bigcup_{u \in^{\triangleleft} [\![q]\!]^{\#}} f^{\#}(u) = f^{\#}(q)$. Y así, $f^{\#}(p) \subseteq f^{\#}(q)$. □

Retomamos ahora el ejemplo 5.4.2:

Ejemplo 5.4.12. Al comienzo de la sección probamos, en el ejemplo 5.4.2, que se cumple la siguiente expresión:

$$\mathrm{Rel} \models 1 \cap x \subseteq (x \cap x^{o}) + y$$

para términos $1, x, y \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$.

Para ello, demostramos que dadas $1, \mathcal{R}$ y $\mathcal{S}$ relaciones sobre un conjunto C cualquiera asociadas mediante una asignación relacional f a los términos $1, x, y$, la inecuación:

$$1 \cap \mathcal{R} \subseteq (\mathcal{R} \cap \mathcal{R}^{o}) \cup \mathcal{S}$$

se cumple.

Como hemos visto, el *Teorema de Decibilidad en Alegorías de Kleene* proporciona dos métodos para probar la validez de una expresión como la anterior. Utilizaremos a continuación ambos métodos para demostrar que se cumple:

$$\mathrm{Rel} \models 1 \cap x \subseteq (x \cap x^{o}) + y$$

donde $1, x, y \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$.

Veamos en primer lugar como probar la expresión utilizando el homomorfismo $[\![\cdot]\!]^{\#}$ que extiende a la aplicación $[\![\cdot]\!]\colon X \longrightarrow \mathcal{P}(\mathrm{T}_{\Sigma\mathrm{Al}'}(X))$, es decir, utilizando lenguajes sobre el álgebra libre $\mathrm{T}_{\Sigma\mathrm{Al}'}(X)$. Para ello hemos de demostrar que se cumple la siguiente expresión:

$$[\![1 \cap x]\!]^{\#} \subseteq^{\triangleleft} [\![(x \cap x^{o}) + y]\!]^{\#}.$$

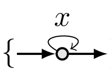
Probémoslo:

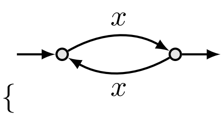
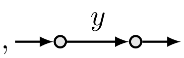
Demostración. $[\![1 \cap x]\!]^{\#} = [\![1]\!]^{\#} \cap [\![x]\!]^{\#} = \{\lambda\} \cap \{x\} = \emptyset$ y, claramente, $\emptyset \subseteq^{\triangleleft} [\![(x \cap x^{o}) + y]\!]^{\#}$. Por lo que queda probada la expresión. □

Por otro lado, podemos probar la validez de la expresión utilizando el homomorfismo $\mathcal{G}^{\#}$ que extiende a la aplicación $\mathcal{G}\colon X \longrightarrow \mathcal{P}(\mathsf{G}(X))$, es decir, utilizando lenguajes de grafos. Así, el segundo método asegura que la expresión $\mathrm{Rel} \models 1 \cap x \subseteq (x \cap x^o) + y$ es válida si y solo si se cumple:

$$\mathcal{G}^{\#}(1 \cap x) \subseteq^{\blacktriangleleft} \mathcal{G}^{\#}((x \cap x^o) + y).$$

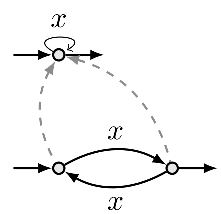
Probemos que así es:

Demostración. $\mathcal{G}^{\#}(1 \cap x) = \{$  $\}$

Por otro lado, $\mathcal{G}^{\#}((x \cap x^o) + y) = \{$  ,  $\}$

Y dado que existe un homomorfismo de uno de los grafos del conjunto $\mathcal{G}^{\#}((x \cap x^o) + y)$ en el grafo del conjunto $\mathcal{G}^{\#}(1 \cap x)$, podemos asegurar que se cumple $\mathcal{G}^{\#}(1 \cap x) \subseteq^{\blacktriangleleft} \mathcal{G}^{\#}((x \cap x^o) + y)$.

El homomorfismo del que hablamos es el siguiente:



Y así queda probado por este segundo método que se cumple la expresión $\mathrm{Rel} \models 1 \cap x \subseteq (x \cap x^o) + y$ para cualesquiera términos $1, x, y \in \mathrm{T}_{\Sigma\mathrm{AK}}(X)$, donde, recordamos, 1 es el término identidad de la alegoría de Kleene. $\square$

Este ejemplo muestra que para ecuaciones relativamente sencillas, resulta más cómodo trabajar con lenguajes de grafos o con lenguajes sobre el álgebra $\mathrm{T}_{\Sigma\mathrm{Al}'}(X)$ para probar la validez de una ecuación en modelos relacionales que probarlo mediante las propiedades de las relaciones directamente como hicimos en el ejemplo 5.4.2. Pero, ¿qué ocurre cuando las ecuaciones a probar son más complicadas? En *Automata for relation algebra and formal proofs* [16], D.Pous explica que él y P.Brunet propusieron un modelo de autómata que permite reconocer lenguajes de grafos asociados a expresiones. Este modelo de autómata se inspira en las redes de Petri (ver [13, 12]) que permiten estudiar estructuras más complejas que las palabras. A cada expresión p, se le asocia lo que han llamado un autómata de Petri, cuyo lenguaje es precisamente $^{\blacktriangleleft}\mathcal{G}^{\#}(p)$. De esta forma, el problema de la validez de ecuaciones o inecuaciones se reduce, gracias al Teorema de Decibilidad en Alegorías de Kleene, a comparar autómatas de Petri. (Véase [3].) Este modelo tiene algunas restricciones de cálculo, por ejemplo deja fuera la intersección y la constante asociada, $\top$. En la línea de obtener una generalización para el cálculo completo, Brunet ha demostrado un teorema de Kleene para su modelo de autómatas de forma que la decibilidad de cualquier ecuacion o inecuación es equivalente a la decibilidad de ese modelo de autómata. (Véase [2].)

En este capítulo hemos definido la signatura algebraica de una alegoría de Kleene: Σ^{AK}, y la consiguiente álgebra de términos, $\mathrm{T}_{\Sigma^{\mathrm{AK}}}(X)$. Hemos visto que el conjunto de las relaciones admite estructura de Σ^{AK}-álgebra con las operaciones composición, unión, intersección, clausura reflexivo-transitiva, inverso, relación vacía e identidad. Además, hemos presentado los lenguajes de grafos y las partes del álgebra libre $\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)$. Hemos definido las operaciones necesarias en cada uno de estos conjuntos de forma que admitan estructura de alegoría de Kleene. Finalmente hemos probado algunos lemas que nos ha permitido demostrar el Teorema de Decibilidad en Alegorías de Kleene. Este teorema proporciona dos métodos para determinar la validez de una ecuación relacional utilizando bien lenguajes de grafos, bien lenguajes sobre el álgebra $\mathrm{T}_{\Sigma^{\mathrm{Al}'}}(X)$. Como ya hemos visto, esos procedimientos se pueden llevar a cabo con el uso de autómatas finitos de forma que la tarea se reduce a introducir una serie de datos a un algoritmo ya existente, haciéndola así menos tediosa que la prueba mediante propiedades relacionales.

Conclusiones

Nuestro objetivo a lo largo del trabajo ha consitido en el estudio de la decibilidad de ecuaciones e inecuaciones en modelos relacionales. Para ello hemos comenzado por estudiar las relaciones y sus propiedades, así como las operaciones que se pueden realizar con ellas.

A continuación hemos presentado el álgebra de términos con un resultado clave para las pruebas de los tres teoremas de decibilidad: la propiedad universal del álgebra de términos. Esta propiedad nos da una forma única de interpretar las variables en cualquier álgebra.

En los capítulos siguientes hemos presentado distintas signaturas algebraicas con sus álgebras de términos asociadas, además de otras álgebras con las mismas estructuras. Hemos definido en cada caso una aplicación del conjunto de las variables en el álgebra, que, cumpliendo la propiedad universal del álgebra de términos, se podía extender a un homomorfismo único de el álgebra de términos con la signatura respectiva en el álgebra correspondiente. Estos homomorfismos nos han servido para viajar entre álgebras con el objetivo de trasladar el problema de la validez de una ecuación en relaciones a un problema equivalente en otra álgebra, pero resoluble mediante autómatas finitos. Esta equivalencia la hemos presentado con los tres teoremas de decibilidad: Teorema de Decibilidad en Álgebras de Kleene, Teorema de Decibilidad en Alegorías y Teorema de Decibilidad en Alegorías de Kleene.

La elección del método a utilizar depende de las operaciones involucradas en la ecuación cuya validez queramos probar. El último teorema pretende generalizar el resultado de los dos teoremas previos de forma que permita provar la validez de cualquier expresión. Aún así, hemos tenido que dejar fuera la operación constante $\top$ porque resultaba problemática al tener distintas interpretaciones dependiendo del álgebra en la que se trabajara.

Las pruebas de los resultados presentados a lo largo del trabajo se han realizado en su mayoría por inducción sobre la estructura de los términos en las distintas Σ-álgebras, por lo que no han resultado complejas aunque sí algo tediosas.

Al extraer resultados de diversos trabajos nos hemos encontrado con notaciones muy distintas para conceptos iguales, además de algunos abusos de notación que podían crear confusión. Por esto, hemos prestado especial atención a la notación a lo largo del trabajo, tratando de ser coherentes con las notaciones ya existentes sin pérdida de rigor.

Como ya hemos explicado al final de los capítulos principales, los resultados que presentamos son útiles cuando se usan autómatas finitos pero no hemos profundizado en ello. Para más información al respecto consultar las referencias citadas a lo largo del trabajo.

Bibliografía

[1] H. Andréka y D. Bredikhin, *The equational theory of union-free algebras of relations.* Algebra Universalis, 33(4):516–532, 1995.

[2] P. Brunet, *A Kleene theorem for Petri automata.* Submitted, 2016.

[3] P. Brunet y D. Pous, *Algorithms for Kleene algebra with converse*, Journal of Logical and Algebraic Methods in Programming, 2015.

[4] P. Brunet y D. Pous, *Petri Automata for Kleene Allegories*, Logic in Computer Science, Kyoto, Japan. IEEE, pp.68-79, Jul 2015.

[5] S. Burris y H.P. Sankappanavar, *A Course in Universal Algebra*, Graduate Texts Math vol.78, 1981.

[6] J. Climent y E. Cosme, *Eilenberg theorems for many-sorted formations*, To appear in Houston Journal of Mathematics, 2017.

[7] J. H. Conway, *Regular algebra and finite machines.* Chapman and Hall, 1971.

[8] E. Cosme y D. Pous, *K4-free Graphs as a Free Algebra*, 42nd International Symposium on Mathematical Foundations of Computer Science, Aalborg, Denmark, Aug 2017.

[9] P. Freyd y A. Scedrov, *Categories, Allegories.* North Holland, 1990.

[10] D. Kozen, *A completeness theorem for Kleene Algebras and the algebra of regular events.* In Proc. LICS, pages 214–225. IEEE Computer Society, 1991.

[11] D. Kozen, *A completeness theorem for Kleene algebras and the algebra of regular events.* Information and Computation, 110(2):366–390, 1994.

[12] T. Murata, *Petri nets: Properties, analysis and applications.* Proc. de IEEE, 77(4):541–580, Apr 1989.

[13] C.A. Petri, *Fundamentals of a theory of asynchronous information flow.* Proc. de IFIP Congress, pages 386–390, 1962.

[14] J.E. Pin, *Mathematical Foundations of Automata Theory*, Lecture notes LIAFA, Université Paris vol. 7, 2010.

[15] M. Pla, *Apuntes de Matemática Basica*, Facultad de Matemáticas, UV, Curso 2012-2013.

[16] D. Pous, *Automata for relation algebra and formal proofs*, Computer Science [cs]. ENS Lyon, 2016.