Curso de Doctorado:

Programación Internet con Lenguajes Declarativos Multiparadigma.

PARTE I: Fundamentos

Pascual Julián Iranzo

Pascual.Julian@uclm.es

Universidad de Castilla – La Mancha. Departamento de Informática.

Indice

Objetivos y Motivación

- Estudiar la lógica ecuacional y su mecanización mediante los sistemas de reescritura de términos.

- **Motivación:**

1. Introducir la programación funcional (aproximación algebraica).
2. Servir de fundamento a la integración de paradigmas declarativos (punto de vista: funcional $+ \Rightarrow$ lógico).

Introducción

- La lógica ecuacional es un subconjunto de la lógica de 1^{er} orden con igualdad.

- **Observación**

1. Por simplicidad expositiva no consideraremos signaturas con varios géneros (*sorts*).

2. Por suficiencia expresiva no consideraremos el caso condicional.

Sintaxis: Vocabulario

- Una signatura, $\mathcal{F}$, es un conjunto finito de *símbolos de función*
  - Cada símbolos de función tiene una aridad asociada: $ar_{\mathcal{F}} : \mathcal{F} \rightarrow \mathbb{N}$.
  - Si $ar_{\mathcal{F}}(f) = 0$, f es un símbolo de constante.
  - $f, g, h, \ldots$ denotarán funciones de aridad distinta de cero; $a, b, c, \ldots$ denotarán constantes.

Metasímbolos y Notaciones

- $\mathcal{F}^0$: conjunto de las constantes de $\mathcal{F}$.
- $\mathcal{F}^n$: conjunto de los símbolos de función de $\mathcal{F}$ cuya aridad es n.
- **Ejemplo**: Dada la signatura $\mathcal{F} = \{cero, suc, pred, mas\}$

$$\mathcal{F}^0 = \{cero\}; \quad \mathcal{F}^1 = \{suc, pred\}; \quad \mathcal{F}^2 = \{mas\}$$

Metasímbolos y Notaciones

- $\mathcal{F}^0$: conjunto de las constantes de $\mathcal{F}$.
- $\mathcal{F}^n$: conjunto de los símbolos de función de $\mathcal{F}$ cuya aridad es n.
- **Ejemplo**: Dada la signatura $\mathcal{F} = \{tt, ff, neg, and, or\}$

$$\mathcal{F}^0 = \{tt, ff\}; \quad \mathcal{F}^1 = \{neg\}; \quad \mathcal{F}^2 = \{and, or\}$$

Sintaxis: Vocabulario

- Conjunto infinito numerable de *variables* $\mathcal{X}$:
  $\mathcal{F} \cap \mathcal{X} = \emptyset$
  - $x, y, z, \ldots$ denotarán variables.
- El único símbolo de predicado: $\approx$
  (posteriormente interpretado como la identidad).
- El resto de los símbolos del alfabeto serán:
  símbolos de puntuación y símbolos definidos.

Sintaxis: Términos

- La expresión t es un término:

1. Si $t \equiv x \in \mathcal{X}$ (i.e., t es una variable).
2. Si $t \equiv c \in \mathcal{F}^0$ (i.e., t es una constante).
3. Si $t \equiv f(t_1, t_2, \ldots t_n)$, $f \in \mathcal{F}^n$ y $t_1, t_2, \ldots t_n$ son términos.

- **Ejemplo**: pred(mas(suc(X), suc(cero)))

Metasímbolos y Notaciones

- $\mathcal{V}ar(s)$: conjunto de las variables que aparecen en el objeto sintáctico s.
- Si $\mathcal{V}ar(t) = \emptyset$, decimos que t es un término básico.
- $\overline{o_n}$: secuencia de objetos $o_1, \ldots, o_n$.
- **Ejemplo**: $f(\overline{x_n})$ denota el término $f(x_1, \ldots, x_n)$

Ocurrencias o Posiciones

- Una ocurrencia u es una cadena de enteros positivos: $u \in \mathbb{N}^* = \{\Lambda\} \cup \{i.v \mid i \in \mathbb{N}^+ \wedge v \in \mathbb{N}^*\}$
- Monoide libre generado por $\mathbb{N}^+$: $\langle \mathbb{N}^*, \ . \ , \Lambda \rangle$.
- Λ : cadena vacía; '.' : concatenación (asociativa).
- **Ejemplos**: Λ; 3; $1.3.1$
- $u \leq v$ si $(\exists w)\ v = u.w$; (orden prefijo)
  $u \parallel v$ si $u \not\leq v$ y $v \not\leq u$. (posiciones disjuntas)

Dominios de Posiciones

- $\mathbb{D} \subseteq \mathbb{N}^*$ es un dominio de posiciones si

1. $\Lambda \in \mathbb{D}$;
2. $(\forall u, v \in \mathbb{N}^*)\ (u.v \in \mathbb{D} \Rightarrow u \in \mathbb{D})$; (cierre por prefijo)
3. $(\forall u \in \mathbb{N}^*)\ (\forall j, k \in \mathbb{N})\ (u.j \in \mathbb{D} \wedge (1 \leq k \leq j) \Rightarrow u.k \in \mathbb{D})$;

- **Ejercicio**: Comprobar que D es un dominio:

$$D = \{\Lambda, 1, 1.1, 1.2, 2, 2.1, 2.2, 2.2.1, 2.2.2, 3, 3.1, 3.2, 3.3\}$$

Términos, Posiciones y Representación Arborescente

- Un término sobre una signatura $\mathcal{F}$:

$$t : \mathbb{D} \subset \mathbb{N}^* \longrightarrow \mathcal{F} \cup \mathcal{X}$$

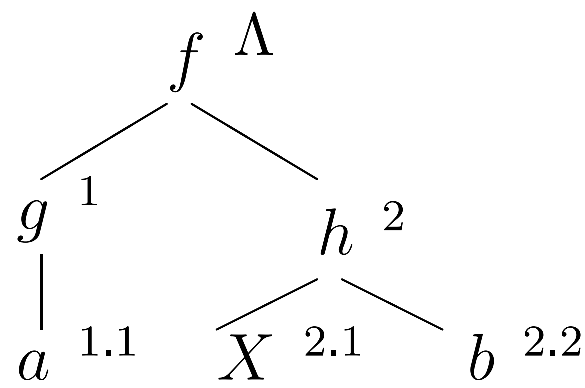
1. $\mathbb{D}$ es un dominio no vacío.

2. $t(p) = f \wedge ar(f) = k \quad \Rightarrow \quad (\forall i \in \{1, \ldots, k\}) p.i \in \mathbb{D}$.

Términos, Posiciones y Representación Arborescente

- Representación del término $t = f(g(a), h(X, b))$:

$$
\begin{aligned}
&t(\Lambda) = f\\
&t(1) = g\\
&t(1.1) = a\\
&t(2) = h\\
&t(2.1) = X \quad t(2.2) = b
\end{aligned}
$$



- **Notación alternativa**: $t[1.1] = a$.

Términos, Posiciones y Representación Arborescente: Metasímbolos y Notaciones

- $\mathcal{P}os(t)$ ($\mathcal{F}\mathcal{P}os(t)$): conjunto de las posiciones (no variables) de t.
- $\mathcal{R}oot(t) = t(\Lambda)$ (Raíz del término t).
- $t|_p$: subtérmino de t en la posición p.
- $t[s]_p$: término resultado de reemplazar $t|_p$ por s en la posición p.
- $\mathcal{T}(\mathcal{F}, \mathcal{X})$ ($\mathcal{T}(\mathcal{F})$): conjunto de los términos (básicos).

Términos, Posiciones y Representación Arborescente: Metasímbolos y Notaciones

- **Ejercicio**: Dado el término $t = f(g(a), h(X, b))$ determinar:

1. $\mathcal{FP}os(t)$ y $\mathcal{R}oot(t)$.
2. $t|_{1.1}$ y $t[s]_{1.1}$ para $s = h(Y, a)$.

Sustituciones

- Una sustitución es una aplicación

$$\begin{array}{rccc} \sigma : & \mathcal{X} & \longrightarrow & \mathcal{T}(\mathcal{F},\mathcal{X}) \\ & X & \hookrightarrow & \sigma(X) \end{array}$$

- Es habitual representar las sustituciones como conjuntos finitos de la forma

$$\sigma = \{X_1/t_1, X_2/t_2, \ldots, X_n/t_n\}$$

donde para cada elemento X_i/t_i, $X_i \neq t_i$

Sustituciones

- $\{X_1, X_2, \ldots, X_n\}$ es el dominio ($\mathcal{D}om(\sigma)$).
- $\{t_1, t_2, \ldots, t_n\}$ es el rango ($\mathcal{R}an(\sigma)$).
- la sustitución identidad, id, se representa mediante el conjunto vacío de elementos: $\{\}$ (*sustitución vacía*).

Sustituciones

- Una sustitución donde los términos t_i son básicos se denomina sustitución básica.
- Ejemplos de sustituciones:
  - $\theta_1 = \{X/f(Z), Z/Y\}$;
  - $\theta_2 = \{X/a, Y/g(Y), Z/f(g(b))\}$;
  - $\theta_3 = \{X/f(a), Z/g(b)\}$. (sustitución básica)

Sustituciones: Aplicación de una sustitución

- La aplicación de una sustitución $\sigma = \{\overline{X_n/t_n}\}$ a una expresión $\mathcal{E}$ [denotado $\sigma(\mathcal{E})$] se obtiene reemplazando **simultaneamente** cada ocurrencia de X_i en $\mathcal{E}$ por el correspondiente t_i.
- Se dice que $\sigma(\mathcal{E})$ es una instancia de $\mathcal{E}$.
- **Notación en programación lógica**: $\mathcal{E}\sigma$ en lugar de $\sigma(\mathcal{E})$.

Sustituciones: (Pre)orden de máxima generalidad para términos

- $\mathcal{E}_1 \leq \mathcal{E}_2 \Leftrightarrow (\exists \sigma)\ \ \sigma(\mathcal{E}_1) = \mathcal{E}_2$.
- **Ejemplo**: $\mathcal{E} \equiv f(X, Y, f(b))$ y $\theta = \{Y/X, X/b\}$.
  - $\theta(\mathcal{E}) = f(b, X, f(b))$.
  - $f(b, X, f(b))$ es una instancia de $f(X, Y, f(b))$.
  - $f(X, Y, f(b)) \leq f(b, X, f(b))$.

Sustituciones: Composición de sustituciones

- La composición de dos sustituciones σ y θ es la aplicación $\sigma \circ \theta$ tal que

$$(\sigma \circ \theta)(\mathcal{E}) = \sigma(\theta(\mathcal{E})).$$

- Propiedades de la composición de sustituciones:
  - **Asociativa**: $(\rho \circ \sigma) \circ \theta = \rho \circ (\sigma \circ \theta)$.
  - **Existencia de elemento neutro**: $id \circ \theta = \theta \circ id = \theta$.

Sustituciones: Composición de sustituciones

- **Ejercicio**: Dadas las sustituciones

$$\theta = \{X/f(Y), Y/Z\} \quad \text{y} \quad \sigma = \{X/a, Y/b, Z/Y\}$$

obtener:

$$\sigma \circ \theta \quad \text{y} \quad \theta \circ \sigma.$$

- **Observación**: Si $\mathcal{V}ar(\sigma) \cap \mathcal{V}ar(\theta) = \emptyset$ entonces $\sigma \circ \theta = \sigma \cup \theta$.

Sustituciones: Idempotencia

- Una sustitución σ se dice idempotente sii $\sigma \circ \sigma = \sigma$.
- **Ejercicio**: Comprobad que $\theta_1 = \{X/f(Z), Z/Y\}$ y $\theta_2 = \{X/a, Y/g(Y), Z/f(g(b))\}$ no son idempotentes.
- **Ejercicio**: Una substitución σ es idempotente si $\mathcal{D}om(\sigma) \cap \mathcal{V}ar(\mathcal{R}an(\sigma)) = \emptyset$.

Sustituciones: Renombramientos y variantes

- Una sustitución ρ se denomina renombramiento, si existe la sustitución inversa ρ^{-1} tal que $\rho \circ \rho^{-1} = \rho^{-1} \circ \rho = id$.

- Las expresiones $\mathcal{E}_1$ y $\mathcal{E}_2$ son variantes si existen dos renombramientos σ y θ, tales que

$$\mathcal{E}_1 = \sigma(\mathcal{E}_2) \text{ y } \mathcal{E}_2 = \theta(\mathcal{E}_1).$$

Sustituciones: (Pre)orden de máxima generalidad

- Dadas dos sustituciones σ y θ. Decimos que σ es más general que θ, denotado $\sigma \leq \theta$, sii
  - existe una sustitución λ tal que $\theta = \lambda \circ \sigma$.

- **Ejemplo**: Sean $\sigma = \{X/a\}$ y $\theta = \{X/a, Y/b\}$.
  - Existe $\lambda = \{Y/b\}$ tal que $\theta = \lambda \circ \sigma \Longrightarrow \sigma \leq \theta$.

Sintaxis: Ecuaciones

- Una ecuación es una expresión

$$s \approx t$$

donde s y t es un par de términos no ordenados.

  - Las variables de una ecuación se suponen cuantificadas universalmente
  - Cuando no contienen variables es una ecuación básica

Sintaxis: Ecuaciones

- Una ecuación expresa que dos términos sintácticamente distintos deben considerarse iguales.

$$f(X) \approx 0$$

- Un conjunto de ecuaciones puede entenderse como la definición de una función:

$$\begin{array}{lcl} 0 + X & \approx & 0 \\ suc(X) + Y & \approx & suc(X + Y) \end{array}$$

Cálculo deductivo: Razonamiento Ecuacional

- $\mathcal{E}$: conjunto de ecuaciones.
- Una teoría ecuacional es el conjunto de ecuaciones que pueden obtenerse por razonamiento ecuacional, usando las ecuaciones de $\mathcal{E}$ como axiomas y el siguiente conjunto de Reglas de Inferencia de la Lógica Ecuacional.

Cálculo deductivo: Razonamiento Ecuacional

- Reglas de Inferencia de la Lógica Ecuacional:

1. Reflexiva $$\frac{}{t \approx t}$$

2. Simétrica $$\frac{s \approx t}{t \approx s}$$

3. Transitiva $$\frac{s \approx r, r \approx t}{s \approx t}$$

Cálculo deductivo: Razonamiento Ecuacional

- Reglas de Inferencia de la Lógica Ecuacional:

4. Sustitución

$$\frac{s_1 \approx t_1, \ldots, s_n \approx t_n}{f(s_1, \ldots, s_n) \approx f(t_1, \ldots, t_n)}$$

$$(\forall f).\ (f \in \mathcal{F} \wedge ar(f) = n)$$

Cálculo deductivo: Razonamiento Ecuacional

- Reglas de Inferencia de la Lógica Ecuacional:

  5. Instanciación

$$\frac{s \approx t}{\sigma(s) \approx \sigma(t)}$$

$$(\forall \sigma).\ \sigma \in Subst(\mathcal{F}, \mathcal{X})$$

Cálculo deductivo: Razonamiento Ecuacional

- Reglas de Inferencia de la Lógica Ecuacional:

  6. Ecuaciones $\dfrac{}{s \approx t}$

  si $s \approx t \in \mathcal{E}$

Cálculo deductivo: Razonamiento Ecuacional

- Dado un conjunto de ecuaciones $\mathcal{E}$, una deducción es una secuencia de ecuaciones

$$t_1 \approx s_1, t_2 \approx s_2, \ldots, t_k \approx s_k, \ldots, t_n \approx s_n$$

tal que, para todo k:

1. $(t_k \approx s_k) \in \mathcal{E}$, o bien
2. $t_k \approx s_k$ inferida de ecuaciones anteriores aplicando reglas del sistema deductivo

- **Notación**: $\mathcal{E} \vdash t_n \approx s_n$ o bien $t_n \approx_{\mathcal{E}} s_n$

Cálculo deductivo: Razonamiento Ecuacional

- La sustitución de variables por términos y la noción de “reemplazamiento de iguales por iguales” conduce a una definición más compacta del sistema de inferencia de la lógica ecuacional en el que las reglas 4 y 5 se fusionan en:

$$\frac{l \approx r, u \in \mathcal{P}os(t)}{t[\sigma(l)]_u \approx t[\sigma(r)]_u}$$

$$(\forall \sigma).\ \sigma \in Subst(\mathcal{F}, \mathcal{X})$$

Cálculo deductivo: Razonamiento Ecuacional

- **Ejemplo** (Axiomas de Grupo): Dado un conjunto de ecuaciones, $\mathcal{E}$,

$$\begin{array}{llll} X + 0 \approx X & (e_1) & -X + X \approx 0 & (e_3) \\ 0 + X \approx X & (e_2) & X + (Y + Z) \approx (X + Y) + Z & (e_4) \end{array}$$

puede comprobarse que $\mathcal{E} \vdash -(-X) \approx X$

$$\begin{array}{lllllll} -(-X) & \approx & -(-X) + 0 & \approx & -(-X) + (-X + X) & & \\ & \approx & (-(-X) + -X) + X & \approx & 0 + X & \approx & X \end{array}$$

Semántica Algebraica: Interpretación

- Las construcciónes sintácticas de la lógica ecuacional cobran significado cuando se las interpreta
- Una interpretación de una signatura $\mathcal{F}$ consiste en asociarle una estructura matemática denominada $\mathcal{F}$–álgebra.

Semántica Algebraica: Interpretación

- Una $\mathcal{F}$–álgebra es un conjunto con estructura.

- Dada una signatura $\mathcal{F}$, una $\mathcal{F}$–álgebra es un par $\langle A, \mathcal{F}_A \rangle$, donde
  - A es un conjunto, denominado soporte
  - $\mathcal{F}_A$ es un conjunto de operaciones: por cada $f \in \mathcal{F}$, existe una operación $f_A : A^{ar(f)} \rightarrow A$ en $\mathcal{F}_A$.

Semántica Algebraica: Interpretación

- **Ejemplo**: Dada la signatura $\mathcal{F} = \mathcal{F}^0 \cup \mathcal{F}^1 \cup \mathcal{F}^2$, donde

$$\mathcal{F}^0 = \{cero\}; \quad \mathcal{F}^1 = \{suc, pred\}; \quad \mathcal{F}^2 = \{mas\}.$$

Entonces, $\langle \mathbb{N}, \mathcal{F}_{\mathbb{N}} \rangle$ es la $\mathcal{F}$–álgebra tal que:

$\mathbb{N}$ es el conjunto de los números naturales

$$\begin{array}{ll}
cero_{\mathbb{N}} : \quad \longrightarrow \mathbb{N} & cero_{\mathbb{N}} = 0 \\
suc_{\mathbb{N}} : \mathbb{N} \longrightarrow \mathbb{N} & suc_{\mathbb{N}}(n) = n + 1; \\
pred_{\mathbb{N}} : \mathbb{N} \longrightarrow \mathbb{N} & pred_{\mathbb{N}}(0) = 0, \quad pred_{\mathbb{N}}(n+1) = n; \\
mas_{\mathbb{N}} : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} & mas_{\mathbb{N}}(n, m) = n + m.
\end{array}$$

Semántica Algebraica: Interpretación

- **Ejemplo**: Dada una signatura $\mathcal{F}$, un tipo especial de $\mathcal{F}$–álgebra es la $\mathcal{F}$–álgebra (libre) de términos $\langle \mathcal{T}, \mathcal{F}_{\mathcal{T}} \rangle$ (generada por $\mathcal{X}$):
  - $\mathcal{T} = \mathcal{T}(\mathcal{F}, \mathcal{X})$ es el conjunto soporte;
  - $\mathcal{F}_{\mathcal{T}} = \{ f_{\mathcal{T}} \mid f \in \mathcal{F} \wedge f_{\mathcal{T}} : \mathcal{T}(\mathcal{F}, \mathcal{X})^{ar(f)} \to \mathcal{T}(\mathcal{F}, \mathcal{X}) \}$

$$f_{\mathcal{T}}(\overline{t_{ar(f)}}) = f(\overline{t_{ar(f)}})$$

- Cuando $\mathcal{X} = \emptyset$ se obtiene la $\mathcal{F}$–álgebra (inicial) de términos básicos $\langle \mathcal{T}(\mathcal{F}), \mathcal{F}_{\mathcal{T}(\mathcal{F})} \rangle$.

Semántica Algebraica: Interpretación

- La elección de una $\mathcal{F}$–álgebra basta para dar significado a los términos básicos generados a partir de $\mathcal{F}$.
- **Ejemplo**: Para la signatura $\mathcal{F}$ y la $\mathcal{F}$–álgebra $\langle \mathbb{N}, \mathcal{F}_{\mathbb{N}} \rangle$ del ejemplo anterior:
  - El significado de $pred(mas(suc(cero), suc(cero)))$ es

$$pred_{\mathbb{N}}(mas_{\mathbb{N}}(suc_{\mathbb{N}}(cero_{\mathbb{N}}), suc_{\mathbb{N}}(cero_{\mathbb{N}}))) = ... = 1$$

Semántica Algebraica: Interpretación

- El álgebra de términos interpreta los términos en ellos mismos.
- **Ejemplo**: Para la signatura $\mathcal{F}$ del ejemplo anterior y la $\mathcal{F}$–álgebra $\langle \mathcal{T}, \mathcal{F}_{\mathcal{T}} \rangle$:
  - El significado de $pred(mas(suc(cero), suc(cero)))$ es

$$pred(mas(suc(cero), suc(cero)))$$

Semántica Algebraica: Interpretación

- Para poder formalizar el anterior resultado introducimos el concepto de $\mathcal{F}$–homomorfismo, que son funciones que preservan la estructura de un $\mathcal{F}$–álgebra.
- Dada una signatura $\mathcal{F}$ y las $\mathcal{F}$–álgebras $\langle A, \mathcal{F}_A \rangle$ y $\langle B, \mathcal{F}_B \rangle$, una aplicación $h : A \longrightarrow B$ es un $\mathcal{F}$–homomorfismo si y sólo si

$$(\forall f \in \mathcal{F})\ [ar(f) = n \quad \Rightarrow \quad h(f_A(\overline{a_n})) = f_B(\overline{h(a_n)})]$$

Semántica Algebraica: Interpretación

- **Proposición**: Para cada $\mathcal{F}$–álgebra $\langle A, \mathcal{F}_A \rangle$, existe un único $\mathcal{F}$–homomorfismo $i_A : \mathcal{T}(\mathcal{F}) \longrightarrow A$.
- **Observación**: i_A puede entenderse como una función de interpretación que a cada término básico le asigna un único significado.

$$i_A(t) = \begin{cases} f_A & \text{si } t \equiv f \in \mathcal{F}^0 \text{ es una constante} \\ f_A(\overline{i_A(t_n)}) & \text{si } t \equiv f(\overline{t_n}) \text{ y } t_i \in \mathcal{T}(\mathcal{F}) \end{cases}$$

Semántica Algebraica: Asignación

- Para dar significado a los términos con variables de $\mathcal{T}(\mathcal{F}, \mathcal{X})$, además de la elección de una $\mathcal{F}$–álgebra se requiere una asignación de valor a las variables

- Dado un conjunto de variables $\mathcal{X}$ y una $\mathcal{F}$–álgebra $\langle A, \mathcal{F}_A \rangle$, una A–asignación es una aplicación

$$\rho_A : \mathcal{X} \to A$$

Semántica Algebraica: Asignación

- **Observación**: una sustitución es una $\mathcal{T}(\mathcal{F}, \mathcal{X})$–asignación.
- **Proposición** (*Freeness*): Dada una A–asignación ρ_A para $\mathcal{X}$ en una $\mathcal{F}$–álgebra $\langle A, \mathcal{F}_A \rangle$, existe un único $\mathcal{F}$–homomorfismo $\hat{\rho}_A : \mathcal{T}(\mathcal{F}, \mathcal{X}) \longrightarrow A$ tal que $(\forall x \in \mathcal{X})\ \hat{\rho}_A(x) = \rho_A(x)$
- Decimos que $\hat{\rho}_A$ extiende ρ_A al álgebra de términos $\mathcal{T}(\mathcal{F}, \mathcal{X})$.

Semántica Algebraica: Asignación

- **Observación:** $\hat{\rho}_A$ generaliza la función de interpretación i_A

$$\hat{\rho}_A(t) = \begin{cases} f_A & \text{si } t \equiv f \in \mathcal{F}^0 \text{ es una constante} \\ \rho_A(t) & \text{si } t \equiv x \in \mathcal{X} \text{ es una variable} \\ f_A(\overline{\hat{\rho}_A(t_n)}) & \text{si } t \equiv f(\overline{t_n}) \text{ y } t_i \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \end{cases}$$

Semántica Algebraica: Asignación

- **Ejemplo**: Para la signatura $\mathcal{F}$ y la $\mathcal{F}$–álgebra $\langle \mathbb{N}, \mathcal{F}_{\mathbb{N}} \rangle$ del ejemplo anterior y la $\mathbb{N}$–asignación $\hat{\rho}_{\mathbb{N}}$ tal que $\hat{\rho}_{\mathbb{N}}(X) = 2$:
  - El significado de $pred(mas(suc(X), suc(cero)))$ es

$$pred_{\mathbb{N}}(mas_{\mathbb{N}}(suc_{\mathbb{N}}(2), suc_{\mathbb{N}}(cero_{\mathbb{N}}))) = ... = 3$$

Semántica Algebraica: Verdad y validez

- Una ecuación $s \approx t$ es verdadera en un $\mathcal{F}$–álgebra A si y sólo si, $\forall \hat{\rho}_A$, $\hat{\rho}_A(s) = \hat{\rho}_A(t)$;
    - Los términos s y t representan el mismo elemento en A cualquiera que sea la A–asignación.
- Si $s \approx t$ es verdadera en A, también decimos que A es modelo de la ecuación $t \approx s$ y escribimos $A \models t \approx s$.

Semántica Algebraica: Verdad y validez

- Un $\mathcal{F}$–álgebra A es modelo de un conjunto de ecuaciones $\mathcal{E}$ si es modelo de cada una de las ecuaciones que lo forman.
  - **Notación**: $Mod(\mathcal{E})$, conjunto de todas las $\mathcal{F}$–álgebras que son modelo de $\mathcal{E}$.
- Una ecuación $t \approx s$ es válida si es verdadera en toda $\mathcal{F}$–álgebra $A \in Mod(\mathcal{E})$ $\quad$ ($Mod(\mathcal{E}) \models t \approx s$).

  [La ecuación $t \approx s$ es consecuencia lógica de $\mathcal{E}$]

Corrección y Completitud

- **Teorema**: (Teorema de la Lógica Ecuacional — Birkhoff) Para todo conjunto de ecuaciones $\mathcal{E}$ y para todo par de términos s y t en $\mathcal{T}(\mathcal{F}, \mathcal{X})$ se cumple:

1. (Corrección)
   Si $\mathcal{E} \vdash (s \approx t)$ entonces $Mod(\mathcal{E}) \models (s \approx t)$;
2. (Completitud)
   Si $Mod(\mathcal{E}) \models (s \approx t)$ entonces $\mathcal{E} \vdash (s \approx t)$.

Semántica Algebraica: Inicialidad y congruencias

- **Problema**: ¿Cuál es el significado de un conjunto de ecuaciones $\mathcal{E}$?
- **Respuesta**: Identificar un álgebra prototípica que sea modelo de $\mathcal{E}$ y permita dar significado al conjunto de ecuaciones.
- Este álgebra prototípica será un álgebra inicial.

Semántica Algebraica: Inicialidad y congruencias

- Un $\mathcal{F}$–álgebra I es inicial en una clase $Class$ de $\mathcal{F}$–álgebras si y sólo si

1. $I \in Class$ y,
2. $(\forall A \in Class)$, existe un único $\mathcal{F}$–homomorfismo $h : I \longrightarrow A$.

- **Proposición**: Si I_1 e I_2 son iniciales en $Class$, son isomorfas.
- Un álgebra inicial puede emplearse para estudiar ciertas propiedades de la clase $Class$.

Semántica Algebraica: Inicialidad y congruencias

- **Proposición**: $\langle \mathcal{T}(\mathcal{F}), \mathcal{F}_{\mathcal{T}(\mathcal{F})} \rangle$ es inicial en la clase de todas las $\mathcal{F}$–álgebras.
- $\langle \mathcal{T}(\mathcal{F}), \mathcal{F}_{\mathcal{T}(\mathcal{F})} \rangle$ no es útil para dar significado a un conjunto de ecuaciones $\mathcal{E}$ ya que no es modelo de $\mathcal{E}$.
- **Ejercicio**: Mostrar que $\langle \mathcal{T}(\mathcal{F}), \mathcal{F}_{\mathcal{T}(\mathcal{F})} \rangle$ no puede ser modelo de $\mathcal{E}$.

Semántica Algebraica: Inicialidad y congruencias

- Una relación sobre la $\mathcal{F}$-álgebra A es una $\mathcal{F}$–congruencia, $\sim$, si y sólo si
  - $\sim$ es una relación de equivalencia y
  - $(\forall f \in \mathcal{F})(\forall a_i, \ldots, a_n, b_1, \ldots, b_n \in A)$ $[a_1 \sim b_1 \wedge \ldots \wedge a_n \sim b_n \;\; \Rightarrow \;\; f(\overline{a_n}) \sim f(\overline{b_n})]$.
- (Teoria Ecuacional Inducida por $\mathcal{E}$) $\approx_{\mathcal{E}} = \{\langle s, t\rangle \in \mathcal{T}(\mathcal{F}, \mathcal{X})^2 \mid \mathcal{E} \vdash (s \approx t)\}$ es una congruencia sobre $\mathcal{T}(\mathcal{F}, \mathcal{X})$.

Semántica Algebraica: Inicialidad y congruencias

- **Ejercicio**: Dado $\mathcal{F} = \{a, b, c, e, f\}$ y $\mathcal{E} = \{a \approx b, b \approx c, e \approx f\}$ hallar $\approx_{\mathcal{E}}$.

- **Ejercicio**: Comprobar que $\approx_{\mathcal{E}}$ es la mínima congruencia sobre $\mathcal{T}(\mathcal{F}, \mathcal{X})$ que contiene al conjunto de ecuaciones $\mathcal{E}$ y es estable bajo substituciones.

Semántica Algebraica: Inicialidad y congruencias

- ($\mathcal{F}$–álgebra cociente) Dada una signatura $\mathcal{F}$, $\langle \mathcal{T}(\mathcal{F})/{\approx_\mathcal{E}}, \mathcal{F}_{\mathcal{T}(\mathcal{F})/\approx_\mathcal{E}} \rangle$ es un $\mathcal{F}$–álgebra:
  - $\langle \mathcal{T}(\mathcal{F})/{\approx_\mathcal{E}} \rangle = \{[t]_{\approx_\mathcal{E}} \mid t \in \mathcal{T}(\mathcal{F})\}$ el conjunto de clases de equivalencia inducido por $\approx_\mathcal{E}$;
  - $\mathcal{F}_{\mathcal{T}(\mathcal{F})/\approx_\mathcal{E}} = \{f_{\mathcal{T}(\mathcal{F})/\approx_\mathcal{E}} \mid f \in \mathcal{F} \wedge$ $f_{\mathcal{T}(\mathcal{F})/\approx_\mathcal{E}} : (\mathcal{T}(\mathcal{F},\mathcal{X})/{\approx_\mathcal{E}})^{ar(f)} \to (\mathcal{T}(\mathcal{F},\mathcal{X})/{\approx_\mathcal{E}})\}$

$$f_{\mathcal{T}(\mathcal{F})/\approx_\mathcal{E}}(\overline{[t_{ar(f)}]_{\approx_\mathcal{E}}}) = [f(\overline{t_{ar(f)}})]_{\approx_\mathcal{E}}$$

Semántica Algebraica: Inicialidad y congruencias

- $\langle \mathcal{T}(\mathcal{F})/{\approx_{\mathcal{E}}}, \mathcal{F}_{\mathcal{T}(\mathcal{F})/\approx_{\mathcal{E}}} \rangle$ es inicial para $Mod(\mathcal{E})$.
- $\langle \mathcal{T}(\mathcal{F})/{\approx_{\mathcal{E}}}, \mathcal{F}_{\mathcal{T}(\mathcal{F})/\approx_{\mathcal{E}}} \rangle$ es el modelo inicial canónico o estándar que se asocia como significado de $\mathcal{E}$.
- **Ejercicio**: Dado $\mathcal{F} = \{a, b, c, e, f\}$, hallar el modelo inicial para $\mathcal{E} = \{a \approx b, b \approx c, e \approx f\}$.
- **Ejercicio**: Dado $\mathcal{F} = \{cero, suc, mas\}$, hallar el modelo inicial para $\mathcal{E} = \{mas(cero, X) \approx X, mas(suc(X), Y) \approx suc(mas(X, Y))\}$.

Corrección y Completitud

- **Teorema**: (Teorema de la Lógica Ecuacional — Birkhoff)

1. (Corrección) para todo s y t en $\mathcal{T}(\mathcal{F}, \mathcal{X})$,

   Si $\mathcal{E} \vdash (s \approx t)$ entonces $(\mathcal{T}(\mathcal{F})/{\approx_{\mathcal{E}}}) \models (s \approx t)$;

2. (Completitud) para todo s y t en $\mathcal{T}(\mathcal{F})$,

   Si $(\mathcal{T}(\mathcal{F})/{\approx_{\mathcal{E}}}) \models (s \approx t)$ entonces $\mathcal{E} \vdash (s \approx t)$.

Corrección y Completitud

- **Observación**: Para el álgebra inicial $\mathcal{T}(\mathcal{F})$ el razonamiento ecuacional solamente es completo cuando se restringe a términos básicos.
  - En general es posible establecer que $(\mathcal{T}(\mathcal{F})/{\approx_{\mathcal{E}}}) \models (s \approx t)$ mediante técnicas inductivas, aún cuando no sea posible establecerlo por métodos deductivos.

El Problema de la Validez y la Satisfacibilidad

- Razonar con ecuaciones conlleva dos actividades prioritarias:

1. Establecer si una ecuación $s \approx t$ es consecuencia de un conjunto de ecuaciones $\mathcal{E}$ (o equivalentemente si es derivable a partir de $\mathcal{E}$): Problema de la Validez.

2. Encontrar los valores de las variables que satisfacen una ecuación $s \approx t$: Problema de la Satisfacibilidad.

El Problema de la Validez y la Satisfacibilidad

- En un contexto formal el Problema de la Validez consiste en decidir si dado un conjunto de ecuaciones $\mathcal{E}$:

1. $Mod(\mathcal{E}) \models (\forall \overline{x})(s \approx t)$

   [Esta es una notación alternativa a: $Mod(\mathcal{E}) \models s \approx t$ o bien $s \approx_{\mathcal{E}} t$]

- **Nomenclatura alternativa**: *word problem* [si la ecuación $s \approx t$ es básica, hablamos del *ground word problem*]

El Problema de la Validez y la Satisfacibilidad

- En un contexto formal el Problema de la Satisfacibilidad consiste en decidir si dado un conjunto de ecuaciones $\mathcal{E}$:
  - $Mod(\mathcal{E}) \models (\exists \overline{x})(s \approx t)$

- Una formulación alternativa es el Problema de la $\mathcal{E}$-unificación: si existe una sustitución σ tal que $\sigma(s) \approx_{\mathcal{E}} \sigma(t)$.

El Problema de la Validez y la Satisfacibilidad

- En los próximos capítulos estudiaremos como solucionar el *(ground) word problem* y el problema de la satisfacibilidad presentando técnicas de semidecisión para casos concretos.

Bibliografía

- Huet G. y Oppen D., 1980. Equations and Rewrite Rules: a Survey. En *Formal Languages: perspectives and open problems*, págs. 349–405. Academic Press.

- Baader F. y Nipkow T., 1998. *Term Rewriting and All That*. Cambridge University Press.