IIC2213 — Lógica para Ciencia de la Computación

Apuntes Semana 12

1. Lógica de Primer Orden

En este curso vamos a definir la lógica de primer orden que solo toma relaciones, por que es lo más usado en computación. Clásicamente, la lógica de primer orden también puede usar funciones, para ver esa definición más completa sugerimos ir a los libros de la bibliografía.

Sintaxis de la Lógica de Primer Orden (LPO)

Vocabulario. Un vocabulario L es la unión de un conjunto de nombres de constantes (que denotaremos por $\{c_1, c_2, \ldots, c_\ell, \ldots\}$) y un conjunto de nombres de relaciones (que denotaremos por $\{R_1, R_2, \ldots, R_\ell, \ldots, S, T, \ldots\}$).

Por ejemplo, $L = \{0, 1, s, +, \times\}$ es un vocabulario usado para estudiar teoría de números. Aquí 0 y 1 son constantes, s es una relación binaria (representa el sucesor) y $+$ y $\cdot$ son relaciones terciarias. La idea es que la relación $+$ represente a triples (a, b, c) tal que $a+b = c$, y lo mismo para $\times$. La aridad de una relación es el número de argumentos de esa relación.

Fórmulas. Ahora definimos de forma inductiva el conjunto de fórmulas en LPO sobre un vocabulario específico L:

- Si R es una relación de aridad n en L y $t_1, \ldots, t_n$ son constantes o variables, entonces $R(t_1, \ldots, t_n)$ es una fórmula en LPO sobre L.
- Si s y t son constantes o variables, entonces $(s = t)$ es una fórmula en LPO sobre L
- Si φ y ψ son fórmulas en LPO sobre L, entonces $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ y $\neg(\varphi)$ son fórmulas en LPO sobre L.
- Si φ es una fórmula en LPO sobre L, y x es libre en φ, entonces $(\forall x \varphi)$ y $(\exists x \varphi)$ son fórmulas en LPO.

Decimos que las fórmulas de la forma $t_1 = t_2$ y $R(t_1, \ldots, t_n)$ son fórmulas atómicas. En otras palabras, $t_1 = t_2$ y $R(t_1, \ldots, t_n)$ son las fórmulas más pequeñas que podemos tener, y todas las otras se construyen en base a esas. Son, de alguna manera, el análogo a las proposiciones de la lógica proposicional.

Como siempre, en este curso vamos a omitir paréntesis siempre que no produzca confusión.

Semántica de la lógica de primer orden: Estructuras

Considera por ejemplo la siguiente fórmula sobre el vocabulario $L = \{0, 1, s, +, \times\}$:

$$\forall x(\exists y \ +(y, y, x))$$

De acuerdo a lo que explicamos, esta fórmula se construye sobre un vocabulario típico de teoría de números, donde hay dos "constantes" 0, 1, y tres relaciones: una para el sucesor (s), otra para la suma y otra para la multiplicación[1]. Intuitivamente la fórmula dice "para todo x existe un y tal que $y + y$ es x. Esta fórmula es falsa en los números naturales, pero es verdadera si tomamos en vez los números reales. En otras palabras, la satisfacción de esa fórmula depende de dónde la evaluamos! Para formalizar este concepto vamos a introducir la noción de estructura.

Definición. Sea L un vocabulario. Una L-estructura es una tupla $\mathcal{A}$ que contiene:

- Un dominio: un conjunto no vacío de elementos.
- Para cada constante c en L, una interpretación $c^{\mathcal{A}} \in A$. Con esto especificamos a qué elemento del dominio corresponde la constante.
- Para cada relación R de aridad n en L, una interpretación $R^{\mathcal{A}} \subseteq A^n$. Con esto especificamos a a qué relación corresponde R en $\mathcal{A}$.

Para especificar estructuras usamos la notación $\mathcal{A} = \langle A, \dots, c^{\mathcal{A}}, \dots, R^{\mathcal{A}}, \dots \rangle$, en donde A es el dominio.

Ejemplo. Supongamos que tenemos un grafo no-dirigido $G = (V, E)$. Podemos representarlo con el vocabulario $\{R\}$, con solo una relación binaria R, y la estructura $\mathcal{A} = \langle A, R^{\mathcal{A}} \rangle$, donde $A = V$, los vértices del grafo, y $R^{\mathcal{A}} = E$, las aristas del grafo.

Ejemplo. Tomando nuevamente $L = (0, 1, s, +, \times)$, la siguiente estructura representa a los números naturales sobre este vocabulario. La estructura es $\mathcal{N} = \langle N, 0^{\mathcal{N}}, 1^{\mathcal{N}}, s^{\mathcal{N}}, +^{\mathcal{N}}, \times^{\mathcal{N}} \rangle$, donde $N = \{0, 1, 2, \dots\}$, $0^{\mathcal{N}} = 0$, $1^{\mathcal{N}} = 1$, $s^{\mathcal{N}} = \{(a, b) \mid a, b \in \mathbb{N}, a+1 = b\}$, $+^{\mathcal{N}} = \{(a, b, c) \mid a, b, c \in \mathbb{N}, a + b = c\}$, y $\times^{\mathcal{N}} = \{(a, b, c) \mid a, b, c \in \mathbb{N}, a \cdot b = c\}$.

Por otro lado, para los reales usaríamos la estructura $\mathcal{R} = \langle R, 0^{\mathcal{R}}, 1^{\mathcal{R}}, s^{\mathcal{R}}, +^{\mathcal{R}}, \times^{\mathcal{R}} \rangle$, donde $R = \mathbb{R}$, $0^{\mathcal{R}} = 0$, $1^{\mathcal{R}} = 1$, $s^{\mathcal{R}} = \{(a, b) \mid a, b \in \mathbb{R}, a+1 = b\}$, $+^{\mathcal{R}} = \{(a, b, c) \mid a, b, c \in \mathbb{R}, a+b = c\}$, y $\times^{\mathcal{R}} = \{(a, b, c) \mid a, b, c \in \mathbb{R}, a \cdot b = c\}$.

Finalmente, considera la estructura $\mathcal{A} = \langle A, 0^{\mathcal{A}}, 1^{\mathcal{A}}, s^{\mathcal{A}}, +^{\mathcal{A}}, \times^{\mathcal{A}} \rangle$, donde tenemos que $A = \{\varepsilon, 1, 11, 111, 1111, \dots\}$, $0^{\mathcal{A}} = \varepsilon$, $1^{\mathcal{N}} = 1$, $s^{\mathcal{A}} = \{(a, b) \mid a, b \in \{1\}^*, a1 = b\}$, $+^{\mathcal{A}} = \{(a, b, c) \mid a, b, c \in \{1\}^*, ab = c\}$, y $\times^{\mathcal{A}}$ esta dada por:

$\times^{\mathcal{A}} = \{(a, b, c) \mid a, b, c \in \{1\}^*,$
c tiene tantos 1s como la cantidad de 1s de b multiplicada por la cantidad de 1's de $a\}$.

[1] Usualmente la suma es una función que recibe dos números a y b y computa $a + b$. Pero podemos pensar que es una relación, asumiendo que guarda todos los triples (a, b, c) donde $a + b = c$.

La estructura $\mathcal{A}$, de cierta forma, también representa a los números naturales. De hecho, podemos mostrarlo de una forma muy precisa.

Definición. Decimos que dos estructuras $\mathcal{A}$ y $\mathcal{A}'$, con dominios A y A', y sobre un vocabulario L son *isomorfas* si existe una función uno-a-uno $f : A \to A'$ tal que (i) para cada constante $c \in L$ se tiene que $f(c^{\mathcal{A}}) = c^{\mathcal{A}'}$, y para cada relación R de aridad j y elementos $a_1, \ldots, a_j$ en A, se tiene que $(a_1, \ldots, a_j) \in R^{\mathcal{A}}$ si y solo si $(f(a_1), \ldots, f(a_j)) \in R^{\mathcal{A}'}$.

De esta forma, podemos mostrar que $\mathcal{N}$ y $\mathcal{A}$ son isomorfas, usando la función f que toma a cada número natural i y lo envía a su representación unaria: una palabra con una cantidad i de 1's. Se puede demostrar que la lógica de primer orden no distingue entre estructuras isomorfas, en el sentido de que una formula va a ser verdad en una estructura si y solo sí va a ser verdad en la otra.

Constantes versus dominio. A veces se confunde la idea de una constante con la de los elementos del dominio de las estructuras. Una forma simple de diferenciarlo: Cuando escribimos una fórmula, esta se tiene que poder evaluar en *cualquier* estructura para el vocabulario usado. Por lo tanto, una fórmula *no puede hacer mención a los elementos del dominio de las estructuras*. Para esto entran en juego la idea de las constantes. Si queremos por ejemplo decir algo sobre el *cero*, el elemento neutro en el vocabulario de arriba, usamos la constante 0, y escribimos

$$\forall x \forall y \big((+(x, 0, y) \vee +(0, x, y)) \to x = y \big).$$

Cualquier estructura que satisfaga esa fórmula va a ser tal que la constante 0 se mapea al elemento neutro de los naturales, el cero.

Importante: sobrecargando la notación. Usualmente vamos a sobrecargar la notación: para representar grafos $G = (V, E)$ vamos a usar un vocabulario donde la relación que representa a las aristas se llame también E, de modo que $E^{\mathcal{A}} = E$. Hacemos esto para simplificar la lectura (ya lo habíamos hecho, por ejemplo, con las constantes 0 y 1.

Semántica de la lógica de primer orden: Variables libres

Las variables libres, son, de alguna forma, los parámetros de las fórmulas en LPO. Por ejemplo, no es lo mismo decir $\forall x R(x)$ que simplemente $R(x)$. La primera no tiene variables libres, y dice que $R(x)$ debe ser verdad para cualquier asignación de x. La segunda, en cambio, es imposible saber si es verdad o mentira hasta que no sepamos la asignación para x.

Dada una L-fórmula φ en LPO, definimos el conjunto de variables libres de φ de esta forma:

- Si φ es $t_1 = t_2$, las variables libres de φ es la union de las variables de t_1 y t_2 (recuerda que t_1 y t_2 pueden ser variables o constantes).
- Si φ es $R(t_1, \ldots, t_n)$, las variables libres de φ es la union de las variables de cada uno de $t_1, \ldots, t_n$ (nuevamente, algunos de estos t_i podrían ser constantes, o dos t_i, t_j podrían ser una misma variable x).

- Si φ es $\psi_1 * \psi_2$ para $* \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, las variables libres de φ es la union de las de ψ_1 y ψ_2
- Si φ es $\neg\psi$, las variables libres de φ son las mismas que las de ψ
- Si φ es $\exists x\ \psi$ o $\forall x\ \varphi$, las variables libres de φ son las variables de ψ salvo x

Como puedes ver, las variables libres de una fórmula son aquellas que no están cuantificadas bajo un operador $\exists$ o $\forall$.

Si φ es una fórmula con variables libres $x_1, \ldots, x_n$, entonces usamos la notación $\varphi(x_1, \ldots, x_n)$. Si φ no tiene variables libres, decimos que φ es una *oración*.

Semántica de la lógica de primer orden: Asignaciones y noción de satisfacer una fórmula

Las asignaciones es el último ingrediente para definir la semantica.

Definición. Sea $\mathcal{A}$ una L-estructura con dominio A. Sea $C = c_1, \ldots, c_\ell$ el conjunto de constantes en L. Una L-asignación para $\mathcal{A}$ es una función parcial $\tau : \mathit{Var} \cup C \to A$ que asigna algunas variables en Var a elementos del dominio, y tal que $\tau(c) = c^{\mathcal{A}}$ para cada $c \in C$ (es decir, τ respeta la interpretación de las constantes en $\mathcal{A}$).

Para una asignación $\tau : \mathit{Var} \cup C \to A$, escribimos $\tau[x \to a]$ para denotar la siguiente asignación:

$$\tau[x \to a](y) = \begin{cases} \tau(y), \text{ si } y \neq x \\ a, \text{ si } y = x. \end{cases}$$

Ahora podemos definir cuándo una estructura $\mathcal{A}$ con dominio A y una asignación τ para $\mathcal{A}$ satisfacen a una fórmula φ. En este caso escribimos $(A, \tau) \models \varphi$, y lo definimos de forma inductiva:

- $(\mathcal{A}, \tau) \models R(t_1, \ldots, t_n)$ si y solo si $(\tau(t_1), \ldots, \tau(t_n)) \in R^{\mathcal{A}}$;
- $(\mathcal{A}, \tau) \models (s = t)$ si y solo si $\tau(s) = \tau(t)$;
- $(\mathcal{A}, \tau) \models \varphi \wedge \psi$ si y solo si $(\mathcal{A}, \tau) \models \varphi$ y $(\mathcal{A}, \tau) \models \psi$;
- $(\mathcal{A}, \tau) \models \varphi \vee \psi$ si y solo si se tiene que $(\mathcal{A}, \tau) \models \varphi$ o $(\mathcal{A}, \tau) \models \psi$;
- $(\mathcal{A}, \tau) \models \varphi \rightarrow \psi$ si y solo si se tiene que $(\mathcal{A}, \tau) \models \psi$ cada vez que $(\mathcal{A}, \tau) \models \varphi$;
- $(\mathcal{A}, \tau) \models \neg\varphi$ si y solo si no es verdad que $(\mathcal{A}, \tau) \models \varphi$;
- $(\mathcal{A}, \tau) \models \forall x\varphi$ si para todo elemento $a \in A$ se tiene que $(\mathcal{A}, \tau[x \to a]) \models \varphi$
- $(\mathcal{A}, \tau) \models \exists x\varphi$ si existe un elemento $a \in A$ tal que $(\mathcal{A}, \tau[x \to a]) \models \varphi$

Si τ es una asignación tal que $\tau(x_i) = a_i$ para cada $1 \leq i \leq n$, entonces para abreviar $(\mathcal{A}, \tau) \models \varphi(x_1, \ldots, x_n)$ podemos usar en vez $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$.

Ejercicio. Considera el vocabulario $L = \{R\}$, con una relación binaria R, con el que representábamos grafos. Considera la estructura $\mathcal{A} = \langle \{a, b, c, d\}, R^{\mathcal{A}} \rangle$, en donde $R^{\mathcal{A}} = \{(a, b), (b, c), (c, d), (d, a), (d, d)\}$. Qué grafo representa esa estructura? ¿Para qué asignación τ se verifica que $(\mathcal{A}, \tau) \models R(x, x)$? ¿Para qué asignación (o asignaciones) τ se verifica que $(\mathcal{A}, \tau) \models \forall x \exists y \; R(x, y)$?

Observación. Si φ es una L-oración, entonces no nos importan las asignaciones al momento de satisfacer una oración (la intuición es que no tiene variables libres, y por tanto no hay nada que asignar). En ese caso escribimos solo $\mathcal{A} \models \varphi$. Y hablamos de que $\mathcal{A}$ satisface o no a la fórmula.

Ejercicio. Considera el vocabulario $L = \{c_1, c_2, R\}$, con dos constantes y una relación binaria R. Escribe una oración que sea verdad en todas las estructuras (grafos) en las que la interpretación de la constante c_1 no está conectada con la interpretación de la constante c_2. Escribe una oración que sea verdad en todos los grafos que son cliques.

2. Aplicación: teoría de grafos

Sea $L = \{E(\cdot, \cdot)\}$ el vocabulario sobre grafos. Usamos STRUCT$[L]$ para denotar a todas las estructuras existentes con un vocabulario: en este caso, STRUCT$[L]$ son todos los grafos.

Una *propiedad* sobre grafos es un subconjunto $P \subseteq$ STRUCT$[L]$ de grafos. Decimos que la propiedad es *definible* en lógica de primer orden si existe una L-oración φ tal que $\mathcal{A} \models \varphi$ si y solo si $A \in P$, es decir, un grafo $\mathcal{A}$ satisface a φ si y solo si $\mathcal{A}$ pertenece a la propiedad.

Muestra que las siguientes propiedades sobre grafos son definibles en lógica de primer orden:

- El grafo es un clique
- El grafo tiene al menos 5 nodos
- El grafo tiene al menos 3 aristas
- El grafo no tiene triángulos

Considera ahora el vocabulario $L' = \{E(\cdot, \cdot), a, b\}$ que ademas incorpora dos constantes. En este caso STRUCT$[L']$ son todos los grafos con dos de sus nodos distinguidos: un nodo es la interpretación de la constante a y el otro es la interpretación de la constante b.

Muestra que las siguientes propiedades son definibles en lógica de primer orden usando L':

- Hay una arista entre la interpretación de a y la interpretación de b.
- El único nodo con más de 2 vecinos es el nodo correspondiente a la interpretación de a.