Agda: Un lenguaje con tipos dependientes desde la práctica

Ferreira Juan David

20 de septiembre de 2022

Introducción

La motivación de este trabajo es analizar el paper "Nominal Sets in Agda. A Fresh and Immature Mechanization"(Miguel Pagano y Jose E. Solsona) a partir del cual presentan el desarrollo de una nueva formalización de un conjunto Nominal en Agda.
Este trabajo contribuye a una mejor comprensión de los conjuntos **Nominales** y aporta una forma de probar sistemas de tipos basados en lógica nominal.

Semigrupo, Monoide y Grupo

Dado un conjunto G, $G \neq \emptyset$, una operación binaria es una función

$$* : G \times G \to G.$$

Un semigrupo es G un conjunto, $G \neq \emptyset$ junto con una operación binaria $* : G \times G \to G$ que es **asociativa**. Es decir,

$$(a * b) * c = a * (b * c); \forall a, b, c \in G.$$

Un monoide es un semigrupo G un conjunto, si existe un **elemento identidad** (a ambos lados) $e \in G$ tal que

$$\forall a \in G | a * e = e * a = a.$$

Un grupo es un monoide G, tal que todo elemento posee **inverso** vía $*$. Es decir,

$$\forall a \in G : \exists a^{-1} \in G | a * a^{-1} = a^{-1} * a = e.$$

Acción

Acción

Una acción de un grupo G en un conjunto S es una función $\cdot : G \times S \to S$, $(g, s) \mapsto g \cdot s$ tal que

i) $(gh) \cdot s = g \cdot (h \cdot s); \forall g, h \in G$ y $\forall s \in S$.

ii) $e \cdot s = s; \forall s \in S$, donde e es el **elemento identidad** de G.

G-Set

Un conjunto S en el cual un grupo G tiene una acción se llama G-set.

Morfismo de G-Set

Morfismo de G-Set

Sean S y T dos G-sets. Un morfismo de G-sets es función $f : S \to T$ tal que

$$f(g \cdot x) = g \cdot f(x)$$

para todo $x \in S$ y $g \in G$.

Estas se llaman funciones **equivariantes**.
Dado que id_S es equivariante y la composición de funciones equivariante resulta ser una función equivariante podemos hablar de la categoría de G-Sets.
Cualquier conjunto S puede ser visto como un G-set dejando $g \cdot x = x$, tal conjunto G se llama conjunto G discreto. Además, cualquier grupo actúa sobre sí mismo por la multiplicación.

Representaciones, acciones lineales y módulos

Representación por Permutacón

Una representación por permutacón de un grupo G en un conjunto S un momorfismo de G en el conjunto de todas las permutaciones de S.

Representación Lineal

Una representación lineal de un grupo G en un espacio vectorial V es un morfismo de G en el grupo de todas las transformaciones lineales inversibles en V.

A menos que los califiquemos con algún otro adjetivo, representación significará en este trabajo representación lineal. Restringiremos nuestra atención en grupos finitos y espacios vectoriales sobre el cuerpo complejo.

Representaciones, acciones lineales y módulos

Sea V un espacio vectorial sobre el cuerpo $\mathbb{F}$ y G un grupo.

Acción Lineal

Una acción de un grupo G en un espacio vectorial V es una función $\cdot : G \times V \to V$, $(g, v) \mapsto g \cdot v$ tal que

i) $(gh) \cdot v = g \cdot (h \cdot v); \forall g, h \in G$ y $\forall v \in V$.

ii) $e \cdot v = v; \forall v \in V$, donde e es el **elemento identidad** de G.

iii) $g \cdot (u + v) = g \cdot u + g \cdot v; \forall g \in G$ y $u, v \in V$.

iv) $g \cdot (\lambda v) = \lambda(g \cdot v); \forall g \in G, v \in V$ y $\forall \lambda \in F$.

Observación 1. Notar que para definir una acción de G en S los items *iii*) y *iv*) no son requeridos en un conjunto.

Luego, una representación de un grupo en un espacio vecotriales equivalente a una acción del grupo en el espacio vectorial.

G-módulo

Un espacio vectorial V en el cual un grupo G tiene una acción lineal se llama G-módulo.

G-submódulo

Un submódulo de un G-módulo V es un subespacio vectorial U de V tal que $g \cdot u \in U$ para todo $g \in G$ y $u \in U$.

Representaciones, acciones lineales y módulos

Teorema

Dada una acción de un grupo G en un espacio vectorial V, para cada g en G definimos una función $\rho g : V \to V$ dada por $(\rho g)v = g \cdot v$ para todo $v \in V$. Luego ρg es una transformación lineal inversible, y la función ρ definida por $g \mapsto \rho g$ es un homomorfismo de G en el grupo de todas las transformaciones lineales invertibles en V.

Recíprocamente, dado un homomorfismo ρ de G en el grupo de todas las tranformaciones lineales inversibles en V, la fórmula $g \cdot v = (\rho g)v$, define una acción de G en V.

Morfismo de G-módulos

Si U y V son G-módulos. Un G-homomorfismo de U en V es una transformación lineal $f : U \to V$ tal que

$$f(g \cdot u) = g \cdot (fu)$$

para todo $g \in G$ y $u \in U$.