Categories

Ross Tate

January 17, 2018

1 Monoids (and Endomorphisms)

Definition. A monoid is comprised of a set A with a distinguished element, denoted e, and a binary operator on A, denoted by juxtaposition, satisfying the following properties

Identity $\forall a \in A.\ ea = a = ae$

Associativity $\forall a_1, a_2, a_3 \in A.\ a_1(a_2a_3) = (a_1a_2)a_3$ (often unambiguously denoted simply by $a_1a_2a_3$)

Example. The tuples $\langle \mathbb{N}, 0, + \rangle$, $\langle \mathbb{Z}, 0, + \rangle$, $\langle \mathbb{R}, 0, + \rangle$, $\langle \mathbb{N}, 1, * \rangle$, $\langle \mathbb{Z}, 1, * \rangle$, and $\langle \mathbb{R}, 1, * \rangle$ are all monoids.

Example. Substraction is *not* an associative operator, which is why we have to memorize that $a - b - c$ means specifically $(a - b) - c$ and *not* $a - (b - c)$.

Definition. Given two monoids A and B, a monoid homomorphism from A to B is a function $f : A \to B$ satisfying the following properties:

Preservation of Identity $f(e_A) = e_B$

Preservation of Multiplication $f(a_1a_2) = f(a_1)f(a_2)$

Example. The inclusions $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{R}$ provide monoid homomorphisms $\langle \mathbb{N}, 0, + \rangle \hookrightarrow \langle \mathbb{Z}, 0, + \rangle \hookrightarrow \langle \mathbb{R}, 0, + \rangle$ and $\langle \mathbb{N}, 1, * \rangle \hookrightarrow \langle \mathbb{Z}, 1, * \rangle \hookrightarrow \langle \mathbb{R}, 1, * \rangle$.

Example. For any $c \in \mathbb{R}^{>}$ (which denotes the set of real numbers strictly greater than 0), the function $\lambda x.\ c^x$ is a monoid homomorphism from $\langle \mathbb{R}, 0, + \rangle$ to $\langle \mathbb{R}, 1, * \rangle$.

Definition. An endomorphism is a morphism from an object to that same object, i.e. a morphism whose domain is the same as its codomain.

Example. For any $c \in \mathbb{R}$, the function $\lambda x.\ cx$ is a monoid endomorphism on $\langle \mathbb{R}, 0, + \rangle$, and the function $\lambda x.\ x^c$ is a monoid endomorphism on $\langle \mathbb{R}^{\neq}, 1, * \rangle$ (where $\mathbb{R}^{\neq}$ denotes the set of real numbers not equal to 0).

Definition. **Mon** is the category whose objects are monoids and whose morphisms are monoid homomorphisms.

2 Groups

Definition. A group is a monoid A with a unary operator $^{-1}$, known as the inverse operator, satisfying the property $\forall a \in A.\ aa^{-1} = e = a^{-1}a$.

Example. $\langle \mathbb{R}, 0, +, - \rangle$ and $\langle \mathbb{R}^{\neq}, 1, *, ^{-1} \rangle$ are both groups.

Definition. A group homomorphism from A to B is a monoid homomorphism $f : A \to B$ that preserves inverses, meaning $\forall a \in A.\ f(a^{-1}) = f(a)^{-1}$.

Definition. **Grp** is the category whose objects are groups and whose morphisms are group homomorphisms.

3 Relations as Morphisms

Definition. **Rel** is the category whose objects are sets and whose morphisms from A to B are relations between A and B, i.e. subsets of $A \times B$.

Identity The identity relation on A is A's equality relation, i.e. the subset $\{\langle a, a \rangle \mid a \in A\} \subseteq A \times A$.

Composition Given two relations $R \subseteq A \times B$ and $S \subseteq B \times C$, the composition $R\,;S$ relates $a \in A$ to $c \in C$ when there exists a $b \in B$ such that $a\ R\ b$ and $b\ S\ c$ hold. In other words, $R\,;S$ is the subset $\{\langle a, c \rangle \mid a \in A, c \in C, \exists b \in B.\ \langle a, b \rangle \in R \land \langle b, c \rangle \in S\} \subseteq A \times C$.

4 Languages

Definition. Given a set Σ conceptually representing characters, Σ-**Lang** is the category of Σ-languages. Its objects are subsets of $\mathbb{L}\Sigma$ (i.e. Σ-strings), and there exists a unique morphism from one object to another if the former is a subset of the latter.

5 Graphs

Definition. **Graph** is the category of (directed) graphs and graph homomorphisms. A graph is comprised of a set V (of vertices), a set E (of edges), and functions s (source) and t (target) from E to V. A graph homomorphism from the graph $\langle V_1, E_1, s_1, t_1 \rangle$ to the graph $\langle V_2, E_2, s_2, t_2 \rangle$ is comprised of a function $f_v : V_1 \to V_2$ and a function $f_e : E_1 \to E_2$ that preserves sources and targets, meaning $\forall e \in E_1.\ s_2(f_e(e)) = f_v(s_1(e))$ and $\forall e \in E_1.\ t_2(f_e(e)) = t_v(s_1(e))$.

Definition. L-**Graph** is the category of (directed) graphs with L-labeled edges. An object is comprised of a graph $\langle V, E, s, t \rangle$ and a (labeling) function $\ell : E \to L$. A morphism from $\langle G_1, \ell_1 \rangle$ to $\langle G_2, \ell_2 \rangle$ is a graph homomorphism $\langle f_v, f_e \rangle : G_1 \to G_2$ that preserves labels, meaning $\forall e \in E_1.\ \ell_2(f_e(e)) = \ell_1$.

6 Circuits

Definition. A circuit from $m \in \mathbb{N}$ to $n \in \mathbb{N}$ is a finite set G (of gates), a function $op : G \to \{\wedge, \vee\} \times \{+, -\}$ (specifying which operator each gate employs: and/or/nand/nor), a well-founded relation $W \subseteq (\mathbb{N}_m + G) \times G$ (indicating when there is a wire from an input/gate to a gate), and a function $out : \mathbb{N}_n \to \mathbb{N}_m + G$ indicating which input/gate generates a given output. Two circuits C_1 and C_2 are equal if there is a bijection between G_1 and G_2 that preserves the relevant structures.

Definition. **Circ** is the category of circuits. Its objects are natural numbers (indicating the number of bits), and its morphisms from m to n are the circuits from m to n. The identity circuits are the empty circuits in which every output is generated by the corresponding input. The composition of circuits C_1 and C_2 uses the disjoint union of the gates of C_1 and C_2 and rewires each input in C_2 to the gate generating the corresponding output in C_1.