Monoids

Ross Tate

August 26, 2014

Definition ((Biased) Monoid)**.** A tuple $\langle M, *, \mathfrak{a}, e, \mathfrak{i} \rangle$ where the components have the following types:

Underlying Set M: $\texttt{Type}$

Operator $*$: $M \times M \to M$ (infix)

Associativity $\mathfrak{a}$: $\forall m_1, m_2, m_3 : M.\ (m_1 * m_2) * m_3 = m_1 * (m_2 * m_3)$

Identity Element e: M

Identity $\mathfrak{i}$: $\forall m : M.\ e * m = m = m * e$

Notation. We use $M : \texttt{Type}$ to say what the reader may more familiarly interpret as saying M is a set. We use $\texttt{Type}$ to indicate that we do not tie our discussion to any particular set theory. In particular, in category theory one often needs higher universes (e.g. the class of all sets, and the conglomerate of all classes), which we will denote with $\texttt{Type}_0$, $\texttt{Type}_1$, and so on. In particular, $\texttt{Type}_i$ is an element of $\texttt{Type}_{i+1}$. We use $\texttt{Type}$ as shorthand for $\texttt{Type}_0$. Note that all this of course should in fact be polymorphic with respect to universes, but we do not want to get distracted by such details.

Remark. We assume proof irrelevance. That is, all proofs of the same proposition are equal. This way we can avoid coherence requirements of proofs. Consequently, often such proofs will be omitted when apparent from context or proven elsewhere, denoted by $\blacksquare$.

Notation. In situations where an infix operator $*$ is associative, we use $a * b * c$ to denote either of the equal terms $(a * b) * c$ and $a * (b * c)$.

Example. $\mathbb{N}_+ = \langle \mathbb{N}, +, \blacksquare, 0, \blacksquare \rangle$

$\mathbb{N}_* = \langle \mathbb{N}, *, \blacksquare, 1, \blacksquare \rangle$

$\mathbb{N}_{\max} = \langle \mathbb{N}, \max, \blacksquare, 0, \blacksquare \rangle$

$\mathbb{Z}_+ = \langle \mathbb{Z}, +, \blacksquare, 0, \blacksquare \rangle$

$\mathbb{Z}_* = \langle \mathbb{Z}, *, \blacksquare, 1, \blacksquare \rangle$

$\mathbb{R}_+ = \langle \mathbb{R}, +, \blacksquare, 0, \blacksquare \rangle$

$\mathbb{R}_* = \langle \mathbb{R}, *, \blacksquare, 1, \blacksquare \rangle$

$\mathbb{N}^\infty_+ = \langle \mathbb{N}^\infty, +, \blacksquare, 0, \blacksquare \rangle$ where $\mathbb{N}^\infty = \mathbb{N} \uplus \{\infty\}$ and $\forall n : \mathbb{N}^\infty.\ \infty + n = \infty = n + \infty$

$\mathbb{N}^\infty_{\min} = \langle \mathbb{N}^\infty, \min, \blacksquare, \infty, \blacksquare \rangle$ where $\forall n : \mathbb{N}^\infty.\ \min(\infty, n) = n = \min(n, \infty)$

$\mathbb{B}_\wedge = \langle \mathbb{B}, \wedge, \blacksquare, \mathbb{t}, \blacksquare \rangle$ where $\mathbb{B}$ denotes the Booleans, $\wedge$ denotes Boolean "and", and $\mathbb{t}$ denotes the true Boolean

$\mathbb{B}_\vee = \langle \mathbb{B}, \vee, \blacksquare, \mathbb{f}, \blacksquare \rangle$ where $\vee$ denotes Boolean "or" and $\mathbb{f}$ denotes the false Boolean

$(\mathbb{L}T)_{++} = \langle \mathbb{L}T, ++, \cdot, [\,], \cdot \rangle$ where $\mathbb{L}T$ denotes (finite) lists of T and $++$ denotes list appending

$(\mathbb{M}T)_+ = \langle \mathbb{M}T, +, \cdot, [\,], \cdot \rangle$ where $\mathbb{M}T$ denotes multisets (a.k.a. bags) of T and $+$ denotes multiset addition

$(\mathbb{S}T)_\cup = \langle \mathbb{S}T, \cup, \cdot, \varnothing, \cdot \rangle$ where $\mathbb{S}T$ denotes finite subsets of T and $\cup$ denotes finite-set union

$(\mathbb{P}T)_\cup = \langle \mathbb{P}T, \cup, \cdot, \varnothing, \cdot \rangle$ where $\mathbb{P}T$ denotes subsets of T and $\cup$ denotes subset union

$(\mathbb{P}T)_\cap = \langle \mathbb{P}T, \cap, \cdot, T, \cdot \rangle$ where $\cap$ denotes subset intersection

$(\mathbb{R} \to \mathbb{R})_; = \langle \mathbb{R} \to \mathbb{R}, ;, \cdot, \lambda x.\ x, \cdot \rangle$ where $f\,;g = \lambda x.g(f(x))$

$(\mathbb{R} \to \mathbb{R})_\circ = \langle \mathbb{R} \to \mathbb{R}, \circ, \cdot, \lambda x.\ x, \cdot \rangle$ where $f \circ g = \lambda x.f(g(x))$

Notation. The operator $\uplus$ denotes disjoint union; we will never use $\cup$ or union except when the two sets are established to be subsets of some larger set in the context. Technically, one needs to explicitly inject elements into the left or right parts of a disjoint union, but the injection to use can usually be inferred from context.

Remark. Note that many of the above have the same underlying set, and some of those even have the same identity element, but no two have the same operator (where $*$ on $\mathbb{N}$ is not considered the same as $*$ on $\mathbb{R}$ or $\mathbb{Z}$).

Exercise 1. Prove that two monoids are equal if (and only if) their operators are equal (possible only if their underlying sets are equal). Due to proof irrelevance, this is equivalent to proving that their identity elements are equal.