University of Leicester

Department of Computer Science

Research Report No. CS-10-004

Nominal Monoids

Alexander Kurz

Tomoyuki Suzuki

Emilio Tuosto

October 2010

Nominal Monoids

Alexander Kurz Tomoyuki Suzuki Emilio Tuosto
Department of Computer Science, University of Leicester, UK

University of Leicester Technical Report CS-10-004, October 2010

Abstract

We investigate different notions of nominal words, that is, words that my contain letters from an alphabet as well as names and name-binders. In a first section we construct them from first principles. In a second section we take the point of view that—as in the classical case—words over an alphabet S form a free monoid over S. We define different notions of nominal monoids and reveal nominal words as elements of free nominal monoids. Applications to computer science will be treated in subsequent work.

1 Introduction

Section 2 introduces several different notions of nominal words from first principles. Depending on how the binder $[n]$ interacts with the other word-forming operations, different notions arise. The most general class of words consists of p-words but they are actually trees rather than words since the binder introduces a notion of scope. The class of ng-words consists of those p-words where the scope always extends as far to the right as possible: they are linear like classical words. In l-words, the binders can be moved to the left into a prefix, prefixing a word without binders in the usual sense. Furthermore, in f-words, this prefix forms a set and each name in this set has to actually appear in the word. These different notions correspond to different intuitions arising from the interpretation of name-binding as resource-allocation and we will briefly discuss this in the summary.

Section 3 reviews these notions taking a more conceptual approach. Following nominal algebra as outlined by Gabbay [1] and Gabbay and Mathijssen [3], we first define the notion of a nominal monoid and then refine it by adding further axioms. We reveal the notions of words defined in the previous section as initial or free algebras in the corresponding categories of monoids.

We conclude with a table summarising the different notions.

2 Nominal words

We denote a countably infinite set of 'names' by $\mathcal{N}$ and an alphabet (finite set of 'letters') by S. Further, the set of all *finite kernel* bijective functions (permutations) $\pi\colon \mathcal{N} \to \mathcal{N}$ is denoted by $Perm(\mathcal{N})$, where a permutation $\pi\colon \mathcal{N} \to \mathcal{N}$ is finite kernel when the set $Ker(\pi) \stackrel{\text{def}}{=} \{a \in \mathcal{N} \mid \pi(a) \neq a\}$ is finite). We often use transpositions $(m\ n)$, which swap m and n, denote the identity permutation by ι, and the empty word ε. We also assume that $\mathcal{N}$ and S are disjoint.

Let A be a set with a $Perm(\mathcal{N})$-action. An element $a \in A$ is called *finitely supported*, if there exists a finite subset $N \subseteq \mathcal{N}$ such that, for all $\pi, \pi' \in Perm(\mathcal{N})$, if $\pi_{|N} = \pi'_{|N}$, then $\pi \cdot a = \pi' \cdot a$. We call such an N a *support*

for a. Among finite supports of a, the minimal one, which always exists, is called *the support of a*, denoted by $supp(a)$. We write $n\#a$ for $n \notin supp(a)$.

Definition 1 (Nominal sets [2]) *A set A equipped with a $Perm(\mathcal{N})$-action $\cdot$ is a* nominal set, *if all its elements are finitely supported. The action satisfies, for each $a \in A$,*

1. $\pi' \cdot (\pi \cdot a) = (\pi'\pi) \cdot a$ *for all* $\pi, \pi' \in Perm(\mathcal{N})$,
2. $\iota \cdot a = a$,

where π, π' denote two permutations and ι denotes identity. We often write $\pi' \circ \pi$ instead of $\pi'\pi$ to denote composition. A function between two nominal sets is called equivariant if it preserves the permutation action.

Let us begin with the definition of words in the classical language theory.

Definition 2 (Finite words) *Given a set A, we inductively define a* (finite) word over *A as follows:*

$$w ::= \varepsilon \mid aw,$$

where $a \in A$. We denote the set of all finite words on A by A^*.

For any set A, it is well-known that A^* forms a monoid with concatenation and the empty word. Among all monoids, it is the *the free monoid over A*. Hereafter, the following two free monoids $\mathcal{N}^*$ and $(\mathcal{N} \cup \mathcal{S})^*$ play fundamental roles. We extend each permutation $\pi \in Perm(\mathcal{N})$ on $\mathcal{N}$ to a permutation on $\mathcal{N}^*$ and $(\mathcal{N} \cup \mathcal{S})^*$ as follows: $\cdot : Perm(\mathcal{N}) \times (\mathcal{N} \cup \mathcal{S})^* \to (\mathcal{N} \cup \mathcal{S})^*$, for each $n \in \mathcal{N}$, each $s \in \mathcal{S}$ and each $w \in (\mathcal{N} \cup \mathcal{S})^*$

1. $\pi \cdot \varepsilon \stackrel{\text{def}}{=} \varepsilon$,
2. $\pi \cdot nw \stackrel{\text{def}}{=} \pi(n)(\pi \cdot w)$,
3. $\pi \cdot sw \stackrel{\text{def}}{=} s(\pi \cdot w)$.

Note that the above also defines how permutations act on $\mathcal{N}^*$. We will often denote $\pi \cdot p$ and $\pi \cdot w$ as $\pi(p)$ and $\pi(w)$ for each $p \in \mathcal{N}^*$ and each $w \in (\mathcal{N} \cup \mathcal{S})^*$. However, when we take a transposition $(m\ n)$, we will always write $(m\ n) \cdot p$ and $(m\ n) \cdot w$. Note that $\mathcal{N}, \mathcal{S}, \mathcal{N}^*$ and $(\mathcal{N} \cup \mathcal{S})^*$ are all nominal sets.

Definition 3 ($\mathcal{G}$, ng-words) *To introduce words with name binders consider:*

$$w ::= \varepsilon \mid nw \mid sw \mid \langle n.w \rangle,$$

where $n \in \mathcal{N}$ and $s \in \mathcal{S}$. We call the words defined above ng-words *and denote by $\mathcal{G}$ the set of all ng-words. We also might write $[n]w$ instead of $\langle n.w \rangle$.*

We also define a $Perm(\mathcal{N})$-action on $\mathcal{G}$. For each $\pi \in Perm(\mathcal{N})$, $n \in \mathcal{N}$, $s \in \mathcal{S}$ and $w \in \mathcal{G}$, we put

1. $\pi \cdot \varepsilon \stackrel{\text{def}}{=} \varepsilon$,
2. $\pi \cdot nw \stackrel{\text{def}}{=} \pi(n)\pi(w)$,
3. $\pi \cdot sw \stackrel{\text{def}}{=} s\pi(w)$,

4. $\pi \cdot \langle n.w \rangle \stackrel{\text{def}}{=} \langle \pi(n).\pi(w) \rangle$.

Unlike the words in Definition 2, $\mathcal{G}$ is not a monoid since it is not closed under concatenation, eg. $\langle n.n \rangle \langle m.m \rangle$ is not a ng-word. This will be repaired in Definition 16. But it also hints at the fact that, in the presence of binders, several different notions of monoid make sense. We identify the following.

The most general notion derives from adding binders to a monoid. Having a binary $\circ$ and binding $\langle n.w \rangle$ actually means that 'p-words' are not linear but have a tree-structure.

Definition 4 (p-word) *A* p-word *is inductively defined as follows:*

$$w ::= \varepsilon \mid n \mid s \mid w \circ w \mid \langle n.w \rangle,$$

where we assume that $n \in \mathcal{N}$, $s \in \mathcal{S}$ and that ε and $\circ$ satisfy the monoid laws. We denote the set of all p-words by $\mathcal{P}$. We might write wv instead of $w \circ v$ and $[n]w$ instead of $\langle n.w \rangle$.

More special than p-words are the ng-words defined above: they have a linear structure. More special again are the l-words, where all binders can be moved to the left, so that a word can be separated into a prefix p of binders and binder-free word w.

Definition 5 (l-word) *A pair (p,w) of $p \in \mathcal{N}^*$ and $w \in (\mathcal{N} \cup \mathcal{S})^*$ is called a* l-word. *We denote with $\mathcal{L}$ the set of all l-words, i.e.*

$$\mathcal{L} \stackrel{\text{def}}{=} \{(p,w) \mid p \in \mathcal{N}^*, w \in (\mathcal{N} \cup \mathcal{S})^*\}.$$

If we further require that order and multiplicity of the binders in the prefix do not matter and that all bound variables actually do occur in w, we arrive at the following notion.

Definition 6 (f-word) *A pair (S,w) of $w \in (\mathcal{N} \cup \mathcal{S})^*$ and $S \subseteq supp(w)$ is called a* f-word. *We denote by $\mathcal{F}$ the set of all f-words, i.e.*

$$\mathcal{F} \stackrel{\text{def}}{=} \{(S,w) \mid w \in (\mathcal{N} \cup \mathcal{S})^*, S \subseteq supp(w)\}.$$

As above for ng-words, $Perm(\mathcal{N})$-actions are defined as follows.

1. On $\mathcal{L}, \cdot : Perm(\mathcal{N}) \times \mathcal{L} \to \mathcal{L}$ is defined as $\pi \cdot (p,w) \stackrel{\text{def}}{=} (\pi(p), \pi(w))$.
2. On $\mathcal{F}, \cdot : Perm(\mathcal{N}) \times \mathcal{F} \to \mathcal{F}$: $\pi \cdot (S,w) \stackrel{\text{def}}{=} (\pi(S), \pi(w))$, where $\pi(S) \stackrel{\text{def}}{=} \{\pi(n) \mid n \in S\}$.
3. On $\mathcal{P}, \cdot : Perm(\mathcal{N}) \times \mathcal{P} \to \mathcal{P}$ is inductively defined as follows:
   (a) $\pi \cdot \varepsilon \stackrel{\text{def}}{=} \varepsilon$,
   (b) $\pi \cdot n \stackrel{\text{def}}{=} \pi(n)$,
   (c) $\pi \cdot s \stackrel{\text{def}}{=} s$,
   (d) $\pi \cdot (w \circ v) \stackrel{\text{def}}{=} \pi(w) \circ \pi(v)$,
   (e) $\pi \cdot \langle n.w \rangle \stackrel{\text{def}}{=} \langle \pi(n).\pi(w) \rangle$.

We want to identify words up to α-equivalence. For example, $\langle n.n \rangle$ and $\langle m.m \rangle$ should be the same word. We first fix the following

Notation 7 *We write* æ *as an abbreviation of "for all but finitely many" that corresponds to the new-quantifier of Gabbay and Pitts [2].*

Definition 8 *On $\mathcal{P}$ (and analogously on $\mathcal{G}$) $\sim$ is defined as follows:*

1. $\varepsilon \sim \varepsilon$,
2. $n \sim n$,
3. $s \sim s$,
4. $w \circ v \sim w' \circ v' \iff w \sim w'$ *and* $v \sim v'$,
5. $\langle n.w \rangle \sim \langle m.v \rangle \iff$ æ $l \in \mathcal{N}.\ (l\ n) \cdot w \sim (l\ m) \cdot v$.

Definition 9 *On $\mathcal{L}$, $\sim$ is given as*

1. $(\varepsilon, w) \sim (\varepsilon, w)$,
2. $(pn, w) \sim (qm, v) \iff$ æ $l \in \mathcal{N}.\ (p, (l\ n) \cdot w) \sim (q, (l\ m) \cdot v)$.

Lemma 10 *For all $(p,w),(q,v) \in \mathcal{L}$, if $(p,w) \sim (q,v)$, then the length of p is the same with that of q. Moreover, if $p = n_1 \cdots n_k$ and $q = m_1 \cdots m_k$,*

$$æ l_1 \in \mathcal{N}, \ldots, æ l_k \in \mathcal{N}.\ (l_1\ n_1) \cdots (l_k\ n_k) \cdot w = (l_1\ m_1) \cdots (l_k\ m_k) \cdot v.$$

Definition 11 *On $\mathcal{F}$, for all $(S,w),(T,v) \in \mathcal{F}$, we let*

$$(S,w) \sim (T,v) \iff \exists k, \exists b_S, \exists b_T, æ l_1 \in \mathcal{N}, \ldots, æ l_k \in \mathcal{N}.(l_1\ b_S(1)) \cdots (l_k\ b_S(k)) \cdot w = (l_1\ b_T(1)) \cdots (l_k\ b_T(k)) \cdot v$$

with bijections $b_S : \{1, \ldots, k\} \to S$ and $b_T : \{1, \ldots, k\} \to T$

Note that $(\emptyset, w) \sim (\emptyset, v)$ if and only if $w = v$.

Proposition 12 *The binary relations $\sim$ in Definitions 9 and 11 are equivalence relations.*

Proof Reflexivity and symmetry are trivial in each case. For all $(p,w),(q,v),(r,u) \in \mathcal{L}_\sim$, if $(p,w) \sim (q,v)$ and $(q,v) \sim (r,u)$, we can assume that $p = n_1 \cdots n_k$, $q = m_1 \cdots m_k$ and $r = l_1 \cdots l_k$, and

$$æ o_1 \in \mathcal{N}, \ldots, æ o_k \in \mathcal{N}.\ (o_1\ n_1) \cdots (o_k\ n_k) \cdot w = (o_1\ m_1) \cdots (o_k\ m_k) \cdot v,$$

$$æ o'_1 \in \mathcal{N}, \ldots, æ o'_k \in \mathcal{N}.\ (o'_1\ m_1) \cdots (o'_k\ m_k) \cdot v = (o'_1\ l_1) \cdots (o'_k\ l_k) \cdot u,$$

by Lemma 10. By the definition of æ, we also have

$$æ o_1 \in \mathcal{N}, \ldots, æ o_k \in \mathcal{N}.\ (o_1\ n_1) \cdots (o_k\ n_k) \cdot w = (o_1\ l_1) \cdots (o_k\ l_k) \cdot u.$$

Hence, $(p,w) \sim (r,u)$. For all $(S,w),(T,v),(U,u) \in \mathcal{F}_\sim$ and $card(S) = k$, if $(S,w) \sim (T,v)$ and $(T,v) \sim (U,u)$, by definition, there are bijections b_S, b_T, b'_T, b_U. Since b_T and b'_T are bijections from the same domain, there is a permutation $\pi : T \to T$ which makes $b'_T = \pi \circ b_T$. Thus, we have

$$æ l_1 \in \mathcal{N}, \ldots, æ l_k \in \mathcal{N}.\ (l_1\ \pi \circ b_S(1)) \cdots (l_k\ \pi \circ b_S(k)) \cdot w = (l_1\ b_U(1)) \cdots (l_k\ b_U(k)) \cdot u,$$

hence $(S,w) \sim (U,u)$. The cases for $\mathcal{G}_\sim$ and $\mathcal{P}_\sim$ are by induction. □

We denote by $\mathcal{G}_\sim, \mathcal{L}_\sim, \mathcal{F}_\sim, \mathcal{P}_\sim$ each quotient set with respect to the appropriate binary relation $\sim$. We will use the terms *ng-word*, *l-word*, *f-word* and *p-word* for equivalence classes as well. To distinguish equivalence classes from the original words, we might call the original words *prewords*. To avoid nesting brackets, we abbreviate the equivalence class with $w, (p,w), (S,w), w$ like the original words.

Proposition 13 *The $Perm(\mathcal{N})$-actions on $\mathcal{G}$, $\mathcal{L}$, $\mathcal{F}$, $\mathcal{P}$ induce $Perm(\mathcal{N})$-actions on $\mathcal{G}_\sim$, $\mathcal{L}_\sim$, $\mathcal{F}_\sim$, $\mathcal{P}_\sim$, respectively.*

Now, we recall Definition 1 and show the following.

Theorem 14 *The quotient sets $\mathcal{G}_\sim, \mathcal{L}_\sim, \mathcal{F}_\sim$ and $\mathcal{P}_\sim$ are all nominal sets. That is, each quotient set $S_\sim$ is finitely supported, and there exists a $Perm(\mathcal{N})$-action $\cdot : Perm(\mathcal{N}) \times S_\sim \to S_\sim$ such that for all $\pi, \pi' \in Perm(\mathcal{N})$ and every element $s \in S_\sim$, we have*

1. $\pi' \cdot (\pi \cdot s) = (\pi' \circ \pi) \cdot s$,
2. $\mathrm{i} \cdot s = s$.

Proof Any word has a finite set of free names, which is its support. Items 1 and 2 are straightforward. □

Lemma 15 (Renaming) *For all l-prewords $(p,w), (q,v)$, there exist l-prewords $(p',w'), (q',v')$ such that $(p,w) \sim (p',w')$, $(q,v) \sim (q',v')$, p' and q' does not share any name, p' and v' share no name, and q' and w' share no name.*

Proof To simplify our argument, we assume that an order is given on $\mathcal{N}$ (notice though that the following arguments do not depend on the chosen order on $\mathcal{N}$).

For each l-preword (p,w), let $fv(p,w)$ be the set of all free variables in w, i.e. $fv(p,w)$ is the collection of names which occurs only in w but not in p. Suppose that $p = n_1 \cdots n_k$ and $q = m_1 \cdots m_l$. Since every l-preword contains a finite number of names, $fv(p,w)$ and $fv(q,v)$ are finite, hence $fv(p,w) \cup fv(q,v)$ is also finite. We let a be the largest name with respect to the order on $\mathcal{N}$, and let

$$p' \stackrel{\text{def}}{=} (a+1) \cdots (a+k) \text{ and } w' \stackrel{\text{def}}{=} (a+1\ n_1) \circ \cdots \circ (a+k\ n_k) \cdot w,$$
$$q' \stackrel{\text{def}}{=} (a+k+1) \cdots (a+k+l) \text{ and } v' \stackrel{\text{def}}{=} (a+k+1\ m_1) \circ \cdots \circ (a+k+l\ m_l) \cdot v.$$

By construction, it is straightforward that they satisfy the required conditions. □

Similar statements hold for ng-prewords, f-prewords and p-prewords. Thanks to Lemma 15, we can define the following functions on each quotient set.

Definition 16 1. $\circ : \mathcal{G}_\sim \times \mathcal{G}_\sim \to \mathcal{G}_\sim$: *for all $w, v \in \mathcal{G}_\sim$ we define by induction on the construction of the first argument:*

   (a) $\varepsilon \circ v \stackrel{\text{def}}{=} v$,

   (b) $nw \circ v \stackrel{\text{def}}{=} n(w \circ v)$,

   (c) $sw \circ v \stackrel{\text{def}}{=} s(w \circ v)$,

   (d) $\langle n.w \rangle \circ v \stackrel{\text{def}}{=} \langle n', (w' \circ v) \rangle$, *where n' is fresh for v and $\langle n.w \rangle \sim \langle n'.w' \rangle$.*

2. $\circ : \mathcal{L}_\sim \times \mathcal{L}_\sim \to \mathcal{L}_\sim$: $(p,w) \circ (q,v) \stackrel{\text{def}}{=} (p'q', w'v')$, *where* $(p,w) \sim (p',w')$, $(q,v) \sim (q',v')$, p' *and* q', p' *and* v', q' *and* w' *do not share any name.*

3. $\circ : \mathcal{F}_\sim \times \mathcal{F}_\sim \to \mathcal{F}_\sim$: $(S,w) \circ (T,v) \stackrel{\text{def}}{=} (S' \cup T', w'v')$, *where* $(S,w) \sim (S',w')$, $(T,v) \sim (T',v')$, *and* $S' \cap T' = S' \cap v' = T' \cap w' = \emptyset$.

4. $\circ : \mathcal{P}_\sim \times \mathcal{P}_\sim \to \mathcal{P}_\sim$: $w \circ v \stackrel{\text{def}}{=} wv$.

5. $[\_]\_ : [\mathcal{N}]\mathcal{G}_\sim \to \mathcal{G}_\sim$: $[n]w \stackrel{\text{def}}{=} \langle n.w \rangle$.

6. $[\_]\_ : [\mathcal{N}]\mathcal{L}_\sim \to \mathcal{L}_\sim$: $[n](p,w) \stackrel{\text{def}}{=} (np, w)$.

7. $[\_]\_ : [\mathcal{N}]\mathcal{F}_\sim \to \mathcal{F}_\sim$: $[n](S,w) \stackrel{\text{def}}{=} \begin{cases} (S,w) & \text{if } n\#(S,w), \\ (S \cup \{n\}, w) & \text{if } n \in \mathit{supp}(S,w). \end{cases}$

8. $[\_]\_ : [\mathcal{N}]\mathcal{P}_\sim \to \mathcal{P}_\sim$: $[n]w \stackrel{\text{def}}{=} \langle n.w \rangle$.

Proposition 17 *For each quotient set, the above concatenation* $\circ$ *and atom-abstraction* $[\_]\_$ *are well-defined equivariants.*

Proof Here, we check only $\circ : \mathcal{G}_\sim \times \mathcal{G}_\sim \to \mathcal{G}_\sim$ and $[\_]\_ : [\mathcal{N}]\mathcal{F}_\sim \to \mathcal{F}_\sim$.

For the first case, it suffices to show that $(\pi \cdot w) \circ (\pi \cdot v) = \pi \cdot (w \circ v)$ for each $\pi \in \mathit{Perm}(\mathcal{N})$ and all $w, v \in \mathcal{G}_\sim$. We use the induction on w.

(Base case $w = \varepsilon$) $(\pi \cdot \varepsilon) \circ (\pi \cdot v) = \varepsilon \circ (\pi \cdot v) = \pi \cdot v$ and $\pi \cdot (\varepsilon \circ v) = \pi \cdot v$.

(Inductive steps) Assume that $(\pi \cdot w) \circ (\pi \cdot v) = \pi \cdot (w \circ v)$.

1. $(\pi \cdot nw) \circ (\pi \cdot v) = (\pi(n)\pi \cdot w) \circ (\pi \cdot v) = \pi(n)((\pi \cdot w) \circ (\pi \cdot v))$ by definition of $\cdot$ and $\circ$. By the assumption, we have $\pi(n)(\pi \cdot (w \circ v))$. On the other hand, $\pi \cdot (nv \circ v) = \pi \cdot (n(w \circ v)) = \pi(n)(\pi \cdot (w \circ v))$ by definition.

2. $(\pi \cdot sw) \circ (\pi \cdot v) = \pi \cdot (sw \circ v)$. This is analogous to Item 1.

3. By Lemma 15, we can assume that n is fresh for v. Now, $(\pi \cdot \langle n.w \rangle) \circ (\pi \cdot v) = \langle \pi(n).\pi \cdot w \rangle \circ (\pi \cdot v)$. Since π is bijective, $\pi(n)$ is fresh for $\pi \cdot v$. Then, we have $\langle \pi(n).(\pi \cdot w) \circ (\pi \cdot v) \rangle$. By assumption, $\langle \pi(n).\pi \cdot (w \circ v) \rangle$, hence $\pi \cdot (\langle n.w \rangle \circ v)$.

For the second case, we recall that, for each $(S,w) \in \mathcal{F}_\sim$ any $n \in \mathcal{N}$ is either $n\#(S,w)$ or $n \in \mathit{supp}(S,w)$. Moreover, since every $\pi \in \mathit{Perm}(\mathcal{N})$ is bijective, $n\#(S,w)$ if and only if $\pi(n)\#(\pi(S),\pi(w))$, hence $n \in \mathit{supp}(S,w) \iff \pi(n) \in \mathit{supp}(\pi(S),\pi(w))$.

If $n\#(S,w)$, then $\pi \cdot ([n](S,w)) = \pi(S,w) = (\pi(S),\pi(w))$ and $[\pi(n)](\pi \cdot (S,w)) = [\pi(n)](\pi(S),\pi(w)) = (\pi(S),\pi(w))$. Conversely, if $n \in \mathit{supp}(S,w)$, then $\pi \cdot ([n](S,w)) = \pi \cdot (S \cup \{n\}, w) = (\pi(S \cup \{n\}),\pi(w))$ and $[\pi(n)](\pi \cdot (S,w)) = [\pi(n)]\ (\pi(S),\pi(w)) = (\pi(S) \cup \pi(n),\pi(w)) = (\pi(S \cup \{n\}),\pi(w))$. Therefore, $\pi \cdot ([n](S,w)) = [\pi(n)](\pi \cdot (S,w))$. □

3 Nominal monoids

This section revisits the four different notions of nominal words from a more abstract point of view and presents corresponding notions of nominal monoids. To carry this out in an elegant way, we make use of the nominal algebra of Gabbay [1] and Gabbay and Mathijssen [3]. The different classes of nominal words from

Section 2 will appear now as explicit descriptions of free algebras of the corresponding classes of nominal monoids.

Definition 18 (Nominal monoid) *A tuple* $\mathfrak{A} = \langle A, \circ, [\_]\_, e\rangle$ *is a* nominal monoid *over* $\mathcal{N} \cup \mathcal{S}$, *if* $\mathcal{N} \cup \mathcal{S} \cup \{e\} \subseteq A$, *A is a nominal set,* $\circ$ *a binary equivariant,* $[\_]\_$ *atom-abstraction [2, 1, 3] and it satisfies*

1. $\vdash X \circ (Y \circ Z) = (X \circ Y) \circ Z$,
2. $\vdash X \circ e = X$,
3. $\vdash e \circ X = X$.

In the definition above, we consider elements of $\mathcal{N}$ and of $\mathcal{S}$ as constants which are part of the signature. In other words, a nominal monoid is an algebra, for the functor on nominal sets

$$A \mapsto 1 + \mathcal{S} + \mathcal{N} + A \times A + [\mathcal{N}]A,$$

satisfying conditions 1, 2, and 3. Our aim is to exhibit $\mathcal{P}_\sim$, $\mathcal{G}_\sim$, $\mathcal{L}_\sim$ and $\mathcal{F}_\sim$ as initial monoids of axiomatically defined classes of nominal monoids.

First, we will prove that $\mathcal{P}_\sim$, $\mathcal{G}_\sim$, $\mathcal{L}_\sim$ and $\mathcal{F}_\sim$ are all nominal monoids. When we reason about $\mathcal{L}_\sim$ and $\mathcal{F}_\sim$, since they do not include $\mathcal{N} \cup \mathcal{S} \cup \{e\}$ syntactically, it is necessary to identify every element in $\mathcal{N} \cup \mathcal{S} \cup \{e\}$ with an element in $\mathcal{L}_\sim$ and $\mathcal{F}_\sim$. In $\mathcal{L}_\sim$, we identify e, each $n \in \mathcal{N}$ and each $s \in \mathcal{S}$ with $(\varepsilon, \varepsilon)$, (ε, n) and (ε, s), and, in $\mathcal{F}_\sim$, with $(\emptyset, \varepsilon)$, $(\emptyset, n)$ and $(\emptyset, s)$, respectively.

Theorem 19 *$\mathcal{G}_\sim$, $\mathcal{L}_\sim$, $\mathcal{F}_\sim$ and $\mathcal{P}_\sim$ are all nominal monoids. Furthermore, $\mathcal{P}_\sim$ is the initial nominal monoid.*

Proof We check only that $\mathcal{G}_\sim$ is a nominal monoid and $\mathcal{P}_\sim$ is the initial one.

Firstly we identify $n\varepsilon$, $s\varepsilon$ and ε with n, s and e, respectively. Then, $\mathcal{N} \cup \mathcal{S} \cup \{e\} \subseteq \mathcal{G}_\sim$.

1. For all $w, v, u \in \mathcal{G}_\sim$,
   (a) If $w = \varepsilon$, then $\varepsilon \circ (v \circ u) = v \circ u$ and $(\varepsilon \circ v) \circ u = v \circ u$.
   (b) Suppose that $w \circ (v \circ u) = (w \circ v) \circ u$.
      i. $nw \circ (v \circ u) = n(w \circ (v \circ u))$ by definition. Hence, by assumption, we have $n(w \circ (v \circ u)) = n((w \circ v) \circ u)$. On the other hand, by definition, $(nw \circ v) \circ u = (n(w \circ v)) \circ u = n((w \circ v) \circ u)$.
      ii. As in Item (i), we have $sw \circ (v \circ u) = (sw \circ v) \circ u$.
      iii. Let n' be fresh for both v and $v \circ u$. Now, $\langle n.w\rangle \circ (v \circ u) = \langle n'.w' \circ (v \circ u)\rangle$, where $\langle n.w\rangle \sim \langle n'.w'\rangle$. By assumption, we have $\langle n'.w' \circ (v \circ u)\rangle = \langle n'.(w' \circ v) \circ u\rangle$. Conversely, $(\langle n.w\rangle \circ v) \circ u = \langle n'.w' \circ v\rangle \circ u$, where $\langle n'.w'\rangle$ is the same with the previous one. Then, we have $\langle n'.w' \circ v\rangle \circ u = \langle n'.(w' \circ v) \circ u\rangle$.

   Therefore, by induction on w, associativity holds.

2. By definition, we have $\varepsilon \circ \varepsilon = \varepsilon$. Assume that $w \circ \varepsilon = w$.
   (a) $nw \circ \varepsilon = n(w \circ \varepsilon) = nw$ for each $n \in \mathcal{N}$.
   (b) $sw \circ \varepsilon = s(w \circ \varepsilon) = sw$ for each $s \in \mathcal{S}$.
   (c) $\langle n.w\rangle \circ \varepsilon = \langle n.w \circ \varepsilon\rangle = \langle n.w\rangle$.

3. $\vdash e \circ X = X$ is analogous.

Next, we check the initiality of $\mathcal{P}_\sim$. Let $\mathcal{A} = \langle A, \circ, [\_]\_, e\rangle$ be any nominal monoid. Then, we inductively define a function $f : \mathcal{P}_\sim \to A$ as follows:

1. $f(\varepsilon) \stackrel{\text{def}}{=} e$,
2. $f(n) \stackrel{\text{def}}{=} n$ for each $n \in \mathcal{N}$,
3. $f(s) \stackrel{\text{def}}{=} s$ for each $s \in \mathcal{S}$,
4. $f(w \circ v) \stackrel{\text{def}}{=} f(w) \circ f(v)$ for all $w, v \in \mathcal{G}_\sim$,
5. $f(\langle n.w\rangle) \stackrel{\text{def}}{=} [n]f(w)$.

We check that f is an equivariant. Namely, for each $\pi \in \mathit{Perm}(\mathcal{N})$ and each $w \in \mathcal{P}_\sim$, $\pi \cdot f(w) = f(\pi \cdot w)$. Induction on w.

1. $\pi \cdot f(\varepsilon) = \pi(\varepsilon) = \varepsilon$ and $f(\pi(\varepsilon)) = f(\varepsilon) = \varepsilon$.
2. $\pi \cdot f(n) = \pi(n)$. On the other hand, since $\pi(n)$ is also in $\mathcal{N}$, $f(\pi(n)) = \pi(n)$.
3. $\pi \cdot f(s) = \pi(s) = s$ and $f(\pi(s)) = f(s) = s$.
4. $\pi \cdot f(w \circ v) = \pi \cdot (f(w) \circ f(v))$. Since $\circ$ is an equivariant on A, we have $\pi \cdot (f(w) \circ f(v)) = (\pi \cdot f(w)) \circ (\pi \cdot f(v))$. By the induction hypothesis, the left hand side is $f(\pi(w)) \circ f(\pi(v))$. On the other hand, $f(\pi \circ (w \circ v)) = f(\pi(w) \circ \pi(v))$, because $\circ$ is an equivariant on $\mathcal{P}_\sim$. Then, by definition, the right hand side is also $f(\pi(w)) \circ f(\pi(v))$.
5. $\pi \cdot f(\langle n.w\rangle) = \pi \cdot [n]f(w)$, by definition. Since $[\_]\_$ is an equivariant on A, we have $[\pi(n)]f(\pi(w))$. On the other hand, $f(\pi \cdot \langle n.w\rangle) = f(\langle \pi(n).\pi(w)\rangle) = [\pi(n)]f(\pi(w))$ by definition.

By definition, f is a homomorphism, and it is the unique one. □

Definition 20 *Let $\mathcal{C}_{ng}$ be the subclass of nominal monoids satisfying $n\#Y \vdash [n]X \circ Y = [n](X \circ Y)$.*

Theorem 21 *$\mathcal{G}_\sim, \mathcal{L}_\sim$ and $\mathcal{T}_\sim$ are in $\mathcal{C}_{ng}$, and $\mathcal{G}_\sim$ is initial.*

Proof Here we only check that $\mathcal{G}_\sim$ is in $\mathcal{C}_{ng}$ and the initiality. For each $n \in \mathcal{N}$ and all $w, v \in \mathcal{G}_\sim$, if n is not in $\mathit{supp}(v)$, then $[n]w \circ v = \langle n.w\rangle \circ v$. By definition, we have $\langle n.w \circ v\rangle$. On the other hand, $[n](w \circ v) = \langle n.w \circ v\rangle$, hence $n\#v \vdash [n]w \circ v = [n](w \circ v)$.

For the initiality, we define a function $f : \mathcal{G}_\sim \to A$ as follows:

1. $f(\varepsilon) \stackrel{\text{def}}{=} e$,
2. $f(nw) \stackrel{\text{def}}{=} n \circ f(w)$,
3. $f(sw) \stackrel{\text{def}}{=} s \circ f(w)$,
4. $f(\langle n.w\rangle) \stackrel{\text{def}}{=} [n]f(w)$.

To prove that f preserves $\circ$, we use induction on the first argument:

1. $f(\varepsilon \circ v) = f(v)$ by definition. On the other hand, $f(\varepsilon) \circ f(v) = e \circ f(v)$. Since e is the unit element, we obtain $f(v)$.

2. $f(nw \circ v) = f(n(w \circ v)) = n \circ f(w \circ v)$, by definition. By induction hypothesis, we have $n \circ (f(w) \circ f(v))$. On the other hand, $f(nw) \circ f(v) = (n \circ f(w)) \circ f(v)$. By associativity, we have $n \circ (f(w) \circ f(v))$.

3. This is analogous to Item 2.

4. Let n be fresh for v. By definition, we have $f(\langle n.w \rangle \circ v) = f(\langle n.w \circ v \rangle) = [n]f(w \circ v)$. On the other hand, $f(\langle n.w \rangle) \circ f(v) = [n]f(w) \circ f(v)$. Finally, we prove that n is also fresh for $f(v)$ by induction on v:

   (a) $f(\varepsilon) = e$, hence $n\#f(\varepsilon)$.

   (b) If $n\#mv$, then $n \neq m$ and $n\#v$. By induction hypothesis, we obtain that $n\#f(v)$. Therefore, $n\#m \circ f(v) (= f(mv))$.

   (c) This is analogous to Item 2.

   (d) Assume that $n \neq m$. If $n\#\langle m.v \rangle$, we have $n\#v$. By induction hypothesis, n is fresh for $f(v)$. So, $n\#f(\langle m.v \rangle))$.

   Now we use the axiom $n\#f(v) \vdash [n]f(w) \circ f(v) = [n](f(w) \circ f(v))$.

It is routine to check that f is equivariant and the unique homomorphism. $\square$

Definition 22 *Let $\mathcal{C}_l$ be the subclass of $\mathcal{C}_{ng}$ satisfying the following axiom:*

$$m\#X \vdash X \circ [m]Y = [m](X \circ Y).$$

Theorem 23 *$\mathcal{L}_\sim$ and $\mathcal{F}_\sim$ are in $\mathcal{C}_l$, and $\mathcal{L}_\sim$ is initial in $\mathcal{C}_l$.*

Proof We prove only that $\mathcal{L}_\sim$ is in $\mathcal{C}_l$ as the initial algebra. For all $n, m \in \mathcal{N} (n \neq m)$ and each (p, w), let n be fresh for (p, w). The left hand side is $(\varepsilon, n) \circ [m](p, w) = (\varepsilon, n) \circ (mp, w) = (mp, nw)$. On the other hand, $[m]((\varepsilon, n) \circ (p, w)) = [m](p, nw) = (mp, nw)$. This is analogous to $\vdash (\varepsilon, s) \circ [m](p, w) = [m]((\varepsilon, s) \circ (p, w))$.

For the initiality, we define a function $f : \mathcal{L}_\sim \to A$ as follows: we let $f(n_1 \cdots n_k, w) \stackrel{\text{def}}{=} [n_1] \cdots [n_k]w$, for each $(n_1 \cdots n_k, w) \in \mathcal{L}_\sim$. Firstly, we check that f is homomorphic. The only case we should investigate is that $f((p, w) \circ (q, v)) = f(p, w) \circ (q, v)$. Let p be $n_1 \cdots n_k$, $q = m_1, \ldots, m_l$, p and q share no name, p is fresh for v and q is fresh for w. Namely, $[n_1] \cdots [n_k][m_1] \cdots [m_l]wv = [n_1] \cdots [n_k]w \circ [m_1] \cdots [m_l]v$. We separate this into the following two arguments:

1. $[n_1] \cdots [n_k]w \circ [m_1] \cdots [m_l]v = [n_1] \cdots [n_k](w \circ [m_1] \cdots [m_l]v)$,

2. $w \circ [m_1] \cdots [m_l]v = [m_1] \cdots [m_l](w \circ v)$.

Iterating the axiom $n\#Y \vdash [n]X \circ Y = [n](X \circ Y)$, we obtain Item 1. For Item 2, we use the induction on w. Note that $w \in (\mathcal{N} \cup \mathcal{S})^*$

1. $\varepsilon \circ [m_1] \cdots [m_l]v = [m_1] \cdots [m_l]v$ and $[m_1] \cdots [m_l](\varepsilon \circ v) = [m_1] \cdots [m_l]v$.

2. Recall that n is fresh for $[m_1]\cdots[m_l]v$. Repeating the axiom $m\#n \vdash n \circ [m]Y = [m](n \circ Y)$, we get $n \circ [m_1]\cdots[m_l]v = [m_1]\cdots[m_l](n \circ v)$.

3. This is analogous to Item 2.

4. Let $o \in \mathcal{N} \cup \mathcal{S}$. $o \circ w \circ [m_1]\cdots[m_l]v = o \circ [m_1]\cdots[m_l](w \circ v)$, by induction hypothesis. By Item 2 or 3, we have $[m_1]\cdots[m_l](o \circ w \circ v)$.

It is routine to check that f is equivariant and the unique homomorphism. □

Definition 24 *Let C_f be the subclass of C_l in which every nominal monoid satisfies:*

1. $\vdash [n][m]X = [m][n]X$,
2. $n\#X \vdash [n]X = X$.

Theorem 25 *$\mathcal{F}_\sim$ is initial in C_f.*

Proof For all $n, m \in \mathcal{N}$ and each $(S,w) \in \mathcal{F}_\sim$, if $m\#(S,w)$ and $n\#(S,w)$, then we have $[n][m](S,w) = (S,w) = [m][n](S,w)$, else if $n\#(S,w)$ and $m \in supp(S,w)$, then $[n][m](S,w) = (S \cup \{m\}, w) = [m][n](S,w)$, and else, namely if $n, m \in supp(S,w)$, then we have $[n][m](S,w) = (S \cup \{n,m\}, w) = [m][n](S,w)$, hence $\vdash [n][m]X = [m][n]X$.

Let $n \in \mathcal{N}$, $(S,w) \in \mathcal{F}_\sim$ and $n\#(S,w)$. Then $[n](S,w) = (S,w)$. So, we have $n\#X \vdash [n]X = X$.

For the initiality of $\mathcal{F}_\sim$, we define a function $f : \mathcal{F}_\sim \to A$ as follows: for each f-word $(S,w) \in \mathcal{F}_\sim$, we let $f(S,w) \stackrel{\text{def}}{=} [n_1]\cdots[n_k]w$, where $S = \{n_1,\ldots,n_k\}$. Due to the axiom $\vdash [n][m]X = [m][n]X$, we have that f is independent of the order of elements in S and f is well-defined. It is also straightforward that f is equivariant and unique.

Here, we prove that f is homomorphic. The important parts are $\circ$ and $[\_]\_$ The following diagrams commute.

$$\begin{array}{ccc} \mathcal{F}_\sim \times \mathcal{F}_\sim & \xrightarrow{f^2} & A \times A \\ {\scriptstyle\circ}\downarrow & & \downarrow{\scriptstyle\circ} \\ \mathcal{F}_\sim & \xrightarrow{f} & A \end{array} \qquad \begin{array}{ccc} [\mathcal{N}]\mathcal{F}_\sim & \xrightarrow{[id]f} & [\mathcal{N}]A \\ {\scriptstyle[\_]\_}\downarrow & & \downarrow{\scriptstyle[\_]\_} \\ \mathcal{F}_\sim & \xrightarrow{f} & A \end{array}$$

For all $(S,w),(T,v) \in \mathcal{F}_\sim$, let $S \cap T = S \cap supp(T,v) = T \cap supp(S,w) = \emptyset$ by the Renaming Lemma, and let $S = \{n_1,\ldots,n_k\}$ and $T = \{m_1,\ldots,m_l\}$.

$$f((S,w) \circ (T,v)) = f(S \cup T, wv) = [n_1]\cdots[n_k][m_1]\cdots[m_l]wv,$$

$$f(S,w) \circ f(T,v) = [n_1]\cdots[n_k]w \circ [m_1]\cdots[m_l]v.$$

By the axioms $n\#Y \vdash [n]X \circ Y = [n](X \circ Y)$, $m\#n \vdash n \circ [m]Y = [m](n \circ Y)$ and $\vdash s \circ [m]Y = [m](s \circ Y)$, we conclude $f(S,w) \circ f(T,v) = [n_1]\cdots[n_k][m_1]\cdots[m_l]wv$. Therefore, $f((S,w) \circ (T,v)) = f(S,w) \circ f(T,v)$. For each $n \in \mathcal{N}$ and each $(S,w) \in \mathcal{F}_\sim$ where $S = \{n_1,\ldots,n_k\}$, if n is fresh for (S,w), which means either $n \in S$ or n does not occur in w, we have $f([n](S,w)) = f(S,w) = [n_1]\cdots[n_k]w$. Conversely, $[n]f(S,w) = [n][n_1]\cdots[n_k]w$. Since n is fresh for (S,w), $n\#[n_1]\cdots[n_k]w$ holds. By the axiom $n\#X \vdash [n]X = X$, we have $[n_1]\cdots[n_k]w$.

Otherwise, if $n \in supp(S,w)$, then $f([n](S,w)) = f(S \cup \{n\}, w) = [n][n_1]\cdots[n_k]w$. Conversely, $[n]f(S,w) = [n][n_1]\cdots[n_k]w$. Therefore, $f([n](S,w)) = [n]f(S,w)$. □

4 Summary

We investigated the following classes of nominal monoids.

Class of monoids	axioms	initial monoid	typical example
C		$\mathcal{P}_\sim$	$[n_1](s_1 n_1 n_4)[n_0](n_0[n_3]s_2)$
C_{ng}	$n\#Y \vdash ([n]X) \circ Y = [n](X \circ Y)$	$\mathcal{G}_\sim$	$[n_1](s_1 n_1 n_4[n_0](n_0[n_3]s_2))$
C_l	C_{ng} plus $n\#X \vdash X \circ [n]Y = [n](X \circ Y)$	$\mathcal{L}_\sim$	$[n_1][n_0][n_3]s_1 n_1 n_4 n_0 s_2$
C_f	C_l plus $\vdash [n][m]X = [m][n]X$ $n\#X \vdash [n]X = X$	$\mathcal{F}_\sim$	$[n_0][n_1]s_1 n_1 n_4 n_0 s_2$

We assume that all monoids contain an infinite countable supply of names $n \in \mathcal{N}$ and a finite supply of letters $s \in S$. Elements of monoids are called words. In addition to the usual operations of neutral element and concatenation, we also have permutations of names acting on words and the operation $[n]w$ binding a name n in a word w. The elements of the monoids are taken up to α-equivalence $\sim$. In particular, $[n]n = [m]m$.

C is the class of monoids just given by the classical laws of monoids, permutation actions, and α-equivalence. Since binding introduces scope and concatenation, words have a tree rather than a linear structure.

C_{ng} is given by an axiom saying that the scope of a binder extends as far to the right as possible (intuitively: resources are never deallocated). Consequently, words have their usual linear structure again.

C_l has an additional axiom stating that binders can be moved two the left (intuitively: the (absolute) time of allocation of a resource does not matter). Consequently, words can be represented by a prefix of binders and a classical word without binders.

If we read $\circ$ as the parallel composition of π-calculus processes the axiom of C_l describes scope-extrusion.

C_f contains two further axioms expressing that the order of the binders does not matter and that 'non-binding binders' can be removed.

References

[1] M. Gabbay. Nominal algebra and the HSP theorem. *J. Logic Computation*, 2008. doi:10.1093/logcom/exn055.

[2] M. Gabbay and A. Pitts. A new approach to abstract syntax involving binders. In *LICS'99*.

[3] M. J. Gabbay and A. Mathijssen. Nominal (universal) algebra: equational logic with names and binding. *J. Logic Computation*, 19(6):1455–1508, 2009.