Control Structures III : Arity monoids and their associated naming monoids[1]

John Power
Edinburgh, August 1994

D R A F T August 94. Comments are welcome.

1 The internal language of a monoid

1.1 Definition (Subbasis) A *subbasis* for a monoid M consists of a subset S of M for which $S^{\wedge} - 1$ forms a basis for M, *i.e.*, every element of M is a tensor product of subnames of elements of S.

Given any monoid M together with a subbasis S, we will construct a monoid $Int(M)$ and a monoid morphism $ar : Int(M) \longrightarrow M$ inductively. $Int(M)$ is called the *internal language* of the monoid M as it is essentially the internal language of the free category with strictly associative finite products on the monoid M, in the same way that the simply typed λ-calculus is the internal language of a cartesian closed category: it is precisely the internal language of the associated category if $S = M - 1$, and is equivalent if M has a countable basis.

1.2 Definition (Internal language of a monoid) $Int(M)$ and ar are generated from a set by some operations, subject to equations, as follows: writing $t : m$ for $ar(t) = m$,

- for each $m \epsilon S$, start with an countable set X_m, each element of which is sent by ar to m
- given $t : m$ and $s : n$, add an element $t \otimes s : mn$
- add an element $e : 1$
- given $m, n \epsilon M$ and $t : mn$, add elements $t_0^{m,n} : m$ and $t_1^{m,n} : n$

subject to the following equations:

- for every t, $t \otimes e = t = e \otimes t$
- for every r, s, t, $(r \otimes s) \otimes t = r \otimes (s \otimes t)$
- if $t : 1$, then $t = e$
- for every $s : m$ and $t : n$, $(s \otimes t)_0^{m,n} = s$ and $(s \otimes t)_1^{m,n} = t$
- for every $t : mn$, $t = t_0^{m,n} \otimes t_1^{m,n}$.

The first two equations ensure that $Int(M)$ is a monoid, and the description of ar ensures that it is a monoid map.

[1]Some terminology and results come from *Control Structures II: Naming monoids* by Robin Milner.

1.3 Lemma If $t : mn$, there exist unique $r : m$ and $s : n$ such that $t = r \otimes s$.

Proof If $t = r \otimes s$, then $r = (r \otimes s)_0^{m,n} = t_0^{m,n}$ and $s = (r \otimes s)_1^{m,n} = t_1^{m,n}$. ■

It is evident that the statement of Lemma 1.3 is equivalent to demanding the presence of the operations $(\ )_0$ and $(\ )_1$ subject to the final two equations of Definition 1.2.

1.4 Lemma If $t : mnp$, then

1. $(t_0^{mn,p})_0^{m,n} = t_0^{m,np}$
2. $(t_0^{mn,p})_1^{m,n} = (t_1^{m,np})_0^{n,p}$
3. $(t_1^{m,np})_1^{n,p} = t_1^{mn,p}$.

Proof It suffices to prove 1 and 2 since 3 follows from 1 by duality: replacing M by its opposite everywhere. To see 1, suppose $t = (q \otimes r) \otimes s$. By 1.3 applied twice, t is uniquely expressible thus. By construction, $(t_0^{mn,p})_0^{m,n} = q$. But $(q \otimes r) \otimes s = q \otimes (r \otimes s)$, and t is also uniquely expressible in that form, again by 1.3. So $t_0^{m,np} = q$ and we are done. For 2, apply the same argument with q replaced by r. ■

We will see later as a result of Lemma 1.4 that if M is confluent (defined by Robin) and weakly left cancellative (to be defined), we can give an explicit description of the elements of $Int(M)$. But for now, we restrict ourselves to the following observation. Given $m, n, p \epsilon M$ and $t : mnp$, let $t^{m,n,p}$ denote the common value of $(t_0^{mn,p})_1^{m,n}$ and $(t_1^{m,np})_0^{n,p}$. Observe that for any refinement of (m, n, p) and any sequence of applications of $(\ )_0$ and $(\ )_1$ via the refinement leading to that copy of n, it follows from Lemma 1.4 and induction that t together with the corresponding decoration equals $t^{m,n,p}$.

2 Coherence

2.1 Lemma (See also Robin's Proposition 2.5) If M is confluent, and if $mn = 1$, then $m = n = 1$.

Proof The composite of the unique vector of length 0 is 1. Moreover, the only refinement of the empty vector is the empty vector. ■.

2.2 Proposition Let $h : N \longrightarrow M$ be a monoid morphism such that

1. $h(x) = 1 \Longrightarrow x = 1$
2. $h(x) = mn \Longrightarrow$ there exist unique y, z with $x = y \otimes z$, $h(y) = m$ and $h(z) = n$.

Then if M is confluent, so is N.

Proof Let $\vec{x} = (x_1, \ldots, x_r)$ and $\vec{y} = (y_1, \ldots, y_s)$ be two vectors of elements of N with the same composite. So $h(x_1) \ldots h(x_r) = h(y_1) \ldots h(y_s)$. Since M is confluent, there exists a common refinement $w_1 \ldots w_k$. Applying 1 and 2 plus induction, the $x_i's$ and $y_j's$ refine according to $\vec{w}$, and by the unicity part of 1 and 2, these two refinements of $x_1 \ldots x_r = y_1 \ldots y_s$ must agree. ■.

2.3 Corollary If M is confluent, so is $Int(M)$.

Proof Condition 1 of Proposition 2.2 is an equation for $Int(M)$; condition 2 is Lemma 1.3.

3 Separation

Recall that in Robin's Proposition 2.9, it was shown that # is redundant for any naming. Here, we will not assert that we have a naming, but for an arbitrary monoid M, we will define # by $x\#y$ if and only if the only subname of both x and y is 1. We say x is *disjoint* from y whenever $x\#y$. We shall show that if M is confluent, $(M, \#)$ is an s-monoid.

Trivially, we have

3.1 Fact If $x\#x$, then $x = 1$.

3.2 Lemma If M is confluent, then for all x, $x\#1$.

Proof Suppose $w \leq x$ and $w \leq 1$. Then, there exist y and z with $ywz = 1$. By two applications of Lemma 2.1, $w = 1$. ■.

3.3 Lemma If $x\#yz$, then $x\#y$ and $x\#z$.

Proof Let $w \leq x$ and $w \leq y$. Then $w \leq yz$. So by hypothesis, $w = 1$. By duality, we are done. ■.

3.4 Lemma Suppose that whenever $w \leq yz$, there exist $w_1 \leq y$ and $w_2 \leq z$ with $w = w_1 w_2$. Then, whenever $x\#y$ and $x\#z$, it follows that $x\#yz$.

Proof Suppose $w \leq x$ and $w \leq yz$. Applying the hypothesis, we have $w_1 \leq x$ and $w_1 \leq y$, so $w_1 = 1$ and dually $w_2 = 1$. Hence $w = 1$. ■.

3.5 Lemma Suppose M is confluent. Then, whenever $w \leq yz$, there exist $w_1 \leq y$ and $w_2 \leq z$ with $w = w_1 w_2$.

Proof If $w \leq yz$, there exist u and v with $uwv = yz$. Now apply confluence to obtain a common refinement $x_1 \dots x_n$. It is routine combinatorics to describe w_1 and w_2.
■.

3.6 Proposition If M is confluent, then

1. $x\#x \Longrightarrow x = 1$.
2. for all x, $x\#1$
3. $x\#yz \Longleftrightarrow x\#y$ and $x\#z$.

Proof This follows trivially from Fact 3.1 and Lemmas 3.2-3.5. ■

In other words, if M is confluent, which it is in all cases of interest to us, and if # is defined as at the start of the section, $(M, \#)$ is an s-monoid.

4 Honesty

Call a monoid M *weakly left cancellative* if $mn = m$ implies $n = 1$. Call it *left cancellative* if $mn = mp$ implies $n = p$.

4.1 Lemma If a confluent monoid M is weakly left cancellative, it is left cancellative.

Proof Let $mn = mp$. It follows from the definition of confluence that there exists q with $m = mq$ and either $n = qp$ or $p = qn$. By weak left cancellation, $q = 1$, so we have the result. ■.

4.2 Lemma Let $h : N \longrightarrow M$ satisfy the condition $h(x) = 1 \Longrightarrow x = 1$, *i.e.*, Condition 1 of Proposition 2.2. Then, if M is weakly left cancellative, so is N.

Proof If $xy = x$, $h(x)h(y) = h(x)$. So $h(y) = 1$. So $y = 1$. ■.

4.3 Lemma Given $s : m$, $t : n$, $s' : m$ and $t' : n$ in $Int(M)$, if $s \otimes t = s' \otimes t'$, then $s = s'$ and $t = t'$.

Proof $s = (s \otimes t)_0^{m,n} = (s' \otimes t')_0^{m,n} = s'$, and dually. ■.

This result leads one to some caution, as we have

4.4 Proposition There exists a confluent monoid M with $x \epsilon X_m$, $y \epsilon X_n$ and $x \otimes y = x$.

Proof Let M be freely generated on three elements m, n, and p, subject to $mn = m$ and $np = p$. Let $x : m$, $y : n$ and $z : p$. Then apply Lemma 4.3 to $(x \otimes y) \otimes z = x \otimes (y \otimes z)$ to see that $x = x \otimes y$. ■.

It follows that confluence of M is not enough to conclude that $Int(M)$ is honest (see Robin's Definition 2.7). However, if we also assert weak left cancellation of M, we can conclude that $Int(M)$ is honest and hence a naming. The way to prove that is by giving an explicit description of the elements of $Int(M)$, as promised at the end of Section 2. From that, one can see immediately that $Int(M)$ has a sharp basis and satisfies H_E^2; we already know it is confluent by Corollary 2.3: hence, by Robin's Proposition 3.9, it is a sharp elementary naming (again see Robin's definitions).

Using the notation established at the end of Section 2,

4.5 Theorem Every element of $Int(M)$ is uniquely expressible as a tensor product of elements of the form $x^{m,n,p}$ $(n \neq 1)$, such that if $x^{m,n,p}$ is immediately followed in the tensor product by $y^{m',n',p'}$, and if $x = y$, then one does not have $mn = m'$. ■.

In order to prove the theorem, we need some notation.

4.6 Notation Let M be confluent and weakly left cancellative. We inductively define, for any term t of $Int(M)$, another term $\bar{t}$ that is equal to it and is of the form a tensor product of terms of the form $x^{m,n,p}$, as follows:

1. if $t \equiv e$, let $\bar{t}$ be the empty tensor
2. if $t \equiv x$ of arity m, let $\bar{t}$ be $x^{1,m,1}$

3. given $\bar{s}$ and $\bar{t}$, let $s \mathbin{\bar{\otimes}} t$ be $\bar{s} \otimes \bar{t}$

4. if $t \equiv s_0^{m,n}$ and given $\bar{s}$, choose a common refinement of (m, n) and the sequence $i_1, \ldots, i_k$ of middle supercripts of the atomic subterms of $\bar{s}$, with no i_j equal 1. That refinement determines an initial sequence of $i_1, \ldots, i_k$ together with a division of the next. Take $\bar{t}$ to be given by the corresponding refinement of $\bar{s}$. Dually for $t \equiv s_1^{m,n}$.

Observe that since M and hence $Int(M)$ is weakly left cancellative, Notation 4.6 is well defined.

4.7 Definition Given confluent and weakly left cancellative M, the *standard interpretation* of a term t, denoted $[t]$, is given from $\bar{t}$ by deleting every element of the form $x^{m,1,p}$, and then replacing any adjacent pair of the form $x^{m,n,p}$,$x^{m',n',p'}$ with $mn = m'$ by $x^{m,nn',p'}$ until no such pair is left.

Observe that it follows from weak left cancellation of M that if $mn = m'$, then $p = n'p$.

Now we can prove Theorem 4.5.

4.8 Proof of Theorem 4.5 For any term t of $Int(M)$, it follows from the construction of the standard interpretation that $t = [t]$ and that $[t]$ is in the desired form. Moreover, it is trivially true that for terms s and t, if $[s] \equiv [t]$, then $s = t$. It remains to show that if $s = t$, then $[s] \equiv [t]$. But that follows immediately because applying any axiom to any $[t]$, then taking the standard interpretation, yields identically $[t]$. ■.

Theorem 4.5 may be reformulated to say that the set of $[t]$'s together with the evident operations forms a sound and complete model of the equational theory of $Int(M)$.

4.9 Corollary If M is confluent and weakly left cancellative, then

1. if $x \epsilon X_m$ and $y \epsilon X_n$ with $x \neq y$, then $x \# y$

2. if $x \epsilon X_m$, x is sharp.

Proof Theorem 4.5 gives an explicit description of the elements of $Int(M)$. One can see by inspection that $[s] \leq [t]$ if and only if $[s]$ is given by refining the middle superscripts of the sequence of atomic elements of $[t]$, then restricting to a contiguous subsequence of the induced refinement of $[t]$. Both our claims now follow immediately from the definitions. ■.

4.10 Corollary $Int(M)$ is a sharp elementary naming.

Proof The collection of X_m's for m in the subbasis of M trivially forms a subbasis for $Int(M)$. It follows from Corollary 4.9 that the induced basis is sharp. Condition H_E^2 follows from confluence and Corollary 4.9. By Corollary 2.3, $Int(M)$ is confluent.
■.

5 Characterizing the internal language

Given a confluent, weakly left cancellative monoid M, in this section we axiomatize $Int(M)$. More precisely, we give conditions on a monoid X and a monoid morphism $h : X \longrightarrow M$ such that X is isomorphic to $Int(M)$ and h and ar agree modulo that isomorphism.

5.1 Definition A subbasis S for a monoid M is *sharp* if

- every element of S is sharp, and
- if b and b' are distinct elements of S, then $b\#b'$.

Observe that Corollary 4.9 shows that for confluent weakly left cancellative M, the collection of X_m's forms a sharp subbasis for $Int(M)$. It is easy to verify

5.2 Proposition If a confluent monoid M has a sharp subbasis S, then the induced basis exhibits M as a sharp elementary naming. ■.

5.3 Theorem Let M be weakly left cancellative with subbasis S, let X be a confluent monoid with sharp subbasis B, and let $h : X \longrightarrow M$ be a monoid morphism such that

- h maps B into S and for each $m \epsilon S$, there is a countable set of elements of B mapping to it
- if $h(x) = mn$, there exist unique y and z with $h(y) = m$, $h(z) = n$ and $x = yz$.

Then there is an isomorphism of monoids $k : Int(M) \longrightarrow X$ commuting with ar and h.

Proof First observe that since X is confluent, so is M, since each element of M is the image of some element of X and our second condition shows that decomposition in M is mimicked in X. So M is both confluent and weakly left cancellative, so we have all our results about $Int(M)$ of previous sections. To define k, first define it on the collection of X_m's by use of the first condition and counting. This determines k completely by the second condition and since $t_0^{m,n}$ and $t_1^{m,n}$ are unique of the right arities with composite equal t. By construction, k commutes with ar and h, and it is surjective since B is a subbasis of X. It remains to show that k is injective. By Theorem 4.5, it suffices to show that if $k[s] = k[t]$, then $s = t$. Applying the unicity clause of the second condition to a common refinement of the sequences of middle superscripts of $[s]$ and $[t]$, we are reduced to showing that if $k(x^{m,n,p}) = k(y^{m',n',p'})$, then $x = y$, and the supersrcipts agree. Since k is injective on the subbasis, B is sharp, and $k(x^{m,n,p}) = k(x)^{m,n,p}$, we have $x = y$. Applying sharpness of B again and confluence, we have the superscipts agreeing.
■.

6 Morphisms of arity and naming monoids

The axioms of control structures use both the monoid structure on the set of names directly and also the disjointness relation $\#$. So the maps of control structures should preserve both the monoid structure on the names and $\#$. In this section, we investigate such maps and the way they may arise from a map of monoids between arity monoids.

We consider confluent and weakly left cancellative monoids M and N, a monoid morphism $h : M \longrightarrow N$, and liftings $k : Int(M) \longrightarrow Int(N)$ of h to $Int(M)$, *i.e.*, monoid morphisms k that respect arities.

Recall that $Int(M)$ satisfies the universal property

6.1 Proposition Given any monoid map $j : P \longrightarrow M$ such that

- $j(x) = 1 \Longrightarrow x = 1$
- $j(x) = mn \Longrightarrow$ there exist unique y and z such that $j(y) = m$, $j(z) = n$, and $x = y \otimes z$,

and given a function f from the subbasis of $Int(M)$ to P that commutes with ar and j, f lifts uniquely to a monoid map from $Int(M)$ to P commuting with ar and j.

6.2 Corollary Every lifting k of $h : M \longrightarrow N$ to $Int(M)$ arises uniquely from a function from the subbasis of $Int(M)$ to $Int(N)$ commuting with the two ar's and h.

Proof Take the pullpack P in the category of monoids of ar along h. It is routine to verify that the induced map from P to M satisfies the condition of the theorem. Moreover, this pullback agrees with the pullback in the category of sets of the underlying functions. The result now follows by routine calculation. ■

6.3 Proposition A lifting k of $h : M \longrightarrow N$ preserves # if and only if the restriction of k to its subbasis preserves # and for all x in the subbasis and for all m, n with $x : mn$, $k(x^m, n_0) \# k(x^m, n_1)$.

Proof The forward direction is trivial. For the converse, observe that $k(x^{m,n,p}) = k(x)^{h(m),h(n),h(p)}$ and k is a monoid map. The result now follows routinely from Theorem 4.5 applied to M. ■.

We now consider a natural, mild variant, which we shall show to be a strengthening, of the condition that k preserves #.

6.4 Definition We say $k : Int(M) \longrightarrow Int(N)$ is *sharp* if k sends sharp elements to sharp elements.

Theorem 4.5 tells us what the sharp elements of $Int(M)$ are, so we have

6.5 Corollary If k is sharp, it preserves #.

Proof If x and y are different subbasic elements, then $x \otimes y$ is sharp. Moreover, x is sharp. Now apply Proposition 6.3. ■.

Observe that k being sharp is strictly stronger than preservation of # as one may preserve # without preserving sharpness by sending a prime p to $p \otimes p$. Moreover, it also follows from Theorem 4.5 that we have

6.6 Corollary The map k is sharp if and only if k sends subbasic elements to sharp elements and its restriction to its subbasis preserves $\#$. $\blacksquare$.

We now consider, given $h : M \longrightarrow N$, how to generate a particular canonical sharp $k : Int(M) \longrightarrow Int(N)$. In fact, we require some extra structure to accompany h.

6.7 Definition Given a monoid M with subbasis B, a *presentation* of an element m of M is a list of ordered triples $(m_1, n_1, p_1), \ldots, (m_k, n_k, p_k)$ such that no n_i is 1, $m = n_1 \ldots n_k$, and each $m_i n_i p_i$ is subbasic.

We now suppose M and N countable.

6.8 Notation Given $h : M \longrightarrow N$ and for each subbasic element m of M, a presentation of $h(m)$, define $Int(h) : Int(M) \longrightarrow Int(N)$ as follows: by Corollary 6.2, it suffices to define $Int(h)(x)$ for all subbasic x. If x is subbasic and $x : m$, then m is subbasic in M. Consider the family of all subbasic elements induced by all presentations in N of all images of subbasic m. Each subbasic b in N may occur countably many times. Each such occurrence is determined by a pair (m, i). Call the set of such pairs $Occ(b)$. Take a partition of X_b indexed by $Occ(b)$, with countably many names in each class. Call the classes $X_{(b,m,i)}$. For each relevant b, m, i establish an injection $h_{(b,m,i)} : X_m \longrightarrow X_{(b,m,i)}$. This yields, for each subbasic name in X_m, a unique subbasic name corresponding to the ith component of its image. We define $Int(h)$ accordingly.

This assignment is not functorial in h because we choose injections and because we cannot distinguish at this level between subbasic elements of the same arity. By construction, we have

6.9 Proposition $Int(h)$ is sharp. $\blacksquare$.

We can almost characterize this construction by saying that it gives all sharp liftings of h that satisfy a uniformity principle. That is not quite true as our construction would not allow $x_0^{m,n}$ and $x_1^{m,n}$ to appear in the same term as it separates the two copies of x. However, a mild increase in delicacy to our construction can resolve this, and will be given in a later draft.