Bull. Austral. Math. Soc. 08A70, 06E99, 08C99
Vol. 50 (1994) [81–89]

TOWARDS A CALCULUS OF ALGORITHMS

M. Bulmer, D. Fearnley-Sander and T. Stokes

We develop a generalised polynomial formalism which captures the concept of an algebra of piece-wise defined polynomials. The formalism is based on the Boolean power construction of universal algebra. A generalisation of the theory of substitution homomorphisms is developed. The abstract operation of composition of generalised polynomials in one variable is defined and shown to correspond to function composition.

On one level, a polynomial may be viewed as an algorithm, giving a sequence of operations to be performed on a finite set of elements of an algebra. We consider an extension of this notion which also captures the important algorithmic notion of branching. The emphasis is entirely algebraic, and the role of substitution is as significant as for standard polynomials. We refer the reader to Lausch and Nobauer [**1**] for the background theory of generalised polynomials for single sorted universal algebras. We build on the many sorted case, although the basic concepts are essentially the same. The notion of a many-sorted algebra is a natural generalisation of the notion of a universal algebra, in which more than one carrier set is permitted.

A *signature* Σ is a pair consisting of a set S whose elements are called *sorts*, and a family of sets $\Sigma_{w,\sigma}$ indexed by $w \in S^*$ (the set of strings over S) and $\sigma \in S$. We usually write $f : w \to b$ instead of $f \in \Sigma_{w,\sigma}$.

A *many sorted algebra* A of signature Σ is a map that associates with each $\sigma \in S$ a set A_σ, and with each $f : \sigma_1\sigma_2 \cdots \sigma_n \to \sigma \in \Sigma_{w,\sigma}$ a function $f^A : A_{\sigma_1} \times A_{\sigma_2} \times \cdots \times A_{\sigma_n} \to A_\sigma$. The image ε^A of the empty string is required to be a 1-element set. We say that the A_σ are the *carriers* of A and the f^A are the *operations* on A.

A *variety* of many-sorted algebras of signature Σ is a class of algebras closed under the formation of homomorphic images, subalgebras and products, where each of these notions is the natural analog of the corresponding notion from universal algebra. Alternatively, a variety consists of all the algebras of signature Σ satisfying a collection of identities.

Received 30th September, 1993

1. Boolean affine combinations

Let R be a Boolean ring, that is, a ring with additive identity $\emptyset$ and multiplicative identity 1 in which every $x \in R$ satisfies $x^2 = x$. Let addition be denoted by $+$ and multiplication by juxtaposition. The finite subset $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ of R is a *partition of unity* if

1. $\sum_{i=1}^{k} \alpha_i = 1$; and
2. $\alpha_s \alpha_t = \emptyset$, for all $s \neq t$.

By the Stone Representation Theorem, every Boolean ring R may be interpreted as a ring of subsets of some set S, whence a partition of unity may be viewed as a collection of mutually disjoint subsets of S whose union is all of S.

Let T be a set and R a Boolean ring. Let $\langle M(T,R), \oplus, \cdot \rangle$ be the free R-module with basis T, elements expressed in the form $\sum_{t \in T} \alpha_t t$ with all but finitely many α_t zero. Define T^R, the *set of Boolean affine combinations over R of elements of T*, to be the set of elements $\sum_{t \in T} \alpha_t t$ of $M(T,R)$ such that $\{\alpha_t : t \in T\}$ is a partition of unity. The set T may be viewed as being embedded in T^R by identifying each $t \in T$ with the element $1 \cdot t \in T^R$. Interpreting R as a ring of subsets of the set S leads readily to the interpretation of T^R as the collection of functions $f : S \to T$ with finite image such that the inverse image of each $t \in Im(f)$ is in R.

Proposition 1.1. *Let $p = \sum_{i=1}^{m} \alpha_i t_i \in M(T,R)$, with $t_1, t_2, \ldots, t_m$ not necessarily distinct elements of T. If $\sum_{i=1}^{m} \alpha_i = 1$ and $\alpha_i \alpha_j = \emptyset$ for all $i \neq j$, then $p \in T^R$.*

Proof: Collecting like t_i terms does not affect the sum of the coefficients and pairwise products will still be zero because of distributivity. ∎

There is an important combinatorial rule for making new Boolean affine combinations from old ones.

Proposition 1.2. *Let $p_1, p_2, \ldots, p_k \in M(T,R)$. If $p_1, p_2, \ldots, p_k \in T^R$, and $\{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq R$ is a partition of unity, then $\sum_i \alpha_i p_i \in T^R$.*

Proof: Let $p_i = \sum_j \beta_{ij} t_{ij}$ for each i. Then

$$\sum_i \alpha_i p_i = \sum_i \alpha_i \sum_j \beta_{ij} t_{ij} = \sum_{i,j} \alpha_i \beta_{ij} t_{ij}$$

with
$$\sum_{i,j} \alpha_i \beta_{ij} = \sum_i \alpha_i \sum_j \beta_{ij} = \sum_i \alpha_i \cdot 1 = 1,$$

and
$$\alpha_{i_1} \beta_{i_1 j_1} \alpha_{i_2} \beta_{i_2 j_2} = (\alpha_{i_1} \alpha_{i_2})(\beta_{i_1 j_1} \beta_{i_2 j_2}) = \emptyset$$

https://doi.org/10.1017/S000497270000959X Published online by Cambridge University Press

providing either $i_1 \neq i_2$ or $j_1 \neq j_2$. Hence by Proposition 1.1, $\sum_i \alpha_i p_i \in T^R$. ∎

We call this process *taking the affine combination of the p_i with respect to the α_i*. With the above interpretation of T^R as functions $S \to T$, the affine combination of the p_i with respect to the α_i is the function $S \to T$ obtained by defining a new function piecewise in terms of the p_i — on the domain subset α_i of S, the function agrees with p_i. The above proposition shows that if each of the component functions p_i is in T^R, then so is their affine combination with respect to the partition of unity given by the α_i.

2. Boolean powers

Let A be a many sorted algebra of signature Σ with sorts S, lying in the variety V. Let A^R denote the collection of sets of Boolean affine combinations $\{A^R_\sigma : \sigma \in S\}$. For $n > 0$, each operation $r : A_{\sigma_1} \times A_{\sigma_2} \times \cdots \times A_{\sigma_n} \to A_\sigma$ on A can be extended to an operation $A^R_{\sigma_1} \times A^R_{\sigma_2} \times \cdots \times A^R_{\sigma_n} \to A^R_{\sigma_0}$ on A^R by setting, for each $a_j = \sum_i \alpha_{ij} a_{ij} \in A^R_{\sigma_j}$, where $j = 1, 2, \ldots, n$ (without loss of generality),

$$r\Big(\sum_{i_1} \alpha_{i_1 1} a_{i_1 1}, \sum_{i_2} \alpha_{i_2 2} a_{i_2 2}, \ldots, \sum_{i_n} \alpha_{i_n n} a_{i_n n}\Big) = \sum_{i_1, i_2, \ldots, i_n} \alpha_{i_1 1} \alpha_{i_2 2} \cdots \alpha_{i_n n} r(a_{i_1 1}, a_{i_2 2}, \ldots, a_{i_n n}).$$

If $n = 0$, so that r is a nullary operation on A which chooses a distinguished $a_0 \in A_{\sigma_0}$, let r induce the nullary operation on A^R determined by the distinguished element $a_0 \in A^R_{\sigma_0}$.

If R is interpreted as a ring of sets on S, then A^R may be viewed as being a subalgebra of the many sorted algebra of all many sorted functions $f = (f_\sigma)_{\sigma \in S}$ with $f_\sigma : S \to A_\sigma$ for each carrier A_σ of A under the pointwise operations. Hence A^R is a many sorted algebra of signature Σ in the variety V having carriers the A^R_σ and operations as described above.

We note that if A is simply a semigroup, then A^R is a particular subsemigroup of the multiplicative semigroup of the semigroup ring $R[A]$, so the construction of A^R for general A may be viewed as a generalisation of a construction based on semigroup rings over Boolean rings.

The extension of A to A^R thus defined is nothing but the *Boolean Power of A by R*. Boolean powers are an important tool in universal algebra. See for example Pinus [2], where the Boolean power A^R is defined to be the algebra of continuous functions with pointwise operations from the Stone space of the Boolean ring (strictly, Boolean algebra) R, and taking values in the algebra A endowed with the discrete topology, in the one-sorted case a definition abstractly equivalent to the purely algebraic one given here, as is in essence pointed out in Pinus [2]. The extension to the many sorted case is a straightforward process.

3. Variables

A^R may be viewed as an abstract algebra of "step functions", or piecewise defined constant functions. However, the more general notion of a piecewise defined algebraic function may be captured by linking the structures of A and R. We do this by letting A be an algebra of polynomials in a set of variables X and letting R be a Boolean ring consisting of predicates in the variables X.

Let A be an algebra of signature Σ in a variety V. Let $A[X]$ be the algebra in V freely generated by A and the generators $X_\sigma = \{x_1^\sigma, x_2^\sigma, \dots, x_{m_\sigma}^\sigma\}$ associated with each carrier A_σ of A, and let $X = \{X_\sigma : \sigma \in S\}$. The carrier $A_\sigma[X]$ in $A[X]$ corresponds to A_σ in A for each $\sigma \in S$. Let $N = \{m_\sigma : \sigma \in S\}$ and denote $\Pi_{\sigma \in S} A_\sigma[X]^{m_\sigma}$ by $A[X]^N$; similarly denote $\Pi_{\sigma \in S} A_\sigma^{m_\sigma}$ by A^N.

Let $f(x) = f\big(x_1^\sigma, x_2^\sigma, \dots, x_{m_\sigma}^\sigma : \sigma \in S\big)$ denote a typical element of $A_\sigma[X]$. Each such $f(x)$ induces a function $A[X]^N \to A_{\sigma_0}[X]$ defined by substitution, namely, for $q = \big(q_1^\sigma, q_2^\sigma, \dots, q_{m_\sigma}^\sigma : \sigma \in S\big) \in A[X]^N$ define $f(q) = f\big(q_1^\sigma, q_2^\sigma, \dots, q_{m_\sigma}^\sigma : \sigma \in S\big) \in A_{\sigma_0}[X]$. There is an obvious restriction of $f : A^N \to A_\sigma$.

We note that essentially all of the definitions and constructions in what follows may just as well be made in terms of the important subalgebra of $A[X]$, $F_V[X]$, the free algebra in V on the many sorted variable set X. $A[X]$ may be viewed as a generalisation of the ring of polynomials in several variables over a field, in which each monomial may be multiplied by a field element and each polynomial has a constant term: the structure of A is built into $A[X]$, whereas $F_V[X]$ simply reflects the nature of the variety V. In viewing $f \in A_\sigma[X]$ as a function $A^N \to A_\sigma$, greater generality is obtained by considering $A[X]$ rather than $F_V[X]$, although it is easy to see that the arguments to follow concerning A[X] apply to the smaller algebra $F_V[X]$ also.

Let P be a collection of function symbols of type X, that is, expressions of the form $\rho(x) = \rho\big(x_1^\sigma, x_2^\sigma, \dots, x_{m_\sigma}^\sigma : \sigma \in S\big)$. Then the set of *algebraic predicates*, Pr, consists of all expressions of the form $\psi\big(q_1^\sigma, q_2^\sigma, \dots, q_{m_\sigma}^\sigma : \sigma \in S\big)$ for some $\psi \in P$ and $q_j^\sigma \in A_\sigma[X]$. Such an algebraic predicate is itself an expression in the x_j^σ and will be denoted by $r(x)$. Denote by $r(x)|_{x \mapsto q}$, or $r(q)$ as convenient, the result of the substitution by each q_i^σ in $q = (q_i^\sigma) \in A[X]^N$ for each x_i^σ occurring in $r(x) \in Pr$. Clearly if $r(x) \in Pr$, then $r(q) \in Pr$ also.

Let $\mathcal{B}(Pr)$ denote the free Boolean ring generated by the elements of Pr. Then $A[X, P] = A[X]^{\mathcal{B}(Pr)}$ is the *algebra of potential piecewise polynomials* (the *PPP-algebra*) of type X associated with A and P.

For $f(x) = \sum \alpha_i(x) f_i(x) \in A_\sigma[X]^{\mathcal{B}(Pr)}$ and $q \in A[X]^N$, define $f(q) = \sum \alpha_i(q) f_i(q)$. Note that if $a \in A^N$, $f(a)$ will generally not be an element of A; for that to be the case we need a functional interpretation of the elements of P.

Let P' be a collection of functions $A^N \to \mathbf{Z}_2$ such that there is a bijection $*: P \to P'$. We call $*$ an *instance* of P. We may extend $*$ to all of Pr as follows: for any $\theta(x) = \rho(f) \in Pr$, where $\rho \in P$ and $f \in A[X]^N$, define $\theta^*(x) = \psi^*(f)$ by setting

$$\psi^*\big(f_1^\sigma, f_2^\sigma, \ldots, f_{m_\sigma}^\sigma : \sigma \in S\big)(a) = \psi^*\big(f_1^\sigma(a), f_2^\sigma(a), \ldots, f_{m_\sigma}^\sigma(a) : \sigma \in S\big)$$

for all $q \in A^N$. Notation: $\psi^*(f)(a) = \psi^*(f(a))$. Let Pr' be the collection of all such θ^*.

Let $\mathcal{B}(Pr')$ denote the ring of functions $A^N \to \mathbf{Z}_2$ generated by Pr' under the pointwise operations of addition and multiplication; then $\mathcal{B}(Pr')$ is a Boolean ring. Because $\mathcal{B}(Pr)$ is free, there is a unique homomorphism $\Phi : \mathcal{B}(Pr) \to \mathcal{B}(Pr')$ determined by the bijection $*: Pr \to Pr'$; let $\alpha^* = \Phi(\alpha)$ for all $\alpha \in \mathcal{B}(Pr)$.

The functional view may be taken one step further. Given an instance $*$ of P (and hence of Pr), elements of $A[X]^{\mathcal{B}(Pr)}$ may be associated with functions $A^N \to A_j$ for each j as follows. For $\delta(x) = \sum \alpha_i(x) p_i(x) \in A_j[X]^{\mathcal{B}(Pr)}$, and $a = (a_i) \in A^N$, define $\delta^*(x) = \sum \alpha_i^*(x) p_i(x) \in A_j[X]^{\mathcal{B}(Pr^*)}$, a carrier of $A[X]^{\mathcal{B}(Pr^*)}$. Define $\delta^* : A^N \to A_\sigma$ by setting $\delta^*(a) = \sum \alpha_i^*(a) p_i(a)$, which may be viewed as an element of $A_j^{\mathbf{Z}_2}$, that is, essentially an element of A_j and hence of A.

The reason for the name "potential piecewise polynomial" is now clearer: given an instance $*$ of P and a potential polynomial $\delta(x) \in A[X]^{\mathcal{B}(Pr)}$, the function $\delta^*(x)$ is evaluated at each point by evaluating a multivariate polynomial. The term "potential" signifies the fact that an instance of ρ must be chosen before $\delta(x)$ becomes an abstract piecewise polynomial.

Let $I_* = \{r(x) \in \mathcal{B}(Pr) : r^*(a) = \emptyset \text{ for all } a \in A^N\}$. It is easily seen that $I_* \triangleleft \mathcal{B}(Pr)$, that is, I_* is a ring ideal of $\mathcal{B}(Pr)$.

Proposition 3.1. *I_* is closed under replacements.*

Proof: For any $i \in I_*$, $i^*(a) = \emptyset$ for all $a \in A^N$; hence if $q \in A[X]^N$ then $i(q)^*(a) = i^*(q(a)) = \emptyset$ since $q(a) \in A^N$, whence $i(q) \in I_*$. ∎

We observe that $I_* = Ker(\Phi)$, so $\mathcal{B}(Pr') \cong \mathcal{B}(Pr)/I_*$. Let

$$\gamma : A[X]^{\mathcal{B}(Pr')} \to A[X]^{\mathcal{B}(Pr)/I_*}$$

be the induced canonical isomorphism, with inverse τ.

More generally, let I be any ideal of $\mathcal{B}(Pr)$ which is closed under replacements. Let $R = \mathcal{B}(Pr)/I$. We note that $A[X]^R$ is a homomorphic image of $A[X]^{\mathcal{B}(Pr)}$, via the mapping taking $\Sigma \alpha_i a_i \in A[X]^{\mathcal{B}(Pr)}$ to $\Sigma(\alpha_i + I) a_i \in A[X]^R$; this is a basic property of Boolean powers. (See Pinus [**2**] for the single sorted case.)

THEOREM 3.2. *Let $q \in A[X]$.*

Define $g_q^I : R \to R$ by setting $g_q^I(r(x) + I) = r(q) + I$ for all $r(x) \in \mathcal{B}(Pr)$. Then g_q^I is well defined and is an endomorphism.

Define $h_q^I : A[X]^R \to A[X]^R$ by setting $h_q^I(\Sigma(r_i + I)(x)p_i(x)) = \Sigma(r_i + I)(q)p_i(q)$ for all $\sum r_i(x)p_i(x) \in A[X]^{\mathcal{B}(Pr)}$. Then h_q^I is well defined and is an endomorphism.

PROOF: We begin by showing g_q^I is well defined. Let $r(x) \in \mathcal{B}(Pr)$. Let $r_1(x) \in \mathcal{B}(Pr)$ be an element of the coset $r(x)+I$ with $r_1(x) \neq r(x)$. We must show that $r_1(q)$ is in the coset $r(q)+I$. Suppose $r_1(x) = r(x) + s(x)$, for some $s(x) \in I$. Then $r_1(q) = r(q)+s(q)$. But by assumption, $s(q) \in I$ and so $r_1(q) \in r(q)+I$. Thus g_q^I is well defined. Now $g_q^I((r_1(x) + I) + (r_2(x) + I)) = g_q^I((r_1(x) + r_2(x)) + I) = (r_1(q(x)) + r_2(q(x))) + I = (r_1(q(x)) + I) + (r_2(q(x)) + I) = g_q^I(r_1(x) + I) + g_q^I(r_2(x) + I)$, and similarly $g_q^I((r_1(x) + I)(r_2(x) + I)) = g_q^I(r_1(x) + I)g_q^I(r_2(x) + I)$. Hence g_q^I is an endomorphism.

Next we show that the mapping $h_q^I : A[X]^R \to A[X]^R$ defined by $h_q^I(\Sigma(r_i + I)(x)p_i(x)) = \Sigma(r_i + I)(q)p_i(q)$ is well defined. Let $\Sigma s_i(x)p_i(x)$ be an element of the congruence class $\Sigma(r_i(x) + I)p_i(x)$. As before, we must show that $\Sigma s_i(q)p_i(q)$ is in the congruence class $\Sigma(r_i + I)(q)p_i(q)$. Suppose $\Sigma s_i(x)p_i(x) = \Sigma(r_i(x) + t_i(x))p_i(x)$, for some $t_i \in I$. Then $\Sigma s_i(q)p_i(q) = \Sigma(r_i(q) + t_i(q))p_i(q)$. But by assumption, each $t_i(q) \in I$ and so $\Sigma s_i(q)p_i(q) \in \Sigma(r_i(q) + I)p_i(q)$. Thus h_q^I is well defined.

Finally, we show that h_q^I is an endomorphism. Let $\rho : A_{\sigma_1} \times A_{\sigma_2} \times \cdots \times A_{\sigma_k} \to A_{\sigma_0}$ be a k-ary operation on A and let $\sum_j r_{ij}(x)p_{ij}(x) \in A_{\sigma_i}[X]$ for each i. Then

$$\begin{aligned}
&\rho\Big(\sum_j (r_{1j}(x) + I)p_{1j}(x), \dots, \sum_j (r_{nj}(x) + I)p_{nj}(x)\Big)|_{x\mapsto q} \\
&\quad = \Sigma_{j_1,\dots,j_n}(r_{1,j_1}(x) + I)\cdots(r_{n,j_n}(x) + I)\rho(p_{1,j_1}(x),\dots,p_{n,j_n}(x))\Big|_{x\mapsto q} \\
&\quad = \Sigma_{j_1,\dots,j_n}(r_{1,j_1}(q) + I)\cdots(r_{n,j_n}(q) + I)\rho(p_{1,j_1}(q),\dots,p_{n,j_n}(q)), \\
&\quad = \rho\Big(\sum_j (r_{1j}(q) + I)p_{1j}(q), \dots, \sum_j (r_{nj}(q) + I)p_{nj}(q)\Big)\Big|_{x\mapsto q}
\end{aligned}$$

since substitution is an endomorphism of R as shown above. ∎

Let $I = \{0\}$ in the above theorem; then we may refer to the substitution in any $f(x) \in A[X]^{\mathcal{B}(Pr)}$ of a tuple q of elements of $A[X]$, and we denote such a substitution by $f(q)$.

COROLLARY 3.3. *For $q \in A[X]^N$, define $\theta_q : A[X,P] \to A[X,P]$ by setting $\theta_q(f(x)) = f(q)$. Then θ_q is an endomorphism.*

Corollary 3.4. *Let $*$ be an instance of P. For $f^*(x) \in A[X]^{\mathcal{B}(Pr')}$ and $q \in A[X]^N$, $s_q : A[X]^{\mathcal{B}(Pr')} \to A[X]^{\mathcal{B}(Pr')}$ given by $s_q(f^*(x)) = f^*(q(x))$ is an endomorphism.*

Proof: Let $f^*(x) = \sum_i \alpha_i^*(x)p_i(x)$. Then, with γ and τ defined after the proof of Proposition 3.1 and θ_q as in Corollary 3.3, we have

$$\begin{aligned}(\tau \circ \theta_q \circ \gamma)(f^*(x)) &= \tau\Big(\theta_q\Big(\gamma\Big(\sum_i \alpha_i^*(x)p_i(x)\Big)\Big)\Big)\\ &= \tau\Big(\theta_q\Big(\sum_i (\alpha_i(x) + I_*)p_i(x)\Big)\Big)\\ &= \tau\Big(\sum_i (\alpha_i(q) + I_*)p_i(q)\Big)\\ &= \sum_i \alpha_i^* q(x)p_i(q(x))\\ &= f^*(q(x)),\end{aligned}$$

so $s_q = \tau \circ \theta_q \circ \gamma$, which is therefore an endomorphism of $A[X]^{\mathcal{B}(Pr')}$. ∎

In particular, if $a \in A^N$ and $f(x) \in A_{\sigma_i}[X, P]$ then $f^*(a) \in A_{\sigma_i}$, and the restriction mapping $s_a : A[X] \to A_{\sigma_i}$ is a homomorphism, the *Evaluation Homomorphism* associated with a, a generalisation of the corresponding idea from the theory of polynomials over a field.

4. Composition

Here we focus on the one variable, single sorted case because the formulation is rather clearer. There is a fairly obvious extension of the ideas discussed here to many variable many sorted situations, although the notion of composition of functions (which we are modelling) is most natural in the single sorted case.

Suppose A is a single sorted (or universal) algebra. Let $X = \{x\}$. We adopt the notation $A[x]$ for $A[X]$. Elements of $A[x]^{\mathcal{B}(Pr')}$ may be viewed as operators on A.

For $f(x) = \sum_i \alpha_i(x)p_i(x)$ and $g(x) = \sum_i \beta_i(x)q_i(x)$ in $A[x]^{\mathcal{B}(Pr)}$, define

$$(g \circ f)(x) = \sum_{i,j} \alpha_i(x)\beta_j(p_i(x))q_j(p_i(x)).$$

We call $(g \circ f)(x)$ the *composition* of $f(x)$ and $g(x)$, for the following reason:

https://doi.org/10.1017/S000497270000959X Published online by Cambridge University Press

PROPOSITION 4.1. *Let $*$ be an instance of P, with $f(x), g(x) \in A[x]^{\mathcal{B}(Pr)}$. Then $(g \circ f)^*(a) = g^*(f^*(a))$ for all $a \in A$.*

PROOF: Let $f(x) = \sum_i \alpha_i(x)p_i(x)$ and $g(x) = \sum_i \beta_i(x)q_i(x)$. The $\alpha_i(x)$ are a partition of unity, so $\alpha_i(x)\alpha_j(x) = \emptyset$ and $\sum_i \alpha_i(x) = 1$, so for $a \in A$, there is a unique j such that $\alpha_j^*(a) = 1$, with $\alpha_k^*(a) = \emptyset$ for all $k \neq i$. Hence $f^*(a) = p_j(a)$, so $g^*(f^*(a)) = g^*(p_j(a))$. Repeating the argument for $f(x)$, there is a unique k such that $\beta_k^*(p_j(a)) = 1$, with $\beta_i^*(p_j(a)) = \emptyset$ for all $i \neq k$. Hence $g^*(f^*(a)) = q_k(p_j(a))$.

On the other hand, $(g \circ f)(x) = \sum_{i,l} \alpha_i(x)\beta_l(p_i(x))q_l(p_i(x))$. So

$$\begin{aligned}(g \circ f)^*(a) &= \sum_{i,l} \alpha_i^*(a)\beta_l^*(p_j(a))q_l(p_i(a)) \\ &= \sum_{l} \alpha_j^*(a)\beta_l^*(p_j(a))q_l(p_j(a)) \\ &= \alpha_j^*(a)\beta_k^*(p_j(a))q_k(p_j(a)) \\ &= 1 \cdot 1 \cdot q_k(p_j(a)) \\ &= g^*(f^*(a)).\end{aligned}$$

□

The analogous formula for compositions of functions applies to elements of $A[x]^{\mathcal{B}(Pr')}$.

COROLLARY 4.2. *Let $f^*(x), g^*(x) \in A[x]^{\mathcal{B}(Pr')}$. Define $g^* \circ f^* = (g \circ f)^*$. Then $(g^* \circ f^*)(a) = g^*(f^*(a))$.*

PROOF: We show that $g^* \circ f^* = (g \circ f)^*$ is well defined on $A[x]^{\mathcal{B}(Pr')}$. Let $f_1, g_1 \in A[x]^{\mathcal{B}(Pr)}$ be such that $f_1^* = f^*$ and $g_1^* = g^*$. Then, for all $a \in A$,

$$(g \circ f)^*(a) = g^*(f^*(a)) = g_1^*(f_1^*(a)) = (g_1 \circ f_1)^*(a)$$

by Proposition 4.1, so $(g \circ f)^* = (g_1 \circ f_1)^*$ and so $g^* \circ f^* = (g \circ f)^*$ is well defined, and

$$(g^* \circ f^*)(a) = (g \circ f)^*(a) = g^*(f^*(a))$$

by Proposition 4.1. □

Much of the motivation for the work of this paper lies in the authors' desire to extend the notion of polynomial so that it can better capture the kinds of functions which are in practice computable. The next obvious extension of the polynomial idea would permit the definition of recursively defined functions.

References

[1] H. Lausch and W. Nobauer, *Algebra of polynomials*, North-Holland mathematical library **5** (North-Holland, Amsterdam, 1973).

[2] A.G. Pinus, 'Boolean Constructions in Universal Algebra', *Russian Math. Surveys* **47** (1992), 157–198.

Department of Mathematics
University of Tasmania
Hobart, Tas 7000 Australia