COMMUNICATING PROCESSES AND ENTROPIC ALGEBRAS

Anna B. ROMANOWSKA and Jonathan D.H. SMITH

Institute of Mathematics, Warsaw University of Sciences and Technology, 00 601 Warsaw, Poland
and
Department of Mathematics, Iowa State University, Ames IA 50011, USA

A significant contribution to the analysis of certain aspects of the communicating processes model was made by D. Benson's proposal to view incompletely specified nondeterministic processes as modules over certain semirings, and dually as comodules over corresponding coalgebras. The effectiveness of the proposal in treating the synthesis of such processes under mutual communication depended on the good behaviour of these algebraic systems with respect to tensor products. The aim of the paper is to draw attention to the algebraic theory underlying Benson's proposal, the theory of entropic algebras. Working with entropic algebras guarantees that tensor products are sufficiently well-behaved to make Benson's theory work.

1. INTRODUCTION

The communicating processes model is a fundamental object of study in many areas of application of modern mathematics. Beyond its familiar use in the analysis of distributed computation [3], [M1], [M2], it appears for example in theoretical biology in the guise of neural nets [AA] and genetic nets [Wa, pp. 18 ff.]. There are also less obvious applications. In a reversal of the usual technique of hiding internal events to merge communicating processes into a single whole, F. ROBERT [Ro, § 1.4] uses the model to study a single iterative process by viewing it as a network of communicating subprocesses.

A significant contribution to the analysis of certain aspects of the model was made by D. BENSON's stimulating and elegant proposal [Be], [BM] to view incompletely specified nondeterministic processes as modules over certain semirings, and dually as comodules over corresponding coalgebras. The effectiveness of the proposal in treating the synthesis of such processes under mutual communication depended on the good behaviour of these algebraic systems with respect to tensor products. Part of BENSON's mo-
tivation was the desire to translate the tensor product formalism from the real vector spaces used in topological dynamics to the semigroups of modules of his approach to communicating processes.

The aim of the current paper, inspired by [8], is to draw attention to the algebraic theory underlying BERNHORN's proposal. This is the theory of entropic algebras - algebras in which each operation is a homomorphism. Examples of entropic algebras are provided by the semilattices of SOE [Sp, A1-A3], [2, Prop. 5.1(2) (4)], the modules of [8], [9], and vector spaces. Working with entropic algebras guarantees that tensor products are sufficiently well-behaved [10] to make BERNHORN's theory work. As an indication of the need for some circumspection when dealing with tensor products, note that the tensor product of semigroups is not associative [8, p. 271].

The basic algebraic theory is presented in the second and third sections. It is then used in the fourth section to give a general formulation of BERNHORN's proposal. The general formulation avoids the use of duality made in [8, pp. 17-12]. The string-reversing anti-isomorphism turns out to be adequate to change a right monoid into a left monoid. This removes the apparent dependence on the synthesis of algebra for CCS (in the sense of [11, 4, 4]), enabling other syntheses level descriptions (such as the parallel compositions "\( \ast \)" and "\( \circ \)" of HOARE-BRENNER-REBOGO [11, 4.5-6]) to be given the elegant description of [8] that avoids the ambiguous elements * and 0 of [11]. Besides giving a theoretical underpinning to the Boolean semiring-module treatments of [8], [9], the general entropic algebra formulation offers two other advantages. Firstly, it makes it easy to attempt a translation of known results from topological dynamics expressed in the language of vector spaces (cf. Example 2.1 below) - simply rewrite them in terms of entropic algebras, and interpret them in other varieties (such as those in further examples of § 2). Secondly, it provides a ready-made framework within which to study extensions of the techniques of [8], [11] from nondeterministic choices to probabilistic choices (cf. [10], [11], [2, 3, 9, 4, 10]) and other contexts, making it potentially available for a wide variety of applications to biology and other fields. In this way, the formulation suggests a procedure "to establish bridges between the continuous methods, the stochastic analysis and the boolean analysis" [12, p. 15] of communicating processes. Of course, there are even more general approaches available, such as that of bi-

triples (cf. [8], etc.) or commutative theories [13], but entropic algebras have the advantage of providing sufficient generality, while at the same time remaining concrete enough for the usual algebraic intuitions to act as reliable guides.

2. ENTROPIC ALGEBRAS

This section and the next give illustrations and a brief summary of those aspects of the theory of entropic algebras that are used here for studying communicating processes. Most of the results are well-known "folk theorems" in universal algebra and category theory. The present applications may prove interesting to specialists in those disciplines. Further details of the algebraic background are given in [14] and [15, Chapter 1].

An algebra \((A, 0)\) is a set \(X\) equipped with an operator domain \(0\) and a type or arity \(\tau\) \(\tau: X + N\) such that each \(\tau\) in \(\tau\) determines a map

\[\mu: X^\tau \to A: \langle a_1, \ldots, a_n \rangle \mapsto a_1 \ldots a_n x\]

where \(X = \tau\). A homomorphism \(f: (A, 0) \to (B, 0)\) of algebras of the same type \(\tau: X + N\) is a set mapping \(f: X \to B\) with \(a_1 \ldots a_n f = f_1 a_1 \ldots f_n a_n\) for all \(\tau = \tau\) in \(\tau\) and \(a_1, \ldots, a_n\) in \(A\).

The direct product \((A, 0)^n\) has componentwise operations, making it an algebra of the same type as \((A, 0)\). Then \((A, 0)\) is said to be entropic if each \(\tau: (A, 0)^n - (A, 0)\) in \(\tau\) is a homomorphism. Varieties \(\mathscr{V}\) are classes of algebras of the same type closed under the taking of subalgebras, arbitrary direct products, and homomorphic images.

Example 2.1 (Vector spaces). For a field \(F\), vector spaces \(A\) over \(F\) form a variety of entropic algebras of type \((+ , 1)\) \(\mu(F(1))\) where \(F\) in \(F\),

\[1_A = A: a = a 1_A\]

is the unary operation of scalar multiplication. The effect \((a_1, \ldots, a_n) \mu(\cdot)\) is a derived operation \(\cdot\) on a set \(\{a_1, \ldots, a_n\}\) of arguments from \(A\) is a linear combination of the arguments.\(\cdot\)

Example 2.2 (Modules over a commutative ring). Example 2.1 may be generalised by relaxing the requirements on \(F\), so that it is merely a commutative ring. One obtains the variety of modules over the ring \(F\). The commutativity of \(F\) corresponds to
Example 2.2 (Semilattices). The variety of semilattices is the variety of algebras \((A,\wedge,\vee)\) with a single binary idempotent commutative associative operation \(\wedge\) of a derived operation \(\vee\) on a set \(\{a_1, \ldots, a_n\}\) of arguments from \(A\) represents a non-empty subset of the arguments. Indeed \((a_1, \ldots, a_n)\) represents \((y_1, \ldots, y_p)\).

Example 2.4 (Barycentric algebras \([9, 2.1])\). Let \(x^p = (p \in \mathbb{R} : 0 < p < 1)\). For \(p \in \mathbb{R}^+, \) set \(y^p = 1-p\). A barycentric algebra is an algebra \((A,\vee)\) of type \(\mathbb{Z}^{\mathbb{R}^+}\), with \(x^p \vee y = x^p \vee y^p = \max(x^p, y^p)\) for \(p \in \mathbb{R}^+,\) satisfying the identities \(x^p \vee x = x\) of idempotence, \(x^p \vee y = x^p \vee y\)' of skew-commutativity, and \(x^p \vee y = x^p \vee y = (p^p + q^p)^{1/p^p+q^p}\) of skew-associativity. Semilattices form a class of barycentric algebras with \(x^p = x\) for all \(p \in \mathbb{R}^+\). Another important class of barycentric algebras consists of the nerve sets as identified in \([9, 2.1]\). Free barycentric algebras are convex sets. The effect \((x_1, \ldots, x_n)\) of a derived operation \(w\) on a set \(\{x_1, \ldots, x_n\}\) of arguments from a convex set \(A\) represents a probability distribution on the arguments. In particular, \(x^p\) represents the distribution with probabilities \(f(x) = 1-p\) and \(g(y) = p\).

Example 2.5 (Semimodules over semirings). A semiring \([9, 9.26]\) is an algebra \((A, \wedge, \vee)\) of type \((\mathbb{Z}^+)\times \mathbb{Z}^+\) where \((A,\wedge)\) and \((A,\vee)\) are semigroups connected by the distributive laws \((a\wedge b)\vee c = a\wedge(b\vee c)\) and \((a\vee b)\wedge c = a\wedge(b\wedge c)\). The semiring \(\mathbb{N}\) is the monoid with the identity \(1\) under the usual operations. The distributive lattice, and indeed all semilattices \([9, 3.26]\), are semirings. The dual of a semiring is a semiring with \(\wedge\) and \(\vee\) interchanged. Such a semiring in \(\mathbb{N}\) is called a skew-associative semiring. In particular, \(\mathbb{N}\) is a skew-associative semiring.

For an entropic semigroup \((B,\wedge)\), the endomorphism semiring \((\text{End}(B,\wedge))\) is a semiring in \(\mathbb{N}\) with \((a\wedge b)\vee c = a\wedge(b\vee c)\) and \((a\vee b)\wedge c = a\wedge(b\wedge c)\). For any \(\text{End}(B,\wedge)\) such that \(\wedge\) is a monoid, \(\text{End}(B,\wedge)\) is a semiring in \(\mathbb{N}\) with \((a\wedge b)\vee c = a\wedge(b\vee c)\) and \((a\vee b)\wedge c = a\wedge(b\wedge c)\). Such a semiring in \(\mathbb{N}\) is a skew-associative semiring. For any entropic semigroup \((B,\wedge)\), the endomorphism semiring \((\text{End}(B,\wedge))\) is a semiring in \(\mathbb{N}\) with \((a\wedge b)\vee c = a\wedge(b\vee c)\) and \((a\vee b)\wedge c = a\wedge(b\wedge c)\). Such a semiring in \(\mathbb{N}\) is a skew-associative semiring.
A * B * B * A is the "twisting" twist + base.

In a variety \( V \) of entropic algebra, a coalgebra \( C \) (cf. [Be, pp. 6-7], [Sw, pp. 4-51]) is a \( V \)-algebra \( C \) equipped with homomorphisms \( \alpha_C : C \to C^2 \) and \( \varepsilon_C : C \to \lambda \) such that the diagram

\[
\begin{array}{ccc}
C & \xrightarrow{\alpha_C} & C^2 \\
\downarrow & & \downarrow \\
C & \xrightarrow{\varepsilon_C} & \lambda
\end{array}
\]

commutes, where the sloping maps are the natural isomorphisms \( \varepsilon_C : C \to C \) and \( \alpha_C : C \to C^2 \). Given coalgebras \( C \) and \( D \) in \( V \), a \( V \)-homomorphism \( f : C \to D \) is a coalgebra homomorphism (cf. [Sw, pp. 13-41]) if the diagram

\[
\begin{array}{ccc}
C & \xrightarrow{f} & D \\
\downarrow & & \downarrow \\
C & \xrightarrow{\varepsilon_C} & \lambda
\end{array}
\]

commutes. A right \( C \)-comodule (cf. [Be, pp. 8-9], [Sw, p. 30]) is a \( V \)-algebra \( N \) with a homomorphism \( \delta : N \to C \) called the structure map such that the diagram

\[
\begin{array}{ccc}
N & \xrightarrow{\delta} & C \\
\downarrow & & \downarrow \\
N & \xrightarrow{\varepsilon_N} & \lambda
\end{array}
\]

commutes. A left \( C \)-comodule is a \( V \)-algebra \( N \) with a homomorphism \( \psi : N \to C \) (again called the structure map) such that the diagram

\[
\begin{array}{ccc}
N & \xrightarrow{\psi} & C \\
\downarrow & & \downarrow \\
N & \xrightarrow{\varepsilon_N} & \lambda
\end{array}
\]

commutes. As in (3.1), the sloping maps in (3.3) and (3.4) denote the natural isomorphisms \( \delta : \delta(\varepsilon_C) = \varepsilon_C \delta \) and \( \varepsilon : \varepsilon(\delta) = \delta \varepsilon \).

The interpretation of these algebraic abstractions in terms of communicating processes may be summarized as follows (more detailed examples are given in the next section). Coalgebras \( C, D \) represent communications channels, into which messages (as distributions of strings or traces of events) may be sent or from which messages may be received. A right \( C \)-comodule \( N \) represents a transmitting machine. An element of \( N \) represents a condition of the machine. The structure map \( \delta : N \to C \) describes the transition of the transmitter from one condition to another; during the transition a message is sent into \( C \). A left \( D \)-comodule \( N \) represents a receiving machine. The structure map \( \varepsilon : N \to D \times N \) describes the transition of the receiver from one condition to another; during the transition a message is received from \( D \). A \( V \)-algebra homomorphism \( \varepsilon C : D \times N \to \lambda \) serves to synchronize communications over the channels \( C \) and \( D \). Thus the composition

\[
\begin{array}{ccc}
N & \xrightarrow{\psi} & C \\
\downarrow & & \downarrow \\
N & \xrightarrow{\varepsilon_N} & \lambda
\end{array}
\]

describes the transition of the coupled machine \( N, N \) from one condition to another as a result of synchronized communications; the message sent by \( N \) into \( C \) is synchronized with the message received by \( N \) from \( D \). In all this, "conditions" and "messages" may stand for non-deterministic or probabilistic combinations of "pure" conditions and messages, according to the variety \( V \) of entropic algebra in which \( N, N, C \) and \( D \) lie.

4. COMMUNICATING PROCESSES

This section discusses some formulations of communicating processes (such as [Be]) in terms of entropic algebras. Throughout, let \( \text{V} \) be a fixed non-trivial variety of entropic algebras. Let \( N \) be the free \( \text{V} \)-algebra on the singleton \( \{ n \} \). In the context
of \([Bz]\), \(V\) is the variety of join semilattices with zero, so that \(x \lor 0 = x \land 0 = 0\). Then \(X = \langle 0, 1 \rangle\). Let \(A\) be a given alphabet. The elements of \(A\) represent events. Let \(D\) be a symmetric and reflexive relation on \(A\), known as the dependency relation on \(A\). If \(A\) is finite, the pair \((A, D)\) is a "concurrent alphabet" in the sense of [15]. Let \(A^D\) or \((A^\ast)^D\) be the monoid generated by \(A\) subject to the relations that independent events (i.e., events \(a, b\) with \((a, b) \notin D\)) commute. If \(A\) is finite, then \(A^D\) is the "algebra of traces over \((A, D)\)" in the sense of [15]. If \(D = A \times A\), so that there are no independent events, then \(A^D\) is just the free monoid \(A^\ast\) on \(A\).

Let \((A^\ast)^D\) denote the opposite of \((A^\ast)^D\) with

\[
(a, b) = b \cdot a.
\]

The identity mapping on \(A\) extends to uniquely mutually inverse monoid homomorphisms \(\tau : (A^\ast)^D \to (A^\ast)^D\) and \(\tau' : (A^\ast)^D \to (A^\ast)^D\), called reversal, with \(a_1 \ldots a_n \cdot a_{n+1} \ldots a_m = a_m \ldots a_{n+1} \cdot a_1 \ldots a_n\) for \(a_1 \ldots a_m\) \(\in A^D\). Let \(C\) be the free algebra in \(V\) on \(A^D\). Since \(V\) is non-trivial, \(A^D\) may be identified with its image in \(C\). The elements of \(C\) are \(V\)-words in the elements of \(A^D\). Note that the multiplication \(\cdot\) in \(A^D\) extends to \(\cdot\) in \(C\) and \(C = C^D\).

Suppose that \(C\) has a coalgebra structure \((C, \Delta, \epsilon)\) as in (3.1) with \(\Delta = \delta_0\). For example, suppose that \(V\) is a variety of unital semilattices over a commutative semiring with 0 and 1. Given a string \(s\) in \(A^\ast\), the pairs \((s', s')'\) for which \(s'as'\) appears as an argument of the \(V\)-word \(s\) may represent factorisations \(s = s'as'\). In (4.2), these pairs are the \(\{s_1, s_2, \ldots, s_n, s'_{n+1}, \ldots, s'_{m-1}\}\). Take \(s_1 = s_2 = \ldots = s_n = \epsilon\). Such coalgebras are called coalgebras \([Bz]\) [15]. Given a choice coalgebra \(C = (C, \Delta, \epsilon)\) with

\[
\Delta = (\Delta_1, \Delta_2, \ldots, \Delta_n, \epsilon)
\]

where \(\Delta_1\) is a derived operation of \(V\) depending on \(s\), a reversed coalgebra \(C^R = (C^R, \Delta^R, \epsilon)\) may be defined by

\[
\Delta^R = (\Delta_1, \Delta_2, \ldots, \Delta_n, \epsilon)
\]

the commuting of the diagram (3.1) for \(C\), interpreted at the element level, gives the commuting of the corresponding diagram for \(C^R\) on reversing the strings appearing. Note that, in general, the coalgebra \(C^R\) is not isomorphic to the coalgebra \(C\).

Define a \(C\)-process to be a right \(C\)-comodule \(U\) for the coalgeb-
and let $U$ denote the machine $U$.

Let $V$ be free in $X$ on $(i, t)$. As a right $C$-comodule, suppose that $V$ has the structure map $\phi_V: V \times C \to X$ with $\phi_V(i) = i * \tau_a + \tau_b$ and $\phi_V(t) = \tau_a$. Let $U$ be free in $Y$ on $(j, u)$. As a right $C$-comodule, suppose that $U$ has the structure map $\phi_U: U \times C \to Y$ with $\phi_U(j) = j * \tau_a + \tau_e$ and $\phi_U(u) = u * i$. According to (4.5), $U$ has a left $C$-comodule structure map $\phi^U: C^* \times U \to U$ with $\phi^U(i) = i * \tau_a + \tau_e$ and $\phi^U(u) = u * i$. Suppose that $V$ and $U$ communicate over the channel $C$ in such a way that event $b$ may occur asynchronously, while event $a$ occurs as a "handshake" between $V$ and $U$. Thus $(i, b) = (b, i) = (i, b) = (1, 1, 1, 1), a$ while $(x, y) = 0$ for other pairs $(x, y)$ in $(A \cup \{1\}) \times (A \cup \{1\})$. A run of the pair $V \cup U$ of communicating machines starting from the (deterministic) initial condition $i * j$ is then described by (4.6) as follows. Under $\phi^V \circ \phi^U$, the element $i * j$ of $V \times U$ is mapped to the element $(i * \tau_a + \tau_e + \tau_b) * (j * \tau_a + \tau_e) = \tau_a i * j + \tau_e i * j + \tau_b i * j + \tau_a j * i + \tau_e j * i + \tau_b j * i + \tau_a i * j + \tau_e i * j + \tau_b i * j$ of $\tau_a C \times C^* \times U \cup \tau_e C \times C^* \times U \cup \tau_b C \times C^* \times U \cup \tau_a i * j + \tau_e i * j + \tau_b i * j$ and $\tau_a j * i + \tau_e j * i + \tau_b j * i + \tau_a i * j + \tau_e i * j + \tau_b i * j$ in $V \cup U$. Thus there are three possible behaviours:

(i) the machines may stay in their initial conditions, without communicating;

(ii) $V$ may change to its terminal condition $t$ via the asynchronous event $b$;

(iii) $V$ and $U$ may "shake hands", communicating via the event $a$ which changes them to their respective terminal conditions $t$ and $u$.

It is interesting to contrast this with the description provided by regarding $V$ and $U$ as [diagram] of "elementary net systems" in the sense of [Ma, §4]. The "composition" $V \cup U$ [Ma, §4.4] is the net system with diagram.


