What is Algebraic in Process Theory?

Bas Luttik

Formal Methods Group
Eindhoven University of Technology

August 1, 2005

In mathematics: two kinds of *algebra*

Elementary algebra is about the real number system

- Solving systems of equations

  Find real numbers x, y such that $4x + 2y = 14$ and $4x - 2y = 2$

- Expressing properties of operations on reals by means of equations

  For all real numbers x, y and z: $x \cdot (y + z) = x \cdot y + x \cdot z$.

Abstract algebra is about the fundamental operations of arithmetic in general (*addition*, *multiplication*, . . .)

Abstract Algebra

"[...] deals not primarily with the manipulation of sums and products of numbers [...] but with sums and products of elements of any sort"

(Mac Lane/Birkhoff)

Desideratum: abstract from objects, concentrate on operations

The abstraction is achieved by axiomatic definitions.

A **group** is *any* set with an associative binary operation with identity and inverse in the set.

Benefits: it *elegant* and *general*, and facilitates *connexions*

Process algebra

A **process algebra** is a set with *process-theoretic* operations (sequencing, choice, parallel composition, etc.) defined on it.

CSP**:** process-theoretic operations defined on *failure sets*.

CCS**:** process-theoretic operations defined on LTSs modulo observation congruence

ACP**:** process-theoretic operations defined by axioms

(Elementary) Algebraic Achievements

Expressiveness results

E.g., $Stack$ is finitely definable (with recursive spec) with choice and sequential composition, but not with choice and prefix multiplication.

Axiomatisations

For many process algebras a ground-complete set of equational axioms has been given.

Unique decomposition results

For many process algebras it has been proved that processes have a unique decomposition w.r.t. parallel composition.

An Abstract Algebraic Result (1)

1. A process algebra is virtually always a *commutative monoid* under parallel composition, i.e.,

$$x \mid y = y \mid x \ ,$$

$$x \mid (y \mid z) = (x \mid y) \mid z \ , \text{ and}$$

$$x \mid \mathbf{0} = \mathbf{0} \mid x = x \ .$$

2. For every commutative monoid it makes sense to ask:

   Does it have unique decomposition?

   (For, the notion has an abstract algebraic definition!)

An Abstract Algebraic Result (2)

A **decomposition order** on a commutative monoid is a well-founded partial order $\longrightarrow^*$ on it such that for all x, y, z:

(i) $x \longrightarrow^* \mathbf{0}$;

(ii) $x \longrightarrow^+ y$ implies $x \mid z \longrightarrow^+ y \mid z$;

(iii) $x \mid y \longrightarrow^* z$ implies $z = x' \mid y'$ with $x \longrightarrow^* x'$ and $y \longrightarrow^* y'$;

(iv) $x \longrightarrow^+ y^n$ for all $n \in \mathbf{N}$ implies $y = \mathbf{0}$.

Theorem: A commutative monoid has unique decomposition iff it can be endowed with a *decomposition order*.

$Proof$: Generalisation of Milner's proof for a concrete process algebra.

Not yet abstract algebraic

1. We're lacking an abstract algebraic definition of *atomic action*

2. Binders are not algebraic!

$$(\nu x)(P \mid Q) = P \mid (\nu x)Q \qquad \text{provided that } x \notin \mathrm{fn}(P)$$

$$(\textstyle\sum_x P) \cdot Q = \textstyle\sum_x (P \cdot Q) \qquad \text{provided that } x \notin \mathrm{FV}(Q)$$

   We're lacking, e.g., an abstract algebraic definition of *mobility*.

3. ...

Conclusion

Most algebra in process theory is elementary.

Many advanced process-theoretic concepts have no abstract algebraic definition.

Benefits of a more abstract algebraic approach:

1. insight in fundamental operations on behaviour;
2. elegant mathematical theory of behaviour; and
3. facilitates connexions with other areas of mathematics/logic.