Rational Coalgebraic Machines on Varieties

Rob Myers

June 24, 2011

Core notions of algorithm/machine:

- Turing machine $\approx$ Finite control states $+$ Infinite tape.
- Register machine $\approx$ Finite control states $+$ Registers $(\mathbb{Z}^m)$.

Can view as possibly *infinite* set of states by absorbing memory.

'Finite state machine $+$ interaction with unbounded memory' permits description of possibly infinite sets of states.

Alternative method of describing possibly infinite states:

- $\mathsf{Alg}(\Sigma, \mathbb{E})$ a variety e.g. Set, $\mathsf{SL}_\perp$, DL, BA, $\mathsf{Vect}(\mathbb{F})$, Ab etc.
- $T : \mathsf{Alg} \to \mathsf{Alg}$ a finitary surjection preserving endofunctor.
- Machines are *finitely presentable coalgebras* i.e.

$$\gamma : A \to TA$$

where γ an Alg-morphism and $A \in \mathsf{Alg}$ finitely presentable.

But how are we to think of these finitely presentable (FP) coalgebras?

Following the work of Silva, Bonsangue and Rutten and also that of Milius, we represent them syntactically using expressions.

$$\mathcal{L}(T) \ni \phi ::= \sigma(\phi_j)_{j \in ar(\sigma)} \mid [\lambda](\phi_j)_{j \in ar(\lambda)} \mid x \mid \mu x.\phi$$

where $\sigma \in \Sigma$, $\lambda \in \Lambda$, $x \in \mathcal{X} = \{x_n : n \in \omega\}$ are fixpoint constants.

- Λ is some 'operator signature' induced by T e.g.

  $$\Lambda = \coprod_{n \in \omega} UTFn \qquad ar(n,t) = n$$

  although usually much too big.

- Restrict to $[\lambda]$-*guarded expressions* $\mathcal{L}_g(T)$, needn't be closed.

Theorem (Kleene theorem)

For finitary surjection preserving $T : \mathrm{Alg} \to \mathrm{Alg}$ *have translations:*

1. *Pointed FP* $T_{\mathcal{X}}$*-coalgebra* (A, γ, a_0) *to* $\phi_{(A,\gamma,a_0)} \in \mathcal{L}_g(T)$.
2. *Guarded* ϕ *to pointed FP* $T_{\mathcal{X}}$*-coalgebra* $(A_\phi, \gamma_\phi, a_\phi)$.

such that:

$$(A, \gamma, a_0) \qquad \textit{and} \qquad (A_{\phi_{(A,\gamma,a_0)}}, \gamma_{\phi_{(A,\gamma,a_0)}}, a_{\phi_{(A,\gamma,a_0)}})$$

are ω*-step behaviourally equivalent.*

- $T_{\mathcal{X}} = F\mathcal{X} + T$ extends T with 'colours' $\mathcal{X}$.
- For all known finitary $T : \mathrm{Alg} \to \mathrm{Alg}$, ω-step behaviourally equivalent $\Rightarrow$ behaviourally equivalent.

Proof sketch: Synthesis of $(A_\phi, \gamma_\phi, a_\phi)$ from $\phi \in \mathcal{L}_g(T)$.

1. Construct subexpressions $S_\phi \subseteq_\omega \mathcal{L}_g(T)$ of ϕ.
2. Can view ϕ as coalgebra for polynomial functor $P : \mathsf{Set} \to \mathsf{Set}$,
$$\Delta_\phi : S_\phi \to P(S_\phi)$$
3. Apply a 'free construction' $\tilde{F} : \mathsf{Coalg}_{\mathsf{Set}}(P) \to \mathsf{Coalg}_{\mathsf{Alg}}(T_\mathcal{X})$:
$$\gamma_\phi := \tilde{F}\Delta_\phi : FS_\phi \to T_\mathcal{X}(FS_\phi)$$
$A_\phi = FS_\phi$ is finitely generated free algebra, $a_\phi = \eta_{S_\phi}(\phi) \in A_\phi$.

Note: If ϕ is closed then $\tilde{F}\Delta_\phi$ effectively a T-coalgebra.

Example

For $T : \mathrm{Vect}(\mathbb{R}) \to \mathrm{Vect}(\mathbb{R})$ where $T = \mathbb{R} \times Id$,

$$\mathcal{L}(T) \ni \phi ::= 0 \mid k.\phi \mid \phi_1 + \phi_2 \mid [*] \mid \bigcirc\phi \mid x \mid \mu x.\phi \qquad (k \in \mathbb{R})$$

If $\phi = \mu x.([*] + \frac{1}{2}\bigcirc x) \in \mathcal{L}_g(T)$ then:

- $S_\phi = \{\phi\}$
- $\Delta_\phi : S_\phi \to PS_\phi$ is defined $\Delta_\phi(\phi) = [[*] + \frac{1}{2}\bigcirc](\phi)$
- $\gamma_\phi : FS_\phi \to \mathbb{R} \times FS_\phi$ is linear transform $\begin{pmatrix} 1 \\ \frac{1}{2} \end{pmatrix} : \mathbb{R} \to \mathbb{R}^2$
- Behaviour is $(1, \frac{1}{2}, \frac{1}{4}, \ldots)$.

Example

Consider $T = 2 \times Id^A$ on Set, $\mathrm{SL}_\perp$, DL and BA where $A = \{a_i : i \in n\}$. The respective expressions are:

- $\phi ::= [0](\phi_j)_{j \in n} \mid [1](\phi_j)_{j \in n} \mid x \mid \mu x.\phi$
- $\phi ::= \perp \mid \phi_1 \oplus \phi_2 \mid [0] \mid [1] \mid [a_i]\phi \mid x \mid \mu x.\phi$
- $\phi ::= \perp \mid \top \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid [0] \mid [1] \mid [a_i]\phi \mid x \mid \mu x.\phi$
- $\phi ::= \perp \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid [0] \mid [1] \mid [a_i]\phi \mid x \mid \mu x.\phi$

The expressions may be viewed as *deterministic*, *nondeterministic*, *alternating* and *boolean automata*, respectively.

In each case the synthesis procedure constructs a *deterministic automaton* over the respective finitely generated free algebra.

Example

Can represent digital circuits (gates + flip flops) by expression linear in its size. Synthesis effectively constructs Mealy machine i.e. performs and hides internal communication.

$$\phi ::= \bot \mid \phi_1 \oplus \phi_2 \mid \mathit{module}_{I:O}(\phi) \mid [\chi_1 \Rightarrow \chi_2]\phi \mid x \mid \mu x.\phi$$

Example

Can represent unbounded memory via e.g. abelian groups with constants. Memory is persistent. (Needs more work)

Other direction: $\phi \in \mathcal{L}_g(T)$ from pointed FP $T_{\mathcal{X}}$-coalgebra.

Example

Consider $T = \mathbb{C} \times Id : \mathrm{Vect}(\mathbb{C}) \to \mathrm{Vect}(\mathbb{C})$ and $\gamma : F2 \to \mathbb{C} \times F2$,

$$\gamma_1 = \begin{pmatrix} 1 & 0 \end{pmatrix} : \mathbb{C}^2 \to \mathbb{C} \qquad \gamma_2 = \begin{pmatrix} 0 & -\frac{i}{2} \\ \frac{i}{2} & 0 \end{pmatrix} : \mathbb{C}^2 \to \mathbb{C}^2$$

If the initial state is $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ the construction yields the expression:

$$\mu x.([*] + \bigcirc\bigcirc\frac{x}{4})$$

i.e. the behaviour is $(1, 0, \frac{1}{4}, 0, \frac{1}{16}, 0, \ldots)$.

For the remainder of the talk we discuss **completeness** and **automatic proof construction**.

Completeness of what?

$$\mathcal{L}(T) \ni \phi ::= \sigma(\phi_j)_{j \in ar(\sigma)} \mid [\lambda](\phi_j)_{j \in ar(\lambda)} \mid x \mid \mu x.\phi$$

Need to give interpretation of expressions.

Theorem

If $T : \mathsf{Alg} \to \mathsf{Alg}$ is a finitary surjection and mono preserving functor with ω-bounded behaviour then the final T-coalgebra is a quotient of a final coalgebra for a polynomial functor on Set*.*

Sketch.

$$\Omega_T = P^{\omega}\mathbb{1}/\approx$$

$t_1 \approx t_2$ iff $\forall n \in \omega$.(depth n restrictions equivalent in algebra $T^n\mathbb{1}$).

$\square$

Note: No counter-examples to ω-bounded behaviour known.

Semantic domain of expressions:

- Have final coalgebra $\gamma_{T_\mathcal{X}} : \Omega_{T_\mathcal{X}} \to T_\mathcal{X}\Omega_{T_\mathcal{X}}$.
- *Coalg*$(T_\mathcal{X})$ inherits cocompleteness from Alg, so let $\gamma_\mathbb{Q} : \Omega_\mathbb{Q} \to T_\mathcal{X}\Omega_\mathbb{Q}$ be colimit of all FP $T_\mathcal{X}$-coalgebras.
- Finally construct morphic image of $\gamma_\mathbb{Q}$ in $\Omega_{T_\mathcal{X}}$:

$$\gamma_{[\mathbb{Q}]} : \Omega_{[\mathbb{Q}]} \to T_\mathcal{X}\Omega_{[\mathbb{Q}]}$$

In many important cases $\gamma_\mathbb{Q} = \gamma_{[\mathbb{Q}]}$, but not always.

Intuitively $\gamma_{[\mathbb{Q}]}$ is subcoalgebra of rational behaviours in $\Omega_{T_\mathcal{X}}$.

For $\phi \in \mathcal{L}_g(T)$ define semantics $[\![\phi]\!]_{\Omega_{[\mathbb{Q}]}} \in \Omega_{[\mathbb{Q}]}$:

$[\![\phi]\!]_{\Omega_{[\mathbb{Q}]}}$ = **behaviour of pointed FP $T_{\mathcal{X}}$-coalgebra** $(A_\phi, \gamma_\phi, a_\phi)$

i.e. behaviour of synthesised coalgebra.

Completeness:

Provide an equational proof system such that:

$$\vdash \phi = \psi \quad \text{iff} \quad [\![\phi]\!]_{\Omega_{[\mathbb{Q}]}} = [\![\psi]\!]_{\Omega_{[\mathbb{Q}]}}$$

The 'natural' choice for this proof system is:

1. Equations from variety $\mathrm{Alg}(\mathbb{\Sigma}, \mathbb{E})$ i.e. the set $\mathbb{E}$.
2. Equations which present functor (rank-1) i.e. we assume $T_{\mathcal{X}}$ is equationally presentable.
3. Unique fixpoint axiom and rule:

$$\mu x.\phi = \phi[x := \mu x.\phi] \qquad \frac{\phi[x := \psi] = \psi}{\mu x.\phi = \psi}$$

They are always **sound** i.e. $\vdash \phi = \psi$ implies $[\![\phi]\!]_{\Omega_{[\mathbb{Q}]}} = [\![\psi]\!]_{\Omega_{[\mathbb{Q}]}}$.

Expressions are **guarded**, so have guarded congruence rule for μx.

Example

$T = 2 \times Id^A : \mathsf{SL}_\perp \to \mathsf{SL}_\perp$ where $A = \{a_i : i \in n\}$,

$$\phi ::= \perp \mid \phi_1 \oplus \phi_2 \mid [0] \mid [1] \mid [a]\phi \mid x \mid \mu x.\phi$$

- $\mathcal{L}_g(T)$ may be viewed as 'nondeterministic automata'.
- $[\![\phi]\!]_{T_\mathcal{X}} = [\![\psi]\!]_{T_\mathcal{X}}$ iff they accept the same language.
- So completeness must construct equational proof that two nondeterministic automata accept the same language.

How are we to prove completeness?

Rough idea:

1. If $[\![\phi]\!]_{\Omega_{[\mathbb{Q}]}} = [\![\psi]\!]_{\Omega_{[\mathbb{Q}]}}$ then ω-step behaviourally equivalent i.e. depth n unwindings equivalent in each $T^n_{\mathcal{X}}\mathbb{1}$.
2. So to 'prove' $\phi = \psi$ try to construct a finite directed graph which can be unwound to arbitrary depth – each depth n proof is an equational proof in $T^n_{\mathcal{X}}\mathbb{1}$.
3. Finally need to convert this non-wellfounded proof into a well-founded equational proof: use unique fixpoint rule.

Constructing non-wellfounded proofs.

- Functor $T : \mathsf{Alg} \to \mathsf{Alg}$ has equational presentation iff T preserves sifted colimits. [Kurz, Rosicky]
- Core technique: present functor $T : \mathsf{Alg} \to \mathsf{Alg}$ by **one-step rules**. [Schröder (BA case)].

Theorem

If $FP = FG$ in Alg *then finitary* $T : \mathsf{Alg} \to \mathsf{Alg}$ *preserves monos iff it has a presentation by one-step complete one-step rules.*

Also many functors on other varieties have such a presentation.

Example

- $\tilde{\mathcal{P}}_\omega : \mathsf{SL}_\perp \to \mathsf{SL}_\perp$ is presented by rules:

$$\frac{\{p_i = q_j \ : (i,j) \in R\}}{\bigoplus_{i \in m} \Diamond p_i = \bigoplus_{j \in n} \Diamond q_j}$$

  whenever $R \subseteq m \times n$ has $R[m] = n$ and $R^\dagger[n] = m$.

- $T : \mathsf{BA} \to \mathsf{BA}$ defined $TA = \begin{cases} \mathbb{1} & A = \mathbb{1} \\ \mathbb{2} & \text{otherwise} \end{cases}$ has presentation:

$$\frac{\perp = \top}{\perp = \top}$$

Examples of rank-1 equations and 'corresponding' one-step rules.

$$(\mathrm{Set}) \quad [2](x,x) = [1]x \qquad \frac{x = z \quad y = z}{[2](x,y) = [1]z}$$

$$(\mathrm{Set}) \quad [1,1,1](x,y,y) = [2,1](y,x) \qquad \frac{x = b \quad y = a \quad z = a}{[1,1,1](x,y,z) = [2,1](a,b)}$$

$$(\mathrm{SL}_\perp) \quad \Diamond x \leq \Diamond(x \oplus y) \qquad \frac{x \leq y}{\Diamond x \leq \Diamond y}$$

$$(\mathrm{SL}_\perp) \quad [a](x \oplus y) \leq [a]x \oplus [a]y \qquad \frac{x \leq y \oplus z}{[a]x \leq [a]y \oplus [a]z}$$

$$(\mathrm{BA}) \quad \Box \top = \top \qquad \frac{x}{\Box x}$$

$$(\mathrm{BA}) \quad \Box(p \vee q) \leq \Box p \vee \Diamond q \qquad \frac{x = y \vee z}{\Box x \leq \Box y \vee \Diamond z}$$

Theorem

For either:

- *The functor* $FU : \mathrm{Alg} \to \mathrm{Alg}$ *on any variety, or*
- *Every mono and surjective preserving functor* $T : \mathrm{Alg} \to \mathrm{Alg}$ *where* Alg *has 'finitely generated relations' e.g. locally-finite varieties,* $\mathrm{Vect}(\mathbb{F})$ *and* Ab.

one can construct a finite 'closed tableau' for a pair of expressions $(\phi, \psi) \in (\mathcal{L}_g(T))^2$ *iff they are behaviourally equivalent.*

$$\mathcal{P}_\omega : \mathsf{Set} \to \mathsf{Set} \qquad \begin{tikzcd} \boxed{x_0} \arrow[loop above] \end{tikzcd} \approx_{beh} \begin{tikzcd} \boxed{y_0} \arrow[r, bend left] & \boxed{y_1} \arrow[l, bend left] \end{tikzcd}$$

$$\begin{tikzcd}
 & \boxed{[1]\mu x_0.[1]x_0 = [1][1]\mu y_0.[1][1]y_0} \arrow[dd, bend left=60, "loop\theta"] \\
 & \boxed{[1]\mu x_0.[1]x_0 = [1]\mu y_0.[1][1]y_0} \arrow[u, "R\theta"] \\
 {} \arrow[r, dashed] & \boxed{[1]\mu x_0.[1]x_0 = [1][1]\mu y_0.[1][1]y_0} \arrow[u, "R\theta"]
\end{tikzcd}$$

Converting non-wellfounded proofs to equational proofs.

The idea comes from Salomaa.

- In the sixties he axiomatised the regular expressions using unique fixed points.
- He required 'ϵ-free' expressions – becomes *guardedness* in our setting.

- Core idea:
  1. If two regular expressions denote same language then can construct finite collection of 'linear' equations over pairs (effectively a bisimulation).
  2. Using the unique fixpoint rule one can unwind these equations, yielding an equational proof.

How to generalise?

1. Desire to construct *bisimulations* leads us to require $T : \mathsf{Alg} \to \mathsf{Alg}$ has a relation lifting $\bar{T} : \mathsf{Rel} \to \mathsf{Rel}$.
2. The relevant notion of bisimulation we use is HJ-bisimulation [Staton]. It fits better than the usual notion of bisimulation.
3. Crucially, we extend the notion of 'one-step rule' to 'one-step relational rule'.

Lemma

- *If* $T : \mathsf{Alg} \to \mathsf{Alg}$ *has one-step complete presentation by relational rules then* T *has a relation lifting.*
- *If* Alg *has finitely generated relations then finitary* $T : \mathsf{Alg} \to \mathsf{Alg}$ *has a relation lifting then* T *has a one-step complete presentation by relational rules.*

Theorem

If T has a one-step complete relational presentation then every closed tableau yields:

- *An HJ-bisimulation.*
- *An equational proof of behavioural equivalence using Salomaa's method.*

Yields completeness for:

- Functors with a relation lifting and ω-bounded behaviour on Set, $\mathrm{SL}_\perp$, DL, BA, $\mathrm{Vect}(\mathbb{F})$, Ab and many others.
- The comonad functor on an arbitrary variety if it has a relation lifting.