A Modular Approach to Linear-Time Logics

Corina Cîrstea

University of Southampton, UK
cc2@ecs.soton.ac.uk

We summarise previous [2] and ongoing work on defining linear-time logics for systems modelled as coalgebras whose type incorporates branching. Instances of such logics support reasoning about the probability, respectively the minimal cost of exhibiting a certain linear-time behaviour. The results of loc. cit. apply to coalgebras of type $\mathsf{T} \circ F$ with T a (branching) monad and F a polynomial endofunctor on Set. Here we show that the approach generalises to arbitrary compositions involving a single branching monad and several endofunctors, not necessarily polynomial. In particular, this covers probabilistic automata and yields an interesting and, to our knowledge, previously unstudied logic for these systems.

We model systems with branching as coalgebras of type $F_1 \circ \mathsf{T} \circ F_2 \circ \mathsf{T} \circ \ldots \circ F_n$, with $\mathsf{T} : \mathsf{Set} \to \mathsf{Set}$ a commutative, *partially additive monad* (as defined in [1]) and $F_1, \ldots, F_n : \mathsf{Set} \to \mathsf{Set}$ arbitrary endofunctors. The monad T accounts for branching behaviour, while $F_1, \ldots, F_n$ jointly specify linear behaviour.

Proposition 1 ([1]). *Any commutative, partially additive monad* $\mathsf{T} : \mathsf{Set} \to \mathsf{Set}$ *induces a partial commutative semiring* $(\mathsf{T}\mathbb{1}, 0, +, \bullet, 1)$*, with* $\mathbb{1} = \{*\}$.

The (partial) + operation in turn induces a natural preorder $\sqsubseteq$ on $\mathsf{T}\mathbb{1}$, with 0 as bottom element. We further assume that $\sqsubseteq$ is a partial order with 1 as top element, and that $\sqsubseteq$ admits limits of both increasing and decreasing chains. These assumptions hold for the ordered semirings $(\{\bot, \top\}, \vee, \bot, \wedge, \top, \leq)$ induced by the powerset monad $\mathcal{P}$ and $W = (\mathbb{N}^\infty, \mathsf{min}, \infty, +, 0, \geq)$ induced by the weighted monad T_W, and for the ordered partial semiring $([0,1], +, 0, *, 1, \leq)$ induced by the sub-probability distribution monad $\mathcal{S}$. We use the set $\mathsf{T}\mathbb{1}$ as domain of truth values for a linear-time logic for coalgebras of type as described above. Thus, our category Pred of predicates has objects (X, P) with $P : X \to \mathsf{T}\mathbb{1}$, and arrows from (X, P) to (Y, Q) given by functions $f : X \to Y$ such that $P \sqsubseteq Q \circ f$.

Definition 1 ([2]). *Let* $\mathcal{V}$ *be a set of variables and* Λ *be a set of (unary) modalities. The* fixpoint logic $\mu\mathcal{L}_\Lambda$ *has syntax given by*

$$\varphi ::= x \mid \top \mid [\lambda]\varphi \mid \mu x.\varphi \mid \nu x.\varphi \qquad\qquad x \in \mathcal{V},\ \lambda \in \Lambda$$

and semantics $[\![\_]\!]^V_\gamma : \mu\mathcal{L}_\Lambda \to \mathsf{Pred}_C$ *(with* (C, γ) *a* $\mathsf{T} \circ F$*-coalgebra and* $V : \mathcal{V} \to \mathsf{Pred}_C$ *a* valuation*) defined inductively on the structure of formulas by*

$$[\![x]\!]^V_\gamma = V(x) \qquad [\![\top]\!]^V_\gamma(c) = \top \qquad [\![[\lambda]\varphi]\!]^V_\gamma = \gamma^*(\mathsf{P}_\mathsf{T}(\mathsf{P}_\lambda([\![\varphi]\!]^V_\gamma)))$$

and the usual clauses for fixpoint formulas. Here, Pred_C *are the predicates over* C*,* $\gamma^* : \mathsf{Pred}_{\mathsf{T}FC} \to \mathsf{Pred}_C$ *performs reindexing along* γ*,* $\mathsf{P}_\lambda : \mathsf{Pred} \to \mathsf{Pred}$ *is a lifting of* F *to* Pred*, and* $\mathsf{P}_\mathsf{T} : \mathsf{Pred} \to \mathsf{Pred}$ *is a canonical lifting of* T *to* Pred.

The semantics of $\mu\mathcal{L}_\Lambda$ resembles that of modal logics induced by predicate liftings [4], except that the so-called *extension lifting* P_T (see [2]) is used to abstract away branching; P_T takes a predicate (X, P) to $(\mathsf{T}X, \mu_\mathbb{1} \circ \mathsf{T}P)$, with μ the monad multiplication. [2] also shows how to canonically associate a set Λ of modalities, together with predicate liftings $(\mathsf{P}_\lambda)_{\lambda\in\Lambda}$, to any polynomial endofunctor F.

Example 1 ([2]). For $F = 1 + A \times \mathsf{Id}$ and $\mathsf{T} = \mathcal{P}$, one obtains an existential version of the linear-time μ-calculus. For $\mathsf{T} = \mathcal{S}$ or $\mathsf{T} = \mathsf{T}_W$, $\mu\mathcal{L}_\Lambda$-formulas measure the likelihood, resp. the minimal cost of exhibiting a certain linear-time property.

Definition 1 generalises to coalgebras whose type is obtained as the composition of several endofunctors $F_1, \ldots, F_n$, not necessarily polynomial, and a single monad T. The resulting (many-sorted) logic has one sort for each F_i, and makes use of liftings of the F_is to Pred, suitably combined with the extension lifting P_T, to provide semantics for the modal operators. Moreover, under the additional assumption (satisfied by the monads $\mathcal{P}$, $\mathcal{S}$ and T_W) that the universe of truth values is a lattice, conjunction and disjunction operators (one for each sort) can be added to the logic. For instance, in the case of $F_1 \circ F_2 \circ \mathsf{T}$-coalgebras, the two-sorted logic $\mu\mathcal{L}_{\Lambda_1,\Lambda_2}$ is parameterised by two sets of liftings $(\mathsf{P}_{\lambda_1})_{\lambda_1\in\Lambda_1}$ and $(\mathsf{P}_{\lambda_2})_{\lambda_2\in\Lambda_2}$, of F_1 and resp. F_2 to Pred, and interprets modalities by:

$$[\![[\lambda_1]\psi]\!]^V_\gamma = \gamma^*(\mathsf{P}_{\lambda_1}([\![\psi]\!]^V_\gamma)) \qquad\qquad [\![[\lambda_2]\varphi]\!]^V_\gamma = \mathsf{P}_{\lambda_2}(\mathsf{P}_\mathsf{T}([\![\varphi]\!]^V_\gamma))$$

Example 2. Probabilistic automata (also known as probabilistic transition systems [3]) are models incorporating both non-determinism and probability. They can be viewed as coalgebras of type $\mathcal{P}(A \times \mathcal{S})$. By taking $F_1 = \mathcal{P}$, $F_2 = A \times \mathsf{Id}$ and $\mathsf{T} = \mathcal{S}$ in the above, we view non-determinism as part of the linear structure and probability as the branching structure. A natural choice of modalities for F_1 and F_2 is then given by $\{\Diamond, \Box\}$ and resp. $\{(a), (-a) \mid a \in A\}$, with semantics:

– $\mathsf{P}_\Diamond(P)(Y) = \mathsf{sup}_{x\in Y} P(x)$, $\mathsf{P}_\Box(P)(Y) = \mathsf{inf}_{x\in Y} P(x)$
– $\mathsf{P}_{(a)}(P)(a, x) = \mathsf{P}_{(-a)}(P)(a', x) = P(x)$, $\mathsf{P}_{(a)}(P)(a', x) = \mathsf{P}_{(-a)}(P)(a, x) = 0$

for $P \in \mathsf{Pred}_X$, $Y \subseteq X$, $a \neq a' \in A$ and $x \in X$. The formulas $\mu x.\Diamond((a)\top \vee (-a)x)$ and $\mu x.\Box((a)\top \vee (-a)x)$ then measure the maximum, resp. minimum probability of eventually observing a, taken over all possible sequences of non-deterministic choices. The resulting logic is thus very different from (a fixpoint extension of) the two-sorted logic for probabilistic automata outlined in [3]. The latter employs *one-step* modalities $\Diamond_p$ with the intended reading "with probability at least p", and $\langle a\rangle, [a]$ with the standard semantics, and therefore does not support reasoning about the probability of a *long-term* linear property being exhibited.

References

1. C. Cîrstea. From branching to linear time, coalgebraically. In *FICS 2013*, 2013.
2. C. Cîrstea. A coalgebraic approach to linear-time logics. In *FOSSACS 2014*, 2014.
3. B. Jonsson, K.G. Larsen, and W. Yi. Probabilistic extensions of process algebras. In *Handbook of Process Algebra*, pages 685–710. Elsevier, 2001.
4. D. Pattinson. Coalgebraic modal logic: soundness, completeness and decidability of local consequence. *Theor. Comput. Sci.*, 309(1-3):177–193, 2003.