Towards Coalgebraic Specification of Rewriting Theories

Dirk Pattinson [*]
Institut für Informatik, LMU München
`pattinson@informatik.uni-muenchen.de`

Abstract

We describe a coalgebraic perspective on models of rewriting logic theories. After establishing a soundness and completeness result, we show how one can use modal logics for coalgebras to reason about the rewrite process. The approach is semantics-driven in the sense that the logic we propose is tailored to the class of models we consider.

1 Introduction

The theory of coalgebras has become increasingly popular over the recent years. Coalgebras – the formal duals of algebras – can be viewed as generalised *transition systems*, which come with a built-in notion of bisimulation. Many different types of systems can be treated within the coalgebraic framework, see for example [13]. This has lead to the development of general logics for coalgebras, generalising at the same time (multimodal) logics ([4]), Hennessy-Milner logic ([10]) and other logics used to reason about automata.

We apply the coalgebraic approach to (models of) *rewriting logic*. Rewriting logic is generally seen to be a logic of *change*, used to model and reason about a great variety of different (concurrent) systems, see [8, 9] for examples and an introduction to the general theory. By bringing together these two theories, we obtain a logic, which can be used to reason about the rewriting process.

Given a rewrite theory $\mathrm{Th} = (\Sigma, E, L, \mathcal{R})$ and a (Σ, E)-algebra A and a relation $R \subseteq A \times A$, we say that (A, R) is a *model* of Th, iff R realises every transition which can be derived by means of Th. The (transition) relation R then plays the role of the transition relation in standard treatments of modal logic. Considering (A, R) as Kripke frame, the only properties we can express so far are

---

[*] Research partially supported by the DFG Graduiertenkolleg "Logik in der Informatik" and the DAAD programme "INIDA"

termination and branching type. To overcome this lack of expressivity, we additionally introduce *observers*, which then determine a set of atomic propositions.

This allows us to *specify* properties of the rewrite process at an abstract level (using observers) and without reference to the rewrite rules. The task of building a system can therefore be split in two: The specifier determines a set of modal formulas, which he requires. In turn, it is the task of the implementor to provide rules which validate the specification.

2 Coalgebraic Modal Logic

2.1 Some Facts on Coalgebras and Bisimulations

We just provide the reader with the basic definitions and refer to [6, 12] for details.

Definition 2.1 (Coalgebras, Morphisms and Bisimulations)**.** Suppose $\Omega : \mathbf{Set} \to \mathbf{Set}$ is an endofunctor. An Ω-*coalgebra* is a pair (C, γ) with C a set and $\gamma : C \to \Omega C$ a function.

Suppose (C, γ) and (D, δ) are Ω-coalgebras.

A *coalgebra morphism* between (C, γ) and (D, δ) is a function $f : C \to D$ such that $\delta \circ f = \Omega f \circ \gamma$, that is, the diagram

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\gamma"] & D \arrow[d, "\delta"] \\ \Omega C \arrow[r, "\Omega f"] & \Omega D \end{tikzcd}$$

commutes.

A relation $R \subseteq C \times D$ is a *bisimulation*, if there exists a transition structure $\rho : R \to \Omega R$ such that the projections $\pi_1 : R \to C$ and $\pi_2 : R \to D$ are coalgebra morphisms $(R, \rho) \to (C, \gamma)$ and $(R, \rho) \to (D, \delta)$, respectively.

In the sequel we will only be concerned with special types of functors, that is, functors Ω of the form

$$\Omega Y = \mathcal{P}(Y) \times O_1 \cdots \times O_k \times Y^l,$$

where $\mathcal{P}$ is the covariant powerset functor, $O_1, \ldots, O_k$ are (constant) sets and Y^l denotes the l-fold cartesian product of Y for some $l \in \mathbb{N}$.

To simplify notation, we write the structure maps $\gamma : Y \to \Omega Y$ as $\gamma = \langle s, (o_i), (p_j) \rangle$. The notion of bisimulation for functors of this particular shape can be characterised as follows:

Proposition 2.2 (Characterisation of Bisimulation)**.** *Suppose* $\Omega Y = \mathcal{P}_f X \times O_1 \cdots \times O_k \times Y^l$ *and* $\gamma = \langle s, o_1, \ldots, o_k, p_1, \ldots, p_l \rangle : Y \to \Omega Y$ *is an* Ω*-coalgebra. A relation* $R \subseteq Y \times Y$ *is a bisimulation on* (Y, γ) *if and only if* *i.* $o_i(y_0) = o_i(y_1)$ *for all* $(y_0, y_1) \in R$ *and* $1 \leq i \leq k$.

ii. $(p_j(y_0), p_j(y_1)) \in R$ *for all* $(y_0, y_1) \in R$ *and* $1 \leq j \leq l$.

iii. If $(y_0, y_1) \in R$, *then for all* $z_0 \in s(y_0)$ *there is a* $z_1 \in s(y_1)$ *such that* $(z_0, z_1) \in R$.

iv. If $(y_0, y_1) \in R$, *then for all* $z_1 \in s(y_1)$ *there is a* $z_0 \in s(y_0)$ *such that* $(z_0, z_1) \in R$.

The conditions (iii) and (iv) are the well known “zig-zag conditions” of bisimulation in modal logic (see eg. [2], Section 2.10 or [14], Section 5.3).

2.2 Multimodal Languages and Logics for Coalgebras

We view Coalgebras for the functor $\Omega Y = \mathcal{P}_f X \times O_1 \cdots \times O_k \times Y^l$ as Kripke-Models and describe a finitary multimodal language to reason about them. Coalgebras for Ω give rise to (special) Kripke Models via a translation similar to the one presented in [7]. We choose to give syntax and semantics directly.

For the remainder of this section let Ω be a functor on $\mathbf{Set}$ defined by $\Omega Y = \mathcal{P}_f X \times O_1 \cdots \times O_k \times Y^l$.

Definition 2.3 (Coalgebraic Modal Logic – Syntax)**.** The multimodal language $\mathcal{L}_\Omega$ is the least set of formulas generated by the clauses

- $\bot \in \mathcal{L}_\Omega$
- For every $1 \leq i \leq k$ and $o \in O_i$, the expression $i : o$ is a formula of $\mathcal{L}_\Omega$.
- If $\varphi \in \mathcal{L}_\Omega$, then so are $\Box\varphi$, $\Box_1\varphi$, …, $\Box_l\varphi$.
- If φ, ψ in $\mathcal{L}_\Omega$, then so is $\varphi \to \psi$.

If we write the transition structure $\gamma : Y \to \Omega Y$ as $\gamma = \langle s, o_1, \dots, o_k, p_1, \dots, p_l \rangle$, the intuition corresponding to the formula $i : o$ is that the i-th observation function o_i gives the value o as result. The box operator is the well know operator from modal logic allowing us to reason about successor states. A formula $\Box_j\varphi$ is intended to denote that, after applying the function p_j, we end up in a state which satisfies φ.

This intuition is reflected (and made precise) in

Definition 2.4 (Coalgebraic Modal Logic – Semantics)**.** Suppose (Y, γ) is an Ω-coalgebra where $\gamma = \langle s, o_1, \dots, o_k, p_1, \dots, p_l \rangle : Y \to \Omega Y$.

Given $y \in Y$, the semantics of a formula $\varphi \in \mathcal{L}_\Omega$ at point y relative to the transition structure γ is inductively defined by the following clauses:

- $(Y, y) \not\models_\gamma \bot$.
- $(Y, y) \models_\gamma i : o$ if $o_i(c) = o$
- $(Y, y) \models_\gamma \Box\varphi$ if for all $y' \in s(y)$ we have $(C, y') \models_\gamma \varphi$
- $(Y, y) \models \varphi \to \psi$ if $(Y, y) \models_\gamma \psi$ or $(Y, y) \not\models_\gamma \varphi$.
- $(Y, y) \models \Box_j\varphi$, if, $(Y, p_j(y)) \models_\gamma \varphi$.

2.3 Expressive Power of Coalgebraic Modal Logic

Proposition 2.5 (Invariance under Bisimulation)**.** *Suppose $\gamma : Y \to \Omega Y$ is an Ω-coalgebra and $y_0, y_1 \in Y$ with $y_0 \leftrightarrows y_1$ and $\varphi \in \mathcal{L}_\Omega$. Then*

$$y_0 \models_\gamma \varphi \quad \textit{iff} \quad y_1 \models_\gamma \varphi.$$

Proof. By induction on the structure of φ using Proposition 2.2. $\Box$

Proposition 2.6 (Bisimilarity is logical equivalence)**.** *Suppose $\gamma = \langle s, (o_i), (p_j)\rangle : Y \to \Omega Y$ is an Ω-coalgebra.*

If $y_0, y_1 \in Y$ with $y_0 \not\leftrightarrows y_1$, then there exists a formula $\varphi \in \mathcal{L}_\Omega$ such that $y_0 \models_\gamma \varphi$ and $y_1 \not\models_\gamma \varphi$.

Proof. See [11], 4.7 and 4.8. $\Box$

3 Application to Rewriting Logic

We disregard the notion of labels in Rewrite Theory and focus on one-sorted theories with a single sort σ_0.

For multisorted signatures Σ with sorts $(\sigma_i)_{i\in I}$ and a family $X = (X_i)_{i\in I}$ of variables for each sort, we denote the freely generated term algebra by $T_\Sigma X$ and the set of terms in $T_\Sigma X$ of sort σ by $(T_\Sigma X)_\sigma$.

3.1 Rewriting with Observations and Induced Language

Definition 3.1 (Rewrite Theory with Observations)**.** Suppose $\mathrm{Th} = (\Sigma, E, \mathcal{R})$ is a rewrite theory. An *observational extension* of Th is a pair $\mathcal{E} = (\Sigma^o, E^o)$, where

- Σ^o extends Σ with new sorts and unary function symbols
- For all terms $t_0, t_1 \in T_\Sigma X$, $E^o \vdash t_0 = t_1$ iff $E \vdash t_0 = t_1$.

We call the pair $(\mathrm{Th}, \mathcal{E})$ a *rewriting theory with observations*. In this context, the set

$$\mathrm{Obs}(\mathrm{Th}, \mathcal{E}) = \{f : \sigma_0 \to \tau \in \Sigma^o \,|\, \tau \neq \sigma_0\}$$

is the set of *observers* of $(\mathrm{Th}, \mathcal{E})$ and

$$\mathrm{SelfObs}(\mathrm{Th}, \mathcal{E}) = \{f : \sigma_0 \to \sigma_0 \in \Sigma^o \,|\, f \notin \Sigma\}$$

the set of *self-observers* of $(\mathrm{Th}, \mathcal{E})$.

Definition 3.2 (Induced Language $\mathcal{L}_{(\mathrm{Th},\mathcal{E})}$)**.** Given a rewrite theory with observations $(\mathrm{Th}, \mathcal{E})$ and a family of variables $X = (X_\sigma)_{\sigma \in \mathrm{sorts}(\Sigma^o)}$, the *language* $\mathcal{L}_{(\mathrm{Th},\mathcal{E})}$ *induced by* $(\mathrm{Th}, \mathcal{E})$ is the coalgebraic modal logic induced by the signature functor

$$\Omega_{(\mathrm{Th},\mathcal{E})}Y = \mathcal{P}_f Y \times \prod_{obs:\sigma_0 \to \sigma \in \mathrm{Obs}(\mathrm{Th},\mathcal{E})} (T_\Sigma X)_\sigma \times \prod_{self \in \mathrm{SelfObs}(\mathrm{Th},\mathcal{E})} Y.$$

where we write $\mathrm{obs} : t$ for the (atomic) formula asserting that the observation defined by (the function symbol) obs yields the value (term) $t \in (T_\Sigma X)_\sigma$ and $\Box_{\mathrm{self}}$ for the formula expressing that application of (the function symbol) self results in a state satisfying φ.

Essentially along the same lines as above we develop the semantics of the language:

Definition 3.3 (Semantics of the Induced Language)**.** Suppose $(\mathrm{Th}, \mathcal{E})$ is a rewriting theory with observations and X is a family of variables for each sort σ of Σ.

A *model* of $(\mathrm{Th}, \mathcal{E})$ is a (Σ^o, E^o)-algebra A together with a function $s : [\![\sigma_0]\!] \to \mathcal{P}([\![\sigma_0]\!])$, such that whenever $\mathcal{R} \vdash_{\mathrm{RWL}} [t_0] \to [t_1]$, we have that $[\![t_1]\!]^\beta \in s([\![\sigma_o]\!]^\beta)$ for all valuations $\beta : X \to A$.

Given a model $M = (A, s)$ of $(\mathrm{Th}, \mathcal{E})$ and a valuation $\beta : X \to A$, the semantics of a formula $\varphi \in \mathcal{L}_{(\mathrm{Th},\mathcal{E})}$ is given by the standard rules for $\perp$ and $\to$, plus the following rules $(a \in A)$:

- $(M, \beta, a) \not\models \perp$
- $(M, \beta, a) \models \mathrm{obs} : s$, if $[\![\mathrm{obs}]\!](a) = [\![s]\!]^\beta$ for $\mathrm{obs} : \sigma_0 \to \sigma \in \mathrm{Obs}(\mathrm{Th})$ and $s \in (T_\Sigma X)_\sigma$.
- $(M, \beta, a) \models \Box\varphi$ if for all $a' \in s(a)$ we have that $(M, \beta, a') \models \varphi$.
- $(M, \beta, a) \models \Box_{\mathrm{self}}\varphi$, if, $(M, \beta, [\![\mathrm{self}]\!](a)) \models \varphi$, for $\mathrm{self} \in \mathrm{SelfObs}(\mathrm{Th})$.

We say that $t \in (T_\Sigma X)_{\sigma_0}$ is a model of $\varphi \in \mathcal{L}_{(\mathrm{Th},\mathcal{E})}$, if every interpretation of t satisfies φ, that is

$$t \models \varphi \quad \text{iff} \quad (M, \beta, [\![t]\!]^\beta) \models \varphi$$

for all models $M = (A, s)$ of $(\mathrm{Th}, \mathcal{E})$ and all valuations $\beta : X \to A$.

3.2 Expressive Power

We can now apply the techniques of section 2.3 to show that the logic presented is adequate in the sense that bisimilar points cannot be distinguished, while we are able to distinguish non-bisimilar points.

Theorem 3.4 (Expressive Power)**.** *Suppose* $M = (A, s)$ *is a model of a rewrite theory with observations* $(\mathrm{Th}, \mathcal{E})$.

i. Suppose $a_0, a_1 \in [\![\sigma_0]\!]$ *and* $a_0 \leftrightarrows a_1$ *with respect to the induced signature* Ω_M*. Then*

$$(M, \beta, a_0) \models \varphi \quad \textit{iff} \quad (M, \beta, a_1) \models \varphi$$

for all $\varphi \in \mathcal{L}_{(\mathrm{Th},\mathcal{E})}$.

ii. Suppose $a_0, a_1 \in [\![\sigma_0]\!]$ *with* $a_0 \not\leftrightarrows a_1$*. Then there exists a formula* $\varphi \in \mathcal{L}_{(\mathrm{Th},\mathcal{E})}$ *and a valuation* $\beta : X \to A$ *such that*

$$(M, \beta, a_0) \models \varphi \quad \textit{and} \quad (M, \beta, a_1) \not\models \varphi.$$

Proof. Combine proposition 2.5 and proposition 2.6. ☐

3.3 Examples of Rewrite Theories and Modal Formulas

We present a simple-minded example concerning the evaluation of terms by means of rewriting rules. Using modal formulas, we can formulate, that every term can be rewritten into a normal form, not allowing for more simplification.

Suppose the algebraic signature Σ consists of a single sort N and the set of function symbols $\{0 :\to N, s : N \to N, + : N, N \to N\}$ and the set E of equations is empty.

The extension Σ^o adds the sort B and the function symbols $\{\mathrm{tt} :\to B, \mathrm{ff} :\to B, \wedge : B, B \to B, \mathrm{fe} : N \to B, \mathrm{cl} : N \to B\}$. The intended meaning of the predicate fe is to denote weather a term is fully evaluated, which is formalised by the equations $E^o = \{\mathrm{fe}(0) = \mathrm{tt}, \mathrm{fe}(sx) = \mathrm{fe}(x), \mathrm{fe}(x + y) = \mathrm{ff}\}$.

Now suppose $(\mathrm{Th}, \mathcal{E})$ is a rewrite theory with observations which realises the signature Σ^o, that is $\mathrm{Th} = (\Sigma, E, \mathcal{R})$ and $\mathcal{E} = (\Sigma^o, E^o)$.

We obtain an atomic formula $\mathrm{fe} : \mathrm{tt}$ with the property that $t \models \mathrm{fe} : \mathrm{tt}$, if the term t can be denoted by a term in which the symbol "+" does not occur.

Similarly we can axiomatise a predicate cl stating that a term is closed by the equations $\mathrm{cl}(0) = \mathrm{tt}, \mathrm{cl}(sx) = \mathrm{cl}(x)$ and $\mathrm{cl}(x+y) = \mathrm{cl}(x) \wedge \mathrm{cl}(y)$ and the obvious equations for $\wedge$. The property that every closed term has a successor which is fully evaluated can then be expressed by the formula $\mathrm{cl} : \mathrm{tt} \to \Diamond \mathrm{fe} : \mathrm{tt}$. Applying this to rewriting logic, we can only express that a term has at least one successor which is fully evaluated, that is, the rewrite rules $\mathcal{R}$ are such that every closed term has a successor which is fully evaluated. However, in computational rewriting logic, the properties that every term will be eventually fully evaluated and that this evaluation terminates can be only expressed by extending the language with an always-operator.

4 First Order Translation

In the previous sections, we have presented a language which allows to express properties of certain states (terms) of models of rewrite theories, that is, we have given a formal language and its semantics, but no formal system, which can be used to derive validity of formulas in a purely syntactical manner.

We now show the modal logic described can be embedded into first order logic in a conservative way, allowing us to use formal deductive systems of first order logic. The translation we use is similar to the one presented in [1].

4.1 First Order Translation

Definition 4.1 (First Order Translation)**.** We consider the (multisorted) first order language $\hat{\mathcal{L}}_{(\mathrm{Th},\mathcal{E})}$ which consists of the sorts and function symbols of Σ^o and a binary relation $R : \sigma_0, \sigma_0$. Given a term $t \in (T_\Sigma X)_{\sigma_0}$ the *first order translation* $\varphi[t]$ of $\varphi \in \mathcal{L}_{(\mathrm{Th},\mathcal{E})}$ is defined by induction on $\mathcal{L}_{(\mathrm{Th},\mathcal{E})}$ as follows:

- $(o : v)[t] \equiv ot = v$ for $o \in \mathrm{Obs}(\mathrm{Th}, \mathcal{E})$.
- $(\neg\varphi)[t] \equiv \neg(\varphi[t])$, $(\varphi \to \psi)[t] \equiv \varphi[t] \to \psi[t]$.
- $(\Box\varphi)[t] \equiv \forall y.tRy \to \varphi[y]$, assuming that y is neither free in t nor in φ.
- $(\Box_p\varphi)[t] \equiv \varphi[pt]$ for $p \in \mathrm{SelfObs}(Th)$.

Depending on the notion of rewriting under consideration, one has to axiomatise the properties of the rewrite relation by different sets of first-order formulas. We do not make this axiomatisation explicit and take the set

$$\Phi_{\mathrm{RWL}} = \{tRt' \mid \mathcal{R} \vdash [t] \to [t']\} \cup E^o$$

as given. Note that entailment "$\vdash$" above can correspond to different notions of rewriting, and can be, for example, also instantiated with rewriting in the style of the Maude language.

Theorem 4.2. *Let* $t \in (T_\Sigma X)_{\sigma_0}$ *and* $\varphi \in \mathcal{L}_{(\mathrm{Th},\mathcal{E})}$. *Then*

$$t \models \varphi \quad \textit{iff} \quad \Phi_{\mathrm{RWL}} \vdash \varphi[t]$$

where "$\vdash$" is entailment in first order logic.

Proof. Remember that $t \models \varphi$ means that $(M, \beta, [\![t]\!]^\beta) \models \varphi$ for every model M of $(\mathrm{Th}, \mathcal{E})$. By completeness of first order logic, we can reduce the statement to showing that $t \models \varphi$ iff $\Phi_{\mathrm{RWL}} \models \varphi[t]$. Note that every model $M = (A, s)$ of $(\mathrm{Th}, \mathcal{E})$ induces a (first order) structure $\hat{M}$ for $\hat{\mathcal{L}}_{(\mathrm{Th},\mathcal{E})}$ by defining $a[\![R]\!]a'$ iff $a' \in s(a)$ (and keeping the interpretation of the sorts and function symbols).

The claim is proved by induction on the structure of φ, closely investigating validity in first order logic. $\Box$

4.2 Proof principles for bisimulation

Having established means to prove the validity of modal formulas at a particular state $t \in (T_\Sigma X)_{\sigma_0}$, we can also formulate a proof principle which allows us to establish that (the interpretation of) two terms t, t' are bisimilar in every model, namely when their first order translations $\varphi[t]$ and $\varphi[t']$ are equivalent in first order logic. This can be seen as a modal analogue of observational equality ([5], Definition 3.5) or of behavioural satisfaction ([3], Definition 5).

Let $(\mathrm{Th}, \mathcal{E})$ be a rewrite theory with observations. We call two terms $t, t' \in (T_\Sigma X)_{\sigma_0}$ *bisimilar*, if, for every model $\mathcal{M} = (A, s)$ of $(\mathrm{Th}, \mathcal{E})$ and every valuation $\beta : X \to A$, we have $[\![t_0]\!]^\beta \leftrightarroweq [\![t_1]\!]^\beta$, where bisimilarity is wrt the induced coalgebraic signature Using this definition, we can prove

Proposition 4.3 (Proof Principle for Bisimulation)**.** *Suppose $t, t' \in (T_\Sigma X)_{\sigma_0}$. Then t_0 is bisimilar to t_1 if and only if*

$$\forall \varphi \in \mathcal{L}_{(\mathrm{Th},\mathcal{E})}.\Phi_{\mathrm{RWL}} \vdash \varphi[t_0] \iff \Phi_{\mathrm{RWL}} \vdash \varphi[t_1].$$

Proof. Use theorem 3.4 and theorem 4.2. □

References

[1] H. Andreka, J. van Benthem, and I. Nemeti. Back and forth between modal and classical logic. *J. of the IGPL*, 3(5):685–720, 1995.

[2] Alexander Chagrov and Michael Zakharyaschev. *Modal Logic*, volume 35 of *Oxford Logic Guides*. Oxford Science Publications, 1997.

[3] J. Goguen and G. Malcolm. A hidden agenda. Technical Report CS97-538, UCSD, 1997.

[4] Robert Goldblatt. *Logics of Time and Computation*, volume 7 of *CSLI Lecture Notes*. Center for the Study of Language and Information, Stanford University, 1992. Second Edition.

[5] R. Hennicker and M. Bidoit. Observational logic. In *Proc. AMAST '98, 7th International Conference on Algebraic Methodology and Software Technology*, number 1548 in Lecture Notes in Computer Science. Springer, 1999.

[6] B. Jacobs and J. Rutten. A tutorial on (co)algebras and (co)induction. *EATCS Bulletin*, 62, 1997.

[7] Alexander Kurz. Specifying coalgebras with modal logic. In B. Jacobs, L. Moss, H. Reichel, and J. Rutten, editors, *Coalgebraic Methods in Computer Science (CMCS'98)*, volume 11 of *Electronic Notes in Theoretical Computer Science*, pages 57–72, 1998.

[8] Narciso Martí-Oliet and José Meseguer. Rewriting logic as a logical and semantic framewor. In *Proc. 1st Intl. Workshop on Rewriting Logic and its Applications*, Electronic Notes in Theoretical Computer Science. Elsevier, 1996.

[9] José Meseguer. Research directions in rewriting logic. In U. Berger and H. Schwichtenberg, editors, *Computational Logic*, NATO Advanced Study Institute. Springer, 1998.

[10] M.Hennesy and R.Milner. Algebraic laws for non-determinism and concurrency. *Journal of the ACM*, 32:137 – 161.

[11] Martin Rößiger. Coalgebras and modal logic. In *Coalgebraic Methods in Computer Science (CMCS'00)*, volume 33 of *Electronic Notes in Theoretical Computer Science*, 2000.

[12] Jan Rutten. Universal coalgebra: A theory of systems. *Theoretical Computer Science*. To appear.

[13] Jan Rutten. Universal coalgebra: A theory of systems. Technical Report CS R 9652, CWI, Amsterdam, 1996.

[14] Colin Stirling. Modal and temporal logics. In S. Abramsky, D. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 2. Oxford Science Publications, 1992.