Effective behaviour algebras

Philippe Darondeau, Serge Yoccoz

INRIA

UNITÉ DE RECHERCHE
INRIA-RENNES

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél.:(1) 39 63 55 11

Rapports de Recherche

N° 776

EFFECTIVE BEHAVIOUR ALGEBRAS

Philippe DARONDEAU
Serge YOCCOZ

DECEMBRE 1987

IRISA

INSTITUT DE RECHERCHE EN INFORMATIQUE
ET SYSTÈMES ALÉATOIRES

Campus Universitaire de Beaulieu
35042 - RENNES CÉDEX
FRANCE
Téléphone : 99 36 20 00
Télex: UNIRISA 950 473 F
Télécopie : 99 38 38 32

EFFECTIVE BEHAVIOUR ALGEBRAS

Philippe DARONDEAU* (CNRS RENNES)
Serge YOCCOZ* (CNRS BORDEAUX)

* IRISA, Campus de Beaulieu, F35042 RENNES CEDEX
**UER de Mathématiques et Informatique,
Université de Bordeaux I,
230 cours de la Libération, F33400 TALENCE

Publication interne n° 383 - Novembre 87 - 18 pages.

abstract : This paper is an attempt to define effective behaviour algebras and effective (i.e. provable) behaviour equivalences. It offers thereby a defense and illustration of the thesis asserting the identity between effective infinitary objects and $\sum_1^1$ sets (and transformations). In this framework, an effective equivalence of indiscernibility is defined, and its logical and topological properties are investigated.

ALGEBRES EFFECTIVES DE COMPORTEMENTS

Résumé : Cet article tente de définir des algèbres effectives de comportements, et des équivalences effectives (c.a.d. prouvables) sur ces algèbres. Il offre par là même une défense et une illustration de la thèse selon laquelle les objets infinitaires effectifs sont essentiellement les ensembles $\sum_1^1$ de $\mathbb{N} \rightarrow \mathbb{N}$ (et leurs transformations). Dans ce cadre, nous introduisons une équivalence effective d'indiscernabilité, et étudions ses propriétés logiques et topologiques.

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE
(L. A. 227)
UNIVERSITÉ DE RENNES 1 I. N. S. A. DE RENNES

INSTITUT NATIONAL DE RECHERCHE
EN INFORMATIQUE ET EN AUTOMATIQUE
(LABORATOIRE DE RENNES)

I Introduction :

Recent work on behaviour algebras such as CCS, TCSP, ACP... has renewed the study of effective transitions systems (t.s for short) and their equivalences [1,2,3,4]. We feel that these equivalences are either too liberal or too strict with respect to infinite behaviours of t.s . Indeed, equivalences really accounting for infinite behaviours fail in the following sense: they have no complete proof systems in first order logic, even with recursive infinitary rules[5], such as complete induction . Our goal is to fill in this gap .

By an effective family of t.s [7], we mean a quintuple $(S, \psi_S, A, \psi_A, f)$ where $\psi_S : S \longrightarrow \mathbb{N}$, resp. $\psi_A : A \longrightarrow \mathbb{N}$ are bijective codings for states, resp. actions , and f is a recursive function enumerating triples $\langle \psi_S(s), \psi_A(a), \psi_S(s') \rangle$, standing for transitions

$s \xrightarrow{a} s'$. A transition system of the family is then given by an initial state s_0.

By an effective algebra of t.s, we mean a family of t.s whose set of states S is an algebra of terms (the operators of the algebra are then induced by the corresponding operators on terms) . In such algebras, one may introduce computations of a t.s as sequences of transitions

$$(s_i \xrightarrow{a_i} s_{i+1}) \ , \ i \leq \gamma$$

between terms, where $\gamma \in \mathbb{N} \cup \{\omega\}$. Clearly, for any term of the algebra, identified with the corresponding transition system, the set of computations of that term may be represented as a Σ^1_1 set of $(\mathbb{N} \rightarrow \mathbb{N})$, i.e a set of the form [6]

$\{f/(\exists g)(\forall i)R(f,g,i)\}$ where R is recursive relation . Further, the operators of the algebra induce operators on Σ^1_1 sets, recursive on their Σ^1_1 codes . The same holds for the alternative behaviour algebra, obtained by erasing states from computations and still holds if some actions are considered as invisible and thus are erased from traces (e.g τ in CCS) .

Conversely, we know effective algebras of t.s, namely MEIJE resp. CCS, in which any Σ^1_1 set of $(\mathbb{N} \rightarrow \mathbb{N})$ represents the behaviour (complete traces resp. visible traces) of a term, given from the code of the set by a recursive procedure (for MEIJE, this results mainly from the two theorems by de Simone queted in [7]) .

This comes as a confirmation of the following thesis :

* Effective infinitary objects are (at most) Σ^1_1
* Effective operations on effectived infinitary objects are Σ^1_1 transformations, i.e they are union additive extensions of relations whose graph is Σ^1_1 .

On behalf of this thesis, we exclude from effective behaviour algebras the factor algebras (of t.s) obtained by greatest bisimulations [8]: not only classes of these equivalences are Π^1_2 sets of terms, but the quotient of an effective transition system by its greatest bisimulation is not always an effective t.s .

In the sequel, we study only linear behaviour of t.s : such behaviours are essentially the Σ^1_1 sets (of $(\mathbb{N}\longrightarrow\mathbb{N})$) .

It appears from the last remark that the existence of complete proof systems for behavioural equivalences of t.s reduces to the corresponding problem for equivalences between Σ^1_1 sets .

Traditionally, proof systems used in Computer Science are defined within first-order logic with recursive infinitary rules (these rules are generally used for complete induction on $\mathbb{N}$ - algorithmic logic- or on more structured domains - Scott's complete induction). We claim that this logical framework is powerful enough to formalize infinitary properties which are not finitely approximable and thus not inductive in the usual sense . Although no complete axiomatization for equality between Σ^1_1 sets can be obtained in this logical fragment [5], the problem is trivial in any fragment of second-order logic . We introduce in the next section a coarser equivalence between Σ^1_1 sets, which is even a congruence for Σ^1_1 transformations, and show that it has a complete proof system in RL (first order logic with recursive infinitary rules) . Furthermore, we believe that this equivalence is the finest equivalence between Σ^1_1 sets provable in RL .

II Indiscernibility as a provable congruence on Σ^1_1 sets :

1) Σ^1_1 sets and transformations :

In the sequel, f,g... range over $\mathcal{N} = (\mathbb{N} \longrightarrow \mathbb{N})$; A,B,... over $P(\mathcal{N})$. Similarly, i,j,... range over $\mathbb{N}$; a,b,... over $P(\mathbb{N})$.

A subset A of $\mathcal{N}$ (resp. a subset a of $\mathbb{N}$) is Σ^1_1 iff there exists a recursive relation R such that

$$A = \{f / (\exists g)(\forall i) R(f,g,i)\}$$

(resp. $a = \{k / (\exists g)(\forall i) R(k,g,i)\}$) .

A Σ^1_1 transformation Φ on $P(\mathcal{N})$ is the union additive extension of a function $\varphi : \mathcal{N} \longrightarrow P(\mathcal{N})$ such that

$$\{(g,f) / g \in \varphi f \} \text{ is } \Sigma^1_1 .$$

It is easy to see that Σ^1_1 transformations preserve Σ^1_1 sets .

2) Σ^1_1 indiscernibility :

For A,B Σ^1_1 subsets of $\mathcal{N}$, we say that A and B are Σ^1_1 indiscernible ($A \sim_\Sigma B$) iff

for any Σ^1_1 subset C of $\mathcal{N}$, $A \cap C = \emptyset \iff B \cap C = \emptyset$.

Clearly, $\sim_\Sigma$ is an equivalence, and moreover a congruence with respect to Σ^1_1 transformations . This follows from two immediate properties :

(i) The class Σ_1^1 is closed under intersection

(ii) For any Σ_1^1 transformation Φ,

$\Phi^{-1}(A) = \{f / (\exists g \in A) g \in \varphi(f)\}$ is a Σ_1^1 transformation .

3) Recursive logic :

We consider Ω, a denumerable and possibly multisorted algebra of terms with variables, and $L(\Omega)$, a first order language constructed in the usual way from Ω and some finite family of relational symbols .

A proof system Σ with recursive infinitary rules is a triple $\langle AX, R, IR \rangle$ where :

* AX is a finite consistent set of formulas from $L(\Omega)$ (the axioms) .

* R is a set of finitary inference rules, written $A \Leftarrow A_1, \ldots, A_n$ with $A, A_1, \ldots, A_n$ belonging to $L(\Omega)$.

* IR is a set of recursive infinitary rules, written $A \Leftarrow A_1, \ldots, A_i, \ldots$ each of which is associated with an effective procedure P such that $P(i) = A_i$ for all i in $\mathbb{N}$.

Proofs in Σ may be defined inductively as finite-path trees whose terminal roots are the concluding stepd of proof .

A formula φ is provable in Σ if :

* φ is an instance of a provable formula ψ ,

* φ belongs to AX ,

* $\varphi = \sigma(A)$ and there are substitutions $\sigma_1, \ldots, \sigma_n$; $\tau_1, \ldots, \tau_n$ such that for all i , $\sigma = \sigma_i \tau_i$ and $\tau_i(A_i)$ is provable in Σ and

$A \Leftarrow A_1, \ldots, A_n$ belongs to R ,

* $\varphi = \sigma(A)$ and there are substitutions σ_i, τ_i ($i \in \mathbb{N}$) such that for all i , $\sigma = \sigma_i \tau_i$ and $\tau_i(A_i)$ is provable in Σ and $A \Leftarrow A_1, \ldots, A_i, \ldots$ belongs to IR .

4) <u>A theorem</u> :

<u>Theorem</u> : There exists a complete proof system for $\sim_\Sigma$ in RL .

5) <u>Complements</u> [6]:

* <u>Kleene normal form theorem for Σ_1^1 sets</u> . For $k \geq 0$ and $l \geq 0$, there exist recursive predicates

$$T'_{k+1,l}(z, f_1, \ldots, f_k, g, x_1, \ldots, x_l, w)$$

where z, $x_1, \ldots, x_l$, w are integer variables, such that for any Σ_1^1 set R, $R \subseteq \mathcal{N}^k \times \mathbb{N}^l$ there is a z such that

$R = \{ \langle f_1, \ldots, f_k, x_1, \ldots, x_l \rangle / (\exists g)(\forall w) \text{ not } T'_{k+1}(z, \mathbf{f}, g, \mathbf{x}, w) \}$

z is then called a Σ_1^1 index for R .

* <u>Π_1^1 , Δ_1^1</u> .

A subset A of $\mathcal{N}$ (resp. a of $\mathbb{N}$) is a Π_1^1 set iff $\mathcal{N} - A$ is a Σ_1^1 set (resp. $\mathbb{N} - a$ is Σ_1^1 set) .

A subset A of $\mathcal{N}$ (resp. a of $\mathbb{N}$) is a Δ_1^1 set iff it is both a Σ_1^1 and a Π_1^1 set .

* <u>Π_1^1-completeness</u> .

A set A is one-one reducible to a set B ($A \leq_1 B$) if there is a one-one recursive function f such that

$$(\forall x)\ [x \in A \iff fx \in B] .$$

A set A is Π_1^1 complete if and only if $B \leq_1 A$ for every Π_1^1 set B.

The set T of finite path trees is Π^1_1 complete (and thus the same holds for proof trees in RL) .

6) Hints for the proof of the theorem :

Notations : $\Sigma_f(x)$ is the Σ^1_1 subset of $\mathcal{N}$ of Σ^1_1 index x .

$\Sigma_N(x)$ is the Σ^1_1 subset of $\mathbb{N}$ of Σ^1_1 index x .

Lemma 1 : Problems $\Sigma_f(x) \sim_\Sigma \Sigma_f(y)$ and $\Sigma_N(x') = \Sigma_N(y')$ are effectively inter-reducible .

Notation : For any theory Θ, RL(Θ) stands for the following assertion :

" There is a complete proof system for Θ in RL "

Lemma 2 : RL($\Sigma_N(x) = \Sigma_N(y)$) is equivalent to

RL($(\forall f)(\exists j)T'_{1,1}(z,f,j)$) & RL($(\exists f)(\forall j)$not $T'_{1,1}(z,f,j)$)

(The recursive infinitary rule

$$\Sigma_N(x) = \Sigma_N(y) \Leftarrow (i \in \Sigma_N(x) \Longleftrightarrow i \in \Sigma_N(y))_{i \in N}$$

is clearly valid and complete) .

Lemma 3 : RL($(\exists f)(\forall j)$ not $T'_{1,1}(z,f,j)$)

(Introduce the infinitary rule

$$(\exists f)(\forall j)\text{not } T'_{1,1}(z,f,j) \Leftarrow (\text{not } T'_{0,i+1}(h(x,i),y_0,\ldots,y_i,i))_{i \in N}$$

where h(x,i) is the recursive function such that

$T'_{1,1}(x,f,i) \Longleftrightarrow T'_{0,i+1}(h(x,i),y_0,\ldots,y_i,i)$ if $f(j) = y_j$.

Lemma 4 : RL ($(\forall f)(\exists j)$ $T'_{1,1}(x,f,j)$)

(Let FPT(φ_z) mean : the recursive function φ_z of index z is the characteristic function of a finite path tree . Then

(i) there is a recursive function p such that

$$(\forall f)(\exists j)\ T'_{1,1}(x,f,j) \Longleftrightarrow \text{FPT}(\varphi_{p(x)})$$

(ii) $FPT(\varphi_z)$ is provable with the help of the recursive infinitary rule :

$FPT(\varphi_z) \Leftarrow (\varphi_z(i) = 0 \text{ or } FPT(\varphi_{h(z,i)}))_{i \in N}$

where $\varphi_{h(z,y_0)}(k) = \varphi_z(l)$ for $k = \langle y_1, \ldots, y_n \rangle$ and $l = \langle y_0, \ldots, y_n \rangle$

III Effective behaviour algebras :

* Summary :

On behalf of our thesis on effective infinitary objects and transformations (cf. Section I) an effective behaviour algebra must satisfy :

(i) the behaviour of a term is a Σ^1_1 subset of $\mathcal{N}$

(ii) the operators in duced by contexts are Σ^1_1 transformations .

So any effective algebra factors through $\sim_\Sigma$ into another effective behaviour algebra whose equality is provable - we conjecture that $\sim_\Sigma$ is the finest equivalence with this nice property .

We delineate in the remaining of this section two generic behaviour algebras which are effective according to our thesis (and cover all models cuurently developped for linear behaviour of concurrent systems) :

* the first model is generic for initial linear models (sets of infinitary transitions sequences)

* the second model is generic for the usual abstraction

therefrom (e.g sets of infinitary traces) .

(a) A generic framework for operational models :

Programming languages under concern are usual term algebras with additional combinators for recursion . Among the latter, one may think of the the rec combinator used in most process algebras - e.g rec(x).t(x) - or more generally of the let-rec combinator of ML .

A possible way to define effective transition systems whose states are terms of the programming language, is to follow the well known method of structured operational semantics [9]due to G.Plotkin . As far as all the side conditions of the inference rules are partial recursive (which is certainly reasonable) , this operational definition results in one global transition system per programming languge, but it is clear that one may also consider the result as an effective algebra of transition systems (defined in the introduction) . Since transition systems are faithfully represented by corresponding sets of (infinitary) transition sequences, th above algebra of transition systems induces an effective poweralgebra of transition sequences .

Let the infinitary sequences of labelled transitions between terms be represented as usual in $\mathcal{N}$; then, the elements of the power algebra become Σ_1^1 subsets of $\mathcal{N}$ and the operators of the poweralgebra are recursive on their Σ_1^1 indexes . But even better, we know from recent work that these operators are union additive extensions of operators $\varphi : \mathcal{N}^n \longrightarrow P(\mathcal{N})$ whose 'graph' $(\{\langle x,y\rangle / y \in \varphi x\})$ is Σ^1_1 - so they are Σ^1_1 transformations .

Now, as regards combinators for recursion, we have shown that they lead naturally to greatest fixpoints with respect to inclusion if the recursive definition satisfies the Greibach condition . But $\lambda U . gfp_X\ F(U,X)$ is a Σ^1_1 transformation if $F(U,X)$ is a Σ^1_1 transformation of U and X . To sum up, all contexts in the programming language induce Σ^1_1 transformations in the corresponding poweralgebra, which is thus an effective behaviour algebra .

The same holds, independently of structural operational semantics, as long as the operational specification of the operators on terms (resp. of the combinators for recursion) gives rise to Σ^1_1 transformations (resp. to greatest fixpoints with respect to inclusion) .

(b) A generic framework for abstraction :

We consider here behaviour algebras derived from the aboved initial algebras through morphisms of poweralgebras, which forget irrelevant details from computations . More precisely, we assume abstraction morphisms α of the form $\alpha = \beta_\circ \gamma$, where γ is any Σ^1_1 transformation (e.g erasing of states, or extraction if infinitely repeated states...) and β is a closure operator with respect to some recursive order on $\gamma(\mathcal{N})$, chosen among the following family which reflects the three versions of powerdomains : downwards closure, convex closure, upwards closure .

Beside being morphisms of algebras, we ask our abstraction morphisms to satisfy the requirement expressed by the commutation of the diagram

$$
\begin{tikzcd}
A_{init} \arrow[r, "\lambda U.\,gfp_X\ F(U,X)"] \arrow[dd, "\lambda Y.\bigcup\,[Y]_\alpha"'] & A_{init} \arrow[dr, "\alpha"] & \\
& & A_{abs} \\
A_{init} \arrow[r, "\lambda U.\,gfp_X\ F(U,X)"] & A_{init} \arrow[ur, "\alpha"'] &
\end{tikzcd}
$$

where . A_{init} is the behaviour algebra defined in II a)

. A_{abs} is $\alpha(A_{init})$ and

. $\lambda Y.\bigcup\,[Y]_\alpha$ is the operator $\lambda Y.\alpha^{-1}(\alpha(Y))$

The intuition behind the diagram is the following : given a recursively defined program C[u] with subprogram u, you may as often as you wish, during an execution of C[u], substitute without damage successive versions u_n of u such that $u_n \sim_\alpha u$, where $\sim_\alpha$ is the obvious equivalence (dynamic adaptation of concurrent programs) . Any morphism α satisfying the above yields an effective behaviour algebra A_{abs}, because the derived interpretations for recursive contexts are then Σ^1_1 transformations .

Examples : 1) γ may be the erasure of states, and β may be closure under prefix-ordering .

2) γ may also erase some actions considered as invisible (e.g τ in CCS or ACP_τ)

3) See [10] for a more complex abstraction yielding a model of CCS in which

$u = v$ iff u and v have identical sets

of infinitary interactions with any program t set in parallel.

IV Topological and metric properties of indiscernibility :

a) The closure operator induced by $\sim_\Sigma$:

For A a Σ^1_1 subset of $\mathcal{N}$, let $A^\frown$ be the the union of all Σ^1_1 subsets B of $\mathcal{N}$ such that $A \sim_\Sigma B$.

The following characterizations of $A^\frown$ are an easy consequence of a result by Louveau [11]:

$A^\frown = \bigcap \{C\ \Pi^1_1 \text{ subset of } \mathcal{N} \ / \ A \subseteq C\} = \bigcap \{C\ \Delta^1_1 \text{ subset of } \mathcal{N} \ / \ A \subseteq C\}$

and $A^\frown$ is the largest Σ^1_1 set in the equivalence class of A .

Besides, the closure operator $(.)^\frown$ satisfies de Morgan's laws .

b) Generalizing $\sim_\Sigma$ into $\sim_\Delta$:

For A, B Σ^1_1 subsets of $\mathcal{N}$, let $A \sim_\Delta B$ iff for any Δ^1_1 subset C of $\mathcal{N}$, $A \cap C = \emptyset \Longleftrightarrow B \cap C = \emptyset$.

The above characterization shows that $A \sim_\Sigma B \Longleftrightarrow A \sim_\Delta B$.

We consider from now on generalized definitions of relations $\sim_\Sigma$ and $\sim_\Delta$ for arbitrary sets A and B . In this generalized framework where the last equivalence is no longer valid, it appears that $\sim_\Delta$ has nicer topological properties than $\sim_\Sigma$.

For A in $P(\mathcal{N})$, let $\overline{A}$ be the intersection of all Δ^1_1 subsets C of $\mathcal{N}$ such that $A \subseteq C$. Then $(\overline{\ })$ is a closure operator inducing a topology T_Δ on $\mathcal{N}$, $A \sim_\Delta B \iff \overline{A} = \overline{B}$, and $\overline{A}$ is the largest Borel set in the equivalence class of A .

c) <u>The topology T_Δ</u> :

T_Δ has a clopen basis, namely the family of Δ^1_1 subsets of $\mathcal{N}$ (but all clopen sets are not Δ^1_1) .

$(\mathcal{N}, T_\Delta)$ is metrizable, but it is neither compact nor locally compact .

The family of isolated points is exactly the family of Δ^1_1 singleton sets.

The latter family is not dense, whereas the Π^1_1 singleton sets form a dense family .

d) <u>Continuous functions</u> :

Although we have no full characterization of continuous functions for T_Δ , we know two important classes of continuous functions, namely :

(i) funtions whose graph is Σ^1_1 (thus including Σ^1_1 transformations) ;

(ii) functions whose graph is the union of a Σ^1_1-indexed family of Δ^1_1 sets (where indexes are Δ^1_1 codes) .

In general, any continuous function is also a closed mapping, since $A\sim_\Delta B$ implies $fA\sim_\Delta fB$ for continuous f . As a consequence, $\sim_\Sigma$ is a congruence with respect to set-extensions of T_Δ-continuous functions .

e) A metric for T_Δ :

Let x,y be in $\mathcal{N}$. An ultrametric distance d(x,y) compatible with T_Δ is defined by

$d(x,y) = 2^{-n}$ where n is the smallest Σ^1_1 index of a Δ^1_1 set C such that $x \in C \Longleftrightarrow y \notin C$.

$= 0$ if there is no such separating set (x=y in this case) .

But no distance compatible with T_Δ makes $\mathcal{N}$ into a complete metric space, so it makes sense to find completions of $(\mathcal{N},d)$.

V Directions for further research :

A first subject of investigation is the logic RL, both from model theoretic and proof theoretic points of view . In particular, the problem of whether the indiscernibility of behaviours is liable to RL proofs in a language built around terms of behaviour algebras, is worth consideration. Another concern about indiscernibility is to show that it is really the finest equivalence (on Σ^1_1) provable in RL . We conjecture that it is also the finest testable equivalence in the sense of effective binary tests (extending De Nicola and Hennesy's tests) . Since the separating sets on which relies indiscernibility are Δ_1^1 sets, one may imagine a strong connection between tests and Δ_1^1 behaviours . A natural question is then the operational meaning of Δ_1^1 sets . A related topic is the search for general (not necessarily profinite) specification techniques for Σ_1^1 transformations, and more generally for T_Δ-continuous functions . This sujpposes of course that we obtain beforehand a full characterization of continuous functions . A last topic, with possible implications in formal language theory, is the (metric) completion of $(\mathcal{N},T_\Delta)$. We have some reasons to believe that bi-infinite words come here into play .

Bibliography

[1] Milner,R. A Calculus of Communicating Systems,

2] De Nicola,R. Hennessy,M. Testing equivalences for processes TCS 34 (1984)

[3] Brook,S.D. Hoare C.A.R. Roscoe A.W A theory of communicating sequential processes JACM 31 (1984)

[4] Bergstra, J.A Klop, J.W Algebra of communicating processes with abstraction TCS 37 (1985)

[5] Darondeau,P. Yoccoz,S. Proof systems for infinite behaviours INRIA report n°632, to appear in Information and Computation

[6] Rogers,H.: Theory of recursive functions and effective

computability MacGraw Hill (1967)

[7] Boudol,G. Notes on algebraic calculi of processes
in Logics and Models of concurrent systems,
K.Apt ed. Springer Verlag (NATO SAI Series 1985)

[8] Park, D. Concurrency and automata on infinite sequences
Springer Verlag LNCS 84 (1980)

[9] Plotkin,G. A structural approach to operational semantics
Daimi report fn 19 University of Aarhus (1981)

[10] Darondeau,P. Gamatie,B. A fully observational model for
infinite behaviours of communicating systems .
Springer Verlag LNCS 249 (1987)

[11] Louveau,A. Relations d'equivalence co-analytiques
Séminaire Choquet d'Initiation à l'Analyse
16e année (1976-77) I.H.P.

****

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique