Axiomatizing process algebra with time:

real-time and stochastic-time

Mario Bravetti
Università di Bologna

Parts are joint work with: Roberto Gorrieri

1. Basic priority: maximal progress

- Extension of the *standard Milner's sound and complete axiomatization* when a new "δ" prefix is introduced representing a *time delay*.
- If we assume that time may elapse only when no standard action can be performed (*maximal progress assumption*) then such extension is not trivial.
- Tecnically, we assume a simple form of *priority of "τ" actions over "δ" actions*: visible actions are interpreted as representing *potential for execution* only.

1.1 The basic calculus

- Similarly as for standard CCS we start from axiomatizing a *basic calculus with recursion*:

$$P ::= \underline{0} \mid \pi.P \mid P + P \mid RecX.P \mid X$$

where "$\pi.P$" is either "$\alpha.P$" (α is a or τ) or "$\delta.P$".

- The operational semantics of this calculus is a simple variant of the standard one:

$$\frac{P \xrightarrow{\delta} P' \quad Q \not\xrightarrow{\tau}}{P + Q \xrightarrow{\delta} P'}$$

- model of *"$\delta.P + \tau.Q$" is isomorphic to "$\tau.Q$"*.

1.2 Weak bisimulation equivalence

- The notion of equivalence is *just standard Milner's observational bisimulation equivalence* where *"δ" is treated as a visible action*.
- Technically, when we'll consider static operators we'll need *a slightly different treatment of "δ" and visible actions*: in observational congruence after an (intial) "δ" step we do not consider weak bisimulation, but still observational congruence.
- In any case it is a *conservative extension of Milner's observational congruence*.
- It is a *congruence* for our prioritized calculus!

1.3 Problems with standard axiomatization

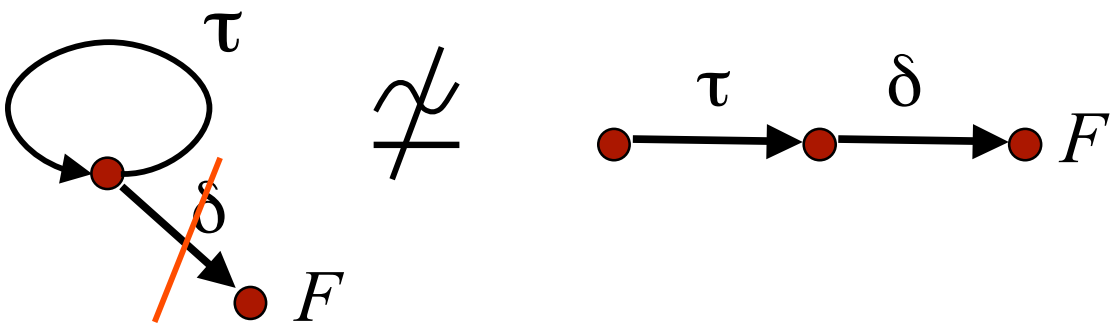
- We have problems with the *soundness of the axioms for unguarded recursion* (the second one):

  (Ung1) $Rec X.(X + E) = Rec X.E$

  (Ung2) $Rec X.(\tau.X + E) = Rec X.\tau.E$

  (Ung3) $Rec X.(\tau.(X + E) + F) = Rec X.(\tau.X + E + F)$

- The problem arises when *E is "δ.F"* in (Ung2).



1.4 A solution based on "scope"

- The role of (Ung2) is important! It *equates τ-divergent expressions to non-divergent ones*.
- A previous proposal (Hermanns – Lorey '98) solved the problem by using an *equivalence which is sensible to τ-divergence*.
- Idea: introducing a new operator "*pri(E)*" which computes the *prioritized behavior of E*! (removes initial "δ" transitions and subsequent behaviors).
- The new axiom is:

  (Ung2) $RecX.(\tau.X + E) = RecX.\tau.pri(E)$

1.5 A complete axiomatization

- Priority:

(Pri1)	$pri(\underline{0})$	$= \underline{0}$
(Pri2)	$pri(\alpha.E)$	$= \alpha.E$
(Pri3)	$pri(\delta.E)$	$= \underline{0}$
(Pri4)	$pri(E + F)$	$= pri(E) + pri(F)$
(Pri5)	$pri(pri(E))$	$= pri(E)$
(Pri6)	$\tau.E + F$	$= \tau.E + pri(F)$

- Note: "$\tau.E + \delta.F = \tau.E$" is a special case

- Unguarded recursion:

(Ung1)	$RecX.(X + E)$	$= RecX.E$
(Ung2)	$RecX.(\tau.X + E)$	$= RecX.\tau.pri(E)$
(Ung3)	$RecX.(\tau.(X+E)+F)$	$= RecX.(\tau.X+E+F)$
(Ung4)	$RecX.(\tau.(pri(X)+E)+F)$	$= RecX.(\tau.X+E+F)$

- (Ung4) is needed to *remove weakly unguarded occurences of pri(X)* introduced by new (Ung2)
- The proof is based on unique solution of standard equation sets whose characterization is a variant of the standard Milner's one.

1.6 Problems with parallel operator

- If *local priority* are assumed (e.g. in "$\tau.E \mid \delta.F$", δ is not pre-empted) then we obtain a calculus for which observational equivalence *is a congruence*:
  - we need to deal with locations in the semantics!
- In the case of *global priority* (e.g. in "$\tau.E \mid \delta.F$", δ is pre-empted):

$$\frac{P \xrightarrow{\delta} P' \quad Q \not\xrightarrow{\tau}}{P \,||\, Q \xrightarrow{\delta} P' \,||\, Q}$$

observational equivalence *is not a congruence*!

1.7 The problem with global priority

- $RecX.\tau.\, X \simeq \tau.\underline{0}$ but

  $RecX.\tau.\, X \,||\, \delta.\underline{0} \not\simeq \tau.\underline{0} \,||\, \delta.\underline{0}$

- The problem with congruence in the global priority approach is related to the behavior of parallel in the presence of *processes which may execute neither "τ" prefixes, nor "δ" prefixes*.

- Such processes (among which is *"$\underline{0}$"*) are managed as allowing *any amount of time to elapse* before executing visible prefixes (if any).

- On the contrary, *observational equivalence* treats them as *processes which do not allow time to elapse*: e.g. "$\tau.\underline{0}$" is equivalent to "$Rec X.\tau.\ X$", i.e. time deadlock.
- A possible solution, adopted, e.g., in Hermanns-Lohrey '98, is *to consider a finer notion of equivalence which is sensitive to τ-divergence*, so to get a congruence.

2. Discrete real-time

- In the discrete real-time approach elapsing of time is represented, exactly as in our basic calculus, by a *special action "δ" called a "tick"*.
- In this context *simple solution* to the problem of introducing parallel in the basic calculus:
  - *adopting the particular form of priority in the Hennessy-Regan calculus which is neither local nor really global, but is specialized for time*.

2.1 The Hennessy-Regan approach

- The parallel operator in such a calculus allows for time to elapse in a process only when the other process *may explicitely allow* for time to pass via δ transitions:

$$\frac{P \xrightarrow{\delta} P' \quad Q \xrightarrow{\delta} Q'}{P \,||_S\, Q \xrightarrow{\delta} P' \,||_S\, Q'}$$

- This is similar to global priority, but *changes the interpretation of processes which may execute neither "τ" prefixes nor "δ" prefixes* as desired: e.g. now "$\underline{0}$" is correctly treated as a time-deadlock from the parallel operator as well!

2.2 New prefix and choice operators

- The calculus that we consider (for specifications):

$$P ::= \underline{0} \mid \pi.P \mid P \underline{+} P \mid P \|_S P \mid P/L \mid RecX.P \mid X$$

- Old "π . *P*" and "*P* + *Q*" are auxiliary operators
- The *new operator "π . P"* is defined to be *"RecX (δ. X + π.P)" if "π" is visible* (it must be explicitely allowed to be delayed), "π . *P*" otherwise.
- The *new operator "P + Q"* is defined in such a way that the execution of *delays* by "P" or "Q" (now used just to represent time passage) *does not resolve the choice* (they must synchronize).

2.3 Axiomatization of new operators

- Complete axiomatizations for the new "$\pi \,.\, P$" and "$P \pm Q$" operators and the parallel operator are produced by turning terms into *normal forms*:

  terms of the basic calculus

- For parallel and "new" choice this is done in a standard way by introducing *auxiliary operators*:
  - left and syncronization merge for parallel
  - analogous of *synchronization merge* for choice

3. Markovian stochastic time

- Elapsing of time is represented by *special prefixes "λ"* (λ is a real number), denoting *time delays with a probabilistic duration*:
  - a (continuous) exponential distribution with parameter "λ" (intuitively *the speed* of the delay).
- Limitation to exponential distributions:
  - *parallel* of delays is simply *their interleaving*
  - we get a simple *Continuous-time Markov Chain*
- We consider a trivial variant of the basic calculus:
  - *numerical "λ" prefixes replace the "δ" prefix* and "λ" transitions are matched according to *standard Markovian bisimulation*.

3.1 Introducing a parallel operator

- Extending the basic Markovian calculus with the parallel operator is not trivial and presents exactly the same problems that we have explained.
- If we consider a parallel operator with a *global priority mechanism* then we have to *modify the notion of weak bisimultion equivalence* that we consider so to get a congruence.
- This is exactly the case of Hermann's *calculus of Interactive Markov Chains* which adopts a notion of *bisimulation sensible to τ-divergence*.

3.2 A technique à la Hennessy-Regan

- An alternative way is to adopt a technique similar to the Hennessy-Regan one where we say that *time is allowed to pass for a process only if the other one may explicitely make it pass*:

$$\frac{P \xrightarrow{\lambda} P' \quad Q \xrightarrow{\lambda'}}{P \,||_S\, Q \xrightarrow{\lambda} P' \,||_S\, Q}$$

- This has the advantage of relying on a *simpler and coarser notion of equivalence*.

3.3 The calculus

- The calculus that we consider (for specifications):

$$P ::= \underline{0} \mid \pi_{\cdot}.P \mid P \underline{+} P \mid P \parallel_S P \mid P/L \mid RecX.P \mid X$$

  where "$\pi_{\cdot}.P$" is either "$\alpha_{\cdot}.P$" (α is a or τ) or "$\lambda_{\cdot}.P$".

- Old "π . P" and "$P + Q$" are auxiliary operators. The new operators "π $\underline{.}$ P" and "$P \underline{+} Q$" are defined similarly as for the discrete real-time case.

- The new prefix and choice operators allow for an even coarser notion of equivalence which *abstracts from exponential selfloops* (they can never be unfolded by an operator like "+").

3.4 Complete axiomatization

- Complete axiomatization is produced by turning terms into *normal forms*:
  - *terms of the basic (Markovian) calculus*
- For parallel and "new" choice this is done in a standard way by introducing *auxiliary operators*:
  - left and syncronization merge for parallel
  - analogous of *left merge* for choice
- A completely new axiom characterizes *abstraction from selfloops in Markovian calculi*:

  (ExpRec) $RecX.(\lambda.X + \lambda'.P + Q) = RecX.(\lambda'.P + Q)$

4. Non-atomic time delays

- In order to represent *more complex time models*, we need to consider semantics where:
  - delays *not executed atomically* in a single transition
  - but that *start in a given state, evolve through several states and terminate in another state*
- This is needed, e.g., to represent *continuous real-time* (as in Alur and Dill's timed automata) or *stochastic-time with general distributions*.

4.1 Not a new problem!

- Considered a simple calculus like:

$$P ::= \underline{0} \mid \pi.P \mid P + P \mid P \parallel_S P \mid P/L \mid RecX.P \mid X$$

  where "$\pi.P$" is either "$\alpha.P$" (α is a or τ) or "$\delta.P$".

- How to represent the execution of a time delay "δ" as the combination of the two events of:

  delay start *delay termination*

  in such a way that termination of a given delay is *uniquely related* to its start?

- Already considered in the literature: *ST semantics* (van Glabbeek and Vaandrager '87)

4.2 Decide & axiomatize ST semantics

- We have introduced *3 techniques* for decideing and axiomatizing ST semantics:
  - *static name technique*:
    - statically generates a name for every action according to its *syntactical position* in the term (location w.r.t. parallel)
    - allows ST bisimulation to be decided for finite-state terms
  - *dynamic name technique*:
    - dynamically generates a *canonical name* for every starting action according to the *order of execution* of actions: smallest number not in use by actions of the same type
    - ST bisimulation in terms of standard bisimulation: complete axiomatization and decidability for finite-state terms
  - *stack technique*:
    - based on *pointers*: same properties of dynamic name technique for an algebra including semantic action refinement

4.3 ST semantics for time delays

- Techniques based on names particularly adequate for timed models:
  - they keep the relationship between delay start and terminations by *producing unique names which are like clock names in a timed automata*.
- In particular, *dynamic name techinque* allows us:
  - to simply use *standard (weak) bisimulation*
  - to produce axiomatizations via a *standard approach based on left and synchronization merge*:

    is based on the technique of *levelwise renaming*: canonical names are recomputed every time delays are taken out from the scope of a parallel operator *in the rule for left merge*.

5. Continuous real-time

- Elapsing of time can be represented by *delay prefixes "D"*, where *D* represents a *set of non-negative real numbers*: the possible durations for the delay.
- *D* can, e.g., be an interval or a set of intervals obtained via a set of constraints.
- Since we are in a continuous domain we want to obtain *models based on clocks* (like a *timed automata*) *where time elapsing is not explicit*, but expressed symbolically via start and termination of clocks.

5.1 The calculus

- The calculus that we consider (for specifications):

$$P ::= \underline{0} \mid \pi.P \mid P \underline{+} P \mid P \|_S P \mid P/L \mid RecX.P \mid X$$

  where "π . P" is either "α . P" or *"D . P"*

- "π . P" and "$P + Q$" are auxiliary operators.

- We apply *ST semantics with dynamic names* to delay prefixes, thus producing clock names D_i:
  - *"i"* is a number generated by the semantics to *distinguish clocks derived from delays of the same type* (with the *same set of possible durations D*).

5.2 Equivalence and axiomatization

- Equivalence is just *Milner's observational congruence* (where D prefixes are considered to be visible actions): the effect is that *it matches delays with the same set of possible durations D*.
- A complete axiomatization is produced by by turning terms into *normal forms*:
  - *terms of a basic calculus (where we use* "π . P" and "$P + Q$" operators and D_i^+ , D_i^- *prefixes)*

  by *combining the two techniques* related to priority (maximal progress) and ST semantics.

6. General stochastic time

- Elapsing of time is represented by *delay prefixes "f"*, where *f* is a *general probability distribution* over non-negative real numbers: it expresses the probabilistic duration of the delay.
- Since we consider continuous general distributions we want to obtain *models based on clocks where time elapsing is not explicit*, but expressed symbolically via start and termination of clocks: a *Generalized Semi-Markov Process*

6.1 The calculus

- The calculus that we consider (for specifications):

$$P ::= \underline{0} \mid \pi.P \mid P \underline{+} P \mid P \|_S P \mid P/L \mid RecX.P \mid X$$

  where "π . P" is either "α . P" or "$\langle f,w \rangle$. P"

- "π . P" and "$P + Q$" are auxiliary operators.

- We apply *ST semantics with dynamic names* to delays $\langle f,w \rangle$, thus producing clock names f_i:
  - *"i" distinguishes clocks derived from delays of the same type* (with the same distribution f).
  - the *weight "w" is associated to the transition of start*

6.2 Equivalence and axiomatization

- Equivalence is just *Milner's observational congruence* combined with *standard probabilistic bisimulation* for start of delays: the effect is that *it matches delays with the same distribution f*.
- A complete axiomatization is produced by by turning terms into *normal forms*:
  - *terms of a basic calculus (where we use* "π . *P*" and "*P* + *Q*" operators and $\langle f_i^+, w \rangle$, f_i^- *prefixes)*

  by *combining the two techniques* related to priority (maximal progress) and ST semantics.

Open problems and future directions

- The continuous real-time and general stochastic time models could support the possibility of *aggregating*, besides τ actions, also *time delays*. How to express this in the semantics and the equivalence is a difficult open problem (a possibility could be using the stack technique).
- When the capability of expressing time is used in real case studies, often it turns out that an elegant way to *express internal/external probability and priority* is also needed. In spite of the several solutions proposed we still miss a very elegant one.

References

- M. Bravetti, R. Gorrieri ``A Complete Axiomatization for Observational Congruence of Prioritized Finite-State Behaviors", in Proc. of the *27th Int. Colloquium on Automata, Languages and Programming (ICALP 2000)* , U. Montanari, J.D.P. Rolim and E. Welzl editors, LNCS 1853:744-755, Geneva (Switzerland), July 2000.
- M. Bravetti, R. Gorrieri ``Deciding and Axiomatizing Weak ST Bisimulation for a Process Algebra with Recursion and Action Refinement", in ACM Transactions on Computational Logic 3(4):465-520, 2002.
- M. Bravetti, R. Gorrieri ``The Theory of Interactive Generalized Semi-Markov Processes", in Theoretical Computer Science 282(1):5-32, 2002.
- M. Bravetti, ``Specification and Analysis of Stochastic Real-Time Systems", PhD Thesis, University of Bologna, Padova and Venezia, February 2002.
- M. Bravetti, ``Revisiting Interactive Markov Chains", in Proc. of the *3rd Workshop on Models for Time-Critical Systems (MTCS 2002)* , ENTCS 68(5), Brno (Czech Republic), August 2002.