Dealing with zero-time transitions in axiom systems·

Angelo Gargantini, Dino Mandrioli, Angelo Morzenti
Dipartimento di Elettronica e Informazione, Politecnico di Milano, Italy
{garganti, mandriol, morzenti}@elet.polimi.it

Abstract

In the modelization of time-dependent systems it is often useful to use the abstraction of *zero-time transitions*, i.e., changes of system state that occur in a time that can be neglected with respect to the whole dynamics of system evolution. Such an abstraction, however, sometimes generates critical situations in the formal system analysis. This may lead to limitations or unnatural use of such formal analysis. In this paper we present an approach that keeps the intuitive appealing of the zero-time transition abstraction yet maintaining simplicity and generality in its use. The approach is based on considering zero-time transitions as occurring in an infinitesimal, yet non-null time. The adopted notation is borrowed from non-standard analysis. The approach is illustrated through Petri nets as a case of state machines and TRIO as a case of logic-based assertion language, but it can be easily applied to any formal system dealing with states, time, and transitions.

Introduction

Several formalisms have been proposed recently for the modelization and analysis of time-critical systems. In many cases systems to be analyzed are described by some abstract machine and their properties are formalized through suitable formulas. Abstract machines are characterized by some notion of *state* and by *transitions* from one state to another. In such formalizations it is often useful to adopt the abstraction of *zero-time transitions*, i.e., transitions whose duration is so short that it can be neglected w.r.t. the whole system evolution.

Allowing transitions to occur in zero-time is certainly intuitively appealing; it exposes however to some risks in mathematical formalization. The main problem arises from the fact that it is quite natural to describe system state evolution by formalizing its state as a total function of the time variable: $s(t)$ denotes system's state at time t. By this way, the effect of a transition tr is described as a state transformation that leads system's state from s_1 at time t_1 (at the beginning of the transition) to s_2 at time t_2 (at the end of the transition). If we allow tr to have a null duration, however, we obtain that $t_1 = t_2$ and, therefore, at t_1 the system is *both* in state s_1 and in state s_2: such a claim contradicts the

• Work partially supported by CNR.

intuitive assertion that at a given instant the system is in exactly one state. It also exposes to the risk of formal contradictions if, e.g., one describes system state as the property that some node is marked or not.

To overcome this difficulty several approaches have been followed in the literature:

- In ASTRAL [CGK97] zero-time transitions are simply excluded.
- At the other extreme, in Esterel [B&C84] all transitions are assumed to take zero time. This is due to the typically synchronous approach on which Esterel is based: the abstraction provided by the model assumes that a whole time unit elapses and that at its end a *finite* sequence of state transitions occurs. As with all synchronous abstract machines time is intrinsically a discrete set[1].
- In [H&L96], instead, time *must* be a dense set. System evolution is described as an alternating sequence of trajectories and actions. A trajectory corresponds to a time interval where the state is constant or changes continuously with time; actions are instantaneous transitions that change the system state. Thus, the system state is a piecewise constant or continuous function of time.
- In other cases [Ost89], [B&D91], [Cer93] time is modeled as a particular system variable and its value is explicitly updated by special transitions (e.g. tick in [Ost89], which imposes a discrete time domain) which are interleaved with other state transformations. This approach sometimes imposes rather unnatural formalizations of system properties, and makes their proof much longer and unintuitive. For instance, it could happen that in system description two states s_1 and s_2 have the same value for the "time variable", which prevents the classical, simple modeling of system state as a function of time, and hinders the use of familiar locutions such as "the system state at time t". Also, in the case of discrete time domains, the unexperienced user must be emphatically warned that "the next value of system variable v" is not necessarily "the value at time t+1".
- In [FMM94] we provided an axiomatization of timed Petri nets which allows zero-time transitions. In the general case, however, such an axiom system must deal with the possibility of several firings of the same transition in the same instant: this imposes a fairly cumbersome notation and requires a convention to define a single state (marking) of the net at a time t when several transitions fire simultaneously. In [S&S96] the authors show that problems arise even when modeling time in Petri nets by means of token time stamps: in presence of instantaneous events, they propose to add to time stamps an index

[1]A typical application of this model is the synthesis of hardware circuits. Not surprisingly their design is based on a synchronous model where combinatorial gates (and, or, not, ...) are modeled as zero-time transitions: obviously, it is the designer responsibility to verify that, in practice, all switchings corresponding to combinatorial evaluation occur within a single machine cycle so that the zero-time abstraction is correct.

denoting the order of production of simultaneously generated tokens. This solution is similar to that proposed in [FMM94] and shares the same weaknesses in terms of naturalness and generality.

To summarize, all approaches proposed so far had to pay a price either in terms of generality, or in terms of naturalness in the expression and proof of system properties, or in terms of heaviness of the mathematical notation.

In this paper we present a novel approach which conjugates intuition with mathematical rigor and generality. Going back to the original intuitive meaning of zero-time transitions we consider such transitions as occurring in an infinitesimal – yet non-null – time; in the traditional continuous mathematics terminology "a zero-time transition actually takes a non-null time whose measure is smaller than any finite positive number".

We fully formalize this approach within the framework of *non-standard analysis* [Rob61, Rob96], which provides a simple and intuitive notation to formalize infinitesimal calculus. We instantiate our approach with reference to timed Petri nets and to the logic language TRIO which we are using for our research in the field of real-time systems [FMM94]. We will show, however, that our approach is absolutely general and can be applied as well to any other abstract machine and assertion language. Furthermore, despite the fact that we deal with infinitesimal numbers, our approach can be applied both to dense and to discrete time domains.

The paper is organized as follows. Section 2 provides a short summary of non-standard analysis; Section 3 provides an axiom system for timed Petri nets based on a minimal subset of the TRIO language and assuming a time domain augmented with infinitesimal numbers. Section 4 provides a few examples of property proofs in the new axiomatization and shows that these new proofs are considerably simpler than those derived with previous approaches. Finally, Section 5 contains a few concluding remarks.

For the sake of shortness we limit ourselves to the essential aspects of the proposed approach; the skipped details, however, can be easily filled out.

2. A summary of non-standard analysis

In this section we introduce the main concepts of the modern theory of infinitesimals founded by A. Robinson [Rob61, Rob96], the non-standard analysis (NSA in brief). We provide only the minimum background that is needed to explain our application of this theory.

The main idea that facilitates practical application of NSA is due to E. Nelson [Nel77]; he defined a theory, called Internal Set Theory (IST), which includes a typical axiomatization of arithmetics (say, ZFC, the Zermelo-Fraenkel set theory with the axiom of Choice [Coh66]) and extends it through the predicate *standard* (briefly *st*), which is left deliberately undefined, plus three additional axiom schemes. Thanks to

the new *st* predicate introduced by IST, we can say whether a number (of the usual numeric sets such as the reals R and the naturals N) is either standard or not. Every concrete number one could write or a computer could generate is standard. Thus numbers such as 1, π, 1/100, are standard.

The predicate standard is used to introduce the concept of infinitesimal in R in the following way: x is infinitesimal if $x \geq 0$ and x is smaller than any positive standard number (smaller then any number we can write or calculate). 0 is infinitesimal; in fact, it is the only infinitesimal standard number. Close to 0 there are the non standard infinitesimal numbers (infinitesimal and greater than zero). They are not the only non standard numbers. R includes many other non standard numbers, that are the result of adding and subtracting infinitesimal amounts to standard numbers. There are also unlimited non standard numbers, i.e., the inverses of infinitesimal non standard numbers, greater than every standard number.

Now we formalize the above concepts in R through first order predicate formulas, where $\forall^{st} x\ A(x)$ is an abbreviation for $\forall x\ (\ st(x) \rightarrow A(x))$:

infinitesimal(ε)	is defined as	$\forall^{st}\ x\ (x>0 \rightarrow \lvert\varepsilon\rvert \leq x)$
nsinfinitesimal(ε)	is defined as	$\forall^{st}\ x\ (x>0 \rightarrow \lvert\varepsilon\rvert \leq x) \wedge \neg st(\varepsilon)$
infinitesimal^{+}(ε)	is defined as	$\forall^{st}\ x\ (x>0 \rightarrow 0<\varepsilon\leq x) \wedge \neg st(\varepsilon)$

Formulas in which the predicate *st* does not occur are called *internal* formulas. whereas formulas using the standard predicate are *external*. The definitions given above are all external formulas, while formulas of classical arithmetic are internal. Given an internal *sentence* (a formula with no free variables) A, the *relativization* of A to the standard sets, denoted as A^{st}, is obtained from A by restricting all quantifications to standard values (i.e., by substituting every occurrence of $\forall x$ by $\forall^{st} x$). A fundamental metatheorem of IST (hereinafter called the Transfer Theorem) asserts that $A^{st} \leftrightarrow A$; hence all theorems of conventional mathematics also hold in IST when relativized to the standard sets, and, conversely, to prove an internal theorem it suffices to prove its relativization to the standard sets. Another fundamental result of IST ensures that it is a *conservative extension* of ZFC, that is, every internal sentence that can be proved in IST can also be proved in ZFC.

The results of the usual operations (*, +, -, and /) between standard and non standard numbers are driven by the so called Leibniz rules [D&D95]. The following tables express some of these rules using the symbol Ø for an infinitesimal, £ for a limited number (i.e., a number that is not larger than any standard number).

+	Ø	£
£	£	£
Ø	Ø	

×	Ø	£
£	Ø	£
Ø	Ø	

From these tables we can derive the intuitive rules: "The sum of two infinitesimal numbers is a infinitesimal number, the product of a limited number by an infinitesimal number is infinitesimal, etc ...."

Here we do not express in our axiom system these rules (as well as operations between standard numbers) and assume other useful properties from the IST theory (e.g. there exists in R and in N an infinitesimal number, ...)

3. A non-standard axiom system for timed Petri nets

In this section we provide an axiom system for timed Petri nets (TPN). We refer to the Merlin and Farber model [M&F76], which is one of the most widely known versions of such nets. Informally, a TPN differs from a traditional PN in that each transition is labeled by a pair <*lb*, *ub*>: once enabled the transition cannot fire before *lb* time units and must fire within *ub*, unless disabled in the meanwhile. The axiom system is expressed in terms of the TRIO language which essentially is a predicate calculus augmented with a unique temporal operator Dist: Dist (F, t) means that formula F holds at a time instant whose distance is exactly *t* time units from the *current time* (that is, informally, from the time when Dist (F, t) is claimed). Several *derived operators* are defined to make formulas shorter and more readable: in this paper we will use:

- $\text{Futr}(F, t) \stackrel{\text{def}}{=} t \geq 0 \wedge \text{Dist}(F, t)$
- $\text{Past}(F, t) \stackrel{\text{def}}{=} t \geq 0 \wedge \text{Dist}(F, -t)$
- $\text{Alw}(F) \stackrel{\text{def}}{=} \forall t\ \text{Dist}(F, t)$
- $\text{WithinF}(F, t) \stackrel{\text{def}}{=} \exists d\ (d \leq t \wedge \text{Futr}(F, t))$

A complete and rigorous treatment of Merlin and Farber model semantics and a summary of the TRIO language can be found in [FMM91].

It will appear, however, that the method illustrated here can be applied as well to any formalism that is based on the notions of state and transition (Finite or infinite state machines) and to several logic-based assertion languages that allow dealing with time issues (e.g., [CGK97], [Koy89], [Ost89]).

Let us first define a suitable time domain T enriched with non-standard numbers and let us denote the augmented domain as $\hat{T}$. For simplicity let us assume that the original time domain is a subset of the set of real numbers R. For instance, we could take as time domain T the set of integers: thus $\hat{T}$ would be the set of integers augmented with the non-standard numbers that are infinitely close to an integer number. Figure 1 suggests an intuitive graphical representation of such a set. In general, $\hat{T}$ can be visualized by surrounding each standard real element of T by a "cloud" of nonstandard reals that differ from it by an infinitesimal number.

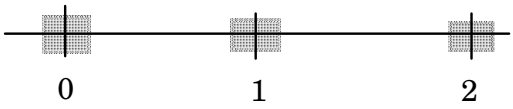


Figure 1. An intuitive display of integer numbers augmented with non-standard neighbors.

Next we introduce the following basic predicates describing TPN behavior:

- *fire(v)* means that the transition v fires now, i.e., at the current instant.
- *tokenF (v, w, d)* means that transition v fires now and the token produced by its firing will be consumed by transition w, d time units in the future. Symmetrically, the tokenP predicate is defined by

$$\text{tokenP}(v, w, d) \leftrightarrow \text{Past}(\text{tokenF}(v, w, d), d).$$

The above predicates are the same as we used in [FMM94]. Notice however, that in [FMM94] they were the result of a simplification from [FMM91] exploiting the restriction to 1-bounded nets. This restriction --together with other minor assumptions-- guaranteed *a priori* that no transition could fire twice in the same instant. Dealing with the general case required more complex predicates (with more arguments) and axioms (see Example 1 and the Appendix).

Also, we keep here a minor simplification that excludes that the same pair of transitions has more than one place in the intersection between pre- and post-sets. This assumption does not cause any loss of generality and only allows some simplification in the notation.

The essential features of our approach are the following:

1. There are no firings occurring *exactly* in null time: in general, if a lowerbound, upperbound pair $<m_v, M_v>$ is associated with a transition v, we will assume that v' s firing may occur at a time distance t since its enabling with $m_v+\varepsilon_1 < t < M_v+\varepsilon_2$, ε_1, ε_2 being two *positive* infinitesimal numbers.
2. No transition can fire more than once exactly at the same instant; it can, however, fire at two instants whose distance is infinitesimal.
3. There is *exactly one* system state associated to every instant (having a standard numerical value or not) of the time domain.

We are now ready to give axioms formalizing the behavior of TPNs. Following the same schema as [FMM94] we consider transitions of the types given in Figure 2:

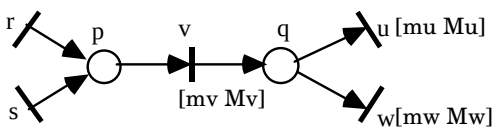


Figure 2. A fragment of timed Petri net

We augment both the lower and the upper bound of every transition by an infinitesimal positive constant amount. This choice allows us to treat in the same manner zero-time transitions, transitions with lowerbound equal to the upperbound, and any other transition with upperbound > lowerbound. Thus the only requirement about m_V and M_V is $0 \le m_V \le M_V$.

For the fragment of Figure 2 the axiom related to v' s lowerbound is

LB(v) $\quad \text{fire}(v) \rightarrow \exists d\ (d > m_V \wedge (\text{tokenP}(r,v,d) \vee \text{tokenP}(s,v,d))$

which means that if v fires it consumes a token produced by r or s strictly more than m_V time units ago. If $m_V=0$ this axiom excludes a –strictly– zero-time firing.

The axiom related to v's upperbound is:

UB(v) $\quad (\ \text{fire}(r) \rightarrow\ \exists d(\ d \le M_V + \varepsilon \wedge \text{tokenF}(r,v,d))\ )$

$\wedge$

$(\ \text{fire}(s) \rightarrow\ \exists d(\ d \le M_V + \varepsilon \wedge \text{tokenF}(s,v,d))\ )$

where ε is a positive infinitesimal number. This is a short notation for:

$\exists e\ (\ \text{infinitesimal+}(e) \wedge$

$(\ \text{fire}(r) \rightarrow\ \exists d(\ d \le M_V + e \wedge \text{tokenF}(r,v,d))\ ) \wedge$

$(\ \text{fire}(s) \rightarrow\ \exists d(\ d \le M_V + e \wedge \text{tokenF}(s,v,d))\ )\quad)$

Notice that the above axioms are the same as [FMM94] with the only addition of infinitesimal numbers.

The UB axiom is slightly more complex when two transitions compete to consume a token from a single place, as do transitions u and w in Figure 2. Let M be the least of the upperbounds of u *and* w, i.e., $M \stackrel{\text{def}}{=} \min(M_u, M_w)$. The axiomatization of UB imposes the firing of either u or w within M time units after v.

UB(u), UB(w): $\text{fire}(v) \rightarrow \exists d(d \le M+\varepsilon \wedge (\text{toeknF}(v, u, d) \vee \text{tokenF}(v, w, d)))$

Finally we add an axiom stating token unicity:

IU(v): $\quad \text{tokenP}(x, v, d) \wedge \text{tokenP}(y, v, e) \rightarrow x=y \wedge d=e$

OU(v): $\quad \text{tokenF}(v, x, d) \wedge \text{tokenF}(v, y, e) \rightarrow x=y \wedge d=e$

(with x and y variables ranging on the set of transitions).

As a result we obtained an axiom system for TPNs with the same simplicity as for 1-bounded TPNs which applies however to general TPNs.

The examples given in the next section show the usefulness of the new axiomatization w.r.t. other approaches.

4. Proving system properties through the non-standard axiom system

In this section we provide a few examples of use of the new axiom system to prove system properties. Comparisons with previous approaches show how the proposed method joins naturalness with generality.

Example 1

We show that having increased by an infinitesimal quantity the lowerbound of a transition does not alter the order of firings.

Let us consider the net fragment in Figure 3.

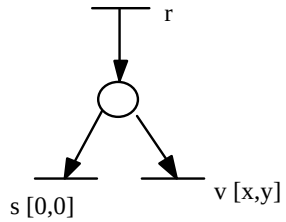


Figure 3. Two transitions in mutual exclusion.

where x is any *standard* positive real number and y any real number $\geq$x.

Then the following property holds

$$\text{Alw}\ (\neg\ \text{fire(v)}) \qquad (\ddagger)$$

i.e., despite the (infinitesimal) increase in the upperbound of s, transition v will never fire.

This property was illustrated and proved in [FMM91], using a different axiomatization: there we could not avoid simultaneous transition firings, hence both the formalization of the behavior of the net and, as a consequence, the proof the property were much less intuitive and transparent. We were compelled to use the predicate *fireth*(v, i) to state that transition v fires *for the i-th time at the current instant*, and therefore we formalized the property as Alw($\neg\ \exists i$ *fireth*(v, i)). Similarly, in that axiomatization *tokenP*(r,j, v,i, d) would mean that transition r fires now (at the current instant) for the j-th time and the token produced by this firing will be consumed after d time units by the i-th firing of transition v. We report the proof based on the axiomatization of [FMM91] in the Appendix, and invite the reader to compare it with the new proof we display next. The latter is much more terse, though similar in structure, thanks to the use of simpler predicates and the absence of quantifications over the number of simultaneous transition firings.

Proof of (‡).

Axiom UB for transition s is:

$$\text{UB(s)}: \text{fire(r)} \rightarrow \exists \text{d}\ (\text{d} \leq \varepsilon \wedge (\ \text{tokenF(r, s, d)} \vee \text{tokenF(r, v, d)}\ )\ )$$

Let us assume, by contradiction, that transition v fires. Then, we can construct the following derivation.

1.	fire(v)	**Hyp**
2.	$\exists d(d>x \wedge tokenP(r, v, d))$	**1, LB(v):** Lower Bound axiom of v
3.	$D>x \wedge tokenP(r, v, D)$	**2, EI:** Existential Instantiation: D for d
4.	$D>x \wedge Past(tokenF(r, v, D), D)$	**3, def:** tokenP(x,y,d) =Past(tokenF(x,y,d),d)
5.	$D>x \wedge Past(fire(r), D)$	**4, def:** tokenF(r,v,d) $\rightarrow$ fire(r)
6.	$D>x \wedge Past(\exists e(e \leq \varepsilon \wedge (tokenF(r, s, e) \vee tokenF(r, v, e)))), D)$	**5, UB(s)** Upper Bound axiom for s
7.	$D>x \wedge \exists e(e \leq \varepsilon \wedge Past(tokenF(r, s, e) \vee tokenF(r, v, e), D))$	**6, th:** Past($\exists$x A(x),d) = $\exists$x Past(A(x),d)
8.	$\exists e(D>x \wedge e \leq \varepsilon \wedge Past((tokenF(r, s, e) \vee tokenF(r, v, e)) \wedge tokenF(r, v, D), D))$	**7,4 AI** And Introduction
9.	$(tokenF(r, s, e) \vee tokenF(r, v, e)) \wedge tokenF(r, v, D) \rightarrow D=e$	**OU(r)** Output Unicity for r
10.	$\exists e(D> x \wedge e \leq \varepsilon \wedge Past(D = e ,D))$	**8,9, MP**
11	$\exists e(D> x \wedge e \leq \varepsilon \wedge D = e)$	**10, th:** Past(A,x)$\rightarrow$ A, if A is time independent
12.	$\exists e(x< e \leq \varepsilon)$	**11, AE** And Elimination

Proposition 12 is false, since x is a positive standard real number, while ε is less than any positive standard. By contradiction, the initial assumption is therefore false. ■

Example 2

Consider the net fragment given in the Figure 4. We want to prove that

(•) fire(s) $\rightarrow$ WithinF (fire(v2), 10)

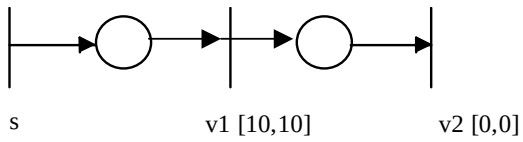


Figure 4. Two transitions firing at the same time.

In this case it is immediate to realize that (•) cannot be derived as a theorem in our non-standard system. In fact the axioms UB given in Section 3 formalize the fact that, once s fires, $v2$ will fire in a right neighborhood of the instant at 10 time units after the firing of s, whereas (•) requires a firing of $v2$ within *exactly* 10 time units. In such cases, the user has the responsibility to state precisely whether timing properties to be proved must hold *exactly or up to an infinitesimal approximation*.

In this case, for instance, the "right" formula to be proved should be

(••) fire(s) $\rightarrow$ WithinF(fire(v), 10+ε)

where, for ease of reading, we use the short notation WithinF(fire(v), 10+ε) as an abbreviation for ∃e (WithinF(fire(v), 10 + e) ∧ infinitesimal$^+$(e)).

Once it is understood that the wished property of the net of Figure 4 is (➥) rather than (➧), its proof with the new axiom system becomes a trivial exercise by exploiting the fact that the sum of two infinitesimals is infinitesimal.

Example 3

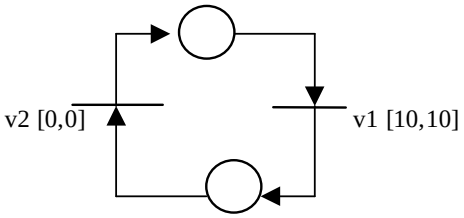


Figure 5. A transition loop.

Consider the net fragment given in the Figure 5. It is interesting to note that the following property can be easily proved through a simple induction

(➧) fire(v1) → $\forall^{st}$ k (Futr(fire(v2), k·10+ε)).

Proof of (➧)

From

1. fire(v2) → Futr(fire(v1), 10 + ε1) and
2. fire(v1) → Futr(fire(v2), ε2)

we find:

fire(v2) → Futr(fire(v2), 10 + ε1 + ε2)

from which we derive

fire(v2) → Futr(fire(v2), n·10 +n· ε1+n· ε2)

from which the thesis follows (since n is standard and by Leibniz rules), taking ε=n· ε1+n· ε2. ■

Notice that the order of quantifications is intended as

∃e $\forall^{st}$n (infinitesimal$^+$(e) ∧ (fire(v2) → Futr(fire(v2), n·10 + e))).

From this we derive, thanks to basic properties of predicate calculus,

$\forall^{st}$n ∃e (infinitesimal$^+$(e) ∧ (fire(v2) → Futr(fire(v2), n·10 +e))).

Then the Transfer theorem of IST allows us to derive

∀n ∃e (infinitesimal$^+$(e) ∧ (fire(v2) → Futr(fire(v2), n·10 + e))),

whereas the formula with the other quantifier alternation, ∃e∀n(...), does not hold. This remark perfectly matches the intuition that, if we want to execute the loop of Figure 5 "an extremely large number of times" keeping the firing times "close to multiples of 10" we can always find a sufficiently short firing time for the single transition firings to fulfill the requirement; this property, however, does not generalize to "an infinite number of times".

5. Conclusions

We have presented a new axiomatic approach that allows dealing with zero-time transitions in a way that is both intuitive and general. The approach is based on considering exact time bounds that are associated with transition firings as *approximations* of time measures up to infinitesimal numbers. As a consequence the user must apply some care in specifying system properties by clearly distinguishing whether some time values are exact or approximated numbers (in most practical cases it will turn out that we are dealing with approximate quantities).

Our short experience with the use of TRIO in a non-standard framework shows that extending the approach from the very basics presented in this paper to the complete language (dealing with several derived operators, with large specifications and more complex proofs, ...) can proceed quite smoothly.

The approach has been formalized for timed Petri nets and the TRIO logic language but it can be applied as well to any abstract machine and logic assertion language.

For instance, our approach can provide a sound and complete explanation of the "arbitrary small constant β" that is introduced in [H&L96] as a "technicality to take into account of possible critical races": a close inspection shows that such a constant is but an infinitesimal positive quantity.

Furthermore, in those approaches, such as [B&D91], [Cer93], and [Ost89], where time is formalized as a state variable updated by special "tick" transitions, time flow could be made implicit, as it is in traditional dynamic system theory, by associating a positive, possibly infinitesimal duration to every "normal" (non-tick) transition. This would permit the unification of the above approaches with other ones, such as [CGK97], where time advances independently but a non-zero duration is associated with every transition.

Acknowledgement

We would like to thank Myla Archer for carefully reading and pointing out some errors in a previous draft of the present work. We also acknowledge the contribution of the reviewers in improving the style of the paper and the exposition of our contribution.

References

[B&C84] G. Berry, L. Cosserat, The ESTEREL Synchronous Programming Language and Its Mathematical Semantics, S. Brooks, A. Roscoe and G. Winskel (eds), Lecture Notes in Computer Science, vol. 197, pp. 389-448, Springer-Verlag, 1984.

[B&D91] B. Barthomieu, M. Diaz, Modeling and Verification of Time Dependent Systems Using Time Petri Nets, *IEEE Transactions on Software Engineering*, vol. 17, N.3, pp. 259-273, March 1991.

[Coh66] Paul J. Cohen, *Set theory and the continuum hypothesis*, Benjamin, New York, 1966, MR 38 #999.

[D&D95] Francine Diener, Marc Diener (editors), *Nonstandard analysis in practice*, Universitext, Springer-Verlag, 1995, ISBN 3-540-60297-6.

[Cer93] A.Cerone, A Net-based Approach for Specifying Real-Time Systems, Universita` degli Studi di Pisa, Dipartimento di Informatica, PhD Thesis, TD-16/93.

[CGK97] A. Coen-Porisini, C. Ghezzi, R.A. Kemmerer, *Specification of Realtime Systems Using ASTRAL*, IEEE Transactions on Software Engineering, vol 23, N 9, pp. 572-598, September 1997.

[FMM91] M.Felder, D.Mandrioli, A.Morzenti, Proving properties of real- time systems through logical specifications and Petri net models, Tech. Report 91-72, Politecnico di Milano Department of Electronic Engineering and Information Sciences, December 1991.

[FMM94] M.Felder, D.Mandrioli, A.Morzenti, *Proving properties of real-time systems through logical specifications and Petri net models*, IEEE TSE-Transactions of Software Engineering, vol.20, N.2, pp.127-141, February 1994.

[H&L96] Constance Heitmeyer and Nancy Lynch, Formal Verification of Real-Time Systems Using Timed Automata, in Constance Heitmeyer and Dino Mandrioli (eds), in *Formal Methods for Real-Time Computing*, John Wiley, New York, 1996.

[Koy89] Koymans, R. *Specifying Message Passing and Time Critical Systems with Temporal Logic*, Ph.D. dissertation, Eindhoven University of Technology, 1989.

[M&F76] P.M. Merlin and D.J. Farber, Recoverability of communication protocols - Implications of a theoretical study, *IEEE Transactions on Communications*, vol 24, N 9, pp.1036-1043, September 1976.

[Nel77] E. Nelson, Internal Set Theory: a new approach to Nonstandard Analysis, *Bulletin American Mathematical Society*, 83, 1977, n. 6, pp. 1165-1198.

[Ost89] J. Ostroff, *Temporal Logic For Real-Time Systems*, Advanced Software Development Series, ed. J. Kramer, Research Studies Press Limited (distributed by John Wiley and Sons), England, 1989.

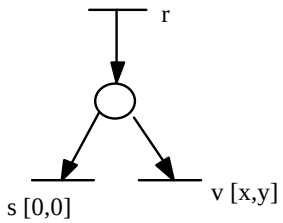
[Rob61] A. Robinson, Nonstandard Analysis, Proc. Roy. Acad. Amsterdam, Ser. A. 64, 432-440 (1961)

[Rob96] A. Robinson, *Non-standard Analysis*, Princeton University Press, 1996, 308 p., ISBN 0-691-04490-2.

[S&S96] S.Schöf and M. Sampels: Fairness and instant reactions in distributed simulation, Proc. of the 8th Europen Simulation Symposium (ESS'96), vol. 1, pp. 96-100, SCS, 1996.

Appendix

Proof of the property (♯) of Example 1 using the axiom system of [FMM91].



In this case the property is expressed as

(•) Alw (¬∃i fireth(v,i))

Next, we prove (•) by contradiction. By using suitable tautologies and generalization arguments, it suffices to prove that ¬∃i fireth(v,i).

1.	fireth(v,i)	**Hyp**
2.	∃d(d≥x ∧ ∃j tokenP(r, j, v, i, d))	**1, LB(v):** Lower Bound axiom for v
3.	D≥x ∧ tokenP(r, J, v, i, D)	**2, EI**: Existential Instantiation: D for d, J for j
4.	D≥x ∧ Past(tokenF(r, J, v, i, D), D)	**3, def**: tokenP(...,d) = Past(tokenF(.., d), d)
5.	D≥x ∧ Past(fireth(r, J), D)	**4, def**: tokenF(r, J, v, i, D) → fireth(r, J)
6.	D≥x ∧ Past(∃e(e≤0 ∧ ∃k(tokenF(r, J, s, k, e) ∧ tokenF(r, J, v, k, e)), D)	**5, UB(s):** Upper Bound axiom for s
7.	∃e(D≥x ∧ e≤0 ∧ ∃k Past(tokenF(r, J, s, k, e) ∧ tokenF(r, J, v, k, e), D)	**6, th:** Past(∃x A(x),d) = ∃x Past(A(x),d)
8.	∃e(D≥x ∧ e≤0 ∧ ∃k Past((tokenF(r,J,s,k,e) ∨ tokenF(r,J, v,k,e)) ∧ tokenF(r,J, v,i,d), D))	**7,4 AI** And Introduction
9.	(tokenF(r, J, s, k, e) ∧ tokenF(r, J, v, k, e)) ∧ tokenF(r, J, v, i, d) → d=e ∧ k=i	**OU(r):** Output Unicity for r
10.	∃e (D≥x ∧ Past((e≤0 ∧ k=i ∧ D=e)), D)	**8, 9, MP**
11.	∃e (D≥x ∧ Past(e≤0 ∧ D=e), D))	**10, AE:** And Elimination
12.	∃e (D≥x ∧ e≤0 ∧ D=e)	**11, th**: Past(A,x) → A, if A time independent
13.	∃e (x ≤ e ≤ 0)	**11, prop**
14.	¬ fireth(v,i)	**12,** by contradiction, since 13 is false