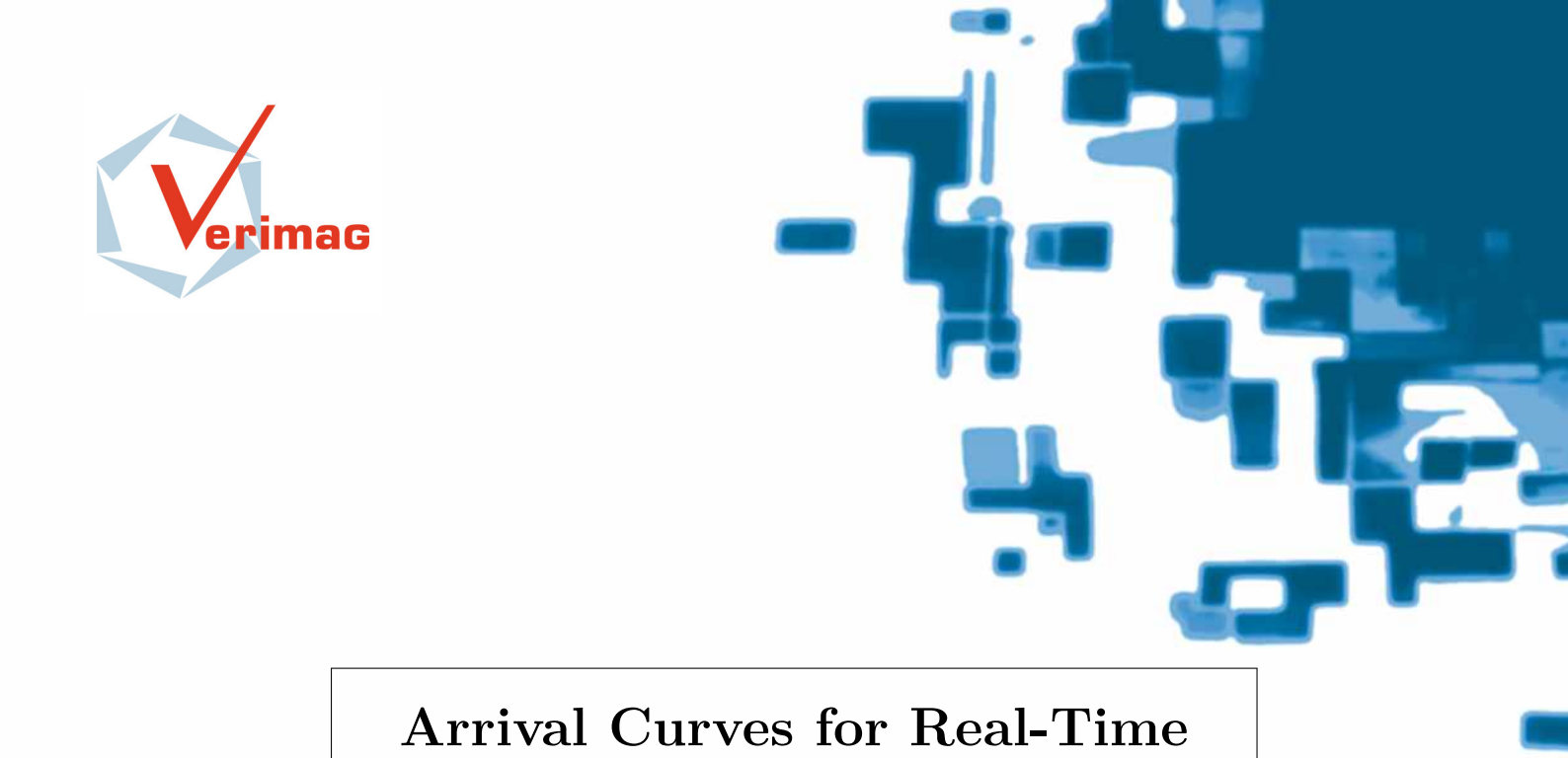


Arrival Curves for Real-Time Calculus: the Causality Problem and its Solutions

Matthieu Moy and Karine Altisen

Verimag Research Report n^o TR-2009-15

October 8, 2010

Unité Mixte de Recherche 5104 CNRS - INPG - UJF
Centre Equation
2, avenue de VIGNATE
F-38610 GIERES
tel : +33 456 52 03 40
fax : +33 456 52 03 50
http://www-verimag.imag.fr

Arrival Curves for Real-Time Calculus: the Causality Problem and its Solutions

Matthieu Moy and Karine Altisen

Verimag (UMR CNRS 5105)
Centre Équation - 2, avenue de Vignate
38610 Gières - FRANCE
E-mail: Matthieu.Moy@imag.fr, Karine.Altisen@imag.fr

October 8, 2010

Abstract

The Real-Time Calculus (RTC) [19] is a framework to analyze heterogeneous real-time systems that process event streams of data. The streams are characterized by pairs of curves, called arrival curves, that express upper and lower bounds on the number of events that may arrive over any specified time interval. System properties may then be computed using algebraic techniques in a compositional way. A well-known limitation of RTC is that it cannot model systems with states and recent works [10, 9, 2, 16, 14] studied how to interface RTC curves with state-based models. Doing so, while trying, for example to generate a stream of events that satisfies some given pair of curves, we faced a causality problem [17]: it can be the case that, once having generated a finite prefix of an event stream, the generator deadlocks, since no extension of the prefix can satisfy the curves afterwards. When trying to express the property of the curves with state-based models, one may face the same problem. This paper formally defines the problem on arrival curves, and gives algebraic ways to characterize causal pairs of curves, i.e. curves for which the problem cannot occur. Then, we provide algorithms to compute a causal pair of curves equivalent to a given curve, in several models. These algorithms provide a canonical representation for a pair of curves, which is the best pair of curves among the curves equivalent to the ones they take as input.

We consider the general case of infinite curves (either discrete or continuous time and events), and give algorithms for particular cases (finite curves in discrete time, piecewise affine functions, and a combination of both).

Keywords: Real-Time Calculus, Arrival Curve, Causality, Forbidden Regions

Reviewers: Florence Maraninchi

How to cite this report:

@techreport {verimag-TR-2009-15,
title = {Arrival Curves for Real-Time Calculus: the Causality Problem and its Solutions},
author = {Matthieu Moy and Karine Altisen},
institution = {{Verimag} Research Report},
number = {TR-2009-15},
year = {2009}
}

1 Introduction

The increasing complexity of modern embedded systems makes their design more and more difficult. Modeling and analysis techniques have been developed that help taking or validating decisions on the conception of a system as early as possible in the design process.

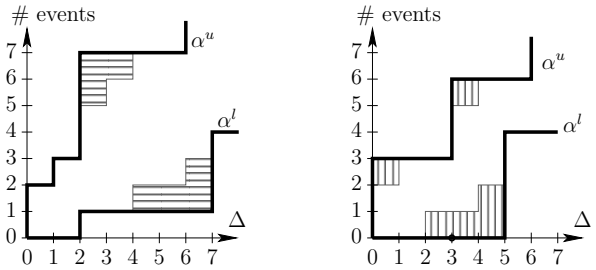
There exists many methods among which we can distinguish two families. *Computational* approaches study fine-grain models of the system to represent its complete behavior. The validation of the system using such a model may involve simulation, testing and verification. As opposed, *analytical* techniques, such as Real Time Scheduling (founded with [12]) and Real Time Calculus [19], use purely analytical models, based on mathematical equations that can be solved efficiently. These models can represent in a simple way the amount of events to be processed and how fast they can be processed. Solving these equations can give, for example, the best and worst cases for performances.

Both families of approaches have their advantages and drawbacks. Simulating precisely an embedded system gives very precise results, but only for one simulation, and one instance of a system. Analytical approaches, on the other hand, give strict worst case execution times, and usually give results very fast, but do so only for cases that the theory can take into account. For example, Real-Time Calculus cannot handle the notion of state in the modeling of a system. Recent studies try to combine the approaches to take the best of both [10, 9, 20, 1]. The work we present in this paper fully takes its root and motivation in one of those studies, while trying to combine Real-Time Calculus, state-based models and abstract interpretation, using synchronous languages [2].

The *Real-Time Calculus (RTC)* [19] is a framework to model and analyze heterogeneous system in a compositional manner. It relies on the modeling of timing properties of event streams with curves called *arrival curves* (and service curves, which count available resources instead of events in a similar fashion). A component can be described with curves for its input stream and available resources and some other curves for the outputs. For already-modeled components, RTC gives exact bounds on the output stream of a component as a function of its input stream. This result can then be used as input for the next component. *Arrival curves* are function of relative time that constrains the number of events that can occur in an interval of time. For any sliding window of time of length Δ, the pair of arrival curves (α^u, α^l) gives *explicitly* the lower $\alpha^l(\Delta)$ and upper $\alpha^u(\Delta)$ bounds on the number of events (see examples in Figure 1). But, arrival curves may also contain *implicit constraints* indirectly deduced from explicit ones. This paper studies those implicit constraints and provides algorithms to make them explicit.

Motivation. Implicit constraints cause problems in several contexts. For simulation purpose [8], it is typical to produce a stream of events that satisfies some given arrival curves using a *generator of events*. Such generators are the computational representation of a pair of curves, they are built to generate any streams that satisfies the curves. There are multiple ways to write such generators [8, 1, 2, 20] but many faced the problem. For the explanation, let us consider a straightforward one, in discrete time: it computes at each point in time the lower and upper bounds on the number of events allowed to be emitted, based on the events already emitted, and it emits a random number of events within these bounds. Now, it may happen, due to implicit constraints, that some upper bound is strictly lower than the lower bound, leading the generator to a deadlock.

Another case where implicit constraints are problematic is the case of formal verification of a system, with inputs and outputs characterized by arrival curves. One may want to prove a property like "If the input complies with the arrival curve pairs α_I, then the output satisfies the arrival curve pairs α_O". But verification tools based on reachability analysis (see, e.g. [6]) usually allow only the expression of "If the input complies with α_I *up to time* t, then the output complies with the α_O *up to time* t". Then, the tool may find a counter-example violating α_O without violating α_I *up to time* t, but it can be the case that this finite counter-example cannot be extended into an infinite execution that satisfies α_I. This would therefore be a *spurious counter-example*. Getting rid of these counter-examples sometimes requires heavyweight state exploration techniques (for example, the `-causal` option of `lesar` [18] does this for Boolean programs) but



(a) Unreachable Regions (b) Forbidden regions

Figure 1: Implicit and explicit constraints on arrival curves

not all tools are able to do it (`nbac` [6] cannot, for example, and the problem is known to be undecidable for integer programs). The technique that translates the constraints of arrival curves into a model to be analyzed by a verifier tool was used for, e.g., timed automata [10, 9, 20], event count automata [16] and synchronous programs [2]. For each tool, one can pose the questions: "what is the behavior of the tool when used on curves with forbidden regions?" and "do the tool output curves with forbidden regions?". Actually, except [2], the papers do not give answer to them. We will see that [10, 9, 20] do not create curves with forbidden regions while [16] could at least in theory, and we explain why. Each of the tools would badly behave in the presence of forbidden regions, and this paper gives a way to get rid of them before using any tool.

Implicit constraints on arrival curves. We distinguish two kinds of implicit constraints, that we call informally "unreachable regions" and "forbidden regions". The first one is a well-studied phenomenon within the Real-Time Calculus community [11] and the second, which may produce deadlocks in generators and spurious counter-examples in verification is the goal of this paper. Let us discover those using a pair of arrival curves (α^u, α^l) (see Figure 1 for an example).

Firstly, by splitting some time interval into smaller ones, we can get additional constraints. As shown in Figure 1.(a), in an interval of size $\Delta = 6$, the curve says explicitly that the lower bound on the number of events is 1, but splitting this interval into three intervals of size 2, one can deduce a better bound, which is 3. Although the curve explicitly specified the bounds $\alpha^l(6)$ and $\alpha^u(6)$ to be 1 and 7, the number of events in a window of size 6 can actually never be equal to 1 ($\alpha^l(6)$). In other words, the actual implicit lower bound is greater than $\alpha^l(6)$: this means that the curve is equivalent to a tighter curve. A well-known result [11] is that the upper (resp. lower) curve does not have this kind of implicit constraints if it is sub-additive (resp. super-additive). The transformation of an arbitrary curve into an equivalent sub-additive (resp. super-additive) curve making those constraints explicit is called *sub-additive closure* (resp. super-additive closure). In this paper, we call the region between the curves and its sub-additive (resp. super-additive) closure *unreachable regions*. Unreachable regions are due to constraints of a single curve on itself, and can be computed at some point by looking only at the past, i.e. smaller Δ.

The second case of implicit constraints can be found by looking at both curves towards the future. Figure 1.(b) gives an example of such a case: since $\alpha^l(3) = 0$, the lower curve does not give a lower bound on the number of events that can occur in a window of time of size 3, but if an execution has no event during such a window, then the upper curve prevents it from emitting more than 3 events in the next 2 units of time, while the lower curve will force it to emit at least 4. It is therefore impossible to emit no events for 3 units of time. We call the regions that contain such points *forbidden regions*. No execution can cross a forbidden region without getting blocked some time latter, due to some contradiction between lower and upper constraints. Borrowing the vocabulary used in [17], we call this kind of implicit constraints *causality constraints*. A pair of curves for which the beginning of an execution never prevents the execution from continuing is called *causal*. Intuitively, this is the same as having no forbidden region (but we will see that the relationship between absence of forbidden region and causality is only a one-way implication).

Surprisingly, this question has received very little attention and to the best of our knowledge, no transformation has been published before [3] to make these implicit constraints explicit. One may wonder if this is a "true" problem, i.e. if such non causal curves can be encountered in practice.

Indeed, part of the answer is that they cannot come from measurements on a real system, since curves derived from execution or simulation of real systems are always well-formed. The common practice is to use such curves for the inputs of RTC models. As RTC computations preserve the causality of the curves, non-causal curves were not considered as a problem so far. This may explain why no studies have been published yet on the subject. Things are different when instead of using RTC, one uses other tools for deriving output arrival curves, given some input arrival curves. Those tools, among them model-checking of timed automata [5] on abstracted models, abstract interpretation of Lustre programs [6], may compute non-causal arrival curves, even when the input is causal.

Additionally, non-causal curves contain implicit constraints that could be made explicit. If the output of a computation gives the curve in Figure 1, then making the implicit constraint explicit gives tighter bounds on the number of events (for example, a tighter bound on the number of events in a window of size 4). We encountered the case, when merging the output of several computations for the same set of flows of events [1] using different approximate methods. This provides several pairs of curves, each of them being a valid over-approximation of the expected result. The basic combination of these curves (point-wise minimum and maximum) can contain implicit constraints, and making them explicit gives more precise results from the same analysis.

Contributions. To solve these issues, this paper formally defines the causality problem and propose several solutions.

- We give a characterization of the notion of causal pairs of arrival curves.
- Combining this property with existing ones, we give a definition for a *canonical representation* of a pair of curves, which is causal and sub-additive/super-additive. We show that it is also the *tightest possible representation* of the original curve.
- We propose an algorithm that transforms a pair of arrival curves into its equivalent causal representation.

All results in the paper are proved and may be applied to dense-time or discrete-time arrival curves on the one hand, to discrete-event or fluid-event models on the other hand. The implementation part has been developed for discrete-time discrete-event models, since this was our context of use, but we believe it could be adapted to other contexts. Furthermore, although all along the paper we talk about arrival curves, the reader should be convinced that every results also apply to service curves.

Compared to previous works on the same subject [3], this paper provides all the details (intermediate lemma, complete proofs, examples...) about the main results that were previously omitted by lack of space, and provides algorithms for two more classes of curves: piecewise affine concave/convex curves, and combination of finite discrete curves with the later (see sections 5.2 and 5.3).

The outline of this paper is as follows: Section 2 defines *arrival curves* and some few algebraic operators; Section 3 defines *causality* and gives a *characterization* of it; Section 4 shows how to compute the *tightest causal representation* of arrival curves; and Section 5 gives an *algorithm* for computing it on particular classes of curves.

2 Arrival Curves

Usually in RTC, arrival curves are given by pairs, to express the upper and lower bounds on the number of events that can occur in any window of time. This section defines arrival curves. It first gives the context — the study allows either discrete or continuous time and discrete or fluid event counts — and recalls some basic notions of Min/Max-plus algebra that will be used later in the paper.

2.1 Basic Notions in Min-plus and Max-plus Algebra

Notations: $\mathcal{R}^+$ denotes the set of non-negative reals; $\overline{\mathcal{R}^+} = \mathcal{R}^+ \cup \{+\infty\}$ the set of non-negative reals extended with $+\infty$; $\mathcal{N}$ the set of naturals and $\overline{\mathcal{N}} = \mathcal{N} \cup \{+\infty\}$ the set of naturals extended

with $+\infty$.

To define arrival curves, we use functions that measure the number of events occurring at a given time. We assume to have a discrete-event model or a fluid-event model (the number of events may be discrete or continuous, in $\mathcal{N}$ or $\mathcal{R}^+$, we give bounds in $\overline{\mathcal{N}}$ or $\overline{\mathcal{R}^+}$, $+\infty$ being used to denote the absence of constraint on upper bounds), and we allow the time to be either discrete or continuous. We note the time $\mathcal{T}$ to represent $\mathcal{R}^+$ or $\mathcal{N}$; and $\mathcal{E}$ the event count to represent $\mathcal{R}^+$ or $\mathcal{N}$ ($\overline{\mathcal{E}}$ being either $\overline{\mathcal{R}^+}$ or $\overline{\mathcal{N}}$). Functions will be from $\mathcal{T}$ to $\overline{\mathcal{E}}$ whatever be the value of $\mathcal{T}$ and $\mathcal{E}$.

Definition 1. *Let f be such a function from $\mathcal{T}$ to $\overline{\mathcal{E}}$.*
f is said to be wide-sense increasing *iff(def)*

$$\forall x, y \in \mathcal{T} \,.\, x \leq y \implies f(x) \leq f(y)$$

We note $\mathcal{F}$ the set of functions f such that f is a function from $\mathcal{T}$ to $\overline{\mathcal{E}}$, f is wide-sense increasing and $f(0) = 0$. $\mathcal{F}_{finite}$ represents the set of functions in $\mathcal{F}$ restricted to functions from $\mathcal{T}$ to $\mathcal{E}$. We use the usual pointwise order on $\mathcal{F}$:

Definition 2. *Let $f, g \in \mathcal{F}$,*

$$f \leq g \overset{def}{\iff} \forall x \in \mathcal{T} \,.\, f(x) \leq g(x)$$

We recall the usual operators $\otimes$, $\overline{\otimes}$, $\oslash$, $\overline{\oslash}$:

Definition 3. *Let f, g be functions from $\mathcal{T}$ to $\overline{\mathcal{E}}$ and $x \in \mathcal{T}$,*

$$(f \otimes g)(x) \overset{def}{=} \inf_{t \in [0,x]} \{f(x-t) + g(t)\} \qquad \textit{((min, +) convolution)}$$

$$(f \,\overline{\otimes}\, g)(x) \overset{def}{=} \sup_{t \in [0,x]} \{f(x-t) + g(t)\} \qquad \textit{((max, +) convolution)}$$

$$(f \oslash g)(x) \overset{def}{=} \sup_{t \geq 0} \{f(x+t) - g(t)\} \qquad \textit{((min, +) deconvolution)}$$

$$(f \,\overline{\oslash}\, g)(x) \overset{def}{=} \inf_{t \geq 0} \{f(x+t) - g(t)\} \qquad \textit{((max, +) deconvolution)}$$

Note that if $f, g \in \mathcal{F}$, $(f \otimes g)$ and $(f \,\overline{\otimes}\, g)$ are in $\mathcal{F}$, but $(f \oslash g)$ and $(f \,\overline{\oslash}\, g)$ may not (since, for instance, $(f \oslash g)(0)$ and $(f \,\overline{\oslash}\, g)(0)$ may not be equal to zero). The following lemma gives conditions for $(f \oslash g)$ and $(f \,\overline{\oslash}\, g)$ to be in $\mathcal{F}$.

Lemma 1. *Let f, g be two functions. If $f, g \in \mathcal{F}$, then*

1. *$f \otimes g \in \mathcal{F}$; $f \,\overline{\otimes}\, g \in \mathcal{F}$;*
2. *$f \oslash g$ and $f \,\overline{\oslash}\, g$ are wide-sense increasing;*
3. *$f \oslash g \in \mathcal{F} \iff f \leq g$*
4. *$f \,\overline{\oslash}\, g \in \mathcal{F} \iff g \leq f$*

Proof.

1. $(f \otimes g)(0) = \inf_{0 \leq t \leq 0}\{f(0-t) + g(t)\} = f(0) + g(0) = 0$; let $x, y \in \mathcal{T}$ such that $x \leq y$, for all t: $f(x-t) + g(t) \leq f(y-t) + g(t)$ since f is wide-sense increasing, this implies that $f \otimes g(x) \leq f \otimes g(y)$.
2. Let $x, y \in \mathcal{T}$ such that $x \leq y$, then for all $t \geq 0$: $f(x+t) - g(t) \leq f(y+t) - g(t)$ since f is wide-sense increasing and this implies that $f \oslash g(x) \leq f \oslash g(y)$. The proof is exactly the same to prove that $f \,\overline{\oslash}\, g(x) \leq f \,\overline{\oslash}\, g(y)$.
3. $f \oslash g(0) = \sup_{t \geq 0}\{f(t) - g(t)\}$. Note that $f \leq g \iff \sup_{t \geq 0}\{f(t) - g(t)\} \leq 0$. If $f \leq g$, as $f(0) = g(0) = 0$, we have $f \oslash g(0) = 0$. Conversely, if $f \oslash g(0) = 0$, this means that $\sup_{t \geq 0}\{f(t) - g(t)\} \leq 0$, hence $f \leq g$.

4. The proof for $\overline{\oslash}$ is the same as for $\oslash$.

□

We now give the formal definition for the intuitive notion of "unreachable regions". Curves have no "unreachable region" if they are sub-additive/super-additive:

Definition 4 (Sub-additivity and Sub-additive Closure)**.** *Let $f \in \mathcal{F}$, f is said to be* sub-additive *iff(def)*

$$\forall s,t \in \mathcal{T} \ . \ f(t+s) \leq f(t) + f(s)$$

Well-known results (see [11] for example) characterize sub-additivity:

1. *$f \in \mathcal{F}$ and f sub-additive $\iff f \otimes f = f$*
2. *Let $f \in \mathcal{F}$. Among all the sub-additive functions $g \in \mathcal{F}$ that are smaller than f $(g \leq f)$ there exists an upper bound called the* sub-additive closure *of f given by:*

$$\overline{f} \stackrel{def}{=} \inf_{n \geq 1} \otimes^n f$$

where $\otimes^1 f = f, \otimes^{n+1} f = f \otimes (\otimes^n f)$.

Proof. of the well-known results

1. Let $f \in \mathcal{F}$. By definition of $\otimes$ this is always the case that $f \otimes f \leq f$. Let then f be sub-additive: let $x \in \mathcal{T}$. Whatever be $s \in [0,x]$, $f(x) \leq f(x-s) + f(s)$ by sub-additivity. Hence, $f \leq f \otimes f$.

   Conversely, let $f \in \mathcal{F}$ such that $f \otimes f = f$. Let $t,s \in \mathcal{T}$, $f(t+s) =_{\text{by assumption}} f \otimes f(t+s) \leq_{\text{by definition}} f(t) + f(s)$.

2. It is easy to show that $(\mathcal{F}, \leq)$ is a complete lattice and that $\otimes$ and min are continuous over $(\mathcal{F}, \leq)$. Finding the smallest function $g \in \mathcal{F}$ such that $g \leq f$ and g is sub-additive is equivalent to finding the greatest fix-point of $F(g) = \min(f, g \otimes g)$. This fix-point exists and is equal to $\inf_{n \geq 1} F^n(T) = \inf_{n \geq 1} \otimes^n f$, where T is the top of $(\mathcal{F}, \leq)$.

□

Definition 5 (Super-additivity and super-additive closure)**.** *Let $f \in \mathcal{F}$, f is said to be* super-additive *iff(def)*

$$\forall s,t \in \mathcal{T} \ . \ f(t+s) \geq f(t) + f(s)$$

Well-known results (see [11] for example) characterize super-additivity:

1. *$f \in \mathcal{F}$ and f super-additive $\iff f \overline{\otimes} f = f$*
2. *Let $f \in \mathcal{F}$. Among all the super-additive functions $g \in \mathcal{F}$ that are greater than f $(g \geq f)$ there exists an lower bound called the* super-additive closure *of f given by:*

$$\underline{f} \stackrel{def}{=} \sup_{n \geq 1} \overline{\otimes}^n f$$

The definition of $\overline{\otimes}^n$ is similar as for $\otimes^n$ and the proofs are the same as for sub-additivity.

2.2 Arrival Curves

2.2.1 Definition of Arrival Curves

Arrival curves defines lower and upper bounds on the amount of event that can occur in a window of time. It defines a set of possible event streams that satisfy all the bounds: as usual, we represent such an event stream with a cumulative curve.

Definition 6 (Cumulative curve)**.** *$R \in \mathcal{F}_{finite}$ can model a* cumulative curve*: $R(t)$ represents the (finite) amount of events that occurred in the interval of time $[0, t]$.*

Definition 7. *A pair of* arrival curves *is a pair of functions (α^u, α^l) in $\mathcal{F} \times \mathcal{F}_{finite}$, such that $\alpha^l \leq \alpha^u$.*

Let R be a cumulative curve and (α^u, α^l) be a pair of arrival curves. R is said to satisfy *(α^u, α^l) (we also use "R complies with (α^u, α^l)"), noted $R \models (\alpha^u, \alpha^l)$ iff(def)*

$$\forall x \in \mathcal{T}, \forall \delta \in \mathcal{T}, \quad R(x+\delta) - R(x) \in [\alpha^l(\delta), \alpha^u(\delta)]$$

We say that an arrival curve (α^u, α^l) is satisfiable *iff(def) there exists a cumulative curve R that satisfies (α^u, α^l).*

Notice that since α^l is a lower bound for cumulative curves, we prevent it from evaluating to ∞.

Definition 8. *Let (α^u, α^l) and $(\alpha^{u\prime}, \alpha^{l\prime})$ be two arrival curves. (α^u, α^l) and $(\alpha^{u\prime}, \alpha^{l\prime})$ are said to be equivalent iff(def) for all cumulative curves $R \in \mathcal{F}_{finite}$,*

$$R \models (\alpha^u, \alpha^l) \iff R \models (\alpha^{u\prime}, \alpha^{l\prime})$$

As a summary, a pair of arrival curves is a pair of positive wide-sense increasing functions (α^u, α^l) such that $\alpha^l(0) = \alpha^u(0) = 0$, $\alpha^l \leq \alpha^u$ and $\forall t > 0 \,.\, \alpha^l(t) \neq +\infty$.

2.2.2 Sub-additivity and Super-additivity

As we saw in the introduction, a pair of arrival curves can have unreachable regions. A curve that does not have any of these is sub-additive if it is an upper curve α^u, and super-additive if it is a lower curve α^l. When the curve has unreachable regions, it is possible to remove them, by using the associated closure operation.

Definition 9. *A pair of arrival curves (α^u, α^l) is Sub-Additive-Super-Additive (denoted SA-SA for short) iff(def) α^u is sub-additive and α^l is super-additive.*

We call $(\overline{\alpha^u}, \underline{\alpha^l})$ the SA-SA closure of (α^u, α^l).

Lemma 2. *Let (α^u, α^l) be a pair of arrival curves. $(\overline{\alpha^u}, \underline{\alpha^l})$ is a SA-SA pair of arrival curves* equivalent to *(α^u, α^l).*

Proof. This is a well-known result [11, 19], and a corollary of lemma 3 and 7 presented below. □

2.2.3 Arrival Curves Satisfied "Up To T"

Real-time calculus usually works on infinite event streams, and the relevant properties are the conformance of the corresponding cumulative functions to arrival curves. In this paper, we need an additional notion, which is the conformance of a cumulative function up to a certain date. Instead of checking the number of events in any window of time, we check only windows of time ending before a given date. The same notation is used, for example in [7].

Definition 10. *Let (α^u, α^l) be a pair of arrival curves and R be a cumulative curve. R satisfies (α^u, α^l)* up to *T (denoted by $R \models_{\leq T} (\alpha^u, \alpha^l)$) iff*

$$\forall t \leq T, \forall \delta \leq t, \quad R(t) - R(t-\delta) \in [\alpha^l(\delta), \alpha^u(\delta)]$$

Intuitively, this means R did not yet violate the arrival curves at time T.

A relationship between $\models_{\leq T}$ and $\models$ can be expressed simply:

Lemma 3. *Let R be a cumulative curve over $\mathcal{T}$, and (α^u, α^l) be a pair of arrival curves. We have:*

$$(\forall T \in \mathcal{T}, R \models_{\leq T} (\alpha^u, \alpha^l)) \iff R \models (\alpha^u, \alpha^l)$$

Proof. The proof is trivial once the definition of $R \models_{\leq T}$ is expanded in the left hand side of the equation. □

3 Causality: Definition and Characterization

We now define the notion of causality. The problem we are studying is the one of an event stream that is correct up to a certain time T, but "can not be continued" without violating the pair of curves. This can be seen as a deadlock of the flow, which could then neither let time elapse nor emit an additional event. A pair of arrival curves for which this problem can not happen is called *causal*. We first give a formal definition for causality, and then give a characterization with algebraic formulas.

3.1 Definition of Causality

Definition 11 (Causal Arrival Curves)**.** *Let (α^u, α^l) be a pair of arrival curves. (α^u, α^l) is said to be* causal *iff any cumulative curve R that satisfies (α^u, α^l)* up to *T can be extended indefinitely into a cumulative curve R' that also satisfies (α^u, α^l). In other words, (α^u, α^l) is causal iff(def)*

$$\forall T \geq 0, \forall R, \left(R \models_{\leq T} (\alpha^u, \alpha^l)\right) \implies \left(\exists R' \mid R' \models (\alpha^u, \alpha^l) \text{ and } \forall t \leq T, R(t) = R'(t)\right)$$

Unlike the sub-additivity and super-additivity properties, the causality is really a property on a *pair* of curves; it does not make sense to say that α^u alone, or α^l alone, is causal since the impossibility to extend a cumulative curve can come only from a contradiction between an upper bound and a lower bound.

3.2 An Overview of Theorems to Characterize Causality

Causality reveals new implicit constraints. Informally, we call *forbidden regions* the points between α^u and α^l that are reachable by finite cumulative curves, but for which the cumulative curves can trivially not be extended into infinite ones.

Let us consider the curve α^l, and try to define α^{l^*}, defined informally as "α^l without its forbidden regions". $\alpha^{l^*}(\Delta)$ is the smallest value for which a cumulative curve R verifying $R(t+\Delta) - R(t) \geq \alpha^{l^*}(\Delta)$ up to some time T is guaranteed to be extensible infinitely by emitting the maximum amount of events allowed by α^u, without violating α^l (this the same as saying that if $R(t+\Delta) - R(t) < \alpha^{l^*}(\Delta)$ for some t, then R cannot be extended without violating either α^u or α^l, which means that the region below α^{l^*} is forbidden). Computing the forbidden region of α^l at abscissa Δ_0 means therefore computing the lowest N for which $\alpha^u(\Delta) + N$ would not cross $\alpha^l(\Delta_0 + \Delta)$ for some $\Delta \geq 0$. This is equivalent to finding the supremum of the N for which the curves would intersect. Formally, this can be written as $\alpha^{l^*} = \sup_{\Delta \geq 0} \left\{\alpha^l(\Delta_0 + \Delta) - \alpha^u(\Delta)\right\}$, which is the definition of the deconvolution: $\alpha^l \oslash \alpha^u$. A similar reasoning would lead to the curve $\alpha^u \overline{\oslash} \alpha^l$ for the forbidden regions of α^u.

We can therefore define more formally forbidden region as the area between a curve α^u (resp. α^l), and $\alpha^u \overline{\oslash} \alpha^l$ (resp. $\alpha^l \oslash \alpha^u$): intuitively, computing $\alpha^u \overline{\oslash} \alpha^l$ means "removing forbidden regions from α^u", and computing $\alpha^l \oslash \alpha^u$ means "removing forbidden regions from α^l". When $\alpha^u = \alpha^u \overline{\oslash} \alpha^l$ and $\alpha^l = \alpha^l \oslash \alpha^u$, we can say that the curves have no forbidden region. The contribution of this paper is the study of these forbidden regions, giving a formal characterization and algorithms to detect their presence and to eliminate them.

The implications and equivalences between a few arrival curves properties are given in Figure 2.

Each of them will be proved in the following section.

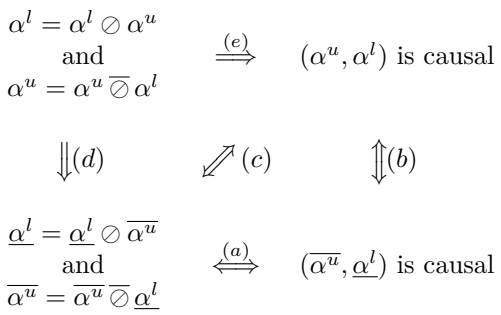


Figure 2: Overall view of theorems in this section

The main result is equivalence **(c)** (theorem 8), which gives an algebraic characterization of causality for any pair of arrival curves. Intuitively, it states that a pair of curves is causal if and only if its SA-SA closure has no forbidden region. A weaker version of this theorem is implication **(e)** (theorem 12), which gives only a sufficient condition: a pair of arrival curves having no forbidden region is causal.

One could have expected for the converse to be true, i.e. that a pair of arrival curves is causal implies that it doesn't have forbidden regions. This result is indeed false in general: a pair of causal curves can have forbidden regions if they are included in their unreachable regions (For completeness, we will give an example in section 3.3.6). The causality implies the absence of forbidden region for SA-SA curves though, since all unreachable regions have been erased from them: this is equivalence **(a)**. The remainders **(b)** and **(d)** are intermediate results.

The implications and equivalences (a), (b), (c), (d) and (e) in Figure 2 are proved as follows:

(a) will be an application of theorem 5 to $(\overline{\alpha^u}, \underline{\alpha^l})$.

(b) will be theorem 6, relatively straightforward and based on the fact that $(\overline{\alpha^u}, \underline{\alpha^l})$ and (α^u, α^l) accept the same set of cumulative curves.

(c) gives a necessary and sufficient condition for (α^u, α^l) to be causal. This characterization is obtained by transitivity of **(a)** and **(b)**.

(d) will be theorem 11, proved using recurrence and continuity of deconvolution operators.

(e) is obtained by transitivity of **(c)** and **(d)**. It gives a sufficient condition for (α^u, α^l) to be causal.

3.3 Characterization of Causality: Theorems and Proofs

3.3.1 A First Characterization of Causality

The following lemma states that causal and SA-SA arrival curves are valid executions of themselves. Intuitively, this means that if the arrival curves have neither "forbidden" nor "unreachable" regions, then we can follow either the lower or the upper curve to get a valid cumulative curve.

Lemma 4. *Let (α^u, α^l) be a causal pair of arrival curves. If α^l is super-additive, then $\alpha^l \models (\alpha^u, \alpha^l)$. Similarly, if α^u is sub-additive and is finite ($\in \mathcal{F}_{finite}$), then $\alpha^u \models (\alpha^u, \alpha^l)$.*

Proof. We show that $\alpha^l \models (\alpha^u, \alpha^l)$.

Since α^l is super-additive, it complies with itself by definition. The only way to have $\alpha^l \not\models (\alpha^u, \alpha^l)$ is to violate the constraint on α^u. The rest of the proof is done by contradiction:

Let $T = \sup_{t>0}\{\alpha^l \models_{\leq t} (\alpha^u, \alpha^l)\} + 1$. If we assume $\alpha^l \not\models (\alpha^u, \alpha^l)$, then T exists and is finite (by lemma 3).

Then, $\alpha^l \not\models_{\leq T} (\alpha^u, \alpha^l)$, and $\exists \Delta > 0 \mid \alpha^l(T) - \alpha^l(T-\Delta) > \alpha^u(\Delta)$. By causality of (α^u, α^l), as $\alpha^l \models_{\leq T-\Delta} (\alpha^u, \alpha^l)$, there exists R with $\forall t \leq T-\Delta, R(t) = \alpha^l(t)$ and $R \models (\alpha^u, \alpha^l)$. Hence, $R(T) - R(T-\Delta) \leq \alpha^u(\Delta) < \alpha^l(T) - \alpha^l(T-\Delta)$. Since $\alpha^l(T-\Delta) = R(T-\Delta)$, this implies $R(T) < \alpha^l(T)$ which is impossible.

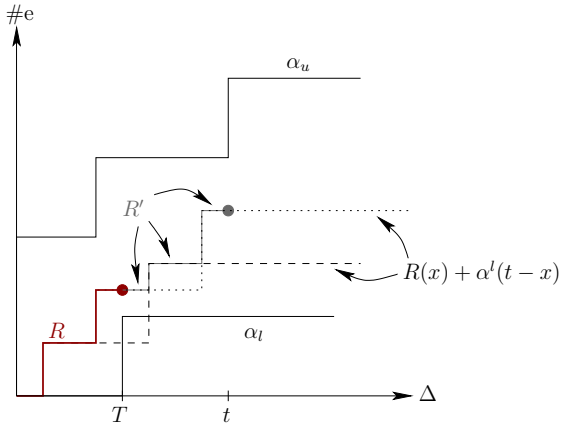


Figure 3: Extension of a cumulative curve

The proof is similar for α^u. □

The following theorem gives a characterization of causality, which is valid only for SA-SA pairs of curves. A more general one will be given in theorem 8, which uses this first one in its proof. It makes the link between forbidden regions and causality: an SA-SA pair of curves is causal if and only if it does not have forbidden regions.

Theorem 5 (Characterization of causality for SA-SA curves)**.** *Let (α^u, α^l) be a SA-SA pair of curves. We have:*

$$\left(\begin{array}{c} \alpha^l = \alpha^l \oslash \alpha^u \\ \textit{and} \\ \alpha^u = \alpha^u \overline{\oslash} \alpha^l \end{array}\right) \iff (\alpha^l, \alpha^u) \textit{ is causal}$$

Applied to $(\overline{\alpha^u}, \underline{\alpha^l})$, this is equivalence (a) on Figure 2.

Proof. $\Rightarrow$: Let (α^u, α^l) be a pair of SA-SA arrival curves such that $\alpha^l = \alpha^l \oslash \alpha^u$ and $\alpha^u = \alpha^u \overline{\oslash} \alpha^l$. Let R be a cumulative curve such that $R \models_{\leq T} (\alpha^u, \alpha^l)$. The intuition is to construct the execution R' that emit the smallest possible number of events that still complies with the lower bounds imposed by α^l and the prefix of R up to T. This execution will be a valid, infinite execution. This is illustrated on Figure 3. We'll prove first that R' is valid with respect to α^l, and then that it is valid with respect to α^u.

Formally, let R' be the cumulative curve defined by

$$\begin{aligned} \forall t \leq T, R'(t) &= R(t) \\ \forall t > T, R'(t) &= \sup_{x \in [0,T]} \{R(x) + \alpha^l(t-x)\} \end{aligned}$$

We will show that $R' \models (\alpha^u, \alpha^l)$. Let $t \in \mathcal{T}, \Delta \in [0, t]$. If $t \leq T$, then by definition of R', $R'(t) - R'(t-\Delta) \in [\alpha^l(\Delta), \alpha^u(\Delta)]$. We now consider $t > T$, and distinguish two cases on Δ:

- If $t - \Delta > T$, then

$$R'(t) - R'(t-\Delta) = \sup_{x \in [0,T]} \{R(x) + \alpha^l(t-x)\} - \sup_{x \in [0,T]} \{R(x) + \alpha^l(t-\Delta-x)\}$$

For all $x \in [0, T]$, we can write

$$\begin{aligned} \alpha^l(t-x-\Delta) + \alpha^l(\Delta) &\leq \alpha^l(t-x) && \text{(by super-additivity of } \alpha^l\text{)} \\ R(x) + \alpha^l(t-x-\Delta) + \alpha^l(\Delta) &\leq \alpha^l(t-x) + R(x) \end{aligned}$$

Hence,

$$\sup_{x\in[0,T]}\left\{R(x)+\alpha^l(t-x-\Delta)+\alpha^l(\Delta)\right\} \leq \sup_{x\in[0,T]}\{R(x)+\alpha^l(t-x)\}$$
$$\sup_{x\in[0,T]}\left\{R(x)+\alpha^l(t-x-\Delta)\right\}+\alpha^l(\Delta) \leq \sup_{x\in[0,T]}\{R(x)+\alpha^l(t-x)\}$$
$$R'(t-\Delta)+\alpha^l(\Delta) \leq R'(t) \qquad \text{(def. of } R')$$

- If $t-\Delta \leq T$, then

$$\begin{aligned} R'(t)-R'(t-\Delta) &= \sup_{x\in[0,T]}\{R(x)+\alpha^l(t-x)\}-R(t-\Delta) \\ &\geq R(t-\Delta)+\alpha^l(t-(t-\Delta))-R(t-\Delta) \qquad (\text{with } x=t-\Delta) \\ &\geq \alpha^l(\Delta) \end{aligned}$$

In both cases, $R'(t)-R'(t-\Delta) \geq \alpha^l(\Delta)$, so R' is valid with respect to α^l. Let's now prove its validity with respect to α^u. We distinguish the same two cases on $t-\Delta$:

- If $t-\Delta > T$, then

  For all $x \in [0,T]$, we can write

$$\alpha^l(t-x-\Delta)+\alpha^u(\Delta) \geq \alpha^l(t-x) \qquad (\text{since } \alpha^l = \alpha^l \oslash \alpha^u)$$
$$R(x)+\alpha^l(t-x-\Delta)+\alpha^u(\Delta) \geq \alpha^l(t-x)+R(x)$$

  Hence,

$$\sup_{x\in[0,T]}\left\{R(x)+\alpha^l(t-x-\Delta)+\alpha^u(\Delta)\right\} \geq \sup_{x\in[0,T]}\{\alpha^l(t-x)+R(x)\}$$
$$\sup_{x\in[0,T]}\left\{R(x)+\alpha^l(t-x-\Delta)\right\}+\alpha^u(\Delta) \geq \sup_{x\in[0,T]}\{\alpha^l(t-x)+R(x)\}$$
$$R'(t-\Delta)+\alpha^u(\Delta) \geq R'(t) \qquad \text{(def. of } R')$$

- If $t-\Delta \leq T$, then

$$R'(t)-R'(t-\Delta) = R'(t)-R(t-\Delta) = \sup_{x\in[0,T]}\{R(x)-R(t-\Delta)+\alpha^l(t-x)\}$$

  For all $x \in [t-\Delta, T]$ we can write

$$R(x)-R(t-\Delta) \leq \alpha^u(x-t+\Delta) \qquad (\text{since } R \models_{\leq T} (\alpha^u,\alpha^l))$$
$$\alpha^l(t-x)+R(x)-R(t-\Delta) \leq \alpha^u(x-t+\Delta)+\alpha^l(t-x)$$

  As $\alpha^u = \alpha^u \overline{\oslash} \alpha^l$, $\alpha^u(x-t+\Delta)+\alpha^l(t-x) \leq \alpha^u(\Delta)$. Combining with the above, for all $x \in [t-\Delta, T]$, we get

$$\alpha^l(t-x)+R(x)-R(t-\Delta) \leq \alpha^u(\Delta)$$

  On the other hand, for all $x \in [0, t-\Delta]$ we can write

$$R(t-\Delta)-R(x) \geq \alpha^l(t-\Delta-x) \qquad (\text{since } R \models_{\leq T} (\alpha^u,\alpha^l))$$
$$\alpha^l(t-x)+R(x)-R(t-\Delta) \leq \alpha^l(t-x)-\alpha^l(t-\Delta-x)$$

  As $\alpha^l = \alpha^l \oslash \alpha^u$, $\alpha^l(t-x)-\alpha^l(t-\Delta-x) \leq \alpha^u(\Delta)$. Hence, for all $x \in [0, t-\Delta]$,

$$\alpha^l(t-x)+R(x)-R(t-\Delta) \leq \alpha^u(\Delta)$$

The two subcases lead to the same conclusion:

$$\begin{aligned}\forall x \in [0,T], \quad \alpha^l(t-x) + R(x) - R(t-\Delta) &\leq \alpha^u(\Delta)\\ \sup_{x\in[0,T]} \{\alpha^l(t-x) + R(x)\} - R(t-\Delta) &\leq \alpha^u(\Delta)\\ R'(t) - R'(t-\Delta) &\leq \alpha^u(\Delta) \qquad \begin{array}{r}(\text{since } t-\Delta \leq T,\\ R(t-\Delta) = R'(t-\Delta))\end{array}\end{aligned}$$

So, R' is valid w.r.t. α^u. This concludes the proof for the first implication.

We can notice that our proof used the fact that (α^u, α^l) is SA-SA, but we will show later that the implication actually holds for any pair of arrival curves. The same is not true for the second implication proved below: not only the proof will use the sub-additivity, but the implication would actually not hold for arbitrary curves.

$\Leftarrow$: Suppose (α^u, α^l) is SA-SA and causal.

- Let's show that $\forall \Delta \in \mathcal{T}, \alpha^l(\Delta) = (\alpha^l \oslash \alpha^u)(\Delta)$. By definition, $(\alpha^l \oslash \alpha^u)(\Delta) = \sup_{t\geq 0}\{\alpha^l(\Delta + t) - \alpha^u(t)\}$. This supremum is obtained for $t = 0$ with the value $\alpha^l(\Delta)$:

  Since (α^u, α^l) is SA-SA and causal, applying the lemma 4, we know that $\alpha^l \models (\alpha^u, \alpha^l)$. So in particular, $\forall t \geq 0, \alpha^l(\Delta + t) - \alpha^l(\Delta) \leq \alpha^u(t)$, which leads to the conclusion.
- We can show that $\alpha^u = \alpha^u \mathbin{\overline{\oslash}} \alpha^l$ in a similar way.

□

3.3.2 Causality and SA-SA closure

The following theorem is the equivalence (b) in Figure 2.

Theorem 6. *Let (α^u, α^l) be a pair of arrival curves.*

$$(\alpha^u, \alpha^l) \text{ is causal} \iff (\overline{\alpha^u}, \underline{\alpha^l}) \text{ is causal}$$

The proof will use the following lemma:

Lemma 7. *For any pair of arrival curves (α^u, α^l), any $T \geq 0$, and any cumulative curve R, we have:*

$$R \models_{\leq T} (\alpha^u, \alpha^l) \iff R \models_{\leq T} (\overline{\alpha^u}, \underline{\alpha^l})$$

To simplify the notations, we write $\alpha^{l(n)} \stackrel{\text{def}}{=} \overline{\otimes}^n \alpha^l$ and $\alpha^{u(n)} \stackrel{\text{def}}{=} \otimes^n \alpha^u$. The notation is ambiguous, but we use the shortcut only when it is clear by the context (lower bounds α^l always use the $\overline{\otimes}$ operator, while upper bounds α^u always use the $\otimes$ operator).

for lemma 7.

- $\Longrightarrow$: We show by induction that $\forall N \geq 1, R \models_{\leq T} \alpha^{u(N)}$. The base case $N = 1$ is our hypothesis, and assuming $R \models_{\leq T} \alpha^{u(N)}$, we have:

$$\begin{aligned}\forall t \geq T, \forall \Delta \in [0,t], \forall s \in [t-\Delta, t] \quad R(t) - R(t-\Delta) &= R(t) - R(s) + R(s) - R(t-\Delta)\\ &\leq \alpha^{u(N)}(t-s) + \alpha^u(s-(t-\Delta))\end{aligned}$$

Therefore, $\forall t \geq T, \forall s \in [0,t]$,

$$R(t) - R(t-\Delta) \leq \inf_{t-s\in[0,\Delta]} \{\alpha^{u(N)}(t-s) + \alpha^u(s-(t-\Delta))\} = \alpha^{u(N+1)}(\Delta)$$

Which concludes the induction:

$$\forall N \in \mathcal{N}, \forall t \geq T, \forall \Delta \in [0,t] \quad R(t) - R(t-\Delta) \leq \alpha^{u(N)}(\Delta)$$

and therefore

$$\forall t \geq T, \forall \Delta \in [0,t], \quad R(t) - R(t-\Delta) \leq \inf_{N \geq 1} \{\alpha^{u(N)}(\Delta)\} = \overline{\alpha^u}(\Delta)$$

This concludes the proof for α^u, the proof for α^l would be the same.

- $\Longleftarrow$: trivial since $(\overline{\alpha^u}, \underline{\alpha^l}) \leq_{AC} (\alpha^u, \alpha^l)$.

□

for theorem 6. The definition of causality states:

$$(\alpha^u, \alpha^l) \text{ causal} \iff \left(\begin{array}{c} \forall T \geq 0, \forall R, \left(R \models_{\leq T} (\alpha^u, \alpha^l)\right) \\ \Longrightarrow \\ \exists R' \mid R' \models (\alpha^u, \alpha^l) \text{ and } \forall t \leq T, R(t) = R'(t) \end{array} \right)$$

Lemma 2 applied to R' gives $R' \models (\alpha^u, \alpha^l) \iff R' \models (\overline{\alpha^u}, \underline{\alpha^l})$, and lemma 7 gives directly $\forall T \geq 0, R \models_{\leq T} (\alpha^u, \alpha^l) \iff R \models_{\leq T} (\overline{\alpha^u}, \underline{\alpha^l})$. Therefore, the equation above can be rewritten as

$$\begin{aligned} (\alpha^u, \alpha^l) \text{ causal} &\iff \left(\begin{array}{c} \forall T \geq 0, \forall R, \left(R \models_{\leq T} (\overline{\alpha^u}, \underline{\alpha^l})\right) \\ \Longrightarrow \\ \exists R' \mid R' \models (\overline{\alpha^u}, \underline{\alpha^l}) \text{ and } \forall t \leq T, R(t) = R'(t) \end{array} \right) \\ &\iff (\overline{\alpha^u}, \underline{\alpha^l}) \text{ is causal} \end{aligned}$$

□

3.3.3 General Characterization of Causality

The result given below can be summarized as "a pair of arrival curves is causal if and only if its SA-SA closure has no forbidden region". This is the equivalence (c) in Figure 2. Formally, this is:

Theorem 8. *Let (α^u, α^l) a pair of arrival curves.*

$$\begin{array}{c} \underline{\alpha^l} = \underline{\alpha^l} \oslash \overline{\alpha^u} \\ \textit{and} \\ \overline{\alpha^u} = \overline{\alpha^u} \overline{\oslash} \underline{\alpha^l} \end{array} \iff (\alpha^u, \alpha^l) \textit{ is causal}$$

This theorem gives a characterization of causality, valid for any pair of curves (unlike theorem 5 which stated an equivalence valid only for SA-SA pairs of curves). The proof for theorem 8 is basically obtained by transitivity of theorems 6 and 5.

3.3.4 Implication Between Absence of Forbidden Regions and Causality

The main result of the section states that if a pair of curves doesn't have any forbidden region, then its SA-SA closure doesn't have any either.

In the whole section, (α^u, α^l) is a pair of arrival curves. The goal of the section is to show that $\left(\begin{array}{c} \alpha^l = \alpha^l \oslash \alpha^u \\ \text{and} \\ \alpha^u = \alpha^u \overline{\oslash} \alpha^l \end{array} \right) \Rightarrow \left(\begin{array}{c} \underline{\alpha^l} = \underline{\alpha^l} \oslash \overline{\alpha^u} \\ \text{and} \\ \overline{\alpha^u} = \overline{\alpha^u} \overline{\oslash} \underline{\alpha^l} \end{array} \right)$ (implication (d) on Figure 2). We will prove this in several steps, given by the following lemmas:

Lemma 9.

$$\left(\begin{array}{c} \alpha^l = \alpha^l \oslash \alpha^u \\ \textit{and} \\ \alpha^u = \alpha^u \overline{\oslash} \alpha^l \end{array} \right) \Rightarrow \left(\begin{array}{c} \alpha^l = \alpha^l \oslash \overline{\alpha^u} \\ \textit{and} \\ \alpha^u = \alpha^u \overline{\oslash} \underline{\alpha^l} \end{array} \right)$$

Lemma 10.

$$\left(\begin{array}{c} \alpha^l = \alpha^l \oslash \alpha^u \\ \textit{and} \\ \alpha^u = \alpha^u \overline{\oslash} \alpha^l \end{array} \right) \Rightarrow \left(\begin{array}{c} \underline{\alpha^l} = \underline{\alpha^l} \oslash \alpha^u \\ \textit{and} \\ \overline{\alpha^u} = \overline{\alpha^u} \overline{\oslash} \alpha^l \end{array} \right)$$

Theorem 11.

$$\left(\begin{array}{c}\alpha^l = \alpha^l \oslash \alpha^u \\ \textit{and} \\ \alpha^u = \alpha^u \,\overline{\oslash}\, \alpha^l\end{array}\right) \Rightarrow \left(\begin{array}{c}\underline{\alpha^l} = \underline{\alpha^l} \oslash \overline{\alpha^u} \\ \textit{and} \\ \overline{\alpha^u} = \overline{\alpha^u} \,\overline{\oslash}\, \underline{\alpha^l}\end{array}\right)$$

For each lemma/theorem, we show only the implication for the first equality, but the proof for the second would be similar.

for lemma 9. We first prove by induction that

$$\forall N \geq 1, \quad \alpha^l \oslash \left(\alpha^{u(N)}\right) = \alpha^l$$

The base case is $\alpha^l = \alpha^l \oslash \alpha^u$, which is the hypothesis of the lemma, and assuming $\alpha^l \oslash \alpha^{u(N)} = \alpha^l$, we have:

$$\begin{aligned}
\alpha^l \oslash \alpha^{u(N+1)} &= \alpha^l \oslash \left[\alpha^{u(N)} \otimes \alpha^u\right] && \text{(by definition of } \alpha^{u(N)}\text{)} \\
&= \left[\alpha^l \oslash \alpha^{u(N)}\right] \oslash \alpha^u && \text{(since } (f \oslash g) \oslash h = f \oslash (g \otimes h)\text{,} \\
& && \text{see [11] p. 123)} \\
&= \alpha^l \oslash \alpha^u && \text{(by induction hypothesis)} \\
&= \alpha^l && \text{(hypothesis of the lemma)}
\end{aligned}$$

Which concludes the induction. Now, we can write, $\forall t \geq 0$,

$$\begin{aligned}
\alpha^l(t) &= \sup_{N\geq 1} \left\{ \left(\alpha^l \oslash \left[\alpha^{u(N)}\right]\right)(t) \right\} \\
&= \sup_{N\geq 1} \left\{ \sup_{\Delta\geq 0} \left\{ \alpha^l(t+\Delta) - \left[\alpha^{u(N)}(\Delta)\right] \right\} \right\} && \text{(definition of } \oslash\text{)} \\
&= \sup_{\Delta\geq 0} \left\{ \alpha^l(t+\Delta) - \inf_{N\geq 1} \left\{ \alpha^{u(N)}(\Delta) \right\} \right\} \\
&= \sup_{\Delta\geq 0} \left\{ \alpha^l(t+\Delta) - \overline{\alpha^u}(\Delta) \right\} && \text{(definition of } \overline{\alpha^u}\text{)} \\
&= (\alpha^l \oslash \overline{\alpha^u})(t) && \text{(definition of } \oslash\text{)}
\end{aligned}$$

□

for lemma 10. We first show, by induction, that:

$$\forall N \geq 1, \quad \alpha^{l^{(N)}} = \alpha^{l^{(N)}} \oslash \alpha^u$$

The base case is $\alpha^l = \alpha^l \oslash \alpha^u$, which is our hypothesis. For $N \geq 1$, we assume $\alpha^{l^{(N)}} = \alpha^{l^{(N)}} \oslash \alpha^u$. To prove $\alpha^{l^{(N+1)}} = \alpha^{l^{(N+1)}} \oslash \alpha^u$, we will show that:

$$\forall t \geq 0, \forall \Delta \geq 0, \quad \alpha^{l^{(N+1)}}(t) + \alpha^u(\Delta) \geq \alpha^{l^{(N+1)}}(t+\Delta) \qquad \text{i.e:}$$

$$\forall t \geq 0, \forall \Delta \geq 0, \quad \alpha^{l^{(N+1)}}(t) + \alpha^u(\Delta) \geq \sup_{x\in[0,t+\Delta]} \{\alpha^{l^{(N)}}(x) + \alpha^l(t+\Delta-x)\} \qquad \text{i.e:}$$

$$\forall t \geq 0, \forall \Delta \geq 0, \forall x \in [0, t+\Delta], \quad \alpha^{l^{(N+1)}}(t) + \alpha^u(\Delta) \geq \alpha^{l^{(N)}}(x) + \alpha^l(t+\Delta-x)$$

Let $t \geq 0$, $\Delta \geq 0$ and $x \in [0, t+\Delta]$. We distinguish two cases on x:

- If $x \geq t$, then we can write:

$$\begin{aligned} \alpha^u(\Delta) - \alpha^l(\Delta - x + t) &\geq \alpha^u(x - t) && \text{(since } \alpha^u = \alpha^u \overline{\oslash}\, \alpha^l \text{, hypothesis of lemma)} \\ {\alpha^l}^{(N)}(x) - \alpha^u(x - t) &\leq {\alpha^l}^{(N)}(t) && \text{(since } {\alpha^l}^{(N)} = {\alpha^l}^{(N)} \oslash \alpha^u \text{,} \\ & && \text{the induction hypothesis)} \end{aligned}$$

  The rest of the proof follows from the combination of these equations:

$$\begin{aligned} \alpha^u(\Delta) - \alpha^l(\Delta - x + t) \geq \alpha^u(x - t) \geq {\alpha^l}^{(N)}(x) - {\alpha^l}^{(N)}(t) \\ \alpha^u(\Delta) + {\alpha^l}^{(N)}(t) \geq {\alpha^l}^{(N)}(x) + \alpha^l(\Delta - x + t) \end{aligned}$$

  Since ${\alpha^l}^{(N+1)}(t) \geq {\alpha^l}^{(N)}(t)$, we can apply the same reasoning, swapping $x - t$ and $t - x$:

$$\begin{aligned} &\alpha^u(\Delta) + {\alpha^l}^{(N+1)}(t) \geq \alpha^u(\Delta) + {\alpha^l}^{(N)}(t) \geq {\alpha^l}^{(N)}(x) + \alpha^l(\Delta - x + t) \\ &{\alpha^l}^{(N+1)}(t) + \alpha^u(\Delta) \geq {\alpha^l}^{(N)}(x) + \alpha^l(t + \Delta - x) && \text{(variables reordering)} \end{aligned}$$

- If $x < t$, then we can write:

$$\begin{aligned} \alpha^l(t + \Delta - x) - \alpha^u(\Delta) &\leq \alpha^l(t - x) && \text{(since } \alpha^l = \alpha^l \oslash \alpha^u \text{, hypothesis of lemma)} \\ {\alpha^l}^{(N+1)}(t) &\geq {\alpha^l}^{(N)}(x) + \alpha^l(t - x) && \text{(by definition of } {\alpha^l}^{(N+1)}\text{)} \end{aligned}$$

  The rest of the proof follows from the combination of these equations:

$$\begin{aligned} \alpha^l(t + \Delta - x) - \alpha^u(\Delta) \leq \alpha^l(t - x) \leq {\alpha^l}^{(N+1)}(t) - {\alpha^l}^{(N)}(x) \\ {\alpha^l}^{(N+1)}(t) + \alpha^u(\Delta) \geq {\alpha^l}^{(N)}(x) + \alpha^l(t + \Delta - x) \end{aligned}$$

Both cases prove that ${\alpha^l}^{(N+1)}(t) + \alpha^u(\Delta) \geq {\alpha^l}^{(N)}(x) + \alpha^l(t + \Delta - x)$, and thus $\forall t \geq 0, \Delta \geq 0, {\alpha^l}^{(N+1)}(t) + \alpha^u(\Delta) \geq {\alpha^l}^{(N+1)}(t + \Delta)$. This implies by definition of $\oslash$ that $\forall t \geq 0, {\alpha^l}^{(N+1)}(t) \geq ({\alpha^l}^{(N+1)} \oslash \alpha^u)(t)$. As for any functions f and g, $f \oslash g \geq f$, the induction goal is proved.

Hence, $\forall N \geq 1, {\alpha^l}^{(N)} = {\alpha^l}^{(N)} \oslash \alpha^u$. The rest of the proof is a simple application of the lower semi-continuity of the $\oslash$ operator with respect to its left operand, as stated in [11] page 135. To make this proof self-contained, we detail the steps:

$$\begin{aligned} \forall t, \underline{\alpha^l}(t) &= \sup_{N \geq 1} \left\{ {\alpha^l}^{(N)}(t) \right\} && \text{(definition of } \underline{\alpha^l}\text{)} \\ &= \sup_{N \geq 1} \left\{ \left({\alpha^l}^{(N)} \oslash \alpha^u \right)(t) \right\} && \text{(applying the result of the induction)} \\ &= \sup_{N \geq 1} \left\{ \sup_{\Delta \geq 0} \left\{ {\alpha^l}^{(N)}(t + \Delta) - \alpha^u(\Delta) \right\} \right\} && \text{(definition of } \oslash\text{)} \\ &= \sup_{\Delta \geq 0} \left\{ \sup_{N \geq 1} \left\{ {\alpha^l}^{(N)}(t + \Delta) \right\} - \alpha^u(\Delta) \right\} \\ &= \underline{\alpha^l} \oslash \alpha^u \end{aligned}$$

□

for theorem 11. Let (α^u, α^l) be a pair of arrival curves, such that

$$\left(\begin{array}{c} \alpha^l = \alpha^l \oslash \alpha^u \\ \text{and} \\ \alpha^u = \alpha^u \overline{\oslash}\, \alpha^l \end{array} \right)$$

From lemma 9 and 10, the following equalities also hold:

$$\alpha^l = \alpha^l \oslash \overline{\alpha^u} \tag{1}$$
$$\overline{\alpha^u} = \overline{\alpha^u} \,\overline{\oslash}\, \alpha^l \tag{2}$$
$$\alpha^u = \alpha^u \,\overline{\oslash}\, \underline{\alpha^l} \tag{3}$$
$$\underline{\alpha^l} = \underline{\alpha^l} \oslash \alpha^u \tag{4}$$

Equations 1 and 2 give us the hypothesis to apply apply lemma 10 to $(\overline{\alpha^u}, \alpha^l)$ and get $\underline{\alpha^l} = \underline{\alpha^l} \oslash \overline{\alpha^u}$. Similarly, equations 3 and 4 allow us to apply lemma 10 to $(\alpha^u, \underline{\alpha^l})$, which gives us $\overline{\alpha^u} = \overline{\alpha^u} \,\overline{\oslash}\, \underline{\alpha^l}$. □

3.3.5 Sufficient Condition for Causality

The last theorem of this section gives a sufficient condition for the causality of a curve. Informally, it states that a pair of curves without forbidden regions is causal. This is implication (e) on Figure 2.

Theorem 12. *Let (α^u, α^l) a pair of arrival curves.*

$$\left(\begin{array}{c} \alpha^l = \alpha^l \oslash \alpha^u \\ \textit{and} \\ \alpha^u = \alpha^u \,\overline{\oslash}\, \alpha^l \end{array}\right) \Longrightarrow (\alpha^u, \alpha^l) \textit{ is causal}$$

The proof is basically obtained by transitivity of theorems 11 and 5.

3.3.6 Causality does not Imply Absence of Forbidden Regions

We just saw that

$$\begin{array}{c} \alpha^l = \alpha^l \oslash \alpha^u \\ \text{and} \\ \alpha^u = \alpha^u \,\overline{\oslash}\, \alpha^l \end{array} \Longrightarrow (\alpha^u, \alpha^l) \text{ is causal}$$

The converse is *false* as shown in the counter-example of Figure 4. The vertically hatched region is a forbidden region, and we do not have $\alpha^l = \alpha^l \oslash \alpha^u$, but the curve is still causal. Actually, the forbidden region is below $\underline{\alpha^l}$, so it is not reachable.

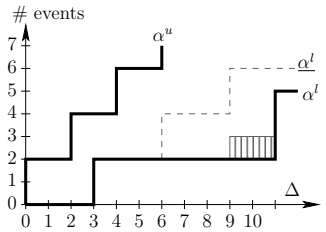
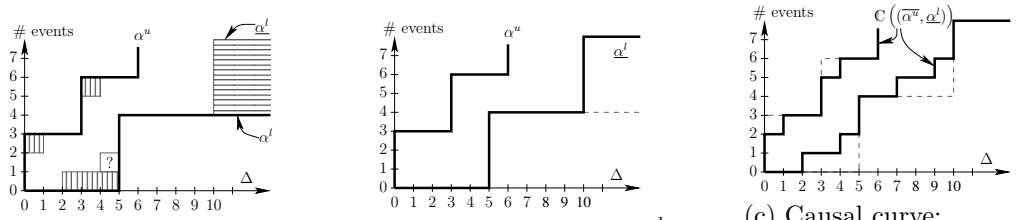


Figure 4: Causal Curve with a Forbidden Region

4 Computing the Causality Closure

The goal of this section is to define the causality closure of a pair of curves (α^u, α^l): it is a pair of arrival curves which is causal and equivalent to (α^u, α^l). The first step is to define the $\mathbb{C}$ operator, which removes the forbidden regions from a pair of curves.

Notice that removing forbidden regions is done on the pair of curves, globally. As a result, while removing the forbidden regions on α^l, one may introduce new ones on α^u and vice-versa.



(a) Original curve: (α^u, α^l) (b) SA-SA curve: $(\overline{\alpha^u}, \underline{\alpha^l})$ (c) Causal curve: $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$

Figure 5: Step-by-step causality closure

One natural way to solve this issue is to iterate the forbidden region removal until one reaches the fix-point (assuming it is reached in a finite number of steps, which is not always the case).

To illustrate this, an example is given in Figure 5. The original curve (a) has both forbidden regions (vertically hatched) and an unreachable region (horizontally hatched).

One region of interest is the little square between $\Delta = 4$ and $\Delta = 5$, marked with a "?" in curve (a): if we consider the curves (α^u, α^l) before any transformation, it does not seem to be a forbidden region. An execution emitting only 1 event in 4 units of time seems to be able to continue by emitting 3 events right after. Actually, this is impossible, and there are at least two ways to show it. the first way to remove this "?"-region is to apply the forbidden regions removal twice: emitting 3 events as suggested above is not possible given the leftmost forbidden region of α^u. So, the "?"-region will have to be removed, as a consequence of the forbidden region on α^u. After the second iteration of the forbidden region removal, we reached the fix-point, and implication **(e)** guarantees the causality. This iterative approach will be detailed in Section 5.1.

However, an interesting property of the $\mathbb{C}$ operator is that it does not create new forbidden regions when applied on SA-SA curves (this will be lemma 17). Back to the example in Figure 5, a second way to show that the "?"-region should be removed from α^l is to work on $\underline{\alpha^l}$ instead of α^l: since $\underline{\alpha^l}(10) = 8$ and $\overline{\alpha^u}(6) = 6$, an execution has to emit at least two events in 4 units of time. This illustrates the approach followed in this section: we eliminate the forbidden regions with $\mathbb{C}$ (5.(c)) only after performing an SA-SA closure (5.(b)). The iterative approach will be kept for cases where the SA-SA closure cannot be applied due to algorithmic and coding limitations.

4.1 Removing Forbidden Regions: the $\mathbb{C}$ Operator

We defined pairs of arrival curves as pairs (α^u, α^l) of functions for which $\alpha^u \geq \alpha^l$. In addition, we write $\perp_{AC}$ the set of pairs of functions in $\mathcal{F}$ such that the former constraint is false. To simplify notations, $\perp_{AC}$ will be used as a single element even if it represents an infinite set of objects. We note AC the set of all pairs of arrival curves *plus* $\perp_{AC}$.

Definition 12 (Order on AC)**.** *Let (α^u, α^l) and $(\alpha^{u\prime}, \alpha^{l\prime})$ be two pairs of arrival curves. We say that $(\alpha^{u\prime}, \alpha^{l\prime})$ is tighter (meaning: more precise) than (α^u, α^l) (noted $(\alpha^{u\prime}, \alpha^{l\prime}) \leq_{AC} (\alpha^u, \alpha^l)$) iff(def) $\alpha^{l\prime} \geq \alpha^l$ and $\alpha^{u\prime} \leq \alpha^u$ We extend the $\leq_{AC}$ relation to any object of AC by: $\forall e \in AC \,.\, \perp_{AC} \leq_{AC} e$*

This is trivial to show that $\leq_{AC}$ is an order on the set AC.

Definition 13. *We define the $\mathbb{C}$ operator from AC to AC as:*

$$\mathbb{C}\left(\perp_{AC}\right) \stackrel{def}{=} \perp_{AC} \quad \text{and} \quad \mathbb{C}\left(\alpha^l, \alpha^u\right) \stackrel{def}{=} \begin{cases} \text{let } L = \alpha^l \oslash \alpha^u, U = \alpha^u \overline{\oslash} \alpha^l \\ \text{if } L \leq U \text{ then } (L, U) \\ \text{else } \perp_{AC} \end{cases}$$

When $\mathbb{C}\left(\alpha^u, \alpha^l\right) \neq \perp_{AC}$, we note $(\alpha^{u*}, \alpha^{l*}) \stackrel{def}{=} \mathbb{C}\left(\alpha^u, \alpha^l\right)$

α^{u*} and α^{l^*} are shortcuts for the $\mathbb{C}$ operator, but the reader should note that α^{u*} is indeed a function of both α^u and α^l.

When (α^u, α^l) is a pair of arrival curves then $L = \alpha^l \oslash \alpha^u$ and $U = \alpha^u \overline{\oslash} \alpha^l$ are functions in $\mathcal{F}$ (i.e. wide-sense increasing and equal to zero at zero). But they may cross each other (it may happen that $L \not\leq U$): in these cases, the $\mathbb{C}$ operator computes the value $\perp_{AC}$. This means that the pair of arrival curves was not satisfiable (i.e. no cumulative curve satisfies it), as stated in lemma 14.

Lemma 13. *Let (α^u, α^l) be a pair of arrival curves. When these values are defined (i.e. $\mathbb{C}\left(\alpha^l, \alpha^u\right) \neq \perp_{AC}$), we have $\alpha^{l^*} \geq \alpha^l$ and $\alpha^{u*} \leq \alpha^u$.*

Proof. Trivial by definition of $\mathbb{C}$. □

Lemma 14 (Equivalence of (α^u, α^l) and $\mathbb{C}\left(\alpha^u, \alpha^l\right)$)**.** *Let (α^u, α^l) be a pair of arrival curves.*

1. *if $\mathbb{C}\left(\alpha^u, \alpha^l\right) = \perp_{AC}$, then (α^u, α^l) is non-satisfiable;*
2. *(α^u, α^l) and $\mathbb{C}\left(\alpha^u, \alpha^l\right)$ are equivalent.*

for lemma 14, point 1. If $\mathbb{C}\left(\alpha^u, \alpha^l\right) = \perp_{AC}$, this means that $L = \alpha^l \oslash \alpha^u$ and $U = \alpha^u \overline{\oslash} \alpha^l$ have crossed, ie that $L \not\leq U$: $\exists x \mid (\alpha^l \oslash \alpha^u)(x) > (\alpha^u \overline{\oslash} \alpha^l)(x)$. This implies there exists T_1 and T_2 such that:

$$\alpha^u(x + T_1) - \alpha^l(T_1) < \alpha^l(x + T_2) - \alpha^u(T_2) \tag{5}$$

If (α^u, α^l) was satisfiable, there would exist a cumulative curve R that complies with (α^u, α^l). We apply the definition to interval $[0, T_1 + T_2 + x]$:

$$R(T_1 + x + T_2) \leq \alpha^u(T_1 + x + T_2) \qquad \text{(definition of } \alpha^u\text{)} \tag{6}$$
$$R(T_1 + x + T_2) \leq \alpha^u(T_2) + \alpha^u(T_1 + x) \qquad \text{(super-additivity of } \alpha^u\text{)} \tag{7}$$
$$R(T_1 + x + T_2) \geq \alpha^l(x + T_2 + T_1) \qquad \text{(definition of } \alpha^l\text{)} \tag{8}$$
$$R(T_1 + x + T_2) \geq \alpha^l(x + T_2) + \alpha^l(T_1) \qquad \text{(sub-additivity of } \alpha^l\text{)} \tag{9}$$

The two equations 7 and 9 contradict the equation 5. This proves that (α^u, α^l) is not satisfiable. □

for lemma 14, point 2. Let R be a cumulative curve.

$R \models \mathbb{C}\left(\alpha^u, \alpha^l\right) \implies R \models (\alpha^u, \alpha^l)$ is a direct consequence of lemma 13.

We show the counter-part by contrapositive. Let us assume that $R \not\models (\alpha^{u*}, \alpha^{l^*})$. Then, either (a) $\exists t, \Delta \geq 0 \mid R(t) - R(t-\Delta) < \alpha^{l^*}(\Delta)$ or (b) $\exists t, \Delta \geq 0 \mid R(t) - R(t-\Delta) > \alpha^{u*}(\Delta)$. We focus on the case (a) (the case (b) is the same): let $t, \Delta \geq 0$ such that $R(t) - R(t-\Delta) < \alpha^{l^*}(\Delta)$. Then, by definition of α^{l^*},

$$R(t) - R(t-\Delta) < \sup_{t' \geq \Delta} \{\alpha^l(t') - \alpha^u(t' - \Delta)\}$$
$$\exists t' \geq \Delta \quad \mid \quad R(t) - R(t-\Delta) < \alpha^l(t') - \alpha^u(t' - \Delta)$$

To simplify the formulas, we set $T_a = t - \Delta$, $T_b = t$ and $T_c = t - \Delta + t'$. The above rewrites to

$$R(T_b) - R(T_a) < \alpha^l(T_c - T_a) - \alpha^u(T_c - T_b) \tag{10}$$

We will now show that R violates either α^u or α^l. If $R \not\models \alpha^l$ then the proof is complete. We therefore assume it is not the case and prove that α^u is violated. We can write:

$$R(T_c) - R(T_a) \geq \alpha^l(T_c - T_a) \qquad \text{(since } R \models \alpha^l\text{)}$$
$$R(T_a) - R(T_b) > \alpha^u(T_c - T_b) - \alpha^l(T_c - T_a) \qquad \text{(reordering of equation 10)}$$

summing the two above equations, we get:

$$R(T_c) - R(T_b) > \alpha^u(T_c - T_b)$$

□

4.2 $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$: the Canonical Representative and its Properties

This section presents the main result of the paper. It basically states that $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$ has many desirable properties: SA-SA, causality, and it is indeed the best possible pair of curves equivalent to (α^u, α^l). We will start with some lemma and their demonstration, and will proceed with the main theorems (easy to prove given the lemmas) in section 4.2.2.

4.2.1 A Few Useful Lemmas

Lemma 15 (SA-SA preservation)**.** *Let (α^u, α^l) be a SA-SA pair of arrival curves. If $\mathbb{C}(\alpha^u, \alpha^l) \neq \perp_{AC}$, then $\mathbb{C}(\alpha^u, \alpha^l)$ is SA-SA.*

Lemma 16 (Validity of α^{l^*} and α^{u*} with respect to themselves)**.** *Let (α^u, α^l) be a SA-SA pair of arrival curves. If $\mathbb{C}(\alpha^u, \alpha^l) \neq \perp_{AC}$, then*

$$\alpha^{l^*} \models (\alpha^{u*}, \alpha^{l^*})$$
$$\alpha^{u*} \models (\alpha^{u*}, \alpha^{l^*})$$

Lemma 17 (Absence of forbidden regions)**.** *Let (α^u, α^l) be a SA-SA pair of arrival curves. If $\mathbb{C}(\alpha^u, \alpha^l) \neq \perp_{AC}$, then $(\alpha^{u*}, \alpha^{l^*})$ is a fix-point of $\mathbb{C}$, i.e.*

$$\alpha^{l^*} = \alpha^{l^*} \oslash \alpha^{u*}$$
$$\text{and}$$
$$\alpha^{u*} = \alpha^{u*} \overline{\oslash} \alpha^{l^*}$$

Applying Theorem 12, this implies that $(\alpha^{u*}, \alpha^{l^*})$ is causal. Intuitively, the theorem states that, removing forbidden regions on SA-SA curves once will not create new forbidden regions. On the example of Figure 5 page 16, this means that since the curve (b) is SA-SA, then (c) has no forbidden regions anymore.

for lemma 15. Let $t \geq 0$, let $s \in [0, t]$. By definition of $\alpha^{l^*}(t-s)$ and $\alpha^{l^*}(s)$, we have:

$$\alpha^{l^*}(t-s) = \sup_{x \geq 0}\{\alpha^l(t-s+x) - \alpha^u(x)\}$$
$$\alpha^{l^*}(s) = \sup_{y \geq 0}\{\alpha^l(s+y) - \alpha^u(y)\}$$

Therefore, we have:

$$\begin{aligned}
&\alpha^{l^*}(t-s) - \alpha^{l^*}(s) \\
&= \sup_{x,y \geq 0} \{\alpha^l(t-s+x) - \alpha^l(s+y) - \alpha^u(x) + \alpha^u(y)\} \\
&= \sup_{x,y \geq 0} \{\alpha^l(t-s+x) - \alpha^l(s+y) - (\alpha^u(x-y+y) - \alpha^u(y))\} \\
&\geq \sup_{x,y \geq 0} \{\alpha^l(t-s+x) - \alpha^l(s+y) - \alpha^u(x-y)\} && \text{(sub-additivity of } \alpha^u\text{)} \\
&\geq \sup_{x,y \geq 0} \{\alpha^l(t-s+x) - \alpha^l(s+y) - \alpha^u(x+y)\} && \left(\begin{array}{l} x+y \geq x-y \Rightarrow \\ -\alpha^u(x-y) \geq -\alpha^u(x+y) \end{array}\right) \\
&\geq \sup_{x,y \geq 0} \{\alpha^l((t+x+y)-(s+y)) - \alpha^l(s+y) - \alpha^u(x+y)\} \\
&\geq \sup_{x,y \geq 0} \{\alpha^l(t+x+y) - \alpha^u(x+y)\} && \text{(super-additivity of } \alpha^l\text{)} \\
&\geq \sup_{z \geq 0}\{\alpha^l(t+z) - \alpha^u(z)\} && \text{(setting } z = x+y\text{)} \\
&\geq \alpha^{l^*}(t) && \text{(definition of } \alpha^{l^*}\text{)}
\end{aligned}$$

□

for lemma 16. We'll prove the first equation (the other is similar).

The key argument is that: $\alpha^{l^*} \models (\alpha^{u*}, \alpha^{l^*}) \iff \alpha^{l^*} \models (\alpha^u, \alpha^{l^*})$. We prove it: the forward implication, $\alpha^{l^*} \models (\alpha^{u*}, \alpha^{l^*}) \Rightarrow \alpha^{l^*} \models (\alpha^u, \alpha^{l^*})$, is obvious since $(\alpha^{u*}, \alpha^{l^*}) \leq_{AC} (\alpha^u, \alpha^{l^*})$. The converse, $\alpha^{l^*} \models (\alpha^{u*}, \alpha^{l^*}) \Leftarrow \alpha^{l^*} \models (\alpha^u, \alpha^{l^*})$, is also true, since any curve accepted by (α^u, α^{l^*}) is also accepted by (α^u, α^l) and therefore by $(\alpha^{u*}, \alpha^{l^*})$ (lemma 14).

α^{l^*} being super-additive (lemma 15), it is valid with respect to itself. We only have to prove that α^{l^*} is valid with respect to α^u: let $t \geq 0$ and $s \leq t$

$$\begin{aligned}
\alpha^{l^*}(t) &= \sup_{x\geq 0}\{\alpha^l(t+x) - \alpha^u(x)\} && \text{(by definition)}\\
\alpha^{l^*}(s) &= \sup_{x\geq 0}\{\alpha^l(s+x) - \alpha^u(x)\} \\
&\geq \sup_{y\geq 0}\{\alpha^l(t+y) - \alpha^u(y+t-s)\} && \text{(with } x = t+y-s\text{)}
\end{aligned}$$

Combining those equations,

$$\begin{aligned}
&\alpha^{l^*}(t) - \alpha^{l^*}(s) \\
&\quad\leq \sup_{x\geq 0, y\geq 0}\{\alpha^l(t+x) - \alpha^l(t+y) + \alpha^u(y+t-s) - \alpha^u(x)\} \\
&\quad\leq \sup_{x\geq 0}\{\alpha^l(t+x) - \alpha^l(t+x) + \alpha^u(x+t-s) - \alpha^u(x)\} && \text{(with } y = x\text{)}\\
&\quad\leq \sup_{x\geq 0}\{\alpha^u(x+(t-s)) - \alpha^u(x)\} \\
&\quad\leq \sup_{x\geq 0}\{\alpha^u(t-s) + \alpha^u(x) - \alpha^u(x)\} && \text{(sub-additivity of } \alpha^u\text{)}\\
&\quad\leq \alpha^u(t-s)
\end{aligned}$$

□

for lemma 17. We'll prove $\alpha^{l^*} = \alpha^{l^*} \oslash \alpha^{u*}$, the other equation could be proved similarly. This is equivalent to prove that $\forall t \geq 0, s \geq t, \alpha^{l^*}(s) - \alpha^{l^*}(t) \leq \alpha^{u*}(s-t)$ which is actually implied by $\alpha^{l^*} \models (\alpha^{u*}, \alpha^{l^*})$, itself guaranteed by lemma 16. □

4.2.2 Key Theorems

Theorem 18. *For any pair of arrival curves (α^u, α^l),*

- $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l}) = \perp_{AC}$ *iff* (α^u, α^l) *is non-satisfiable;*
- $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$ *is causal, SA-SA and equivalent to* (α^u, α^l)*, otherwise.*

Proof. Firstly, lemma 2 (stating that (α^u, α^l) and $(\overline{\alpha^u}, \underline{\alpha^l})$ are equivalent) and Lemma 14 (stating that $\mathbb{C}\underline{\alpha^l}, \overline{\alpha^u} = \perp_{AC} \implies (\overline{\alpha^u}, \underline{\alpha^l})$ is not satisfiable) give the first direction of the equivalence. Conversely, if (α^u, α^l) is non-satisfiable, let us assume that $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l}) \neq \perp_{AC}$. By lemma 16, $\underline{\alpha^{l^*}}$ complies with $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$ which is thus satisfiable. Lemma 1 ($(\overline{\alpha^u}, \underline{\alpha^l})$ and $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$ are equivalent) contradicts the assumptions.

Secondly, let (α^u, α^l) be satisfiable ($\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l}) \neq \perp_{AC}$) $(\overline{\alpha^u}, \underline{\alpha^l})$ is SA-SA, therefore, lemma 17 applies, which gives us the hypothesis for theorem 5, which ensures causality. Lemma 15 gives the SA-SA property and lemma 1 the equivalence with (α^u, α^l). □

Theorem 19. *For any pair of arrival curves (α^u, α^l),*

- *when (α^u, α^l) is satisfiable, $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$ is the tightest pair of curves equivalent to (α^u, α^l).*

Proof. We note $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l}) = (\overline{\alpha^u}^*, \underline{\alpha^{l^*}})$. Lemma 16 tells that $\underline{\alpha^{l^*}} \models (\overline{\alpha^u}^*, \underline{\alpha^{l^*}})$ and $\overline{\alpha^u}^* \models (\overline{\alpha^u}^*, \underline{\alpha^{l^*}})$.

Any pair of curves equivalent to (α^u, α^l) would therefore have to accept $\underline{\alpha^{l^*}}$ and $\overline{\alpha^u}^*$. $(\overline{\alpha^u}^*, \underline{\alpha^{l^*}})$ would therefore be tighter than any such pair of curves. □

These last two theorems give an interesting result: given any pair of curves, one can compute $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$, and get either the information that the curves are not satisfiable, or the best possible pair of curves equivalent to the original one. In addition to this optimality, one also gets the desirable properties: causality and SA-SA. This result is implementable on top of any algorithmic toolbox implementing the basic operators: convolution, deconvolution, sub-additive and super-additive closure.

Theorem 19 also provides the existence and uniqueness of a tightest pair of curves equivalent to a given one. As a result, the following theorem also holds:

Theorem 20. *Let (α^u, α^l) be a pair of curves. If (α^u, α^l) is the tightest pair of curves representing a set of cumulative curves, then (α^u, α^l) is causal.*

Any computation giving the best possible pair of curves also gives a causal pair of curves. Theorem 20 *explains why*, in practice, most pairs of arrival curves usually manipulated in Real-Time Calculus are causal. Indeed, curves obtained for example by measurements on a real system are causal by construction; furthermore computations made in the RTC framework compute the optimal solution and thus preserve the causality property. It also probably explains why this problem received so little attention up to now.

On the other side, non-causal pairs of curves may arise whenever a computation is done in an *inexact manner*. This typically occurs using other tools than RTC algebraic solutions. Indeed, the recent works that interfaces RTC with state-based models face the problem. In [10, 9], the authors get rid of it by constraining the class of curves they compute which are causal by definition (the extension to arbitrary curves which is part of their future works will have to deal with it though). But, in [1], the output curves are computed, one point at a time on an abstract model: this does result into non causal curves, which are refined after being computed with a causality closure. The CATS tool [20] relies on exact model-checking, so applied on a causal pair of curves, the tool would output causal curves (as long as the model-checker never finishes with a timeout). [16] also uses exact model-checking, but the long-term rate computation uses an approximation, which could generate non-causal curves.

An example where the procedure described in [16] would produce non-causal pairs of curves is given in Figure 6. The black curves are the input curves of the system, the system considered is the identity (i.e. the actual output curves are the same as the input curves). The procedure computes first a finite set of points at the beginning of the curve. In our example, we compute (α^u, α^l) up to $\Delta = 3$. Then, to estimate the long-term rate, one more point is computed, with a larger Δ. In our example, we consider $\Delta = 9$. The actual curve α^l has the value 4 for $\Delta \in [6, 8]$, but we didn't use ECA to compute this value, therefore, the best information we can get using α^l alone is the super-additive closure, represented in dashed red line. As one can see, this curve is not causal: the big step between $\alpha^l(8)$ and $\alpha^l(9)$ is greater than $\alpha^u(1)$.

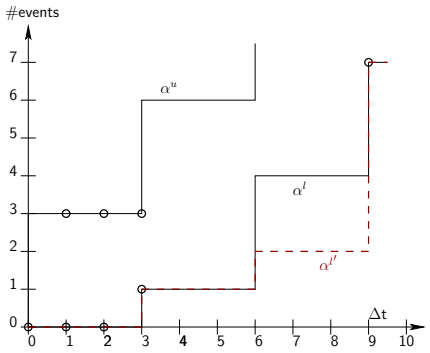


Figure 6: Example of computation of non-causal curve using ECA

On the other hand, computing the causality closure of (α^u, α^l) would remove the forbidden region. In this case, we would re-obtain the exact curve for $\alpha^{l'}$.

Finally, in `ac2lus` [2] we use the abstract interpreter `nbac` [6], which also does some abstractions, and hence doesn't guarantee the causality of the curves computed. The tool applies the causality closure before the computation, so doesn't have problem with non-causal input curves, and can apply the causality operator to the output to possibly increase the precision.

In general, when an algorithm A computes output curves as a function of input curves ($O = A(I)$), and if the algorithm do not work on non-causal curves I and/or may produce non-causal curves O, we can transform this algorithm A into an algorithm A' which accepts non-causal curves and produces only causal curves the following way:

$I^{\text{causal}} \leftarrow \emptyset$
for all $(\alpha^u, \alpha^l) \in I$ **do**
  $I^{\text{causal}} \leftarrow I^{\text{causal}} \cup \mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$ // Causality closure on input
end for
$O^{\text{non-causal}} \leftarrow A(I^{\text{causal}})$ // Actual computation
$O \leftarrow \emptyset$
for all $(\alpha^u, \alpha^l) \in O^{\text{non-causal}}$ **do**
  $O \leftarrow O \cup \mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$ // Causality closure on output
end for
return O

In all the approaches combining RTC and another formalism cited above, the line $O^{\text{non-causal}} \leftarrow A(I^{\text{causal}})$ is by far the most expansive (in time and memory). Hence, the overhead of the causality closure is small, and makes the algorithm more general (accepting non-causal curves) and more precise.

5 Application to Special Classes of Arrival Curves

5.1 Algorithms for Discrete Finite Curves

5.1.1 Definitions of Finite Arrival Curves

Up to this point, we dealt with infinite pairs of curves, but, as mentionned in the introduction, the original work that brought us to studying causality was to connect RTC curves to synchronous programming languages in the tool `ac2lus` [2]. The simplest model of `ac2lus` uses simple computer representation of arrival curves: we work in *discrete-time*, *discrete-event* model, and consider only *finite curves*, which makes them easy to represent and manipulate algorithmically speaking. We consider the infinite extension of the curves to remain in the theoretical framework presented in the previous sections and to be able to apply the same theorems. Therefore, instead of formalizing the notion of *finite* curves, we consider the *restriction* of infinite curves on a *finite* interval.

Working with discrete-time (resp. discrete-event) models doesn't change the above results, since we considered time (resp. event count) as the set $\mathcal{T}$ (resp. $\mathcal{E}$), being either $\mathcal{R}^+$ or $\mathcal{N}$. We now (in this chapter) set $\mathcal{T} = \mathcal{E} = \mathcal{N}$. On the other hand, working with finite curves will change the results a bit: the notion of SA-SA-closure doesn't fit well in the finite model, since the SA-SA-closure of a finite curve could be infinite.

We will first give some definitions for finite arrival curves, and the finite restriction of the $\mathbb{C}$ operator. Then, we will give an algorithm to compute the causality closure using this restricted $\mathbb{C}$ operator.

Definition 14 (Finite restriction of arrival curves)**.** *We denote by* $(\alpha^u|_T, \alpha^l|_T)$ *the restriction of* (α^u, α^l) to $[0, T]$ *defined as:*

$$\forall t \leq T, \quad \alpha^u|_T(t) \stackrel{def}{=} \alpha^u(t) \text{ and } \alpha^l|_T(t) \stackrel{def}{=} \alpha^l(t)$$
$$\forall t > T, \quad \alpha^u|_T(t) \stackrel{def}{=} +\infty \text{ and } \alpha^l|_T(t) \stackrel{def}{=} \alpha^l(T)$$

$(\alpha^u|_T, \alpha^l|_T)$ still applies to infinite event streams, but only gives constraints for finite windows of time. Intuitively, it could be a pair of curves defined over $[0, T]$. Defining them as functions

over $\mathcal{N}$ has the advantage of remaining within the definition of arrival curves given above: $\alpha^l|_{\mathrm{T}}$ and $\alpha^u|_{\mathrm{T}}$ are still functions in $\mathcal{F}$, but they can be represented easily as finite arrays of naturals.

5.1.2 SA-SA Closure for Finite Discrete Curves

The SA-SA closure has the interesting property that $\overline{\alpha}(t)$ can be computed by looking only at the fragment of the curve *before* t. In other words, one can compute an SA-SA closure by looking only at the past of a curve. As a consequence, working with finite curves works well, since we can compute the closure of $\alpha|_{\mathrm{T}}$ without looking at the portion of α beyond T. Since the finite restriction of a curve is never SA-SA, we need first to define the notion of SA-SA on an interval:

Definition 15 (SA-SA on an interval)**.** *A pair of curves (α^u, α^l) is said to be SA-SA on interval $[0, T]$ iff*

$$\forall t_1, t_2 \geq 0, \quad t_1 + t_2 \leq T \implies \alpha^l(t_1) + \alpha^l(t_2) \leq \alpha^l(t_1 + t_2)$$
$$\forall t_1, t_2 \geq 0, \quad t_1 + t_2 \leq T \implies \alpha^u(t_1) + \alpha^u(t_2) \geq \alpha^l(t_1 + t_2)$$

Definition 16 (Finite SA-SA closure)**.** *The finite SA-SA closure of (α^u, α^l) on interval $[0, T]$ is* $\left(\overline{\alpha^u}|_T, \underline{\alpha^l}|_T\right)$.

Theorem 21 (SA-SA closure for finite curves)**.** *SA-SA closures for the finite restriction of arrival curves are equivalent to the finite restriction of the SA-SA closures.*

$$\begin{aligned} (\overline{\alpha^u})|_T &= \overline{(\alpha^u|_T)}|_T \\ (\underline{\alpha^l})|_T &= \overline{(\alpha^l|_T)}|_T \end{aligned}$$

Proof. Immediate when expanding the definitions of $\overline{\alpha^u}$, $\underline{\alpha^l}$ and $\alpha|_{\mathrm{T}}$ in the equations. □

Strictly speaking, the mathematical object $\overline{(\alpha^u|_{\mathrm{T}})}$ is still an infinite curve, and we do not want to have to deal with it. We therefore work directly with its restriction $\overline{(\alpha^u|_{\mathrm{T}})}|_{\mathrm{T}}$, which is not subadditive.

This implies in particular that we can compute the SA-SA closure of finite curves by considering only the finite fragment, with no loss of precision.

Additionally, an efficient way to compute the SA-SA closure in discrete events is given in [4] page 7.

$$\overline{\alpha^u}(0) = 0; \quad \overline{\alpha^u}(t) = \min\left\{\alpha^u(t), \min_{s \in]0,t[}\{\overline{\alpha^u}(s) + \overline{\alpha^u}(t-s)\}\right\}$$

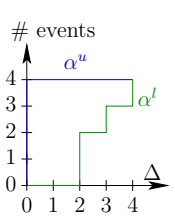
A similar one can be given for $\underline{\alpha^l}$:

$$\underline{\alpha^l}(0) = 0; \quad \underline{\alpha^l}(t) = \max\left\{\alpha^l(t), \max_{s \in]0,t[}\{\underline{\alpha^l}(s) + \underline{\alpha^l}(t-s)\}\right\}$$

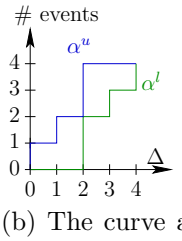
This gives a simple, quadratic algorithm to compute $(\overline{\alpha^u}, \underline{\alpha^l})$.

5.1.3 Causality closure for Finite Discrete Curves

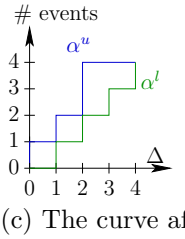
Unfortunately, the valid result for infinite curves, stating that $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l})$ was a causal curve equivalent to (α^u, α^l) is helpless from the algorithmic point of view with finite curves: computing it would require computing $(\overline{\alpha^u}, \underline{\alpha^l})$, which is an infinite curve. But lemma 14 and theorem 12



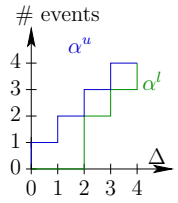
(a) Original curve: (α^u, α^l)



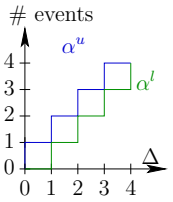
(b) The curve after one step without SA-SA closure: $\mathbb{C}(\alpha^u, \alpha^l)$



(c) The curve after two steps without SA-SA closure: $\mathbb{C}\left(\mathbb{C}(\alpha^u, \alpha^l)\right)$



(d) The curve after one full iteration: SA-SA closure of $\mathbb{C}(\alpha^u, \alpha^l)$



(e) The curve after two full iterations.

Figure 7: Step-by-step causality closure for finite curves

still hold. In other words, applying the $\mathbb{C}$ operator doesn't change the set of accepted cumulative curves, and the fix-points of $\mathbb{C}$ are causal. So, given the fact that we know how to compute the $\mathbb{C}$ operator, an algorithm will therefore be to apply it repeatedly until a fix-point is reached.

We illustrate the process with an example in Figure 7. The original pair of curves is (a), and one can see that although the curves are SA-SA on $[0, 4]$ (but clearly not SA-SA because of the curve α^u with $+\infty$ values), one application of $\mathbb{C}$ is not sufficient: the curve (b) is not even SA-SA on interval $[0, 4]$, and still has forbidden regions. We iterate the $\mathbb{C}$ operator once more and get (c), which is causal, but not SA-SA.

Another option which may speed up the algorithm, is to apply a finite SA-SA closure before applying $\mathbb{C}$ again: this gives curves (d) and then (e) by applying $\mathbb{C}$ again. Then, neither the SA-SA closure nor $\mathbb{C}$ would change the curve anymore: we reached the fix-point. In this case, the final curve has both the causality and the SA-SA properties on interval $[0, 4]$.

Theorem 22. *For any $T > 0$ and any pair of arrival curves (α^u, α^l) with $\forall t \in [0, T], \alpha^u(t) \neq +\infty$, the sequence $\mathbb{C}^n(\alpha^u|_T, \alpha^l|_T)$ admits a fix-point (denoted by $\mathbb{C}^\infty(\alpha^u|_T, \alpha^l|_T)$, which is either $\perp_{AC}$ or a causal pair of arrival curves equivalent to $(\alpha^u|_T, \alpha^l|_T)$.*

Proof. By definition, $\mathbb{C}(\perp_{AC}) = \perp_{AC}$, so if one of the elements of the sequence is $\perp_{AC}$, then it is the fix-point of the sequence.

If none of the elements are $\perp_{AC}$, then, since $\mathbb{C}(\overline{\alpha^u}, \underline{\alpha^l}) \leq_{AC} (\overline{\alpha^u}, \underline{\alpha^l})$ (lemma 13), the sequence is decreasing. The sequence has only a finite set of possible values, and therefore admits a fix-point. By lemma 14, this pair of curves is equivalent to $(\alpha^u|_T, \alpha^l|_T)$, and theorem 12 implies the causality. □

The convergence of the iterations can be accelerated by using, in addition to $\mathbb{C}$, other tightening operators that preserves the set of accepted cumulative curves like the SA-SA closure. This is expressed in the following theorem and applied in the example in Figure 7.(d) and 7.(e).

Theorem 23. *For any $T > 0$ and any pair of arrival curves (α^u, α^l) with $\forall t \in [0, T], \alpha^u(t) \neq +\infty$, the sequence defined by $({\alpha^u}_0, {\alpha^l}_0) = (\alpha^u|_T, \alpha^l|_T)$ and $\forall n \geq 1$, $({\alpha^u}_{n+1}, {\alpha^l}_{n+1}) = \mathbb{C}(\overline{{\alpha^u}_n}|_T, \underline{{\alpha^l}_n}|_T)$ admits a fix-point, which is either $\perp_{AC}$ or a causal and SA-SA pair of arrival curves equivalent to $(\alpha^u|_T, \alpha^l|_T)$.*

Proof. Same as theorem 22. □

We still need a way to compute $\mathbb{C}$ efficiently: the definition of $\mathbb{C}$ contains the supremum of an infinite set, which as it is, would not be computable. Fortunately, the operator $\mathbb{C}$ applied to finite restrictions of curves is indeed much simpler.

Theorem 24. *Let (α^u, α^l) be a pair of curves, and L_r and U_r be defined by:*

$$L_r(x) = \sup_{t\in[0,T-x]} \{\alpha^l\big|_T(x+t) - \alpha^u\big|_T(t)\}$$
$$U_r(x) = \inf_{t\in[0,T]} \{\alpha^u\big|_T(x+t) - \alpha^l\big|_T(t)\}$$

If $L_r \leq U_r$, then $\mathbb{C}(\alpha^u\big|_T, \alpha^l\big|_T) = (L_r, U_r)$, otherwise, $\mathbb{C}(\alpha^u\big|_T, \alpha^l\big|_T) = \bot_{AC}$.

Proof. From the definition of $\mathbb{C}$, we reuse the L and U intermediate variables defined as $L = \alpha^l\big|_{\mathrm{T}} \oslash \alpha^u\big|_{\mathrm{T}}$ and $U = \alpha^u\big|_{\mathrm{T}} \overline{\oslash}\, \alpha^l\big|_{\mathrm{T}}$. By definition of $\alpha^l\big|_{\mathrm{T}}$, we have:

$$\forall t > T - x, \quad \alpha^l\big|_{\mathrm{T}}(x+t) = \alpha^l\big|_{\mathrm{T}}(T)$$

therefore

$$\begin{aligned}\sup_{t>T-x} \{\alpha^l\big|_{\mathrm{T}}(x+t) - \alpha^u\big|_{\mathrm{T}}(t)\} &= \sup_{t>T-x} \{\alpha^l\big|_{\mathrm{T}}(T) - \alpha^u\big|_{\mathrm{T}}(t)\} \\ &= \alpha^l\big|_{\mathrm{T}}(T) - \alpha^u\big|_{\mathrm{T}}(T-x) \qquad \text{(since } \alpha^u\big|_{\mathrm{T}} \text{ is increasing)}\end{aligned}$$

So U can be written as:

$$\begin{aligned}U(x) = (\alpha^l\big|_{\mathrm{T}} \oslash \alpha^u\big|_{\mathrm{T}})(x) &= \sup_{t\geq 0}\{\alpha^l\big|_{\mathrm{T}}(x+t) - \alpha^u\big|_{\mathrm{T}}(t)\} \qquad \text{(by definition)} \\ &= \sup_{t\in[0,T-x]} \{\alpha^l\big|_{\mathrm{T}}(x+t) - \alpha^u\big|_{\mathrm{T}}(t)\} \\ &= U_r(x)\end{aligned}$$

Similarly for L: $\forall t > T - x, \alpha^u\big|_{\mathrm{T}}(x+t)$ is infinite and $\alpha^l\big|_{\mathrm{T}}(t)$ is finite. Therefore

$$\inf_{t\geq T-x} \{\alpha^u\big|_{\mathrm{T}}(x+t) - \alpha^l\big|_{\mathrm{T}}(t)\} = +\infty$$

so L can be written as:

$$L(x) = (\alpha^u\big|_{\mathrm{T}} \overline{\oslash}\, \alpha^l\big|_{\mathrm{T}})(x) = \inf_{t\in[0,T]} \{\alpha^u\big|_{\mathrm{T}}(x+t) - \alpha^l\big|_{\mathrm{T}}(t)\} = L_r(x)$$

Finally, $L_r = L$ and $U_r = U$, and by definition of $\mathbb{C}$, the theorem holds. □

With this theorem, the supremum and infimum used in the expression of the causality closure $\mathbb{C}(\alpha^u\big|_{\mathrm{T}}, \alpha^l\big|_{\mathrm{T}})$ are used over finite sets. $\mathbb{C}$ can now be computed with a simple, quadratic algorithm.

5.1.4 Algorithm

The full algorithm for computing the causal and SA-SA pair of curves equivalent to the finite pair of arrival curves A_0 defined on $[0, T]$ is given in Figure 8.

The loop terminates but finding a bound on the number of iterations other than the brute-force (just knowing that the sequence is decreasing and that there is a finite number of possible curves tighter that the original one) is still an open question. In practice, however, the number of iterations required is low (one or two in most of the examples we tried, and up to 6 in tricky corner-cases).

After the loop, A is either $\bot_{AC}$ or a causal pair of finite discrete curves; it is equivalent to A_0, the original pair of curves; and it is SA-SA on the interval $[0, T]$ if the SA-SA closure was applied (first line within the loop). In this case, it is the best pair of curves equivalent to the original A_0.

$A \leftarrow A_0$
repeat
  $A \leftarrow$ SA-SA-closure(A) // Not mandatory, but speeds up convergence,
    // and ensures SA-SA property of the result
  $A' \leftarrow A$
  $A \leftarrow \mathbb{C}(A)$
until $A \neq \bot_{AC}$ or $A' = A$

Figure 8: Computation of causality closure for finite, discrete curves

5.2 Piecewise Affine, Convex/Concave Curves

An interesting class of curves, used for example in [10, 9], is the class of piecewise affine, convex/concave curves (i.e. α^l is convex, and α^u is concave). An interesting property is that α^u (resp α^l) can be expressed as the minimum (resp. maximum) of a set of affine functions. When reasoning about these curves, the minimum and maximum are naturally translated in conjunction of conditions. These curves are always causal:

Theorem 25. *Let $(\alpha^u, \alpha^l) \neq \bot_{AC}$ be a pair of piecewise affine, convex/concave curves. Then (α^u, α^l) is causal.*

Proof. Let $a^u\Delta + b^u$ (resp. $a^l\Delta + b^l$) be the last affine piece of α^u (resp. α^l).

A direct consequence of the convex/concave property is that $\forall 0 \leq \Delta_1 \leq \Delta_2$, $\alpha^u(\Delta_2) - \alpha^u(\Delta_1) \geq a^u(\Delta_2 - \Delta_1)$ and $\alpha^l(\Delta_2) - \alpha^l(\Delta_1) \leq a^l(\Delta_2 - \Delta_1)$, since the slope of α^u (resp. α^l) keeps increasing (resp. decreasing) until it reaches a^u (resp. a^l). In particular, $\forall \Delta \geq 0, \alpha^u(\Delta) \geq a^u\Delta$ and $\alpha^l(\Delta) \leq a^l\Delta$.

Then, if we set $(\alpha^{u*}, \alpha^{l*}) = \mathbb{C}(\alpha^u, \alpha^l)$,

$$\forall \Delta \geq 0, \forall t \geq 0, \quad \alpha^u(\Delta + t) - \alpha^l(t) \geq \alpha^u(\Delta) + a^u t - a^l t$$
$$\alpha^{u*}(\Delta) = \inf_{t \geq 0}\{\alpha^u(\Delta) + a^u t - a^l t\} \geq \inf_{t \geq 0}\{\alpha^u(\Delta) + t(\underbrace{a^u - a^l}_{\geq 0})\}$$
$$\alpha^{u*}(\Delta) \geq \alpha^u(\Delta)$$
$$\alpha^{u*}(\Delta) = \alpha^u(\Delta) \qquad \text{(since } \alpha^{u*}(\Delta) \leq \alpha^u(\Delta) \text{ too)}$$

□

5.3 Combination of Finite Prefix and Piecewise Affine

We now study the set of curves $\mathcal{U}pac$ comprising both a finite prefix given by a set of points and a long-term rate given by a piecewise-affine, convex/concave pair of curves. This class of curves is the one used in the tool `ac2lus` [2], and is a super-set of the class of curves considered in [9]. It allows a precise description of the initial portion of the curves, as well as a set of constraints on the long-term rate of the event stream; it may be easily machine-representable: the finite portion is basically an array and each affine piece is encoding with its slope and its Y-intercept.

We first define formally this class of curves, then present a few intermediate definitions and lemmas needed to compute the causality closure, presented afterwards.

5.4 The Class of Ultimately Piecewise Affine Curves, $\mathcal{U}pac$

In this section, we are considering only discrete-time, but can consider the fluid event model. Our implementation is restricted to the discrete-event model.

Definition 17 ($\mathcal{U}pac$)**.** *We define the class of curves $\mathcal{U}pac$ as the set of pairs of curves (α^u, α^l) such that there exists*

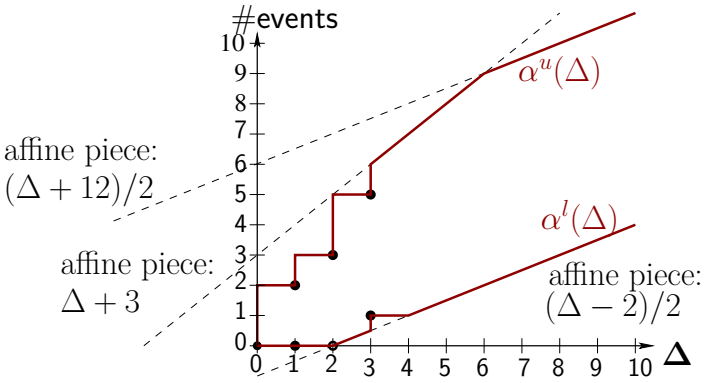


Figure 9: Example curve with explicit points and affine pieces

- $P(\alpha^u), P(\alpha^l) \in \mathcal{N}$*: size of the finite prefix (i.e. abscissa of the last point explicitly given in the representation)*
- $N(\alpha^u), N(\alpha^l) \in \mathcal{N}$*: number of pieces of the piecewise affine part of the curves.*
- *a set of values* $p_i^u \in \mathcal{N}$*,* $i \in [0, P(\alpha^u)]$*, and a set of rational values* a_j^u, b_j^u*,* $j \in [1, N(\alpha^u)]$*: representation of the curve* α^u
- *a set of values* $p_i^l \in \mathcal{N}$*,* $i \in [0, P(\alpha^l)]$*, and a set of rational values* a_j^l, b_j^l*,* $j \in [1, N(\alpha^l)]$*: representation of the curve* α^l

such that, $\forall \Delta \geq 0$*:*

$$F^u(\Delta) = \text{if } \Delta \in [0, P(\alpha^u)] \text{ then } p^u_\Delta \text{ else } +\infty;$$
$$F^l(\Delta) = \text{if } \Delta \in [0, P(\alpha^l)] \text{ then } p^l_\Delta \text{ else } 0;$$
$$I^u(\Delta) = \text{if } N(\alpha^u) > 0 \text{ then } \min_{j \in [1, N(\alpha^u)]} \left\{a^u_j \Delta + b^u_j\right\} \text{ else } +\infty;$$
$$I^l(\Delta) = \text{if } N(\alpha^l) > 0 \text{ then } \min_{j \in [1, N(\alpha^l)]} \left\{a^l_j \Delta + b^l_j\right\} \text{ else } 0;$$

with $\alpha^u(\Delta) = \min\left\{F^u(\Delta), I^u(\Delta)\right\}$ *and* $\alpha^l(\Delta) = \max\left\{F^l(\Delta), I^l(\Delta)\right\}$.

The tuple $\big(P(\alpha^u), P(\alpha^l), N(\alpha^u), N(\alpha^l), \{p^u_i\}_{i\in[0,P(\alpha^u)]}, \{a^u_j, b^u_j\}_{j\in[1,N(\alpha^u)]}, \{p^l_i\}_{i\in[0,P(\alpha^l)]}, \{a^l_j, b^l_j\}_{i\in[1,P(\alpha^l)]}\big)$ *is called the* representation *of the pair* (α^u, α^l)*. It corresponds to the data-structure to be used in algorithms. We call the set of points* p^u_i *and* p^l_i *the* finite prefix *and each line* $a_j\Delta + b_j$ *the* affine pieces *of* (α^u, α^l).

For simplicity of the notations, we identify the abscissa of the points of the finite prefix with ther index, but this is not a limitation. Note also that we require the individual points to be integers (this will be necessary to ensure the convergence of the algorithms later), but remain in the fluid-event model. Figure 9 shows an example: the upper part is made of 3 points and two affine pieces; the lower part, 3 points, one affine piece.

5.4.1 Motivation for the Normal Form

As shown above, the causality closure of piecewise affine convex/concave curves is trivial. The difficulty here comes from the points of α^u and α^l, which can interact together, or with the affine pieces of the other curve. The particularity of curves comprising only points was that such curves were not SA-SA, and could not be made so. This difficulty can be eliminated thanks to the piecewise affine part of the curves: we can apply the SA-SA closure to the points of the curves, and only a finite number of points will remain under the affine pieces (if this is not the case, then it means the affine pieces add no information, and can be removed). This transformation will be called the normalization, and will be presented in algorithm 1.

After this, we will get a SA-SA curve (theorem 30) made of points and affine pieces, and will be able to apply the $\mathbb{C}$ operator on it to get a causal pair of curves. The computation of $\mathbb{C}$ will be made easy by theorem 31, which will reduce the computation of $\mathbb{C}$ to a version where all the operators will be bounded.

5.4.2 Properties of Sub-additive Closure of Finite Curves

Definition 18 (Slope of finite arrival curves)**.** *Let (α^u, α^l) be a pair of arrival curves, and $P > 0$. We define the following:*

$$S^P(\alpha^u) \stackrel{def}{=} \min_{\Delta \leq P} \{\alpha^u(\Delta)/\Delta\} \qquad \text{(slope of } \alpha^u\big|_P\text{)}$$

$$S^P(\alpha^l) \stackrel{def}{=} \max_{\Delta \leq P} \{\alpha^l(\Delta)/\Delta\} \qquad \text{(slope of } \alpha^l\big|_P\text{)}$$

$$\Delta^P(\alpha^u) \stackrel{def}{=} \min_{\Delta \leq P} \{S^P(\alpha^u) \times \Delta = \alpha^u(\Delta)\} \qquad \text{(point of maximal influence of } \alpha^u\big|_P\text{)}$$

$$\Delta^P(\alpha^l) \stackrel{def}{=} \min_{\Delta \leq P} \{S^P(\alpha^l) \times \Delta = \alpha^l(\Delta)\} \qquad \text{(point of maximal influence of } \alpha^l\big|_P\text{)}$$

$$d_m(\alpha^u) \stackrel{def}{=} \sup_{\Delta \leq \Delta^P(\alpha^u)} \{\overline{\alpha^u}(\Delta) - S^P(\alpha^u) \times \Delta\} \qquad \text{(maximal drift of } \alpha^u\big|_P\text{)}$$

$$d_m(\alpha^l) \stackrel{def}{=} \sup_{\Delta \leq \Delta^P(\alpha^l)} \{S^P(\alpha^l) \times \Delta - \underline{\alpha^l}(\Delta)\} \qquad \text{(maximal drift of } \alpha^l\big|_P\text{)}$$

Since we work here in discrete time, the min and max are over finite sets, and are well-defined.

The point of maximal influence defines the linear function $S^P(\alpha^u) \times \Delta$. The curve $\overline{\alpha^u}$ remains above this line, and touches it infinitely often. Also, $\overline{\alpha^u}$'s distance to the line remains bounded. Formally, this is expressed by the three following lemmas, illustrated by Figure 10 on α^u.

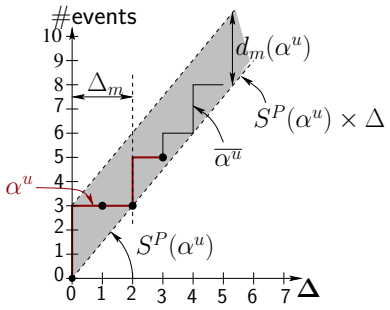


Figure 10: Point of maximal influence of α^u. The curve (α^u, α^l) remains in the greyed area, and touches $S^P(\alpha^u) \times \Delta$ at least with period $\Delta^P(\alpha^u)$.

Lemma 26. *Let (α^u, α^l) be a pair of arrival curves and $T > 0$. Then:*

$$\forall \Delta, \quad \alpha^u(\Delta) \geq \overline{\alpha^u\big|_T}(\Delta) \geq S^P(\alpha^u) \times \Delta$$
$$\alpha^l(\Delta) \leq \underline{\alpha^l\big|_T}(\Delta) \leq S^P(\alpha^l) \times \Delta$$

Lemma 27. *Let (α^u, α^l) be a pair of arrival curves and $T > 0$. Then:*

$$\forall k \in \mathcal{N}, \quad \overline{\alpha^u\big|_T}(k \times \Delta^P(\alpha^u)) = k \times \Delta^P(\alpha^u) \times S^P(\alpha^u)$$
$$\underline{\alpha^l\big|_T}(k \times \Delta^P(\alpha^l)) = k \times \Delta^P(\alpha^l) \times S^P(\alpha^l)$$

Lemma 28. *Let (α^u, α^l) be a pair of arrival curves. Then:*

$$\forall \Delta \geq 0, \quad \overline{\alpha^u}(\Delta) - S^P(\alpha^u) \times \Delta \leq d_m(\alpha^u)$$
$$S^P(\alpha^l) \times \Delta - \underline{\alpha^l}(\Delta) \leq d_m(\alpha^l)$$

A consequence of this is that affine pieces $a\Delta + b$ with a slope steeper than $S^P(\alpha^u) \times \Delta$ do not add information to the curve (provided the explicit points of α^u (resp. α^l) are below (resp. above) the affine piece), and can be removed. This is formalized by the following lemma:

Lemma 29. *Let (α^u, α^l) be a pair of arrival curves in $\mathcal{U}pac$, different from $\perp_{AC}$, and $J \in [1, N(\alpha^u)]$ such that these two conditions are satisfied:*

$$\forall i \in [0, P(\alpha^u)], \forall j \in [1, N(\alpha^u)], \quad p_i^u \leq a_j^u \times i + b_j^u$$
$$a_J^u \geq S^P(\alpha^u)$$

Then, removing the affine piece $a_J^u + b_J^u$ from (α^u, α^l) yields an equivalent curve.

Similarly for α^l, if

$$\forall i \in [0, P(\alpha^l)], \forall j \in [1, N(\alpha^l)], \quad p_i^l \leq a_j^l \times i + b_j^l$$
$$a_J^l \geq S^P(\alpha^l)$$

Then, removing the affine piece $a_J^l + b_J^l$ from (α^u, α^l) yields an equivalent curve.

For lemma 26. We prove by induction that $\forall n \geq 1, \otimes^n \left(\alpha^u|_{\mathrm{T}}\right) \geq S^P(\alpha^u) \times \Delta$. The base case is obvious by definition of $S^P(\alpha^u)$. Assuming $\otimes^n \left(\alpha^u|_{\mathrm{T}}\right) \geq S^P(\alpha^u) \times \Delta$, we have:

$$\begin{aligned}
\otimes^{n+1}\left(\alpha^u|_{\mathrm{T}}\right)(\Delta) &= \left(\left(\otimes^n \left(\alpha^u|_{\mathrm{T}}\right)\right) \otimes \left(\alpha^u|_{\mathrm{T}}\right)\right)(\Delta) \\
&= \inf_{t \in [0,\Delta]} \Bigg\{ \underbrace{\underbrace{\left(\otimes^n \left(\alpha^u|_{\mathrm{T}}\right)\right)(\Delta - t)}_{\geq S^P(\alpha^u) \times (\Delta - t)} + \underbrace{\left(\alpha^u|_{\mathrm{T}}\right)(t)}_{\geq S^P(\alpha^u) \times t}}_{\geq S^P(\alpha^u) \times \Delta} \Bigg\} \\
&\geq S^P(\alpha^u) \times \Delta
\end{aligned}$$

which concludes the induction proof. By definition of $\overline{\alpha^u}$, this proves the first equation of the lemma. The proof for the α^l equation is the same. □

For lemma 27. This lemma is also proved by a simple induction on k. The base cases for $k = 0$ and $k = 1$ follow from the definition. Assuming $\overline{\alpha^u|_{\mathrm{T}}}(k \times \Delta^P(\alpha^u)) = k \times \Delta^P(\alpha^u) \times S^P(\alpha^u)$, we have:

$$\begin{aligned}
&\overline{\alpha^u|_{\mathrm{T}}}((k+1) \times \Delta^P(\alpha^u)) \\
&\leq \overline{\alpha^u|_{\mathrm{T}}}(1 \times \Delta^P(\alpha^u)) + \overline{\alpha^u|_{\mathrm{T}}}(k \times \Delta^P(\alpha^u)) && \text{(sub-additivity of } \overline{\alpha^u|_{\mathrm{T}}}) \\
&\leq \overline{\alpha^u|_{\mathrm{T}}}(\Delta^P(\alpha^u)) + k \times \overline{\alpha^u|_{\mathrm{T}}}(\Delta^P(\alpha^u)) && \text{(induction hypothesis)} \\
&\leq (k+1) \times \overline{\alpha^u|_{\mathrm{T}}}(\Delta^P(\alpha^u)) \\
&= (k+1) \times \overline{\alpha^u|_{\mathrm{T}}}(\Delta^P(\alpha^u)) && \text{(lemma 26 gives} \\
& && \overline{\alpha^u|_{\mathrm{T}}}((k+1) \times \Delta^P(\alpha^u)) \geq (k+1) \times \overline{\alpha^u|_{\mathrm{T}}}(\Delta^P(\alpha^u)))
\end{aligned}$$

The proof for the second equation is the same. □

For lemma 28. The definition of d_m states the inequality for $\Delta \in [0, \Delta_m(\alpha^u)]$. We need to prove that the inequality also holds for $\Delta \geq \Delta_m(\alpha^u)$. We consider such Δ, and define X, difference between Δ and the abscissa of the last point of contact between α^u and $S^P(\alpha^u) \times \Delta$ before Δ, by:

$$X = \Delta - \left\lfloor \frac{\Delta}{\Delta^P(\alpha^u)} \right\rfloor \times \Delta^P(\alpha^u)$$

By construction, $\Delta - X$ is a multiple of $\Delta^P(\alpha^u)$, hence $\overline{\alpha^u|_{\mathrm{T}}}(\Delta - X) = \Delta^P(\alpha^u) \times (\Delta - X)$ (by lemma 27).

Also, $0 \leq X \leq \Delta^P(\alpha^u) \leq P(\alpha^u)$, hence, by definition of $d_m(\alpha^u)$, we have $d_m(\alpha^u) \geq \overline{\alpha^u}(X) - S^P(\alpha^u) \times X$ (i.e. $\overline{\alpha^u}(X) \leq d_m(\alpha^u) + S^P(\alpha^u) \times X$). Then, we can write:

$$\begin{aligned}
\overline{\alpha^u}(\Delta) &= \overline{\alpha^u}(\Delta - X + X) \\
&\leq \overline{\alpha^u}(\Delta - X) + \overline{\alpha^u}(X) && \text{(sub-additivity of } \overline{\alpha^u}) \\
&\leq S^P(\alpha^u) \times (\Delta - X) + (d_m(\alpha^u) + S^P(\alpha^u) \times X) \\
&\leq S^P(\alpha^u) \times \Delta + d_m(\alpha^u) \\
\overline{\alpha^u}(\Delta) - S^P(\alpha^u) \times \Delta &\leq d_m(\alpha^u)
\end{aligned}$$

□

for lemma 29. We denote by α'^u the curve obtained by removing the J-th affine piece to α^u.

The first hypothesis implies that we can compute $S^P(\alpha^u)$, $d_m(\alpha^u)$ and $\Delta^P(\alpha^u)$ based only on the explicit points p_i^u, hence, $S^P(\alpha^u) = S^P(\alpha'^u)$, $d_m(\alpha^u) = d_m(\alpha'^u)$ and $\Delta^P(\alpha^u) = \Delta^P(\alpha'^u)$.

The second hypothesis implies that $(a_J^u \Delta + b^u) - (S^P(\alpha^u) \times \Delta)$ is a non-decreasing function, hence $\forall \Delta \geq \Delta_m(\alpha^u)$,

$$\begin{aligned}
(a_J^u \Delta + b^u) - (S^P(\alpha^u) \times \Delta) &\geq \sup_{t \leq \Delta^P(\alpha^u)} \{(a_J^u t + b^u) - S^P(\alpha^u) \times t\} \\
&\geq \sup_{t \leq \Delta^P(\alpha^u)} \{\overline{\alpha^u}(t) - S^P(\alpha^u) \times t\} && \text{(first hypothesis)} \\
&\geq d_m(\alpha^u) = d_m(\alpha'^u) && \text{(Definition of } d_m(\alpha^u)) \\
&\geq \overline{\alpha'^u}(\Delta) - S^P(\alpha'^u) \times \Delta && \text{(lemma 28)} \\
(a_J^u \Delta + b^u) &\geq \overline{\alpha'^u}(\Delta)
\end{aligned}$$

In other words, the affine piece $a_J^u \Delta + b^u$ remain above $\overline{\alpha'^u}$, hence the conclusion. □

5.4.3 Normal Form of Curves in $\mathcal{U}pac$

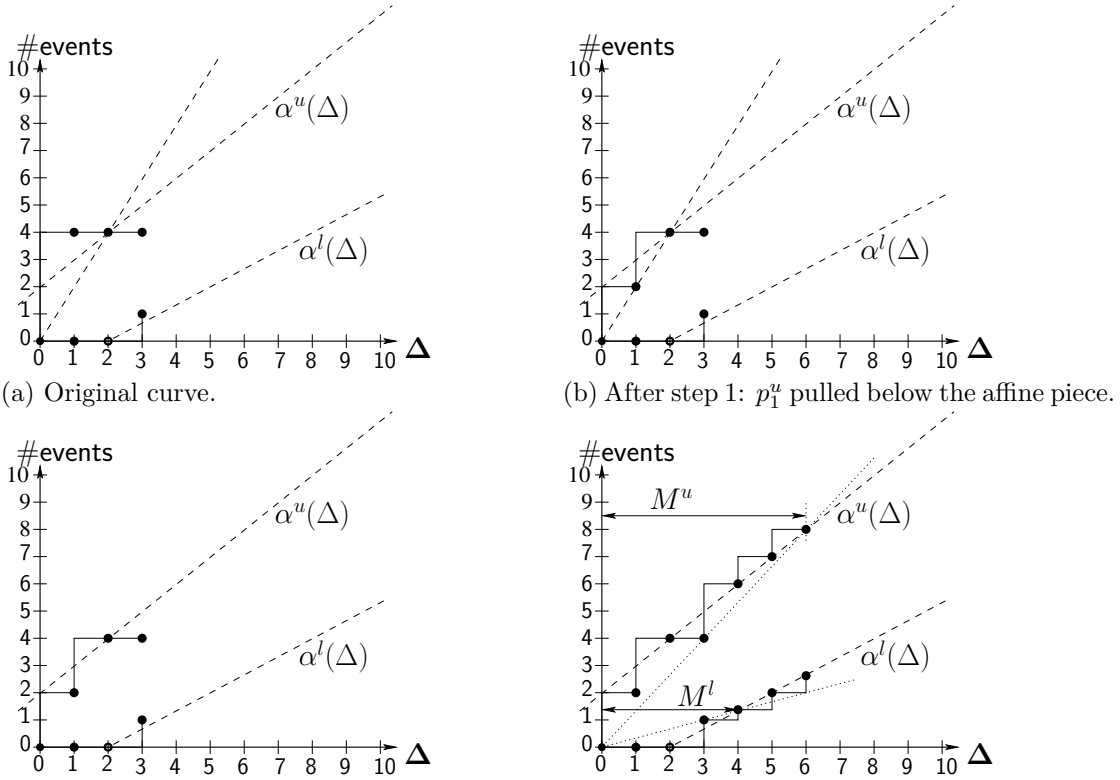
Arbitrary curves made of points and affine pieces are hard to deal with (in particular they are not necessarily SA-SA). To simplify the proofs, we consider only curves obeying a few well-formedness properties, which we call the normal form. Converting an arbitrary curve into a normal-form is straightforward (the algorithm is given below), hence we don't loose generality.

Definition 19 (Normal form of curves in $\mathcal{U}pac$)**.** *A pair of arrival curves (α^u, α^l) in $\mathcal{U}pac$ is said to be in normal form if $P(\alpha^u) = P(\alpha^l) = P$ and at least one of the following conditions is satisfied:*

1. $(\alpha^u, \alpha^l) = \perp_{AC}$
2. $N(\alpha^u) = N(\alpha^l) = 0$ *and* (α^u, α^l) *is SA-SA up to* P
3. $N(\alpha^u) = 0$, α^u *is sub-additive up to* P *and* α^l *is super-additive.*
4. $N(\alpha^l) = 0$, α^l *is super-additive up to* P *and* α^u *is sub-additive.*
5. (α^u, α^l) *is SA-SA*

Case 2 corresponds to the case of discrete, finite curves. In this case, we say that (α^u, α^l) *has no relevant affine pieces. Cases 3 and 4 correspond to asymetric cases where only one of* α^u *and* α^l *has relevant affine pieces. In these cases, we consider the SA-SA curves in theory, but the representation is restricted to the SA-SA set of points* on the prefix.

For the common case where both curves have relevant affine pieces *(case 5)*, the transformation of a pair of curves into normal form is illustrated by Figure 11. It essentially consists in adding explicit points to the curve until one can be sure all the points are above the affine pieces. In the



(a) Original curve.
(b) After step 1: p_1^u pulled below the affine piece.
(c) After step 2: one affine piece removed.
(d) After steps 3-6: Curve in normal form.

Figure 11: Step by step transformation into normal form

general case, the transformation is as follows:

Algorithm 1 (Normalization of curves in $\mathcal{U}pac$)**.** *For any curve in* $\mathcal{U}pac$*, we apply the steps:*

1. *Make sure all the explicit points* p_i^u *(resp.* p_i^l*) are under (resp. above) all affine pieces; if not, modify* p_i^u *(resp.* p_i^l*); add points on* α^u *or* α^l *until* $P(\alpha^u) = P(\alpha^l) = P$*. See Figure 11.(b).*

2. *Eliminate affine pieces of* α^u *(resp.* α^l*) which have a slope greater or equal (resp. lower or equal) to* $S^P(\alpha^u)$ *(resp.* $S^P(\alpha^l)$*). By lemma 29, this does not change the curve. See Figure 11.(c).*

Then, multiple cases can occur:

If $N(\alpha^u) = N(\alpha^l) = 0$ **then**

3. *Apply the SA-SA closure up to* P*.*

If $N(\alpha^u) \neq 0$ **and** $N(\alpha^l) \neq 0$ **then**

3. *Compute the abscissa M_j^u of the intersection between $S^P(\alpha^u) \times \Delta$ and the affine piece j of α^u (and similarly M^l for α^l). Set $M^u = \min_j\{M_j^u\}$, $M^l = \min_j\{M_j^l\}$, $M = \max\{M^u, M^l\}$.*
4. *Add explicit points p^u and p^l to the curves, so that $P(\alpha^u) = P(\alpha^l) = M$.*
5. *Apply the SA-SA closure up to M to (α^u, α^l). See Figure 11.(d).*

If $N(\alpha^u) \neq 0$ **and** $N(\alpha^l) = 0$ **then**

3. *Compute the abscissa M_j^u of the intersection between $S^P(\alpha^u) \times \Delta$ and the affine piece j of α^u. Set $M = \min_j\{M_j^u\}$.*
4. *Add explicit points p^u and p^l to the curves, so that $P(\alpha^u) = P(\alpha^l) = M$.*
5. *Apply the SA-SA closure up to M to (α^u, α^l).*

If $N(\alpha^u) = 0$ **and** $N(\alpha^l) \neq 0$ **then** *apply the same transformation as above, replacing α^l by α^u and vice-versa in the text.*

The normalization trivially implies SA-SA closure up to M. The SA-SA property is actually true for the whole curve, when it has some relevant affine pieces:

Theorem 30. *Let (α^u, α^l) be a pair of curves obtained by applying the normalization (algorithm 1) on a pair of curves in $\mathcal{U}pac$. Then (α^u, α^l) is in $\mathcal{U}pac$ and in normal form. In particular, if α^l (resp. α^u) has at least one relevant affine piece, then α^l is super-additive (resp. sub-additive).*

Proof. We prove the first case (α^u is sub-additive), the second being similar, that is:

$$\forall \Delta_1, \Delta_2 \geq 0, \quad \alpha^u(\Delta_1) + \alpha^u(\Delta_2) \geq \alpha^u(\Delta_1 + \Delta_2)$$

If α^u has no relevant affine piece, then by definition of the normal form, α^u is sub-additive (although its representation, $\alpha^u|_M$, is not).

In the case where α^u has at least one affine piece, we consider several cases, depending on the values of Δ_1 and Δ_2:

$\Delta_1 \leq M$ **and** $\Delta_2 \leq M$**:**

$$\begin{aligned}
\alpha^u(\Delta_1) + \alpha^u(\Delta_2) &= \overline{\alpha^u|_M}(\Delta_1) + \overline{\alpha^u|_M}(\Delta_2) && \text{(Since } \Delta_1 \leq M, \Delta_2 \leq M \\
&&& \text{and } \alpha^u \text{ is sub-additive up to } M) \\
&\geq \overline{\alpha^u|_M}(\Delta_1 + \Delta_2) && \text{(Sub-additivity of } \overline{\alpha^u|_M}) \\
&\geq \alpha^u(\Delta_1 + \Delta_2) && \text{(Because } (\alpha^u, \alpha^l) \text{ is in normal form)}
\end{aligned}$$

$\Delta_1 > M$ **or** $\Delta_2 > M$**:** Without loss of generality, we assume $\Delta_1 > M$, i.e. Δ_1 is in the piecewise affine part of the curve. In other words, $\alpha^u(\Delta_1) = a_i\Delta_1 + b_i$ where $a_i\Delta + b_i$ is one of the affine piece of α^u.

$$\begin{aligned}
\alpha^u(\Delta_1 + \Delta_2) &\leq a_i(\Delta_1 + \Delta_2) + b_i && \text{(Since } \Delta_1 + \Delta_2 \geq \Delta_1) \\
&\leq a_i\Delta_1 + b_i + a_i\Delta_2 \\
&\leq \alpha^u(\Delta_1) + a_i\Delta_2 \\
&\leq \alpha^u(\Delta_1) + \alpha^u(\Delta_2) && \text{(See demonstration of theorem 25)}
\end{aligned}$$

□

5.4.4 $\mathbb{C}$ for $\mathcal{U}pac$ Curves With at Least one Affine Piece

We now focus on the general case, e.i. curves in normal form in $\mathcal{U}pac$, *with either* α^l *or* α^u *having affine pieces, or both*: $N(\alpha^u) > 0$ or $N(\alpha^l) > 0$. We show that we can directly apply the operator $\mathbb{C}$ on the curves and that its computation can be done in low polynomial time.

Theorem 31. *Let* (α^u, α^l) *be a pair of curves in* $\mathcal{U}pac$*, in normal form, such that* $(\alpha^u, \alpha^l) \neq \perp_{AC}$*, with either* α^u *or* α^l *having relevant affine pieces. Let* $M = P(\alpha^l) = P(\alpha^u)$ *be the index of the last point of* (α^u, α^l) *given explicitly (as it was computed in algorithm 1). Let* $\mathbb{C}|_M = \left(\mathbb{C}|_M^u, \mathbb{C}|_M^l\right)$ *be the following operator:* $\forall \Delta \geq 0$,
$\mathbb{C}|_M^u(\alpha^u, \alpha^l)(\Delta) = \inf_{t\in[0,M]}\{\alpha^u(\Delta + t) - \alpha^l(t)\}$ *and*
$\mathbb{C}|_M^l(\alpha^u, \alpha^l)(\Delta) = \sup_{t\in[0,M]}\{\alpha^l(\Delta + t) - \alpha^u(t)\}$

1. $\forall \Delta \geq 0, \mathbb{C}\left(\overline{\alpha^u}, \underline{\alpha^l}\right)(\Delta) = \mathbb{C}|_M\left(\overline{\alpha^u}, \underline{\alpha^l}\right)(\Delta)$
2. *If* $N(\alpha^u) \neq 0$ *then* $\forall \Delta > M$, $\mathbb{C}^u\left(\overline{\alpha^u}, \underline{\alpha^l}\right)(\Delta) = \alpha^u(\Delta)$
3. *If* $N(\alpha^l) \neq 0$ *then* $\forall \Delta > M$, $\mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right)(\Delta) = \alpha^l(\Delta)$

As a consequence, the $\mathbb{C}$ operator can easily be computed algorithmically: for each point to compute, the inf{} and the sup{} can be computed with a simple `for` loop iterating from 0 to M. The expression of $\mathbb{C}|_M\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$ includes a SA-SA closure. When the curve has affine pieces, it is already SA-SA, hence no SA-SA closure needs to be applied However, for curve with no affine pieces, since we only use the values of the SA-SA curves for $\Delta \leq 2M$, it is sufficient to compute the SA-SA closure up to $2M$. Furthermore, when the curve has at least one affine piece, this computation has to be done for the points of abscissa from 0 to M, the other points are given by the original curve itself.

For theorem 31, point 1. We prove only the equation for $\alpha^{u*} \stackrel{\text{def}}{=} \mathbb{C}|_M^u\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$, the other proof would be similar.

If we denote by M the last relevant point of the curve, we have:

$$\mathbb{C}\left(\overline{\alpha^u}, \underline{\alpha^l}\right) = \inf_{t\geq 0}\{\overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t)\} \tag{11}$$

$$= \min\left\{\inf_{t\in[0,M]}\{\overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t)\}, \inf_{t\in]M,+\infty[}\{\overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t)\}\right\} \tag{12}$$

The theorem basically states that the second part of the min{} in equation 12 can be omitted.

We distinguish two cases, depending on whether α^u has relevant affine pieces (i.e. whether $N(\alpha^u) = 0$ or not):

We perform the proof by contradiction. Let's assume

$$\inf_{t\in[0,M]}\{\overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t)\} > \inf_{t\in]M,+\infty[}\{\overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t)\}$$

This implies that there is a value of T in $]M, +\infty[$ for which:

$$\overline{\alpha^u}(\Delta + T) - \underline{\alpha^l}(T) < \inf_{t\in[0,M]}\{\overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t)\}$$

$$\forall t \in [0, M], \quad \overline{\alpha^u}(\Delta + T) - \underline{\alpha^l}(T) < \overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t)$$

- If α^u has no relevant affine pieces ($N(\alpha^u) = 0$): In this case, since (α^u, α^l) has at least one affine piece (hypothesis of theorem), then $N(\alpha^l) \neq 0$ and $\alpha^l = \underline{\alpha^l}$ (by definition of the normal form). Hence,

$$\forall t \in [0, M], \quad \overline{\alpha^u}(\Delta + T) - \alpha^l(T) < \overline{\alpha^u}(\Delta + t) - \alpha^l(t)$$

We define X, difference between Δ and the abscissa of the first point of contact between $\overline{\alpha^u}$ and $S^P(\alpha^u) \times \Delta$ following Δ, by:

$$X = \left\lceil \frac{\Delta}{\Delta^P(\alpha^u)} \right\rceil \times \Delta^P(\alpha^u) - \Delta$$

By construction, $X + \Delta$ is a multiple of $\Delta^P(\alpha^u)$, hence $\overline{\alpha^u}(X + \Delta) = \Delta^P(\alpha^u) \times (X + \Delta)$ (by lemma 27). Also, $0 \leq X \leq \Delta^P(\alpha^u) \leq M \leq T$.

We set $t = X$ in the above equation and get:

$$\begin{aligned}
\overline{\alpha^u}(\Delta + T) - \alpha^l(T) &< \overline{\alpha^u}(\Delta + X) - \alpha^l(X) \\
\overline{\alpha^u}(\Delta + T) - \alpha^l(T) &< S^P(\alpha^u) \times (\Delta + X) - \alpha^l(X)
\end{aligned}$$

By definition of α^l, and since $T > M$, $\alpha^l(T)$ is in the piecewise affine part of α^l, which means there is a n such that $\alpha^l(T) = (a^l_n T + b^l_n)$, i.e. $\alpha^l(T)$ is in the n-th affine piece:

$$\begin{aligned}
\overline{\alpha^u}(\Delta + T) - (a^l_n T + b^l_n) &< S^P(\alpha^u) \times (\Delta + X) - \alpha^l(X) \\
\alpha^l(X) - (a^l_n T + b^l_n) &< S^P(\alpha^u) \times (\Delta + X) - \overline{\alpha^u}(\Delta + T) \\
(a^l_n X + b^l_n) - (a^l_n T + b^l_n) &< S^P(\alpha^u) \times (\Delta + X) - \overline{\alpha^u}(\Delta + T) && \text{(by definition, } a^l_n X + b^l_n \leq \alpha^l(X)\text{)} \\
a^l_n(X - T) &< S^P(\alpha^u) \times (\Delta + X) - \overline{\alpha^u}(\Delta + T) \\
a^l_n(X - T) &< S^P(\alpha^u) \times (\Delta + X) - S^P(\alpha^u) \times (\Delta + T) && \text{(lemma 26)} \\
a^l_n(X - T) &< S^P(\alpha^u) \times (X - T) \\
a^l_n &> S^P(\alpha^u) && \text{(Since } X - T < 0\text{)}
\end{aligned}$$

In other words, the slope of one of the affine pieces of α^l is steeper than the one of α^u. This is a contradiction since it implies that $S^P(\alpha^u) \times \Delta$ will ultimately be strictly below α^l, and since lemma 27 implies that α^u will also become strictly smaller than α^l, i.e. $(\alpha^u, \alpha^l) = \bot_{AC}$.

- If α^u has relevant affine pieces ($N(\alpha^u) \neq 0$): in this case, $\alpha^u = \overline{\alpha^u}$ and

$$\begin{aligned}
\forall t \in [0, M], \quad \alpha^u(\Delta + T) - \underline{\alpha^l}(T) &< \alpha^u(\Delta + t) - \underline{\alpha^l}(t) \\
\alpha^u(\Delta + T) - \underline{\alpha^l}(T) &< \alpha^u(\Delta) && \text{(Setting } t = 0\text{)} \\
a^u_n(\Delta + T) + b^u_n - \underline{\alpha^l}(T) &< \alpha^u(\Delta) && \text{(}\Delta + T \text{ is in the } n\text{-th segment of } \alpha^u\text{)} \\
a^u_n(\Delta + T) + b^u_n - \underline{\alpha^l}(T) &< a^u_n \Delta + b^u_n && \text{(}\alpha^u(x) \geq a^u_n(x) + b^u_n \text{ by definition)} \\
a^u_n(T) &< \underline{\alpha^l}(T) && \text{(simple reordering)} \\
a^u_n(T) &< S^P(\alpha^l) \times T && \text{(By definition of } S^P(\alpha^l)\text{)} \\
a^u_n &< S^P(\alpha^l)
\end{aligned}$$

Hence the slope of α^l is greater than the one of one of the segments of α^u, which implies that $(\alpha^u, \alpha^l) = \bot_{AC}$.

□

For theorem 31, case 2. The proof is similar to the second case in the above proof. Basically, if α^u has relevant affine piece, then the slope of α^l has to be lower than the slope of the affine piece

$a^u_n\Delta + b^u_n$ of α^u with lowest slope. In other words:

$$\begin{aligned}
\forall t \geq 0, \Delta \geq 0, \quad \underline{\alpha^l}(t) &\leq S^P(\alpha^l) \times t \\
&\leq a^u_n t \\
&\leq \alpha^u(\Delta + t) - \alpha^u(\Delta) \\
\overline{\alpha^u}(\Delta) &\leq \overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t) \qquad \text{(Since } \overline{\alpha^u} = \alpha^u\text{)} \\
\overline{\alpha^u}(\Delta) &\leq \inf_{t \geq 0}\{\overline{\alpha^u}(\Delta + t) - \underline{\alpha^l}(t)\} \\
\overline{\alpha^u}(\Delta) &\leq \mathbb{C}^u\left(\overline{\alpha^u}, \underline{\alpha^l}\right)
\end{aligned}$$

Since by construction, $\mathbb{C}^u\left(\overline{\alpha^u}, \underline{\alpha^l}\right) \leq \overline{\alpha^u}(\Delta)$, we get the result. □

The symmetrical proof applies for theorem 31, case 3.

Based on these remarks, the algorithm for the causality closure for $\mathcal{U}pac$ curves with at least one relevant affine piece follows:

Algorithm 2. *Given a pair of curves (α^u, α^l) in $\mathcal{U}pac$ in normal form represented by p^u_i, a^u_j, b^u_j, p^l_i, a^l_k, b^l_k ($i \in [0, M]$, $j \in [1, N(\alpha^u)]$, $k \in [1, N(\alpha^l)]$), we denote by p^{u*}_i, a^{u*}_j, b^{u*}_j, p^{l*}_i, a^{l*}_k, b^{l*}_k the representation of the causality closure $\mathbb{C}\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$. This representation is computed as follows:*

- *In all cases, the affine pieces do not change (this is ensured by cases 2 and 3 of theorem 31):*

$$a^{u*}_j = a^u_j, \quad b^{u*}_j = b^u_j, \quad a^{l*}_k = a^l_k, \quad b^{l*}_k = b^l_k$$

- *To compute the points p_i of the finite prefix, define $({\alpha^u}_{2M}, {\alpha^l}_{2M})$, a pair of curves: if $N(\alpha^u) \neq 0$ then $\alpha^u_{2M} = \alpha^u$ else the finite prefix of α^u_{2M} is the subadditive closure of α^u up to $2M$ and it has no affine pieces (likewise for α^l_{2M}). Then:*

$$p^u_i = \mathbb{C}|^u_M(\alpha^u_{2M}, \alpha^u_{2M})(i) \quad \text{and} \quad p^l_i = \mathbb{C}|^l_M(\alpha^u_{2M}, \alpha^u_{2M})(i)$$

The Figure 12 illustrates the whole causality closure algorithm on an example. The pair of curves is given in Figure 12.(a): α^u has no affine piece, and α^l has one. Figure 12.(b) shows an attempt to use the $\mathbb{C}$ operator on the curves without performing a normalization. Since the curves are not SA-SA, $\mathbb{C}$ is able to remove *some* forbidden regions but misses one (the point $\alpha^l(4) = 2$). On the other hand, the normalization algorithm (12.(c)) adds some points to the prefix of the curves, and applying $\mathbb{C}|_M$ on the result yields a causal pair of curves, without further iteration (12.(d)).

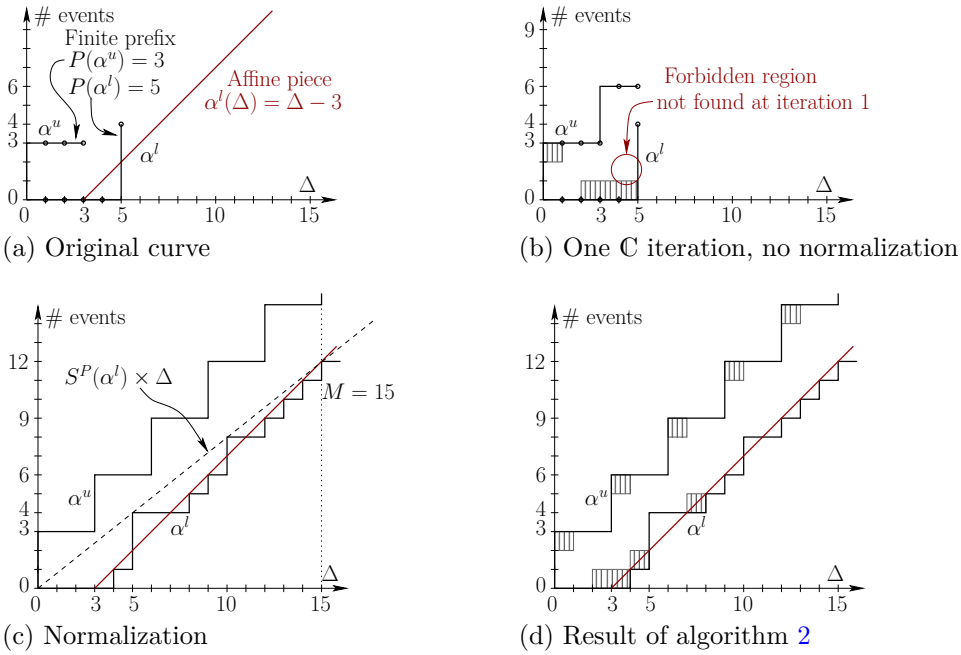
5.4.5 Optimized Causality Closure Algorithm in $\mathcal{U}pac$

The algorithm presented in section 5.4.4 is relatively simple, but its complexity is slightly more than what is really needed: it requires to compute the SA-SA closure of curves without affine pieces up to $2M$. We show in this section an alternate approach that requires only the computation up to M.

Curves with up and low affine pieces For curves in normal form in $\mathcal{U}pac$ with relevant affine pieces on α^u and α^l *(case 5 of the normal form)*, the theorems 18 and 31 can directly be applied. Indeed, the curves are already SA-SA, hence the application of $\mathbb{C}$ on the curves results in their causal representative and this application is easy to compute. Formally, let (α^u, α^l) be a pair of arrival curves in normal form in $\mathcal{U}pac$ with up and low affine pieces. The pair of curves $(\alpha^{u*}, \alpha^{l^*})$ computed by:

- $\forall \Delta \in [0, M]$, $\alpha^{u*}(\Delta) = \mathbb{C}|^u_M\left(\alpha^u, \alpha^l\right)$, $\alpha^{l^*}(\Delta) = \mathbb{C}|^l_M\left(\alpha^u, \alpha^l\right)$
- $\forall \Delta > M$, $\alpha^{u*}(\Delta) = \alpha^u(\Delta)$, $\alpha^{l^*}(\Delta) = \alpha^l(\Delta)$

is $\mathbb{C}\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$, namely, it is SA-SA, causal and the tightest pair of curves among the ones equivalent to (α^u, α^l). The algorithm requires to compute M points, each computation being linear.



(a) Original curve

(b) One $\mathbb{C}$ iteration, no normalization

(c) Normalization

(d) Result of algorithm 2

Figure 12: Causality Closure on a $\mathcal{U}pac$ Curve With One Affine Piece

Curves with up but no low affine pieces (and conversely) We now consider curves in normal form in $\mathcal{U}pac$ with one side having relevant affine pieces but not the other *(case 3 and 4 of the normal form)*. Let us fix for the explanation α^u to have no affine pieces: the problem here is that α^u is not SA-SA: the computation of $\mathbb{C}$ on the curves will not provide the result. The idea here is to compute separately the two curves. We begin with the computation of the lower curve $\mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$: theorem 31 provides an algorithm. We then compute the finite prefix of $\mathbb{C}^u\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$ using the operator on α^u and $\mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$.

Formally, let (α^u, α^l) be a pair of arrival curves in normal form in $\mathcal{U}pac$, with α^l having affine pieces, but not α^u. Let $M = P(\alpha^l) = P(\alpha^u)$ be the last abscissa of the finite prefix. The following algorithm computes the causality closure $\mathbb{C}\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$.

Algorithm 3. *1. Computation of α^{l^*} given by:*

$$\forall \Delta \in [0, M],\ \alpha^{l^*}(\Delta) = \mathbb{C}\big|_M^l(\alpha^u, \alpha^l) \text{ and } \forall \Delta > M,\ \alpha^{l^*}(\Delta) = \alpha^l(\Delta)$$

2. Computation of α^{u^*} given by:

$$\forall \Delta \in [0, M],\ \alpha^{u^*}(\Delta) = \mathbb{C}\big|_M^u\left(\alpha^u, \alpha^{l^*}\right)(\Delta) \text{ and } \forall \Delta > M,\ \alpha^{u^*}(\Delta) = +\infty$$

3. Computation of $\alpha^{u^{*\prime}}$ given by the sub-additive closure up to M of α^{u^*}:

$$\forall \Delta \in [0, M],\ \alpha^{u^{*\prime}}(\Delta) = \overline{\alpha^{u^*}}(\Delta) \text{ and } \forall \Delta > M,\ \alpha^{u^{*\prime}}(\Delta) = +\infty$$

Theorem 32. *Let (α^u, α^l) be a pair of arrival curves in normal form in $\mathcal{U}pac$, with α^l having affine pieces, but not α^u. Let α^{l^*}, α^{u^*} and $\alpha^{u^{*\prime}}$ be the curves computed by the algorithm 3:*

$$\alpha^{l^*} = \mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right) \quad \text{and} \quad \overline{\alpha^{u^{*\prime}}} = \overline{\alpha^{u^*}} = \mathbb{C}^u\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$$

The first step of the algorithm computes the low part of causal representative. The second step computes α^{u^*} such that $(\alpha^{l^*}, \alpha^{u^*})$ is causal, but α^{u^*} is not sub-additive up to M. The last step obtains the sub-additivity up to M for α^{u^*} while keeping the causality of the pair.

The theorem is proved in [15], it ensures that $(\alpha^{u^{*\prime}}, \alpha^{l^*})$ is the causal representative of (α^u, α^l) in $\mathcal{U}pac$: it is causal, super-additive for α^{l^*}, sub-additive upt to M for $\alpha^{u^{*\prime}}$, and the tightest pair of curves equivalent to (α^u, α^l).

Those following lemmas prove the above theorem.

Lemma 33. $\alpha^{l*} = \mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$

Proof. α^l is super-additive; this implies that $\alpha^l = \underline{\alpha^l}$, hence

$$\begin{aligned}\forall \Delta \in [0, M], \quad \mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right)(\Delta) &= \mathbb{C}^l\left(\overline{\alpha^u}, \alpha^l\right)(\Delta) \\ &= \mathbb{C}|_{\mathrm{M}}^{l}\left(\overline{\alpha^u}, \alpha^l\right)(\Delta) \qquad \text{(By theorem 31)}\end{aligned}$$

For the points between 0 and M, the computation of $\mathbb{C}^l\left(\overline{\alpha^u}, \alpha^l\right)$ only uses the value of $\overline{\alpha^u}$ between 0 and M: as α^u is sub-additive up to M, $\alpha^u(t) = \overline{\alpha^u}(t)$, $\forall t \in [0, M]$. Hence,

$$\forall \Delta \in [0, M], \quad \mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right)(\Delta) = \mathbb{C}|_{\mathrm{M}}^{l}\left(\alpha^u, \alpha^l\right)(\Delta) = \alpha^{l*}$$

Also, $\forall \Delta > M$, $\alpha^{l*}(\Delta) = \alpha^l(\Delta) = \mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$ (by theorem 31). □

Lemma 34. $(\alpha^{u*}, \alpha^{l*})$ *is a fix-point of* $\mathbb{C}$*, i.e.*

$$\alpha^{u*} = \mathbb{C}^u\left(\alpha^{u*}, \alpha^{l*}\right) \tag{13}$$

$$\alpha^{l*} = \mathbb{C}^l\left(\alpha^{u*}, \alpha^{l*}\right) \tag{14}$$

For equation 13. Notice that $\alpha^{u*}(\Delta) = \inf_{t\in[0,M], \Delta+t\leq M} \alpha^u(\Delta + t) - \alpha^{l*}(t)$, if $\Delta \leq M$ and $\alpha^{u*}(\Delta) = +\infty$ if $\Delta > M$.

$\mathbb{C}^u\left(\alpha^{u*}, \alpha^{l*}\right) = \alpha^{u*} \overline{\oslash} \alpha^{l*} \leq \alpha^{u*}$

By theorem 31, $\forall \Delta \geq 0$,

$$\begin{aligned}\mathbb{C}^u\left(\alpha^{u*}, \alpha^{l*}\right)(\Delta) &= \inf_{t\in[0,M]}\{\alpha^{u*}(\Delta + t) - \alpha^{l*}(t)\} \\ &= \inf_{t\in[0,M]} \inf_{x\in[0,M]}\{\alpha^u(\Delta + t + x) - (\alpha^{l*}(t) + \alpha^{l*}(x))\} \\ &= \inf_{t+x\in[0,M]}\{\alpha^u(\Delta + t + x) - (\alpha^{l*}(t) + \alpha^{l*}(x))\} \\ &\quad \text{(since for } t + x > M, \alpha^u(\Delta + t + x) = +\infty) \\ &\geq \inf_{x+t\in[0,M]}\{\alpha^u(\Delta + t + x) - \alpha^{l*}(t + x)\} \\ &\quad \text{(super-additivity of } \alpha^{l*}) \\ &\geq \alpha^{u*}(\Delta)\end{aligned}$$

□

For equation 14. By definition of $\mathbb{C}$, $\alpha^{l*} \leq \mathbb{C}^l\left(\alpha^{u*}, \alpha^{l*}\right)$, and by construction of $(\alpha^{u*}, \alpha^{l*})$, it is equivalent to (α^u, α^l).

$\mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right)$ is the tightest curve equivalent to (α^u, α^l), therefore:

$$\begin{aligned}\alpha^{l*} = \mathbb{C}^l\left(\overline{\alpha^u}, \underline{\alpha^l}\right) &\geq \mathbb{C}^l\left(\alpha^{u*}, \alpha^{l*}\right) \\ \alpha^{l*} &\leq \mathbb{C}^l\left(\alpha^{u*}, \alpha^{l*}\right) \leq \alpha^{l*} \\ \alpha^{l*} &= \mathbb{C}^l\left(\alpha^{u*}, \alpha^{l*}\right)\end{aligned}$$

□

Applying the implication (e) in the causality characterization theorems, this proves that $(\alpha^{u*}, \alpha^{l*})$ is causal.

6 Conclusion

We formally defined the notion of causality for RTC curves, and set up a formal framework to study it. As already mentioned, and although all along the paper we talk about arrival curves, the results are applicable to arrival curves *as well as* to service curves. We started from the intuitive notion of forbidden region, and the definition of causality based on the possibility to extend a curve, and stated the equivalence (valid for SA-SA pairs of curves) between absence of forbidden regions and the definition.

To the best we know, the phenomenon has received little attention and no work has been carried out on the subject yet except [3]. This is mainly due to the usual way arrival curves were used within the RTC framework on the one hand and to the restrictions of the studies to some already causal class of arrival curves in the other hand. We detailed in which conditions causality can appear and be problematic. Dealing with general causal pairs of curves in a simulator or a formal verification tool is very often mandatory (unless using, if at all possible, heavyweight roundabout computations). To avoid non-causal curves, we propose an algorithm that turns a non-causal pair of curves into a causal one. After application of this algorithm, event generators based on arrival curves cannot deadlock, and formal verifiers do no more produce spurious counter-examples linked to causality.

The additional benefit of the transformation is that it gives the tightest pair of curves equivalent to the original one, which is also a canonical representative of all arrival curve pairs defining the same set of event streams. Indeed, compared to the "mathematical refinement algorithm" proposed in [13], our algorithm is more general and potentially more precise. Indeed, the next version of this work [1] uses directly the causality closure instead.

The theorems and algorithms work for discrete and fluid event model, discrete and continuous time for infinite curves. Given any subset of these models, one just has to implement the basic operators ($\otimes$, $\overline{\otimes}$, $\oslash$, $\overline{\oslash}$ and SA-SA closure) to be able to use them. They have also been adapted to discrete time and event model for the case of finite arrival curves, where the sub-additive and super-additive closure operators do not make sense (this was implemented in the `ac2lus` [2] toolbox). We also presented the case of concave/convex piecewise affine curves, which do not have the problem at all, and a combination of finite discrete curves with this model, which also needed some adaptation of the general algorithm.

References

[1] Karine Altisen, Yanhong Liu, and Matthieu Moy. Performance evaluation of components using a granularity-based interface between real-time calculus and timed automata. In *QAPL*, 2010. 1, 1, 4.2, 6

[2] Karine Altisen and Matthieu Moy. ac2lus: Bringing SMT-solving and abstract interpretation techniques to real-time calculus through the synchronous language Lustre. In *22nd Euromicro Conference on Real-Time Systems (ECRTS)*, Brussels, Belgium, Jully 2010. (document), 1, 4.2, 5.1.1, 5.3, 6

[3] Karine Altisen and Matthieu Moy. Arrival curves for real-time calculus: the causality problem and its solutions. In *TACAS*, March 2010. 1, 6

[4] A. Bouillard and É. Thierry. An algorithmic toolbox for network calculus. *Discrete Event Dynamic Systems*, 18(1):3–49, 2008. 5.1.1

[5] Thomas A. Henzinger, Xavier Nicollin, Joseph Sifakis, and Sergio Yovine. Symbolic model checking for real-time systems. *Information and Computation*, 111:394–406, 1992. 1

[6] B. Jeannet. Dynamic partitioning in linear relation analysis. application to the verification of reactive systems. *Formal Methods in System Design*, 2003. 1, 1, 4.2

[7] Bengt Jonsson, Simon Perathoner, Lothar Thiele, and Wang Yi. Cyclic dependencies in modular performance analysis. In *EMSOFT*, 2008. 2.2.3

[8] Simon Künzli, Francesco Poletti, Luca Benini, and Lothar Thiele. Combining simulation and formal methods for system-level performance analysis. In *DATE '06: Proceedings of the conference on Design, automation and test in Europe*, pages 236–241, 3001 Leuven, Belgium, Belgium, 2006. European Design and Automation Association. 1

[9] K. Lampka, S. Perathoner, and L. Thiele. Analytic real-time analysis and timed automata: a hybrid methodology for the performance analysis of embedded real-time systems. *Design Automation for Embedded Systems*, pages 1–35, June 2010. (document), 1, 4.2, 5.2, 5.3

[10] Kai Lampka, Simon Perathoner, and Lothar Thiele. Analytic real-time analysis and timed automata: A hybrid method for analyzing embedded real-time systems. In *EMSOFT*, 2009. (document), 1, 4.2, 5.2

[11] Jean-Yves Le Boudec and Patrick Thiran. *Network Calculus*. Springer Verlag, 2001. 1, 4, 5, 2.2.2, 3.3.4

[12] C. L. Liu and James W. Layland. Scheduling algorithms for multiprogramming in a hard-real-time environment. *J. ACM*, 20(1):46–61, 1973. 1

[13] Yanhong Liu, Karine Altisen, and Matthieu Moy. Granularity-based interfacing between RTC and timed automata performance models. Technical Report TR-2009-10, Verimag, 2009. 6

[14] Leonid Mokrushin. Compositional analysis of timed systems by abstraction. PowerPoint Slides, 2007. (document)

[15] Matthieu Moy and Karine Altisen. Arrival curves for real-time calculus: the causality problem and its solutions. Technical Report TR-2009-15, Verimag, 2009. 5.4.5

[16] Linh T.X. Phan, Samarjit Chakraborty, P.S. Thiagarajan, and Lothar Thiele. Composing functional and state-based performance models for analyzing heterogeneous real-time systems. In *RTSS*, 2007. (document), 1, 4.2

[17] Pascal Raymond. *Compilation efficace d'un langage declaratif synchrone: Le generateur de code Lustre-v3*. PhD thesis, Institut National Polytechnique de Grenoble - INPG, November 1991. Section 13.7, "Causalité" (pages 119–123). (document), 1

[18] Pascal Raymond. *Lustre v4 Manual*. Verimag, February 2000. 1

[19] Lothar Thiele, Samarjit Chakraborty, and Martin Naedele. Real-time calculus for scheduling hard real-time systems. In *ISCAS*, 2000. (document), 1, 2.2.2

[20] Uppsala University. Cats tool, 2007. `http://www.timestool.com/cats`. 1, 4.2

Contents