

Informe correspondiente al proyecto de iniciación a la investigación

# **Verificación de Sistemas Reactivos y de Tiempo Real en Teoría de Tipos**

Carlos Daniel Luna<sup>†</sup>

*Instituto de Computación (InCo). Facultad de Ingeniería.  
Universidad de la República. Montevideo, Uruguay.*

cluna@fing.edu.uy

Junio de 2002

---

<sup>†</sup> El proyecto de iniciación a la investigación fue solventado con una beca CSIC.

## Resumen

---

Para el análisis de sistemas reactivos y de tiempo real dos importantes enfoques formales se destacan: la verificación de modelos y el análisis deductivo basado en asistentes de pruebas. El primero se caracteriza por ser completamente automatizable pero presenta dificultades al tratar con sistemas con un gran número de estados o que tienen parámetros no acotados. El segundo permite tratar con sistemas arbitrarios pero requiere la interacción del usuario.

Este trabajo explora una metodología de trabajo que permita compatibilizar el uso de un verificador de modelos como *Kronos* y el asistente de pruebas *Coq* en el análisis de sistemas de tiempo real. Para ello formalizamos grafos (autómatas) temporizados y la lógica TCTL (y CTL) en el cálculo de construcciones inductivas y co-inductivas de *Coq*, a fin de disponer de lenguajes de especificación y análisis comunes a ambas herramientas. Los grafos permiten describir los sistemas, mientras que la lógica se usa para especificar los requerimientos temporales. Una parte importante del trabajo está dedicada a estudiar cómo razonar deductivamente en *Coq* sobre esta clase de sistemas –la utilidad de tipos inductivos y la necesidad de tipos co-inductivos– asumiendo inicialmente un modelo de tiempo discreto.

---

**Palabras Claves.** Especificación y Análisis de Sistemas de Tiempo Real. Autómatas (Grafos) Temporizados. Lógicas TCTL y CTL. Verificación de Modelos (“Model Checking”). Teoría de Tipos y Coq. Verificación-Demostración de Corrección.

## Contenidos

|   |    |
|---|----|
| <b>Capítulo 1: Introducción</b> .....                                       | 1  |
| 1.1 Verificación de Modelos .....   | 2  |
| 1.2 Demostración de Corrección .....  | 2  |
| 1.3 Complementariedad de los Enfoques .....                                 | 3  |
| 1.4 Acerca de <i>Coq</i> .....  | 5  |
| 1.5 Organización del Trabajo .....  | 6  |
| <b>Capítulo 2: Grafos Temporizados y TCTL</b> .....                         | 7  |
| 2.1 Grafos (Autómatas) Temporizados .....                                   | 7  |
| 2.1.1 Semántica Formal .....  | 8  |
| 2.1.2 Trazas de Ejecución .....   | 10 |
| 2.2 Composición Paralela de Grafos Temporizados .....                       | 10 |
| 2.2.1 Definición de Composición .....                                       | 11 |
| 2.1.2 Semántica .....   | 11 |
| 2.3 Lógica TCTL: “Timed Computation Tree Logic” .....                       | 12 |
| 2.3.1 Semántica de TCTL .....   | 13 |
| 2.3.2 Algunas Abreviaturas .....  | 14 |
| 2.4 Verificación de Modelos: Grafos Temporizados y TCTL .....               | 14 |
| 2.5 Discretización del Tiempo .....   | 15 |
| 2.5.1 Tiempo Continuo versus Tiempo Discreto .....                          | 15 |
| 2.5.2 Un Modelo de Tiempo Discreto .....                                    | 16 |
| 2.5.3 Interpretación Algorítmica de Grafos Temporizados .....               | 17 |
| <b>Capítulo 3: Formalización de Grafos Temporizados y TCTL en Coq</b> ..... | 21 |
| 3.1 Nociones Temporales .....   | 21 |
| 3.2 Definiciones Elementales de Grafos Temporizados .....                   | 22 |
| 3.3 Operadores Temporales con Tipos Inductivos .....                        | 24 |
| 3.3.1 Estados Alcanzables .....   | 24 |

|  |           |
|--|-----------|
| 3.3.2 Invarianza y Alcanzabilidad .....                                      | 25        |
| 3.3.3 Algunas Propiedades .....  | 27        |
| 3.4 Necesidad de Tipos Co-Inductivos .....                                   | 29        |
| 3.4.1 Nociones Preliminares .....  | 29        |
| 3.4.2 Operadores Temporales Cualitativos .....                               | 30        |
| 3.4.3 Operadores Temporales Cuantitativos .....                              | 34        |
| <b>Capítulo 4: Caso de Estudio: Control de un Paso a Nivel de Tren .....</b> | <b>39</b> |
| 4.1 Descripción del Problema .....   | 39        |
| 4.2 Especificación del Sistema en <i>Coq</i> .....                           | 41        |
| 4.3 Análisis del Sistema TCG .....   | 47        |
| 4.3.1 Demostración de Invariantes .....                                      | 47        |
| Invariantes .....  | 47        |
| Comentarios .....  | 52        |
| Algunas Tácticas (Simples) Útiles .....                                      | 52        |
| 4.3.2 Propiedad Fundamental de <i>Safety</i> .....                           | 56        |
| 4.3.3 Propiedad de <i>Liveness Non-Zeno</i> .....                            | 56        |
| Un Sistema Mal Temporizado .....   | 58        |
| 4.3.4 Acerca de los Términos de Prueba .....                                 | 59        |
| 4.4 Parametrización del Sistema TCG .....                                    | 60        |
| 4.5 Trabajos Relacionados .....  | 62        |
| <b>Capítulo 5: Representaciones Genéricas de Grafos Temporizados .....</b>   | <b>65</b> |
| 5.1 Grafos Temporizados Genéricos en <i>Coq</i> .....                        | 65        |
| 5.1.1 Representación .....   | 65        |
| 5.1.2 Composición Paralela .....   | 67        |
| 5.1.3 Trazas de Ejecución .....  | 68        |
| 5.1.4 Una Representación Alternativa .....                                   | 70        |
| 5.1.4 Discusión .....  | 71        |
| 5.2 Grafos con Tiempo Continuo .....   | 72        |

|   |            |
|---|------------|
| 5.2.1 Adaptación de las Formalizaciones Previas .....                           | 72         |
| 5.2.2 Limitaciones de los Reales y los Racionales en <i>Coq</i> .....           | 73         |
| <b>Capítulo 6: Conclusiones, Trabajos Relacionados y Trabajos Futuros .....</b> | <b>75</b>  |
| 6.1 Conclusiones .....  | 75         |
| Una Metodología de Trabajo .....  | 76         |
| 6.2 Trabajos Relacionados .....   | 79         |
| 6.3 Trabajos Futuros .....  | 79         |
| <b>Referencias Bibliográficas .....</b>   | <b>83</b>  |
| <b>Apéndice A: Nociones Temporales .....</b>                                    | <b>89</b>  |
| <b>Apéndice B: Operadores Temporales: Definiciones y Propiedades .....</b>      | <b>91</b>  |
| B.1 Invarianza y Alcanzabilidad (con Tipos Inductivos) .....                    | 91         |
| B.1.1 Definiciones .....  | 91         |
| B.1.2 Propiedades .....   | 92         |
| B.1.3 Definiciones Complementarias .....  | 94         |
| B.2 Operadores CTL (con Tipos Co-Inductivos) .....                              | 95         |
| B.2.1 Definiciones .....  | 95         |
| B.2.2 Propiedades .....   | 96         |
| B.3 Operadores TCTL (con Tipos Co-Inductivos) .....                             | 99         |
| B.3.1 Definiciones .....  | 99         |
| B.3.2 Propiedades .....   | 100        |
| <b>Apéndice C: Especificación y Análisis del Sistema TCG .....</b>              | <b>103</b> |
| C.1 Especificación .....  | 103        |
| C.2 Análisis .....  | 105        |
| C.2.1 Propiedades de los Relojes y los Parámetros del Sistema .....             | 105        |
| C.2.2 Lemas de Inversión .....  | 110        |
| C.2.3 Algunas Tácticas Útiles .....   | 111        |
| C.2.4 Invariantes y Propiedad de <i>Safety</i> : Demostraciones .....           | 113        |

---

|   |     |
|---|-----|
| C.2.5 Propiedad de <i>Liveness Non-Zero</i> ..... | 119 |
| Lemas, Definiciones y Tácticas Auxiliares .....   | 119 |
| Demostración de <i>Non-Zero</i> .....             | 122 |

# Capítulo 1

## *Introducción*

---

Cada vez son más frecuentes las aplicaciones donde el tiempo juega un rol importante. Por ejemplo en: protocolos de comunicación, controladores de robots, de comandos de aviones, de pasos a nivel de trenes, de dispositivos electrónicos (o electro-mecánicos) y de procesos industriales automatizados, aplicaciones multimedia y de internet, entre otras. En general éstas son aplicaciones críticas, en las cuales una falla o mal funcionamiento pueden acarrear consecuencias graves, tales como poner en juego vidas humanas y/o grandes inversiones económicas. El comportamiento de estos sistemas, llamados *sistemas de tiempo real*, no está determinado únicamente por la sucesión de acciones que se ejecutan, sino también por el momento en que las mismas ocurren y son procesadas. El tiempo de ejecución es “*t*” parámetro fundamental en el comportamiento de esta clase de sistemas y una gran parte, quizás la más importante, de los requerimientos de los mismos son temporales: “tal acción debe ejecutarse en un lapso de tiempo determinado”, “el tiempo transcurrido entre dos eventos o señales debe estar acotado por un valor constante”, “si un tren está próximo a cruzar un paso a nivel y han pasado más de *t* unidades de tiempo desde que se activó una señal de acercamiento, la barrera debe estar baja”, etc.

Es indiscutible hoy la influencia que tiene en la industria y en casi todos los ámbitos el uso del software. La cantidad de aplicaciones reales y potenciales de la computación ha alcanzado cotas inimaginables apenas veinte años atrás. A pesar de su uso extensivo, uno de los costos más alto no se da en la producción del software, sino en la corrección de errores que son detectados posteriormente al desarrollo del sistema. En la actualidad, el método más usado para validar software es el “*testing*”, que consiste en la simulación sobre casos de prueba representativos. No obstante, este método no garantiza la corrección del software analizado, por ser incompleto en la mayoría de los casos [MGJ91]. En las aplicaciones críticas, que tratan con vidas humanas y/o grandes inversiones económicas, la *certeza de corrección* es, en general, un criterio indispensable. De un software correcto se espera que resuelva un problema determinado por una *especificación* y que exista una justificación formal –matemática– de que el programa la satisface.

En los últimos años un gran esfuerzo de investigación se ha invertido en el desarrollo de métodos y herramientas para la especificación y el análisis de la corrección de

sistemas de tiempo real. Sin embargo no hay un formalismo, una metodología o una herramienta claramente preferibles a otras en todas circunstancias.

Para el análisis de la corrección de esta clase de sistemas dos importantes enfoques formales se destacan:

- **Verificación de corrección.** En este enfoque un sistema es considerado correcto cuando se prueba que *toda* ejecución posible satisface la especificación. Existen algunas técnicas bien conocidas que permiten recorrer de manera exhaustiva el espacio de ejecuciones posibles y herramientas que las implementan.
- **Demostración de corrección.** En este caso se construye o deriva una *prueba* matemática de que el sistema satisface su especificación. Aquí las herramientas asisten al programador en el proceso de construcción de la prueba.

## 1.1 Verificación de Modelos

El método de verificación llamado *verificación de modelos* (“*model checking*”) fue desarrollado para verificar *sistemas reactivos* –aquellos que se comportan como una secuencia de estímulos-respuestas en relación al medio– y posteriormente ha sido extendido también a *sistemas de tiempo real*, en los cuales la corrección depende de las magnitudes de los retardos temporales.

Usando esta metodología los sistemas se modelan como *grafos* y la especificación se expresa, generalmente, mediante fórmulas en una *lógica temporal* (por ejemplo, [Pnu85, CES86, Eme95]). Un procedimiento eficiente se utiliza para determinar automáticamente si las especificaciones son satisfechas por los grafos. Esta técnica ha sido usada con éxito para detectar errores sutiles en distintos sistemas, en particular en protocolos de comunicaciones (por ejemplo, [WH95]).

Durante los últimos años el tamaño de los sistemas que pueden ser verificados de esta manera se ha incrementado notoriamente. Esto ha sido consecuencia del desarrollo de nuevas técnicas dentro de la misma estrategia, como el “*symbolic model checking*” y la verificación “*on the fly*”. Entre las herramientas que implementan algunas de estas técnicas se destacan *Kronos* [Yov97], *HyTech* [HHW<sup>+</sup>97] y *Uppaal* [LPY97].

## 1.2 Demostración de Corrección

Esta aproximación permite construir una *demostración* –en el sentido matemático del término– de que un sistema satisface una especificación. En este trabajo estamos interesados en herramientas basadas en *teorías constructivas de tipos* [CH85, Coq86, CH88], las cuales han sido formuladas como fundamento de la Matemática Constructiva.

En la última década, varios equipos de investigación han dedicado un considerable esfuerzo al diseño e implementación de editores de prueba interactivos basados en teorías de tipos. Ejemplos de estos sistemas son *ALF* [Mag94], *Coq* [Bar<sup>+</sup>99] y *LEGO* [LP92].



Una de las principales características de los mismos es el carácter unificador de la teoría que implementan, en la cual pueden ser expresados programas, teoremas y pruebas de éstos. Otro punto destacable es que el usuario es guiado en forma interactiva por el sistema en el proceso de construcción de un programa o una prueba, siendo verificada inmediatamente la validez de cada paso del desarrollo. El principal objetivo de estos sistemas es convertirse en sofisticadas herramientas que asistan en la tarea del desarrollo incremental de programas correctos. Sin embargo, el marco conceptual necesario para desarrollar software verificado es de una muy alta complejidad y requiere cubrir muchos aspectos que en realidad escapan a la construcción de un asistente de pruebas.

Estos sistemas disponen de un lenguaje de especificación de orden superior, permiten hacer pruebas en lógica de alto orden y proveen definiciones de tipos inductivos y co-inductivos. La experimentación desarrollada en su uso se ha enfocado principalmente en demostrar la corrección de programas secuenciales, pero dado su poder expresivo consideramos que pueden ser también adecuados para razonar sobre sistemas reactivos y, en particular, de tiempo real. Algunas experiencias llevadas a cabo en esta dirección y particularmente en *Coq* son [Gim95, -96, -99], entre otras.

### 1.3 Complementariedad de los Enfoques

Los verificadores de modelos (“model-checkers”) son usados actualmente en la industria con éxito para verificar sistemas reactivos, paralelos y de tiempo real, ya que son fáciles de usar y no requieren la asistencia del usuario en el proceso de prueba. Sin embargo, ellos en general presentan problemas al tratar con sistemas grandes (con muchos estados) o donde se tienen parámetros variables, no acotados. Los asistentes de prueba antes citados y otros como [ORS92, Gor93, Pau93b] proveen una solución alternativa para estos casos, aunque la complejidad del proceso de análisis se incrementa muchas veces en forma considerable. No obstante, el enfoque deductivo presenta como ventajas comparativas, además de las nombradas, entre otras, las siguientes:

- Al demostrar una propiedad de un sistema no sólo se tiene la certeza de que vale la propiedad, sino por qué esto es así. El desarrollo de una prueba induce a tener un conocimiento más profundo del sistema, muchas veces a descubrir nuevas propiedades o generalizarlas. Asimismo, en el proceso de prueba se puede llegar a descubrir las causas por las cuales una propiedad no vale e incluso, algunas veces, las modificaciones necesarias del sistema para que la cumpla.
- El proceso de construcción de las pruebas es incremental y composicional. Esto es, las propiedades demostradas pueden ser utilizadas en la prueba de otras, sin ser necesario hacer dicho proceso cada vez desde cero. Asimismo, una demostración bien pensada permite, en general, reutilizar una estrategia de prueba en la demostración de otros teoremas.

- El enfoque deductivo permite mayor rehuso. En el método de verificación de modelos cuando una modificación es introducida en el sistema, todo el proceso de verificación debería ser ejecutado nuevamente desde el comienzo. Sin embargo, muchas veces las pruebas, o algunas de ellas, o partes de las mismas, pueden mantenerse luego de un cambio, si la estrategia de demostración está bien estructurada (por ejemplo, al modificar algunas de las constantes del problema o alguna condición lógica entre las mismas).
- Las demostraciones de propiedades de un sistema pueden permitir generalizar la especificación del mismo, preservando las propiedades de interés. Esta característica será explotada en el trabajo en el análisis de un caso de estudio.

Los dos enfoques referidos se consideraban al comienzo diametralmente opuestos para el análisis de sistemas reactivos y de tiempo real. Sin embargo, en los últimos años surgió un interés creciente en combinarlos, debido, en parte, a que los mismos pueden ser cooperativos y no sólo competitivos entre sí. La idea es compensar las desventajas de un enfoque con las ventajas del otro, aunque aún no está claro cómo lograr dicho objetivo. Algunos referentes en esta dirección son [MN95, RSS95, HS96, BMS<sup>+</sup>97, SS99, KKP99], entre otros muchos.

Este trabajo está enmarcado en una propuesta de proyecto de investigación que vincula al proyecto *Coq* del INRIA –Rocquencourt (Francia)– y al grupo de Métodos Formales del Instituto de Computación de la Universidad de la República (Uruguay). El proyecto, titulado “Integración de dos enfoques para la verificación formal de sistemas reactivos: Teoría de Tipos y Verificación de Modelos”, tiene por objetivo estudiar la integración de los dos enfoques previamente referidos para la verificación de sistemas reactivos y de tiempo real (Octubre de 1998).

En este marco, nuestro objetivo es dar un pequeño paso en una combinación posible entre ambos enfoques, estableciendo una metodología de trabajo que permita compatibilizar el uso de un *model checker* como *Kronos* y el asistente de pruebas *Coq*. A fin de lograr esto nos proponemos formalizar *grafos (autómatas) temporizados* [ACD90, Oli94, HNS<sup>+</sup>92] y la *lógica TCTL (timed computation tree logic)* [ACD90, HNS<sup>+</sup>92] en el *cálculo de construcciones inductivas y co-inductivas* de *Coq* [Bar<sup>+</sup>99]. Los grafos temporizados permiten describir sistemas de tiempo real, mientras que la lógica TCTL es un lenguaje adecuado y ampliamente usado para especificar propiedades (requerimientos) temporales. *Kronos* permite verificar si un grafo temporizado satisface una fórmula TCTL, siempre que los parámetros del sistema sean valores constantes. El análisis deductivo nos permite trabajar con parámetros variables y de esta manera verificar sistemas más generales. En este contexto, a las ventajas citadas del enfoque deductivo se suma una muy importante: la posibilidad de realizar *síntesis de programas* a partir de una formalización en teoría de tipos. Esta es una línea que no será explotada en el trabajo pero que justifica aún más el interés de esta experiencia.

## 1.4 Acerca de *Coq*

El asistente de pruebas *Coq* es una implementación del *cálculo de construcciones inductivas*, una lógica intuicionista de alto orden con tipos dependientes y tipos inductivos como objetos primitivos [CH88, P-M93]. El usuario introduce definiciones y hace demostraciones en un estilo de *deducción natural*, las cuales son chequeadas mecánicamente por el sistema.

Dicho formalismo permite especificar y probar en lógica intuicionista de alto orden. Esta lógica asocia una interpretación computacional a las pruebas, la noción de veracidad de una proposición corresponde a la existencia de una prueba. Curry y Howard demostraron que los siguientes juicios son equivalentes:

- “ $t$  es una demostración de la proposición  $A$ ”.
- “el término  $t$  tiene tipo  $A$ ”.
- “ $t$  es un programa de la especificación  $A$ ”.

Esto es, probar una proposición  $A$  es equivalente a construir un término de tipo  $A$ . Esta equivalencia es conocida como isomorfismo de Curry-Howard [CF58, How80] y está basada en que las pruebas en deducción natural pueden ser representadas como términos de un cálculo lambda tipado [How80], o que es lo mismo, de un lenguaje de programación funcional (por ejemplo, *Caml* [WL99]). Consecuentemente, *Coq* puede ser considerado, rigurosamente hablando, un chequeador de tipos (“type-checker”).

A los efectos de diferenciar objetos computacionales de información lógica, distinguimos dos clases de tipos importantes en *Coq*: *Prop* para los tipos que contienen términos lógicos (las proposiciones) y *Set* que agrupa a los tipos que contienen información computacional (los conjuntos). Por ejemplo, los números naturales se definen en *Set* y las relaciones  $\leq$  y la conjunción  $\wedge$  en *Prop*. *Set* y *Prop* pertenecen a *Type*, que es en realidad una familia infinita de tipos notada de esta forma. Un procedimiento de *extracción de programas* puede ser usado para remover las partes lógicas de los términos, manteniendo sólo las partes de información computacional [P-M89a, P-M89b].

Además de los habituales tipos inductivos (o sea, conjuntos definidos inductivamente, como por ejemplo los números naturales o las listas finitas), *Coq* permite también la definición de tipos *co-inductivos*. Estos son tipos recursivos que pueden contener objetos infinitos, no bien fundados. Un ejemplo de tipos co-inductivos es el de las secuencias infinitas, usualmente llamadas *streams*, de elementos de un tipo dado.

En el proceso de prueba de un teorema, *Coq* entra en un ciclo interactivo donde el usuario completa la demostración usando *tácticas*, las cuales implementan reglas de inferencia o de tipado (esquemas de prueba). El conjunto de tácticas puede ser incrementado por el usuario, a partir de un lenguaje diseñado para tal fin.

En este trabajo no estamos interesados en dar una descripción completa del cálculo de construcciones inductivas y co-inductivas, ni del sistema de *Coq*, en general. Por aspectos teóricos el lector puede referirse a [CH85, Coq86, CH88] por el cálculo puro de

construcciones, a [P-M93] por tipos inductivos y a [Coq93, Pau93a, Gim96] por tipos co-inductivos. Acerca de *Coq*, una buena introducción son los tutoriales [HKP96, Gim98] y detalles adicionales pueden encontrarse en el manual de referencia [Bar<sup>+</sup>99].

## 1.5 Organización del Trabajo

La organización del trabajo es como sigue. En el capítulo 2 introducimos los grafos temporizados, usados para describir sistemas de tiempo real, y la lógica TCTL, utilizada como lenguaje de especificación de propiedades temporales. Asimismo, analizamos una discretización del dominio temporal continuo inherente a los grafos y la lógica considerados, en base a la cual obtenemos una semántica alternativa, que asumiremos en el resto de este trabajo.

En el capítulo 3 formalizamos en *Coq* grafos temporizados y la lógica TCTL. Incluimos además operadores de la lógica CTL (*computation tree logic*) [CES86] y algunas definiciones alternativas para los operadores que permiten expresar *invarianza* y *alcanzabilidad*, con tipos inductivos (bajo la noción de estados alcanzables) y co-inductivos (bajo la noción de trazas –infinitas– de ejecución). Asimismo, formulamos y demostramos algunas propiedades generales de los operadores temporales.

En el capítulo 4 consideramos un caso de estudio: *el control de un paso a nivel de tren* (“*the railroad crossing example*”). Especificamos el sistema en *Coq* en base a las formalizaciones introducidas en el capítulo 3. Analizamos luego la demostración de *invariantes*, incluyendo la propiedad de seguridad esencial del sistema, y verificamos la divergencia del tiempo en las ejecuciones. Posteriormente generalizamos la especificación: parametrizamos las constantes del problema y definimos restricciones entre estos parámetros y los relojes del sistema a fin de preservar las propiedades estudiadas. La mayor parte del trabajo está dedicada al análisis de este caso de estudio.

En el capítulo 5 definimos dos representaciones genéricas de grafos temporizados para la semántica de tiempo discreto considerada en los capítulos previos, una de las cuales es extendida a tiempo continuo. Estas representaciones permiten definir sistemas como instancias particulares y simplifican el proceso de definición de sistemas compuestos.

Las conclusiones, algunos trabajos relacionados y los trabajos futuros se incluyen en el capítulo 6. En particular, describimos una metodología de trabajo para la especificación y el análisis de grafos temporizados en función de las formalizaciones introducidas en los capítulos 3 y 5, y el caso de estudio abordado en el capítulo 4. Finalmente, las formalizaciones y las pruebas completas del trabajo se adjuntan como apéndices.

# Capítulo 2

## *Grafos Temporizados y TCTL*

---

En este capítulo introducimos los grafos temporizados, que permiten describir sistemas de tiempo real, y la lógica TCTL, usada como lenguaje de especificación de propiedades temporales. Asimismo, analizamos una discretización del dominio temporal continuo inherente a los grafos y la lógica considerados, en base a la cual obtenemos una semántica alternativa, que asumiremos en el resto de este trabajo.

### 2.1 Grafos (Autómatas) Temporizados

Los grafos temporizados constituyen un modelo matemático-computacional en el cual pueden representarse de manera formal, simple, clara y modular muchos problemas del mundo real donde hay restricciones temporales que interfieren con transiciones discretas, las cuales representan acciones o eventos. Varias definiciones similares de *grafos (autómatas) temporizados* han sido propuestas, como es el caso de [ACD90, HNS<sup>+</sup>92, Yov93, Oli94, AD94].

Un grafo temporizado es un autómata extendido con un conjunto *finito* de variables reales, llamadas *relojes*, cuyos valores se incrementan uniformemente con el paso del tiempo. Dichos relojes son utilizados para medir, por ejemplo, el tiempo transcurrido entre dos eventos, el tiempo de espera o la demora de una comunicación. Las restricciones temporales inherentes a las acciones del sistema son expresadas ligando condiciones de *activación* a cada una de las transiciones del autómata. Una transición está *habilitada*, es decir puede ser atravesada, cuando su condición asociada es satisfecha por los valores de los relojes. Un reloj puede ser puesto a cero en cualquier transición. A todo instante, el valor de un reloj es igual al tiempo transcurrido desde la última vez en que fue puesto a cero [ACD90, DOY96].

**Definición 2.1.** Sea  $A$  un conjunto (global) de *etiquetas* que asumiremos fijo en este capítulo. Un *grafo (autómata) temporizado* es una quintupla  $G = \langle L, X, E, l^0, I \rangle$ , donde:

- $L$  es un conjunto finito de nodos llamados *locaciones*.
- $X$  es un conjunto finito de *relojes*. Una *valuación*  $v$  de los relojes es una función que asigna un valor  $v(x) \in \mathcal{R}^+$  a cada reloj  $x \in X$ , donde  $\mathcal{R}^+$  son los números reales no

negativos.  $V$  denota el conjunto de las valuaciones. Escribiremos  $v+t$  como la valuación  $v'$  tal que  $v'(x)=v(x)+t$  para todos los relojes  $x \in X$ .

- $E$  es un conjunto finito de aristas llamadas *transiciones*. Cada transición es una quintupla  $e = \langle l, \alpha, \psi_X, \rho_X, l' \rangle$  que consiste en una locación origen  $l \in L$ , una locación destino  $l' \in L$ , una etiqueta  $\alpha \in A$ , una condición  $\psi_X$  y un conjunto  $\rho_X \subseteq X$  de relojes que son puestos a cero (reseteados) simultáneamente con la transición. Una condición es una combinación booleana de átomos de la forma  $x < c$ , donde  $x \in X$ ,  $<$  es una relación binaria en el conjunto  $\{<, \leq, =, \geq, >\}$  y  $c$  es una constante entera positiva. Denotamos  $\Psi_X$  al conjunto de los predicados  $\psi_X$  definibles sobre  $X$ . La transición  $e = \langle l, \alpha, \psi_X, \rho_X, l' \rangle$  está habilitada en un estado  $\langle l, v \rangle$  si  $v$  satisface la condición  $\psi_X$ . Escribiremos  $v[\rho_X := 0]$  como la valuación  $v'$  tal que  $v'(x)=0$  si  $x \in \rho_X$  y  $v'(x)=v(x)$  en caso contrario.
- $l^0$  es la *locación inicial*. El estado inicial del sistema es  $\langle l^0, v^0 \rangle$ , con  $v^0(x)=0$  para todo  $x \in X$ , es decir, la locación inicial con todos los relojes puestos en cero.
- $I$  es el conjunto de *invariantes de las locaciones* del grafo. Para cada  $l \in L$ ,  $I_l \in \Psi_X$  es el *invariante* de la locación. Cuando el sistema se encuentra en un estado  $\langle l, v \rangle$ , éste puede permanecer en la locación  $l$  dejando pasar el tiempo, mientras la valuación corriente de los relojes satisfaga el invariante  $I_l$ .

## Observaciones

- Los grafos temporizados pueden ser alternativamente definidos como una séxtupla, agregando un conjunto de etiquetas en vez de considerar un conjunto global  $A$  [AD94].
- Cada transición está rotulada con una sola etiqueta. Sin embargo, algunos trabajos consideran transiciones rotuladas con conjuntos de etiquetas (por ejemplo, [AD94]).
- En algunas definiciones de grafos temporizados no se distingue un estado inicial.

En lo que sigue del trabajo usaremos indistintamente los términos grafos temporizados y autómatas temporizados.

### 2.1.1 Semántica Formal

La semántica de un grafo temporizado puede definirse en función de *un sistema de transiciones etiquetado* [Oli94], donde los estados son pares  $\langle l, v \rangle \in L \times V$  y las transiciones son de dos tipos:

- *Temporales*. Los nodos del grafo representan una actividad continua, dada por el paso del tiempo. El paso de un tiempo  $t$  es representado por una transición etiquetada con  $t$ .

- *Discretas (instantáneas)*. Las aristas del grafo representan acciones discretas. La ejecución de una acción  $\alpha$  es una transición que lleva la etiqueta  $\alpha$ .

**Definición 2.2.** El modelo de un grafo temporizado  $G = \langle L, X, E, I^0, I \rangle$  es el sistema de transiciones etiquetado  $T = \langle Q, \rightarrow \rangle$ , donde:

- $Q = \{ \langle l, v \rangle \mid l \in L, v \in V, I_l[v] \}$  es el conjunto de estados.  $I_l[v]$  significa que  $I_l$  es verdadero para la valuación  $v$  de los relojes. Los estados de  $Q$  serán llamados *estados válidos* del sistema (satisfacen los invariantes de las locaciones). Para  $q = \langle l, v \rangle \in Q$ ,  $Loc(q)$  denota la locación  $l$ .
- $\rightarrow \subseteq Q \times (A \cup \mathcal{F}^+) \times Q$  es la relación de transición, definida por las siguientes reglas:

$$\frac{I_l[v+t'] \quad 0 \leq t' \leq t}{\langle l, v \rangle \xrightarrow{t} \langle l, v+t \rangle}$$

Es una *transición temporal* sobre la locación  $l$ . El sistema puede permanecer en dicha locación mientras los valores de los relojes satisfagan  $I_l$ . El estado  $\langle l, v+t \rangle$  es un *sucesor temporal* del estado  $\langle l, v \rangle$ .

$$\frac{\langle l, \alpha, \psi_X, \rho_X, l' \rangle \in E \quad \psi_X[v]}{\langle l, v \rangle \xrightarrow{\alpha} \langle l', v[\rho_X := 0] \rangle}$$

Es una *transición discreta* de  $l$  a  $l'$  por la acción  $\alpha$ , cuando  $v$  satisface la restricción  $\psi_X$ . El estado  $\langle l', v[\rho_X := 0] \rangle$  es el *sucesor discreto* del estado  $\langle l, v \rangle$  por  $\alpha$ . La condición  $I_l(v) \wedge I_{l'}(v[\rho_X := 0])$  está implícita en la regla anterior, ya que la relación de transición se define entre estados válidos, es decir  $\langle l, v \rangle \in Q$  y  $\langle l', v[\rho_X := 0] \rangle \in Q$ .

**Notación.** Escribimos  $q \xrightarrow{lab} q'$  en lugar de  $\langle q, lab, q' \rangle \in \rightarrow$ , para  $lab \in A \cup \mathcal{F}^+$ .

### Observaciones

- El tiempo pasa sólo en las locaciones (*transiciones temporales*).
- Para todo estado  $q$  hay una transición al mismo estado que toma tiempo cero.
- Atravesar una arista no insume tiempo (*transiciones instantáneas*).
- Los valores de los relojes crecen *uniformemente* con el tiempo.
- Respecto a las *transiciones temporales*, el sistema es determinístico, pero respecto a las transiciones instantáneas, el sistema no lo es en el caso general [Oli94].

## 2.1.2 Trazas de Ejecución

Una *ejecución* (*traza de ejecución*) de un grafo temporizado  $G$  es una secuencia de estados  $q_0 \xrightarrow{t_0} q_0' \xrightarrow{\alpha_0} q_1 \xrightarrow{t_1} q_1' \xrightarrow{\alpha_1} q_2 \dots$ , donde  $q_i \xrightarrow{t_i} q_i'$  representa una transición temporal,  $q_i' \xrightarrow{\alpha_i} q_{i+1}$  es una transición discreta o una transición temporal con tiempo cero, y  $q_0$  es el estado inicial de la ejecución. Denotamos  $R_G$  al conjunto de todas las ejecuciones de  $G$  y  $R_G(q_0)$  a las que comienzan en el estado  $q_0$ .

Observemos que una transición  $q_i \xrightarrow{t_i} q_i'$  representa conceptualmente a los *infinitos* estados de la forma  $q_i + t'$ , con  $t' \leq t_i$ , y que la definición de ejecución dada permite que dos o más eventos discretos sucedan consecutivamente en el tiempo, asumiendo transiciones temporales intermedias con tiempo nulo. Notemos además que dos o más transiciones temporales consecutivas pueden ser representadas por una única cuyo valor temporal está dado por la suma de los valores correspondientes a los pasos individuales o intercalando una transición temporal con tiempo cero.

Sea  $r$  una ejecución  $q_0 \xrightarrow{t_0} q_0' \xrightarrow{\alpha_0} q_1 \xrightarrow{t_1} q_1' \xrightarrow{\alpha_1} q_2 \dots$  de  $R_G(q_0)$ , una *posición*  $\pi$  de  $r$  es un par  $\langle i, t \rangle \in \mathcal{L} \times \mathcal{T}^+$ , con  $0 \leq t \leq t_i$ . Escribimos  $\sigma_r(\pi)$  para denotar al estado  $\langle l, v+t \rangle$  con  $q_i = \langle l, v \rangle$ , y  $\delta_r(\pi)$  para el tiempo  $\sum_{j < i} t_j + t$  transcurrido desde el comienzo de la ejecución  $r$ . Llamaremos  $\Pi(r)$  al conjunto de todas las posiciones de  $r$ .

Una ejecución  $r \in R_G$  es *divergente* si para cada  $t \in \mathcal{T}^+$  existe una posición  $\pi$  de  $r$  tal que  $\delta_r(\pi) > t$ . Las ejecuciones divergentes son aquellas en las cuales el tiempo avanza más allá de cualquier límite (diverge); en la literatura son denominadas “*non-Zeno*” [Alu91].  $\Delta_G$  denota al conjunto de las secuencias de ejecución *divergentes* de  $G$  y  $\Delta_G(q_0)$  a las que poseen comienzo  $q_0$ . Nosotros estamos interesados, al igual que los trabajos previos, en sistemas de tiempo real –grafos temporizados– en los cuales todo prefijo finito de una ejecución en  $R_G$  es prefijo de una secuencia en  $\Delta_G$ . Llamaremos a los mismos *sistemas bien temporizados*. El comportamiento de los sistemas bien temporizados –cada traza de ejecución– puede ser generado, tal como se describió al comienzo, transición a transición, comenzando en un estado inicial y repetidamente eligiendo entre incrementar el tiempo (mientras no se violen las condiciones invariantes) y hacer una transición discreta (si ésta está habilitada). En estos sistemas todas las trazas de ejecución deben ser necesariamente secuencias *infinitas*. Sin embargo, esta no es una condición suficiente para asegurar *non-Zeno* (por ejemplo, un sistema cuyas trazas de ejecución son todas secuencias infinitas que repiten siempre el mismo estado, con transiciones temporales nulas, o que alternan consecutivamente en forma cíclica uno o más estados a través de transiciones discretas, no cumple *non-Zeno*).

## 2.2 Composición Paralela de Grafos Temporizados

Para facilitar la descripción modular de los sistemas se utiliza la *composición paralela* de grafos temporizados. La composición paralela de dos grafos temporizados es el producto



de ambos donde las transiciones que comparten etiquetas deben *sincronizar*, es decir, las acciones correspondientes tienen que ejecutarse simultáneamente. Por cada par de dichas transiciones el sistema global tendrá una única transición tal que la etiqueta es la misma, la condición es la conjunción de las condiciones y el conjunto de relojes a resetear es la unión de los conjuntos correspondientes.

### 2.2.1 Definición de Composición

La composición paralela de dos grafos temporizados  $G_1$  y  $G_2$ , sincronizando las etiquetas de  $\Lambda \subseteq A$  –comunes a  $G_1$  y  $G_2$ –, es notada  $G_1[[\Lambda]]G_2$  y se define como sigue. Sean  $G_1 = \langle L_1, X_1, E_1, l_1^0, I_1 \rangle$  y  $G_2 = \langle L_2, X_2, E_2, l_2^0, I_2 \rangle$  tales que  $X_1 \cap X_2 = \emptyset$ ,  $G_1[[\Lambda]]G_2$  es el grafo  $G = \langle L, X, E, l^0, I \rangle$ , donde:

- $X = X_1 \cup X_2$
- $L \subseteq L_1 \times L_2$
- $\langle \langle l_1, l_2 \rangle, \alpha, \psi_X, \rho_X, \langle l_1', l_2' \rangle \rangle \in E$  si y sólo si:
  1.  $\langle l_1, \alpha, \psi_X, \rho_X, l_1' \rangle \in E_1 \wedge \alpha \notin \Lambda \wedge l_2 = l_2'$
  2.  $\langle l_2, \alpha, \psi_X, \rho_X, l_2' \rangle \in E_2 \wedge \alpha \notin \Lambda \wedge l_1 = l_1'$
  3.  $\langle l_i, \alpha, \psi_{iX}, \rho_{iX}, l_i' \rangle \in E_i \wedge \alpha \in \Lambda \wedge \psi_X = (\psi_{1X} \wedge \psi_{2X}) \wedge \rho_X = (\rho_{1X} \cup \rho_{2X})$
- $I(\langle l_1, l_2 \rangle) = I_1(l_1) \wedge I_2(l_2)$
- $l^0 = \langle l_1^0, l_2^0 \rangle$

### 2.2.2 Semántica

El comportamiento del grafo  $G = G_1[[\Lambda]]G_2$  está ligado a los comportamientos de  $G_1$  y  $G_2$ . Sean  $T_1 = \langle Q_1, \rightarrow_1 \rangle$  y  $T_2 = \langle Q_2, \rightarrow_2 \rangle$  modelos de  $G_1$  y  $G_2$ , respectivamente. El modelo de  $G$  es  $\langle Q_1 \times Q_2, \rightarrow \rangle$ , donde  $\rightarrow$  es la relación más pequeña que satisface las reglas que se enuncian a continuación.

- *Transiciones temporales.* La evolución temporal del sistema compuesto en un estado está condicionada a la de cada componente. Si cada componente permite el paso de un tiempo  $t$ , el sistema compuesto puede entonces avanzar  $t$  unidades. Esto determina que los relojes del sistema compuesto crecen uniformemente con el tiempo. Formalmente,

$$\frac{q_1 \xrightarrow{t} q_1' \quad q_2 \xrightarrow{t} q_2'}{\langle q_1, q_2 \rangle \xrightarrow{t} \langle q_1', q_2' \rangle}$$

• *Transiciones discretas (instantáneas)*. En este caso existen dos posibilidades:

1. Si desde cada componente de un estado compuesto  $q$  hay una transición etiquetada con  $\alpha$  entonces hay una transición con  $\alpha$  desde  $q$  al estado formado por los estados destinos de cada componente. Formalmente,

$$\frac{q_1 \xrightarrow{\alpha} {}_1 q_1' \quad q_2 \xrightarrow{\alpha} {}_2 q_2'}{\langle q_1, q_2 \rangle \xrightarrow{\alpha} \langle q_1', q_2' \rangle}$$

2. Si desde uno de los estados componentes hay una transición etiquetada con  $\alpha$  y  $\alpha$  no es de sincronización ( $\alpha \notin \Lambda$ ), entonces hay una transición discreta con  $\alpha$  en el sistema compuesto que permite avanzar sólo este componente. Formalmente,

$$\frac{q_1 \xrightarrow{\alpha} {}_1 q_1' \quad \alpha \notin \Lambda}{\langle q_1, q_2 \rangle \xrightarrow{\alpha} \langle q_1', q_2 \rangle} \quad \text{y} \quad \frac{q_2 \xrightarrow{\alpha} {}_2 q_2' \quad \alpha \notin \Lambda}{\langle q_1, q_2 \rangle \xrightarrow{\alpha} \langle q_1, q_2' \rangle}$$

### 2.3 Lógica TCTL: “Timed Computation Tree Logic”

Muchas propiedades importantes de los sistemas encuentran una expresión natural en lógica temporal [Pnu81]. La lógica temporal de tiempo real TCTL (“timed computation tree logic”) [ACD90, Alu91, HNS<sup>+</sup>92] extiende los operadores temporales  $\exists\mu$  (*existe una ejecución*) y  $\forall\mu$  (*para todas las ejecuciones*) de CTL (“computation tree logic”) [EC82, CES86] con restricciones temporales que permiten un razonamiento “cuantitativo” del tiempo. Si bien CTL es una lógica temporal adecuada para sistemas reactivos, ésta permite razonamiento “cualitativo” del tiempo basado en la noción de *secuencialidad* en las ejecuciones, pero no es posible expresar en ella restricciones temporales cuantitativas. En CTL pueden expresarse propiedades tales como “inevitablemente sucederá el evento  $e$ ” ó “la propiedad  $p$  se satisface continuamente en todas las ejecuciones del sistema”. Las fórmulas de TCTL permiten expresar, además, propiedades tales como “inevitablemente antes de un tiempo  $t$  sucederá el evento  $e$ ” ó “la propiedad  $p$  se satisface continuamente entre los tiempos  $t_i$  y  $t_f$  para toda ejecución del sistema”.

Las fórmulas de TCTL son interpretadas sobre los estados de un sistema de tiempo real y se definen a partir de un conjunto de predicados básicos (proposiciones atómicas) sobre los estados. El conjunto  $P$  de predicados sobre los estados de un grafo temporizado se define en [Oli94] como sigue,

$$p := @ = l \mid x_i \prec c \mid x_i - x_j \prec d$$

donde  $l \in L$ ,  $x_i, x_j \in X$ ,  $c \in \mathcal{L}$ ,  $d \in \mathcal{Q}$  y  $\prec \in \{<, \leq, =, \geq, >\}$ . Adicionalmente suelen considerarse los siguientes predicados básicos: *init*, *enable(e)* y *after(e)* [Oli94]. Informalmente, *init* define el estado inicial, *enable(e)* el conjunto de los estados que

tienen una transición habilitada etiquetada con  $e$  y,  $after(e)$  el conjunto de los estados que son alcanzados por una transición etiquetada con  $e$ . Asimismo,  $@ = l$  define al conjunto de los estados cuya locación es  $l$ . La semántica formal será descrita en la próxima sección.

Las fórmulas de TCTL se definen por la siguiente gramática:

$$\varphi := p \mid \neg\varphi_1 \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \exists \mu_I \varphi_2 \mid \varphi_1 \forall \mu_I \varphi_2$$

donde  $p \in P$  e  $I$  es un intervalo con extremos enteros positivos ( $I$  puede ser abierto o cerrado, acotado o no acotado).

Intuitivamente,  $\varphi_1 \exists \mu_I \varphi_2$  significa que existe una ejecución (divergente) del sistema tal que  $\varphi_2$  se cumple en un estado de la misma, en un tiempo  $t$  dentro del intervalo  $I$  y  $\varphi_1$  se satisface continuamente en los estados previos.  $\varphi_1 \forall \mu_I \varphi_2$  expresa que para todas las ejecuciones la propiedad anterior se cumple.

### 2.3.1 Semántica de TCTL

TCTL es una lógica que considera tiempo *ramificado* y es interpretada sobre una estructura arbórea de estados. Cada árbol representa un sistema reactivo, cuyas posibles secuencias de ejecución corresponden a caminos en el árbol, generados desde la raíz.

**Definición 2.3.** Para un sistema de transiciones etiquetado  $T = \langle Q, \rightarrow \rangle$  correspondiente a un grafo temporizado  $G$ , un estado  $q = \langle l, v \rangle \in Q$  y una fórmula  $\varphi$  de TCTL, la relación de satisfactibilidad  $q \models \varphi$  es definida por inducción en  $\varphi$ , de la siguiente manera [ACD90, Oli94]:

$$q \models @ = l \text{ si y solamente si, } Loc(q) = l$$

$$q \models x_i < c \text{ si y solamente si, } v(x_i) < c$$

$$q \models x_i - x_j < d \text{ si y solamente si, } v(x_i) - v(x_j) < d$$

$$q \models \neg\varphi \text{ si y solamente si, } q \not\models \varphi$$

$$q \models \varphi_1 \wedge \varphi_2 \text{ si y solamente si, } q \models \varphi_1 \text{ y } q \models \varphi_2$$

$$q \models \varphi_1 \exists \mu_I \varphi_2 \text{ si y solamente si, } \exists r \in \Delta_G(q). \exists \pi \in \Pi(r). \sigma_r(\pi) \models \varphi_2 \wedge \delta_r(\pi) \in I \wedge \forall \pi' \prec \pi. \sigma_r(\pi') \models \varphi_1$$

$$q \models \varphi_1 \forall \mu_I \varphi_2 \text{ si y solamente si, } \forall r \in \Delta_G(q). \exists \pi \in \Pi(r). \sigma_r(\pi) \models \varphi_2 \wedge \delta_r(\pi) \in I \wedge \forall \pi' \prec \pi. \sigma_r(\pi') \models \varphi_1$$

donde, la relación  $\prec$  entre posiciones de una ejecución se define como el orden lexicográfico de los pares  $\langle i, t \rangle \prec \langle i', t' \rangle$  si y solamente si:  $i < i'$  ó,  $i = i'$  y  $t < t'$ .

El conjunto de estados que satisface una fórmula  $\varphi$  es  $[[\varphi]]$ , el *conjunto característico* de  $\varphi$ .

### 2.3.2 Algunas Abreviaturas

- Escribiremos  $\exists\mu$  y  $\forall\mu$  para  $I=[0, \infty)$ ;  $\exists\mu_{\leq c}$  por  $\exists\mu_{[0,c]}$  y  $\forall\mu_{\leq c}$  por  $\forall\mu_{[0,c]}$ .
- $\exists\Diamond_I\varphi$  (*posible  $\varphi$* ) en lugar de  $true\exists\mu_I\varphi_2$ .
- $\forall\Diamond_I\varphi$  (*inevitable  $\varphi$* ) en lugar de  $true\forall\mu_I\varphi_2$ .
- $\exists\Box_I\varphi$  en lugar de  $\neg\forall\Diamond_I\neg\varphi$ .
- $\forall\Box_I\varphi$  (*siempre  $\varphi$* ) en lugar de  $\neg\exists\Diamond_I\neg\varphi$ .

De acuerdo a las abreviaturas dadas,  $\exists\Diamond_I\varphi$  es satisfecha por el conjunto de estados desde los cuales es posible alcanzar un estado que verifica la fórmula  $\varphi$ , dentro del intervalo  $I$ . De esta manera se especifican los problemas de *alcanzabilidad acotada*.  $\forall\Diamond_I\varphi$  establece que  $\varphi$  es *inevitable*. Un estado  $q$  satisface esta fórmula si, y solamente si, a partir de toda ejecución con estado inicial  $q$  existe un estado, que dentro del intervalo  $I$ , satisface  $\varphi$ . La fórmula  $\forall\Diamond_{\leq c}\varphi$  expresa la propiedad de tiempo real de respuesta en tiempo acotado, en la cual un evento debe ocurrir antes de un cierto tiempo acotado  $c$ .  $\forall\Box_I\varphi$  especifica que  $\varphi$  es un *invariante*. Esto es, un estado  $q$  satisface  $\forall\Box_I\varphi$  si, y solamente si, toda ejecución con comienzo en  $q$  satisface continuamente  $\varphi$ , dentro del intervalo  $I$ . Finalmente,  $\exists\Box_I\varphi$  caracteriza al conjunto de estados a partir de los cuales existe una ejecución que satisface continuamente  $\varphi$ , dentro del intervalo  $I$ .

## 2.4 Verificación de Modelos: Grafos Temporizados y TCTL

Dado un grafo temporizado  $G$ , que describe un sistema de tiempo real  $T$  (un sistema de transiciones etiquetado), y una fórmula  $\varphi$  de TCTL, que especifica un requerimiento, el problema de decidir, algorítmicamente, si  $T$  *satisface*  $\varphi$  es una instancia del problema de *verificación de modelos* (“*model-checking problem*”). Para esta instancia el problema fue solucionado por Alur, Courcoubetis y Dill [ACD90]. Su solución está basada en la construcción explícita, a partir del grafo de transiciones de estados  $T$  *infinito*, de un grafo cociente finito, llamado *grafo de regiones* (“*region graph*”). Las regiones están determinadas por una relación de equivalencia sobre el conjunto  $X$  –de los relojes de un grafo– que unifica configuraciones de los relojes desde las cuales los comportamientos futuros son esencialmente idénticos. Es decir, dos relojes  $x_1$  y  $x_2$  son equivalentes si las mismas secuencias de transiciones discretas son posibles desde  $x_1$  y  $x_2$ .

La construcción del grafo de regiones conduce a un algoritmo de verificación de modelos que es exponencial en el número de relojes de entrada y en el tamaño de la más grande constante de  $G$ . Sin embargo, en la práctica es a menudo innecesario construir el

grafo de regiones entero. Puede representarse únicamente el conjunto de estados requerido para solucionar un problema específico (para una sentencia  $\varphi$  dada) y pueden representarse simbólicamente conjuntos de estados como predicados de estados. En otras palabras, en lugar de enumerar todas las regiones, un algoritmo de verificación de modelos *simbólico* (“*symbolic model-checking algorithm*”) computa las regiones selectivamente y simbólicamente. El algoritmo propuesto en [HNS<sup>+</sup>92] usa transformadores de predicados para computar el conjunto de *sucesores* –análisis hacia adelante (“*forward analysis*”)– o *predecesores* –análisis hacia atrás (“*backward analysis*”)– de conjuntos de estados. El conjunto característico  $[[\varphi]]$  de una fórmula  $\varphi$  es computado como un punto fijo definido en términos de los transformadores de predicados. Una explicación detallada del método de verificación de modelos simbólico puede encontrarse en [HNS<sup>+</sup>92, ACH<sup>+</sup>95]. Otros algoritmos son descriptos, por ejemplo, en [LL95, SS95, HKV96].

## 2.5 Discretización del Tiempo

### 2.5.1 Tiempo Continuo versus Tiempo Discreto

El *tiempo continuo* es generalmente representado usando números reales o racionales. Estos proveen todas las posibilidades de una matemática rica que generalmente es necesaria para tratar muchas clases de problemas. Los reales tienen dos propiedades principales que lo diferencian de los enteros y los racionales: la *densidad* y la *completitud*. La propiedad de densidad establece que entre dos puntos de tiempo cualesquiera existe siempre otro; la propiedad de completitud, que si una serie de puntos está acotada superiormente entonces existe un punto que es la mínima cota superior de la serie. La densidad distingue a los reales y los racionales de los enteros, la completitud distingue a los reales de los otros.

La principal ventaja de esta representación es que los reales (y los racionales) son los números generalmente usados en física para representar el tiempo. De esta manera es más fácil basar teorías sobre leyes físicas y representar cambio continuo. Asimismo, los reales (y los racionales) son un superconjunto de los enteros, por lo que son más generales y apropiados que estos últimos para representar tiempo, aunque poseen también algunas desventajas. Es difícil hacer teorías basados en los reales, debido en parte a la propiedad de densidad, la cual introduce el concepto de “infinito” aún en un intervalo acotado. Otra desventaja es en cuanto a su representación, especialmente en computadoras; la manera usual de representarlos es por medio de números de punto flotante, que son sólo una aproximación. Luego, surgen problemas, por ejemplo, para determinar si dos números son iguales o no (ellos pueden ser diferentes aproximaciones del mismo número).

El *tiempo discreto* es generalmente representado usando números enteros y más precisamente, naturales. La principal ventaja de esta representación es que una teoría

basada en enteros es más fácil de formular y de usar. Asimismo, los enteros tienen una representación directa y exacta en las computadoras, no es necesario trabajar con aproximaciones. La principal desventaja de los enteros es debida a su falta de expresividad, especialmente cuando deseamos representar cambio continuo. Por ejemplo, con enteros no es posible representar la solución de un sistema de ecuaciones si la misma es fraccional. Sin embargo, existen varios enfoques que permiten representar cambio continuo (es decir, funciones continuas) usando tiempo discreto. Por ejemplo, enfoques basados en los conceptos de “errores” y “granularidad” [Hob85, BB94, Euz95, BM97].

### 2.5.2 Un Modelo de Tiempo Discreto

En este trabajo estamos interesados en el análisis de sistemas de tiempo real para un dominio temporal discreto y particularmente en el marco de *grafos temporizados*. Numerosos trabajos previos consideran modelos de tiempo discreto que usan a los números naturales para modelar el tiempo [EMS<sup>+</sup>89, Ost87, Bur89, AH92, PL92, HMP92, AH93, AH94]. Este modelo es apropiado para, por ejemplo, ciertas clases de circuitos digitales sincrónicos, donde los eventos ocurren a valores exactos de incremento del tiempo de un reloj global.

En los casos en que ello no ocurre, el enfoque puede resultar igualmente válido y requiere que el tiempo continuo sea aproximado por la elección de una determinada *granularidad*: la unidad temporal más pequeña referenciable en el sistema. La idea es que la elección de una granularidad pequeña resulta suficiente para verificar ciertas propiedades donde valores temporales menores son indistinguibles para el proceso de verificación [EMS<sup>+</sup>89, ACD90].

En el enfoque de *relojes ficticios* las transiciones (los eventos) pueden ocurrir en tiempo continuo pero son registradas por un reloj global, en tiempo discreto. En este modelo se introduce generalmente una transición especial *tick* y el tiempo incrementa una unidad con cada *tick* (ver, por ejemplo, [Ost87, Bur89, HMP92, AH93, AH94]). Con la semántica de relojes ficticios, si varios eventos ocurren entre dos instantes consecutivos de tiempo (entre dos *ticks*) ellos pueden ser distinguidos solamente por el ordenamiento temporal, no por el valor real del tiempo.

Para los grafos temporizados hay una semántica alternativa basada en tiempo discreto (tomando valores en  $\mathbb{Z}$ ), la cual ha sido discutida en trabajos previos (ver, por ejemplo, [AH92]). De acuerdo a esta visión, los pasos temporales son múltiplos de una constante (*ticks* de un reloj global), y a cada instante el autómata puede elegir entre incrementar el tiempo o hacer alguna transición discreta. Consideremos el fragmento de un autómata temporizado con 2 relojes, de la figura 2.1(a). El autómata puede permanecer en el estado dejando pasar el tiempo (es decir, los valores de  $x_1$  y  $x_2$  aumentan simultáneamente) mientras  $x_1 \leq u$ . Asimismo, cuando  $x_1$  alcanza un valor  $k$  (asumiendo que  $k \leq u$ ) el autómata puede tomar una transición a otro estado y resetear  $x_1$  a cero. Restringiendo el dominio del tiempo a  $\mathbb{Z}$ , las condiciones de permanencia en cada estado (los *invariantes* de las

locaciones) pueden ser reemplazadas –interpretadas– por transiciones *tick* como se muestra en la figura 2.1(b).

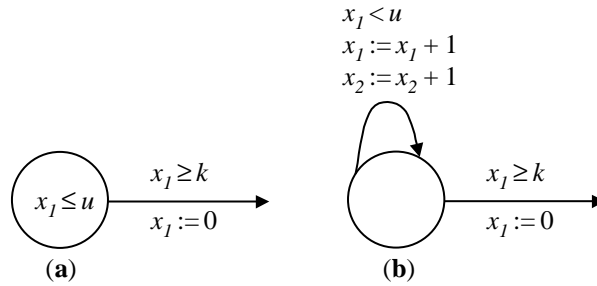


Fig. 2.1: Un autómata temporizado y su interpretación en tiempo discreto

Bajo esta interpretación los relojes son simplemente variables enteras no negativas acotadas, cuyos valores son incrementados simultáneamente por transiciones temporales y algunas de ellas reseteadas a cero por transiciones discretas. En particular, cualquier esquema de representación para una semántica densa, basada en desigualdades de relojes, puede ser especializado para una semántica discreta [BMT99]. Dado que, sobre un orden discreto, cualquier desigualdad de la forma  $x_i < c$  puede ser escrita como la desigualdad no estricta  $x_i \leq c-1$ , las *regiones* discretas pueden ser expresadas usando exclusivamente desigualdades no estrictas. Esta observación que ha sido aprovechada para mejorar la eficiencia de algoritmos de verificación modelos (ver, por ejemplo, [BMT99]), es considerada con particular interés en el presente trabajo ya que permite resaltar que con una discretización del tiempo “no mucho se pierde” [HMP92, GPV94, HK97, AMP98, BMT99]. En particular, [GPV94] construye dos discretizaciones de autómatas temporizados las cuales generan los mismos lenguajes “no temporizados” que sus versiones densas y satisfacen el mismo conjunto de propiedades TCTL.

Con una discretización, una *ejecución discreta* puede ser una ligera variación de algunas de las *ejecuciones densas* que ella representa, donde algunas transiciones tienen que tomarse simultáneamente mientras que en una ejecución densa las transiciones son separadas por una pequeña cantidad de tiempo. En el caso de estudio que abordaremos en el capítulo 4, las propiedades que son verificadas sobre un dominio discreto valen para el dominio denso de los reales o los racionales, según los resultados establecidos en [HMP92, AMP98, BMT99].

### 2.5.3 Interpretación Algorítmica de Grafos Temporizados

Dado un grafo temporizado  $G = \langle L, X = \{x_1, \dots, x_n\}, E, l^0, I \rangle$  y su sistema de transiciones etiquetado  $T = \langle Q, \rightarrow \rangle$ , una interpretación algorítmica del sistema en un dominio temporal discreto puede concebirse como un “loop” –sin cota de terminación– con inicialización,

en un lenguaje imperativo tipo *Small* [Gri81]. Las transiciones temporales y discretas son interpretadas por comandos guardados de un ciclo *Do*. Las guardas no son necesariamente disjuntas y se asume una elección *no determinista* de las mismas en la ejecución –el *Do* es *no determinístico*. El algoritmo tiene como precondition: el estado inicial del sistema es *válido* (satisface el invariante de la locación inicial). La figura 2.2 describe la interpretación algorítmica del grafo  $G$ .

---

```

stateG: L; // tipo de la variable estado del programa
stateG := l0; // inicialización del estado
x1 := 0; ...; xn := 0 // inicialización de los relojes

{ precondition: Il0(x1, ..., xn) = true } // precondition: el estado inicial es válido

Do // ciclo Do
  □ ψl(x1, ..., xn) ∧ stateG = ll ∧ Ill((updateX(x1, ρl), ..., updateX(xn, ρl)))
    ↦αl stateG := ll';
    x1 := updateX(x1, ρl); ...; xn := updateX(xn, ρl)

  .....

  □ ψm(x1, ..., xn) ∧ stateG = lm ∧ Ilm((updateX(x1, ρm), ..., updateX(xn, ρm)))
    ↦αm stateG := lm';
    x1 := updateX(x1, ρm); ...; xn := updateX(xn, ρm)

  □ IstateG(x1 + δ, ..., xn + δ) ↦tick x1 := x1 + δ; ...; xn := xn + δ

```

---

**EndDo**

Fig. 2.2: Interpretación algorítmica de un grafo temporizado

Cada uno de los  $m$  primeros comandos guardados rotulados con etiquetas  $\alpha_i \in \Lambda$  (con  $\Lambda$  el conjunto de etiquetas del sistema) corresponde a una transición  $\langle l_i, \alpha_i, \psi_i, \rho_i, l_i' \rangle \in E$ ; donde,  $\text{update}_X(x_j, \rho_i) = 0$ , si  $x_j \in \rho_i$  y  $\text{update}_X(x_j, \rho_i) = x_j$ , en caso contrario (cada rótulo  $\alpha_i$  sería interpretado como una sentencia que inspecciona la ocurrencia del evento  $\alpha_i$ ). El último comando guardado representa un *tick* del *reloj global* que se refleja en el incremento de cada reloj de  $X$  con  $\delta$ , el valor de granularidad elegido para el sistema. Un valor de  $\delta = 1/M$ , con  $M > |X|$  resulta suficiente para asegurar que cada desigualdad de la forma  $0 < x_1 < \dots < x_n < 1$  tiene al menos una asignación posible (una solución,  $x_j = j \cdot \delta$ ). De esta manera aseguramos que todo estado posible del sistema tiene al menos un representante, un elemento en cada clase de equivalencia del grafo de regiones que caracteriza al sistema. Elegir a  $\delta = 1/M$  es equivalente a asumir a  $\mathcal{Z}$  como dominio



temporal y multiplicar la escala del problema, es decir las constantes, por  $M$  –tanto en el grafo como en las propiedades a verificar. Esto permite trabajar con la aritmética de  $\mathcal{Z}$ .

Las primitivas básicas consideradas de los relojes son 4: de *inicialización*, *reseteo*, *incremento* e *inspección (consulta)*. Las primeras dos corresponden a una asignación con cero, el incremento es con  $\delta$  y la inspección de un reloj es su valor.

Una versión equivalente a la anterior que hace explícita la utilización de un único *reloj global* se obtiene con ligeras variaciones. Se incorpora un reloj global *clock* al ambiente e inicializa cada reloj  $x_j$  del sistema representado por el grafo  $G$  con el valor de *clock*. Las condiciones  $\psi_i(x_1, \dots, x_n)$  e  $I_{loc}(vx_1, \dots, vx_n)$  del cuerpo del *Do* son reemplazadas por  $\psi_i(\text{clock} - x_1, \dots, \text{clock} - x_n)$  e  $I_{loc}(\text{clock} - vx_1, \dots, \text{clock} - vx_n)$ .  $\text{update}_x(x_j, \rho_i)$  se redefine como  $\text{update}_x(x_j, \rho_i) = \text{clock}$ , si  $x_j \in \rho_i$  y  $\text{update}_x(x_j, \rho_i) = x_j$ , en caso contrario. El último comando guardado (*tick*) sólo incrementa el reloj global *clock* con  $\delta$  (los  $x_j$  no son modificados). Esta versión resalta la existencia de un único reloj –el reloj del sistema– que regula el paso del tiempo y que no es reseteado nunca. Cada  $x_j$  es en realidad un cronómetro que mide el tiempo transcurrido desde la última vez que fue reseteado. Consecuentemente, las cuatro primitivas básicas de los relojes  $x_j$  del sistema se definen para esta versión como sigue. Las primitivas de inicialización y reseteo corresponden a la asignación  $x_j := \text{clock}$ ; el incremento es implícito para cada  $x_j$  (sólo se incrementa explícitamente el reloj global *clock*); y, la *inspección* del reloj  $x_j$  es el valor  $\text{clock} - x_j$ .

Cada ejecución de un programa *Do* es una traza de ejecución válida del grafo  $G$ , a partir de  $T$ , y el conjunto de todas las ejecuciones es capturado por el *no-determinismo* del programa.

La *composición paralela* de dos programas *Do* –como el de la figura 2.2– es un programa *Do* que compone las acciones de inicialización de cada componente y donde cada comando guardado resulta de la composición de las transiciones correspondientes. Esto es, si  $\alpha_i$  es de sincronización entonces se genera un comando guardado que compone con conjunción las guardas y con “;” los comandos. Para cada  $\alpha_i$  que no es de sincronización, el comando guardado del *Do* componente se incluye en el *Do* de la composición. Los comandos guardados de incremento temporal (*tick*) reciben el mismo tratamiento que las transiciones con etiquetas de sincronización, ya que un paso temporal es el mismo en cada componente.

Verificar que un predicado  $P$  es un invariante de un programa *Do* corresponde a probar las siguientes dos condiciones:

- $\text{Init} \Rightarrow P$
- $P \wedge B_k \Rightarrow \text{wp}(S_k, P)$ , para todo comando  $B_k \mapsto_{\text{lab}} S_k$ , con  $\text{lab} \in A \cup \{\text{tick}\}$

donde *Init* es el predicado que caracteriza al estado inicial y *wp* (weakest precondition) es el transformador de predicados propuesto por Dijkstra en [Dij79]. En el cálculo *wp*, un programa  $S$  termina en un estado verificando un predicado  $q$ , cuando la ejecución es comenzada en un estado que satisface el predicado  $\text{wp}(S, q)$ . Cabe notar que si se

demuestra que  $P$  es un invariante, para cualquier elección del no-determinismo,  $P$  vale continuamente.

Existen extensiones recientes del cálculo  $wp$  que definen nuevos transformadores de predicados para trabajar, en el contexto de programas concurrentes, con propiedades de seguridad y estabilidad de propiedades en un proceso *-safety-*, la invarianza de predicados en las computaciones *-to-always-* y propiedades de progreso *-progress-*, tales como la *alcanzabilidad* de un estado (predicado) desde otro *-leads-to-*. Algunos de estos trabajos son: [JKR89, Kna90, Lam90, ChS95, DS97]. Las áreas de aplicación consideradas en la práctica hasta el momento se restringen al análisis de flujo de datos no determinístico en redes, sistemas tolerantes a fallas y protocolos simples de comunicación [DS97]. Sin embargo, la considerable complejidad del enfoque en las extensiones, el escaso estado de desarrollo, la indisponibilidad de herramientas computacionales de asistencia y la falta de consideraciones de nociones temporales, hacen que este enfoque sea, por un lado, insatisfactorio para la especificación de sistemas con requerimientos temporales y por el otro, una promisoría dirección para la realización de nuevos trabajos de investigación.

# Capítulo 3

## *Formalización de Grafos Temporizados y TCTL en Coq*

---

En este capítulo formalizamos en *Coq grafos temporizados* y la lógica *TCTL*. Incluimos además operadores de la lógica *CTL* (“computation tree logic”) [CES86] y algunas definiciones alternativas para los operadores que permiten expresar *invarianza* y *alcanzabilidad*, con tipos *inductivos* (bajo la noción de estados alcanzables) y *co-inductivos* (bajo la noción de trazas –infinitas– de ejecución). Las formalizaciones introducidas serán utilizadas en el próximo capítulo en el análisis de un caso de estudio y en el capítulo 5, en descripciones *genéricas* de grafos temporizados.

### 3.1 Nociones Temporales

En nuestra formalización asumiremos a  $\mathbb{Z}$  como dominio temporal discreto. Este corresponde al tipo inductivo `nat` de *Coq*. A continuación introducimos algunas definiciones básicas en una sección *Coq*.

```
Section Time_Clocks.

  Definition Instant := nat.
  Definition Clock := nat.

  Definition lt_Ck := lt.
  Definition le_Ck := le.
  Definition gt_Ck := gt.
  Definition ge_Ck := ge.
  Definition eq_Ck := [x,y:Clock] x=y.

  Definition Ini_Ck := 0.
  Definition tick : Instant := (1).
  Definition plus_Ck := plus.
  Definition Inc := [x:Clock] (plus_Ck x tick).
```

```

Definition Reset      := 0.
Definition time0     := 0.

End Time_Clocks.

```

Instant y Clock corresponden al tipo de los valores temporales y las valuaciones de los relojes; lt\_Ck (<), le\_Ck (≤), gt\_Ck (>), ge\_Ck (≥) y eq\_Ck (=) son las relaciones binarias habituales sobre  $\mathcal{L}$ ; Ini\_Ck es el valor inicial de los relojes; tick es la *granularidad* del sistema (la más pequeña unidad temporal referenciable); plus\_Ck es la suma de nat; Inc es la operación que incrementa un tick (es una función que recibe un objeto  $x$  de tipo Clock y retorna su suma con tick) y, Reset y time0 corresponden al valor de reseteo de los relojes y el tiempo inicial del sistema, respectivamente.

**Nota 3.1.** En las formalizaciones en *Coq* de este capítulo y del resto del trabajo obviaremos los argumentos en las aplicaciones que pueden ser automáticamente inferidos por el sistema. Esto se consigue en *Coq* inicializando el desarrollo con el comando `Implicit Arguments On` [Bar<sup>+</sup>99].

## 3.2 Definiciones Elementales de Grafos Temporizados

Sea  $G = \langle Loc = \{loc_0, \dots, loc_n\}, X, Trans, loc_0, Inv \rangle$  un grafo temporizado. En la formalización de los sistemas asumiremos un conjunto global Label de etiquetas en vez de conjuntos particulares para cada grafo  $G$ , de acuerdo a lo expresado en el capítulo 2 (definición 2.1). El conjunto Label puede definirse por un tipo inductivo de la siguiente manera:

```

Inductive Label : Set := Lab1 : Label | ... | Labm : Label
  | Tick : Label.

```

Lab<sub>1</sub>, ..., Lab<sub>m</sub> y Tick son los constructores del tipo Label. Lab<sub>1</sub>, ..., Lab<sub>m</sub> representan las etiquetas que corresponden a las transiciones discretas; Tick es una etiqueta distinguida que caracteriza a las transiciones temporales.

Las *locaciones* del grafo temporizado  $G$  pueden especificarse también como un tipo enumerado,

```

Inductive Loc : Set := Loc0 : Loc | ... | Locn : Loc.

```

El estado del sistema, en un instante dado, está determinado por una locación de Loc y una tupla de valores de tipo Clock (la cantidad de componentes de esta tupla dependerá en cada caso del sistema concreto que se esté analizando). Asumiremos que Clocks representa el tipo de dicha tupla (correspondiente al conjunto  $X$ ); InicAll es la tupla de

relojes inicializados (todos puestos en cero); e, `IncAll` es la función que incrementa todos los relojes de  $X$  con la función `Inc` (formalizada en la sección 3.1).

```
Definition State := Loc * Clocks.
```

```
Definition st_ini : State := (Loc0, IncAll).
```

`st_ini` es el estado inicial del sistema, compuesto por la locación inicial y la tupla de relojes inicializados.

**Notación.** La cuantificación universal sobre un tipo  $S$  se escribe en *Coq* “ $(x:S) P$ ”. Sin embargo, usaremos la notación “ $\forall x \in S P$ ” en este trabajo para dar más claridad a las especificaciones.

Los *invariantes* de las locaciones del grafo pueden ser definidos por predicados sobre los estados, bajo el siguiente patrón

```
Inductive Inv : State -> Prop :=
  | ILoc0 :  $\forall x \in \text{Clocks} \text{ (Icond}_1 \text{ x) } \rightarrow \text{(Inv (Loc}_0 \text{, x))}$ 
  ...
  | ILocn :  $\forall x \in \text{Clocks} \text{ (Icond}_n \text{ x) } \rightarrow \text{(Inv (Loc}_n \text{, x))}$ .
```

$\text{Icond}_i$  es el predicado de permanencia en la locación  $\text{Loc}_i$ , para  $0 \leq i \leq n$ . El constructor  $\text{ILoc}_i$  construye pruebas del invariante en la locación  $\text{Loc}_i$ , para los valores de los relojes que cumplen  $\text{Icond}_i$ . Esto es, dado un objeto  $x$  de tipo `Clocks` y una prueba  $H$  de  $(\text{Icond}_i \text{ x})$ ,  $(\text{ILoc}_i \text{ x H})$  es una prueba de  $(\text{Inv (Loc}_i \text{, x)})$ .

**Nota 3.2.** Asumiremos de aquí en adelante en este trabajo que el predicado que describe a los invariantes de las locaciones  $\text{Inv}$  de un sistema  $G$  se satisface para el estado inicial `st_ini` de  $G$  (esto es, `st_ini` es un estado *válido* de  $G$ ).

Las transiciones discretas y temporales pueden ser definidas como relaciones entre estados y etiquetas. En *Coq*, usando `Inductive`, de la siguiente manera:

```
Inductive Trans : State -> Label -> State -> Prop :=
  | trans1 :  $\forall x \in \text{Clocks} \text{ (Tcond}_1 \text{ x) } \rightarrow \text{(Inv (Loc}_j \text{, new\_x}_1)) \rightarrow$ 
    (Trans (Loci, x) Labk (Locj, new_x1))
  ...
  | transp :  $\forall x \in \text{Clocks} \text{ (Tcond}_p \text{ x) } \rightarrow \text{(Inv (Loc}_j \text{, new\_x}_p)) \rightarrow$ 
    (Trans (Loci, x) Labk (Locj, new_xp))
  | tTick :  $\forall x \in \text{Clocks} \forall l \in \text{Loc} \text{ (Inv (l, (IncAll x))) } \rightarrow$ 
    (Trans (l, x) Tick (l, (IncAll x)))
```

$Tcond_1, \dots, Tcond_p$  son los predicados asociados a cada una de las  $p$  transiciones del grafo;  $new\_x_i$  es la tupla de `Clocks` donde cada reloj conserva su valor de  $x$  o es reseteado a cero, con la constante `Reset`;  $trans_1, \dots, trans_p$  corresponden a transiciones discretas (del conjunto  $Trans$  de  $G$ ) y  $tTick$  al conjunto de transiciones temporales –una por locación.

$trans_i$  (para  $1 \leq i \leq p$ ) construye pruebas de transiciones de una locación  $Loc_i$  a otra  $Loc_j$  por una etiqueta  $Lab_k$ , para los valores de los relojes que satisfacen  $Tcond_i$  e  $(Inv(Loc_j, new\_x_i))$ ;  $tTick$  construye pruebas de transiciones de una locación a ella misma, incrementando el valor de los relojes en un *tick* con `IncAll`, siempre que se cumple el predicado `Inv` para los nuevos valores de los relojes en la misma locación.

### Observaciones

- Al asumir un conjunto global `Label` de etiquetas simplificamos las formalizaciones, reduciendo también el tamaño de las pruebas sobre los sistemas, ya que evitamos trabajar con conjuntos y con operaciones de conjuntos (como la pertenencia) en el análisis de las transiciones de un sistema compuesto. Es importante aclarar que esta hipótesis no condiciona el incremento de un sistema al agregar nuevos componentes.
- El estado inicial del sistema asume valores nulos para los relojes, en relación a la definición de grafos temporizados dada en la sección 2.1. Sin embargo, esta es una convención y podríamos entonces permitir valores iniciales distintos de cero e incluso diferentes para cada reloj.
- Las transiciones, discretas y temporales, formalizadas preservan el cumplimiento del predicado `Inv` y asumen que éste vale en el estado de origen de la transición. Esta suposición se justifica porque consideraremos conjuntos de estados generados por transiciones –trazas de ejecución– a partir de un estado inicial *válido*. Luego, todos los estados de una ejecución serán estados válidos del sistema, tal cual lo establece la definición 2.2 de la sección 2.1.1.

## 3.3 Operadores Temporales con Tipos Inductivos

En esta sección formalizamos dos operadores temporales con tipos inductivos que permiten especificar *invarianza* y *alcanzabilidad*. Incluimos la versión de CTL y la cuantitativa temporal de TCTL.

### 3.3.1 Estados Alcanzables

Los estados *alcanzables* desde uno inicial dado representan estados pertenecientes a trazas de ejecución de un grafo temporizado que comienzan en dicho estado. Sea  $S$  el tipo de los estados de un sistema de tiempo real y  $\tau_r$  una relación de transición entre estados

de  $S$  que respeta el formato dado en la sección previa. El conjunto de estados alcanzables desde uno inicial  $S_{ini}$  a través de  $tr$  puede definirse inductivamente como sigue,

```
Variable S : Set.
Variable tr : S -> Label -> S -> Prop.

Inductive RState [Sini:S] : S -> Prop :=
  rsIni : (RState Sini Sini)
  | rsNext : ∀s1,s2∈S ∀l∈Label
    (RState Sini s1) ->
    (tr s1 l s2) ->
    (RState Sini s2).
```

Esto es, el estado inicial es alcanzable ( $rsIni$ ) y los estados a los que se llega desde un estado alcanzable por una transición también son alcanzables ( $rsNext$ ). Asimismo, los estados alcanzables en tiempo  $t$  desde un estado inicial  $S_{ini}$  pueden definirse como una generalización de la definición previa.

```
Inductive RState_T [Sini:S] : S -> Instant -> Prop :=
  rsIni_T : (RState_T Sini Sini time0)
  | rsNoTime_T : ∀s1,s2∈S ∀l∈Label ∀t∈Instant
    (RState_T Sini s1 t) ->
    ~l=Tick ->
    (tr s1 l s2) ->
    (RState_T Sini s2 t)
  | rsTime_T : ∀s1,s2∈S ∀t∈Instant
    (RState_T Sini s1 t) ->
    (tr s1 Tick s2) ->
    (RState_T Sini s2 (Inc t)).
```

El estado inicial es alcanzable en tiempo  $time0$  ( $rsIni\_T$ ); las transiciones discretas no insumen tiempo ( $rsNoTime\_T$ ); y, las transiciones temporales representan el paso de un *tick* ( $rsTime\_T$ ).

### 3.3.2 Invarianza y Alcanzabilidad

En esta sección formalizamos los operadores temporales cualitativos  $\forall\Box$  y  $\exists\Diamond$ , y sus versiones temporales cuantitativas, con tipos inductivos.

- $\forall\Box P$  y  $\forall\Box_t P$  permiten especificar propiedades invariantes e invarianza acotada (ver sección 2.3.2).

```

Definition ForAll := [Sini:S; P:S->Prop]
  ∀s∈S (RState Sini s) -> (P s).

```

```

Definition ForAll_T := [Sini:S; P:S->Prop; bound:Instant->Prop]
  ∀s∈S ∀t∈Instant (bound t) -> (RState_T Sini s t) -> (P s).

```

ForAll especifica que todos los estados alcanzables desde un estado inicial  $Sini$  cumplen la propiedad  $P$ , mientras que ForAll\_T especifica la propiedad anterior para todos los valores temporales  $t$  que satisfacen  $(bound\ t)$ , es decir  $t \in I$ . La primera definición se obtiene de la segunda instanciando a  $bound$  con el predicado constante  $True$ , para todo  $t \in Instant$ .

- $\exists\Diamond P$  y  $\exists\Diamond_I P$  permiten especificar problemas de alcanzabilidad no acotada y acotada, respectivamente (ver sección 2.3.2).

```

Inductive Exists [Sini:S; P:S->Prop] : Prop :=
  exists : ∀s∈S (RState Sini s) -> (P s) ->
    (Exists Sini P).

```

```

Inductive Exists_T [Sini:S; P:S->Prop; bound:Instant->Prop] : Prop :=
  exists_T : ∀s∈S ∀t∈Instant (bound t) ->
    (RState_T Sini s t) -> (P s) ->
    (Exists_T Sini P bound).

```

La relación inductiva  $Exists$  especifica que existe un estado alcanzable desde un estado inicial  $Sini$  que cumple la propiedad  $P$ , mientras que  $Exists_T$  define la propiedad anterior para todos los valores temporales  $t$  que satisfacen  $(bound\ t)$ . Luego, una prueba de  $\exists\Diamond P$  ( $\exists\Diamond_I P$ ) se obtiene a partir de un estado alcanzable que verifica  $P$  (y  $(bound\ t)$ ) en la versión temporal acotada sobre un intervalo  $I$  y consiste en la construcción de un camino desde el estado inicial.

**Nota 3.3.** En la demostración de propiedades de un sistema  $G$  que involucran los operadores  $\forall\Box$  ( $\forall\Box_I$ ) y  $\exists\Diamond$  ( $\exists\Diamond_I$ ) requerimos que el estado inicial considerado satisfaga el invariante de las locaciones  $inv$  de  $G$ . Es decir, si este estado es el inicial de  $G$  ( $Sini_G$ ) el requerimiento se satisface pues previamente exigimos que  $Sini_G$  debe ser un estado *válido* de  $G$  (ver nota 3.2). En otro caso, las propiedades demostradas tienen sentido si el estado inicial considerado es *válido*. Este requerimiento podría ser explicitado en la definición de estados alcanzables (el estado inicial es alcanzable a partir de él mismo si cumple el invariante  $inv$ ), sin embargo de esta manera complicaríamos la estructura de las pruebas (particularmente las de alcanzabilidad) y aumentaríamos el tamaño de los términos de prueba. Asimismo, puesto que las transiciones preservan, por definición, el cumplimiento de  $inv$ , en propiedades compuestas del tipo  $\forall\Box\exists\Diamond P$ , los estados iniciales considerados para  $\exists\Diamond P$  trivialmente satisfacen el requerimiento si el estado inicial para  $\forall\Box\exists\Diamond P$  lo



cumple. Luego, en la demostración de toda propiedad requerimos la prueba adicional de que el estado inicial es *válido*.

Definiciones más generales de los operadores  $\forall\Box$  ( $\forall\Box_I$ ) y  $\exists\Diamond$  ( $\exists\Diamond_I$ ) pueden ser útiles para especificar propiedades donde los estados iniciales están caracterizados por un predicado  $Q$ . Estas versiones pueden definirse a partir de las previas, como sigue.

- $\forall\Box(Q \Rightarrow \forall\Box P)$  y  $\forall\Box(Q \Rightarrow \forall\Box_I P)$

```
Definition ForAll_from := [Sini:S; Q,P:S->Prop]
  (ForAll Sini ( [s:S] (Q s)->(ForAll s P) )).
```

```
Definition ForAll_from_T :=
  [Sini:S; Q,P:S->Prop, bound:Instant->Prop]
  (ForAll Sini ( [s:S] (Q s)->(ForAll_T s P bound) )).
```

- $\forall\Box(Q \Rightarrow \exists\Diamond P)$  y  $\forall\Box(Q \Rightarrow \exists\Diamond_I P)$ .

```
Definition Exists_from := [Sini:S; Q,P:S->Prop]
  (ForAll Sini ( [s:S] (Q s)->(Exists s P) )).
```

```
Definition Exists_from_T :=
  [Sini:S; Q,P:S->Prop; bound:Instant->Prop]
  (ForAll Sini ( [s:S] (Q s)->(Exists_T s P bound)) ).
```

### 3.3.3 Algunas Propiedades

Propiedades conocidas de los operadores temporales formalizados en la sección previa pueden demostrarse utilizando el asistente de pruebas *Coq*. A continuación destacamos, a modo de ejemplo, algunas de ellas. Las demostraciones pueden consultarse en el apéndice B.1.2.

```
Theorem Mon_I :  $\forall Sini \in S \ \forall Pg, Pp \in (S \rightarrow Prop)$ 
  (ForAll Sini Pg) -> ( $\forall s \in S$  (Pg s)->(Pp s)) -> (ForAll Sini Pp).
```

```
Theorem Mon_I_T :  $\forall Sini \in S \ \forall Pg, Pp \in (S \rightarrow Prop) \ \forall bound \in (Instant \rightarrow Prop)$ 
  (ForAll_T Sini Pg bound) -> ( $\forall s \in S$  (Pg s)->(Pp s)) ->
  (ForAll_T Sini Pp bound).
```

```
Theorem Mon_I_EX :  $\forall Sini \in S \ \forall Pg, Pp \in (S \rightarrow Prop)$ 
  (Exists Sini Pg) -> ( $\forall s \in S$  (Pg s)->(Pp s)) -> (Exists Sini Pp).
```

```

Theorem Mon_I_EX_T :  $\forall \text{Sini} \in S \ \forall P_g, P_p \in (S \rightarrow \text{Prop})$ 
   $\forall \text{bound} \in (\text{Instant} \rightarrow \text{Prop})$  (Exists_T Sini P_g bound) ->
  ( $\forall s \in S$  (P_g s) -> (P_p s)) -> (Exists_T Sini P_p bound).

Theorem Conj :  $\forall \text{Sini} \in S \ \forall P_1, P_2 \in (S \rightarrow \text{Prop})$  (ForAll Sini P_1) ->
  (ForAll Sini P_2) -> (ForAll Sini ( [s:S] (P_1 s) /\ (P_2 s) ) ).

Theorem Conj_T :  $\forall \text{Sini} \in S \ \forall P_1, P_2 \in (S \rightarrow \text{Prop}) \ \forall \text{bound} \in (\text{Instant} \rightarrow \text{Prop})$ 
  (ForAll_T Sini P_1 bound) -> (ForAll_T Sini P_2 bound) ->
  (ForAll_T Sini ( [s:S] (P_1 s) /\ (P_2 s) ) bound).

```

El teorema `Mon_I` permite probar un invariante  $P_p$  a partir del invariante  $P_g$  si  $P_p$  es consecuencia lógica de  $P_g$ . `Mon_I_EX` es la propiedad previa para el problema de alcanzabilidad ( $\exists\Diamond$ ). `Conj` establece que la conjunción de invariantes es un invariante. `Mon_I_T`, `Mon_I_EX_T` y `Conj_T` son las versiones para los operadores temporales acotados de `Mon_I`, `Mon_I_EX` y `Conj`, respectivamente.

```

Lemma RState_Trans :  $\forall s_1, s_2, s_3 \in S$ 
  (RState s1 s2) -> (RState s2 s3) -> (RState s1 s3).

Lemma RState_Trans_T :  $\forall s_1, s_2, s_3 \in S \ \forall t_1, t_2 \in \text{Instant}$ 
  (RState_T s1 s2 t1) -> (RState_T s2 s3 t2) ->
  (RState_T s1 s3 (plus_Ck t1 t2)).

Theorem StepsEX :  $\forall s_1, s_2 \in S \ \forall P \in (S \rightarrow \text{Prop})$ 
  (RState s1 s2) -> (Exists s2 P) -> (Exists s1 P).

```

`RState_Trans` es la transitividad de la relación de alcanzabilidad `RState` y, `RState_Trans_T` la correspondiente a la relación `RState_T`. `StepsEX` establece que si  $\exists\Diamond P$  vale a partir de una estado inicial  $s_2$  y  $s_2$  es alcanzable a partir del estado  $s_1$  entonces  $\exists\Diamond P$  vale a partir del estado inicial  $s_1$ . `StepsEX` usa en su prueba al lema `RState_Trans`.

Los siguientes dos teoremas corresponden a las equivalencias  $\forall\Box P \Leftrightarrow \neg\exists\Diamond\neg P$  y  $\forall\Box\neg P \Leftrightarrow \neg\exists\Diamond P$ . Los mismos se prueban en lógica clásica, usando el principio del tercero excluido; en *Coq*, el axioma `classic`:  $\forall P \in \text{Prop} \ P \vee \neg P$ .

```

Theorem ForAll_EX :  $\forall \text{Sini} \in S \ \forall P \in (S \rightarrow \text{Prop})$ 
  (ForAll Sini P) <->  $\sim$ (Exists Sini ( [s:S]  $\sim$ (P s) ) ).

Theorem ForAll_EX_T :  $\forall \text{Sini} \in S \ \forall P \in (S \rightarrow \text{Prop}) \ \forall \text{bound} \in (\text{Instant} \rightarrow \text{Prop})$ 
  (ForAll_T Sini P bound) <->  $\sim$ (Exists_T Sini ( [s:S]  $\sim$ (P s) ) bound).

```

### 3.4 Necesidad de Tipos Co-Inductivos

Si bien muchas propiedades pueden especificarse usando los operadores  $\exists\Diamond$  y  $\forall\Box$  ( $\exists\Diamond_I$  y  $\forall\Box_I$ ), otras requieren el uso de las versiones más generales de  $\exists\mu$  y  $\forall\mu$  ( $\exists\mu_I$  y  $\forall\mu_I$ ). Por ejemplo, los problemas de respuesta en tiempo acotado (“siempre antes de un tiempo  $t$  se cumple una propiedad  $P$ , para toda ejecución del sistema”). Los operadores  $\forall\Diamond$  y  $\exists\Box$  ( $\forall\Diamond_I$  y  $\exists\Box_I$ ) no pueden ser formalizados en base a solamente tipos inductivos y la noción de *estados alcanzables*, sino que resulta necesario formalizar el concepto de *traza de ejecución* y consecuentemente, la definición de tipos *co-inductivos* para una descripción completa de todas las fórmulas de TCTL.

#### 3.4.1 Nociones Preliminares

Como expresamos en el capítulo 1, los tipos *co-inductivos* son tipos recursivos que pueden contener objetos infinitos (no bien fundados). Un ejemplo de éstos es el tipo de las secuencias infinitas formadas con elementos de un tipo  $T$ , también llamadas “*streams*”. Este tipo se formaliza en *Coq* de la siguiente manera (y se carga en el ambiente *Coq* con la declaración `Require Streams`):

```
CoInductive Stream [T:Set] : Set := Cons : T -> (Stream T) -> (Stream T).
```

`Cons` es el constructor del tipo `Stream`. Asumiremos alternativamente una notación infija para `Cons` dada por operador  $\wedge$ , que definimos asociativo a derecha con el uso del comando `Infix RIGHTA 9 “^” Cons`.

```
Infix RIGHTA 9 “^” Cons.
```

La *inducción estructural* es la manera de expresar que los tipos *inductivos* pueden contener sólo objetos *bien fundados*. Para tipos *co-inductivos* este principio de eliminación no es válido, aunque sí el principio de *análisis de casos* (válido también para tipos inductivos). Este principio puede ser usado, por ejemplo, para definir las funciones `hd` y `tl` que retornan la cabeza y la cola, respectivamente, de una secuencia infinita de tipo `Stream` [Gim98].

```
Definition hd := [T:Set; x:(Stream T)] Cases x of (Cons a y) => a end.
```

```
Definition tl := [T:Set; x:(Stream T)] Cases x of (Cons a y) => y end.
```

Por más información acerca de *streams* y tipos *co-inductivos* en general, ver [Coq93, Pau93a, Gim95, Gim96, Gim98, Bar<sup>+</sup>99].

### 3.4.2 Operadores Temporales Cualitativos

En esta sección presentamos una formalización de los operadores temporales cualitativos de CTL. Es decir, del fragmento de TCTL que no permite razonamiento cuantitativo del tiempo.

Sea  $S$  el tipo de los estados de un sistema de tiempo real y  $tr$  una relación de transición entre estados de  $S$  que respeta el formato dado en la sección 3.3.1. Definimos las trazas de estados generadas por  $tr$  como un predicado co-inductivo  $isTrace$  sobre secuencias infinitas ( $Stream$ ) de estados de  $S$ , que llamaremos  $SPath$ . Más precisamente, como el más grande predicado cerrado bajo la regla de introducción  $is\_trace$  que se enuncia abajo.  $isTraceFrom$  define a las trazas que poseen comienzo en un estado inicial dado.

```

Variable S : Set.
Variable tr : S -> Label -> S -> Prop.

Definition SPath := (Stream S).

CoInductive isTrace : SPath -> Prop :=
  is_trace : ∀x∈SPath ∀s1,s2∈S ∀l∈Label
    (tr s1 l s2) -> (isTrace s2^x) ->
    (isTrace s1^s2^x).

Definition isTraceFrom := [Sini:S; x:SPath]
  Sini=(hd x) /\ (isTrace x).

```

Una prueba de  $(isTrace\ x)$  es semejante a una secuencia infinita decorada en cada posición con un subsecuencia  $z$  de  $x$  y una prueba de que hay una transición al comienzo de  $z$ .

Observemos que, al igual que en la sección 3.3, no explicitamos en la formalización de  $isTraceFrom$  que el estado inicial de la traza debe ser un estado *válido*. Las razones son las mismas que las expuestas en dicha sección.

Usualmente las propiedades se definen sobre estados, sin embargo en esta sección consideramos que las mismas tienen como dominio a *streams* de estados, a fin de permitir definir a los operadores temporales composicionales (es decir, poder expresar fórmulas compuestas tales como:  $\forall\exists\Diamond P$ ,  $\forall\Diamond\exists P$ , etc). Esta concepción generaliza y no restringe las propiedades definibles –las propiedades sobre los estados refieren al primer elemento del *stream*.

El operador *until* ( $\mu$ ) –no cuantificado– puede ser definido por un predicado inductivo sobre las secuencias infinitas de estados.  $P\mu Q$  expresa que  $Q$  vale en un estado y  $P$  continuamente en los estados previos.

```

Inductive Until [P,Q:SPath->Prop] : SPath -> Prop :=
  UntilFurther :  $\forall s \in S \ \forall x \in SPath \ (P \ s^x) \rightarrow (Until \ P \ Q \ x) \rightarrow$ 
    (Until P Q s^x)
  | UntilHere :  $\forall x \in SPath \ (Q \ x) \rightarrow$ 
    (Until P Q x).

```

Una prueba de  $P\mu Q$  es un objeto finito. Esto significa que la búsqueda de un testigo de la verdad de  $Q$  no puede postergarse indefinidamente. Es decir, la prueba sólo aplica *UntilFurther* un número finito de veces (posiblemente nulo) antes de aplicar *UntilHere*.

Podemos formalizar ahora los operadores  $\exists\mu (P\exists\mu Q)$  y  $\forall\mu (P\forall\mu Q)$  sobre las trazas de un sistema con estado de origen dado, como sigue:

```

Inductive EX_Until [Sini:S; P,Q:SPath->Prop] : Prop :=
  ExUntil :  $\forall x \in SPath \ (isTraceFrom \ Sini \ x) \rightarrow (Until \ P \ Q \ x) \rightarrow$ 
    (EX_Until Sini P Q).

Definition FA_Until := [Sini:S; P,Q:SPath->Prop]  $\forall x \in SPath$ 
  (isTraceFrom Sini x)  $\rightarrow (Until \ P \ Q \ x)$ .

```

*EX\_Until* es un predicado inductivo que permite expresar una propiedad  $P\exists\mu Q$  para una traza con origen en un estado inicial *Sini*; *FA\_Until* es una definición para  $P\forall\mu Q$  sobre las trazas con estado inicial *Sini*.

Luego, podríamos definir las abreviaturas dadas en 2.3.2 para los operadores  $\exists\Diamond$ ,  $\forall\Diamond$ ,  $\exists\Box$  y  $\forall\Box$  a partir de las formalizaciones para  $\exists\mu$  y  $\forall\mu$ . Sin embargo optamos por dar una definición explícita de éstos para simplificar las pruebas, ya que sino las mismas se tornan más complejas, porque es necesario trabajar con negaciones. Por ejemplo, según la sección 2.3.2,  $\forall\Box P = \neg(true\exists\mu\neg P)$  y esto equivale a probar que no existe un estado alcanzable –subtraza– que cumpla  $\neg P$  (es decir, que no existe un prefijo finito de una traza infinita que cumpla  $\neg P$ ). Sin embargo, resulta más fácil verificar que todos los estados alcanzables –todas las subtrazas– cumplen  $P$ . Nuevamente, estamos razonando bajo la hipótesis del tercero excluido, en lógica clásica.

A continuación formalizamos  $\Box P$  como un predicado co-inductivo *ForAllS* y  $\Diamond P$  como un predicado inductivo *ExistsS*, ambos sobre secuencias infinitas de estados (*SPath*).

```

CoInductive ForAllS [P:SPath->Prop]: SPath -> Prop :=
  ForallS :  $\forall x \in SPath \ \forall s \in S \ (P \ s^x) \rightarrow (ForAllS \ P \ x) \rightarrow$ 
    (ForAllS P s^x).

```

```

Inductive ExistsS [P:SPath->Prop] : SPath -> Prop :=
  Here : ∀x∈SPath (P x) -> (ExistsS P x)

  | Further : ∀x∈SPath ∀s∈S (ExistsS P x) -> (ExistsS P s^x).

```

**ForAllS** caracteriza a las secuencias infinitas que satisfacen continuamente un predicado  $P$ . **ExistsS** a las que poseen al menos una subsecuencia que cumple  $P$ . Una prueba de la proposición  $\Box P(x)$  es semejante a una secuencia infinita decorada en cada posición con una subsecuencia  $z$  de  $x$  y una prueba de que  $z$  satisface  $P$ . En tanto que una prueba de  $\Diamond P(x)$  es un camino desde  $x$  a alguna subsecuencia  $z$  de  $x$  que verifica  $P$ . En este último caso, la exhibición de  $z$  no puede ser postergada indefinidamente y por ello  $\Diamond$  es definido inductivamente.

En función de **ForAllS** y **ExistsS** especificamos  $\exists\Diamond$  (**Posible**),  $\forall\Diamond$  (**Inevitable**),  $\exists\Box$  (**SafePath**) y  $\forall\Box$  (**Always**). Las propiedades existenciales las formalizamos como predicados inductivos y las universales como definiciones *Coq*. Todas ellas usan **isTraceFrom** para permitir cuantificar sobre las trazas de ejecución generadas a partir de un estado inicial **Sini**.

```

Inductive Posible [Sini:S; P:SPath->Prop] : Prop :=
  posible : ∀x∈SPath (isTraceFrom Sini x) -> (ExistsS P x) ->
    (PosibleS Sini P).

Definition Inevitable := [Sini:S; P:SPath->Prop]
  ∀x∈SPath (isTraceFrom Sini x) -> (ExistsS P x).

Inductive SafePath [Sini:S; P:SPath->Prop] : Prop :=
  safePath : ∀x∈SPath (isTraceFrom Sini x) -> (ForAllS P x) ->
    (SafePath Sini P).

Definition Always := [Sini:S; P:SPath->Prop]
  ∀x∈SPath (isTraceFrom Sini x) -> (ForAllS P x).

```

**Nota 3.4.** Es importante remarcar que es imposible representar los operadores  $\forall\Diamond$  y  $\exists\Box$  exclusivamente con tipos inductivos, tal como lo hicimos en la sección 3.3 para  $\exists\Diamond$  y  $\forall\Box$ , debido a que no se puede expresar inductivamente la noción de secuencialidad entre los estados por ser ésta de naturaleza *infinita* para la clase de sistemas en estudio. Es por ello que los tipos co-inductivos resultan necesarios y en particular la formalización de *traza de ejecución* –como una secuencia infinita (*stream*) de estados– en lugar de *conjunto de estados alcanzables* –suficiente para verificar invarianza y alcanzabilidad (acotadas o no).

**Ejemplo 3.1.** Sea  $P$  una propiedad sobre los estados del sistema e  $IsSini$  el predicado característico de un estado **Sini**. La fórmula  $IsSini \Rightarrow \forall\Box P$  se especifica como sigue: (**Always tr Sini P'**), donde **tr** es la relación de transición del sistema y  $P'$

corresponde al predicado “[ $x$ :SPath] (P (hd x))” –con SPath el tipo (Stream S) y S es el tipo de los estados ( $Sini \in S$ ). Asimismo, una fórmula temporal compuesta  $IsSini \Rightarrow \forall \diamond \exists \diamond P$  puede especificarse como: (Inevitable tr Sini Q), donde Q es el predicado “[ $x$ :SPath] (Posible tr (hd x) P’)” y P’ el predicado anterior. En las fórmulas anteriores, si P es una propiedad sobre los *streams*, entonces P’ es P en las especificaciones dadas. Si en lugar de tener el predicado *IsSini*, que caracteriza a un único estado, disponemos de un predicado Q que caracteriza a múltiples estados, las especificaciones se expresan en forma análoga a como señalamos al final de la sección 3.3.2 (con Always al comienzo).

Las abreviaturas dadas en 2.3.2 para  $\diamond$  y  $\square$  pueden ahora ser demostradas como teoremas. A continuación formulamos los teoremas, cuyas demostraciones se incluyen en el apéndice B.2.2.

```
Theorem Equiv1 :  $\forall Sini \in S \ \forall P \in (SPath \rightarrow Prop)$ 
  (Posible Sini P) <-> (EX_Until Sini ( [_:SPath] True ) P).
```

```
Theorem Equiv2 :  $\forall Sini \in S \ \forall P \in (SPath \rightarrow Prop)$ 
  (Inevitable Sini P) <-> (FA_Until Sini ( [_:SPath] True ) P).
```

```
Theorem Equiv3 :  $\forall Sini \in S \ \forall P \in (SPath \rightarrow Prop)$ 
  (Always Sini P) <->  $\sim$ (Posible Sini ( [s:SPath]  $\sim$ (P s) )).
```

```
Theorem Equiv4 :  $\forall Sini \in S \ \forall P \in (SPath \rightarrow Prop)$ 
  (SafePath Sini P) <->  $\sim$ (Inevitable Sini ( [s:SPath]  $\sim$ (P s) )).
```

Los teoremas *Equiv1* y *Equiv2* se prueban por inducción, mientras que *Equiv3* y *Equiv4* requieren co-inducción y se demuestran en lógica clásica con el uso del principio del tercero excluido.

Asimismo, algunas de las propiedades previamente formuladas en 3.3.3 pueden ser probadas para la definición de los operadores temporales sobre *streams* de estados.

```
Theorem Mon_I :  $\forall x \in SPath \ \forall Pg, Pp \in (SPath \rightarrow Prop)$ 
  (ForAlls Pg x) -> ( $\forall s \in SPath$  (Pg s) -> (Pp s)) -> (ForAlls Pp x).
```

```
Theorem Conj :  $\forall x \in SPath \ \forall P1, P2 \in (SPath \rightarrow Prop)$ 
  (ForAlls P1 x) -> (ForAlls P2 x) ->
  (ForAlls ( [s:SPath] (P1 s) /\ (P2 s) ) x).
```

```
Theorem Mon_I_EX :  $\forall x \in SPath \ \forall Pg, Pp \in (SPath \rightarrow Prop)$ 
  (ExistsS Pg x) -> ( $\forall s \in SPath$  (Pg s) -> (Pp s)) -> (ExistsS Pp x).
```

```
Theorem OneStep_EX :  $\forall x \in SPath \ \forall P \in (SPath \rightarrow Prop)$  (ExistsS P x) ->
   $\forall s \in S$  (ExistsS P s^x).
```

Los cuatro teoremas se demuestran fácilmente. En los dos primeros la prueba es por co-inducción. Las demostraciones se incluyen en el apéndice B.2.2.

### 3.4.3 Operadores Temporales Cuantitativos

Las formalizaciones dadas en la sección previa de los operadores temporales pueden extenderse para caracterizar la versión general de la lógica TCTL, que permite razonamiento cuantitativo temporal, con su semántica de tiempo discreto.

Nuevamente, sea  $S$  el tipo de los estados de un sistema de tiempo real y  $tr$  una relación de transición entre estados de  $S$ . Asumimos además que la pertenencia de un valor temporal a un intervalo es representada por un predicado  $bound : Instant \rightarrow Prop$ .

Definimos las trazas de estados generadas por  $tr$  como un predicado co-inductivo  $isTrace\_T$  sobre secuencias infinitas ( $SPath\_T$ ) de pares ( $State\_T$ ) de estados de  $S$  y valores temporales. Cada elemento de estas trazas es un par que representa al estado del sistema en un punto dado y al valor del *reloj global* en dicho punto. Este reloj es transparente para los sistemas, no es reseteado nunca, y se utiliza para demarcar el tiempo de las ejecuciones.  $isTraceFrom\_T$  define a las trazas temporizadas que poseen comienzo en un estado inicial dado (para un determinado valor del reloj global).

```

Variable S      : Set.
Variable tr    : S -> Label -> S -> Set.
Variable bound : Instant -> Prop.

Definition State_T := S * Instant.
Definition SPath_T := (Stream State_T).

CoInductive isTrace_T : SPath_T -> Prop :=
  | isTraceDisc :  $\forall x \in SPath\_T \forall s1, s2 \in S \forall l \in Label$ 
    (tr s1 l s2) ->
    ~l=Tick ->
    (isTrace_T (s2, t)^x) ->
    (isTrace_T ( (s1, t)^(s2, t)^x ))
  | isTraceTick :  $\forall x \in SPath\_T \forall s1, s2 \in S \forall t \in Instant$ 
    (tr s1 Tick s2) ->
    (isTrace_T (s2, (Inc t))^x) ->
    (isTrace_T ( (s1, t)^(s2, (Inc t))^x )).

Definition isTraceFrom_T := [Sini:State_T; x:SPath_T]
  Sini=(hd x) /\ (isTrace_T x).

```



$isTraceDisc$  corresponde a una transición discreta, la cual no insume tiempo.  $isTraceTick$  a una transición temporal etiquetada con `Tick`. El paso del tiempo está representado por `Inc`, que incrementa el *reloj global* del sistema en un *tick*.

Al igual que en la sección previa, consideramos que las propiedades tienen como dominio a *streams* de estados, a fin de permitir caracterizar operadores temporales composicionales; pero donde estos estados son pares compuestos por un estado del sistema y el valor del reloj global (elementos de tipo `State_T`). Dado  $x \in SPath\_T$ , las propiedades que sólo refieren al estado del sistema se expresan sobre el elemento  $Fst(hd\ x)$ . Donde, la función `Fst` retorna el primer componente de un par (`Snd` retorna el segundo).

La versión de tiempo acotado del operador *until* ( $\mu_t$ ) se define como una extensión natural de la planteada en 3.4.2.  $P\mu_t Q$  se formaliza como un predicado inductivo de la siguiente manera:

```
Inductive Until_bound [P,Q:SPath_T->Prop]: SPath_T -> Prop :=
  UntilFurther_bound :  $\forall s \in State\_T \ \forall x \in SPath\_T$ 
    (P s^x) -> (Until_bound P Q x) ->
    (Until_bound P Q s^x)
  | UntilHere_bound :  $\forall s \in State\_T \ \forall t \in Instant \ \forall x \in SPath\_T$ 
    (Q (s,t)^x) -> (bound t) ->
    (Until_bound P Q (s,t)^x).
```

Respecto a la definición no acotada de *until*, la prueba de satisfactibilidad de un predicado  $Q$  sobre un *stream*  $x$  está restringida al cumplimiento de `bound` sobre la componente temporal del primer estado del *stream*.

A partir de la definición anterior, las formalizaciones de los operadores  $\exists \mu_t (P \exists \mu_t Q)$  y  $\forall \mu_t (P \forall \mu_t Q)$ , sobre trazas con estado de origen dado, se obtienen generalizando `EX_Until` y `FA_Until` sobre intervalos de tiempo especificados con `bound`.

```
Inductive EX_Until_bound [Sini:State_T; P,Q:SPath_T->Prop] : Prop :=
  ExUntil_bound :  $\forall x \in SPath\_T$  (isTraceFrom_T Sini x) ->
    (Until_bound P Q x) ->
    (EX_Until_bound Sini P Q).

Definition FA_Until_bound := [Sini:State_T; P,Q:SPath_T->Prop]
   $\forall x \in SPath\_T$  (isTraceFrom_T Sini x) -> (Until_bound P Q x).
```

Al igual que en la sección previa definimos algunas de las abreviaturas más comúnmente usadas –introducidas en la sección 2.3.2– a través de `ExistsS` y `ForAllS`.  $\exists \diamond P$ ,  $\forall \diamond P$ ,  $\exists \square P$  y  $\forall \square P$  se obtienen a partir de `Posible_T`, `Inevitable_T`, `SafePath_T` y `Always_T`, respectivamente.

```

Inductive Possible_T [Sini:State_T; P:SPath_T->Prop] : Prop :=
  posible_T : ∀x∈SPath_T (isTraceFrom_T Sini x) ->
    (ExistsS ( [s:SPath_T] (bound (Snd (hd s))) /\ (P s) ) x) ->
    (PossibleS_T Sini P).

Definition Inevitable_T := [Sini:State_T; P:SPath_T->Prop]
  ∀x∈SPath_T (isTraceFrom_T Sini x) ->
    (ExistsS ( [s:SPath_T] (bound (Snd (hd s))) /\ (P s) ) x).

Inductive SafePath_T [Sini:State_T; P:SPath_T->Prop]: Prop :=
  safePath_T : ∀x∈SPath_T (isTraceFrom_T Sini x) ->
    (ForAllS ( [s:Path_T] (bound (Snd (hd s))) -> (P s) ) x) ->
    (SafePath_T Sini P).

Definition Always_T := [Sini:State_T; P:SPath_T->Prop]
  ∀x∈SPath_T (isTraceFrom_T Sini x) ->
    (ForAllS ( [s:SPath_T] (bound (Snd (hd s))) -> (P s) ) x).

```

**Ejemplo 3.2.** Sea  $P$  una propiedad básica sobre los estados del sistema e  $IsSini$  el predicado característico de un estado  $Sini$ . La fórmula  $IsSini \Rightarrow \forall \square_I P$  se especifica ( $Always\_T \text{ tr boundI } (Sini, time0) P'$ ); donde,  $\text{tr}$  es la relación de transición del sistema,  $\text{boundI}$  es el predicado que corresponde a la pertenencia del valor del reloj global al intervalo  $I$  y  $P'$  es el predicado “[ $x:SPath\_T$ ] ( $P (Fst (hd x))$ )” –con  $SPath\_T$  el tipo ( $Stream\ S*Instant$ ),  $S$  el tipo de los estados ( $Sini \in S$ ) y  $time0$  el instante de tiempo inicial. Asimismo, una fórmula compuesta  $IsSini \Rightarrow \forall \diamond_I \exists \diamond_J P$  puede especificarse como sigue: ( $Inevitable\_T \text{ tr boundI } (Sini, time0) Q$ ); donde,  $Q$  es el predicado “[ $x:SPath\_T$ ] ( $Possible\_T \text{ tr boundJ}' (hd x) P'$ )”, con  $P'$  el predicado anterior y  $\text{boundJ}'$  la actualización del predicado  $\text{boundJ}$  “[ $t:Instant$ ] ( $\text{boundJ } (\text{plus\_Ck } t (Snd (hd x)))$ )” ( $\text{boundJ}$  es el predicado que corresponde a la pertenencia de un valor temporal al intervalo  $J$ ). En las fórmulas anteriores el valor  $time0$  puede generalizarse a cualquier instante  $t$ , actualizando el predicado  $\text{boundI}$  de la misma manera que describimos para  $\text{boundJ}$  (“[ $t':Instant$ ] ( $\text{boundI } (\text{plus\_Ck } t t')$ )”). Si en lugar de tener el predicado  $IsSini$ , que caracteriza a un único estado, disponemos de un predicado  $Q$  que caracteriza a múltiples estados, las especificaciones se expresan en forma análoga a como señalamos al final de la sección 3.3.2 (con  $Always\_T$  al comienzo y “[ $t:Instant$ ] True” el predicado correspondiente a su intervalo acotado).

Nuevamente, las abreviaturas dadas en 2.3.2 pueden ser demostradas como teoremas, ahora para las versiones más generales de los operadores  $\exists \mu_i$  y  $\forall \mu_i$ .

```
Theorem Equiv1_T :  $\forall \text{Sini} \in \text{State\_T} \ \forall P \in (\text{SPath\_T} \rightarrow \text{Prop})$ 
  (Possible_T Sini P) <->
  (EX_Until_bound Sini ( [_:SPath_T] True ) P).
```

```
Theorem Equiv2_T :  $\forall \text{Sini} \in \text{State\_T} \ \forall P \in (\text{SPath\_T} \rightarrow \text{Prop})$ 
  (Inevitable_T Sini P) <->
  (FA_Until_bound Sini ( [_:SPath_T] True ) P).
```

```
Theorem Equiv3_T :  $\forall \text{Sini} \in \text{State\_T} \ \forall P \in (\text{SPath\_T} \rightarrow \text{Prop})$ 
  (Always_T Sini P) <->
   $\sim$ (Possible_T Sini ( [s:SPath_T]  $\sim$ (P s) )).
```

```
Theorem Equiv4_T :  $\forall \text{Sini} \in \text{State\_T} \ \forall P \in (\text{SPath\_T} \rightarrow \text{Prop})$ 
  (SafePath_T Sini P) <->
   $\sim$ (Inevitable_T Sini ( [s:SPath_T]  $\sim$ (P s) )).
```

Equiv3\_T y Equiv4\_T se demuestran en lógica clásica, con el uso del principio del tercero excluido. Las pruebas para estos dos teoremas son por co-inducción, mientras que Equiv1\_T y Equiv2\_T se demuestran por inducción. Las demostraciones se incluyen en el apéndice B.3.2.

**Nota 3.5.** Las formalizaciones dadas en la sección 3.4.2 resultan de las presentadas en esta sección para trazas temporizadas, asumiendo que los intervalos son no acotados; es decir, cada predicado  $\text{bound} : \text{Instant} \rightarrow \text{Prop}$  es True para todo  $t \in \text{Instant}$ .



# Capítulo 4

## *Caso de Estudio: Control de un Paso a Nivel de Tren*

---

En este capítulo consideramos un caso de estudio: *el control de un paso a nivel de tren* (“*the railroad crossing example*”). Especificamos el sistema en *Coq* en base a las formalizaciones introducidas en el capítulo 3. Analizamos luego la demostración de *invariantes*, incluyendo la propiedad de seguridad esencial del sistema, y verificamos la divergencia del tiempo en las ejecuciones. Posteriormente generalizamos la especificación, parametrizando las constantes del problema y definimos restricciones entre estos parámetros y los relojes del sistema a fin de preservar las propiedades analizadas.

### 4.1 Descripción del Problema

Numerosos trabajos consideran a este problema como “*benchmark*” para analizar diferentes técnicas de especificación y herramientas de análisis. Entre otros, [HNS<sup>+</sup>92, CHR92, Sha93, HJL93, HK94, DY95, AB96, BMS<sup>+</sup>97]. Nosotros tomamos la especificación del problema de [AD94] (basada en [LS85]).

El sistema consiste de tres procesos paralelos: un tren (*train*), un controlador (*controller*) y una barrera (*gate*). Cada proceso puede ser modelado por un grafo temporizado tal como lo ilustra la figura 4.1.

La variable de control *st* del tren varía sobre tres locaciones: *st = Far* si el tren está lejos de cruzar el paso a nivel (no hay trenes cerca del cruce); *st = Near* si el tren está próximo a cruzar; y, *st = Inside* si está cruzando. *Far* es la locación del estado inicial. Cuando el tren está próximo a cruzar (es decir, se mueve de la locación *Far* a *Near*), él envía una señal *Approach* al controlador, avisando sobre la proximidad de un tren. Esto ocurre *n* unidades de tiempo antes, con  $n > kt1$ , que el tren este cruzando el paso a nivel. Cuando el tren termina de cruzar (es decir, se mueve de la locación *Inside* a *Far*) envía una señal *Exit* al controlador, indicando el alejamiento del tren del paso a nivel. Esto ocurre antes que *kt2* unidades de tiempo han pasado desde la señal *Approach*.

La variable de control *sc* del controlador varía sobre cuatro locaciones: *sc = Sc1* si el controlador está esperando que el tren arribe; *sc = Sc2* si la señal *Approach* ha sido

recibida;  $sc = Sc3$  si el controlador está esperando la señal *Exit*; y,  $sc = Sc4$  si la señal *Exit* ha sido recibida.  $Sc1$  es la locación del estado inicial. Cuando la señal *Approach* es recibida (es decir, el controlador se mueve de  $Sc1$  a  $Sc2$ ), el controlador envía a la barrera la señal *Lower*, exactamente  $kc1$  unidades de tiempo después, indicando que ésta debe bajar. Cuando *Exit* es recibida (es decir, el controlador se mueve de  $Sc3$  a  $Sc4$ ), antes de  $kc2$  unidades de tiempo el controlador envía a la barrera la señal *Raise*, para que la barrera comience a subir.

La variable de control  $sg$  de la barrera varía sobre cuatro locaciones:  $sg = Open$  si la barrera está levantada y esperando la señal *Lower*;  $sg = Lowering$  si la señal *Lower* ha sido recibida;  $sg = Closed$  si la barrera está baja y esperando la señal *Raise*; y,  $sg = Raising$  si la señal *Raise* ha sido recibida. *Open* es la locación del estado inicial. Cuando la señal *Lower* es recibida (es decir, la barrera se mueve de *Open* a *Lowering*), la barrera está baja antes de  $kg1$  unidades de tiempo y cuando *Raise* llega, antes de  $kg3$  y por lo menos  $kg2$  unidades de tiempo después la barrera está levantada nuevamente.

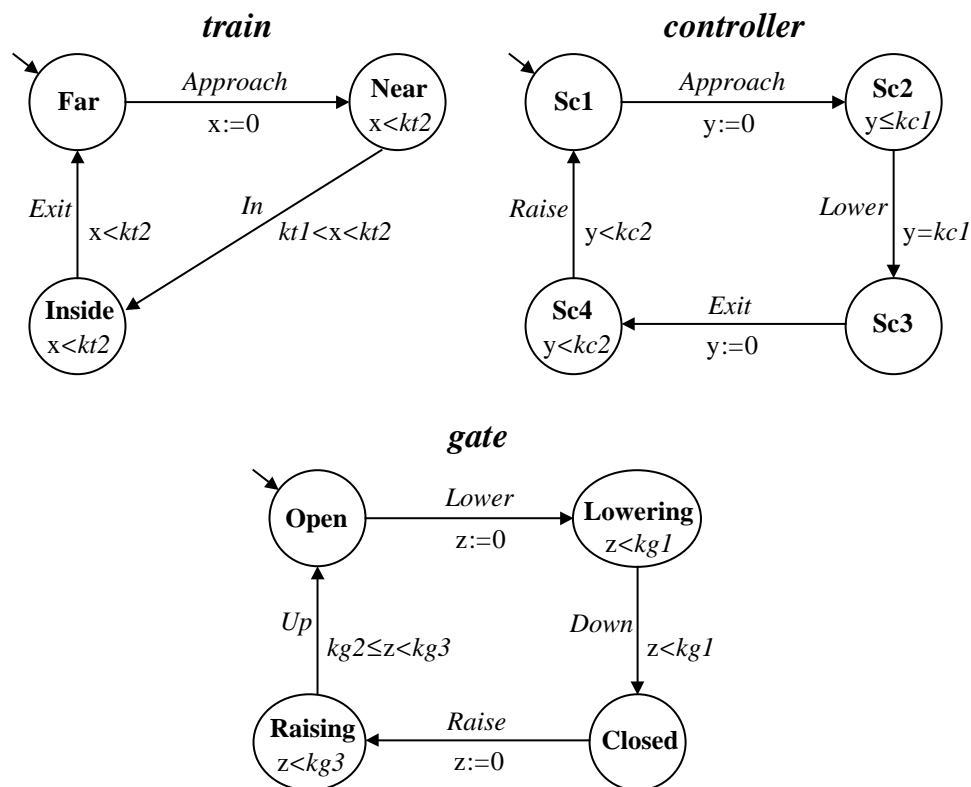


Fig. 4.1: Grafos temporizados del sistema “control de un paso a nivel de tren”

En [AD94] los valores de las constantes son los siguientes:  $kt1 = 2$ ,  $kt2 = 5$ ,  $kc1 = 1$ ,  $kc2 = 1$ ,  $kg1 = 1$ ,  $kg2 = 1$  y  $kg3 = 2$ . En este trabajo asumimos dichos valores de base

multiplicados por 4. Esto es  $M = 4 > |X|$ , en virtud de las consideraciones de la sección 2.5.3, con  $X$  el conjunto de los relojes del sistema compuesto.

## 4.2 Especificación del Sistema en Coq

En esta sección especificamos en *Coq* el sistema descrito en la sección previa, siguiendo los lineamientos generales dados en la sección 3.2. Llamaremos TCG al sistema compuesto (*train*  $\parallel$  *controller*  $\parallel$  *gate*).

El conjunto de las etiquetas del sistema está integrado por siete componentes correspondientes a transiciones discretas y una que rotula las transiciones temporales. En el primer grupo están *In*, *Down*, *Up*, *Approach*, *Exit*, *Lower* y *Raise*. Las tres primeras no son de sincronización, mientras que las cuatro últimas si lo son (*Approach* y *Exit* entre el tren y el controlador; *Lower* y *Raise* entre el controlador y la barrera). La etiqueta que representa las transiciones temporales es *Tick*, que es también de sincronización.

```
Inductive Label : Set := Approach : Label | In : Label | Exit : Label |
  Lower : Label | Raise : Label | Up : Label | Down : Label |
  Tick : Label.
```

Las locaciones del tren (*ST*), del controlador (*SC*) y la barrera (*SG*) se definen por los siguientes tipos enumerados,

```
Inductive ST : Set := Far : ST | Near : ST | Inside : ST.
Inductive SC : Set := Sc1 : SC | Sc2 : SC | Sc3 : SC | Sc4 : SC.
Inductive SG : Set := Open : SG | Lowering : SG | Closed : SG |
  Raising : SG.
```

Cada grafo temporizado del sistema TCG posee un reloj. Definimos el tipo de los estados compuestos por un único reloj como el siguiente tipo paramétrico,

```
Definition S_Ck := [State:Set] State * Clock.
```

Los estados del tren tienen tipo (*S\_Ck* *ST*), los del controlador (*S\_Ck* *SC*) y los de la barrera (*S\_Ck* *SG*).

Las constantes del sistema TCG se especifican con las siguientes declaraciones:

```
Definition kt1 : Instant := (8).
Definition kt2 : Instant := (20).
Definition kc1 : Instant := (4).
Definition kc2 : Instant := (4).
```

Definition **kg1** : Instant := (4).

Definition **kg2** : Instant := (4).

Definition **kg3** : Instant := (8).

Los invariantes de las locaciones son predicados sobre los estados que limitan la permanencia del sistema en las locaciones. Para el tren, el predicado es el siguiente,

```
Inductive InvT: (S_Ck ST) -> Prop :=
  Ifar      : ∀x∈Clock (InvT (Far,x))
| Inear     : ∀x∈Clock (lt_Ck x kt2) -> (InvT (Near,x))
| Iinside   : ∀x∈Clock (lt_Ck x kt2) -> (InvT (Inside,x)).
```

El invariante de la locación Far es True (el sistema puede permanecer en dicha locación sin restricciones) y el de las locaciones Near e Inside,  $(lt\_Ck \ x \ kt2)$ . Para el controlador y la barrera, los invariantes se definen como sigue

```
Inductive InvC: (S_Ck SC) -> Prop :=
  Isc1      : ∀y∈Clock (InvC (Sc1,y))
| Isc2      : ∀y∈Clock (le_Ck y kc1) -> (InvC (Sc2,y))
| Isc3      : ∀y∈Clock (InvC (Sc3,y))
| Isc4      : ∀y∈Clock (lt_Ck y kc2) -> (InvC (Sc4,y)).
```

```
Inductive InvG: (S_Ck SG) -> Prop :=
  Iopen      : ∀z∈Clock (InvG (Open,z))
| Ilowering  : ∀z∈Clock (lt_Ck z kg1) -> (InvG (Lowering,z))
| Iclosed    : ∀z∈Clock (InvG (Closed,z))
| Iraising   : ∀z∈Clock (lt_Ck z kg3) -> (InvG (Raising,z)).
```

Las transiciones son relaciones entre estados e involucran etiquetas. La especificación de éstas para cada uno de los tres sistemas componentes sigue la estructura descrita en la sección 3.2, con una pequeña modificación: no se exige el cumplimiento del invariante de las locaciones para el estado destino de una transición discreta. Esta simplificación es válida debido a que las transiciones discretas para cada uno de estos tres sistemas preservan el cumplimiento del invariante de las locaciones correspondiente. Formalmente esta simplificación se justifica probando que:  $SiniT \Rightarrow \forall \square InvT$ ,  $SiniC \Rightarrow \forall \square InvC$  y  $SiniG \Rightarrow \forall \square InvG$ ; donde,  $SiniT$ ,  $SiniC$  y  $SiniG$  son los estados iniciales del tren, el controlador y la barrea, respectivamente. Las demostraciones pueden consultarse en el apéndice C.2.4. Observemos que tanto las transiciones discretas como las temporales asumen que el estado de origen es *válido*, de acuerdo a lo establecido en la sección 3.2.

La figura 4.2 presenta los sistemas de transiciones para los tres componentes, según la notación introducida en el capítulo 2.



$$\begin{array}{c}
 \frac{}{\langle \text{Far}, x \rangle \xrightarrow{\text{Approach}}_T \langle \text{Near}, 0 \rangle} \\
 \frac{x < kt2}{\langle \text{Inside}, x \rangle \xrightarrow{\text{Exit}}_T \langle \text{Far}, x \rangle} \\
 \frac{}{\langle \text{Sc1}, y \rangle \xrightarrow{\text{Approach}}_C \langle \text{Sc2}, 0 \rangle} \\
 \frac{}{\langle \text{Sc3}, y \rangle \xrightarrow{\text{Exit}}_C \langle \text{Sc4}, 0 \rangle} \\
 \frac{\text{InvC}(sc, y + tick)}{\langle sc, y \rangle \xrightarrow{\text{Tick}}_C \langle sc, y + tick \rangle} \\
 \frac{}{\langle \text{Open}, z \rangle \xrightarrow{\text{Lower}}_G \langle \text{Lowering}, 0 \rangle} \\
 \frac{}{\langle \text{Closed}, z \rangle \xrightarrow{\text{Raise}}_G \langle \text{Raising}, 0 \rangle} \\
 \frac{\text{InvG}(sg, z + tick)}{\langle sg, z \rangle \xrightarrow{\text{Tick}}_G \langle sg, z + tick \rangle}
 \end{array}
 \qquad
 \begin{array}{c}
 \frac{kt1 < x < kt2}{\langle \text{Near}, x \rangle \xrightarrow{\text{In}}_T \langle \text{Inside}, x \rangle} \\
 \frac{\text{InvT}(st, x + tick)}{\langle st, x \rangle \xrightarrow{\text{Tick}}_T \langle st, x + tick \rangle} \\
 \frac{y = kc1}{\langle \text{Sc2}, y \rangle \xrightarrow{\text{Lower}}_C \langle \text{Sc3}, y \rangle} \\
 \frac{y < kc2}{\langle \text{Sc4}, y \rangle \xrightarrow{\text{Raise}}_C \langle \text{Sc1}, y \rangle} \\
 \frac{z < kg1}{\langle \text{Lowering}, z \rangle \xrightarrow{\text{Down}}_G \langle \text{Closed}, z \rangle} \\
 \frac{kg2 \leq z < kg3}{\langle \text{Raising}, z \rangle \xrightarrow{\text{Up}}_G \langle \text{Open}, z \rangle}
 \end{array}$$

**Fig. 4.2:** Transiciones del tren, el controlador y la barrera

En *Coq*, las transiciones discretas y temporales del tren se definen por la siguiente relación inductiva ( $\text{TrT}$  representa la relación  $\rightarrow_T$ ),

```

Inductive TrT : (S_Ck ST) -> Label -> (S_Ck ST) -> Prop :=
  ttApproach : ∀x∈Clock (TrT (Far,x) Approach (Near,Reset))
| ttIn       : ∀x∈Clock (gt_Ck x kt1) -> (lt_Ck x kt2) ->
                (TrT (Near,x) In (Inside,x))
| ttExit     : ∀x∈Clock (lt_Ck x kt2) -> (TrT (Inside,x) Exit (Far,x))
| ttTick     : ∀x∈Clock ∀s∈ST (InvT (s,(Inc x))) ->
                (TrT (s,x) Tick (s,(Inc x))).
    
```

*ttApproach* permite construir transiciones de la locación *Far* a la locación *Near* para cualquier valor del reloj (la condición de activación es *True*); *ttIn* de *Near* a *Inside* para los valores del reloj *x* que cumplen la conjunción de las condiciones  $(gt\_Ck \ x \ kt1)$  y  $(lt\_Ck \ x \ kt2)$ ; *ttExit* de *Inside* a *Far* para los valores del reloj *x*

que verifican la restricción  $(lt\_Ck \times kt2)$ ; finalmente,  $ttTick$  de una locación a ella misma incrementando el reloj en un *tick*, si el invariante se satisface para el nuevo valor.

Las transiciones para el controlador y la barrera se definen de manera similar ( $TrC$  representa a  $\rightarrow_C$  y  $TrG$  a  $\rightarrow_G$ ).

```

Inductive TrC : (S_Ck SC) -> Label -> (S_Ck SC) -> Prop :=
  TcApproach :  $\forall y \in \text{Clock}$  (TrC (Sc1,y) Approach (Sc2,Reset))
| tcLower    :  $\forall y \in \text{Clock}$  (eq_Ck y kc1) -> (TrC (Sc2,y) Lower (Sc3,y))
| tcExit     :  $\forall y \in \text{Clock}$  (TrC (Sc3,y) Exit (Sc4,Reset))
| tcRaise    :  $\forall y \in \text{Clock}$  (lt_Ck y kc2) -> (TrC (Sc4,y) Raise (Sc1,y))
| tcTick     :  $\forall y \in \text{Clock} \forall s \in SC$  (InvC (s,(Inc y))) ->
              (TrC (s,y) Tick (s,(Inc y))).

Inductive TrG : (S_Ck SG) -> Label -> (S_Ck SG) -> Set :=
  tgLower    :  $\forall z \in \text{Clock}$  (TrG (Open,z) Lower (Lowering,Reset))
| tgDown     :  $\forall z \in \text{Clock}$  (lt_Ck z kg1) ->
              (TrG (Lowering,z) Down (Closed,z))
| tgRaise    :  $\forall z \in \text{Clock}$  (TrG (Closed,z) Raise (Raising,Reset))
| tgUp       :  $\forall z \in \text{Clock}$  (ge_Ck z kg2) -> (lt_Ck z kg3) ->
              (TrG (Raising,z) Up (Open,z))
| tgTick     :  $\forall z \in \text{Clock} \forall s \in SG$  (InvG (s,(Inc z))) ->
              (TrG (s,z) Tick (s,(Inc z))).

```

Los estados del sistema compuesto TCG son una séxtupla, que definimos por el constructor de pares de tipos  $*$ .

```

Definition St_Global := (S_Ck ST) * (S_Ck SC) * (S_Ck SG).

```

Un estado de  $St\_Global$  consta de las locaciones y los valores de los relojes para cada uno de los tres sistemas componentes (esto equivale al producto de las locaciones y la unión de los relojes en el modelo de base).

**Notación.** Un elemento de tipo  $St\_Global$  es un par  $(st, (sc, sg))$  ( $*$  asocia a derecha). Sin embargo, para simplificar la notación, escribiremos la terna  $(st, sc, sg)$  por  $(st, (sc, sg))$ .

Las transiciones para grafos compuestos las especificamos teniendo en cuenta la definición de la sección 2.2. La figura 4.3 exhibe las transiciones del sistema TCG, según la notación del capítulo 2.

$$\begin{array}{c}
 \frac{\langle st, x \rangle \xrightarrow{In} \langle st', x' \rangle}{\langle \langle st, sc, sg \rangle, \langle x, y, z \rangle \rangle \xrightarrow{In} \langle \langle st', sc, sg \rangle, \langle x', y, z \rangle \rangle} \\
 \\
 \frac{\langle sg, z \rangle \xrightarrow{L} \langle sg', z' \rangle}{\langle \langle st, sc, sg \rangle, \langle x, y, z \rangle \rangle \xrightarrow{L} \langle \langle st, sc, sg' \rangle, \langle x, y, z' \rangle \rangle} \quad L \in \{Down, Up\} \\
 \\
 \frac{\langle st, x \rangle \xrightarrow{L} \langle st', x' \rangle \quad \langle sc, y \rangle \xrightarrow{L} \langle sc', y' \rangle}{\langle \langle st, sc, sg \rangle, \langle x, y, z \rangle \rangle \xrightarrow{L} \langle \langle st', sc', sg \rangle, \langle x', y', z' \rangle \rangle} \quad L \in \{Approach, Exit\} \\
 \\
 \frac{\langle sc, y \rangle \xrightarrow{L} \langle sc', y' \rangle \quad \langle sg, z \rangle \xrightarrow{L} \langle sg', z' \rangle}{\langle \langle st, sc, sg \rangle, \langle x, y, z \rangle \rangle \xrightarrow{L} \langle \langle st, sc', sg' \rangle, \langle x, y', z' \rangle \rangle} \quad L \in \{Lower, Raise\} \\
 \\
 \frac{\langle st, x \rangle \xrightarrow{Tick} \langle st', x' \rangle \quad \langle sc, y \rangle \xrightarrow{Tick} \langle sc', y' \rangle \quad \langle sg, z \rangle \xrightarrow{Tick} \langle sg', z' \rangle}{\langle \langle st, sc, sg \rangle, \langle x, y, z \rangle \rangle \xrightarrow{Tick} \langle \langle st', sc', sg' \rangle, \langle x', y', z' \rangle \rangle}
 \end{array}$$

Fig. 4.3: Transiciones del sistema compuesto TCG.

En *Coq*, la relación de transición entre estados de `St_Global` puede especificarse como sigue (`TrGlobal` representa la relación  $\rightarrow_{TCG}$ ):

```

Inductive TrGlobal : StGlobal -> Label -> StGlobal -> Prop :=
| tG1_In : ∀st1, st2 ∈ (S_Ck ST) (TrT st1 In st2) ->
  ∀sce ∈ (S_Ck SC) ∀sg ∈ (S_Ck SG)
  (TrGlobal (st1, sc, sg) In (st2, sc, sg))
| tG1_Down : ∀sg1, sg2 ∈ (S_Ck SG) (TrG sg1 Down sg2) ->
  ∀ste ∈ (S_Ck ST) ∀sce ∈ (S_Ck SC)
  (TrGlobal (st, sc, sg1) Down (st, sc, sg2))
| tG1_Up : ∀sg1, sg2 ∈ (S_Ck SG) (TrG sg1 Up sg2) ->
  ∀ste ∈ (S_Ck ST) ∀sce ∈ (S_Ck SC)
  (TrGlobal (st, sc, sg1) Up (st, sc, sg2))
| tG1_Approach : ∀st1, st2 ∈ (S_Ck ST) ∀sc1, sc2 ∈ (S_Ck SC)
  (TrT st1 Approach st2) -> (TrC sc1 Approach sc2) -> ∀sg ∈ (S_Ck SG)
  (TrGlobal (st1, sc1, sg) Approach (st2, sc2, sg))
| tG1_Exit : ∀st1, st2 ∈ (S_Ck ST) ∀sc1, sc2 ∈ (S_Ck SC)
  (TrT st1 Exit st2) -> (TrC sc1 Exit sc2) -> ∀sg ∈ (S_Ck SG)
  (TrGlobal (st1, sc1, sg) Exit (st2, sc2, sg))
    
```

```

| tGl_Lower : ∀sc1,sc2∈(S_Ck SC) (sg1,sg2:(S_Ck SG))
  (TrC sc1 Lower sc2) -> (TrG sg1 Lower sg2) -> ∀st∈(S_Ck ST)
  (TrGlobal (st,sc1,sg1) Lower (st,sc2,sg2))

| tGl_Raise : ∀sc1,sc2∈(S_Ck SC) ∀sg1,sg2∈(S_Ck SG)
  (TrC sc1 Raise sc2) -> (TrG sg1 Raise sg2) -> ∀st∈(S_Ck ST)
  (TrGlobal (st,sc1,sg1) Raise (st,sc2,sg2))

| tGl_Tick : ∀st1,st2∈(S_Ck ST) ∀sc1,sc2∈(S_Ck SC)
  ∀sg1,sg2∈(S_Ck SG)
  (TrT st1 Tick st2) -> (TrC sc1 Tick sc2) -> (TrG sg1 Tick sg2) ->
  (TrGlobal (st1,sc1,sg1) Tick (st2,sc2,sg2)).

```

$tGl\_In$  corresponde a la transición discreta del tren rotulada con  $In$ , en el sistema compuesto TCG;  $tGl\_Down$  y  $tGl\_Up$  a las de la barrera, rotuladas con  $Down$  y  $Up$ . Estas tres no son de sincronización, permiten modificar sólo la componente del estado que corresponde al grafo al cual pertenece la transición básica.  $tGl\_Approach$  y  $tGl\_Exit$  corresponden a las transiciones discretas que sincronizan el tren y el controlador con  $Approach$  y  $Exit$ .  $tGl\_Lower$  y  $tGl\_Raise$  a las que sincronizan el controlador y la barrera con  $Lower$  y  $Raise$ .  $tGl\_Tick$  representa a las transiciones temporales para el sistema TCG. La misma se especifica como de sincronización de las correspondientes a cada uno de los tres sistemas componentes. Esto es posible debido a que todos los incrementos temporales suman una misma cantidad (un *tick*). La condición asociada es la conjunción de los invariantes correspondientes a cada uno de los sistemas básicos. Luego, bajo la semántica de tiempo discreto asumida para la representación y el análisis de grafos temporizados, las transiciones temporales pueden ser tratadas igual que las discretas de sincronización.

El estado inicial para el sistema TCG se especifica a partir de los estados iniciales de cada uno de los grafos componentes. Esto es,

```

Definition SiniT : (S_Ck ST) := (Far,Ini_Ck).
Definition SiniC : (S_Ck SC) := (Sc1,Ini_Ck).
Definition SiniG : (S_Ck SG) := (Open,Ini_Ck).

Definition SiniTCG : StGlobal := (SiniT,SiniC,SiniG).

```

Observemos que el estado inicial de cada grafo temporizado satisface el *invariante* de las locaciones correspondiente (se cumple el requisito formulado en la sección 3.2). Esto es, valen  $InvT(SiniT)$ ,  $InvC(SiniC)$ ,  $InvG(SiniG)$  y obviamente el invariante  $InvTCG$  del sistema TCG para el estado compuesto  $SiniTCG$ . Donde,

```

Definition InvTCG := [s:StGlobal] Cases s of (st_x,sc_y,sg_z) =>
  ((InvT st_x) /\ (InvC sc_y) /\ (InvG sg_z)) end.

```

### 4.3 Análisis del Sistema TCG

En esta parte del trabajo estamos interesados en analizar la demostración de dos clases típicas de propiedades: *safety* y *liveness*. Las primeras se usan para especificar que “nada malo ocurrirá durante cierto tiempo”. Las mismas se formulan, generalmente, mediante el operador  $\Box_I$ . Las propiedades de *liveness* permiten especificar que “algo bueno ocurrirá dentro de un intervalo de tiempo especificado”. Estas se formalizan, generalmente, mediante el operador  $\Diamond_I$ . Una definición formal de propiedades de *safety* y *liveness* fue dada por Alpern y Shneider en [AS85], donde ellos muestran que cualquier propiedad de una traza (ejecución) puede ser expresada como una conjunción de una propiedad de *safety* y una de *liveness*.

Un requerimiento de seguridad asociado al sistema TCG es la propiedad de *safety* “siempre que el tren está cruzando el paso a nivel, la barrera se encuentra baja”. Observemos que aunque esta propiedad es puramente *cualitativa*, la misma no vale si eliminamos las restricciones temporales o cambiamos ciertos valores de las mismas. Una propiedad esencial de todo sistema es la propiedad de *liveness* “*sistema bien temporizado*”, la cual asegura que el tiempo diverge en todas las ejecuciones del sistema (ver sección 2.1.2). En las dos próximas subsecciones analizaremos la demostración de propiedades *invariantes*, incluyendo la propiedad de *safety* previamente descrita. La propiedad “*sistema bien temporizado*”, para el sistema TCG, será tratada en la sección 4.3.3.

#### 4.3.1 Demostración de Invariantes

Para verificar una propiedad del tipo  $Q \Rightarrow \forall \Box_I P$  sobre un grafo temporizado  $G$  podemos proceder según analizamos en la sección 2.5.3. Esto equivale, según la formalización de  $G$  y la definición con tipos inductivos del operador  $\forall \Box$ , a hacer inducción sobre el conjunto de estados alcanzables y la definición de las transiciones. En esta sección analizaremos la prueba de invariantes para el sistema TCG, los cuales nos permitirán adquirir un conocimiento mayor del sistema, a fin de analizar otras propiedades más complejas, por ejemplo la de “*sistema bien temporizado*”. Para nuestro caso de estudio el intervalo  $I$  no será significativo, esto es  $I=[0, \infty)$  –usaremos la versión no acotada de  $\forall \Box$ . Adoptaremos la formalización con tipos inductivos del operador  $\forall \Box$  dada en 3.3.2, en vez de la correspondiente con tipos co-inductivos presentada en 3.4.2 (aunque los mismos resultados se siguen de ambas representaciones).

#### Invariantes

Seguidamente describimos algunas de las propiedades invariantes analizadas del sistema TCG. Las mismas fueron demostradas con el asistente de pruebas *Coq* y la utilización de algunas tácticas especialmente definidas para este caso de estudio.

En las demostraciones de las propiedades hacemos uso de una de las principales ventajas de los métodos deductivos, la *composicionalidad* de las pruebas. Esto es, algunos invariantes (y teoremas en general) serán utilizados en las demostraciones de otros invariantes u otra clase de propiedades.

La especificación de una propiedad invariante  $Inv_i$  del sistema TCG corresponde a la fórmula  $Init \Rightarrow \forall \square Inv_i$ . Donde  $Init$  es el predicado que caracteriza al estado inicial del sistema:  $SiniTCG$ .

Adoptaremos la siguiente abreviatura para el operador  $ForAll$  sobre propiedades del sistema TCG:

```
Definition ForAll_TCG: StGlobal -> (StGlobal->Prop) -> Prop :=
  (ForAll TrGlobal).
```

Dado un estado  $Sini$  y una propiedad  $Inv_i$ ,  $ForAll\_TCG$  especifica que todos los estados (de tipo  $StGlobal$ ) alcanzables desde el estado  $Sini$  (con transiciones de tipo  $TrGlobal$ ) satisfacen  $Inv_i$ . Luego, la demostración de una propiedad

$$Init \Rightarrow \forall \square Inv_i$$

corresponderá a la prueba de un lema en *Coq*, que puede enunciarse como sigue:

```
Lemma lema_Inv_i : (ForAll_TCG SiniTCG Inv_i).
```

A continuación enunciamos los invariantes analizados del sistema TCG, las demostraciones son omitidas y pueden consultarse en el apéndice C.2.4.

- *Invariante 1.*

```
Definition Inv_1 := [s:StGlobal] Cases s of ((st,_),(sc,_),(sg,_)) =>
  st=Near \ / st=Inside -> sc=Sc3 -> sg=Closed \ / sg=Lowering end.
```

Esto es, siempre se cumple que si el tren está próximo a cruzar ( $st=Near$ ) o está cruzando ( $st=Inside$ ) el paso a nivel, y el controlador está esperando la señal *exit* ( $sc=Sc3$ ), la barrera se encuentra baja ( $sg=Closed$ ) o está descendiendo ( $sg=Lowering$ ).

- *Invariante 2.*

```
Definition Inv_2 := [s:StGlobal] Cases s of ((st,_),(sc,_),(sg,_)) =>
  st=Far -> sg=Open \ / sg=Raising -> sc=Sc1 end.
```

Siempre se cumple que: si el tren está lejos –no hay un tren próximo ni cruzando– ( $st=Far$ ) y la barrera está arriba ( $sg=Open$ ) o levantándose ( $sg=Raising$ ), entonces el controlador permanece a la espera de la señal *Approach* de un nuevo tren ( $sc=Sc1$ ).

- *Invariante 3.*

```
Definition Inv3 := [s:StGlobal] Cases s of ((st,x),(_,y),_) =>
  st=Near \ / st=Inside -> (eq_Ck x y) end.
```

Siempre se cumple que: si el tren está próximo a cruzar ( $st=Near$ ) o está cruzando ( $st=Inside$ ) el paso a nivel, los valores de los relojes de ambos sistemas coinciden (ambos relojes son inicializados al mismo tiempo cuando el tren y el controlador se comunican a través de la señal *Approach*). Esta propiedad se relaciona más con la formalización del problema que con el problema en sí. La misma es utilizada para demostrar otras propiedades más relevantes del sistema.

- *Invariante 4.*

```
Definition Inv4 := [s:StGlobal] Cases s of ((st,_),(sc,_),_) =>
  st=Near -> sc=Sc2 \ / sc=Sc3 end.
```

Siempre se cumple que: si el tren está próximo a cruzar el paso a nivel ( $st=Near$ ) entonces el controlador ha recibido la señal *Approach*, aunque no ha enviado aún la señal *lower* ( $sc=Sc2$ ), o bien si la envió y está esperando la señal *exit* del tren ( $sc=Sc3$ ).

- *Invariante 5.*

```
Definition Inv5 := [s:StGlobal] Cases s of ((st,_),(sc,y),(_,z)) =>
  st=Near -> sc=Sc3 -> (eq_Ck y (plus_Ck z kc1)) end.
```

Siempre se cumple que: si el tren está próximo a cruzar el paso a nivel ( $st=Near$ ) y el controlador está esperando la señal *exit* del tren ( $sc=Sc3$ ), el tiempo transcurrido desde que la señal *Approach* fue procesada por el controlador excede en  $kc1$  unidades al tiempo que pasó desde que la barrera comenzó a bajar. Esto se observa intuitivamente a partir de la transición que sincroniza el controlador y la barrera con *lower*.

- *Invariante 6.*

```
Definition Inv6 := [s:StGlobal] Cases s of ((st,x),(sc,_),_) =>
  st=Near \ / (gt_Ck x kc1) \ / st=Inside -> sc=Sc3 end.
```

Siempre se cumple que: si el tren está próximo a cruzar el paso a nivel ( $st=Near$ ) y el tiempo transcurrido en ese estado (desde el origen de la señal *Approach*) superó ya  $kc1$

unidades, o bien el tren está cruzando el paso a nivel ( $st=Inside$ ), entonces el controlador se encuentra esperando la señal *exit* y ha enviado la señal *lower* a la barrera ( $sc=Sc3$ ).

- *Invariante 7.*

```
Definition Inv7 := [s:StGlobal] Cases s of ((st,_),(sc,_),(sg,_)) =>
  st=Near \ / st=Inside -> sc=Sc3 -> sg=Lowering \ / sg=Closed end.
```

Siempre se cumple que: si el tren está próximo a cruzar ( $st=Near$ ) o está cruzando el paso a nivel ( $st=Inside$ ), y el controlador está esperando la señal *exit* y ha enviado ya la señal *lower* a la barrera, entonces ésta se encuentra descendiendo ( $sg=Lowering$ ) o está baja ( $sg=Closed$ ).

- *Invariante 8.*

```
Definition Inv8 := [s:StGlobal] Cases s of ((st,x),(sc,_),(sg,_)) =>
  st=Near \ / (gt_Ck x kt1) \ / st=Inside -> sg=Closed end.
```

Siempre se cumple que: si el tren está próximo a cruzar el paso a nivel ( $st=Near$ ) y el tiempo transcurrido en ese estado (desde el origen de la señal *Approach*) superó ya  $kt1$  unidades, o bien el tren está cruzando el paso a nivel ( $st=Inside$ ), entonces la barrera se encuentra baja ( $sg=Closed$ ). Este invariante asegura la satisfacción de la propiedad de seguridad más importante del sistema.

- *Invariante 9.*

```
Definition Inv9 := [s:StGlobal] Cases s of ((st,x),(_,y),(_,z)) =>
  st=Near \ / (gt_Ck x kc1) \ / st=Inside -> (eq_Ck y (plus_Ck z kc1)) end.
```

Siempre se cumple que: si el tren está próximo a cruzar el paso a nivel ( $st=Near$ ) y el tiempo transcurrido en ese estado (desde el origen de la señal *Approach*) superó ya  $kc1$  unidades, o bien el tren está cruzando el paso a nivel ( $st=Inside$ ), entonces el tiempo transcurrido desde que la señal *Approach* fue procesada por el controlador excede en  $kc1$  unidades al tiempo que pasó desde que la barrera comenzó a bajar.

- *Invariante 10.*

```
Definition Inv10 := [s:StGlobal] Cases s of (_, (sc,_), (sg,_)) =>
  sc=Sc1 \ / sc=Sc2 -> sg=Open \ / sg=Raising end.
```



Siempre se cumple que: si el controlador está esperando la señal *Approach* del tren ( $sc=Sc1$ ) o ya la recibió pero aún no envió la señal *lower* a la barrea ( $sc=Sc2$ ), entonces ésta se encuentra alta ( $sg=Open$ ) o está levantándose ( $sg=Raising$ ).

- *Invariante 11.*

```
Definition Inv11 := [s:StGlobal] Cases s of (_, (sc, _), (sg, _)) =>
  sg=Lowering /\ sg=Closed -> sc=Sc3 /\ sc=Sc4 end.
```

Esta propiedad expresa básicamente lo mismo que el invariante *Inv<sub>10</sub>* (es en cierto sentido su contra-recíproco). La misma se demuestra a través del teorema *Mon\_I* (ver sección 3.3.3), que permite probar invariantes a partir de otros invariantes cuando existe una relación de consecuencia entre dichas fórmulas.

- *Invariante 12.*

```
Definition Inv12 := [s:StGlobal] Cases s of (_, (sc, y), (_, z)) =>
  sc=Sc2 -> (ge_Ck z y) end.
```

Siempre se cumple que: si el controlador recibió la señal *Approach* pero aún no envió la señal *lower* a la barrea ( $sc=Sc2$ ), el tiempo transcurrido desde que la barrera comenzó a subir la última vez es por lo menos el tiempo que pasó desde que el controlador procesó la señal *Approach*.

- *Invariante 13.*

```
Definition Inv13 := [s:StGlobal] Cases s of ((st, _), (sc, _), _) =>
  sc=Sc2 -> st=Near end.
```

Siempre se cumple que: si el controlador recibió la señal *Approach* pero aún no envió la señal *lower* a la barrea ( $sc=Sc2$ ), entonces el tren se encuentra en el estado próximo a cruzar el paso a nivel ( $sc=Near$ ).

- *Invariante 14.*

```
Definition Inv14 := [s:StGlobal] Cases s of ((st, _), (sc, _), (sg, _)) =>
  sc=Sc4 -> st=Far /\ sg=Closed end.
```

Siempre se cumple que: si el controlador recibió la señal *exit* del tren pero aún no envió la señal *raise* a la barrea ( $sc=Sc4$ ), entonces el tren se encuentra lejos –no hay un tren próximo ni cruzando– y la barrera está baja.

- *Invariante 15.*

```
Definition InvSc3 := [s:StGlobal] Cases s of (_, (sc, y), _) =>
  sc=Sc3 -> (ge_Ck y kc1) end.
```

Siempre se cumple que: si el controlador está esperando la señal *exit*, el tiempo transcurrido desde el comienzo de la aproximación del tren al paso a nivel (origen de la señal *Approach*) es por lo menos *kc1* unidades.

- *Invariante 16.*

```
Definition InvInside := [s:StGlobal] Cases s of ((st, x), _) =>
  st=Inside -> (gt_Ck x kt1) end.
```

Siempre se cumple que: si el tren está cruzando el paso a nivel, el tiempo transcurrido desde que comenzó su aproximación al cruce (origen de la señal *Approach*) excede *kt1* unidades.

## Comentarios

Aunque no usamos la versión acotada del operador  $\forall\Box$ , muchas de las propiedades invariantes previas expresan restricciones cuantitativas de tiempo. Por ejemplo, para indicar el tiempo transcurrido desde un evento (una señal) –invariantes 15 y 16– o el tiempo de separación entre dos eventos –invariantes 5, 9 y 12. Otros invariantes reflejan propiedades básicamente cualitativas que relacionan las locaciones de los estados posibles –invariantes 1, 2, 4, 7, 10, 11, 13 y 14. Finalmente, existen propiedades que son al mismo tiempo cualitativas y cuantitativas, según la clasificación previa. Por ejemplo, los invariantes 6 y 8.

## Algunas Tácticas (Simples) Útiles

Una táctica de prueba en *Coq* permite abreviar un esquema de demostración. Las tácticas implementan razonamiento “hacia atrás”, es decir, la clase de razonamiento “para probar una meta *M* es necesario probar esto y esto...” [Bar<sup>+</sup>99]. Si bien existen varios niveles en los que se clasifican las tácticas, nosotros consideraremos tácticas básicas (simples) que incluyen (posiblemente) a otras tácticas básicas.

A continuación describimos algunas de ellas a modo de ejemplo. El conjunto completo de tácticas utilizadas en el análisis del sistema TCG puede ser consultado en el apéndice C.2.3.

La táctica `BeginForAll` permite inicializar una prueba para el operador  $\forall\Box$  formalizado con tipos inductivos (`ForAll`). La misma aplica inducción sobre el conjunto de estados alcanzables (de `RState`), y luego simplifica y trata de probar el caso base –la propiedad para el estado inicial– con la táctica `Simpl` y la táctica `Easy`. Esta última

táctica intenta probar un objetivo usando la táctica `Discriminate` y posteriormente, si esta no tiene éxito, la táctica automática `Auto`.

```
Tactic Definition BeginForAll :=
  [<tactic:<
    Unfold ForAll; Induction 1; [Simpl; Intros; Easy | Idtac]
  >>].
```

Las tácticas `SplitTrans` y `SplitTrans_Simpl` simplifican la prueba por inducción de una propiedad  $P$  sobre los estados alcanzables (de `RState`) para los pasos inductivos, con `TrGlobal` el tipo de las transiciones. Estas tácticas se usan en las pruebas luego de haber aplicado la táctica `BeginForAll` y probado el caso base. Esto es, simplifican las pruebas del tipo  $P \wedge B_i \Rightarrow wp(S_i, P)$  para toda transición cuya condición de activación es  $B_i$  y su efecto en el estado del sistema está determinado por  $S_i$ . Las dos tácticas intentan probar automáticamente las implicaciones para algunos casos triviales de antecedente falso, consecuente verdadero o donde la prueba del consecuente se sigue trivialmente del antecedente. Los casos a considerar son ocho, uno para cada transición de `TrGlobal` (siete transiciones discretas y una que representa a las transiciones temporales).

```
Tactic Definition SplitTrans :=
  [<tactic:<
    Intros s1 s2 l rs_s1 p_s1 tr_gl;
    (Generalize rs_s1; Clear rs_s1);
    (Generalize p_s1; Clear p_s1);
    Elim tr_gl
  >>].
```

```
Tactic Definition SplitTrans_Simpl :=
  [<tactic:<
    SplitTrans; [Simpl_In | Simpl_Down | Simpl_Up | Simpl_Approach |
    Simpl_Exit | Simpl_Lower | Simpl_Raise | Simpl_Tick]
  >>].
```

Las tácticas `Simpl_In`, `Simpl_Down`, `Simpl_Up`, `Simpl_Approach`, `Simpl_Exit`, `Simpl_Lower`, `Simpl_Raise` y `Simpl_Tick` permiten simplificar las instancias correspondientes de  $P \wedge B_i \Rightarrow wp(S_i, P)$ . Estas tácticas podrían ser reducidas a tres si agrupamos las transiciones que no sincronizan, las que sincronizan dos componentes y las que sincronizan tres (esto último para el caso de las transiciones temporales). Sin embargo, definimos una para cada transición a fin de poder usar lemas de inversión particulares. Estos lemas definen principios de análisis de casos para subfamilias [Bar<sup>+</sup>99]. El uso de lemas de inversión nos permite evitar repetir una misma prueba de inversión en la

demostración de distintas propiedades (o de una misma), logrando de esta manera reducir el tamaño de los términos de prueba y obtener mayor claridad sobre los mismos.

Tres de las ocho tácticas se enuncian a continuación: `Simpl_In` simplifica el caso correspondiente a una transición etiquetada con `In` –que no es de sincronismo–; `Simpl_Approach` simplifica el caso correspondiente a una transición de sincronismo etiquetada con `Approach`; y, `Simpl_Tick` simplifica el caso correspondiente a una transición de sincronismo entre los tres sistemas etiquetada con `Tick`.

Tactic Definition **Simpl\_In** :=

```
[<:tactic:<
  Intros st1 st2 trt_In;
  Inversion trt_In using cl_TRT_IN;
  Intros x gt_x_kt1 lt_x_kt2 sc sg;
  Elim sc; Elim sg;
  Simpl; Intros; Easy
>>].
```

Tactic Definition **Simpl\_Approach** :=

```
[<:tactic:<
  Intros st1 st2 sc1 sc2 trt_Approach trc_Approach;
  Inversion trt_Approach using cl_TRT_APPROACH;
  Inversion trc_Approach using cl_TRC_APPROACH;
  Intros y x sg;
  Elim sg;
  Simpl; Intros; Easy
>>].
```

Tactic Definition **Simpl\_Tick** :=

```
[<:tactic:<
  Intros st1 st2 sc1 sc2 sg1 sg2 trt_Tick trc_Tick trg_Tick;
  Inversion trt_Tick using cl_TRT_INC_TIME;
  Inversion trc_Tick using cl_TRC_INC_TIME;
  Inversion trg_Tick using cl_TRG_INC_TIME;
  Simpl; Intros; Easy
>>].
```

Los lemas de inversión: `cl_TRT_IN`, `cl_TRT_APPROACH`, `cl_TRC_APPROACH`, `cl_TRT_INC_TIME`, `cl_TRC_INC_TIME` y `cl_TRG_INC_TIME` son generados por las siguientes declaraciones *Coq*

```

Derive Inversion_clear cl_TRT_IN with (st1,st2:(S_Ck ST))
  (TrT st1 In st2) Sort Prop.

Derive Inversion_clear cl_TRT_APPROACH with (st1,st2:(S_Ck ST))
  (TrT st1 Approach st2) Sort Prop.

Derive Inversion_clear cl_TRC_APPROACH with (sc1,sc2:(S_Ck SC))
  (TrC sc1 Approach sc2) Sort Prop.

Derive Inversion_clear cl_TRT_INC_TIME with (st1,st2:(S_Ck ST))
  (TrT st1 Tick st2) Sort Prop.

Derive Inversion_clear cl_TRC_INC_TIME with (sc1,sc2:(S_Ck SC))
  (TrC sc1 Tick sc2) Sort Prop.

Derive Inversion_clear cl_TRG_INC_TIME with (sg1,sg2:(S_Ck SG))
  (TrG sg1 Tick sg2) Sort Prop.

```

El conjunto completo de lemas de inversión utilizados puede consultarse en el apéndice C.2.2.

**Ejemplo 4.1.** La demostración del invariante  $Inv_1$  corresponde a probar el siguiente lema:

Lemma **lema\_Inv<sub>1</sub>** : (ForAll\_TCG  $Inv_1$  SiniTCG).

Este lema se demuestra fácilmente por inducción en los estados alcanzables utilizando algunas de las tácticas desarrolladas.

```

Proof.
  BeginForAll.
  SplitTrans_Simpl.
  Simpl_or (p_s1 H0 H1).
Qed.

```

Observemos que luego de aplicar las tácticas `BeginForAll` y `SplitTrans_Simpl`, la propiedad para el caso base fue probada (con `BeginForAll`) y de las ocho transiciones del sistema TCG sólo una necesitó la aplicación de tácticas adicionales (la transición etiquetada con *Up*). `Simpl_or` aplica el principio de eliminación a su argumento (en general, una disyunción) y luego intenta probar la meta con la táctica `Easy`.

### 4.3.2 Propiedad Fundamental de Safety

El requerimiento de seguridad más importante del sistema es: “*siempre que el tren este cruzando el paso a nivel, la barrera debe estar baja*”. Este puede ser formalizado como una propiedad de *safety* a través del siguiente invariante:

```
Definition safeTCG := [s:StGlobal] Cases s of ((st,_),_,(sg,_)) =>
  st=Inside -> sg=Closed end.
```

La demostración de  $Init \Rightarrow \forall \square safeTCG$  corresponde a probar el siguiente lema:

```
Lemma lema_safeTCG : (ForAll_TCG SiniTCG safeTCG).
```

La demostración se sigue del invariante  $Inv_8$ , que es más general que la propiedad  $safeTCG$ , ya que no sólo asegura que cuando el tren está cruzando el paso a nivel la barrera está baja, sino que también luego de que han pasado más de  $k+1$  unidades de tiempo desde que el tren comenzó a aproximarse al cruce (origen de la señal *Approach*). La prueba usa el teorema  $Mon_I$  (ver sección 3.3.3), ya que vale:  $Inv_8 \Rightarrow safeTCG$ . La misma puede consultarse en el apéndice C.2.4.

Algunos de los invariantes formulados en la sección previa especifican propiedades relevantes para el análisis de  $safeTCG$ , los mismos fueron concebidos a partir de las condiciones de prueba necesarias para la demostración de esta propiedad de *safety*. Sin embargo, no se usaron técnicas de deducción automática de invariantes para este caso de estudio.

### 4.3.3 Propiedad de Liveness Non-Zeno

El interés fundamental en el proceso de verificación del sistema TCG residió en la demostración de invariantes. Estos permiten describir el comportamiento del sistema en cualquier estado en el cual éste se encuentre. Los invariantes, como vimos en la sección previa, permiten establecer propiedades de *safety* y como veremos en esta sección, ayudan a demostrar también otro tipo de propiedades, como las de *liveness*. En esta sección estamos particularmente interesados en el análisis de la propiedad de *liveness Non-Zeno* (“*sistema bien temporizado*”). Esta propiedad asegura que el tiempo no se bloquea, diverge en todas las ejecuciones del sistema. La importancia de *Non-Zeno* para un sistema de tiempo real fue destacada en la sección 2.1.2. *Non-Zeno* puede ser descripta por la siguiente fórmula TCTL:

$$Init \Rightarrow \forall \square \exists \diamond_{=1} True$$

Es decir, desde cualquier estado alcanzable del sistema es posible alcanzar un nuevo estado, habiendo transcurrido un tiempo estrictamente positivo. Esta propiedad puede especificarse en *Coq* para el sistema TCG a través de las formalizaciones introducidas en

el capítulo 3 (en particular, las que corresponden a las definiciones de los operadores con tipos inductivos), como sigue:

```
Lemma NonZeno : (ForAll_TCG SiniTCG
  ( [s:StGlobal] (Exists_T_TCG s ([_:StGlobal] True) (eq_Ck tick)) ) ).
```

La especificación de “puede avanzar” es expresada a través del incremento de un *tick* (condición que es equivalente a  $(gt\_Ck\ 0)$ ). `Exists_T_TCG` es la abreviatura

```
Definition Exists_T_TCG : StGlobal -> (StGlobal->Prop) -> Prop :=
  (Exists_T TrGlobal).
```

Una formalización equivalente a la anterior que hace uso de la versión no acotada del operador  $\exists\Diamond$  puede expresarse como sigue,

```
Lemma NonZeno : (ForAll_TCG SiniTCG
  ( [s:StGlobal] (Exists_TCG s InvTick) ) ).
```

donde, `InvTick` es la condición de habilitación para la transición temporal del sistema TCG (“el tiempo puede avanzar”) y `Exists_TCG` es una abreviatura. Formalmente,

```
Definition InvTick := [s:StGlobal] Cases s of ((st,x),(sc,y),(sg,z)) =>
  ( InvTCG ((st,(Inc x)),(sc,(Inc y)),(sg,(Inc z))) ) end.
```

```
Definition Exists_TCG: StGlobal -> (StGlobal->Prop) -> Prop :=
  (Exists TrGlobal).
```

Para la demostración de *Non-Zeno* adoptamos su segunda formalización, que corresponde a la fórmula TCTL  $Init \Rightarrow \forall\Box\exists\Diamond InvTick$ . La estructura general de la prueba corresponde a una inducción en los estados alcanzables (desde el estado inicial `SiniTCG`) y las transiciones del sistema TCG, en función del operador  $\forall\Box$ . La propiedad a verificar en cada instancia corresponde a la construcción de un camino hacia un estado a partir del cual es posible incrementar el tiempo ( $\exists\Diamond InvTick$ ). En este proceso se utilizaron los invariantes y las tácticas especificadas en la sección previa. Asimismo, se formularon abreviaciones y tácticas específicas, y se utilizó el teorema `StepsEX` introducido en la sección 3.3.3.

En la demostración, el análisis para la transición temporal resultó más complejo que en los otros casos. La prueba en este punto se divide en dos partes según el principio del tercero excluido: vale *InvTick* en el estado alcanzable por la transición temporal –la prueba se sigue trivialmente en este caso– o no vale *InvTick* y entonces la prueba se sigue por análisis de casos de las situaciones posibles: las que pueden violar los invariantes de las locaciones. Por ejemplo, el tren podría estar en la locación *Near* y el valor del reloj

podría superar, luego del incremento, la constante  $kt2$ , pero entonces sabríamos que el valor sin incrementar del reloj sería mayor que la constante  $kt1$ . Notemos sin embargo, que si  $InvTick$  valiera para el controlador y la barrera, el tren no podría estar en la locación  $Far$ , pues su invariante es  $True$ . Los casos considerados son seis y relacionan las locaciones cuyos invariantes no son  $True$  (ver el lema `noInvTick` en el apéndice C.2.5 –sección: lemas, definiciones y tácticas auxiliares–). La demostración completa de *Non-Zeno* puede consultarse en el apéndice C.2.5 –sección: demostración de *Non-Zeno*.

### Un Sistema Mal Temporizado

El sistema de “control de un paso a nivel de tren” presentado en [AD94] –tomado de base en este trabajo– difiere del presentado en la sección 4.1 únicamente en la condición de activación para la transición de la barrera, rotulada con  $Up$ , que vincula las locaciones  $Raising$  y  $Open$ . En [AD94] esta condición es  $kg2 < z < kg3$ , mientras que en la formulación del problema dada en la sección 4.1 la misma es debilitada a  $kg2 \leq z < kg3$ .

En este trabajo:

$$\frac{kg2 \leq z < kg3}{\langle Raising, z \rangle \xrightarrow{Up}_G \langle Open, z \rangle}$$

En [AD94]:

$$\frac{kg2 < z < kg3}{\langle Raising, z \rangle \xrightarrow{Up}_G \langle Open, z \rangle}$$

**Fig. 4.4:** Diferencia con la formalización dada en [AD94]

La modificación previa fue introducida en este trabajo debido a que la propiedad *Non-Zeno* para el sistema presentado en [AD94] no se cumple. La especificación del sistema original no garantiza que el tiempo diverge en todas las ejecuciones. A partir del análisis de *Non-Zeno* para dicho sistema dedujimos una condición suficiente que nos permitió transformar el sistema mal temporizado en el sistema bien temporizado analizado en este capítulo. La condición suficiente es precisamente la que distingue a ambas versiones y fue deducida en la etapa de prueba de *Non-Zeno* que corresponde al análisis de la transición temporal.

Un contra-ejemplo para el sistema original está dado por la siguiente traza de ejecución, generada a partir del estado inicial  $SiniTCG = ((Far,0),(Sc1,0),(Open,0))$ :

$$\begin{array}{l} ((Far,0),(Sc1,0),(Open,0)) \xrightarrow{App} ((Near,0),(Sc2,0),(Open,0)) \xrightarrow{t=1} \\ ((Near,1),(Sc2,1),(Open,1)) \xrightarrow{Lower} ((Near,1),(Sc3,1),(Lowering,0)) \xrightarrow{Down} \\ ((Near,1),(Sc3,1),(Closed,0)) \xrightarrow{t=2} ((Near,3),(Sc3,3),(Closed,2)) \xrightarrow{In} \\ ((Inside,3),(Sc3,3),(Closed,2)) \xrightarrow{Exit} ((Far,3),(Sc4,0),(Closed,2)) \xrightarrow{Raise} \\ ((Far,3),(Sc1,0),(Raising,0)) \xrightarrow{Approach} ((Near,0),(Sc2,0),(Raising,0)) \xrightarrow{t=1} \\ ((Near,1),(Sc2,1),(Raising,1)) \end{array}$$



El estado  $((Near,1),(Sc2,1),(Raising,1))$  es alcanzable a partir de *SiniTCG*, sin embargo ninguna transición está habilitada para este estado en el sistema presentado en [AD94]. La modificación al sistema introducida en este trabajo garantiza, en particular, que la transición *Up* está habilitada en este punto y, en general, que *Non-Zeno* vale.

#### 4.3.4 Acerca de los Términos de Prueba

El tamaño de los términos de prueba de los invariantes analizados es proporcional a la suma de los tamaños de las demostraciones para las transiciones del sistema compuesto (hacemos inducción en el conjunto de estados alcanzables). Para la propiedad de *safety*, se sigue del invariante  $Inv_8$ . El tamaño del término de prueba para *NonZeno* es proporcional a la suma de los tamaños de los caminos construidos a partir de cada transición del sistema compuesto. La longitud de estos caminos no supera la construcción de tres pasos o transiciones –salvo para el análisis de la transición temporal– y si bien fue necesario hacer análisis de casos sobre las locaciones de los estados, nunca se analizaron simultáneamente todos los casos para los tres sistemas componentes; se usaron los invariantes demostrados para deducir los valores de algunas locaciones y ciertas condiciones de los relojes. El camino de prueba de mayor costo corresponde al de la transición temporal, ya que este se dividió en seis a partir del caso en que no vale *InvTick* (ver sección 4.3.3).

Para simplificar la construcción de las pruebas se desarrollaron tácticas (ver sección 4.3.1) que automatizan ciertas partes de las mismas. Estas si bien permiten reducir el *script* de prueba –lista de tácticas usadas en la demostración–, no reducen el tamaño de los términos de prueba. Para el caso de estudio de este capítulo algunas decisiones tomadas condujeron a disminuir el tamaño de los términos de prueba para las propiedades analizadas:

- Uso de lemas de inversión para las transiciones y los invariantes de las locaciones. El desarrollo de estos lemas nos permite evitar repetir más de una vez en las pruebas el principio de análisis de casos para algunas subfamilias (ver sección 4.3.1).
- Abstracción en las transiciones discretas de la condición que establece que el invariante de la locación destino de las transiciones se satisface (ver sección 4.2). Esta es una simplificación sobre el formato establecido en la sección 3.2.
- Definición particular de la relación de transición para el sistema compuesto. La definición de composición de transiciones puede ser expresada con un operador genérico, como veremos en el capítulo 5, pero de esta manera se incrementan los tamaños y oscurece la estructura de las pruebas, si no se implementan tácticas adicionales.

- Utilización de la formalización de estados alcanzables que no explicita que los estados iniciales deben satisfacer los invariantes de las locaciones (ver discusión en la sección 3.3.2).  $\text{InvTCG}$  vale para el estado inicial considerado en cada propiedad analizada:  $\text{SiniTCG}$ .
- Utilización de un conjunto global de etiquetas en vez de conjuntos particulares para cada subsistema. Esta discusión fue planteada a nivel general en la sección 3.2, de acuerdo a la hipótesis establecida en la sección 2.1.

## 4.4 Parametrización del Sistema TCG

En esta sección mostramos una posible generalización de la especificación del sistema presentado en la sección 4.1 que preserva las propiedades analizadas del mismo. El objetivo es poder definir una familia de sistemas que cumplan las propiedades de interés; donde el sistema especificado al comienzo de este capítulo sea un miembro particular de la familia.

Para la formulación de las propiedades analizadas a lo largo de la sección 4.3 consideramos los valores de las constantes del sistema TCG especificados en [AD94] multiplicados por cuatro, tal como lo señalamos en la sección 4.1. En la demostración de las propiedades consideramos lemas especiales para aquellas demostraciones que involucran relaciones elementales (triviales) entre los valores de las constantes y los relojes del sistema. El conjunto completo de lemas, con sus demostraciones, se incluye en el apéndice C.2.1. A continuación exhibimos algunos ejemplos.

Lemma Trivial6 :  $\forall x, y \in \text{Clock} \text{ (ge\_Ck } x \ y \rightarrow \text{ (ge\_Ck (Inc } x) \text{ (Inc } y) ) .}$

Lemma Trivial10 :  $\forall x \in \text{Clock} \text{ (gt\_Ck } x \text{ kt1} \rightarrow \text{ (gt\_Ck } x \text{ kc1} ) .}$

Lemma Trivial12 :  $\forall x, y \in \text{Clock} \text{ (gt\_Ck (Inc } x) \ y \rightarrow \text{ (eq\_Ck } x \ y) \ \wedge \ \text{ (gt\_Ck } x \ y) .}$

Lemma Trivial18 :  $\text{ (lt\_Ck (Inc Reset) kc2) .}$

Lemma Trivial30 :  $\forall x \in \text{Clock} \text{ (lt\_Ck } x \text{ kg2} \rightarrow \text{ (lt\_Ck (Inc } x) \text{ kg3) .}$

Trivial6 es una de las propiedades elementales acerca de las relaciones binarias de comparación y la operación de incremento temporal. Trivial10 establece una relación entre valores constantes del sistema:  $\text{kt1} \geq \text{kc1}$ . Trivial12 es una propiedad fundamental de la discretización que expresa que los incrementos temporales son los mínimos para el dominio elegido ( $\angle$  en este caso). Esta propiedad podría ser considerada un axioma de la discretización si deseáramos axiomatizar la estructura temporal. Trivial18 expresa que la constante  $\text{tick}$  es menor que  $\text{kc2}$ ; esta propiedad vale por el factor de discretización elegido  $\delta = 1/M$ , donde  $M$  es la constante en base a la cual aumentamos la escala del problema. Trivial30 es otra relación entre constantes del problema que expresa la condición:  $\text{kg3} > \text{kg2}$ .

Muchas de estas propiedades se demuestran fácilmente a partir de la estructura temporal elegida ( $\angle$  y las relaciones binarias de comparación habituales), teniendo en cuenta el factor de multiplicación de escala  $M$ . Por ejemplo `Trivial16`, `Trivial112` y `Trivial118`. Las propiedades que establecen relaciones entre las constantes del problema se demuestran también muy fácilmente a partir de sus valores. Sin embargo, si consideramos a estas últimas como axiomas podemos entonces extender la especificación del problema, parametrizando las constantes. De esta manera obtenemos una formulación más general del sistema que preserve las propiedades analizadas.

Las propiedades que vinculan a las constantes del problema en la demostración de *safeTCG* resultan válidas si se consideramos la siguiente restricción:

$$kt1 - kc1 + 1 \geq kg1$$

La especificación del sistema TCG que preserva *safeTCG* puede entonces darse para valores cualesquiera de las constantes que cumplan con la desigualdad anterior, que es una condición suficiente.

Todas las propiedades elementales utilizadas –que involucran a las constantes del problema– en la demostración de las propiedades analizadas en este trabajo (incluyendo *Non-Zeno*) se satisfacen para el siguiente conjunto de restricciones entre los parámetros del sistema:

- $kt1 \geq kg1 + kc1$
- $kg3 > kg2$
- $kc1 \geq kg2$
- $kt2 - 1 > kt1$
- $kc1 \geq kc2$
- $ki > 1$ , para todo parámetro  $ki \in \{kt1, kt2, kc1, kc2, kg1, kg2, kg3\}$ .

Esta última condición resulta válida para el factor de discretización en función de constantes no nulas.

Las restricciones presentadas son condiciones suficientes, deducidas a partir de las propiedades elementales utilizadas en las pruebas de las propiedades destacadas del sistema TCG. Las mismas generalizan “parametrizan” la especificación en función de las propiedades de interés. Luego, podemos incluir como variables las constantes del sistema y especificar como axiomas las condiciones establecidas:

```
Parameter kt1,kt2,kc1,kc2,kg1,kg2,kg3 : Instant.
Axiom AxTCG_1 : kt1 - kc1 + 1 ≥ kg1.
.....
```

## 4.5 Trabajos Relacionados

Como señalamos al comienzo de este capítulo, la especificación del sistema abordado fue tomada de [AD94]. Numerosos trabajos previos consideran a este problema como caso de estudio (“benchmark”) para analizar diferentes técnicas de especificación y herramientas de análisis. Entre otros, [HNS<sup>+</sup>92, CHR92, Sha93, HJL93, HK94, DY95, AB96, BMS<sup>+</sup>97]. En particular, en [BMS<sup>+</sup>97] se hace un análisis comparativo del caso de estudio en diversos formalismos. Algunos de los trabajos citados consideran una versión generalizada del problema que permite modelar un número arbitrario de trenes en el sistema. En nuestro caso de estudio el sistema fuerza a secuencializar la subida y bajada de la barrera (y por lo tanto impone una distancia entre trenes que difiere al menos en el tiempo que lleva subir y bajar la barrera).

Respecto a los trabajos previos, nuestro enfoque consiste en el análisis del sistema a partir de su formulación como un conjunto de grafos temporizados (sistemas de transiciones de estados que permiten la utilización de relojes explícitos), que interactúan según la composición paralela de los mismos. Consecuentemente, no son necesarios operadores tales como *since* para registrar el tiempo transcurrido desde la última vez que valía una propiedad ni otros similares [Sha93]. En la formalización de sistemas de tiempo real con el operador *since* no se requieren contadores o relojes para medir el tiempo transcurrido en torno a una propiedad, la especificación de *since* está dada por un conjunto de axiomas y el comportamiento de un sistema se expresa a través de condiciones en una lógica de orden superior que permite el uso del operador *since* sobre los predicados.

La utilización de múltiples relojes, que pueden ser reseteados en cualquier transición, y la disponibilidad de un mecanismo de definición composicional facilitan el proceso de definición del sistema, su comprensión (aún por personas no expertas) y también su análisis, ya que resulta bastante fácil y natural la formulación de propiedades. Las demostraciones de invariantes y de la propiedad de *safety* considerada son bien tratables con el enfoque seguido, aunque en general las propiedades de *liveness* como *Non-Zeno* son complejas (al igual que en los demás enfoques deductivos). Luego, estas últimas podrían ser probadas con un *model checker* automático sobre el grafo y consideradas axiomas en el ambiente de teoría de tipos.

En la especificación de un grafo temporizado necesitamos, en general, la definición de valores constantes para los parámetros del sistema, a fin de poder verificar propiedades con un *model checker*. Sin embargo, como vimos en la sección 4.4, es posible generalizar la especificación del sistema en estudio preservando ciertas propiedades de interés, asumiendo parámetros variables sujetos a determinadas restricciones (deducidas a partir de condiciones de prueba de las propiedades que se intentan preservar).

Otra ventaja de la formalización del sistema en torno a grafos temporizados, en contraste con métodos axiomáticos para especificar restricciones temporales, reside en el contenido algorítmico de la especificación, tal como analizamos en la sección 2.5.3, que

permite simular el sistema con el control de los múltiples relojes. Creemos que esta formalización, además de permitirnos usar un *model checker* automático como asistente para la demostración de ciertas propiedades, es adecuada para la síntesis de programas, en el marco de teoría de tipos y en particular del cálculo de construcciones inductivas y co-inductivas de *Coq*.



# Capítulo 5

## *Representaciones Genéricas de Grafos Temporizados*

---

En el capítulo 3 incluimos algunas definiciones básicas para describir grafos temporizados simples. Las mismas fueron utilizadas para la especificación y el análisis del caso de estudio abordado en el capítulo 4. En este capítulo definimos dos representaciones genéricas de grafos temporizados para la semántica de tiempo discreto considerada en los capítulos previos, una de las cuales es extendida a tiempo continuo. Estas representaciones permiten definir sistemas como instancias particulares y simplifican el proceso de definición de sistemas compuestos.

### **5.1 Grafos Temporizados Genéricos en *Coq***

En el capítulo 4 especificamos la composición paralela de los tres sistemas componentes del sistema TCG de manera particular, sin el uso de un operador genérico de composición. Sin embargo, de la sección 2.2 se desprende que la definición de tal operador es posible. En esta sección presentamos dos formalizaciones genéricas de grafos temporizados que permiten simplificar el proceso de definición de sistemas compuestos.

Asumiremos, al igual que en los capítulos previos, un tipo `Label` que representa el conjunto global de etiquetas. Sin embargo, no exigimos la existencia de una etiqueta distinguida `Tick` para caracterizar a las transiciones temporales.

#### **5.1.1 Representación**

Un grafo temporizado puede ser visto como una 4-upla paramétrica en el tipo de los estados, compuesta por una relación que define a las transiciones discretas, un estado inicial, un predicado que caracteriza a los invariantes de las locaciones (utilizado para caracterizar a las transiciones temporales) y una función que permite incrementar los relojes de los estados para un valor temporal dado. En *Coq* este tipo puede formalizarse a través de *registros paramétricos* como sigue:

```

Record Tgraph [S:Set] : Type :=
  mkTG { trans : S->Label->S->Prop;
        sini  : S;
        inv   : S->Prop;
        inc   : S->Instant->S
        }.

```

mkTG construye objetos de tipo (Tgraph S) y trans, sini, inv e inc son las proyecciones de esta clase de objetos. Esto es, dados tr de tipo S->Label->S->Prop, si de tipo S, iv de tipo S->Prop e ic de tipo S->Instant->S, (mkTG tr si iv ic) es un objeto de tipo (Tgraph S). Asimismo, dado TG de tipo (Tgraph S), (trans TG) es un objeto de tipo S->Label->S->Prop, (sini TG) tiene tipo S, (inv TG) tiene tipo S->Prop e (inc TG), tipo S->Instant->S.

El estado inicial de un grafo G debe ser un estado válido, esto es la proyección sini de G tiene que satisfacer el predicado (inv G). Esta restricción puede plasmarse en el siguiente tipo de grafos válidos:

```

Record Tgraph_V [S:Set] : Type :=
  mkTG_V { TG : (Tgraph S); siniV : ((inv TG) (sini TG)) }.

```

**Nota 5.1.** En lo que sigue nos referiremos a grafos de tipo Tgraph pero asumiremos que estos corresponden a grafos válidos, es decir son la proyección de un objeto de tipo Tgraph\_V.

**Ejemplo 5.1.** Para el caso de estudio del capítulo 4, los grafos componentes del sistema TCG pueden instanciarse de la siguiente manera:

```

Definition Inc_simple := [S:Set; st:(S_Ck S); t:Instant]
  Cases st of (s,x) => (s,(plus_Ck x t)) end.

Definition Train      := (mkTG TrT' SiniT InvT (Inc_simple 1!ST)).

Definition Controller := (mkTG TrC' SiniC InvC (Inc_simple 1!SC)).

Definition Gate      := (mkTG TrG' SiniG InvG (Inc_simple 1!SG)).

```

TrT', TrC' y TrG' se definen como las relaciones TrT, TrC y TrG de la sección 4.2 para las transiciones discretas. Esto es, sin considerar las reglas para los constructores *ttTick*, *tcTick* y *tgTick*. Inc\_simple es la operación de incremento temporal sobre estados con un único reloj. Con 1! explicitamos el primer argumento de Inc\_simple, que es asumido implícito en función del segundo argumento de la función.



### 5.1.2 Composición Paralela

La composición paralela de dos grafos temporizados puede especificarse de manera genérica para la representación introducida en la sección previa. El tipo de los estados del sistema compuesto es definido como el producto de los correspondientes a cada subsistema.

Las transiciones del sistema compuesto se definen de manera similar que en la sección 2.2, para las transiciones discretas. Distinguimos transiciones de sincronización, que comparten una misma etiqueta, y asíncronas. Estas últimas contemplan dos casos, uno para cada componente. La caracterización de “no es una transición de sincronización” está dada por un predicado `no_label` que especifica que una etiqueta no pertenece a las transiciones de un grafo. Formalmente,

```
Definition no_label := [S:Set; tr:S->Label->S->Prop; l:Label]
  ∀s,s'∈S ~(tr s l s').
```

Section **Composition**.

```
Variable S1,S2:Set.
```

```
Variable tr1:S1->Label->S1->Prop.
```

```
Variable tr2:S2->Label->S2->Prop.
```

```
Inductive tr_c : (S1*S2)->Label->(S1*S2)->Prop :=
```

```
  tr_c_syn : ∀s1,s1'∈S1 ∀s2,s2'∈S2 ∀l∈Label
    (tr1 s1 l s1') ->
    (tr2 s2 l s2') ->
    (tr_c (s1,s2) l (s1',s2'))
```

```
|tr_c_nosyn1 : ∀s1,s1'∈S1 ∀s2,s2'∈S2 ∀l∈Label
  (tr1 s1 l s1') ->
  (no_label tr2 l) ->
  (tr_c (s1,s2) l (s1',s2))
```

```
|tr_c_nosyn2 : ∀s1,s1'∈S1 ∀s2,s2'∈S2 ∀l∈Label
  (tr2 s2 l s2') ->
  (no_label tr1 l) ->
  (tr_c (s1,s2) l (s1,s2')).
```

End **Composition**.

El predicado que define a los invariantes de las locaciones de la composición está dado por la conjunción de los invariantes correspondientes y la operación de incremento temporal se define a partir de la de cada componente. Esto es,

```

Definition inv_c := [S1,S2:Set; inv1:S1->Prop; inv2:S2->Prop;
  s:(S1*S2)]
  Cases s of (s1,s2) => (inv1 s1) /\ (inv2 s2) end.

Definition inc_c := [S1,S2:Set; inc1:S1->Instant->S1;
  inc2:S2->Instant->S2; s:(S1*S2); t:Instant]
  Cases s of (s1,s2) => ((inc1 s1 t),(inc2 s2 t)) end.

```

Finalmente, la composición paralela de dos grafos temporizados  $G_1$  y  $G_2$ ,  $G_1 \parallel G_2$ , se define de la siguiente manera:

```

Definition Parallel_composition :=
  [S1,S2:Set; G1:(Tgraph S1); G2:(Tgraph S2)]
  (mkTG
    (tr_c (trans G1) (trans G2))
    ((sini G1),(sini G2))
    (inv_c (inv G1) (inv G2))
    (inc_c (inc G1) (inc G2))).

```

Las transiciones temporales de la composición, al igual que las de cada componente, están implícitamente representadas por los invariantes de las locaciones y serán explicitadas en la definición de trazas de ejecución.

**Ejemplo 5.2.** Para el caso de estudio del capítulo 4, el grafo correspondiente a la composición paralela ( $\text{Train} \parallel \text{Controller} \parallel \text{Gate}$ ) puede especificarse como sigue

```

Definition system_TCG :=
  (Parallel_composition Train (Parallel_composition Controller Gate)).

```

El tipo de los estados de la composición de los tres sistemas coincide con el asumido en el capítulo 4:  $(S\_Ck\_ST) * (S\_Ck\_SC) * (S\_Ck\_SG)$ . El estado inicial  $\text{siniTCG}$  es  $(\text{sini\_system\_TCG})$  y las transiciones discretas del tipo  $\text{TrGlobal}$  (todas menos la correspondiente al constructor  $\text{tGl\_Tick}$ ) corresponden conceptualmente a las transiciones del tipo  $(\text{tr\_system\_TCG})$ .

### 5.1.3 Trazas de Ejecución

Dado un grafo temporizado  $G$ , las trazas de ejecución válidas de  $G$ , que no involucran referencias temporales (correspondiente a  $\text{isTrace}$  de la sección 3.4.2), pueden ser caracterizadas por el siguiente predicado co-inductivo:

```

CoInductive isTraceTG [S:Set; G:(Tgraph S)] : (Stream S)->Prop :=
  isTraceDisc : ∀x∈(Stream S) ∀s1,s2∈S ∀l∈Label
    (trans G s1 l s2) ->
    (inv G s2) ->
    (isTraceTG S G s2^x) ->
    (isTraceTG S G s1^s2^x)

  | isTraceTick : ∀x∈(Stream S) ∀s∈S
    (inv G (inc G s tick)) ->
    (isTraceTG S G (inc G s tick)^x) ->
    (isTraceTG S G s^(inc G s tick)^x).

```

*isTraceDisc* corresponde a pasos representados por transiciones discretas; *isTraceTick* construye pruebas de transiciones temporales de un estado  $s_1$  a otro  $s_2$  –que posee la misma locación que  $s_1$  pero con los relojes incrementados en un *tick*– si se satisface el invariante de la locación en  $s_2$ . En la formalización de las transiciones, tanto discretas como temporales, explicitamos que el estado destino de la transición debe cumplir el invariante de la locación (en el capítulo 3, sección 3.2, esta hipótesis se refleja en el formato exigido a las transiciones).

Notemos que mientras los pasos discretos en una traza se obtienen por transiciones rotuladas del grafo, los pasos temporales están representados por transiciones implícitamente rotuladas y definidos en función de los invariantes de las locaciones.

Las trazas generadas a partir de un estado inicial dado pueden ser definidas como sigue,

```

Definition isTraceFromTG :=
  [S:Set; G:(Tgraph S); Sini:S; x:(Stream S)]
  Sini=(hd x) /\ (inv G Sini) /\ (isTraceTG G x).

```

De acuerdo a la discusión planteada en el capítulo 3 (secciones 3.3.2 y 3.4.2), podemos obviar la restricción  $(inv G Sini)$ , considerándola una hipótesis a corroborar.

Asimismo, las trazas que explicitan el valor temporal del *reloj global* y sobre las cuales definimos los operadores de la lógica TCTL se definen, al igual que en la sección 3.4.3, como una generalización de las definiciones anteriores.

```

CoInductive isTraceTG_T [S:Set; G:(Tgraph S)] :
  (Stream S*Instant)->Prop :=

  isTraceDisc_T : ∀x∈(Stream S*Instant) ∀s1,s2∈S ∀l∈Label ∀t∈Instant
    (trans G s1 l s2) ->
    (inv G s2) ->
    (isTraceTG_T S G (s2,t)^x) ->
    (isTraceTG_T S G ( (s1,t)^(s2,t)^x ))

```

```

| isTraceTick_T : ∀x∈(Stream S*Instant) ∀s∈S ∀t∈Instant
  (inv G (inc G s tick)) ->
  (isTraceTG_T S G ((inc G s tick),(Inc t))^x) ->
  (isTraceTG_T S G ( (s,t)^((inc G s tick),(Inc t))^x )).

```

Cada elemento de una traza de ejecución de un grafo  $G$  es un par compuesto por un estado de  $G$  (la locación más las valuaciones de los relojes) y el valor temporal del *reloj global*. Este último se incrementa con cada paso temporal ( $isTraceTick_T$ ), manteniendo su valor en los pasos correspondientes a las transiciones discretas ( $isTraceDisc_T$ ).

Asimismo, las trazas que poseen comienzo en un estado, para un valor temporal dado del reloj global se definen por la siguiente abreviatura:

```

Definition isTraceFromTG_T :=
  [S:Set; G:(Tgraph S); Sini:S*Instant; x:(Stream S*Instant)]
  Sini=(hd x) /\ (inv G Sini) /\ (isTraceTG_T G x).

```

Nuevamente, la restricción  $(inv G Sini)$  puede ser obviada, considerándola una hipótesis a corroborar en el análisis de propiedades sobre las trazas.

Los operadores temporales se definen como en la sección 3.4, tanto los correspondientes al fragmento CTL (sobre trazas caracterizadas con  $isTraceTG$ ) como los de TCTL (sobre trazas caracterizadas con  $isTraceTG_T$ ).

### 5.1.4 Una Representación Alternativa

Una representación genérica más simple de grafos temporizados se obtiene si consideramos, como en la sección 3.2, que las transiciones temporales y las discretas están representadas por una relación de tipo  $S \rightarrow Label \rightarrow S \rightarrow Prop$ , con  $S$  el tipo de los estados del grafo y  $Tick$  de tipo  $Label$  una etiqueta distinguida que denota las transiciones temporales. De esta manera un grafo es simplemente un par (los invariantes de las locaciones y la función que permite incrementar los relojes son innecesarios).

```

Record Tgraph [S:Set] : Type :=
  mkTG { trans : S->Label->S->Prop; sini: S }.

```

**Ejemplo 5.3.** Para el caso de estudio del capítulo 4, los grafos componentes del sistema TCG se instancian de la siguiente manera:

```

Definition Train      := (mkTG TrT SiniT).
Definition Controller := (mkTG TrC SiniC).
Definition Gate       := (mkTG TrG SiniG).

```

La composición paralela de dos grafos temporizados es el grafo que compone las transiciones según la relación inductiva  $tr\_c$  definida previamente y cuyo estado inicial se define como antes. A diferencia que en la versión previa, el constructor  $tr\_c\_syn$  de  $tr\_c$  permite sincronizar, además de transiciones discretas, transiciones temporales con  $Tick$ .

```

Definition Parallel_composition :=
  [S1,S2:Set; G1:(Tgraph S1); G2:(Tgraph S2)]
  (mkTG (tr_c (trans G1) (trans G2))
    ((sini G1),(sini G2))).

```

Para el caso de estudio del capítulo 4, el sistema TCG ( $Train \parallel Controller \parallel Gate$ ) se define igual que en el ejemplo 5.2.

Las trazas temporizadas y las no temporizadas se definen igual que en la sección 3.4 (para el formato de transiciones establecido en la sección 3.2), como así también los operadores temporales de CTL y TCTL.

### 5.1.5 Discusión

La primera generalización permite instanciar grafos temporizados sin necesidad de incluir explícitamente la definición de las transiciones temporales. La segunda supone que éstas son definidas junto con las transiciones discretas. Mientras la primera facilita más el proceso de definición de los grafos básicos, la segunda es más compacta y permite simplificar la estructura y el tamaño de las pruebas.

Ambas generalizaciones definen a las transiciones de una composición de manera uniforme, a diferencia que en el capítulo 4 donde especificamos la relación de composición para los tres grafos básicos con una definición particular. Con el enfoque genérico simplificamos el proceso de definición; sin embargo, las demostraciones se vuelven más complejas y los términos de prueba crecen en tamaño. Con el fin de experimentar, demostramos algunas propiedades para una especificación genérica del sistema TCG analizado en el capítulo 4. Las pruebas resultaron más extensas que para la versión original, tanto en relación al número de tácticas del *script* de prueba, como al tamaño de los términos de dichas pruebas. La razón se debe a la utilización del operador genérico de composición de transiciones que aumenta el número de subpruebas estrictamente necesarias y obliga a eliminar casos inválidos (transiciones no definidas), tanto para las transiciones de sincronización como las que no sincronizan, sobre el conjunto de las etiquetas del sistema. Los casos inválidos para determinadas etiquetas pueden ser eliminados realizando *inversiones* sobre las transiciones involucradas, aunque de esta manera aumentan los tamaños de los términos de prueba.

Al trabajar con una definición general de composición de transiciones deberían desarrollarse tácticas que permitan simplificar el desarrollo de las pruebas sobre estas transiciones, reduciendo al mismo tiempo los tamaños de los términos de prueba.

## 5.2 Grafos con Tiempo Continuo

### 5.2.1 Adaptación de las Formalizaciones Previas

*Coq* posee librerías que permiten trabajar con números racionales ( $\mathbb{Q}$ ) y reales ( $\mathbb{R}$ ) [Bar<sup>+</sup>99]. Luego, la formalización genérica de grafos temporizados dada en la sección 5.1 puede ser adaptada a un modelo temporal continuo, salvo la propuesta alternativa presentada en la subsección 5.1.4. Las modificaciones necesarias son las siguientes:

- Los tipos `Instant` y `Clock` son abreviaciones del tipo `T`. Donde `T` representa el dominio temporal continuo elegido ( $\mathbb{Q}$  o  $\mathbb{R}$ ). Los operadores considerados en la sección 3.1 se redefinen en función de `T` (salvo `tick` e `Inc` que no son considerados en el dominio continuo).
- Las definiciones de trazas de ejecución dadas en 5.1.3 deberían ser modificadas como sigue:

```
CoInductive isTraceTG [S:Set; G:(Tgraph S)] : (Stream S)->Prop :=
```

```
  IsTraceDisc :  $\forall x \in (\text{Stream } S) \forall s_1, s_2 \in S \forall l \in \text{Label}$ 
```

```
  .....
```

```
| IsTraceTick :  $\forall x \in (\text{Stream } S) \forall s \in S \forall t \in \text{Instant}$   

  ( $\forall t' \in \text{Instant} (le\_Ck\ 0\ t') \rightarrow (le\_Ck\ t'\ t) \rightarrow$   

  ( $inv\ G\ (inc\ G\ s\ t')$ ))  $\rightarrow$   

  ( $isTraceTG\ S\ G\ (inc\ G\ s\ t)^x$ )  $\rightarrow$   

  ( $isTraceTG\ S\ G\ s^{(inc\ G\ s\ t)^x}$ ).
```

```
CoInductive isTraceTG_T [S:Set; G:(Tgraph S)] :
```

```
  (Stream S*Instant)->Prop :=
```

```
  IsTraceDisc_T :  $\forall x \in (\text{Stream } S * \text{Instant}) \forall s_1, s_2 \in S$   

   $\forall l \in \text{Label} \forall t \in \text{Instant}$ 
```

```
  .....
```

```
| IsTraceTick_T :  $\forall x \in (\text{Stream } S * \text{Instant}) \forall s \in S \forall t, tg \in \text{Instant}$   

  ( $\forall t' \in \text{Instant} (le\_Ck\ 0\ t') \rightarrow (le\_Ck\ t'\ t) \rightarrow$   

  ( $inv\ G\ (inc\ G\ s\ t')$ ))  $\rightarrow$   

  ( $isTraceTG\_T\ S\ G\ ((inc\ G\ s\ t), (plus\_Ck\ tg\ t))^x$ )  $\rightarrow$   

  ( $isTraceTG\_T\ S\ G\ (s, tg)^{(inc\ G\ s\ t), (plus\_Ck\ tg\ t)^x}$ ).
```

En las transiciones temporales no existe un valor mínimo de tiempo que sea el “siguiente” del instante previo, por la propiedad de densidad, propia de un modelo continuo. Es por esto que la formalización dada en la sección 5.1.4 (basada en las formalizaciones de la sección 3.2) no es válida en un modelo de tiempo continuo, debido a que si bien las transiciones temporales de los grafos particulares de un sistema deben sincronizar con una etiqueta distinguida `Tick`, el tiempo podría evolucionar diferente en cada subsistema (los valores de incremento podrían diferir).

En las definiciones de `isTraceTG` e `isTraceTG_T` los pasos temporales son definidos como en la sección 2.1.1. Es decir, hay una transición temporal del sistema de  $t$  unidades de tiempo, si el invariante de las locaciones vale continuamente para todo incremento menor o igual que  $t$ .

Los operadores temporales se definen como en la sección 3.4, tanto los correspondientes al fragmento CTL (sobre trazas caracterizadas con `isTraceTG`) como los de TCTL (sobre trazas caracterizadas con `isTraceTG_T`).

### 5.2.2 Limitaciones de los Reales y los Racionales en *Coq*

Los números reales en *Coq* están formalizados a partir de una axiomatización (18 axiomas) más algunos lemas de base sobre las partes fraccionarias y enteras [Bar<sup>+</sup>99]. Consecuentemente, la manipulación de estos números es compleja, aunque todas las propiedades válidas para los mismos podrían ser probadas. Al presente, el autor no conoce trabajos que usen la formalización de los reales en aplicaciones concretas, salvo un trabajo de matemática pura relacionado con el teorema de los tres intervalos (“the three gap theorem”) [May97]. Asimismo, tampoco hay tácticas que permitan automatizar o simplificar ciertas pruebas, o partes de las mismas, como en el caso de los enteros y los naturales (por ejemplo, con la táctica *Omega*), excepto con la táctica *Ring* que está definida tanto para números naturales, enteros, racionales, como reales. Esta táctica permite hacer reescritura en anillos; normaliza términos de una meta con respecto a la conmutatividad y la asociatividad y los reemplaza por su forma normal; cuando la meta es una igualdad, intenta solucionarla o simplificarla [Bar<sup>+</sup>99]. Otra limitación de los reales en *Coq* es que no es posible para los reales usar el procedimiento de *extracción de programas* de *Coq*, ya que éstos están definidos en el tipo *Type* de *Coq*. Esta última restricción puede ser significativa en una etapa de síntesis de programas.

Los números racionales en *Coq* están definidos como el producto de enteros y enteros estrictamente positivos cocientados por la relación usual [Bar<sup>+</sup>99]. En la formalización se asumen dos conjuntos de axiomas, uno correspondiente a los cocientes y el otro a subconjuntos. Las observaciones relativas a la complejidad de la utilización de los racionales son análogas que las argumentadas para los reales. La igualdad para los racionales se define en función de clases de equivalencia, ya que, por ejemplo,  $1 = 2/2$  pero ambos términos son constructivamente diferentes. Al igual que para los reales, el autor desconoce, hasta el momento, aplicaciones que usen a los racionales en otros

trabajos. Tampoco existen automatizaciones (tácticas especializadas) que simplifiquen pruebas en este dominio, exceptuando aquellas tratables con la táctica *Ring*.

Todas las limitaciones analizadas que complican el trabajo con los números reales y los racionales en *Coq* son líneas actuales de investigación.



# Capítulo 6

## *Conclusiones, Trabajos Relacionados y Trabajos Futuros*

---

### 6.1 Conclusiones

En este trabajo formalizamos en teoría de tipos –y en particular en *Coq*– sistemas de tiempo real representados como grafos temporizados, asumiendo una semántica de tiempo discreto. A fin de especificar y demostrar requerimientos temporales sobre los sistemas, formalizamos la lógica TCTL y su restricción CTL para operadores temporales no cuantitativos. Dimos algunas definiciones alternativas para los operadores que permiten expresar invarianza y alcanzabilidad, con tipos inductivos (bajo la noción de estados alcanzables) y co-inductivos (bajo la noción de trazas –infinitas– de ejecución). Estos últimos necesarios para una descripción completa de todas las fórmulas de la lógica TCTL (y CTL). Asimismo, formulamos y probamos en *Coq* propiedades generales de los operadores temporales que permiten simplificar ciertas pruebas.

En el trabajo pusimos un especial énfasis en la especificación y el análisis de un caso de estudio, considerado como “*benchmark*” en diferentes trabajos: *el control de un paso a nivel de tren* (“*the railroad crossing example*”). Establecimos un conjunto de invariantes y en función de ellos probamos la propiedad de seguridad esencial del sistema y la propiedad de *liveness Non-Zeno* que justifica la corrección temporal del sistema. Las demostraciones fueron parametrizadas en un conjunto de restricciones entre los parámetros del sistema, inicialmente considerados constantes y posteriormente generalizados a variables sujetas a las restricciones establecidas –deducidas a partir de las condiciones de prueba de las propiedades que se decidieron preservar. De esta manera generalizamos la especificación del sistema, que es tratable con un *model checker* sólo para valores constantes de los parámetros.

Finalmente, definimos dos representaciones genéricas de grafos temporizados para la semántica de tiempo discreto considerada, una de las cuales fue extendida a tiempo continuo. Estas representaciones permiten obtener sistemas como instancias particulares y simplifican el proceso de definición de sistemas compuestos con el uso de un operador genérico de composición (evitando definir la composición de dos o más grafos temporizados de forma particular cada vez).

Las formalizaciones de grafos temporizados y las lógicas consideradas, traducidas en bibliotecas *Coq*, y la validación de éstas a través de un *benchmark*, constituyen los aportes de este trabajo y un punto de partida para la realización de nuevos trabajos de investigación en torno al análisis de sistemas de tiempo real en teoría de tipos.

A continuación proponemos una metodología de trabajo que relaciona el contenido de los capítulos previos y busca compatibilizar el uso de un *model checker* (MC) con el desarrollo de sistemas en un ambiente de pruebas. Los objetivos de la misma son:

- Definir un esquema de representación de los sistemas común a los dos enfoques de análisis en cuestión.
- Establecer un proceso de análisis de los sistemas que vincule los resultados de la verificación de propiedades para los enfoques considerados.
- Permitir trabajar con sistemas de tiempo real con *parámetros variables*.
- Abarcar una etapa de *síntesis* de sistemas de tiempo real.

La metodología generaliza el análisis realizado para el caso de estudio abordado en el capítulo 4 y es esquematizada en la figura 6.1.

## Una Metodología de Trabajo

El análisis de sistemas de tiempo real, representados por grafos temporizados, podría dividirse en dos etapas, no necesariamente independientes entre sí ni secuenciales. La primera –optativa y no profundizada en este trabajo– consiste en la especificación y verificación de ciertas propiedades de un sistema en estudio usando un MC automático, por ejemplo Kronos, HyTech o Uppaal (“delegación de pruebas” en la figura 6.1). Entre estas propiedades consideramos relevantes las de *liveness*, como *Non-Zeno*, y las de alcanzabilidad que son, en general, más difíciles de demostrar deductivamente, aunque algunas de éstas pueden transformarse en otras equivalentes más simples.

La segunda etapa consiste en la especificación y el análisis del sistema en el cálculo de construcciones inductivas y co-inductivas de *Coq* (otros sistemas de pruebas similares a *Coq* son, por ejemplo, ALF [Mag94] y LEGO [LP92]). Para esta etapa podemos asumir una semántica de tiempo discreto, como en la mayor parte de este trabajo, o trabajar en un modelo de tiempo continuo, tal como analizamos en la sección 5.2.

Una manera de incorporar las propiedades demostradas con un MC en la metodología de trabajo en teoría de tipos consiste en asumir a las mismas como axiomas o hipótesis. Como el lenguaje de especificación de los requerimientos temporales –la lógica TCTL y/o CTL– y el formalismo de descripción de los sistemas –los grafos temporizados– son los mismos en ambas etapas, no son necesarias traducciones significativas para compatibilizar el uso de un MC como Kronos con un ambiente de teoría de tipos como *Coq*.

La especificación de un sistema puede obtenerse de una representación genérica de los grafos y la composición paralela de los mismos, como describimos en las secciones previas de este capítulo, o a través de definiciones particulares para la composición, tal como procedimos en el caso de estudio del capítulo 4. Las ventajas de ambos enfoques fueron analizadas en la sección 5.1.5.

Los operadores lógicos de TCTL y CTL, formalizados en el capítulo 3, permiten formular requerimientos temporales, es decir pueden ser utilizados para la verificación de propiedades sobre los sistemas especificados. Para propiedades que sólo involucran  $\exists\Diamond$ , y  $\forall\Box$ , ( $\exists\Diamond$  y  $\forall\Box$ ) podemos optar entre una formalización con tipos inductivos y una con tipos co-inductivos. Para propiedades arbitrarias, la formalización requiere el uso de tipos co-inductivos y por lo tanto, el uso de co-inducción como mecanismo de prueba de determinadas propiedades.

Las demostraciones de las propiedades de *safety* y de *liveness* del sistema TCG se basaron fuertemente en el conocimiento de un conjunto de propiedades invariantes del sistema. La deducción y prueba de invariantes permite incrementar el conocimiento de un sistema y consecuentemente probar otras propiedades con su ayuda [MP91]. Luego, en el análisis de los sistemas sugerimos trabajar de esta manera. Para la deducción de invariantes existen algunos trabajos que podrían ser considerados [MP95, BBM97, BMS<sup>+</sup>97, BL99].

A partir de las propiedades analizadas de un sistema y consideradas relevantes puede intentarse generalizar la especificación del sistema asumiendo a las constantes del mismo como variables que deben satisfacer un conjunto de restricciones (deducidas en función de condiciones de prueba elementales entre los relojes y las constantes), tal como fue hecho en la sección 4.4 para el sistema TCG. Esta es una clara ventaja del enfoque deductivo utilizado que está condicionada respecto a la utilización de un MC. Para el sistema TCG todas las pruebas se hicieron exclusivamente en el ambiente de pruebas *Coq* y fue posible una generalización de la especificación del problema que preserva todas las propiedades analizadas. Si ciertas pruebas se hicieran con el auxilio de un MC –para determinados valores constantes de los parámetros–, la generalización completa no sería posible. Sin embargo, en función de las propiedades demostradas en el ambiente de pruebas podría ensayarse una generalización que especifique un superconjunto de valores posibles para los parámetros, que hagan verdaderas a estas propiedades. Siendo un subconjunto de éstos los valores que hacen verdaderas a todas las propiedades del sistema, incluyendo a las demostradas con el MC. Luego, al elegir valores constantes para los parámetros del sistema distintos a los usados para la verificación de las propiedades con el MC, deberían demostrarse todas estas propiedades nuevamente con el MC, pero no las demostradas con el asistente de pruebas –los nuevos valores constantes serían seleccionados a partir de las posibles instancias de los parámetros que satisfacen las propiedades demostradas deductivamente.

Finalmente, una etapa no abordada en este trabajo corresponde a la síntesis de programas, que creemos es una línea promisoría a seguir y en la cual un ambiente de

teoría de tipos como *Coq* es particularmente adecuado, ya que permite expresar pruebas y programas en una teoría unificada. El sistema *Coq* guía a un usuario en forma interactiva en el proceso de construcción de las pruebas y los programas, siendo verificada inmediatamente la validez de cada paso del desarrollo.

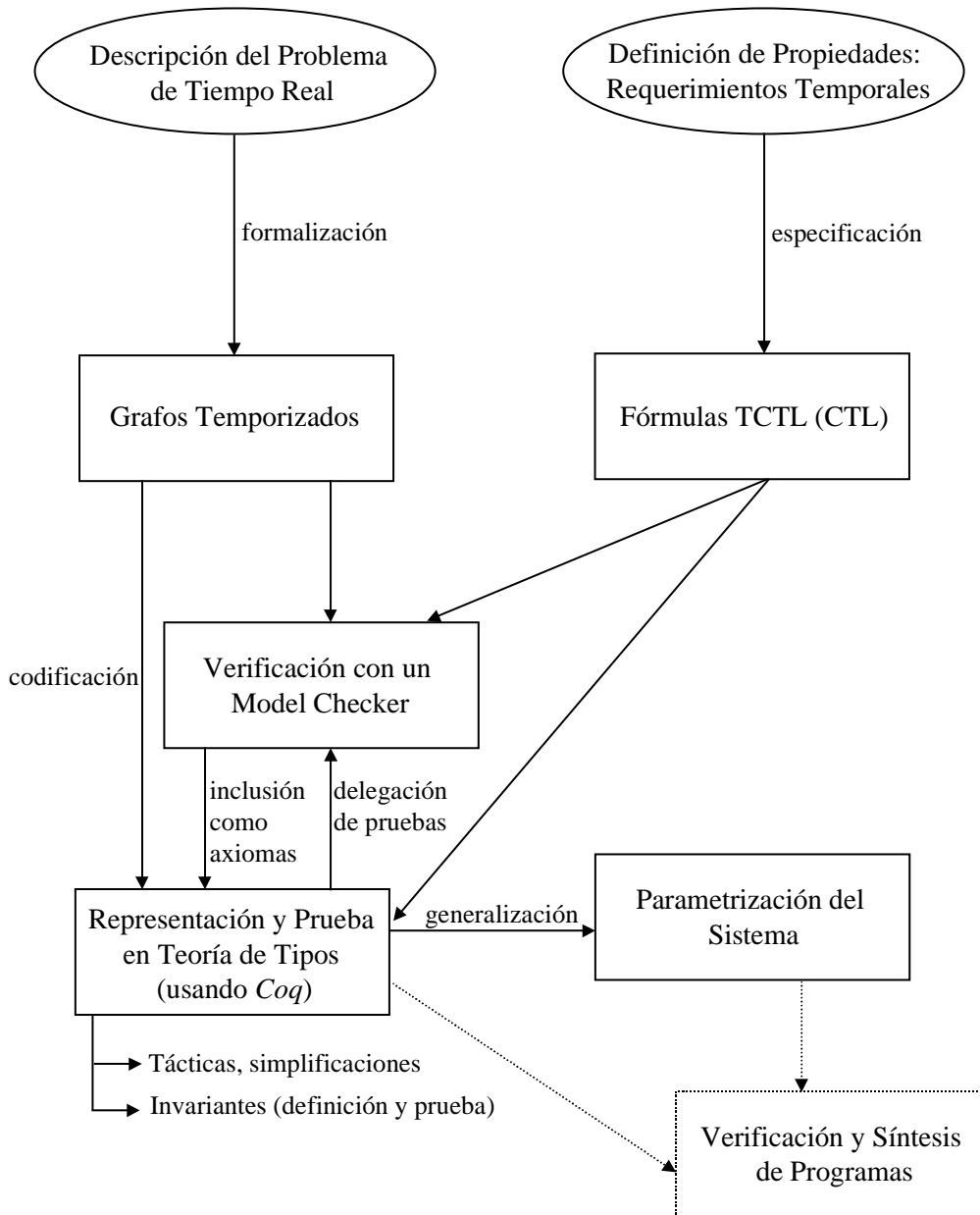


Fig. 6.1: Una metodología de trabajo

## 6.2 Trabajos Relacionados

En [Lun98] el autor compara algunas de las distintas opciones para la especificación, el análisis y la automatización de sistemas que involucran nociones temporales, tales como los autómatas (grafos) temporizados, las redes de Petri con tiempo y algunas lógicas temporales. Se describe una discretización de un dominio temporal continuo y un particular interés es puesto en la concepción de versiones algorítmicas de modelos temporizados de autómatas y redes de Petri, a partir de la utilización de transformadores de predicados. Se analizan variaciones y extensiones temporales –para sistemas restringidos– del *wp* (weakest precondition) propuesto por Dijkstra.

En la sección 4.5 analizamos algunos trabajos relacionados al marco de especificación y análisis de sistemas de tiempo real en torno al caso de estudio abordado en dicho capítulo. Respecto a la utilización –exclusiva– de un *model checker* en la verificación, nuestro enfoque permite trabajar con parámetros variables y suma las ventajas de los métodos deductivos de análisis, descritas sucintamente en la sección 1.3. En la sección 4.5 analizamos también las diferencias con otros otros modelos de especificación y análisis deductivos (por ejemplo, PVS [Sha93]). Nosotros pensamos que la utilización de relojes en el modelo de especificación y la disponibilidad de un mecanismo de definición composicional facilitan el proceso de definición de los sistemas, su comprensión (aún por personas no expertas) y también su análisis, ya que resulta bastante fácil y natural la formulación de propiedades. Asimismo, los grafos temporizados tienen una interpretación algorítmica que permite simular el sistema con el control de los múltiples relojes. Creemos que esta formalización, además de permitirnos usar un *model checker* automático como asistente para la demostración de ciertas propiedades, es adecuada para la síntesis de programas, en el marco de teoría de tipos y en particular del cálculo de construcciones inductivas y co-inductivas de *Coq*.

Algunos otros trabajos que buscan relacionar métodos deductivos de prueba y *model checking* son: [MN95, RSS95, HS96, BMS<sup>+</sup>97, SS99, KKP99, Gim99]. En particular, [Gim99] analiza posibles combinaciones, en *Coq*, de métodos de demostración asistida de programas y *model checking* para la verificación de programas concurrentes sobre memorias compartidas. Sin embargo, el *tiempo* no es considerado un parámetro relevante en la clase de problemas abordados.

## 6.3 Trabajos Futuros

Algunos trabajos futuros son:

- Desarrollar tácticas generales que permitan simplificar la prueba de propiedades sobre grafos temporizados obtenidos como instancias de las representaciones genéricas.

- Analizar la construcción y corrección, en teoría de tipos, de *abstracciones* de sistemas a fin de demostrar ciertas propiedades sobre sistemas reducidos –más abstractos–, que puedan ser posteriormente generalizadas a los sistemas originales. Un trabajo relacionado en esta dirección es [MN95]. Una abstracción permite particionar el espacio de estados para obtener un sistema –autómata– más pequeño, el cuál pueda ser más tratable (en particular, por un *model checker*). La construcción formal de abstracciones constituiría una etapa en la metodología de trabajo propuesta en la sección previa para el análisis de *ciertas* propiedades. Estas propiedades se probarían sobre una versión simplificada de un sistema, pero serían válidas para el sistema original, de acuerdo a la corrección de la abstracción respecto de las propiedades analizadas, que sería demostrada a través del asistente de pruebas.
- Estudiar la posibilidad de realizar síntesis de programas de tiempo real en teoría de tipos.

Respecto a la última propuesta, algunas ideas surgen a partir del trabajo [Gim99]. Una noción –primitiva– de programa de tiempo real podría concebirse, inicialmente, como una función que dada una serie (un *stream*) de *eventos* construye una traza de ejecución del sistema. Sin embargo, a diferencia de [Gim99], no toda posible serie de eventos produce una traza válida de ejecución del sistema, ya que el tiempo aquí es un parámetro a considerar. Es decir, la función que dado un estado del sistema y un evento devuelve el nuevo estado del sistema, no es una función total. Podríamos entonces considerar que el tipo de los estados (*State*) incluye un estado distinguido de error (*ErrState*), a partir del cual el sistema es incorrecto. La función que construye las trazas de ejecución –en realidad, *streams* de tipo *State*, donde se incluyen posibles trazas erróneas– sería entonces una función co-recursiva (*mkTrace*) que recibe un estado y una secuencia de eventos. *mkTrace* es en realidad un simulador del sistema. Esto es,

```

Definition Trace := (Stream State).

Definition Events := (Stream Event).

Parameter NextState : State -> Event -> State

CoFixpoint mkTrace [s:State; evs:Events]: Trace :=
  (Cons s (mkTrace (NextState s (hd evs))) (tl evs)).

```

Donde, *Event* es el tipo de los eventos (para sistemas determinísticos éste podría ser el tipo *Label*) y *NextState* es una función que implementa la relación de transición. Dado un estado y un evento, *NextState* devuelve el nuevo estado del sistema, siendo éste *ErrState* cuando el estado del sistema no es válido para el evento dado o cuando es precisamente el estado de entrada (propagación del estado de error).

Las propiedades del sistema se demuestran para las trazas *válidas*, esto es, aquellas generadas a partir de secuencias de eventos que no generan en ningún punto el estado `ErrState`.

## Referencias Bibliográficas

- [AB96] J. Armstrong and L. Barroca. “Specification and verification of reactive systems behaviour: The railroad crossing example”. *Real-Time Systems*, 10:143-178, 1996.
- [ACD90] R. Alur, C. Courcoubetis, and D. Dill. “Model-checking for real-time systems”. In *Proc. 5<sup>th</sup> Symp on Logics in Computer Science*, pages 414-425. IEEE Computer Society Press, 1990.
- [ACH<sup>+</sup>95] R. Alur, C. Courcoubetis, N. Halbwachs, T. Henzinger, P. Ho, X. Nicollin, A. Oliver, J. Sifakis, and S. Yovine. “The algorithmic analysis of hybrid systems”. *Theoretical Computer Science*, 138:3-34, 1995.
- [AD94] R. Alur and D. Dill. “A theory of timed automata”. *Theoretical Computer Science*, 126:183-235, 1994.
- [AH91] R. Alur and T. Henzinger. “Time for logic”. *SIGACT News*, 22(3), 1991.
- [AH92] R. Alur and T. Henzinger. “Logics and models of real time: A survey”. In J. W. de Bakker, K. Huizing, W.-P. de Roever, and G. Rozenberg, editors, *Real Time Theory in Practice, LNCS 600*, pages 74-106. Springer-Verlag, 1992.
- [AH93] R. Alur and T. Henzinger. “Real-time logics: Complexity and expressiveness”. *Information and Computation*, 104(1):35-77, 1993.
- [AH94] R. Alur and T. Henzinger. “A Really Temporal Logic”. *Journal of the ACM*, 41(1):181-204, 1994.
- [AH97] R. Alur and T. Henzinger. “Real-time system = discrete system + clock variables”. *Software Tools for Technology Transfer*, 1:86-109, 1997.
- [Alu91] R. Alur. *Techniques for automatic verification of real-time systems*. PhD thesis, Department of Computer Science, Stanford University, 1991.
- [AMP98] A. Asarin, O. Maler, and A. Pnueli. “On the discretization of delays in timed automata and digital circuits”. In R. de Simone and D. Sangiorgi (Eds.), *Proc. Concur’98, LNCS 1466*, pages 470-484, Springer-Verlag, 1998.
- [AS85] B. Alpern and F. Schneider. “Defining liveness”. *Information Processing Letters*, 21(4):181-185, 1985.
- [Bar<sup>+</sup>99] B. Barras, S. Boutin, C. Cornes, J. Courant, Y. Coscoy, D. Delahaye, D. de Rauglaudre, J-C. Filliâtre, E. Giménez, H. Herbelin, G. Huet, H. Laulhère, C. Muñoz, Ch. Murthy, C. Parent-Vigouroux, P. Loiseleur, Ch. Paulin-Mohring, A. Saïbi, and B. Werner. “The Coq Proof Assistant. Reference Manual, Versión 6.2.4”. *INRIA*, 1999.
- [BB94] S. Badaloni and M. Berati. “Dealing with time granularity”. Technical Report, Departamento de Informática – Universidad de Jaume – Castellon – Technical Report DI 06-11/95, 1995.
- [BBM97] N. S. Bjørner, A. Browne, and Z. Manna. “Automatic generation of invariants and intermediate assertions”. *Theoretical Computer Science*, 173(1):49-87, 1997.
- [Ben91] J. F. A. K. Van Benthem. *The Logic of Time (second edition)*. Reidel, 1991.



- [BL99] S. Bensalem and Y. Lakhench. "Automatic generation of invariants". Accepted in *Formal Methods in System Design*. To appear.
- [BM97] F. Barber and S. Moreno. "Representation of continuous change with discrete time". IEEE pages 175-179, 1997.
- [BMS<sup>+</sup>97] N. Bjørner, Z. Manna, H. Spima, and T. Uribe. "Deductive Verification of Real-time Systems Using SteP". *ARTS-97*, vol. 1231 of LNCS, pp. 22-43, Springer-Verlag, 1997.
- [BMT99] M. Bozga, O. Maler, and S. Tripakis. "Efficient verification of timed automata using dense and discrete time semantics". In L. Pierre and T. Kropf (Eds.), *Proc CHARME'99*, Springer-Verlag, 1999.
- [Bur89] J. Burch. "Combining CTL, trace theory and timing models", *Automatic Verification Methods for Finite State Systems*, LNCS 407, 1989.
- [CES86] E. Clarke, E. Emerson, and A. Sistla. "Automatic verification of finite-state concurrent systems using temporal logic specifications". *ACM Transactions on Programming Languages and Systems*, 8(2):244-263, 1986.
- [CF58] H. Curry and R. Feys. *Combinatory Logic*, volume I. North-Holland, 1958.
- [CH85] T. Coquand and G. Huet. "Constructions: A higher order proof system for mechanizing mathematics". In *EUROCALL '85*, LNCS 203, Linz, 1985, Springer-Verlag.
- [CH88] T. Coquand and G. Huet. "The calculus of constructions". *Information and Computation*, 76(2/3), 1988.
- [CHR92] Z. Chaochen, C. Hoare, and A. Ravn. "A calculus of durations". *Information Processing Letters*, 40(5):269-276, 1992.
- [ChS95] K. Chandy and B. Sanders. "Predicate transformers for reasoning about concurrent computation". *Science of Computer programming*, 24:129-148, 1995.
- [Coq86] T. Coquand. "Metamathematical investigations of a calculus of constructions". INRIA and Cambridge, University, 1986.
- [Coq93] T. Coquand. "Infinite objects in type theory". In H. Barendregt and T. Nipkow, editors, *Workshop on Types for Proofs and Programs*, number 806 in LNCS, pages 62-78. Springer-Verlag, 1993.
- [Dij79] E. Dijkstra, "A Discipline of Programming". *Prentice-Hall, Englewood Cliffs, NJ*, 1976.
- [DOT<sup>+</sup>96] C. Daws, A. Olivero, S. Tripakis, and S. Yovine. "The tool Kronos". In *Hybrid Systems III, Verification and Control*, LNCS 1066, 1996.
- [DOY96] C. Daws, A. Olivero, and S. Yovine. "Verificación automática de sistemas temporizados utilizando KRONOS". *Jornadas de Informática y telecomunicaciones*, IEEE Uruguay, 1996.
- [DS97] R. Dijkstra and B. Sanders. "A predicate transformer for the progress property to-always". *Formal Aspects of Computing*, 9:270-282, 1997.

- [DY95] C. Daws and S. Yovine. “Verification of multirate timed automata with KRONOS: two exemples”. Technical Report Spectre-95-06, VERIMAG, 1995.
- [EC82] E. Amerson and E. Clarke. “Using branching-time temporal logic to synthesize synchronization skeletons”. *Science of Computer Programming*, 2:241-266,1982.
- [Eme95] E. Emerson. “Automated temporal reasoning about rective systems”. In *Logics for Concurrency*. Springer-Verlag, 1995.
- [EMS<sup>+</sup>89] E. Emerson, A. Mok, A. Sistla, and J. Srinivasan. “Quantitative temporal reasoning”. *Workshop on Automatic Verification Methods for Finite State Systems*, Grenoble, France, 1989.
- [Euz95] J. Euzenat. “An Algebraic approach to the granularity in time representation”. In *Proceedings of Time 95*, 1995.
- [Gim95] E. Giménez. “An application of Co-inductive Types in Coq: Verification of the Alternating Bit Protocol”. In *BRA Workshop on Types for Proofs and Programs (TYPES’95)*, LNCS 1158, pages 135-152, Springer-Verlag, 1995.
- [Gim96] E. Giménez. *A Calculus of Infinite Constructions and its application to the verification of communicating systems*. PhD thesis, Ecole Normale Supérieure de Lyon, 1996, Unité de Recherche Associée au CNRS No. 1398, 1996.
- [Gim98] E. Giménez. *A tutorial on recursive types in Coq*, Technical Report 0221, INRIA, 1998.
- [Gim99] E. Giménez. “Two Approaches to the Verification of Concurrent Programs in Coq”. To appear, 1999.
- [Gor93] M. Gordon. *Introduction to HOL: a theorem proving environment based for higher order logic*. Cambridge University, Press, 1993.
- [GPV94] A. Göllü, A. Puri, and P. Varaiya. “Discretization of timed automata”. *Proc. 33<sup>rd</sup> CDC*, Orlando, Florida, 1994.
- [Gri81] D. Gries. *The science of programming*, Springer-Verlag New York Inc., 1981.
- [HHW<sup>+</sup>97] T. Henzinger, P.-H. Ho, and H. Wong-Toi. “Hytech: a model checker for hybrid systems”. *Software Tools for Technology Transfer*, 1997.
- [HJL93] C. Heitmeyer, R. Jeffords, and B. Labaw. “A benchmark for comparing different approaches for specifying real-time systems”. *Real Time: Theory and Practice*, LNCS 600, REX Workshop, Mook, The Netherlands, 1991. Springer-Verlag.
- [HK94] T. Henzinger and O. Kopke. “Verification methods for the divergent runs of clock systems”. In *FTRTFT’94: Formal Techniques in Real-time and Fault-tolerant Systems*, volume 863 of LNCS, pages 351-372. Springer-Verlag, 1994.
- [HK97] T. Henzinger and O. Kupferman. “From quantity to quality”. In *Proc. of the First International Workshop on Hybrid and Real-Time Systems, HART’97*, LNCS 1201, pages 48-62, Springer-Verlag, 1997.
- [HKP96] G. Huet, G. Kahn, and C. Paulin-Mohring. *The Coq proof assistant version 6.1, A tutorial*, 1996.

- [HKV96] T. Henzinger, O. Kupferman, and M. Vardi. “A space-efficient on-the-fly algorithm for real-time model checking”. In *Proc 7<sup>th</sup> Conference on Concurrency Theory, LNCS 1119*, pages 514-529, Springer-Verlag, 1996.
- [HLP90] E. Harel, O. Lichtenstein, and A. Pnuelli. “Explicit clock temporal logic”. In *Proceedings of the 5<sup>th</sup> Annual Symposium on Logic in Computer Science*, pages 402-413, 1990.
- [HMP92] T. Henzinger, Z. Manna, and A. Pnuelli. “What good are digital clocks?”. In *W. Kuich, editor, ICALP 92: Automata, Languages and Programming, LNCS 623*, pages 545-558. Springer-Verlag, 1992.
- [HMP94] T. Henzinger, Z. Manna, and A. Pnuelli. “Temporal Proof Methodologies for Timed Transition Systems”. *Information and Computation* 112, pp. 273-337, 1994.
- [HNS<sup>+</sup>92] T. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. “Symbolic model-checking for real-time systems”. In *Proc. 7<sup>th</sup> Symp on Logics in Computer Science*. IEEE Computer Society Press, 1992.
- [Hob85] J. Hobbs. “Granularity”. In *Proceedings of the IJCAI 85*, pages 432-435. IJCAI, 1985.
- [How80] W. Howard. “The formulae-as-types notion of construction”. In J. Seldin and J. Hindley, editors, *To H. Curry: Essays on combinatory logic, lambda calculus and formalism*. Academic Press, 1980. A reprint of an unpublished manuscript from 1969.
- [HS96] K. Havelund and N. Shankar. “Experiments in Theorem Proving Model Checking for Protocol Verification”. In *proceedings of FME’96*, Oxford. LNCS 1051, pages 662-681, 1996.
- [JKR89] C. Julta, E. Knapp, and J. Rao. “A Predicate transformer approach to semantics of parallel programs”. In *Proceeding of the 8<sup>th</sup> ACM Symposium on Principles of Distributed Computing*, 1989.
- [KKP99] Y. Kesten, A. Klein, A. Pnuelli, and G. Raanan. “A Perfecto Verification: combining model checking with deductive analysis to verify real-life software”. In *FM’99*, Toulouse, France. LNCS 1709, pages 173-194, 1999.
- [Kna90] E. Knapp. “A predicate transformer for progress”. *Information Processing Letters*, 33, 1990.
- [Lam90] L. Lamport. “win and sin: predicate transformers for concurrency”. *ACM Transactions on Programming Languages and Systems*, 12(3), 1990.
- [LL95] F. Laroussinie and K. Larsen. “Compositional model checking of real time systems”. In *Proc. 6<sup>th</sup> Conference on Concurrency Theory*, pages 27-41, Philadelphia, Springer-Verlag, 1995.
- [LP92] Z. Luo and R. Pollack. “Lego proof development system: User’s manual”. *Technical Report ECS-LFCS-92-211*, LFCS, 1992.
- [LPY97] K. Larsen, P. Pettersson, and W. Yi. “Uppaal in a nutshell”. *Software Tools for Technology Transfer*, 1997.

- [LS85] N. Leveson and J. Stolzy. “Analyzing safety and fault tolerance using timed Petri nets”. In *Proc. Internat. Joint Conf. On Theory and Practice of Software Development, LNCS 186*, pages 339-355, Springer-Verlag, 1985.
- [Lun00] C. Luna. *Especificación y análisis de sistemas de tiempo real en teoría de tipos. Caso de estudio: the railroad crossing example*. Master thesis, Technical Report 00-01, InCo, PEDECIBA Informática, Fac. de Ingeniería, U. de la República, Uruguay, Febrero de 2000.
- [Lun98] C. Luna. “Sistemas Temporizados: Especificación, análisis y verificación. Estudio comparativo”. Reporte técnico 9806, InCo, Fac. de Ingeniería, U. de la República, Montevideo, Uruguay. 1998.
- [Mag94] L. Magnusson. *The implementation of ALF – a proof editor based on Martin Löf’s Monomorphic Type Theory with Explicit Substitution*. PhD thesis, Chalmers University of Göteborg, 1994.
- [May97] M. Mayero, “Le théorème des trois intervalles spécification et preuves en Coq”. *Rapport du DEA sémantique preuves et programmation*. Université Paris 6, 1997
- [MGJ91] D. Mandrioli, Carlo Ghezzi, and Mehdi Jazayeri. *Fundamentals of Software Engineering*. Prentice Hall, 1991.
- [MN95] Olaf Müller and T. Nipkow. “Combining Model Checking and Deduction for I/O-Automata”. In *Tools and Algorithms for the Construction and Analysis of Systems, LNCS 1019*, pages 1-16, 1995.
- [MP90] Z. Manna and A. Pnuelli. “A hierarchy of temporal properties”. In *Proceedings of the 9<sup>th</sup> Annual ACM Symposium on Principles of Distributed Computing*, pages 377-408. ACM Press, 1990.
- [MP91] Z. Manna and A. Pnueli. “Completing the temporal picture”. In *Theoretical Computer Science*, 83(1):97-130, 1991.
- [MP92] Z. Manna and A. Pnueli. “The temporal logic of reactive and concurrent systems: specification”. *Springer-Verlag*, Berlin, 1992.
- [MP95] Z. Manna and A. Pnueli. “Temporal verification of reactive systems: Safety”, *Springer-Verlag*, 1995.
- [Oli94] A. Olivero. *Modélisation et Analyse de Systèmes Temporisés et Hybrides*. PhD thesis, Institut National Polytechnique de Grenoble. France, 1994.
- [ORS92] S. Owre, J. Rushby, and N. Shankar. “PVS: A prototype verification system”. In Deepak Kapur, editor, *11<sup>th</sup> International Conference on Automated Deduction (CADE)*. LNIA 607, Saratoga, NY, 1992. Springer Verlag.
- [Ost87] J. Ostroff. *Temporal logic of real-time systems*, Ph.D. thesis, Univ. of Toronto, 1987.
- [Pau93a] L. Paulson. “Co-induction and Co-recursion in Higher-order Logic”. *Technical Report 304*, Computer Laboratory, University of Cambridge, 1993.
- [Pau93b] L. Paulson. “The Isabelle reference manual”. *Technical Report 283*, Computer Laboratory, University, 1993.
- [PL92] A. Pnueli and L. Lamport. “An old-fashioned recipe for real-time”. In J. W. De Baker, K. Huizing, W. P. De Roever, and G. Rozenberg, editors, *Real Time:*

*Theory in Practice*, LNCS 600, Springer-Verlag, 1992.

- [P-M89a] C. Paulin-Mohring. “Extracting  $F_\omega$ 's programs from proofs in the calculus of constructions”. In *Sixteenth Annual ACM Symposium on Principles of Programming Languages*, Austin, 1989. ACM.
- [P-M89b] C. Paulin-Mohring. *Extraction de programmes dans le calcul des constructions*. Thèse de doctorat, Université de Paris VII, 1989.
- [P-M93] C. Paulin-Mohring. “Inductive definitions in the system Coq – rules and properties”. In M. Bezem and J. Groote, editors, *Proceedings of the conference Typed Lambda Calculi and Applications*, LNCS 664, 1993.
- [Pnu81] A. Pnueli. “The temporal logic of programs”. *Theoretical Computer Science*, 1981.
- [Pnu85] A. Pnueli. “Linear and branching structures in the semantics and logics of reactive systems”. In *Proc. 12<sup>th</sup> ICALP, Nafplion*, LNCS 194, 1985.
- [RSS95] S. Rajan, N. Shankar, and M. Srivas. “An integration of model checking with automated proof checking”. In *Computer-Aided Verification, CAV'95*. LNCS 939, Belgium, 1995.
- [Sha93] N. Shankar. “Verification of real-time systems using PVS”. *CAV'93*, Costas Courcoubetis, editor, Elounda, Greece, LNCS 697, pages 280-291, 1993.
- [SS95] O. Sokolsky and S. Smolka. “Local model checking for real-time systems. In *Computer Aided Verification, Proc. 7<sup>th</sup> Int. Workshop*, Liege, LNCS 939, pages 211-224, 1995.
- [SS99] H. Saïdi and N. Shankar. “Abstract and model Check while you prove”. In *CAV'99*, Trento, Italy, 1999.
- [WH95] H. Wong-Toi and P. Ho. “Automated analysis of an audio control protocol”. In *Proc. in Computer Aided Verification*, 1995.
- [WL99] P. Weis et X. Leroy. “Le Langage CAML”. Second edition, Dunod, Paris, 1999. First edition, InterEditions, Paris, 1993.
- [Yov93] S. Yovine, *Méthodes et outils pour la vérification symbolique de systèmes temporisés*. PhD thesis, Institut National Polytechnique de Grenoble, France, 1993.
- [Yov97] S. Yovine. “Kronos: A verification tool for real-time systems”. *Software Tools for Technology Transfer*, 1997.

# Apéndice A

## *Nociones Temporales*

---

**time\_clocks.v** (disponible en <http://www.fing.edu.uy/~cluna>)

Versión de *Coq*: 6.2.2. Archivo generado con el utilitario *coq2html*.

---

**Require Export** Arith.

**Section** Time\_Clocks.

(\* Nociones temporales para tiempo discreto \*)

**Definition** Instant := nat.

**Definition** Clock := nat.

**Definition** lt\_Ck := lt. (\* < \*)

**Definition** le\_Ck := le. (\* ≤ \*)

**Definition** gt\_Ck := gt. (\* > \*)

**Definition** ge\_Ck := ge. (\* ≥ \*)

**Definition** eq\_Ck := [x,y:Clock] x=y. (\* = \*)

**Definition** Ini\_Ck : Instant := O.

**Definition** tick : Instant := (1).

**Definition** plus\_Ck := plus. (\* + \*)

**Definition** Inc := [x:Clock] (plus\_Ck x tick).

**Definition** Reset : Instant := O.

**Definition** time0 : Instant := O.

**End** Time\_Clocks.

---



# Apéndice B

## *Operadores Temporales: Definiciones y Propiedades*

---

**TemporalOperators.v** (disponible en <http://www.fing.edu.uy/~cluna>)

Versión de *Coq*: 6.2.2. Archivo generado con el utilitario *coq2html*.

---

### B.1 Invarianza y Alcanzabilidad (con Tipos Inductivos)

Implicit Arguments On.

Require time\_clocks. (\* nociones temporales para tiempo discreto \*)

(\* Las formalizaciones asumen declarado un tipo Label con una etiqueta distinguida Tick \*)

(\* Inductive Label : Set := L1 : Label | ... | Ln : Label | Tick : Label. \*)

#### B.1.1 Definiciones

Section TemporalOperators\_Ind.

**Variable** S : Set. (\* tipo de los estados \*)

**Variable** tr : S->Label->S->Prop. (\* transiciones del sistema \*)

(\* Estados alcanzables desde el estado "Sini" con transiciones "tr" \*)

**Inductive** RState [Sini:S]: S -> Prop :=

rsIni : (RState Sini Sini)

| rsNext : (s1,s2:S) (l:Label) (RState Sini s1) -> (tr s1 l s2) ->  
(RState Sini s2).

(\* Estados alcanzables en unidades de tiempo desde el estado "Sini" con transiciones "tr" \*)

**Inductive** RState\_T [Sini:S]: S -> Instant -> Prop :=

rsIni\_T : (RState\_T Sini Sini time0)

| rsTime\_T : (s1,s2:S) (t:Instant) (RState\_T Sini s1 t) -> (tr s1 Tick s2) ->  
(RState\_T Sini s2 (Inc t))

| rsNoTime\_T : (s1,s2:S) (l:Label) (t:Instant) (RState\_T Sini s1 t) -> ~(l=Tick) -> (tr s1 l s2) ->  
(RState\_T Sini s2 t).



(\* Init =>  $\forall \square P$  \*)

**Definition** ForAll := [Sini:S] [P:S->Prop]  
(s:S) (RState Sini s) -> (P s).

(\* Init =>  $\forall \square (\text{bound } t) P$  \*)

**Definition** ForAll\_T := [Sini:S] [P:S->Prop] [bound:Instant->Prop]  
(s:S) (t:Instant) (RState T Sini s t) -> (P s).

(\* Init =>  $\exists \diamond P$  \*)

**Inductive** Exists [Sini:S; P:S->Prop] : Prop :=  
exists : (s:S) (RState Sini s) -> (P s) -> (Exists Sini P).

(\* Init =>  $\exists \diamond (\text{bound } t) P$  \*)

**Inductive** Exists\_T [Sini:S; P:S->Prop; bound:Instant->Prop] : Prop :=  
exists\_T : (s:S) (t:Instant) (RState T Sini s t) -> (P s) -> (Exists T Sini P bound).

## B.1.2 Propiedades

**Theorem** Mon\_I : (Sini:S) (Pg,Pp:(S->Prop))  
(ForAll Sini Pg) -> ((s:S) (Pg s) -> (Pp s)) -> (ForAll Sini Pp).

**Proof.**  
Unfold ForAll; Intros.  
Apply H0.  
Apply H; Assumption.

**Qed.**

**Theorem** Mon\_I\_T : (Sini:S) (Pg,Pp:(S->Prop)) (bound:Instant->Prop)  
(ForAll\_T Sini Pg bound) -> ((s:S) (Pg s) -> (Pp s)) -> (ForAll\_T Sini Pp bound).

**Proof.**  
Unfold ForAll\_T; Intros.  
Apply H0.  
Apply (H s t); Assumption.

**Qed.**

**Theorem** Conj : (Sini:S) (P1,P2:(S->Prop))  
(ForAll Sini P1) -> (ForAll Sini P2) -> (ForAll Sini ([s:S] (P1 s)^(P2 s))).

**Proof.**  
Unfold ForAll; Intros.  
Split; [ Apply H | Apply H0 ]; Assumption.

**Qed.**

**Theorem** `Conj_T` : (Sini:S) (P1,P2:(S->Prop)) (bound:Instant->Prop)  
 (ForAll T Sini P1 bound) -> (ForAll T Sini P2 bound) ->  
 (ForAll T Sini ([s:S] (P1 s)^(P2 s)) bound).

**Proof.**

Unfold `ForAll_T`; Intros.

Split; [ Apply (H s t) | Apply (H0 s t) ]; Assumption.

**Qed.**

**Theorem** `Mon_I_EX` : (Sini:S) (Pg,Pp:(S->Prop))  
 (Exists Sini Pg) -> ((s:S) (Pg s) -> (Pp s)) -> (Exists Sini Pp).

**Proof.**

Intros.

Inversion\_clear H.

Apply (exists H1 (H0 s H2)).

**Qed.**

**Theorem** `Mon_I_EX_T` : (Sini:S) (Pg,Pp:(S->Prop)) (bound:Instant->Prop)  
 (Exists\_T Sini Pg bound) -> ((s:S) (Pg s) -> (Pp s)) -> (Exists\_T Sini Pp bound).

**Proof.**

Intros.

Inversion\_clear H.

Apply (exists\_T H1 H2 (H0 s H3)).

**Qed.**

**Lemma** `RState_Trans` : (s1,s2,s3:S) (RState s1 s2) -> (RState s2 s3) -> (RState s1 s3).

**Proof.**

Intros.

Elim H0; [ Assumption | Intros ].

Apply (rsNext H2 H3).

**Qed.**

**Lemma** `RState_Trans_T` : (s1,s2,s3:S) (t1,t2:Instant)  
 (RState\_T s1 s2 t1) -> (RState\_T s2 s3 t2) -> (RState\_T s1 s3 (plus\_Ck t1 t2)).

**Proof.**

Induction 2; Unfold `plus_Ck`; Intros.

Rewrite (`plus_sym` t1 `time0`); Unfold `time0`; Simpl; Assumption.

Unfold `Inc`; Unfold `plus_Ck`; Rewrite (`plus_assoc_l` t1 t `tick`).

Apply (`rsTime_T` H2 H3).

Apply (`rsNoTime_T` H2 H3 H4).

**Qed.**

**Theorem** `StepsEX` : (s1,s2:S) (P:S->Prop)  
 (RState s1 s2) -> (Exists s2 P) -> (Exists s1 P).

**Proof.**

Intros.

Inversion H0.

Apply (exists (RState\_Trans H H1) H2).

**Qed.**

**Require** Classical.

**Theorem** ForAll\_EX : (Sini:S) (P:S->Prop)  
 (ForAll Sini P) <-> ~(Exists Sini ([s:S]~(P s))).

**Proof.**

Unfold not; Unfold ForAll; Red; Intros; Split; Intros.  
 Inversion H0.  
 Apply (H2 (H s H1)).  
 Elim (classic (P s)); [ Trivial | Intro; Absurd (Exists Sini [s:S]~(P s)) ].  
 Assumption.  
 Apply exists with 1:=H0; Assumption.

**Qed.**

**Theorem** ForAll\_EX\_T: (Sini:S) (P:S->Prop) (bound:Instant->Prop)  
 (ForAll\_T Sini P bound) <-> ~(Exists\_T Sini ([s:S]~(P s)) bound).

**Proof.**

Unfold not; Unfold ForAll\_T; Red; Intros; Split; Intros.  
 Inversion H0.  
 Apply (H3 (H s t H1 H2)).  
 Elim (classic (P s)); [ Trivial | (Intro; Absurd (Exists\_T Sini [s:S]~(P s) bound)) ].  
 Assumption.  
 Apply exists\_T with 2:= H1; Assumption.

**Qed.**

### B.1.3 Definiciones Complementarias

(\* Q =>  $\forall \square P$  \*)

**Definition** ForAll\_from := [Sini:S] [Q,P:S->Prop]  
 (ForAll Sini ([s:S](Q s)->(ForAll s P))).  
 (\* (s:S) (RState Sini s) -> (Q s) -> (ForAll s P). \*)

(\* Q =>  $\forall \square(\text{bound } t) P$  \*)

**Definition** ForAll\_from\_T := [Sini:S] [Q,P:S->Prop] [bound:Instant->Prop]  
 (ForAll Sini ([s:S](Q s)->(ForAll\_T s P bound))).  
 (\* (s:S) (RState Sini s) -> (Q s) -> (ForAll\_T s P bound). \*)

(\* Q =>  $\exists \diamond P$  \*)

**Definition** Exists\_from := [Sini:S] [Q,P:S->Prop]  
 (ForAll Sini ([s:S](Q s)->(Exists s P))).  
 (\* (s:S) (RState Sini s) -> (Q s) -> (Exists s P). \*)

(\* Q =>  $\exists \diamond(\text{bound } t) P$  \*)

**Definition** Exists\_from\_T := [Sini:S] [Q,P:S->Prop] [bound:Instant->Prop]  
 (ForAll Sini ([s:S](Q s)->(Exists\_T s P bound))).  
 (\* (s:S) (RState Sini s) -> (Q s) -> (Exists\_T s P bound). \*)

**End** TemporalOperators\_Ind.

## B.2 Operadores CTL (con Tipos Co-Inductivos)

### B.2.1 Definiciones

**Infix** RIGHTA 9 "^" Cons.

**Section** TemporalOperators\_CTL.

**Variable** S : Set. (\* tipo de los estados \*)

**Variable** tr : S->Label->S->Prop. (\* transiciones del sistema \*)

**Syntactic Definition** SPath := (Stream S).

**CoInductive** ForAllS [P:SPath->Prop] : SPath->Prop :=  
forAllS : (x:SPath) (s:S) (P s^x) -> (ForAllS P x) -> (ForAllS P s^x).

**Inductive** ExistsS [P:SPath->Prop] : SPath->Prop :=  
Here : (x:SPath) (P x) -> (ExistsS P x)  
| Further : (x:SPath) (s:S) (ExistsS P x) -> (ExistsS P s^x).

(\* Trazas de ejecución \*)

**CoInductive** isTrace : SPath->Prop :=  
is\_trace : (x:SPath) (s1,s2:S) (l:Label) (tr s1 l s2) -> (isTrace s2^x) -> (isTrace s1^s2^x).

**Definition** isTraceFrom := [Sini:S] [x:SPath]  
Sini=(hd x) ^ (isTrace x).

(\* Definición del operador Until \*)

**Inductive** Until [P,Q:SPath->Prop] : SPath -> Prop :=  
UntilFurther : (s:S) (x:SPath) (P s^x) -> (Until P Q x) -> (Until P Q s^x)  
| UntilHere : (x:SPath) (Q x) -> (Until P Q x).

**Inductive** EX\_Until [Sini:S; P,Q:SPath->Prop] : Prop :=  
ExUntil : (x:SPath) (isTraceFrom Sini x) -> (Until P Q x) -> (EX\_Until Sini P Q).

**Definition** FA\_Until := [Sini:S] [P,Q:SPath->Prop]  
(x:SPath) (isTraceFrom Sini x) -> (Until P Q x).

(\* Init =>  $\forall \square P$  \*)

**Definition** Always := [Sini:S] [P:SPath->Prop]  
(x:SPath) (isTraceFrom Sini x) -> (ForAllS P x).

(\* Init =>  $\forall \diamond P$  \*)

**Definition** Inevitable := [Sini:S] [P:SPath->Prop]  
(x:SPath) (isTraceFrom Sini x) -> (ExistsS P x).

(\* Init =>  $\exists \diamond P$  \*)

**Inductive** Possible [Sini:S; P:SPath->Prop]: Prop :=  
 posible : (x:SPath) (isTraceFrom Sini x) -> (ExistsS P x) -> (Possible Sini P).

(\* Init =>  $\forall \exists \square P$  \*)

**Inductive** SafePath [Sini:S; P:SPath->Prop] : Prop :=  
 safePath : (x:SPath) (isTraceFrom Sini x) -> (ForAllS P x) -> (SafePath Sini P).

## B.2.2 Propiedades

**Theorem** Equiv1 : (Sini:S) (P:SPath->Prop)  
 (Possible Sini P) <-> (EX\_Until Sini ([\_:SPath] True) P).

**Proof.**

Unfold iff; Intros; Split; Intro.  
 Inversion\_clear H.  
 Apply ExUntil **with** P:=[\_:SPath]True 1:=H0.  
 Elim H1; Intros.  
 Constructor 2; Assumption.  
 Constructor 1; Trivial.  
 Inversion\_clear H.  
 Apply posible **with** 1:=H0.  
 Elim H1; Intros.  
 Constructor 2; Assumption.  
 Constructor 1; Assumption.

**Qed.**

**Theorem** Equiv2 : (Sini:S) (P:SPath->Prop)  
 (Inevitable Sini P) <-> (FA\_Until Sini ([\_:SPath] True) P).

**Proof.**

Unfold iff Inevitable FA\_Until; Intros; Split; Intros.  
 Elim (H x H0); Intros.  
 Constructor 2; Assumption.  
 Constructor 1; Trivial.  
 Elim (H x H0); Intros.  
 Constructor 2; Assumption.  
 Constructor 1; Assumption.

**Qed.**

**Lemma** ConsTrace : (s1,s2:S) (x,z:SPath)  
 (isTraceFrom s2 z) -> (isTraceFrom s1 s1^s2^x) -> (isTraceFrom s1 s1^z).

**Proof.**

Unfold isTraceFrom; Simpl.  
 Destruct z; Destruct 1; Destruct 3; Simpl; Intros.  
 Compute **in** H0; Rewrite H0 **in** H4.  
 Inversion\_clear H4.  
 Split; [ Trivial | Apply (is\_trace H5 H1) ].

**Qed.**

**Lemma** notPossible : (P:SPath->Prop) (s1:S) ~(Posible s1 P) ->  
 (z:SPath) (s2:S) (isTraceFrom s1 s1^s2^z) -> ~(Posible s2 P).

**Proof.**

Unfold 2 not; Intros.  
 Elim H1; Intros.  
 Apply H; Cut (isTraceFrom s1 (Cons s1 x)).  
 Intro H4; Apply (posible 2!P H4).  
 Apply Further; Assumption.  
 Apply ConsTrace with 1:=H2 2:=H0; Assumption.

**Qed.**

**Theorem** Equiv3 : (Sini:S) (P:SPath->Prop)  
 (Always Sini P) <-> ~(Posible Sini ([s:SPath]~(P s))).

**Proof.**

Unfold iff Always not; Intros; Split.  
 Intros H H0; Inversion\_clear H0.  
 Generalize (H x H1); Elim H2; Intros.  
 Inversion\_clear H3 in H0.  
 Apply (H0 H4).  
 Inversion\_clear H4.  
 Apply (H3 H6).  
 Generalize Sini; Cofix u.  
 Destruct x; Intros; Constructor.  
 Elim (classic (P s^s0)); [ Trivial | Intros ].  
 Absurd (Posible Sini0 [s:SPath]~(P s)).  
 Assumption.  
 Apply posible with 1:=H0.  
 Constructor 1; Assumption.  
 Elim H0; Simpl; Intros.  
 Apply (u (hd s0)); Intros.  
 Generalize H0; Clear H0; Generalize H3; Clear H3.  
 Rewrite **Case** s0; Simpl; Intros.  
 Apply (notPossible 1!([s:SPath]~(P s)) H H0); Assumption.  
 Inversion\_clear H2; Simpl.  
 Unfold isTraceFrom; Split; Trivial.

**Qed.**

**Lemma** not\_EX : (P:(Stream S)->Prop) (x:(Stream S)) (s:S)  
 ~(ExistsS P (Cons s x)) -> ~(ExistsS P x).

**Proof.**

Unfold not; Intros.  
 Apply (H (Further s H0)).

**Qed.**

**Theorem** Equiv4 : (Sini:S) (P:SPath->Prop)  
 (SafePath Sini P) <-> ~(Inevitable Sini ([s:SPath]~(P s))).

**Proof.**

Unfold iff Inevitable not; Intros; Split.  
 Intro sp; Inversion sp; Intros.  
 Generalize H0; Elim (H1 x H); Intros.  
 Inversion\_clear H3 in H2.  
 Apply (H2 H4).  
 Apply H3; Inversion\_clear H4; Assumption.  
 Intro H.  
 Elim (not\_all\_ex\_not (Stream S) [x:(Stream S)] (isTraceFrom Sini x)->(ExistsS [s:SPath]~(P s) x) H).  
 Intros.

Generalize (not\_imply\_elim2 (isTraceFrom Sini x) (ExistsS [s:SPath]~(P s) x) H0).  
 Generalize (not\_imply\_elim (isTraceFrom Sini x) (ExistsS [s:SPath]~(P s) x) H0); Intros.  
 Apply safePath **with** 1:=H1.  
 Generalize H1; Clear H1; Generalize H2; Clear H2.  
 Generalize x; Generalize Sini; Cofix u.  
 Destruct x; Intros; Constructor.  
 Elim (classic (P s^s0)); [ Trivial | Intro ].  
 Elim (H2 (Here 1!([s:SPath]~(P s) H3)).  
 Apply u **with** Sini:=(hd s0).  
 Generalize H2; Clear H2; **Case** s0; Unfold not; Intros.  
 Apply (not\_EX H2 H3).  
 Elim H1; Intros ig trace; Inversion\_clear trace.  
 Unfold isTraceFrom; Split; Trivial.  
**Qed.**

**Theorem** Mon\_I\_S : (x:SPath) (Pg,Pp:(SPath->Prop))  
 (ForAllS Pg x) -> ((s:SPath) (Pg s) -> (Pp s)) -> (ForAllS Pp x).

**Proof.**  
 Cofix u; Intro x; **Case** x; Intros.  
**Case** H; Constructor.  
 Apply (H0 s1^x0 H1).  
 Apply (u x0 Pg Pp H2 H0).

**Qed.**

**Theorem** Conj\_S : (x:SPath) (P1,P2:(SPath->Prop))  
 (ForAllS P1 x) -> (ForAllS P2 x) -> (ForAllS ([s:SPath] (P1 s)^(P2 s)) x).

**Proof.**  
 Cofix u; Intro x; **Case** x; Intros.  
 Inversion\_clear H; Inversion\_clear H0.  
 Constructor; [ Split | Apply (u s0) ]; Assumption.

**Qed.**

**Theorem** Mon\_I\_EX\_S : (x:SPath) (Pg,Pp:(SPath->Prop))  
 (ExistsS Pg x) -> ((s:SPath) (Pg s) -> (Pp s)) -> (ExistsS Pp x).

**Proof.**  
 Induction 1; Intros.  
 Constructor 1; Apply (H1 x0 H0).  
 Constructor 2; Apply (H1 H2).

**Qed.**

**Theorem** OneStep\_EX : (x:SPath) (P:SPath->Prop)  
 (ExistsS P x) -> (s:S) (ExistsS P s^x).

**Proof.**  
 Intros; Constructor 2; Assumption.

**Qed.**

**End** TemporalOperators\_CTL.

## B.3 Operadores TCTL (con Tipos Co-Inductivos)

### B.3.1 Definiciones

Section TemporalOperators\_TCTL.

**Variable** S : Set. (\* tipo de los estados \*)  
**Variable** tr : S->Label->S->Prop. (\* transiciones del sistema \*)  
**Variable** bound : Instant->Prop. (\* invariante de las locaciones \*)

**Syntactic Definition** State\_T := S \* Instant.

**Syntactic Definition** SPath\_T := (Stream State\_T).

(\* Trazas de ejecución \*)

**CoInductive** isTrace\_T : SPath\_T->Prop :=

isTraceTick: (x:SPath\_T) (s1,s2:S) (t:Instant) (tr s1 Tick s2) -> (isTrace\_T (s2,(Inc t)^x) ->  
(isTrace\_T ( (s1,t)^(s2,(Inc t)^x )

| isTraceDisc: (x:SPath\_T) (s1,s2:S) (t:Instant) (l:Label) (tr s1 l s2) -> ~l=Tick -> (isTrace\_T (s2,t)^x) ->  
(isTrace\_T ( (s1,t)^(s2,t)^x ).

**Definition** isTraceFrom\_T := [Sini:State\_T] [x:SPath\_T]

Sini=(hd x) ^ (isTrace\_T x).

(\* Definición del operador Until \*)

**Inductive** Until\_bound [P,Q:SPath\_T->Prop] : SPath\_T -> Prop :=

UntilFurther\_bound: (s:State\_T) (x:SPath\_T) (P s^x) -> (Until\_bound P Q x) ->  
(Until\_bound P Q s^x)

| UntilHere\_bound : (s:S) (t:Instant) (x:SPath\_T) (bound t) -> (Q (s,t)^x) ->  
(Until\_bound P Q (s,t)^x).

**Inductive** EX\_Until\_bound [Sini:State\_T; P,Q:SPath\_T->Prop] : Prop :=

ExUntil\_bound : (x:SPath\_T) (isTraceFrom\_T Sini x) -> (Until\_bound P Q x) ->  
(EX\_Until\_bound Sini P Q).

**Definition** FA\_Until\_bound := [Sini:State\_T] [P,Q:SPath\_T->Prop]

(x:SPath\_T) (isTraceFrom\_T Sini x) -> (Until\_bound P Q x).

(\* Init =>  $\forall \square$ (bound t) P \*)

**Definition** Always\_T := [Sini:State\_T] [P:SPath\_T->Prop]

(x:SPath\_T) (isTraceFrom\_T Sini x) -> (ForAllS ([s:SPath\_T](bound (Snd (hd s))) -> (P s)) x).

(\* Init =>  $\forall \diamond$ (bound t) P \*)

**Definition** Inevitable\_T := [Sini:State\_T] [P:SPath\_T->Prop]

(x:SPath\_T) (isTraceFrom\_T Sini x) -> (ExistsS ([s:SPath\_T](bound (Snd (hd s))) ^ (P s)) x).



(\* Init =>  $\exists \diamond$ (bound t) P \*)

**Inductive** Possible\_T [Sini:State\_T; P:SPath\_T->Prop] : Prop :=  
 posible\_T : (x:SPath\_T) (isTraceFrom\_T Sini x) -> (ExistsS ([s:SPath\_T](bound (Snd (hd s))))^(P s)) x ->  
 (Possible\_T Sini P).

(\* Init =>  $\exists \square$ (bound t) P \*)

**Inductive** SafePath\_T [Sini:State\_T; P:SPath\_T->Prop] : Prop :=  
 safePath\_T : (x:SPath\_T) (isTraceFrom\_T Sini x) ->  
 (ForAllS ([s:SPath\_T](bound (Snd (hd s))))->(P s)) x ->  
 (SafePath\_T Sini P).

### B.3.2 Propiedades

**Theorem** Equiv1\_T : (Sini:State\_T) (P:SPath\_T->Prop)  
 (Possible\_T Sini P) <-> (EX\_Until\_bound Sini ([\_ :SPath\_T] True) P).

**Proof.**

Unfold iff; Intros; Split; Intro.  
 Inversion\_clear H.  
 Apply ExUntil\_bound **with** P:=[\_ :SPath\_T]True 1:=H0.  
 Elim H1.  
 Destruct x; Simpl.  
 Destruct p; Destruct 1; Simpl; Intros.  
 Constructor 2; Assumption.  
 Destruct s; Intros.  
 Constructor 1; Trivial.  
 Inversion\_clear H.  
 Apply posible\_T **with** 1:=H0.  
 Elim H1.  
 Destruct s; Intros.  
 Constructor 2; Assumption.  
 Intros; Constructor 1; Simpl; Split; Assumption.

**Qed.**

**Theorem** Equiv2\_T : (Sini:State\_T) (P:SPath\_T->Prop)  
 (Inevitable\_T Sini P) <-> (FA\_Until\_bound Sini ([\_ :SPath\_T] True) P).

**Proof.**

Unfold iff Inevitable\_T FA\_Until\_bound; Intros; Split; Intros.  
 Elim (H x H0); Destruct x.  
 Destruct p; Intros.  
 Elim H1; Intros.  
 Constructor 2; Assumption.  
 Constructor 1; Trivial.  
 Elim (H x H0); Intros.  
 Constructor 2; Assumption.  
 Constructor 1; Split; Assumption.

**Qed.**

**Lemma**  $\text{ConsTrace\_T} : (s1, s2 : \text{State\_T}) (x, z : \text{SPath\_T})$   
 $(\text{isTraceFrom\_T } s2 \ z) \rightarrow (\text{isTraceFrom\_T } s1 \ s1^s2^x) \rightarrow (\text{isTraceFrom\_T } s1 \ s1^z)$ .

**Proof.**

Unfold  $\text{isTraceFrom\_T}$ ; Simpl.  
 Destruct  $z$ ; Destruct  $1$ ; Destruct  $3$ ; Simpl; Intros.  
 Compute **in**  $H0$ ; Rewrite  $H0$  **in**  $H4$ .  
 Inversion\_clear  $H4$  **in**  $H1$ .  
 Split; [ Trivial | Apply ( $\text{isTraceTick } H5 \ H1$ ) ].  
 Split; [ Trivial | Apply ( $\text{isTraceDisc } H5 \ H6 \ H1$ ) ].

**Qed.**

**Lemma**  $\text{notPossible\_T} : (P : \text{SPath\_T} \rightarrow \text{Prop}) (s1 : \text{State\_T}) \sim (\text{Possible\_T } s1 \ P) \rightarrow$   
 $(z : \text{SPath\_T}) (s2 : \text{State\_T}) (\text{isTraceFrom\_T } s1 \ s1^s2^z) \rightarrow \sim (\text{Possible\_T } s2 \ P)$ .

**Proof.**

Unfold  $2$  not; Intros.  
 Elim  $H1$ ; Intros.  
 Apply  $H$ ; Cut ( $\text{isTraceFrom\_T } s1 \ (\text{Cons } s1 \ x)$ ).  
 Intro  $H4$ ; Apply ( $\text{possible\_T } 2!P \ H4$ ).  
 Apply Further; Assumption.  
 Apply  $\text{ConsTrace\_T}$  **with**  $1 := H2 \ 2 := H0$ ; Assumption.

**Qed.**

**Theorem**  $\text{Equiv3\_T} : (\text{Sini} : \text{State\_T}) (P : \text{SPath\_T} \rightarrow \text{Prop})$   
 $(\text{Always\_T } \text{Sini } P) \leftrightarrow \sim (\text{Possible\_T } \text{Sini } ([s : \text{SPath\_T}] \sim (P \ s)))$ .

**Proof.**

Unfold iff  $\text{Always\_T}$  not; Intros; Split.  
 Intros  $H \ H0$ ; Inversion\_clear  $H0$ .  
 Generalize ( $H \ x \ H1$ ); Elim  $H2$ ; Intros.  
 Inversion\_clear  $H3$  **in**  $H0$ .  
 Elim  $H0$ ; Intros.  
 Elim ( $H6 \ (H4 \ H3)$ ).  
 Inversion\_clear  $H4$ .  
 Apply ( $H3 \ H6$ ).  
 Generalize  $\text{Sini}$ ; Cofix  $u$ .  
 Destruct  $x$ ; Intros; Constructor.  
 Intro; (Elim ( $\text{classic } (P \ p^s)$ )); [ Trivial | Intros ].  
 Absurd ( $\text{Possible\_T } \text{Sini}0 \ [s : \text{SPath\_T}] \sim (P \ s)$ ).  
 Assumption.  
 Apply  $\text{possible\_T}$  **with**  $1 := H0$ .  
 Constructor  $1$ ; Split; Assumption.  
 Elim  $H0$ ; Simpl; Intros.  
 Apply ( $u \ (\text{hd } s)$ ); Intros.  
 Generalize  $H0$ ; Clear  $H0$ ; Generalize  $H3$ ; Clear  $H3$ .  
 Rewrite **Case**  $s$ ; Simpl; Intros.  
 Apply ( $\text{notPossible\_T } 1!([s : \text{SPath\_T}] \sim (P \ s)) \ H \ H0$ ); Assumption.  
 Unfold  $\text{isTraceFrom\_T}$ ; Inversion\_clear  $H2$ ; Simpl.  
 Split; Trivial.  
 Split; Trivial.

**Qed.**

**Theorem**  $\text{Equiv4\_T} : (\text{Sini}:\text{State } T) (P:\text{SPath } T \rightarrow \text{Prop})$   
 $(\text{SafePath\_T Sini } P) \leftrightarrow \sim(\text{Inevitable\_T Sini } (\lambda s:\text{SPath } T. \sim(P s)))$ .

**Proof.**

Unfold iff  $\text{Inevitable\_T}$  not; Intros; Split.  
Intro sp; Inversion sp; Intros.  
Generalize H0; Elim (H1 x H); Intros.  
Inversion\_clear H3 in H2.  
Elim H2; Intros.  
Apply (H6 (H4 H3)).  
Apply H3; Inversion\_clear H4; Assumption.  
Intro H; Elim (not\_all\_ex\_not  $\text{SPath } T$  [x:SPath T] (isTraceFrom T Sini x) →  
 $(\exists s:\text{SPath } T. (\text{bound } (\text{Snd } (\text{hd } s))) \wedge \sim(P s) x) H)$ ).  
Intros.  
Generalize (not\_imply\_elim2 (isTraceFrom T Sini x)  
 $(\exists s:\text{SPath } T. (\text{bound } (\text{Snd } (\text{hd } s))) \wedge \sim(P s) x) H0)$ ).  
Generalize (not\_imply\_elim (isTraceFrom T Sini x)  
 $(\exists s:\text{SPath } T. (\text{bound } (\text{Snd } (\text{hd } s))) \wedge \sim(P s) x) H0)$ ; Intros.  
Apply safePath\_T with 1:=H1.  
Generalize H1; Clear H1; Generalize H2; Clear H2.  
Generalize x; Generalize Sini; Cofix u.  
Destruct x; Intros; Constructor.  
Elim (classic (P p^s)); [ Trivial | Intros ].  
Cut  $(\exists s0:(\text{Stream } S^*\text{Instant}). (\text{bound } (\text{Snd } (\text{hd } s0))) \wedge \sim(P s0) p^s)$ .  
Intro ex; Elim (H2 ex).  
Apply Here with P:= $(\lambda s:(\text{Stream } S^*\text{Instant}). (\text{bound } (\text{Snd } (\text{hd } s))) \wedge \sim(P s))$ .  
Split; Assumption.  
Apply u with Sini:=(hd s).  
Generalize H2; Clear H2; **Case** s; Unfold not; Intros.  
Apply (not\_EX H2 H3).  
Unfold isTraceFrom\_T; Elim H1; Intros ig trace; Inversion\_clear trace.  
Split; Trivial.  
Split; Trivial.  
**Qed.**

**End** TemporalOperators\_TCTL.

---

# Apéndice C

## *Especificación y Análisis del Sistema TCG*

---

**SystemTCG.v** (disponible en <http://www.fing.edu.uy/~cluna>)

Versión de *Coq*: 6.2.2. Archivo generado con el utilitario *coq2html*.

---

### C.1 Especificación

Implicit Arguments On.

**Require** time\_clocks. (\* nociones temporales para tiempo discreto \*)

**Section** Automatas\_TCG.

(\* Definición del conjunto de etiquetas de los autómatas, en un único tipo \*)

**Inductive** Label : Set := Approach : Label | In : Label | Exit: Label | Lower : Label  
| Raise : Label | Up : Label | Down : Label | Tick : Label.

(\* Tick es un label distinguido que representa a las transiciones temporales \*)

(\* Locaciones del tren ST, del controlador SC y de la barrera SG \*)

**Inductive** ST : Set := Far : ST | Near : ST | Inside : ST.  
**Inductive** SC : Set := Sc1 : SC | Sc2 : SC | Sc3 : SC | Sc4 : SC.  
**Inductive** SG : Set := Open : SG | Lowering : SG | Closed : SG | Raising: SG.

(\* Tipo de los estados con un reloj \*)

**Definition** S\_Ck := [S:Set] S \* Clock.

(\* Constantes del sistema \*)

**Definition** kt1 : Instant := (8).

**Definition** kt2 : Instant := (20).

**Definition** kc1 : Instant := (4).

**Definition** kc2 : Instant := (4).

**Definition** kg1 : Instant := (4).

**Definition** kg2 : Instant := (4).

**Definition** kg3 : Instant := (8).

(\* Invariantes de las locaciones del tren \*)

**Inductive** InvT : (S\_Ck ST) -> Prop :=  
 Ifar : (x:Clock) (InvT (Far,x))  
 | Inear : (x:Clock) (lt\_Ck x kt2) -> (InvT (Near,x))  
 | Inside : (x:Clock) (lt\_Ck x kt2) -> (InvT (Inside,x)).

(\* Invariantes de las locaciones del controlador \*)

**Inductive** InvC : (S\_Ck SC) -> Prop :=  
 Isc1 : (y:Clock) (InvC (Sc1,y))  
 | Isc2 : (y:Clock) (le\_Ck y kc1) -> (InvC (Sc2,y))  
 | Isc3 : (y:Clock) (InvC (Sc3,y))  
 | Isc4 : (y:Clock) (lt\_Ck y kc2) -> (InvC (Sc4,y)).

(\* Invariantes de las locaciones de la barrera \*)

**Inductive** InvG : (S\_Ck SG) -> Prop :=  
 Iopen : (z:Clock) (InvG (Open,z))  
 | Ilowering : (z:Clock) (lt\_Ck z kg1) -> (InvG (Lowering,z))  
 | Iclosed : (z:Clock) (InvG (Closed,z))  
 | Iraising : (z:Clock) (lt\_Ck z kg3) -> (InvG (Raising,z)).

(\* Transiciones del tren \*)

**Inductive** TrT : (S\_Ck ST) -> Label -> (S\_Ck ST) -> Prop :=  
 ttApproach : (x:Clock) (TrT (Far,x) Approach (Near, Reset))  
 | ttIn : (x:Clock) (gt\_Ck x kt1) -> (lt\_Ck x kt2) -> (TrT (Near,x) In (Inside,x))  
 | ttExit : (x:Clock) (lt\_Ck x kt2) -> (TrT (Inside,x) Exit (Far,x))  
 | ttTick : (x:Clock) (s:ST) (InvT (s, (Inc x))) -> (TrT (s,x) Tick (s, (Inc x))).

(\* Transiciones del controlador \*)

**Inductive** TrC : (S\_Ck SC) -> Label -> (S\_Ck SC) -> Prop :=  
 tcApproach : (y:Clock) (TrC (Sc1,y) Approach (Sc2,Reset))  
 | tcLower : (y:Clock) (eq\_Ck y kc1) -> (TrC (Sc2,y) Lower (Sc3,y))  
 | tcExit : (y:Clock) (TrC (Sc3,y) Exit (Sc4,Reset))  
 | tcRaise : (y:Clock) (lt\_Ck y kc2) -> (TrC (Sc4,y) Raise (Sc1,y))  
 | tcTick : (y:Clock) (s:SC) (InvC (s, (Inc y))) -> (TrC (s,y) Tick (s, (Inc y))).

(\* Transiciones de la barrera \*)

**Inductive** TrG : (S\_Ck SG) -> Label -> (S\_Ck SG) -> Prop :=  
 tgLower : (z:Clock) (TrG (Open,z) Lower (Lowering,Reset))  
 | tgDown : (z:Clock) (lt\_Ck z kg1) -> (TrG (Lowering,z) Down (Closed,z))  
 | tgRaise : (z:Clock) (TrG (Closed,z) Raise (Raising,Reset))  
 | tgUp : (z:Clock) (ge\_Ck z kg2) -> (lt\_Ck z kg3) -> (TrG (Raising,z) Up (Open,z))  
 | tgTick : (z:Clock) (s:SG) (InvG (s, (Inc z))) -> (TrG (s,z) Tick (s, (Inc z))).

(\* Tipo de los estados del sistema TCG \*)

**Definition** StGlobal := (S\_Ck ST) \* (S\_Ck SC) \* (S\_Ck SG).

(\* Transiciones del sistema compuesto train || controller || gate \*)

**Inductive** TrGlobal : StGlobal -> Label -> StGlobal -> Prop :=

```

| tGl_In      : (st1,st2:(S_Ck ST)) (TrT st1 In st2) -> (sc:(S_Ck SC)) (sg:(S_Ck SG))
              (TrGlobal (st1,(sc,sg)) In (st2,(sc,sg)))
| tGl_Down    : (sg1,sg2:(S_Ck SG)) (TrG sg1 Down sg2) -> (st:(S_Ck ST)) (sc:(S_Ck SC))
              (TrGlobal (st,(sc,sg1)) Down (st,(sc,sg2)))
| tGl_Up      : (sg1,sg2:(S_Ck SG)) (TrG sg1 Up sg2) -> (st:(S_Ck ST)) (sc:(S_Ck SC))
              (TrGlobal (st,(sc,sg1)) Up (st,(sc,sg2)))
| tGl_Approach: (st1,st2:(S_Ck ST)) (sc1,sc2:(S_Ck SC))
              (TrT st1 Approach st2) -> (TrC sc1 Approach sc2) -> (sg:(S_Ck SG))
              (TrGlobal (st1,(sc1,sg)) Approach (st2,(sc2,sg)))
| tGl_Exit    : (st1,st2:(S_Ck ST)) (sc1,sc2:(S_Ck SC))
              (TrT st1 Exit st2) -> (TrC sc1 Exit sc2) -> (sg:(S_Ck SG))
              (TrGlobal (st1,(sc1,sg)) Exit (st2,(sc2,sg)))
| tGl_Lower   : (sc1,sc2:(S_Ck SC)) (sg1,sg2:(S_Ck SG))
              (TrC sc1 Lower sc2) -> (TrG sg1 Lower sg2) -> (st:(S_Ck ST))
              (TrGlobal (st,(sc1,sg1)) Lower (st,(sc2,sg2)))
| tGl_Raise   : (sc1,sc2:(S_Ck SC)) (sg1,sg2:(S_Ck SG))
              (TrC sc1 Raise sc2) -> (TrG sg1 Raise sg2) -> (st:(S_Ck ST))
              (TrGlobal (st,(sc1,sg1)) Raise (st,(sc2,sg2)))
| tGl_Tick    : (st1,st2:(S_Ck ST)) (sc1,sc2:(S_Ck SC)) (sg1,sg2:(S_Ck SG))
              (TrT st1 Tick st2) -> (TrC sc1 Tick sc2) -> (TrG sg1 Tick sg2)->
              (TrGlobal (st1,(sc1,sg1)) Tick (st2,(sc2,sg2))).

```

(\* Estado inicial para el sistema TCG y para sus componentes \*)

**Definition** ini\_CkT := O.

**Definition** ini\_CkC := O.

**Definition** ini\_CkG := O.

**Definition** SiniT : (S\_Ck ST) := (Far, ini\_CkT).

**Definition** SiniC : (S\_Ck SC) := (Sc1, ini\_CkC).

**Definition** SiniG : (S\_Ck SG) := (Open, ini\_CkG).

**Definition** SiniTCG : StGlobal := (SiniT, (SiniC, SiniG)).

**End** Automatas\_TCG.

**Hint** Ifar Inear Iinside Isc1 Isc2 Isc3 Isc4 Iopen Ilowering Iclosed Iraising.

**Hint** ttApproach ttIn ttExit ttTick tcApproach tcLower tcExit tcRaise tcTick.

**Hint** tgLower tgDown tgRaise tgUp tgTick tGl\_In tGl\_Down tGl\_Up.

**Hint** tGl\_Approach tGl\_Exit tGl\_Lower tGl\_Raise tGl\_Tick.

## C.2 Análisis

**Load** TemporalOperators. (\* biblioteca de operadores temporales \*)

### C.2.1 Propiedades de los los Relojes y los Parámetros del Sistema

**Lemma** Trivial1 : (eq\_Ck ini\_CkT ini\_CkC).

**Proof.**

Unfold eq\_Ck ini\_CkT ini\_CkC; Trivial.

**Qed.**

**Lemma** Trivial2 : (x:Clock) (eq\_Ck x x).

**Proof.**

Unfold eq\_Ck; Trivial.

**Qed.**

**Lemma** Trivial3 : (x,y:Clock) (eq\_Ck x y) -> (eq\_Ck (Inc x) (Inc y)).

**Proof.**

Unfold eq\_Ck Inc; Intros x y eq\_x\_y; Rewrite eq\_x\_y; Trivial.

**Qed.**

**Lemma** Trivial4 : (x,y,z:Clock) (eq\_Ck x (plus\_Ck y z)) -> (eq\_Ck (Inc x) (plus\_Ck (Inc y) z)).

**Proof.**

Unfold eq\_Ck Inc plus\_Ck; Intros.

Rewrite H; Rewrite (plus\_assoc\_r y z tick); Rewrite (plus\_sym z tick); Trivial.

**Qed.**

**Lemma** Trivial5 : (x:Clock) (ge\_Ck x Reset).

**Proof.**

Unfold Clock ge\_Ck Reset; Auto.

**Qed.**

**Lemma** Trivial6 : (x,y:Clock) (ge\_Ck x y) -> (ge\_Ck (Inc x) (Inc y)).

**Proof.**

Unfold Clock ge\_Ck Inc plus\_Ck; Auto.

**Qed.**

**Lemma** Trivial7 : (x,y:Clock) (eq\_Ck x y) -> (ge\_Ck x y).

**Proof.**

Unfold Clock ge\_Ck eq\_Ck; Intros.

Rewrite H; Auto.

**Qed.**

**Lemma** Trivial8 : (x,y:Clock) (ge\_Ck x y) -> (ge\_Ck (Inc x) y).

**Proof.**

Unfold Clock ge\_Ck Inc plus\_Ck tick plus; Auto.

**Qed.**

**Lemma** Trivial9 : (x,y:Clock) (gt\_Ck x y) -> (gt\_Ck (Inc x) y).

**Proof.**

Unfold Clock gt\_Ck Inc plus\_Ck; Auto.

**Qed.**

**Lemma** Trivial10 : (x:Clock) (gt\_Ck x kt1) -> (gt\_Ck x kc1).

**Proof.**

Unfold Clock gt\_Ck kt1 kc1; Intros.

Apply (gt\_trans x (8) (4) H).

Unfold gt; Repeat (Apply lt\_n\_S); Apply lt\_O\_Sn.

**Qed.**

**Lemma** Trivial11 : (x:Clock) ~(gt\_Ck Reset x).

**Proof.**

Unfold Clock gt\_Ck Reset; Auto.

**Qed.**

**Lemma** Trivial12 : (x,y:Clock) (gt\_Ck (Inc x) y) -> (eq\_Ck x y)  $\vee$  (gt\_Ck x y).

**Proof.**

Unfold Clock Inc eq\_Ck gt\_Ck plus\_Ck tick; Intros x y.

Rewrite (plus\_sym x (1)); Simpl; Intros.

Elim (le\_lt\_or\_eq y x (gt\_S\_le y x H)); Auto.

**Qed.**

**Lemma** Trivial13 : (x,y,z:Clock) (gt\_Ck (Inc x) z) -> (eq\_Ck x y) ->  $\sim$ (le\_Ck (Inc y) z).

**Proof.**

Unfold Clock Inc plus\_Ck tick eq\_Ck le\_Ck gt\_Ck; Intros x y z.

Rewrite (plus\_sym x (1)); Rewrite (plus\_sym y (1)); Simpl; Intros.

Rewrite

**Qed.**

**Lemma** Trivial14 : (x:Clock) (gt\_Ck x kt1)  $\vee$  (eq\_Ck x kt1) -> (gt\_Ck x kc1).

**Proof.**

Unfold Clock kt1 kc1 tick eq\_Ck gt\_Ck; Intros.

Elim H; Intro H1; [ Apply (gt\_trans x (8) (4) H1) | Rewrite H1 ];

Unfold gt; Repeat (Apply lt\_n\_S); Apply lt\_O\_Sn .

**Qed.**

**Lemma** Trivial15 : (x,y,z:Clock) (eq\_Ck x kt1) -> (eq\_Ck x y) -> (eq\_Ck y (plus\_Ck z kc1)) ->  $\sim$ (lt\_Ck (Inc z) kg1).

**Proof.**

Unfold Clock kt1 kc1 kg1 Inc plus\_Ck tick eq\_Ck lt\_Ck; Intros.

Rewrite H in H0; Rewrite in H1.

Apply lt\_not\_sym.

Rewrite (plus\_sym z (4)) in H1; Rewrite (plus\_sym z (1)); Simpl.

Rewrite (plus\_minus (8) (4) z H1); Simpl.

Repeat (Apply lt\_n\_S); Apply lt\_O\_Sn.

**Qed.**

**Lemma** Trivial16: (x,y:Clock) (lt\_Ck x kc2) ->  $\sim$ (eq\_Ck x (plus\_Ck y kc1)).

**Proof.**

Unfold Clock kc1 kc2 eq\_Ck plus\_Ck tick lt\_Ck not; Intros.

Rewrite H0 in H; Elim (le\_not\_lt (4) (plus y (4)) (le\_plus\_r y (4)) H).

**Qed.**

**Lemma** Trivial17: (x,y,z:Clock) (eq\_Ck x y) -> (eq\_Ck x z) ->  $\sim$ (le\_Ck (Inc z) y).

**Proof.**

Unfold Clock eq\_Ck Inc plus\_Ck tick le\_Ck; Intros.

Rewrite

Rewrite plus\_sym; Simpl; Unfold not; Intro.

Elim (n\_Sn x (le\_antisym x (S x) (le\_n\_Sn x) H1)).

**Qed.**

**Lemma** Trivial18: (lt\_Ck (Inc Reset) kc2).

**Proof.**

Unfold lt\_Ck Inc tick plus\_Ck Reset kc2.

Rewrite (plus\_sym (0) (1)); Simpl.

Apply lt\_n\_S; Apply lt\_O\_Sn.

**Qed.**



**Lemma Trivial19:**  $(x,y,z:\text{Clock}) (\text{lt\_Ck } x \text{ kg1}) \rightarrow (\text{eq\_Ck } y (\text{plus\_Ck } x \text{ kc1})) \rightarrow (\text{eq\_Ck } z y) \rightarrow (\text{lt\_Ck } (\text{Inc } z) \text{ kt2}).$

**Proof.**

Unfold Clock lt\_Ck eq\_Ck Inc tick plus\_Ck kg1 kc1 kt2; Intros.  
 Rewrite **H0** **in** H1; Rewrite H1.  
 Rewrite (plus\_sym x (4)); Rewrite (plus\_sym (plus (4) x) (1)); Simpl.  
 Repeat (Apply lt\_n\_S).  
 Apply (lt\_le\_trans x (4) (15) H).  
 Repeat (Apply le\_n\_S); Apply le\_O\_n.

**Qed.**

**Lemma Trivial20:**  $(x,y,z:\text{Clock}) (\text{lt\_Ck } x \text{ kg1}) \rightarrow (\text{eq\_Ck } y (\text{plus\_Ck } x \text{ kc1})) \rightarrow (\text{eq\_Ck } z y) \rightarrow \sim(\text{gt\_Ck } z \text{ kt1}).$

**Proof.**

Unfold Clock gt\_Ck lt\_Ck eq\_Ck plus\_Ck kg1 kc1 kt1 gt; Intros.  
 Apply le\_not\_lt.  
 Rewrite **in** H0; Rewrite H0.  
 Generalize (lt\_reg\_r x (4) (4) H); Simpl; Intro.  
 Apply (lt\_le\_weak (plus x (4)) (8) (lt\_reg\_r x (4) (4) H)).

**Qed.**

**Lemma Trivial21:**  $(\text{lt\_Ck } (\text{Inc } \text{Reset}) \text{ kg3}).$

**Proof.**

Unfold lt\_Ck Inc tick plus\_Ck Reset kg3.  
 Rewrite (plus\_sym (0) (1)); Simpl.  
 Apply lt\_n\_S; Apply lt\_O\_Sn.

**Qed.**

**Lemma Trivial22:**  $(x,y:\text{Clock}) (\text{le\_Ck } x y) \rightarrow (\text{lt\_Ck } x y) \vee (\text{eq\_Ck } x y).$

**Proof.**

Unfold Clock le\_Ck lt\_Ck eq\_Ck; Intros.  
 Apply (le\_lt\_or\_eq x y H).

**Qed.**

**Lemma Trivial23:**  $(x,y:\text{Clock}) (\text{lt\_Ck } x \text{ kc1}) \rightarrow (\text{eq\_Ck } y x) \rightarrow (\text{lt } (\text{Inc } y) \text{ kt2}).$

**Proof.**

Unfold Clock lt\_Ck eq\_Ck Inc tick plus\_Ck kc1 kt2; Intros.  
 Rewrite **in** H; Rewrite (plus\_sym y (1)); Simpl.  
 Apply lt\_n\_S.  
 Apply (lt\_le\_trans y (4) (19) H).  
 Repeat (Apply le\_n\_S); Apply le\_O\_n.

**Qed.**

**Lemma Trivial24:**  $(x,y:\text{Clock}) (\text{lt\_Ck } x y) \rightarrow (\text{le\_Ck } (\text{Inc } x) y).$

**Proof.**

Unfold Clock lt\_Ck le\_Ck Inc tick plus\_Ck; Intros.  
 Rewrite (plus\_sym x (1)); Simpl.  
 Apply (lt\_le\_S x y H).

**Qed.**

**Lemma Trivial25:**  $(x,y:\text{Clock}) (\text{eq\_Ck } y \text{ kc1}) \rightarrow (\text{eq\_Ck } x y) \rightarrow (\text{lt\_Ck } (\text{Inc } x) \text{ kt2}).$

**Proof.**

Unfold Clock eq\_Ck lt\_Ck Inc tick plus\_Ck kc1 kt2; Intros.  
 Rewrite (plus\_sym x (1)); Simpl.  
 Apply lt\_n\_S.  
 Rewrite **H** **in** H0; Rewrite H0.  
 Repeat (Apply lt\_n\_S); Apply lt\_O\_Sn.

**Qed.**

**Lemma** Trivial26: (lt\_Ck (Inc Reset) kg1).

**Proof.**

Unfold lt\_Ck Inc plus\_Ck tick kg1 Reset.

Rewrite (plus\_sym (0) (1)); Simpl.

Apply lt\_n\_S; Apply lt\_O\_Sn.

**Qed.**

**Lemma** Trivial27: (lt\_Ck (Inc Reset) kt2).

**Proof.**

Unfold lt\_Ck Inc plus\_Ck tick kt2 Reset.

Rewrite (plus\_sym (0) (1)); Simpl.

Apply lt\_n\_S; Apply lt\_O\_Sn.

**Qed.**

**Lemma** Trivial28: (le\_Ck (Inc Reset) kc1).

**Proof.**

Unfold le\_Ck Inc plus\_Ck tick kc1 Reset.

Rewrite (plus\_sym (0) (1)); Simpl.

Apply le\_n\_S; Apply le\_O\_n.

**Qed.**

**Lemma** Trivial29: (x:Clock) (lt\_Ck x kg3) -> (lt\_Ck x kg2)  $\vee$  ((ge\_Ck x kg2)  $\wedge$  (lt\_Ck x kg3)).

**Proof.**

Unfold Clock lt\_Ck ge\_Ck kg2 kg3 ge; Intros.

Elim (le\_or\_lt (4) x); Auto.

**Qed.**

**Lemma** Trivial30: (x:Clock) (lt\_Ck x kg2) -> (lt\_Ck (Inc x) kg3).

**Proof.**

Unfold Clock lt\_Ck Inc plus\_Ck tick kg2 kg3; Intros.

Rewrite (plus\_sym x (1)); Simpl.

Apply lt\_n\_S.

Apply (lt\_le\_trans x (4) (7) H).

Repeat (Apply le\_n\_S); Apply le\_O\_n.

**Qed.**

**Lemma** Trivial31: (x,y:Clock) (eq\_Ck x kc1) -> (ge\_Ck y x) -> (ge\_Ck y kg2).

**Proof.**

Unfold Clock ge\_Ck eq\_Ck kc1 kg2 ge; Intros.

Rewrite H in H0; Assumption.

**Qed.**

**Lemma** not\_lt\_le: (x,y:nat)  $\sim$ (lt x y) -> (le y x).

**Proof.**

Unfold not; Intros x y no\_lt\_x\_y.

Elim (le\_or\_lt y x);

[ Trivial | (Intro lt\_x\_y; Elim (no\_lt\_x\_y lt\_x\_y)) ].

**Qed.**

**Lemma** Trivial32: (x:Clock) (lt\_Ck x kt2) ->  $\sim$ (lt\_Ck (Inc x) kt2) -> (gt\_Ck x kt1).

**Proof.**

Unfold Clock lt\_Ck gt\_Ck Inc plus\_Ck tick kt1 kt2 gt; Intros.

Generalize (not\_lt\_le H0); Rewrite (plus\_sym x (1)); Simpl; Intro.

Generalize (le\_antisym (19) x (le\_S\_n (19) x H1) (lt\_n\_Sm\_le x (19) H)); Intro H4; Rewrite

Repeat (Apply lt\_n\_S); Apply lt\_O\_Sn.

**Qed.**

**Lemma** not\_le\_lt: (x,y:nat)  $\sim$ (le x y) -> (lt y x).

**Lemma** Trivial33:  $(x:\text{Clock}) (\text{le\_Ck } x \text{ kc1}) \rightarrow \sim(\text{le\_Ck } (\text{Inc } x) \text{ kc1}) \rightarrow (\text{eq\_Ck } x \text{ kc1})$ .

**Proof.**

Unfold Clock le\_Ck eq\_Ck Inc plus\_Ck tick kc1; Intros.  
 Generalize (not\_le\_lt H0); Rewrite (plus\_sym x (1)); Simpl; Intro.  
 Apply (le\_antisym x (4) H (lt\_n\_Sm\_le (4) x H1)).

**Qed.**

**Lemma** Trivial34:  $(x:\text{Clock}) (\text{lt\_Ck } x \text{ kg3}) \rightarrow \sim(\text{lt\_Ck } (\text{Inc } x) \text{ kg3}) \rightarrow (\text{ge\_Ck } x \text{ kg2})$ .

**Proof.**

Unfold Clock lt\_Ck ge\_Ck Inc plus\_Ck tick kg3 kg2; Intros.  
 Generalize (not\_lt\_le H0); Rewrite (plus\_sym x (1)); Simpl; Intro.  
 Generalize (le\_antisym (7) x (le\_S\_n (7) x H1) (lt\_n\_Sm\_le x (7) H)); Intro H4; Rewrite  
 Unfold ge; Repeat (Apply le\_n\_S); Apply le\_O\_n.

**Qed.**

**Lemma** trivial\_inv\_1:  $(\text{lt\_Ck } \text{Reset } \text{kt2})$ .

**Proof.**

Unfold lt\_Ck Reset kt2; Auto.

**Qed.**

**Lemma** trivial\_inv\_2:  $(x:\text{Clock}) (\text{le\_Ck } \text{Reset } x)$ .

**Proof.**

Unfold Clock le\_Ck Reset; Auto.

**Qed.**

**Lemma** trivial\_inv\_3:  $(\text{lt\_Ck } \text{Reset } \text{kc2})$ .

Unfold lt\_Ck Reset kc2; Auto.

**Qed.**

**Lemma** trivial\_inv\_4:  $(\text{lt\_Ck } \text{Reset } \text{kg1})$ .

**Proof.**

Unfold lt\_Ck Reset kg1; Auto.

**Qed.**

**Lemma** trivial\_inv\_5:  $(\text{lt\_Ck } \text{Reset } \text{kg3})$ .

**Proof.**

Unfold lt\_Ck Reset kg3; Auto.

**Qed.**

(\* NOTA: Los lemas previos pueden ser demostrados también con la táctica automática Omega, de la biblioteca Omega. Deben hacerse todos los Unfold de las constantes, luego Intros y entonces Omega \*)

## C.2.2 Lemas de Inversión

(\* Lemas de inversión para las transiciones y los invariantes de las locaciones \*)

Derive Inversion\_clear cl\_TRT\_APPROACH **with** (st1,st2:(S\_Ck ST)) (TrT st1 Approach st2) Sort Prop.

Derive Inversion\_clear cl\_TRT\_IN **with** (st1,st2:(S\_Ck ST)) (TrT st1 In st2) Sort Prop.

Derive Inversion\_clear cl\_TRT\_EXIT **with** (st1,st2:(S\_Ck ST)) (TrT st1 Exit st2) Sort Prop.

Derive Inversion\_clear cl\_TRT\_INC\_TIME **with** (st1,st2:(S\_Ck ST)) (TrT st1 Tick st2) Sort Prop.

Derive Inversion\_clear cl\_TRC\_APPROACH **with** (sc1,sc2:(S\_Ck SC)) (TrC sc1 Approach sc2) Sort Prop.

Derive Inversion\_clear cl\_TRC\_LOWER **with** (sc1,sc2:(S\_Ck SC)) (TrC sc1 Lower sc2) Sort Prop.

Derive Inversion\_clear cl\_TRC\_EXIT **with** (sc1,sc2:(S\_Ck SC)) (TrC sc1 Exit sc2) Sort Prop.

Derive Inversion\_clear cl\_TRC\_RAISE **with** (sc1,sc2:(S\_Ck SC)) (TrC sc1 Raise sc2) Sort Prop.

Derive Inversion\_clear cl\_TRC\_INC\_TIME **with** (sc1,sc2:(S\_Ck SC)) (TrC sc1 Tick sc2) Sort Prop.

Derive Inversion\_clear cl\_TRG\_LOWER **with** (sg1,sg2:(S\_Ck SG)) (TrG sg1 Lower sg2) Sort Prop.

Derive Inversion\_clear cl\_TRG\_DOWN **with** (sg1,sg2:(S\_Ck SG)) (TrG sg1 Down sg2) Sort Prop.  
 Derive Inversion\_clear cl\_TRG\_RAISE **with** (sg1,sg2:(S\_Ck SG)) (TrG sg1 Raise sg2) Sort Prop.  
 Derive Inversion\_clear cl\_TRG\_UP **with** (sg1,sg2:(S\_Ck SG)) (TrG sg1 Up sg2) Sort Prop.  
 Derive Inversion\_clear cl\_TRG\_INC\_TIME **with** (sg1,sg2:(S\_Ck SG)) (TrG sg1 Tick sg2) Sort Prop.

Derive Inversion\_clear cl\_Ifar **with** (x:Clock) (InvT (Far,x)) Sort Prop.  
 Derive Inversion\_clear cl\_Inear **with** (x:Clock) (InvT (Near,x)) Sort Prop.  
 Derive Inversion\_clear cl\_Iinside **with** (x:Clock) (InvT (Inside,x)) Sort Prop.

Derive Inversion\_clear cl\_Isc1 **with** (y:Clock) (InvC (Sc1,y)) Sort Prop.  
 Derive Inversion\_clear cl\_Isc2 **with** (y:Clock) (InvC (Sc2,y)) Sort Prop.  
 Derive Inversion\_clear cl\_Isc3 **with** (y:Clock) (InvC (Sc3,y)) Sort Prop.  
 Derive Inversion\_clear cl\_Isc4 **with** (y:Clock) (InvC (Sc4,y)) Sort Prop.

Derive Inversion\_clear cl\_Iopen **with** (z:Clock) (InvG (Open,z)) Sort Prop.  
 Derive Inversion\_clear cl\_Ilowering **with** (z:Clock) (InvG (Lowering,z)) Sort Prop.  
 Derive Inversion\_clear cl\_Iclosed **with** (z:Clock) (InvG (Closed,z)) Sort Prop.  
 Derive Inversion\_clear cl\_Iraising **with** (z:Clock) (InvG (Raising,z)) Sort Prop.

### C.2.3 Algunas Tácticas Útiles

Tactic **Definition** Easy :=  
 [<tactic:<  
 Try Discriminate; Auto  
 >>].

Tactic **Definition** Easy2 :=  
 [<tactic:<  
 Intros; Try Discriminate; Auto  
 >>].

Tactic **Definition** Simpl\_or [Seq] :=  
 [<tactic:<  
 Elim Seq; Intro; Easy  
 >>].

Tactic **Definition** Simpl\_and [Seq] :=  
 [<tactic:<  
 Elim Seq; Intros; Easy  
 >>].

Tactic **Definition** Generalize\_Easy [Seq] :=  
 [<tactic:<  
 Generalize Seq; Intro; Easy  
 >>].

Tactic **Definition** Split3\_Trivial :=  
 [<tactic:<  
 Split; [ Auto | Split; Auto ]  
 >>].

Tactic **Definition** BeginForAll :=  
 [<tactic:<  
 Unfold ForAll; Induction 1; [ Simpl; Intros; Easy | Idtac ]  
 >>].

Tactic **Definition** SplitTrans :=

```
[<tactic:<
  Intros s1 s2 l rs_s1 p_s1 tr_gl;
  Generalize rs_s1; Clear rs_s1; Generalize p_s1; Clear p_s1;
  Elim tr_gl
>>].
```

Tactic **Definition** SplitTrans\_Simpl :=

```
[<tactic:<
  SplitTrans; [ Simpl_In | Simpl_Down | Simpl_Up | Simpl_Approach | Simpl_Exit
                | Simpl_Lower | Simpl_Raise | Simpl_Tick]
>>].
```

Tactic **Definition** Simpl\_In :=

```
[<tactic:<
  Intros st1 st2 trt_In;
  Inversion trt_In using cl_TRT_IN;
  Intros x gt_x_kt1 lt_x_kt2 sc sg;
  Elim sc; Elim sg;
  Simpl; Intros; Easy
>>].
```

Tactic **Definition** Simpl\_Down :=

```
[<tactic:<
  Intros sg1 sg2 trg_Down;
  Inversion trg_Down using cl_TRG_DOWN;
  Intros z lt_z_kg1 st sc;
  Elim st; Elim sc;
  Simpl; Intros; Easy
>>].
```

Tactic **Definition** Simpl\_Up :=

```
[<tactic:<
  Intros sg1 sg2 trg_Up;
  Inversion trg_Up using cl_TRG_UP;
  Intros z ge_z_kg2 lt_z_kg3 st sc;
  Elim st; Elim sc;
  Simpl; Intros; Easy
>>].
```

Tactic **Definition** Simpl\_Approach :=

```
[<tactic:<
  Intros st1 st2 sc1 sc2 trt_Approach trc_Approach;
  Inversion trt_Approach using cl_TRT_APPROACH;
  Inversion trc_Approach using cl_TRC_APPROACH;
  Intros y x sg;
  Elim sg;
  Simpl; Intros; Easy
>>].
```

Tactic **Definition** Simpl\_Exit :=

```
[<tactic:<
  Intros st1 st2 sc1 sc2 trt_Exit trc_Exit;
  Inversion trt_Exit using cl_TRT_EXIT;
  Inversion trc_Exit using cl_TRC_EXIT;
  Intros y x lt_x_kt2 sg;
  Elim sg;
  Simpl; Intros; Easy
>>].
```

Tactic **Definition** Simpl\_Lower :=  
 [<tactic:<  
 Intros sc1 sc2 sg1 sg2 trc\_Lower trg\_Lower;  
 Inversion trc\_Lower using cl\_TRC\_LOWER;  
 Inversion trg\_Lower using cl\_TRG\_LOWER;  
 Intros z y eq\_y\_kc1 st;  
 Elim st;  
 Simpl; Intros; Easy  
 >>].

Tactic **Definition** Simpl\_Raise :=  
 [<tactic:<  
 Intros sc1 sc2 sg1 sg2 trc\_Raise trg\_Raise;  
 Inversion trc\_Raise using cl\_TRC\_RAISE;  
 Inversion trg\_Raise using cl\_TRG\_RAISE;  
 Intros z y lt\_y\_kc2 st;  
 Elim st;  
 Simpl; Intros; Easy  
 >>].

Tactic **Definition** Simpl\_Tick :=  
 [<tactic:<  
 Intros st1 st2 sc1 sc2 sg1 sg2 trt\_Tick trc\_Tick trg\_Tick;  
 Inversion trt\_Tick using cl\_TRT\_INC\_TIME;  
 Inversion trc\_Tick using cl\_TRC\_INC\_TIME;  
 Inversion trg\_Tick using cl\_TRG\_INC\_TIME;  
 Simpl; Intros; Easy  
 >>].

## C.2.4 Invariantes y Propiedad de *Safety*: Demostraciones

**Syntactic Definition** InvTCG := [s:StGlobal] **Cases** s of (st\_x,(sc\_y,sg\_z)) =  
 (InvT st\_x)  $\wedge$  (InvC sc\_y)  $\wedge$  (InvG sg\_z) **end**.

**Syntactic Definition** ForAll\_TCG := (ForAll TrGlobal).

**Syntactic Definition** Exists\_TCG := (Exists TrGlobal).

(\* El estado inicial del sistema TCG satisface el invariante de las locaciones \*)

**Lemma** Inv\_SiniTCG : (InvTCG SiniTCG).

**Proof.**

Simpl; Unfold SiniT SiniC SiniG; Split3 Trivial.

**Qed.**

**Definition** Inv1 := [s:StGlobal] **Cases** s of ((st,\_),((sc,\_),(sg,\_))) =  
 st=Near  $\vee$  st=Inside  $\rightarrow$  sc=Sc3  $\rightarrow$  sg=Closed  $\vee$  sg=Lowering **end**.

**Lemma** lema\_Inv1 : (ForAll TCG SiniTCG Inv1).

**Proof.**

BeginForAll.

SplitTrans Simpl.

Simpl\_or (p\_s1 H0 H1).

**Qed.**

**Hint** lema\_Inv1.

**Definition** Inv2 := [s:StGlobal] **Cases** s of ((st,\_),((sc,\_),(sg,\_))) =  
st=Far -> sg=Open\sg=Raising -> sc=Sc1 **end**.

**Lemma** lema\_Inv2 : (ForAll TCG SiniTCG Inv2).

**Proof.**

BeginForAll.

SplitTrans Simpl.

Simpl or H1.

Elim (lema\_Inv1 rs\_s1 (or\_intror Inside=Near Inside=Inside (refl\_equal ST Inside)) (refl\_equal SC Sc3));

Intro H2; Rewrite H2 in H1; Simpl or H1.

Simpl or H1.

**Qed.**

**Hint** lema\_Inv2.

**Definition** Inv3 := [s:StGlobal] **Cases** s of ((st,x),((\_,y),\_)) =  
st=Near\st=Inside -> (eq\_Ck x y) **end**.

**Lemma** lema\_Inv3 : (ForAll TCG SiniTCG Inv3).

**Proof.**

BeginForAll.

Apply Trivial1.

SplitTrans Simpl.

Apply (Trivial2 Reset.)

Simpl or H0.

Apply (Trivial3 (p\_s1 H3).)

**Qed.**

**Hint** lema\_Inv3.

**Definition** Inv4 := [s:StGlobal] **Cases** s of ((st,\_),((sc,\_),\_)) =  
st=Near -> sc=Sc2\sc=Sc3 **end**.

**Lemma** lema\_Inv4 : (ForAll TCG SiniTCG Inv4).

**Proof.**

BeginForAll.

SplitTrans Simpl.

Simpl or (p\_s1 H0).

**Qed.**

**Hint** lema\_Inv4.

**Definition** Inv5 := [s:StGlobal] **Cases** s of ((st,\_),((sc,y),(\_,z))) =  
st=Near -> sc=Sc3 -> (eq\_Ck y (plus\_Ck z kc1)) **end**.

**Lemma** lema\_Inv5 : (ForAll TCG SiniTCG Inv5).

**Proof.**

BeginForAll.

SplitTrans Simpl.

Apply (Trivial4 (p\_s1 H3 H4).)

**Qed.**

**Hint** lema\_Inv5.

**Definition** Inv6 := [s:StGlobal] **Cases** s of ((st,x),((sc,\_),\_)) =  
st=Near\(\gt\_Ck x kc1) \st=Inside -> sc=Sc3 **end**.

**Lemma** lema\_Inv6 : (ForAll TCG SiniTCG Inv6).

**Proof.**

BeginForAll.

Decompose [and or] H0; Discriminate.

SplitTrans Simpl.

Apply p\_s1; Left; Split; [ Auto | Apply (Trivial10 gt\_x kt1) ].

Decompose [and or] H0; [ Elim (Trivial11 H3) | Discriminate ].

Decompose [and or] H0; Discriminate.

Generalize Easy (p\_s1 H0).

Decompose [and or] H3; [ Elim (Trivial12 H6) | Auto ].

Elim (lema\_Inv4 rs\_s1 H4); [Generalize (lema\_Inv3 rs\_s1 (or\_introl s4=Near s4=Inside H4)); Intros | Auto].

Rewrite H7 in H1; Inversion H1 using cl\_Isc2; Intro H9; Elim (Trivial13 H6 H5 H9).

Intro H7; Apply p\_s1; Left; Split; [ Assumption | Generalize Easy (Trivial9 H7) ].

**Qed.**

**Hint** lema\_Inv6.

**Definition** Inv7 := [s:StGlobal] **Cases** s of ((st,\_),((sc,\_),(sg,\_))) =  
st=Near∨st=Inside -> sc=Sc3 -> sg=Lowering∨sg=Closed **end.**

**Lemma** lema\_Inv7 : (ForAll TCG SiniTCG Inv7).

**Proof.**

BeginForAll.

SplitTrans Simpl.

Simpl\_or (p\_s1 H0 H1).

**Qed.**

**Hint** lema\_Inv7.

**Definition** Inv8 := [s:StGlobal] **Cases** s of ((st,x),((sc,\_),(sg,\_))) =  
st=Near^(gt\_Ck x kt1) ∨ st=Inside -> sg=Closed **end.**

**Lemma** lema\_Inv8 : (ForAll TCG SiniTCG Inv8).

**Proof.**

BeginForAll.

Decompose [and or] H0; Discriminate.

SplitTrans Simpl.

Generalize Easy (p\_s1 H0).

Decompose [and or] H0; [ Elim (Trivial11 H3) | Discriminate ].

Generalize Easy (p\_s1 H0).

Generalize (lema\_Inv6 rs\_s1); Simpl; Intro.

Decompose [and or] H0.

Generalize Easy (H1 (or\_introl y0=Near^(gt\_Ck y1 kt1) y0=Inside <(y0=Near),(gt\_Ck y1 kt1)>  
{H2, (Trivial14 (or\_introl (gt\_Ck y1 kt1) (eq\_Ck y1 kt1) H4)})))).

Generalize Easy (H1 (or\_intror y0=Near^(gt\_Ck y1 kt1) y0=Inside H3)).

Decompose [and or] H3; [ Simpl\_or (Trivial12 H6) | Auto ].

Generalize (lema\_Inv6 rs\_s1 (or\_introl s4=Near^(gt\_Ck x kt1) s4=Inside <(s4=Near),(gt\_Ck x kt1)>  
{H4, (Trivial14 (or\_intror (gt\_Ck x kt1) (eq\_Ck x kt1) H5)})))); Intro.

Simpl\_or (lema\_Inv1 rs\_s1 (or\_introl s4=Near s4=Inside H4) H7).

Rewrite H8 in H0; Inversion H0 using cl\_lowering; Intro.

Elim (Trivial15 H5 (lema\_Inv3 rs\_s1 (or\_introl s4=Near s4=Inside H4)) (lema\_Inv5 rs\_s1 H4 H7) H9).

**Qed.**

**Hint** lema\_Inv8.

**Definition** safeTCG := [s:StGlobal] **Cases** s of ((st,\_),(\_,(sg,\_))) =  
st=Inside -> sg=Closed **end.**



**Lemma** *lema\_safeTCG* : (ForAll TCG SiniTCG safeTCG).

**Proof.**

Apply *Mon\_I* with *Pg:=Inv8 Pp:=safeTCG*; [ *Auto* | (Unfold *Inv8 safeTCG*; *Simpl*) ].

Unfold *Inv8 safeTCG*; *Simpl*; *Intro* s; *Elim* s.

*Intros* y y0; *Elim* y; *Elim* y0;

*Intros* y1 y2 y3 y4; *Elim* y1; *Elim* y2; *Auto*.

**Qed.**

**Hint** *lema\_safeTCG*.

**Definition** *Inv9* := [s:StGlobal] **Cases** s of ((st,x),((\_,y),(\_,z))) =  
st=Near^(gt\_Ck x kc1) ∨ st=Inside -> (eq\_Ck y (plus\_Ck z kc1)) **end**.

**Lemma** *lema\_Inv9* : (ForAll TCG SiniTCG *Inv9*).

**Proof.**

*BeginForAll*.

*Decompose* [and or] *H0*; *Discriminate*.

*SplitTrans* *Simpl*.

Apply *p\_s1*; *Left*; *Split*; [ *Auto* | Apply (*Trivial10* *gt\_x\_kt1*) ].

*Decompose* [and or] *H0*; [ *Elim* (*Trivial11* *H3*) | *Discriminate* ].

*Decompose* [and or] *H0*; *Discriminate*.

*Elim* (*Trivial16* *lt\_y\_kc2* (*p\_s1* *H0*)).

*Decompose* [and or] *H3*.

*Elim* (*Trivial12* *H6*); *Intro*.

*Elim* (*lema\_Inv4* *rs\_s1* *H4*); *Intro*.

*Rewrite* *H7* in *H1*; *Inversion* *H1* using *cl\_Isc2*; *Intro*.

*Generalize* (*lema\_Inv3* *rs\_s1* (or\_introl *s4*=Near *s4*=Inside *H4*)); *Intro*.

*Elim* (*Trivial17* *H5* *H9* *H8*).

Apply (*Trivial4* (*lema\_Inv5* *rs\_s1* *H4* *H7*)).

Apply *Trivial4*; Apply *p\_s1*; *Left*; *Split*; *Assumption*.

Apply (*Trivial4* (*p\_s1* (or\_intror *s4*=Near^(gt\_Ck x kc1) *s4*=Inside *H5*))).

**Qed.**

**Hint** *lema\_Inv9*.

**Definition** *Inv10* := [s:StGlobal] **Cases** s of (\_,((sc,\_),(sg,\_))) =  
sc=Sc1∨sc=Sc2 -> sg=Open∨sg=Raising **end**.

**Lemma** *lema\_Inv10* : (ForAll TCG SiniTCG *Inv10*).

**Proof.**

*BeginForAll*.

*SplitTrans* *Simpl*.

*Simpl* or (*p\_s1* *H0*).

*Simpl* or *H0*.

*Simpl* or *H0*.

**Qed.**

**Hint** *lema\_Inv10*.

**Definition** *Inv11* := [s:StGlobal] **Cases** s of (\_,((sc,\_),(sg,\_))) =  
sg=Lowering∨sg=Closed -> sc=Sc3∨sc=Sc4 **end**.

**Lemma** lema\_Inv11 : (ForAll TCG SiniTCG Inv11).

**Proof.**

Generalize (Mon\_I 2!TrGlobal 3!SiniTCG 4!Inv10 5!Inv11); Unfold ForAll; Intros.

Apply H; [ Auto | Idtac | Assumption ].

Unfold Inv10 Inv11; Simpl; Intro.

Elim s0; Do 2 Intro; Elim y; Elim y0; Do 4 Intro; Elim y1; Elim y2.

Intros sg ck sc; Elim sg.

Intros ck1 H1 H2; Simpl or H2.

Elim sc; Intros ck1 H1; [ (Elim H1; Easy2) | (Elim H1; Easy2) | (Left; Auto) | (Right; Auto) ].

Elim sc; Intros ck1 H1; [ (Elim H1; Easy2) | (Elim H1; Easy2) | (Left; Auto) | (Right; Auto) ].

Intros ck1 H1 H2; Simpl or H2.

**Qed.**

**Hint** lema\_Inv11.

**Definition** Inv12 := [s:StGlobal] **Cases** s of (\_,((sc,y),(\_,z))) =  
sc=Sc2 -> (ge\_Ck z y) **end**.

**Lemma** lema\_Inv12:(ForAll TCG SiniTCG Inv12).

**Proof.**

BeginForAll.

SplitTrans Simpl.

Apply Trivial5.

Apply (Trivial6 (p\_s1 H3)).

**Qed.**

**Hint** lema\_Inv12.

**Definition** Inv13 := [s:StGlobal] **Cases** s of ((st,\_),((sc,\_),\_)) =  
sc=Sc2 -> st=Near **end**.

**Lemma** lema\_Inv13 : (ForAll TCG SiniTCG Inv13).

**Proof.**

BeginForAll.

SplitTrans Simpl.

Generalize (lema\_Inv6 rs\_s1); Simpl.

Rewrite H0.

Intro H1; Generalize Easy (H1 (or\_introl Near=Near^(gt\_Ck x kc1) Near=Inside  
<(Near=Near),(gt\_Ck x kc1)> {(refl\_equal ST Near),(Trivial10 gt\_x\_kt1)})).

**Qed.**

**Hint** lema\_Inv13.

**Definition** Inv14 := [s:StGlobal] **Cases** s of ((st,\_),((sc,\_),(sg,\_))) =  
sc=Sc4 -> st=Far^sg=Closed **end**.

**Lemma** lema\_Inv14 : (ForAll TCG SiniTCG Inv14).

**Proof.**

BeginForAll.

SplitTrans Simpl.

Simpl and (p\_s1 H0).

Simpl and (p\_s1 H0).

Simpl and (p\_s1 H0).

Split; [ Auto | Apply (lema\_safeTCG rs\_s1 (refl\_equal ST Inside)) ].

**Qed.**

**Hint** lema\_Inv14.

**Definition**  $\text{InvSc3} := [s:\text{StGlobal}] \text{Cases } s \text{ of } (\_,((sc,y),\_)) =$   
 $sc=\text{Sc3} \rightarrow (\text{ge\_Ck } y \text{ kc1}) \text{ end.}$

**Lemma**  $\text{lema\_InvSc3} : (\text{ForAll\_TCG SiniTCG InvSc3}).$

**Proof.**

BeginForAll.

SplitTrans\_Simpl.

Apply (Trivial7 eq\_y\_kc1).

Apply (Trivial8 (p\_s1 H3)).

**Qed.**

**Hint** lema\_InvSc3.

**Definition**  $\text{InvInside} := [s:\text{StGlobal}] \text{Cases } s \text{ of } ((st,x),\_) =$   
 $st=\text{Inside} \rightarrow (\text{gt\_Ck } x \text{ kt1}) \text{ end.}$

**Lemma**  $\text{lema\_InvInside} : (\text{ForAll\_TCG SiniTCG InvInside}).$

**Proof.**

BeginForAll.

SplitTrans\_Simpl.

Apply (Trivial9 (p\_s1 H3)).

**Qed.**

**Hint** lema\_InvInside.

**Lemma**  $\text{INV\_TCG\_general} : (s:\text{StGlobal}) (\text{InvTCG } s) \rightarrow (\text{ForAll\_TCG } s \text{ InvTCG}).$

**Proof.**

Intros.

BeginForAll.

SplitTrans\_Simpl ; Elim p\_s1; Intros H1 H2; Elim H2; Intros; Auto; (Split; [ Auto | Split; Auto ]).

Apply Inear; Apply trivial\_inv\_1.

Apply Isc2; Apply trivial\_inv\_2.

Apply Isc4; Apply trivial\_inv\_3.

Apply llowering; Apply trivial\_inv\_4.

Apply lraising; Apply trivial\_inv\_5.

**Qed.**

**Hint** INV\_TCG\_general.

**Lemma**  $\text{INV\_T\_general} : (s1,s2:\text{StGlobal}) (\text{InvTCG } s1) \rightarrow (\text{RState TrGlobal } s1 \text{ } s2) \rightarrow (\text{InvT } (\text{Fst } s2)).$

**Proof.**

Intros.

Generalize (INV\_TCG\_general H H0).

Elim s2; Simpl.

Intros st\_sc\_sg.

Elim sc\_sg; Intros.

Elim H1; Auto.

**Qed.**

**Lemma**  $\text{INV\_C\_general} : (s1,s2:\text{StGlobal}) (\text{InvTCG } s1) \rightarrow (\text{RState TrGlobal } s1 \text{ } s2) \rightarrow (\text{InvC } (\text{Fst } (\text{Snd } s2))).$

**Proof.**

Intros.

Generalize (INV\_TCG\_general H H0).

Elim s2; Simpl.

Intros st\_sc\_sg.

Elim sc\_sg; Simpl; Intros.

Elim H1; Intros inv\_T inv\_C\_G; Elim inv\_C\_G; Auto.

**Qed.**

**Lemma**  $\text{INV\_G\_general} : (s1,s2:\text{StGlobal}) (\text{InvTCG } s1) \rightarrow (\text{RState TrGlobal } s1 \ s2) \rightarrow (\text{InvG } (\text{Snd } (\text{Snd } s2)))$ .

**Proof.**

Intros.

Generalize ( $\text{INV\_TCG\_general } H \ H0$ ).

Elim  $s2$ ; Simpl.

Intros  $st \ sc\_sg$ .

Elim  $sc\_sg$ ; Simpl; Intros.

Elim  $H1$ ; Intros  $inv\_T \ inv\_C\_G$ ; Elim  $inv\_C\_G$ ; Auto.

**Qed.**

## C.2.5 Propiedad de *Liveness Non-Zeno*

### Lemas, Definiciones y Tácticas Auxiliares

**Lemma**  $\text{InvT}' : (s:(\underline{S\_Ck} \ \underline{ST})) \text{Cases } s \text{ of } (st,x) =$   
 $st=\text{Far} \vee st=\text{Near} \wedge (\underline{lt\_Ck} \ x \ \underline{kt2}) \vee st=\text{Inside} \wedge (\underline{lt\_Ck} \ x \ \underline{kt2}) \rightarrow (\text{InvT } s) \text{ end.}$

**Proof.**

Intro  $s$ ; Elim  $s$ .

Intros.

Elim  $H$ ; [ Intro  $st$ ; Rewrite  $st$ ; Auto | Intro  $n\_i$ ; Elim  $n\_i$ ; Intro  $H1$ ; Elim  $H1$ ; Intros  $st \ cond$ ; Rewrite  $st$ ;

[ Apply  $\text{Inear}$  | Apply  $\text{Iinside}$  ]; Auto ].

**Qed.**

**Lemma**  $\text{InvC}' : (s:(\underline{S\_Ck} \ \underline{SC})) \text{Cases } s \text{ of } (sc,y) =$   
 $sc=\text{Sc1} \vee sc=\text{Sc2} \wedge (\underline{le\_Ck} \ y \ \underline{kc1}) \vee sc=\text{Sc3} \vee sc=\text{Sc4} \wedge (\underline{lt\_Ck} \ y \ \underline{kc2}) \rightarrow (\text{InvC } s) \text{ end.}$

**Proof.**

Intro  $s$ ; Elim  $s$ .

Intros.

Elim  $H$ ; [ Intro  $sc$ ; Rewrite  $sc$ ; Auto | Intro  $sc2\_4$ ; Elim  $sc2\_4$ ;

[ Intro  $H1$ ; Elim  $H1$ ; Intros  $sc \ cond$ ; Rewrite  $sc$ ; Apply  $\text{Isc2}$ ; Auto | Intro  $sc3\_4$ ; Elim  $sc3\_4$ ;

[ Intro  $sc$ ; Rewrite  $sc$ ; Auto | Intro  $H1$ ; Elim  $H1$ ; Intros  $sc \ cond$ ; Rewrite  $sc$ ; Apply  $\text{Isc4}$ ; Auto ] ].

**Qed.**

**Lemma**  $\text{InvG}' : (s:(\underline{S\_Ck} \ \underline{SG})) \text{Cases } s \text{ of } (sg,z) =$   
 $sg=\text{Open} \vee sg=\text{Lowering} \wedge (\underline{lt\_Ck} \ z \ \underline{kg1}) \vee sg=\text{Closed} \vee sg=\text{Raising} \wedge (\underline{lt\_Ck} \ z \ \underline{kg3}) \rightarrow (\text{InvG } s) \text{ end.}$

**Proof.**

Intro  $s$ ; Elim  $s$ .

Intros.

Elim  $H$ ; [ Intro  $sg$ ; Rewrite  $sg$ ; Auto | Intro  $sg2\_4$ ; Elim  $sg2\_4$ ;

[ Intro  $H1$ ; Elim  $H1$ ; Intros  $sg \ cond$ ; Rewrite  $sg$ ; Apply  $\text{Ilowering}$ ; Auto | Intro  $sg3\_4$ ; Elim  $sg3\_4$ ;

[ Intro  $sg$ ; Rewrite  $sg$ ; Auto | Intro  $H1$ ; Elim  $H1$ ; Intros  $sg \ cond$ ; Rewrite  $sg$ ; Apply  $\text{Iraising}$ ; Auto ] ].

**Qed.**

**Lemma**  $\text{NoImpl} : (A,B:\text{Prop}) (A \rightarrow B) \rightarrow \sim B \rightarrow \sim A$ .

**Proof.**

Unfold  $\text{not}$ ; Auto.

**Qed.**

**Lemma** not\_3\_and: (A,B,C:Prop)  $\sim(A \wedge B \wedge C) \rightarrow \sim A \vee A \wedge \sim B \vee A \wedge B \wedge \sim C$ .

**Proof.**

Intros.

Elim (not\_and\_or ? ? H); Intro H2; [ Idtac | Elim (not\_and\_or ? ? H2); Intro ].

Auto.

Elim (classic A); Auto.

Elim (classic A); Elim (classic B); Auto.

**Qed.**

**Syntactic Definition** no\_invT := [s:(S\_Ck ST)] **Cases** s of (st,x) =  
st=Near $\wedge\sim$ (lt\_Ck x kt2)  $\vee$  st=Inside $\wedge\sim$ (lt\_Ck x kt2) **end.**

**Lemma** No\_invT : (s:(S\_Ck ST))  $\sim$ (InvT s)  $\rightarrow$  (no\_invT s).

**Proof.**

Intro s; Elim s.

Intros st x inv.

Generalize (not\_or\_and ? ? (NoImpl (InvT' (st,x) inv))); Elim st; Intro H0;

Elim H0; Intros H1 H2; Elim (not\_or\_and ? ? H2); Intros.

Absurd Far=Far; Auto.

Elim (not\_and\_or ? ? H); Intros; [ Absurd Near=Near; Auto | Auto ].

Elim (not\_and\_or ? ? H3); Intros; [ Absurd Inside=Inside; Auto | Auto ].

**Qed.**

**Syntactic Definition** no\_invC := [s:(S\_Ck SC)] **Cases** s of (sc,y) =  
sc=Sc2 $\wedge\sim$ (le\_Ck y kc1)  $\vee$  sc=Sc4 $\wedge\sim$ (lt\_Ck y kc2) **end.**

**Lemma** No\_invC : (s:(S\_Ck SC))  $\sim$ (InvC s)  $\rightarrow$  (no\_invC s).

**Proof.**

Intro s; Elim s.

Intros sc y inv.

Generalize (not\_or\_and ? ? (NoImpl (InvC' (sc,y) inv))); Elim sc; Intro H0;

Elim H0; Intros H1 H2; Elim (not\_or\_and ? ? H2); Intros.

Absurd Sc1=Sc1; Auto.

Elim (not\_and\_or ? ? H); Intros; [ Absurd Sc2=Sc2; Auto | Auto ].

Elim (not\_or\_and ? ? H3); Intros; Absurd Sc3=Sc3; Auto.

Elim (not\_or\_and ? ? H3); Intros H4 H5; Elim (not\_and\_or ? ? H5); Intros;

[ Absurd Sc4=Sc4; Auto | Auto ].

**Qed.**

**Syntactic Definition** no\_invG := [s:(S\_Ck SG)] **Cases** s of (sg,z) =  
sg=Lowering $\wedge\sim$ (lt\_Ck z kg1)  $\vee$  sg=Raising $\wedge\sim$ (lt\_Ck z kg3) **end.**

**Lemma** No\_invG : (s:(S\_Ck SG))  $\sim$ (InvG s)  $\rightarrow$  (no\_invG s).

**Proof.**

Intro s; Elim s.

Intros sc y inv.

Generalize (not\_or\_and ? ? (NoImpl (InvG' (sc,y) inv))); Elim sc; Intro H0;

Elim H0; Intros H1 H2; Elim (not\_or\_and ? ? H2); Intros.

Absurd Open=Open; Auto.

Elim (not\_and\_or ? ? H); Intros; [ Absurd Lowering=Lowering; Auto | Auto ].

Elim (not\_or\_and ? ? H3); Intros; Absurd Closed=Closed; Auto.

Elim (not\_or\_and ? ? H3); Intros H4 H5; Elim (not\_and\_or ? ? H5); Intros;

[ Absurd Raising=Raising; Auto | Auto ].

**Qed.**

**Definition**  $\text{InvTick} := [s:\text{StGlobal}] \text{Cases } s \text{ of } ((st,x),((sc,y),(sg,z))) =$   
 $(\text{InvTCG } ((st,(\text{Inc } x)),((sc,(\text{Inc } y)),(sg,(\text{Inc } z)))) \text{ end.}$

**Definition**  $\text{noInvTick} := [s:\text{StGlobal}] \text{Cases } s \text{ of } ((st,x),((sc,y),(sg,z))) =$   
 $\sim(\text{InvTick } ((st,x),((sc,y),(sg,z)))) \rightarrow (\text{RState } \text{TrGlobal } \text{SiniTCG } ((st,x),((sc,y),(sg,z)))) \rightarrow$   
 $((st=\text{Near} \wedge (\text{gt\_Ck } x \text{ kt1}) \vee st=\text{Inside})$   
 $\vee ((\text{InvT } (st,(\text{Inc } x))) \wedge (sc=\text{Sc2} \wedge (\text{eq\_Ck } y \text{ kc1}) \vee sc=\text{Sc4}))$   
 $\vee ((\text{InvT } (st,(\text{Inc } x))) \wedge (\text{InvC } (sc,(\text{Inc } y))) \wedge (sg=\text{Lowering} \vee sg=\text{Raising} \wedge (\text{ge\_Ck } z \text{ kg2)))) \text{ end.}$

**Lemma**  $\text{NoInvTick} : (s:\text{StGlobal}) (\text{noInvTick } s).$

**Proof.**

Intro s; Elim s.  
 Intros st sc\_sg; Elim sc\_sg; Intros sc sg; Elim st; Elim sc; Elim sg; Intros.  
 Simpl; Intros.  
 Elim (not 3 and H); [ Intro no\_invt | Intro H1; Decompose [and or] H1 ].  
 Elim (No\_invt no\_invt); Intro H1; Elim H1; Intros st' x; Rewrite st'; Rewrite st' in H0.  
 Generalize (INV\_T\_general 1!SiniTCG Inv\_SiniTCG H0); Simpl; Intro inv\_near;  
 Inversion inv\_near using cl\_Inear; Intro lt\_x\_kt2.  
 Left; Left; Split; [ Auto | Apply (Trivial32 lt\_x\_kt2 x) ].  
 Auto.  
 Elim (No\_invc H4); Intro H5; Elim H5; Intros sc' y; Rewrite sc'; Rewrite sc' in H0.  
 Generalize (INV\_C\_general 1!SiniTCG Inv\_SiniTCG H0); Simpl; Intro inv\_sc2;  
 Inversion inv\_sc2 using cl\_Isc2; Intro le\_y\_kc1.  
 Generalize (Trivial33 le\_y\_kc1 y5); Intro.  
 Right; Left; Auto.  
 Auto.  
 Elim (No\_invg H5); Intro H6; Elim H6; Intros sg' z; Rewrite sg'; Rewrite sg' in H0.  
 Right; Right; Auto.  
 Generalize (INV\_G\_general 1!SiniTCG Inv\_SiniTCG H0); Simpl; Intro inv\_raising;  
 Inversion inv\_raising using cl\_Iraising; Intro lt\_z\_kg3.  
 Generalize (Trivial34 lt\_z\_kg3 z); Intro.  
 Right; Right; Auto.

**Qed.**

**Syntactic Definition**  $\text{rsNext\_In} :=$

$[x:\text{Clock}] [\text{gt\_x\_kt1}:(\text{gt\_Ck } x \text{ kt1})] [\text{lt\_x\_kt2}:(\text{lt\_Ck } x \text{ kt2})] [sc\_y:(\text{S\_Ck } \text{SC})] [sg\_z:(\text{S\_Ck } \text{SG})]$   
 $(\text{rsNext } (\text{rsIni } \text{TrGlobal } ((\text{Near},x),(\text{sc\_y},\text{sg\_z})))$   
 $(\text{tGl\_In } (\text{ttIn } 1!x \text{ gt\_x\_kt1 } \text{lt\_x\_kt2}) \text{sc\_y } \text{sg\_z})).$

**Syntactic Definition**  $\text{rsNext\_Down} :=$

$[z:\text{Clock}] [\text{lt\_z\_kg1}:(\text{lt\_Ck } z \text{ kg1})] [st\_x:(\text{S\_Ck } \text{ST})] [sc\_y:(\text{S\_Ck } \text{SC})]$   
 $(\text{rsNext } (\text{rsIni } \text{TrGlobal } (st\_x,(\text{sc\_y},(\text{Lowering},z))))$   
 $(\text{tGl\_Down } (\text{tgDown } \text{lt\_z\_kg1}) \text{st\_x } \text{sc\_y})).$

**Syntactic Definition**  $\text{rsNext\_Up} :=$

$[z:\text{Clock}] [\text{ge\_z\_kg2}:(\text{ge\_Ck } z \text{ kg2})] [\text{lt\_z\_kg3}:(\text{lt\_Ck } z \text{ kg3})] [st\_x:(\text{S\_Ck } \text{ST})] [sc\_y:(\text{S\_Ck } \text{SC})]$   
 $(\text{rsNext } (\text{rsIni } \text{TrGlobal } (st\_x,(\text{sc\_y},(\text{Raising},z))))$   
 $(\text{tGl\_Up } (\text{tgUp } \text{ge\_z\_kg2 } \text{lt\_z\_kg3}) \text{st\_x } \text{sc\_y})).$

**Syntactic Definition**  $\text{rs\_Next\_Approach} :=$

$[x,y:\text{Clock}] [sg\_z:(\text{S\_Ck } \text{SG})]$   
 $(\text{rsNext } \text{StGlobal } (\text{rsIni } \text{StGlobal } \text{TrGlobal } ((\text{Far},x),((\text{Sc1},y),\text{sg\_z})))$   
 $(\text{tGl\_Approach } (\text{ttApproach } x) (\text{tcApproach } y) \text{sg\_z})).$

**Syntactic Definition** rsNext\_Exit :=  
 [x,y:Clock] [lt\_x\_kt2:(lt\_Ck x kt2)] [sg\_z:(S\_Ck SG)]  
 (rsNext (rsIni TrGlobal ((Inside,x),(Sc3,y),sg\_z)))  
 (tGl\_Exit (ttExit lt\_x\_kt2) (tcExit y) sg\_z)).

**Syntactic Definition** rsNext\_Lower :=  
 [y,z:Clock] [eq\_y\_kc1:(eq\_Ck y kc1)] [st\_x:(S\_Ck ST)]  
 (rsNext (rsIni TrGlobal (st\_x,((Sc2,y),(Open,z))))  
 (tGl\_Lower (tcLower eq\_y\_kc1) (tgLower z) st\_x)).

**Syntactic Definition** rsNext\_Raise :=  
 [y,z:Clock] [lt\_y\_kc2:(lt\_Ck y kc2)] [st\_x:(S\_Ck ST)]  
 (rsNext (rsIni TrGlobal (st\_x,((Sc4,y),(Closed,z))))  
 (tGl\_Raise (tcRaise lt\_y\_kc2) (tgRaise z) st\_x)).

**Tactic Definition** SplitTrans' :=  
 [<tactic:<  
 Intros s1 s2 l rs\_s1 p\_s1 tr\_gl;  
 Generalize (rsNext rs\_s1 tr\_gl);  
 Generalize rs\_s1; Clear rs\_s1;  
 Generalize p\_s1; Clear p\_s1;  
 Elim tr\_gl  
 >>].

**Tactic Definition** SplitTrans'\_Simpl :=  
 [<tactic:<  
 SplitTrans'; [Simpl\_In | Simpl\_Down | Simpl\_Up | Simpl\_Approach | Simpl\_Exit  
 | Simpl\_Lower | Simpl\_Raise | Simpl\_Tick]  
 >>].

**Tactic Definition** ExistsHere\_ITick [\$\$] :=  
 [<tactic:<  
 Apply exists with tr:=TrGlobal P:=InvTick l:=(rsIni TrGlobal \$\$)  
 >>].

## Demostración de *Non-Zeno*

**Lemma** NonZeno : (ForAll TCG SiniTCG ([s:StGlobal] (Exists TCG s InvTick))).

**Proof.**

BeginForAll.  
 ExistsHere ITick SiniTCG.  
 Split3 Trivial.  
 SplitTrans'\_Simpl ; Generalize H0.  
 Rewrite (lema Inv6 H0 (or\_intror Inside=Near^(gt\_Ck x kc1) Inside=Inside (refl\_equal ST Inside))).  
 Rewrite (lema safeTCG H0 (refl\_equal ST Inside)); Intro rs\_s2.  
 Apply StepsEX with s2:=((Far,x),(Sc4,Reset),(Closed,y0)).  
 Apply (rsNext\_Exit x y2 lt\_x\_kt2 (Closed,y0)).  
 ExistsHere ITick ((Far,x),(Sc4,Reset),(Closed,y0)).  
 Split3 Trivial ; (Apply Isc4; Apply Trivial18).  
 Elim (lema Inv11 H0 (or\_intror Closed=Lowering Closed=Closed (refl\_equal SG Closed)));  
 Intro sc\_closed; Rewrite sc\_closed.  
 Elim y1; Intro rs\_s2.  
 ExistsHere ITick ((Far,y2),(Sc3,y0),(Closed,z)).  
 Split3 Trivial.  
 ExistsHere ITick ((Near,y2),(Sc3,y0),(Closed,z)).  
 Split3 Trivial.  
 Apply Inear.

Apply (Trivial19 lt\_z\_kg1  
 (lema\_Inv5 rs\_s2 (refl\_equal ST Near) (refl\_equal SC Sc3))  
 (lema\_Inv3 rs\_s2 (or\_intror Near=Near Near=Inside (refl\_equal ST Near)))).  
 Elim (Trivial20 lt\_z\_kg1  
 (lema\_Inv9 rs\_s2 (or\_intror Inside=Near^(gt\_Ck y2 kc1) Inside=Inside (refl\_equal ST Inside)))  
 (lema\_Inv3 rs\_s2 (or\_intror Inside=Near Inside=Inside (refl\_equal ST Inside)))  
 (lema\_InvInside rs\_s2 (refl\_equal ST Inside))).  
 Elim y1; Intro rs\_s2.  
 Generalize (INV\_C\_general 1!SiniTCG Inv\_SiniTCG rs\_s2); Simpl;  
 Intro inv\_sc4; Inversion inv\_sc4 using cl\_Isc4; Intro le\_y0\_kc2.  
 Apply StepsEX with s2:=((Far,y2),((Sc1,y0),(Raising,Reset))).  
 Apply (rsNext\_Raise y0 z le\_y0\_kc2 (Far,y2)).  
 ExistsHere ITick ((Far,y2),((Sc1,y0),(Raising,Reset))).  
 Split3 Trivial ; (Apply Iraising; Apply Trivial21).  
 Elim (lema\_Inv4 rs\_s2 (refl\_equal ST Near));  
 Intro sc\_near; Rewrite sc\_near in sc\_closed; Discriminate.  
 Elim (Trivial20 lt\_z\_kg1  
 (lema\_Inv9 rs\_s2 (or\_intror Inside=Near^(gt\_Ck y2 kc1) Inside=Inside (refl\_equal ST Inside)))  
 (lema\_Inv3 rs\_s2 (or\_intror Inside=Near Inside=Inside (refl\_equal ST Inside)))  
 (lema\_InvInside rs\_s2 (refl\_equal ST Inside))).  
 Elim y1.  
 Intro rs\_s2; Generalize rs\_s2; Rewrite (lema\_Inv2 rs\_s2 (refl\_equal ST Far)  
 (or\_intror Open=Open Open=Raising (refl\_equal SG Open))); Intro rs\_s2fin.  
 ExistsHere ITick ((Far,y2),((Sc1,y0),(Open,z))).  
 Split3 Trivial.  
 Intro rs\_s2; Generalize rs\_s2; Elim (lema\_Inv4 rs\_s2 (refl\_equal ST Near)); Intro sc\_near; Rewrite sc\_near.  
 Intro rs\_s2; Generalize (INV\_C\_general 1!SiniTCG Inv\_SiniTCG rs\_s2); Simpl;  
 Intro inv\_sc2; Inversion inv\_sc2 using cl\_Isc2; Intro le\_y0\_kc1.  
 Elim (Trivial22 le\_y0\_kc1); Intro.  
 ExistsHere ITick ((Near,y2),((Sc2,y0),(Open,z))).  
 Split; [ Apply Inear | Split; [ Apply Isc2 | Auto ] ].  
 Apply (Trivial23 H1 (lema\_Inv3 rs\_s2' (or\_intror Near=Near Near=Inside (refl\_equal ST Near)))).  
 Apply (Trivial24 H1).  
 Apply StepsEX with s2:=((Near,y2),((Sc3,y0),(Lowering,Reset))).  
 Apply (rsNext\_Lower y0 z H1 (Near,y2)).  
 ExistsHere ITick ((Near,y2),((Sc3,y0),(Lowering,Reset))).  
 Split; [ Apply Inear | Split; [ Auto | Apply Ilowering ] ].  
 Apply (Trivial25 H1 (lema\_Inv3 rs\_s2' (or\_intror Near=Near Near=Inside (refl\_equal ST Near)))).  
 Apply Trivial26.  
 Intro rs\_s2fin; Elim (lema\_Inv1 rs\_s2fin (or\_intror Near=Near Near=Inside (refl\_equal ST Near)  
 (refl\_equal SC Sc3))); Intro; Discriminate.  
 Intro rs\_s2; Generalize\_Easy (lema\_safeTCG rs\_s2 (refl\_equal ST Inside)).  
 Elim (lema\_Inv10 H0 (or\_intror Sc2=Sc1 Sc2=Sc2 (refl\_equal SC Sc2)));  
 Intros H1; Rewrite H1; Intro rs\_s2.  
 ExistsHere ITick ((Near,Reset),((Sc2,Reset),(Open,y1))).  
 Split; [ Apply Inear; Apply Trivial27 | Split; [ Apply Isc2; Apply Trivial28 | Auto ] ].  
 Generalize (INV\_G\_general 1!SiniTCG Inv\_SiniTCG rs\_s2); Simpl;  
 Intro inv\_raising; Inversion inv\_raising using cl\_Iraising; Intro lt\_y1\_kg3.  
 Elim (Trivial29 lt\_y1\_kg3); Intro.  
 ExistsHere ITick ((Near,Reset),((Sc2,Reset),(Raising,y1))).  
 Split; [ Apply Inear; Apply Trivial27 |  
 Split; [ Apply Isc2; Apply Trivial28 | Apply Iraising; Apply (Trivial30 H2) ] ].  
 Apply StepsEX with s2:=((Near,Reset),((Sc2,Reset),(Open,y1))).  
 Elim H2; Intros H3 H4.  
 Apply (rsNext\_Up y1 H3 H4 (Near,Reset) (Sc2,Reset)).  
 ExistsHere ITick ((Near,Reset),((Sc2,Reset),(Open,y1))).  
 Split; [ Apply Inear; Apply Trivial27 | Split; [ Apply Isc2; Apply Trivial28 | Auto ] ].  
 Elim y0; Intro rs\_s2.  
 ExistsHere ITick ((Far,x),((Sc4,Reset),(Open,y1))).



Split3 Trivial .  
 Apply Isc4; Apply Trivial18.  
 Generalize (INV\_G\_general 1!SiniTCG Inv\_SiniTCG rs\_s2); Simpl;  
 Intro inv\_lowering; Inversion inv\_lowering using cl\_llowering; Intro lt\_y1\_kg1.  
 Apply StepsEX **with** s2:=((Far,x),(Sc4,Reset),(Closed,y1))).  
 Apply (rsNext\_Down y1 lt\_y1\_kg1 (Far,x) (Sc4,Reset)).  
 ExistsHere ITick ((Far,x),(Sc4,Reset),(Closed,y1))).  
Split3 Trivial.  
 Apply Isc4; Apply Trivial18.  
 ExistsHere ITick ((Far,x),(Sc4,Reset),(Closed,y1))).  
Split3 Trivial.  
 Apply Isc4; Apply Trivial18.  
 Generalize Easy (lema Inv2 rs\_s2 (refl\_equal ST Far)  
 (or\_intror Raising=Open Raising=Raising (refl\_equal SG Raising))).  
 Intro rs\_s2; ExistsHere ITick ((y0,y1),(Sc3,y),(Lowering,Reset))).  
 Split; [ Generalize rs\_s2; Elim y0; Intro rs\_s2' | Split; [ Auto | Apply llowering; Apply Trivial26 ] ].  
 Auto.  
 Apply Inear; Apply (Trivial25 eq\_y\_kc1 (lema Inv3 rs\_s2'  
 (or\_intror Near=Near Near=Inside (refl\_equal ST Near))).  
 Generalize Easy (lema\_safeTCG rs\_s2' (refl\_equal ST Inside)).  
 Intro rs\_s2; ExistsHere ITick ((y0,y1),(Sc1,y),(Raising,Reset))).  
 Split; [ Generalize rs\_s2; Elim y0; Intro rs\_s2' | Split; [ Auto | Apply Iraising; Apply Trivial21 ] ].  
 Auto.  
Simpl or (lema Inv4 rs\_s2' (refl\_equal ST Near)).  
 Generalize Easy (lema\_safeTCG rs\_s2' (refl\_equal ST Inside)).  
 Intro; Elim (classic (InvTick ((s4,(Inc x)),(s3,(Inc y)),(s0,(Inc z))))); Intro inv\_tick.  
 ExistsHere ITick ((s4,(Inc x)),(s3,(Inc y)),(s0,(Inc z))); Auto.  
 Generalize H3; Elim (NoInvTick ((s4,(Inc x)),(s3,(Inc y)),(s0,(Inc z)))) inv\_tick H3).  
 Intro no\_st; Decompose [and or] no\_st; [ Rewrite H5 | Rewrite H6 ].  
 Intro rs\_near; Generalize (INV\_T\_general 1!SiniTCG Inv\_SiniTCG rs\_near); Simpl;  
 Intro inv\_near; Inversion inv\_near using cl\_inear; Intro lt\_incx\_kt2.  
 Generalize (rsNext\_In (Inc x) H7 lt\_incx\_kt2 (s3,(Inc y)) (s0,(Inc z))); Intro rs\_inside.  
 Generalize rs\_near; Generalize rs\_inside; Rewrite (lema Inv6 (RState\_Trans rs\_near rs\_inside)  
 (or\_intror Inside=Near/(gt\_Ck (Inc x) kc1) Inside=Inside (refl\_equal ST Inside))).  
 Rewrite (lema\_safeTCG (RState\_Trans rs\_near rs\_inside) (refl\_equal ST Inside)).  
 Intros; Apply StepsEX **with** s2:=((Far,(Inc x)),(Sc4,Reset),(Closed,(Inc z))).  
 Apply (RState\_Trans rs\_inside0 (rsNext\_Exit (Inc x) (Inc y) lt\_incx\_kt2 (Closed,(Inc z)))).  
 ExistsHere ITick ((Far,(Inc x)),(Sc4,Reset),(Closed,(Inc z))).  
Split3 Trivial ; Apply Isc4; Apply Trivial18.  
 Intro rs\_inside; Generalize rs\_inside;  
 Rewrite (lema\_safeTCG rs\_inside (refl\_equal ST Inside)); Intro rs\_inside0.  
 Generalize rs\_inside0; Rewrite (lema Inv6 rs\_inside0 (or\_intror Inside=Near/(gt\_Ck (Inc x) kc1)  
 Inside=Inside (refl\_equal ST Inside))); Intro rs\_inside1.  
 Apply StepsEX **with** s2:=((Far,(Inc x)),(Sc4,Reset),(Closed,(Inc z))).  
 Generalize (INV\_T\_general 1!SiniTCG Inv\_SiniTCG rs\_inside0); Simpl;  
 Intro inv\_inside; Inversion inv\_inside using cl\_inside; Intro lt\_incx\_kt2.  
 Apply (rsNext\_Exit (Inc x) (Inc y) lt\_incx\_kt2 (Closed,(Inc z))).  
 ExistsHere ITick ((Far,(Inc x)),(Sc4,Reset),(Closed,(Inc z))).  
Split3 Trivial ; Apply Isc4; Apply Trivial18.  
 Intro no\_sc\_sg; Elim no\_sc\_sg; [ Intro st\_no\_sc; Decompose [and or] st\_no\_sc | Intro no\_sg ].  
 Rewrite H7; Rewrite H7 **in** rs\_s1.  
 Elim (lema Inv10 rs\_s1 (or\_intror Sc2=Sc1 Sc2=Sc2 (refl\_equal SC Sc2))); Intro sg'; Rewrite sg'.  
 Intro rs\_s2; Apply StepsEX **with** s2:=((s4,(Inc x)),(Sc3,(Inc y)),(Lowering,Reset))).  
 Apply (rsNext\_Lower (Inc y) (Inc z) H8 (s4,(Inc x))).  
 ExistsHere ITick ((s4,(Inc x)),(Sc3,(Inc y)),(Lowering,Reset))).  
Split3 Trivial; Apply llowering; Apply Trivial26.  
 Intro rs\_s2; Apply StepsEX **with** s2:=((s4,(Inc x)),(Sc2,(Inc y)),(Open,(Inc z))).  
 Generalize (lema Inv12 rs\_s2 (refl\_equal SC Sc2)); Intro ge\_incz\_incy.  
 Generalize (INV\_G\_general 1!SiniTCG Inv\_SiniTCG rs\_s2); Simpl; Intro inv\_raising;

Inversion `inv_raising` using `cl_Iraising`; Intro `lt_incz_kg3`.  
 Apply `(rsNext_Up (Inc z) (Trivial31 H8 ge_incz_incy) lt_incz_kg3 (s4,(Inc x)) (Sc2,(Inc y)))`.  
 Apply StepsEX **with** `s2:=((s4,(Inc x)),(Sc3,(Inc y)),(Lowering,Reset))`.  
 Apply `(rsNext_Lower (Inc y) (Inc z) H8 (s4,(Inc x)))`.  
 ExistsHere `ITick ((s4,(Inc x)),(Sc3,(Inc y)),(Lowering,Reset))`.  
 Split3 `Trivial`; Apply `Ilowering`; Apply `Trivial26`.  
 Rewrite H5; Intro `rs_s2`; Generalize `rs_s2`; Generalize `(lema_Inv14 rs_s2 (refl_equal SC Sc4))`;  
 Intro `far_closed`; Elim `far_closed`; Intros `far_closed`; Rewrite `closed`.  
 Intro `rs_s2`; Apply StepsEX **with** `s2:=((s4,(Inc x)),(Sc1,(Inc y)),(Raising,Reset))`.  
 Generalize `(INV_C_general !SiniTCG Inv_SiniTCG rs_s2)`; Simpl; Intro `inv_sc4`;  
 Inversion `inv_sc4` using `cl_Isc4`; Intro `le_incy_kc2`.  
 Apply `(rsNext_Raise (Inc y) (Inc z) le_incy_kc2 (s4,(Inc x)))`.  
 ExistsHere `ITick ((s4,(Inc x)),(Sc1,(Inc y)),(Raising,Reset))`.  
 Split3 `Trivial`; Apply `Iraising`; Apply `Trivial21`.  
 Decompose [and or] `no_sg`.  
 Rewrite H7; Intro `rs_s2`; Generalize `(INV_G_general !SiniTCG Inv_SiniTCG rs_s2)`; Simpl;  
 Intro `inv_lowering`; Inversion `inv_lowering` using `cl_Ilowering`; Intro `lt_incz_kg1`.  
 Apply StepsEX **with** `s2:=((s4,(Inc x)),(s3,(Inc y)),(Closed,(Inc z)))`.  
 Apply `(rsNext_Down (Inc z) lt_incz_kg1 (s4,(Inc x)) (s3,(Inc y)))`.  
 ExistsHere `ITick ((s4,(Inc x)),(s3,(Inc y)),(Closed,(Inc z)))`.  
 Split3 `Trivial`.  
 Rewrite H8; Intro `rs_s2`; Apply StepsEX **with** `s2:=((s4,(Inc x)),(s3,(Inc y)),(Open,(Inc z)))`.  
 Generalize `(INV_G_general !SiniTCG Inv_SiniTCG rs_s2)`; Simpl; Intro `inv_raising`;  
 Inversion `inv_raising` using `cl_Iraising`; Intro `lt_incz_kg3`.  
 Apply `(rsNext_Up (Inc z) H9 lt_incz_kg3 (s4,(Inc x)) (s3,(Inc y)))`.  
 ExistsHere `ITick ((s4,(Inc x)),(s3,(Inc y)),(Open,(Inc z)))`.  
 Split3 `Trivial`.

**Qed.**

(\*

Especificación alternativa de `NonZero`, usando operadores temporales acotados:

Definition `S_true := [_:StGlobal] True`.

Lemma `NonZero : (ForAll_TCG SiniTCG ([s:StGlobal] (Exists_TCG s S_true (eq_Ck tick))))`.

\*)

---