Verificación de Sistemas de Tiempo Real en Teoría de Tipos
Un Caso de Estudio
"The RailRoad Crossing example in Coq"[§]

Carlos Daniel Luna
Instituto de Computación, U. de la República, Uruguay
E-mail: cluna@fing.edu.uy. Web: http://www.fing.edu.uy/~cluna

Resumen

Para el análisis de sistemas de tiempo real se destacan dos enfoques formales: 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 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 que permite compatibilizar el uso de un verificador de modelos como *Kronos* y el asistente de pruebas *Coq* en el análisis de sistemas de tiempo real. Un especial énfasis es puesto en el análisis de un caso de estudio, considerado como *benchmark* en diferentes trabajos: *el control de un paso a nivel de tren*.

Palabras claves: Especificación y Análisis de Sistemas de Tiempo Real. Autómatas (Grafos) Temporizados. Lógicas TCTL y CTL. Verificación de Modelos. Teoría de Tipos y Coq. Verificación-Demostración de Corrección.

Abstract

Two formal approaches arise as the most used for the analysis of real time systems: model checking and deductive analysis based on proof assistants. The former is characterized by its fully automatization but it presents some difficulties when dealing with systems that involve a great number of states or unbound parameters. The latter, on the other hand, turns out to be appropriate for working with arbitrary systems, though user's interaction is required. This work explores a methodology that combines the use of a model checker like *Kronos* and the proof assistant *Coq* for the analysis of real time systems. We specially emphasize the analysis of the railroad crossing example, a case study considered a benchmark by different works in this field.

Keywords: Specification and Analysis of Real Time Systems. Timed Automata. TCTL and CTL. Model Checking. Type Theory and Coq. **Verification** and Proof Correction.

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 procesos industriales automatizados y de dispositivos electrónicos; aplicaciones multimedia y de internet. 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 "el" 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" o "el tiempo transcurrido entre dos eventos o señales debe estar acotado por un valor constante", etc.

Es indiscutible hoy la influencia que tiene en la industria y en casi todos los ámbitos el uso del software. A pesar de su uso extensivo, uno de los costos más altos 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*". No obstante, este método no garantiza la corrección del software analizado, por ser incompleto en la mayoría de los casos [24]. En 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 las circunstancias. Para el análisis de la corrección de esta clase de sistemas dos importantes enfoques formales se destacan:

[§] La versión completa de este trabajo es el reporte [22].

- ***Verificación* de corrección (de modelos)**. 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 la construcción de la prueba.

1.1 Verificación de Modelos

El método de verificación llamado *verificación de modelos* ("*model checking*") fue desarrollado para analizar *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, [10]). 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. 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*, *HyTech* y *Uppaal*.

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* [6], 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*, *Coq* y *LEGO*. 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 (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*, para sistemas reactivos, son [15, 14].

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 que involucran un gran número de estados o que tienen parámetros variables, no acotados. Los asistentes de prueba antes citados 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: (1) 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 pueden llegarse a descubrir las causas por las cuales una propiedad no vale e incluso, algunas veces, las modificaciones necesarias del sistema para que la cumpla. (2) 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. Además, una demostración bien pensada permite reutilizar una estrategia de prueba en la demostración de otros teoremas. (3) 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 ciertas constantes del problema o algunas relaciones entre ellas). (4) Las pruebas de un sistema pueden permitir generalizar la especificación del mismo preservando propiedades de interés.

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 [25, 28], entre otros muchos.

Este trabajo está enmarcado en un proyecto de investigación que vincula al grupo de Métodos Formales del Instituto de Computación de la Universidad de la República (Uruguay) y al proyecto *Coq* del INRIA –Rocquencourt (Francia). 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. En este marco, nuestro objetivo es dar los primeros pasos en una combinación entre ambos enfoques, estableciendo una metodología de trabajo que permita compatibilizar el uso de un *model checker* como *Kronos* [30] y el asistente de pruebas *Coq* en el análisis de sistemas de tiempo real. A fin de lograr esto proponemos formalizar *grafos* (*autómatas*) *temporizados* [4, 26, 19] y la *lógica TCTL* (*timed computation tree logic*) [1, 12] en el *cálculo de construcciones (co)inductivas* de *Coq* [15]. Los grafos temporizados permiten describir sistemas de tiempo real, mientras que la lógica *TCTL* es un lenguaje adecuado y ampliamente usado para especificar requerimientos temporales. *Kronos* permite verificar si un grafo temporizado satisface una fórmula *TCTL*, siempre que los parámetros del sistema sean valores constantes. El enfoque deductivo permite trabajar con parámetros variables y estructuras infinitas, y de esta manera analizar 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. En [23] desarrollamos una metodología para la especificación y el análisis de sistemas reactivos y de tiempo real. En este artículo ponemos énfasis en 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).

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. El usuario introduce definiciones y hace demostraciones en un estilo de *deducción natural*, usando *tácticas*, 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. 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 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 [11] por el cálculo puro de construcciones, a [27] por tipos inductivos y a [12, 15] por tipos co-inductivos. Acerca de *Coq*, una buena descripción es el manual de referencia [6].

1.5 Organización del Trabajo

La organización del trabajo es como sigue. En la sección 2 introducimos los grafos temporizados, usados para describir sistemas de tiempo real, y la lógica *TCTL*, utilizada como lenguaje de especificación de propiedades temporales. 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 la sección 3 formalizamos en *Coq* grafos temporizados y la lógica *TCTL*. Incluimos además operadores de la lógica *CTL* (*computation tree logic*) [5], que permite razonar sobre sistemas reactivos. En la sección 4 consideramos un caso de estudio: el control de un paso a nivel de tren. Especificamos el sistema en *Coq* en base a las formalizaciones introducidas en la sección 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. Finalmente, en la sección 5 incluimos trabajos relacionados y conclusiones.

2. Sistemas de Tiempo Real: Grafos Temporizados y TCTL

2.1 Grafos (Autómatas) Temporizados

Los grafos –también llamados autómatas– 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 temporizados han sido propuestas, como es el caso de [4, 19, 26]. 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 [4, 26]. 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.

Definición. Sea A un conjunto global de *etiquetas*. Un *grafo temporizado* es una quíntupla $G = \langle L, X, E, l^0, I \rangle$:

- 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 $v(x) \in R^+$ a cada reloj $x \in X$, donde R^+ son los números reales no negativos. V denota el conjunto de las valuaciones. $v + t$ denota 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 $e = \langle l, \alpha, \psi_X, \rho_X, l' \rangle$ consiste en una locación origen $l \in L$, una locación destino $l' \in L$, una etiqueta $\alpha \in A$, una condición ψ_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 $x \prec c$; donde, $x \in X$, $\prec$ es una relación binaria en el conjunto $\{<, \leq, =, \geq, >\}$ y c es una constante entera positiva. 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 ψ_X. El estado $\langle l', v[\rho_X := 0] \rangle$ es el *sucesor discreto* del estado $\langle l, v \rangle$ por α, con $v[\rho_X := 0]$ 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 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. El estado $\langle l, v + t \rangle$ es un *sucesor temporal* del estado $\langle l, v \rangle$, si $v + t'$ satisface I_l para todo $0 \leq t' \leq t$.

La semántica formal de un grafo temporizado puede definirse en función de *un sistema de transiciones etiquetado* [26], donde los estados son pares de $L \times V$ y las transiciones son de dos tipos: *Temporales* o *Discretas* (*instantáneas*). 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. Las aristas del grafo representan acciones discretas. La ejecución de una acción α es una transición que lleva la etiqueta α.

2.1.1 Trazas de Ejecución

Una *ejecución* o *traza de ejecución* de un grafo temporizado G con estado inicial q_0 es una secuencia infinita de estados $q_0 \xrightarrow{t_0} q_0' \xrightarrow{\alpha_0} q_1 \xrightarrow{t_1} q_1' \xrightarrow{\alpha_1} q_2 \ldots$, donde $q_i \xrightarrow{t_i} q_i'$ representa una transición temporal y $q_i' \xrightarrow{\alpha_i} q_{i+1}$ es una transición discreta o una transición temporal con tiempo cero. Sea r una ejecución de G con estado inicial q_0, una *posición* π de r es un par $\langle i, t \rangle \in N \times R^+$, 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 $\Sigma_{j<i}\, t_j + t$ transcurrido desde el comienzo de la ejecución r. Una ejecución r de G es *divergente* si para cada $t \in R^+$ existe una posición π 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*". Nosotros estamos interesados, al igual que los trabajos previos (por ejemplo [4, 19, 26]), en sistemas de tiempo real en los cuales todo prefijo finito de una ejecución de G es prefijo de una ejecución divergente de G. El comportamiento (cada traza de ejecución) de estos sistemas, que llamaremos *sistemas bien temporizados*, puede ser generado transición a transición, comenzando en un estado inicial y repetidamente eligiendo entre incrementar el tiempo y hacer una transición discreta.

2.1.2 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. Por más detalles ver [26, 22].

2.2 Lógica TCTL: "Timed Computation Tree Logic"

Muchas propiedades importantes de los sistemas encuentran una expresión natural en lógica temporal. La lógica temporal de tiempo real TCTL ("timed computation tree logic") [4, 19] extiende los operadores temporales $\exists\mu$ (*existe una ejecución*) y $\forall\mu$ (*para todas las ejecuciones*) de CTL ("computation tree logic") [10] 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*” o “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*” o “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 sobre los estados. El conjunto *P* de predicados sobre los estados de un grafo temporizado se define en [26]: $p := @ = l \mid x_i \prec c \mid x_i - x_j \prec d \mid Init$. Donde, $l \in L$, x_i, $x_j \in X$, $c \in$ N, $d \in$ Z y $\prec \in \{<, \leq, =, \geq, >\}$. Informalmente, *Init* caracteriza al estado inicial y $@ = l$ al conjunto de los estados cuya locación es *l*. 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 φ_2 se cumple en un estado de la misma, en un tiempo *t* dentro del intervalo *I* y que φ_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. La semántica formal de TCTL es descripta en [4, 26] y puede también ser consultada en [22].

2.2.1 Algunas Propiedades Relevantes

Usaremos abreviaturas típicas, como $\exists\Diamond_I\varphi$ (*posible* φ), $\forall\Diamond_I\varphi$ (*inevitable* φ) y $\forall\Box_I\varphi$ (*siempre* φ) en lugar de $true\exists\mu_I\varphi_2$, $true\forall\mu_I\varphi_2$ y $\neg\exists\Diamond_I\neg\varphi$, respectivamente. Para $I=[0, \infty)$ omitiremos el subíndice *I*, caracterizando a fórmulas de la lógica CTL. La fórmula $\exists\Diamond_I\varphi$ es satisfecha por los estados a partir de los cuales existe una ejecución divergente del sistema tal que φ se cumple en un estado de la misma, en un tiempo *t* dentro del intervalo *I*. De esta manera se especifican problemas de *alcanzabilidad* acotada. $\forall\Diamond_I\varphi$ establece que φ es *inevitable*. Un estado *q* satisface esta fórmula si y sólo si a partir de toda ejecución divergente con estado inicial *q* existe un estado que satisface φ, dentro del intervalo *I*. $\forall\Diamond_{\leq c}\varphi$ expresa la propiedad de tiempo real de respuesta en tiempo acotado, en la cual un evento debe ocurrir antes de un cierto tiempo *c*. Finalmente $\forall\Box_I\varphi$ especifica que φ es un *invariante*. Esto es, un estado *q* satisface $\forall\Box_I\varphi$ si y sólo si toda ejecución con estado inicial *q* satisface continuamente φ, dentro del intervalo *I*.

2.3 Verificación de Modelos: Grafos Temporizados y TCTL

Dado un grafo temporizado *G* y una fórmula φ de TCTL, el problema de decidir, algorítmicamente, si *G satisface* φ es una instancia del problema de *verificación de modelos*, solucionada por Alur, Courcoubetis y Dill [4]. Su solución está basada en la construcción explícita de un grafo cociente finito, llamado *grafo de regiones*, a partir del sistema de transiciones de estados *infinito* que caracteriza al grafo *G*. Las regiones están determinadas por una relación de equivalencia sobre el conjunto de los relojes del 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 y consecuentemente pueden desarrollarse algoritmos más eficientes. Por más detalles ver [22].

2.4 Un Modelo de Tiempo Discreto

En [22] analizamos ventajas y desventajas de modelos de tiempo discreto –usando números enteros o naturales– y modelos de tiempo continuo –usando racionales o reales. 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 representar el tiempo [21, 3]. 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 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 [4]. En el enfoque de *relojes ficticios* los eventos (las transiciones) pueden ocurrir en tiempo continuo pero son registrados 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* [21, 3]. Si varios eventos ocurren entre dos instantes consecutivos de tiempo, ellos pueden ser distinguidos solamente por el ordenamiento temporal, no por el valor real del tiempo.

Para grafos temporizados es posible considerar una semántica alternativa basada en tiempo discreto, tomando valores en N, la cual ha sido discutida en algunos trabajos previos (ver, por ejemplo, [8]). 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 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 $x_1 \leq u$. 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 N, 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 1(b).

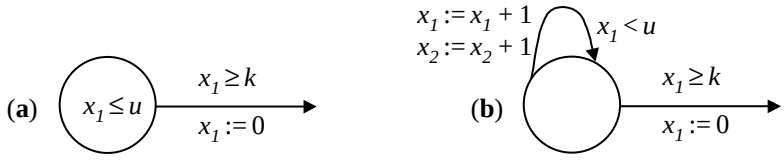

Fig. 1: Un autómata temporizado y su interpretación en tiempo discreto

Bajo esta interpretación los relojes son simplemente variables naturales 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 [8]. 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, [8]), es considerada con particular interés en el presente trabajo ya que permite resaltar que con una discretización del tiempo "no mucho se pierde" [21, 16, 8]. En particular, [16] 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 la sección 4, las propiedades verificadas sobre un dominio discreto valen en el dominio denso de los reales o los racionales, según los resultados establecidos en [21, 8].

3. Formalización de Grafos Temporizados y TCTL en *Coq*

3.1 Nociones Temporales

En la formalización asumimos a N como dominio temporal discreto, que corresponde al tipo inductivo `nat` de *Coq*. A continuación introducimos algunas definiciones básicas sobre nociones temporales:

```
Definition Instant := nat. Definition Clock := nat. Definition Ini_Ck := 0.
Definition tick : Instant := (1). Definition Inc := [x:Clock] (plus x tick).
Definition Reset :=0. Definition time0:= 0.
```

`Instant` y `Clock` corresponden al tipo de los valores temporales y las valuaciones de los relojes; `Ini_Ck` es el valor inicial de los relojes; `tick` es la *granularidad* del sistema; `Inc` es la operación que incrementa en un `tick` un reloj `x`; y, `Reset` y `time0` corresponden al valor de reseteo de los relojes y el tiempo inicial del sistema, respectivamente.

3.2 Definiciones Elementales de Grafos Temporizados

Sea $G = \langle Loc = \{loc_0, \ldots, loc_n\}, X, Trans, loc_0, Inv \rangle$ un grafo temporizado. El conjunto global `Label` de etiquetas puede definirse por un tipo inductivo, al igual que las locaciones del grafo G:

```
Inductive Label : Set := Lab1 : Label | ... | Labm : Label | Tick : Label.
Inductive Loc : Set := Loc0 : Loc | ...| Locn : Loc.
```

Lab$_1$, …, *Lab*$_m$ y *Tick* son los constructores del tipo `Label`. *Lab*$_1$, …, *Lab*$_m$ son las etiquetas que corresponden a las transiciones discretas; *Tick* es una etiqueta distinguida que caracteriza a las transiciones temporales.

El estado del sistema en un instante dado está determinado por una locación de `Loc` y una tupla de valores de tipo `Clock`. 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`.

```
Definition State := Loc * Clocks. Definition St_ini : State := (Loc0,InicAll).
```

`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 "`∀x∈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, como sigue:

```
Inductive Inv : State -> Prop :=
   ILoc0   : ∀x∈Clocks (Icond0 x) -> (Inv (Loc0,x))
   ...
   |ILocn  : ∀x∈Clocks (Icondn x) -> (Inv (Locn,x)).
```

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

Las transiciones discretas y temporales de *G* son relaciones entre estados y etiquetas. Esto es,

```
Inductive Trans : State -> Label -> State -> Prop :=
  trans1: ∀x∈Clocks (Tcond1 x) -> (Inv (Loc j1,new_x1)) -> (Trans (Loc i1,x) Lab k1 (Loc j1,new_x1))
  ...
  |transp:∀x∈Clocks (Tcondp x) -> (Inv (Loc jp,new_xp)) -> (Trans (Loc ip,x) Lab kp (Loc jp,new_xp))
  |tTick: ∀x∈Clocks ∀l∈Loc (Inv (l,(IncAll x))) -> (Trans (l,x) Tick (l,(IncAll x))).
```

$\texttt{Tcond}_1$, …, $\texttt{Tcond}_p$ son los predicados asociados a cada una de las *p* transiciones del grafo; $\texttt{new\_x}_i$ es la tupla de `Clocks` donde cada reloj conserva su valor de *x* o es reseteado a cero, con la constante `Reset`; $\textit{trans}_1$, …, $\textit{trans}_p$ corresponden a transiciones discretas (del conjunto *Trans* de *G*) y *tTick* al conjunto de transiciones temporales (una por locación). $\textit{trans}_i$ construye pruebas de transiciones de una locación $\texttt{Loc}_{iq}$ a otra $\texttt{Loc}_{jq}$ por una etiqueta $\texttt{Lab}_{kq}$, para los valores de los relojes que satisfacen $\texttt{Tcond}_i$ e $(\texttt{Inv}\ (\texttt{Loc}_{jq},\texttt{new\_x}_i))$; *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.

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 un estado q_0 son estados pertenecientes a trazas de ejecución con estado inicial q_0. 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 previa. El conjunto de estados alcanzables desde uno inicial `Sini` a través de `tr` puede definirse inductivamente como sigue,

```
Variables S : Set; 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).
```

Los estados alcanzables en tiempo *t* desde un estado `Sini` se formalizan generalizando 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

- $\forall\Box P$ y $\forall\Box_I P$ permiten especificar propiedades invariantes e invarianza acotada.

```
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` y `ForAll_T`, la propiedad anterior para todos los valores temporales `t` que satisfacen `(bound t)`, es decir $t \in I$.

- $\exists\Diamond P$ y $\exists\Diamond_I P$ permiten especificar problemas de alcanzabilidad no acotada y acotada.

```
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`. `Exists_T` define la propiedad anterior para todos los valores temporales `t` que satisfacen `(bound t)`. Una prueba de $\exists\Diamond P$ ($\exists\Diamond_I P$) se obtiene a partir de un estado alcanzable que verifica *P* –y `(bound t)`– y consiste en la construcción de un camino desde el estado inicial. $\forall\Box$ y $\exists\Diamond$ pueden alternativamente definirse instanciando en las formalizaciones de $\exists\Diamond_I$ y $\forall\Box_I$ a `bound` con el predicado constante `True`.

3.3.3 Algunas Propiedades

En [22] probamos un conjunto de propiedades para los operadores temporales definidos en la sección previa. A continuación destacamos dos de ellas, a modo de ejemplo.

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

El teorema `StepsEX` establece que si $\exists\Diamond P$ vale a partir de una estado inicial `s2` y `s2` es alcanzable a partir del estado `s1` entonces $\exists\Diamond P$ vale a partir del estado inicial `s1`. `ForAll_EX_T` es la equivalencia: $\forall\Box_I P \Leftrightarrow \neg\exists\Diamond_I\neg P$.

3.4 Necesidad de Tipos Co-Inductivos

Si bien muchas propiedades temporales cuantitativas pueden especificarse usando los operadores $\exists\Diamond_I$ y $\forall\Box_I$, otras requieren el uso de las versiones más generales de $\exists\mu_I$ y $\forall\mu_I$. Por ejemplo las propiedades de respuesta en tiempo acotado. El operador $\forall\Diamond_I$ no se formaliza, de forma natural, en base a solamente tipos inductivos y la noción de *estados alcanzables* en tiempo acotado. Es por esto 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 (y de CTL). En [22] presentamos una formalización en *Coq* de TCTL y CTL con tipos co-inductivos.

4. Control de un Paso a Nivel de Tren

En esta sección analizamos un caso de estudio: *el control de un paso a nivel de tren* (“*the railrod crossing example*”). Numerosos trabajos consideran a este problema como *benchmark* para analizar diferentes técnicas de especificación y herramientas de análisis. Entre otros, [19, 9, 29, 17, 18, 13, 5, 7]. Nosotros tomamos la especificación del problema de [2]. 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 2.

La variable de control *st* del tren varía sobre tres locaciones: *st = Far* si el tren está lejos de cruzar el paso a nivel; *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, envía una señal *Approach* al controlador. 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 envía una señal *Exit* al controlador, indicando el alejamiento del tren del paso a nivel. Esto ocurre antes de *kt2* unidades de tiempo desde el origen de 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, el controlador envía a la barrera la señal *Lower* exactamente *kc1* unidades de tiempo después, indicando que ésta debe bajar. Cuando *Exit* es recibida, 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, 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.

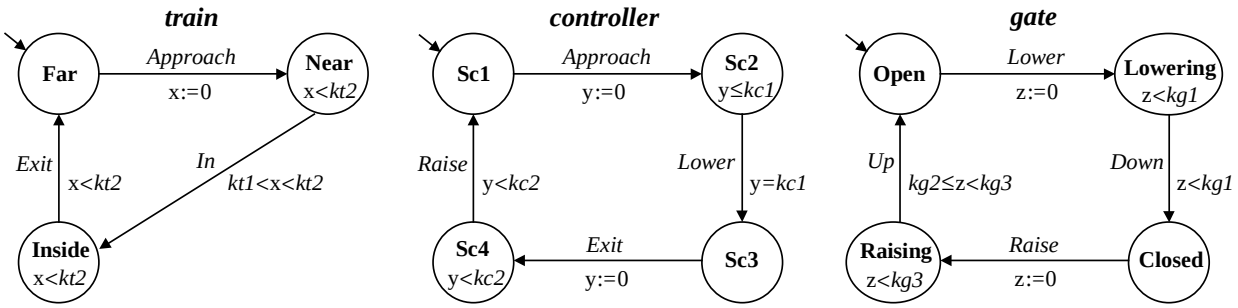

Fig. 2: Grafos temporizados del sistema “*control de un paso a nivel de tren*”

En [2] los valores de los parámetros del sistema son las constantes: *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 una constante δ, con $\delta>|X|$ y X el conjunto de los relojes del sistema compuesto. De esta manera aseguramos que toda desigualdad que vincule a los relojes del sistema tenga al menos una asignación posible, una solución. En general para cualquier sistema, multiplicar las constantes por un valor δ mayor a la cantidad de relojes del sistema determina que las desigualdades extremas $0 < x_1 < \ldots < x_n < 1$ (con $n=|X|$) tengan al menos una solución posible. Por más detalles ver [22].

4.1 Especificación del Sistema en Coq

La especificación formal y completa del sistema en *Coq* respeta las formalizaciones definidas en la sección 3.2 y puede ser consultada en [22]. Las etiquetas del sistema, el tipo de los estados, las locaciones, los invariantes de las locaciones, las transiciones de cada sistema componente y los estados iniciales los definimos con tipos inductivos. Para el sistema compuesto, que llamaremos sistema TCG, el tipo de los estados corresponde a una terna y las transiciones las definimos según la composición paralela de los tres sistemas componentes, a través de un tipo inductivo. Este tipo consta de 8 constructores: 3 correspondientes a las transiciones que no son de sincronización (*In*, *Down* y *Up*); 4 relacionados a las transiciones de sincronización (*Approach*, *Exit*, *Lower* y *Raise*); y el último que representa a las transiciones temporales y permite sincronizar el paso del tiempo en cada sistema componente.

4.2 Análisis del Sistema TCG

En esta parte del trabajo estamos interesados en analizar la demostración de dos clases importantes de propiedades: *safety* y *liveness*. Las primeras permiten especificar que "nada malo ocurrirá durante cierto tiempo". Estas se formulan, generalmente, mediante el operador $\Box_I$. Las propiedades de *liveness* permiten especificar que "algo bueno ocurrirá dentro de cierto intervalo de tiempo". 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 [1], donde muestran que cualquier propiedad de una traza puede ser expresada como una conjunción de propiedades de *safety* y *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". Aunque esta propiedad es puramente *cualitativa*, la misma no vale si eliminamos o cambiamos restricciones temporales. Una propiedad esencial de todo sistema es la propiedad de *liveness non-Zeno*, la cual asegura que el tiempo diverge en todas las ejecuciones del sistema.

4.2.1 Demostración de Invariantes

Para especificar una propiedad $Q \Rightarrow \forall\Box_I P$ sobre un grafo temporizado *G* podemos adoptar la formalización con tipos inductivos del operador $\forall\Box_I$. La prueba corresponde, generalmente, a una inducción en el conjunto de los estados alcanzables y las transiciones de *G*. En esta sección analizamos la prueba de invariantes para el sistema TCG, los cuales nos permiten adquirir un conocimiento mayor del sistema, a fin de analizar otras propiedades más complejas, como por ejemplo *non-Zeno*. Para nuestro caso de estudio el intervalo *I* no es significativo, usamos la versión no acotada de $\forall\Box_I$: $\forall\Box$. Adoptamos la formalización con tipos inductivos del operador $\forall\Box$, en vez de la correspondiente con tipos co-inductivos, aunque los mismos resultados se siguen de ambas representaciones.

Invariantes

La especificación de una propiedad invariante Inv_i del sistema TCG corresponde a la fórmula $Init \Rightarrow \forall\Box Inv_i$, donde *Init* es el predicado que caracteriza al estado inicial del sistema. En [22] analizamos 16 invariantes, algunos de los cuales describimos en la figura 3. Aunque no usamos la versión acotada del operador $\forall\Box$, muchas de las propiedades invariantes expresan restricciones cuantitativas de tiempo. Por ejemplo para indicar el tiempo transcurrido desde un evento –invariante Inv_1– o el tiempo de separación entre dos eventos –invariante Inv_2. Otros invariantes reflejan propiedades básicamente cualitativas que relacionan locaciones de los estados del sistema –invariante Inv_3. Finalmente existen propiedades que son al mismo tiempo cualitativas y cuantitativas, según la clasificación previa. Por ejemplo el invariante Inv_4.

Inv_1:	$@_C$=*Sc3* $\Rightarrow$ y $\geq$ *kc1*. "Si el controlador está esperando la señal *exit*, el tiempo transcurrido desde el origen de la señal *Approach* (comienzo de la aproximación del tren al cruce) es por lo menos *kc1* unidades".
Inv_2:	$@_C$=*Sc2* $\Rightarrow$ z $\geq$ *y*. "Si el controlador recibió la señal *Approach* pero aún no envió la señal *lower* a la barrera, 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*".
Inv_3:	$@_T$=*Far* $\Rightarrow$ $@_G$=*Open* $\vee$ $@_G$=*Raising* $\Rightarrow$ $@_C$=*Sc1*. "Si el tren está lejos y la barrera está arriba o levantándose, el controlador se encuentra a la espera de la señal *Approach* de un nuevo tren".
Inv_4:	($@_T$=*Near* $\wedge$ x > *kt1*) $\vee$ $@_T$=*Inside* $\Rightarrow$ $@_G$=*Closed*. "Si el tren está próximo a cruzar el paso a nivel y el tiempo transcurrido en ese estado (desde el origen de la señal *Approach*) superó `kt1` unidades, o bien el tren está cruzando el paso a nivel, entonces la barrera se encuentra baja".

Fig. 3: Algunos invariantes del sistema TCG

Demostramos los invariantes del sistema TCG con el asistente de pruebas *Coq* y la utilización de algunas tácticas que especialmente definimos para este caso de estudio. Las *tácticas* de prueba en *Coq* permiten abreviar esquemas de demostración, implementan reglas de inferencia. Para simplificar la construcción de las pruebas del sistema TCG desarrollamos tácticas que automatizan ciertas partes de las mismas, particularmente en casos de invariantes. Por ejemplo, tácticas que realizan inducción sobre los estados alcanzables del sistema e intentan probar el paso base y los pasos inductivos automáticamente, dejando sólo aquellos objetivos no resueltos como obligaciones de prueba. Estas tácticas permiten reducir el *script* de prueba –lista de tácticas usadas en la demostración–, aunque no reducen

el tamaño de los términos de prueba. En [22] describimos algunas medidas que conducen a disminuir el tamaño de los términos de prueba para las propiedades y el sistema analizados.

4.2.2 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*". Podemos formalizar esta propiedad de *safety* a través de la siguiente fórmula de TCTL: $Init \Rightarrow \forall\Box\ (@_T=Inside \Rightarrow @_G=Closed)$. En *Coq* formalizamos la propiedad usando el predicado `ForAll` definido en la sección 3.3.2. La demostración se sigue del invariante Inv_4, que es más general que la propiedad de *safety*, y de un teorema que establece la propiedad de monotonía para la implicación en propiedades de invarianza [22].

4.2.3 Propiedad de Liveness non-Zeno

Los invariantes permiten establecer propiedades de *safety* y ayudan a demostrar otras clases de propiedades, como las de *liveness*. En esta sección estamos particularmente interesados en el análisis de la propiedad de *liveness non-Zeno*. Esta propiedad asegura que el tiempo no se bloquea, diverge en todas las ejecuciones del sistema. *non-Zeno* puede ser descripta por la fórmula TCTL: $Init \Rightarrow \forall\Box\exists\Diamond_{=c}\ True$. En *Coq*, a través de los predicados `ForAll` y `Exists`.

La estructura de la prueba corresponde a una inducción en los estados alcanzables, desde el estado inicial, 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 ($\exists\Diamond_{=c}\ True$). En este proceso utilizamos los invariantes y las tácticas referidos previamente, formulamos tácticas específicas para propiedades de alcanzabilidad y usamos el teorema `StepsEX` de la sección 3.3.3. Por detalles ver [22].

Un Sistema Mal Temporizado

El sistema presentado en [2] difiere del introducido en este trabajo únicamente en la condición de activación para la transición de la barrera, rotulada con *Up*, que vincula las locaciones *Raising* y *Open*.

Fig. 4: Diferencia con la formalización dada en [2]

Introdujimos la modificación previa en este trabajo debido a que el sistema presentado en [2] no cumple *non-Zeno* (en [22] construimos un contra-ejemplo). A partir del análisis de *non-Zeno* para dicho sistema dedujimos una condición suficiente que permitió transformar el sistema mal temporizado en el sistema bien temporizado analizado en este trabajo. La condición suficiente es precisamente la que distingue a ambas versiones.

4.3 Generalización del Sistema TCG

En esta sección presentamos una generalización de la especificación del sistema presentado en la sección 4 que preserva las propiedades analizadas del mismo. En la formulación de las propiedades introducidas en la sección 4.2 consideramos los valores de las constantes del sistema TCG especificados en [2], multiplicados por una constante. En las pruebas desarrollamos lemas especiales para las demostraciones que involucran relaciones elementales entre los valores de las constantes y los relojes del sistema. El conjunto completo de lemas con sus demostraciones pueden consultarse en [22]. A continuación mostramos algunos ejemplos.

Lemma *Triv1*: $\forall x \in \text{Clock}.\ x > kt1 \rightarrow x > kc1$.	Lemma *Triv3*: $\forall x,y \in \text{Clock}.\ (\text{Inc } x) > y \rightarrow x = y \vee x > y$.
Lemma *Triv2*: $\forall x \in \text{Clock}.\ x < kg2 \rightarrow (\text{Inc } x) < kg3$.	Lemma *Triv4*: $(\text{Inc Reset}) < kc2$.

Triv1 y *Triv2* establecen relaciones entre valores constantes del sistema: $kt1 \geq kc1$ y $kg3 > kg2$. Triv3 es una propiedad de la discretización que expresa que los incrementos temporales son los mínimos para el dominio temporal elegido. Triv4 expresa que la constante *tick* es menor que *kc2*. Muchas de estas propiedades se demuestran fácilmente a partir de la estructura temporal elegida, por ejemplo *Triv3* y *Triv4*. Las propiedades que establecen relaciones entre las constantes del sistema se prueban también fácilmente a partir de sus valores. Sin embargo, si consideramos a estas últimas como axiomas podemos extender la especificación del sistema, parametrizando las constantes. De esta manera obtenemos una formulación más general del sistema que preserva las propiedades analizadas. Es decir, definimos una familia de sistemas que satisfacen las mismas propiedades.

Las propiedades que vinculan a las constantes del problema en la demostración de *safety* resultan válidas si consideramos la restricción: $kt1 - kc1 + 1 \geq kg1$. La especificación del sistema TCG que preserva *safety* 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:

$kt1 \geq kg1 + kc1$; $kg3 > kg2$; $kc1 \geq kg2$; $kt2 - 1 > kt1$; $kc1 \geq kc2$; $ki > 1$; $ki \in \{kt1, kt2, kc1, kc2, kg1, kg2, kg3\}$.
Estas restricciones 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 originales del sistema y especificar como axiomas las restricciones establecidas entre las mismas:

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

5. Trabajos Relacionados y Conclusiones

5.1 Trabajos Relacionados

Numerosos trabajos consideran a este problema como *benchmark* para analizar diferentes técnicas de especificación, metodologías y herramientas de análisis de sistemas de tiempo real. Entre otros, [2, 20, 9, 29, 17, 18, 13, 5, 7]. En particular [7] 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 este trabajo 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 que interactúan según su composición paralela. Consecuentemente no son necesarios operadores tales como *since* para registrar el tiempo transcurrido desde la última vez que valía una propiedad ni otros similares [29]. 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. 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 que permite simular el sistema con el control de los múltiples relojes (ver [22]). Entendemos 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 (co)inductivas de *Coq*. Algunos otros trabajos que buscan relacionar métodos deductivos de prueba y *model checking* son: [25, 28, 14]. En particular [14] 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.

La demostración de invariantes y de propiedades *safety* (como las consideradas en el caso de estudio de este trabajo) 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* (por ejemplo, *Kronos* [30]). Sin embargo, como vimos en la sección 4.3, es posible generalizar la especificación del sistema en estudio preservando ciertas propiedades de interés, asumiendo parámetros variables sujetos a determinadas restricciones.

5.2 Conclusiones

En este trabajo analizamos cómo representar nociones temporales y razonar deductivamente en teoría de tipos sobre sistemas reactivos y de tiempo real. Formalizamos 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 operadores de la lógica TCTL, y su restricción CTL para razonar sobre sistemas reactivos. En [22] formalizamos completamente las lógicas TCTL y CTL, y definimos dos representaciones genéricas de grafos temporizados en *Coq* para la semántica de tiempo discreto considerada, una de las cuales extendimos 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.

En este artículo 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. Parametrizamos las demostraciones en un conjunto de restricciones entre los parámetros del sistema, inicialmente considerados constantes y posteriormente generalizados a variables sujetas a ciertas restricciones establecidas –deducidas a partir de las condiciones de prueba de las propiedades analizadas del sistema que decidimos preservar. De esta manera generalizamos la especificación del sistema considerado, que es tratable con un *model checker* sólo para valores constantes de los parámetros. En [22] presentamos también una metodología de trabajo para la especificación y el

análisis de sistemas reactivos y de tiempo real que relaciona el contenido de las secciones previas y busca compatibilizar el uso de un *model checker* 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; 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*; y, abarcar una etapa de *síntesis* de sistemas de tiempo real. La metodología generaliza el desarrollo del caso de estudio presentado en este artículo.

Referencias

[1] B. Alpern and F. Schneider. "Defining liveness". *Information Processing Letters*, 21(4):181-185, 1985.

[2] R. Alur and D. Dill. "A theory of timed automata". *Theorical Computer Science*, 126:183-235, 1994.

[3] R. Alur and T. Henzinger. "A Really Temporal Logic". *Journal of the ACM*, 41(1):181-204, 1994.

[4] R. Alur, C. Courcoubetis, and D. Dill. "Model-checking for real-time systems". In *Proc. 5th Symp on Logics in Computer Science*, pages 414-425. IEEE Computer Society Press, 1990.

[5] J. Armstrong and L. Barroca. "Specification and verification of reactive systems behaviour: The railroad crossing example". *Real-Time Systems*, 10:143-178, 1996.

[6] 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.

[7] 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.

[8] 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.

[9] Z. Chaochen, C. Hoare, and A. Ravn. "A calculus of durations". *Information Processing Letters*, 40(5):269-276,1992.

[10] 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.

[11] T. Coquand and G. Huet. "The calculus of constructions". *Information and Computation*, 76(2/3), 1988.

[12] 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.

[13] C. Daws and S. Yovine. "Verification of multirate timed automata with KRONOS: two exemples". Technical Report Spectre-95-06, VERIMAG, 1995.

[14] E. Giménez. "Two Approaches to the Verification of Concurrent Programs in Coq". To appear, 1999.

[15] 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.

[16] A. Göllü, A. Puri, and P. Varaiya. "Discretization of timed automata". *Proc. 33rd CDC*, Orlando, Florida, 1994.

[17] 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.

[18] 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.

[19] T. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. "Symbolic model-checking for real-time systems". In *Proc. 7th Symp on Logics in Computer Science*. IEEE Computer Society Press, 1992.

[20] T. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. "Symbolic model-checking for real-time systems". In *Proc. 7th Symp on Logics in Computer Science*. IEEE Computer Society Press, 1992.

[21] T. Henzinger, Z. Manna, and A. Pnueli. "What good are digital clocks?". In *W. Kuich, editor, ICALP 92: Automata, Languages and Programming*, *LNCS* 623, pages 545-558. Springer-Verlag, 1992.

[22] 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. Disponible también en http://www.fing.edu.uy/~cluna.

[23] C. Luna. "Análisis de sistemas de tiempo real en teoría de tipos. Una metodología de trabajo". *Proc. 5to Workshop Iberoamericano de Ingeniería de Requisitos y Ambientes de Software, IDEAS'2002*. La Habana, Cuba, Abril de 2002.

[24] D. Mandrioli, Carlo Ghezzi, and Mehdi Jazayeri. *Fundamentals of Software Engineering*. Prentice *Hall*, 1991.

[25] 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.

[26] A. Olivero. *Modélisation et Analyse de Systèmes Temporisés et Hybrides*. PhD thesis, Institut National Polytéchnique de Grenoble. France, 1994.

[27] C. Paulin-Mohring. "Inductive definitions in the system Coq – rules and properties". In M. Bezem and J. Groote, editors, *Proceeedings of the conference Typed Lambda Calculi and Aplications*, *LNCS* 664, 1993.

[28] 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.

[29] N. Shankar. "Verification of real-time systems using PVS". In *CAV'93*, Greece. *LNCS* 697, pages 280-291, 1993.

[30] S. Yovine. "Kronos: A verification tool for real-time systems". *Software Tools for Technology* Transfer, 1997.