

Práctica 4: Especificaciones en TLA+

M. Cristiá

N. Colussi

A. Krapf

S. Scandolo

LCC – FCEIA – UNR

2026

Introducción

Para cada uno de los ejercicios se deberá:

- (i) Escribir las designaciones de los fenómenos que sean necesarias para resolver los problemas que se indican en cada sección.
- (ii) Detallar los requerimientos (R).
- (iii) Describir formalmente la especificación (S) en el lenguaje TLA.
- (iv) Enunciar el conocimiento del dominio (DK) mínimo para comprender R y S .

En todos los problemas el objetivo es modelar el software que controle los dispositivos físicos mencionados según los requerimientos que se expresan en cada caso.

1 Sistema de Iluminación

Describa un sistema de iluminación consistente en una lámpara y dos botones. Si la lámpara está apagada, al pulsar cualquiera de los dos botones, esta se enciende; y en caso contrario, la lámpara se apaga.

2 Puertas del Aeropuerto

Las puertas de los aeropuertos están provistas de un mecanismo que permite que una persona no necesite abrirlas o cerrarlas cada vez que las va a atravesar. Para ello poseen detectores de ambos lados que le permiten saber cuando una persona se encuentra en una zona específica de cercanía a las mismas, lo cual resulta ser un indicio de que se intentará atravesarlas. Una vez que la persona se retira de esta zona de influencia y transcurren T unidades de tiempo, las puertas se cierran.

Describir el mecanismo de funcionamiento de apertura y cierre de las puertas del aeropuerto.

3 Mouse

Describe el funcionamiento de un *mouse* de tres botones: izquierdo, central y derecho. A saber:

- El **botón central** no tiene asignada ninguna función.
- Con el **botón izquierdo** se puede realizar click simple, doble click y arrastrar.
- Con el **botón derecho** sólo se puede hacer click simple y arrastrar.

Pulsar más de un botón al mismo tiempo no tiene efecto.

4 Guardia Hospitalaria

Los pacientes de una guardia de terapia intensiva son monitoreados por dispositivos electrónicos analógicos adosados a sus cuerpos mediante sensores de varias clases. A través de los sensores, los dispositivos miden tres signos vitales de los pacientes, a saber:

- (i) un dispositivo mide el pulso;
- (ii) otro dispositivo mide la temperatura;
- (iii) y el último mide la presión sanguínea.

Se necesita un modelar un programa que lea los signos vitales con una frecuencia determinada para cada paciente. Los factores leídos serán comparados con rangos de seguridad especificados para cada paciente y las lecturas que excedan dichos rangos serán reportadas con mensajes de alarma en el monitor del box de enfermería. También debe mostrarse un mensaje apropiado si falla alguno de los dispositivos.

5 Cruce Peatonal

Sobre una calle de un sólo sentido existe un cruce peatonal. Para mayor seguridad de las personas que lo utilizan se decide colocar un semáforo con dos grupos de botones ubicados a cada uno de los lados de la calle.

Cuando el semáforo está en verde y se presiona uno de los botones, debe pasar T_1 unidades de tiempo para que se encienda la luz amarilla del semáforo y T_2 para que se encienda la luz roja. Esta última permanecerá encendida por T_3 unidades de tiempo.

Presionar alguno de los botones no tendrá ningún efecto, hasta que hayan pasado al menos T_4 unidades de tiempo desde la última vez que se presionó uno.

Analizar la situación cuando:

- A) Hay 1 (un) semáforo con sus botoneras tal cual se describió en el párrafo anterior.
- B) Hay 2 (dos) semáforos (cada uno con su propia botonera), los cuáles deben respetar los mismos requerimientos dados en la parte inicial del ejercicio.

6 Cinta Transportadora (Parte I)

Consideremos en este caso una celda de producción muy simple, la cual consta de dos cintas transportadoras y un brazo robótico para mover objetos. Las cintas de transporte funcionan concurrentemente y son supervisadas por la computadora que controla la celda de producción. El brazo robótico toma ítems de una u otra cinta según lo que ordene la computadora, para luego soltarlos en algún lugar. Se puede detener o reanudar la marcha de cada cinta (independientemente) por medio de una única señal por cinta.

Existen sensores que detectan el paso de un ítem por cada una de las cintas. Estos sensores pueden ser configurados para que emitan las señales apropiadas en caso de que dos ítem, sobre la misma o diferentes cintas, estén demasiado juntos. Dos ítem están demasiado juntos si el robot no es capaz de tomarlos a ambos sin que uno se caiga. El requerimiento para el sistema de control es que no debe caerse ningún ítem de ninguna cinta.

Modelar el software para controlar el funcionamiento de la celda de producción.

7 Cinta Transportadora (Parte II)

Reconsidere el problema anterior. Suponga ahora que los sensores no son tan inteligentes como para poder indicar la proximidad de dos ítem. Es decir, sólo son capaces de emitir una señal cada vez que pasa un ítem. Por otro lado, el robot demora un tiempo T_r para tomar un ítem, soltarlo, y volver a estar en condiciones de tomar otro.

Los requerimientos para el sistema de control son los siguientes:

- No debe caerse ningún ítem.
- Eventualmente todos los ítems de ambas cintas serán tomados por el robot.
- Por razones de eficiencia se espera que se tomen ítems de ambas cintas de forma más o menos regular (siempre que haya alguno disponible).

8 Luces del Museo

Un museo de bellas artes desea instalar un sistema de iluminación automático que mantenga la cantidad de luz dentro de cierto rango lumínico. Controlar los índices de luminosidad permitiría a los visitantes apreciar correctamente las obras de arte expuestas, y al mismo tiempo evitar que la luz de la sala produzca daños serios a las obras de arte.

El museo cuenta con ventanas e iluminación artificial. A las ventanas se les colocan persianas tipo americanas que pueden ser movidas por motores eléctricos de la siguiente manera:

- Las varillas horizontales pueden moverse desde su posición inicial (ventana cerrada) de a 1 (un) grado hasta que el motor emite una señal que indica que ya no es posible seguir girando y viceversa.
- La persiana puede elevarse o bajarse de a 1 (un) centímetro hasta que el motor emite una señal que indica que no es posible seguir bajando o subiendo.

Por otro lado, los artefactos de iluminación artificial son modificados de manera tal que es posible regular su intensidad (aumentándola o disminuyéndola) discretamente.

Al mismo tiempo, cerca de cada obra de arte se ha instalado un sensor que mide la cantidad de luz que llega. Este emite una señal cada vez que la cantidad de luz aumenta o disminuye en cierta medida fija. El sensor puede ser inicializado desde el exterior lo que hace que este emita varias señales consecutivas desde su estado de máxima obscuridad hasta medir la luz real en ese momento.

En primer lugar, el sistema de software deberá mantener la cantidad de luz sobre cada obra dentro de ciertos límites; y en segundo lugar, el sistema deberá optar primero por utilizar la luz proveniente de las ventanas y si esta no es suficiente deberá hacer uso de iluminación artificial.

Se pide modelar el sistema de software que controla la luminosidad de la sala según lo antes descripto.

9 El Automóvil

Modelar el software que permite controlar los siguientes mecanismos de un automóvil según lo indicado a continuación.

Las Llaves

El automóvil tiene una llave de encendido; la misma puede estar en tres posiciones, apagado, contacto o encendido. Se pasa de la primera posición a la segunda, de la segunda a la tercera y viceversa.

- Cuando la llave esta en contacto se pueden subir y bajar los vidrios.
- Cuando la llave esta en encendido se puede conducir.
- Cuando la llave se apaga se tienen 20" extras por si se quieren subir o bajar los vidrios.

La Caja de Cambio

Este automóvil tiene caja de cambios automática, es decir que los cambios de marcha se efectúan automáticamente con el aumento o disminución de la velocidad. Posee 4 marchas y punto muerto.

- Está en punto muerto cuando el auto esta frenado.

- Está en 1ra cuando su velocidad está entre 0.1 y 30km/h.
- Está en 2da cuando su velocidad está entre 30,1 y 50km/h.
- Está en 3era cuando su velocidad está entre 50,1 y 70 km/h.
- Está en 4ta cuando su velocidad supera los 70km/h.

Las Luces

Las luces del auto se controlan con una perilla mecánica, de tres posiciones: apagadas, posición y cortas.

- Las luces sólo están encendidas (en posición o cortas) cuando la llave de encendido del auto está en contacto o encendido.
- Al pasar la llave a “apagado”, se apagan las luces, pero la perilla mecánica se mantiene en su estado.
- Al volver a pasar la llave a posición de contacto o encendido, el estado de las luces dependerá del estado de la perilla. Esto implica que la perilla mecánica es independiente de la llave del auto, pero el estado de las luces no.

10 El Termómetro

El termómetro posee una tapa que al abrirse muestra un display (apagado) más dos botones, uno para encender el termómetro y otro para seleccionar la escala de temperaturas (°F o °C).

El termómetro se apaga al cerrar la tapa o cuando se termina la batería. Además, el termómetro posee una punta que se introduce en el oído del paciente y un botón que debe ser pulsado al menos un segundo para que la lectura sea exitosa. Deben mediar 10 segundos entre dos mediciones consecutivas. El display muestra un indicador de batería, la temperatura medida (o nada si recién se encendió) y la escala de temperaturas seleccionada (este dato es “recordado” por el termómetro aún luego de ser apagado).

Si una medición de temperatura es fallida, se muestra una E invertida. Una vez pulsado el botón de encendido, el termómetro chequea su funcionamiento durante 5 segundos y luego emite los datos iniciales al display (cualquier acción que se intente antes de esos 5 segundos debe ser obviada).

Un dato importante que se registra durante el chequeo es el estado de la batería. Esta pierde un cuanto de energía cada un segundo si sólo se usa el display, 3 quantos si se cambia la escala y 5 en cada medición errónea o no de temperatura. Cuando quedan 10 quantos de energía se enciende un icono en el display.

11 Horno Microondas

El horno microondas posee un panel de control semejante a algunos modelos populares. Los botones numerados del 1 al 4 se utilizan para fijar la potencia de cocción. La perilla circular puede girar en ambos sentidos y sirve para fijar el tiempo de cocción: si lo hace en sentido horario aumenta el tiempo de a 5 segundos, en el sentido contrario disminuye en la misma cantidad. Normalmente, en el display se muestra la hora actual pero cuando se fija el tiempo de cocción se la reemplaza por el tiempo que el usuario selecciona a medida que hace girar la perilla. Una vez que detiene la perilla, debe seleccionar una de las potencias de cocción y finalmente pulsar el botón **Start**. Al hacerlo la puerta debe estar cerrada y en el display se comienza a decrementar el tiempo de a un segundo.

- Si se pulsa **Stop** se borra el tiempo de cocción, se resetea la selección de la potencia y se vuelve a mostrar la hora.
- Si durante la cocción se abre la puerta, se detiene el tiempo de cocción y si se vuelve a cerrar se deberá pulsar **Start** nuevamente para continuar la cocción desde el punto donde se la abandonó.
- Se puede cambiar la potencia de cocción mientras se está cocinando.
- Si durante la cocción el usuario hace girar la perilla, el tiempo de cocción debe actualizarse.
- La cocción se detendrá automáticamente cuando el tiempo llegue a cero, luego de lo cual se volverá a mostrar la hora y se reseteará la potencia seleccionada.

12 Barco de Guerra

Un barco de guerra cuenta con un radar principal (RP), dos cañones idénticos (C1 y C2) cada uno con su radar (RS1 y RS2) y una sala de comando desde donde se indica si un objetivo apuntado por alguno de los dos cañones debe ser abandonado o destruido .

El RP está permanentemente escrutando el área de disparo en busca de objetivos. Cada vez que RP encuentra uno se lo debe asignar a uno de los dos cañones si alguno de ellos está libre (sin objetivo en su mira); al asignarlo se le indica la posición y la trayectoria del objetivo.

La posición inicial del cañón al asignársele un nuevo objetivo es conocida por el software. En función de la posición inicial y de los datos transmitidos por el RP, el software apunta el cañón y el RS al objetivo. Normalmente, un RS está inactivo hasta que le es asignado un objetivo. Desde ese momento el RS comienza a seguir su objetivo hasta que:

- A) Recibe la orden de disparar;
- B) Recibe la orden de abandonar el objetivo;

C) El objetivo se va fuera de alcance.

En cualquiera de los tres casos, el RS luego pasa a estar inactivo. El seguimiento del objetivo por parte de un RS implica mover el cañón lo cual está a cargo de un motor.

El software tiene a su cargo emitir las órdenes de movimiento del motor las cuales tienen la forma:

- Arriba (ang),
- Abajo(ang),
- GiroA(ang), y
- GiroH (ang),

donde ang es un ángulo.

Modelar el software para controlar el funcionamiento de los cañones del barco de guerra antes detallado.