Departamento de Cs. e Ingeniería de la Computación
Universidad Nacional del Sur

Métodos Formales para Ingeniería de Software

Trabajo Práctico N° 2

Modelado y Verificación - Alloy

Segundo Cuatrimestre de 2018

Importante: Para la resolución de los ejercicios de este trabajo práctico, es imprescindible el uso del *analizador* de Alloy. A tal efecto, deberá definir comandos para generar instancias significativas del modelo y verificar las restricciones impuestas sobre el mismo.
De manera similar, deberá verificarse que los predicados y/o funciones definidos siguen el comportamiento esperado de su definición.

Deberá dejarse constancia de los comandos utilizados (es decir, deberán quedar escritos en el archivo .als correspondiente).

Ejercicios

1. Considere el siguiente modelo en Alloy:

```
one sig Juan, Pedro {}

sig Culpable in univ {}

fact { Juan not in Culpable }

fact { Juan in Culpable implies Pedro in Culpable }

assert conclusion { Pedro not in Culpable }
```

   a) Analice el modelo brindado. Para ello, puede utilizar la funcionalidad de visualización provista por Alloy.

   b) Describa el significado intuitivo de los hechos incluidos en el modelo.

   c) Genere instancias del modelo provisto mediante el uso del comando `run { }`. ¿Cuál es el significado intuitivo de este comando? ¿Qué características observa en las instancias generadas?

   d) Defina el comando correspondiente para chequear la aserción definida. ¿Qué observa con respecto al resultado mostrado por la herramienta? ¿Qué sucede si se vuelve a chequear la aserción, habiendo removido el primer hecho? Justifique sus respuestas.

2. Considere el siguiente modelo en Alloy:

```
sig Candidato { }

one sig Alejo, Luca, Carlos, David in Candidato { }

one sig Maria {
                alto : set Candidato,
                moreno : set Candidato,
                buenmozo : set Candidato
              }
```

   a) Analice el modelo brindado. Para ello, puede utilizar la funcionalidad de visualización provista por Alloy.

   b) Genere instancias del modelo, sin restricciones adicionales, y analice sus características.

   c) Considere un escenario en el que María tiene cuatro candidatos: Alejo, Luca, Carlos y David. Dicha situación ¿se corresponde con las instancias del modelo anteriormente generadas? En caso negativo, añada las restricciones necesarias para modelar el escenario aquí planteado.

   d) El hombre ideal de María, es alto, moreno y buen mozo. Sólo uno de los cuatro hombres tiene todas las características que María desea ¿cuál es?

   Hallar la respuesta a esta pregunta mediante el uso de la herramienta, agregando especificaciones sobre el modelo para garantizar que:

   - Sólo tres de los hombres son altos, sólo dos son morenos, y sólo uno es buenmozo.
   - Cada uno de los cuatro hombres tiene al menos una de las características buscadas por María.
   - Alejo y Luca tienen la misma complexión (ambos son morenos o ambos no lo son).
   - Luca y Carlos tienen la misma altura.
   - O bien Carlos es alto o David lo es, pero ambos no lo son.

3. Dada la siguiente definición de modelo en Alloy:

```
abstract sig Person {
    children: set Person,
    siblings: set Person
}

sig Man, Woman extends Person {}

sig Married in Person {
    spouse: one Married
}
```

   a) Analice el modelo brindado. ¿Parece correcto?

b) Genere y analice tres instancias del modelo brindado. ¿Qué irregularidades detecta?

c) Defina una restricción para el modelo que permita identificar los padres de una persona.

d) Modifique el modelo brindado, añadiendo las restricciones indicadas en cada ítem:

- Ninguna persona puede ser su propio ancestro.
- Ninguna persona puede tener más de una madre, ni más de un padre.
- Los hermanos de una persona son aquellas personas que poseen un padre en común (es decir, considere la existencia de medio-hermanos).

e) A partir del modelo resultante de añadir las restricciones indicadas hasta el momento, la relación *siblings* ¿es simétrica? Defina una restricción para chequear esto en Alloy.

f) A partir del modelo resultante de añadir las restricciones indicadas hasta el momento, la relación *siblings* ¿admite que una persona sea hermana de sí misma? Defina una restricción para chequear esto en Alloy. ¿Cómo modificaría el modelo para asegurar que esta restricción se cumpla?

g) Defina en Alloy una restricción para determinar si dos personas son parientes de sangre. (Observación: En general, dos personas son parientes de sangre si poseen un ancestro en común).

h) A partir del modelo resultante de añadir las restricciones indicadas hasta el momento ¿es posible que dos parientes de sangre tengan hijos en común? Defina la restricción necesaria para chequear esto en Alloy. Modifique el modelo para garantizar que dicha restricción se cumpla.

i) A partir del modelo resultante de añadir las restricciones indicadas hasta el momento, ¿la relación *spouse* es simétrica? ¿Es posible que una persona esté casada con más de una persona? ¿Es posible que una persona esté casada consigo misma? Defina restricciones en Alloy para chequear esto. ¿Cómo modificaría el modelo para asegurar la primera restricción y evitar la segunda y tercera?

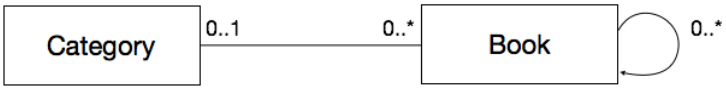
j) A partir del modelo resultante de añadir las restricciones indicadas hasta el momento ¿es posible que una persona esté casada con un familiar de sangre? Defina en Alloy una restricción para chequear esto. ¿Cómo modificaría el modelo para evitar dicha situación?

k) A partir del modelo resultante de añadir las restricciones indicadas hasta el momento ¿es posible que haya personas que no posean padre ni madre? Defina una restricción que permita identificar si una persona se encuentra en tal situación, y otra restricción que permita obtener el conjunto de personas en tal condición.

l) Defina comandos `run` para crear, en caso de ser posible, instancias del modelo que cumplan con las siguientes restricciones:

- Crear una instancia en la que las relaciones *spouse* y *siblings* no sean vacías.
- Crear una instancia con dos parejas casadas *diferentes*.
- Crear una instancia con a lo sumo un átomo en cada signatura de alto nivel y con un hombre casado.
- Crear una instancia con a lo sumo dos átomos en cada signatura de alto nivel y con un hombre casado.
- Crear una instancia donde haya a lo sumo una persona, alguna mujer y ningún hombre.

4. Considere el siguiente diagrama de clases, el cual modela una colección de libros:



Cada libro puede pertenecer a una categoría, la cual está conformada por todos los libros que pertenecen a ella. Asimismo, cada libro puede clasificar a un conjunto de libros como similares a él. Escriba un modelo en Alloy para representar este dominio, añadiendo las restricciones que considere necesarias.

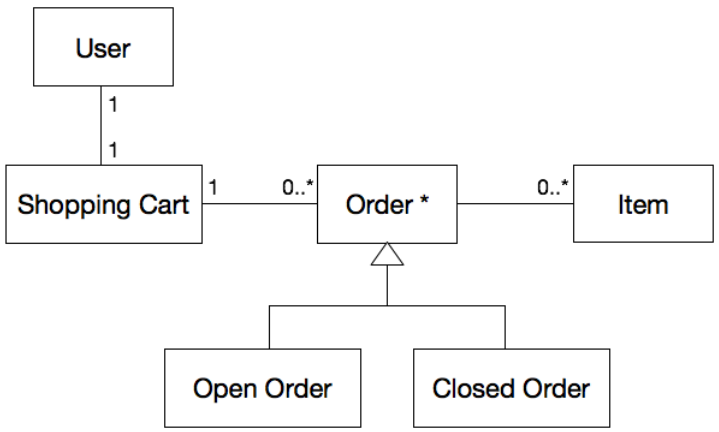
5. Considere el siguiente diagrama de clases, el cual modela la existencia de un almacenamiento de mensajes, que gestiona el envío y recepción de mensajes de computadoras que tienen acceso autorizado a él. Un mensaje posee una computadora de origen, una computadora destino, y un texto que representa el contenido del mensaje. Una computadora puede enviar al almacenamiento un mensaje cuya destinataria sea una de sus computadoras vecinas. Asimismo, una computadora puede recibir del almacenamiento un mensaje del cual sea destinataria. El almacenamiento tiene limitaciones de espacio en cuanto a la cantidad de mensajes que puede albergar (máximo 50 mensajes). De manera similar, el almacenamiento no puede gestionar pedidos de más de 5 computadoras autorizadas.

Escriba un modelo en Alloy para representar este dominio, añadiendo las restricciones que considere necesarias. Asimismo, deberá definir un conjunto de restricciones que permitan verificar que el modelo admite el siguiente comportamiento:

- Una computadora puede enviar (añadir) al almacenamiento un mensaje para sí misma o para una computadora vecina.
- Una computadora puede recibir (retirar) del almacenamiento un mensaje que la tenga como destinataria.
- Una computadora puede consultar al almacenamiento (sin retirar) todos los mensajes que la tengan como destinataria.
- Una computadora puede consultar al almacenamiento (sin retirar) todos los mensajes que la tengan como destinataria y que hayan sido enviados por una de sus computadoras vecinas.
- Una computadora puede recibir (retirar) del alacenamiento todos los mensajes que la tengan como destinataria y que hayan sido enviados por una de sus computadoras vecinas.
- Una computadora puede recibir (retirar) del alacenamiento todos los mensajes que la tengan como destinataria.
- Agregar una computadora al conjunto de computadoras autorizadas de un almacenamiento.
- Remover una computadora del conjunto de computadoras autorizadas de un almacenamiento. Dicha computadora puede ser removida únicamente si el almacenamiento no posee mensajes que la tengan como destinataria.

- Remover una computadora del conjunto de computadoras autorizadas de un almacenamiento. Al remover dicha computadora, el almacenamiento mantiene todos los mensajes que la tengan como destinataria.
- Remover una computadora del conjunto de computadoras autorizadas de un almacenamiento. Al remover dicha computadora, el almacenamiento elimina todos los mensajes que la tengan como destinataria.

6. Considere el siguiente diagrama de clases, el cual modela un sistema en el que usuarios pueden hacer uso de carritos de compras para efectuar diversas órdenes con el objetivo de comprar ítems:



Escriba un modelo en Alloy para representar este dominio, añadiendo las restricciones que considere necesarias. Asimismo, deberá definir un conjunto de restricciones que permitan verificar que el modelo admite el siguiente comportamiento:

- Añadir un ítem a una orden.
- Remover un ítem de una orden.
- Añadir una nueva orden para un usuario.
- Remover una orden de un usuario.
- Cerrar una orden de un usuario.
- Despachar el carrito de compras de un usuario.