Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur

Métodos Formales para Ingeniería de Software

Segundo Cuatrimestre de 2023

Trabajo Práctico N° 3: **Modelado Estático y Verificación Formal en Alloy**

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, o bien chequear propiedades satisfechas por toda instancia del modelo. De manera similar, deberá verificarse que los predicados y/o funciones definidos siguen el comportamiento esperado en su definición.

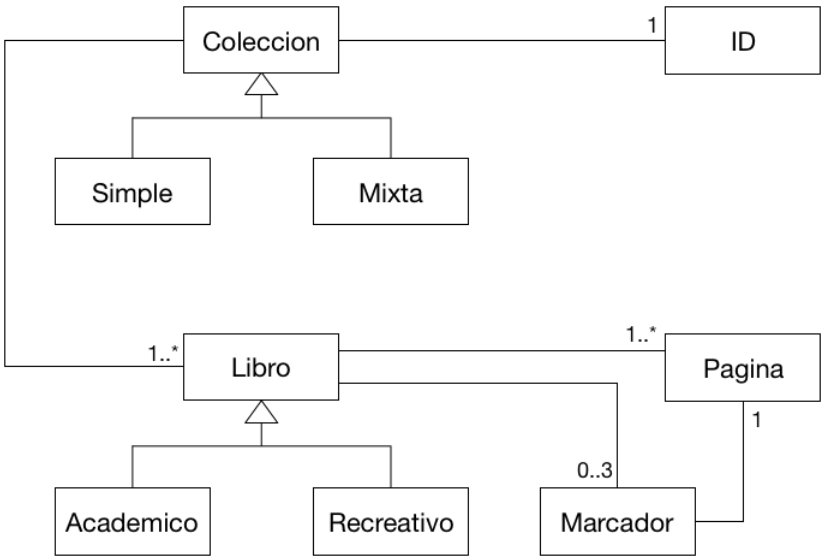
Deberá dejarse constancia de los comandos utilizados para la resolución de cada ejercicio.

En caso de utilizar el evaluador para complementar la validación del modelo, deberá dejarse registro (mediante capturas de pantalla) de la verificación realizada con el evaluador, indicando el comando utilizado para generar la instancia sobre la cual se utilizó el mismo.

Puede brindar cualquier otra especificación (hecho, aserción, predicado, función, etc.) adicional que considere necesaria y sea sensata.

Ejercicios

1. Considere el siguiente diagrama, el cual modela información acerca de las colecciones de libros que tiene una biblioteca. Toda colección posee un identificador y está categorizada como simple o mixta, pero no ambas. En particular, una colección simple no tiene libros de distinta categoría (ni tampoco mezcla libros categorizados con no categorizados). Por otra parte, un libro puede pertenecer a la categoría recreativo o académico, siendo estas mutuamente excluyentes, pero no necesariamente todo libro está categorizado. Por último, un libro posee un conjunto de páginas y un grupo de hasta tres marcadores, cada uno de los cuales puede referenciar a una página del libro.



a) Escriba el siguiente modelo en Alloy, correspondiente al dominio antes presentado:

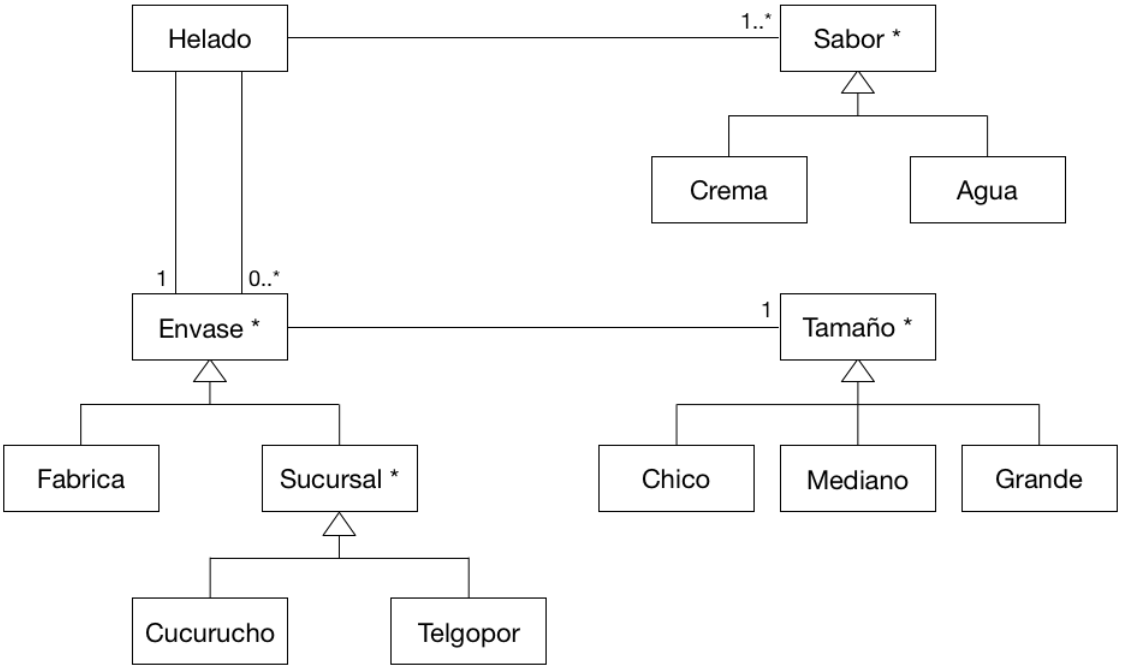
```
sig Coleccion {  ident: ID,
                 librosCol: set Libro }

sig ID { }

sig Simple, Mixta in Coleccion { }

sig Libro { paginas: some Pagina,
            marcadores: set Marcador }

sig Marcador { pag: Pagina }

sig Academico, Recreativo in Libro { }

sig Pagina { }

fact { some c: Coleccion | (c in Mixta) or (c in Simple) }

fact { disj[Academico, Recreativo] }

fact {#Marcador > 0}

fact {#Marcador < 4}

fact {no m: Marcador, l: Libro | (m in l.marcadores) and (m.pag in l.paginas) }
```

b) Utilice el analizador para validar si el modelo brindado cumple con las características contempladas en el diagrama brindado y su correspondiente descripción.
Para cada comando utilizado en la verificación formal del modelo, deberá explicar el propósito del mismo y el resultado obtenido por el analizador en respuesta a su ejecución.

c) Para cada propiedad o característica deseada y no satisfecha por el modelo (identificada a partir de la validación realizada en el inciso previo), explique qué cambios realizaría en el modelo para que se cumpla.
Análogamente, para cada propiedad o característica no deseada pero satisfecha por el modelo (identificada a partir de la validación realizada en el inciso previo), explique qué cambios efectuaría sobre el modelo para impedirla.

d) Para cada propiedad o característica analizada en el inciso anterior, realice los cambios necesarios en el modelo (ya sea el modelo de base y/o las restricciones brindadas) y valide el modelo resultante.
Para cada comando utilizado en el proceso de validación, explique el propósito del mismo y el resultado obtenido por el analizador en respuesta a su ejecución (de manera análoga a lo realizado en el inciso *b*).

2. Considere el siguiente diagrama, el cual modela información acerca de los helados que vende una heladería. Cada helado posee al menos un sabor, y el tipo de todo sabor es *a la crema* o *al agua*. Asimismo, cada helado posee un envase principal (el recipiente en el que se entrega el helado) y, posiblemente, un conjunto de envases adicionales. Los envases son de fábrica (para helados pre-envasados) o de sucursal (para helados servidos en la sucursal), pero no a ambos. En particular, todo envase de sucursal es de telgopor o es un cucurucho comestible, siendo los cucuruchos los únicos utilizables como envases adicionales y solo para aquellos helados cuyo envase principal es de telgopor. Además, todo envase posee un tamaño, el cual es chico, mediano o grande. En cuanto a los tamaños de los envases, los cucuruchos solo se encuentran disponibles en tamaño mediano o grande. Por otra parte, los helados pre-envasados (en fábrica) no contienen sabores al agua, mientras que los helados servidos en cucurucho no pueden contener sabores de distinto tipo (es decir, no pueden tener simultáneamente sabores al agua y a la crema). Finalmente, en cuanto a la cantidad de sabores que es posible servir en un helado, los helados cuyo envase principal es un cucurucho pueden tener hasta dos sabores, mientras que los helados con envase principal de telgopor pueden tener hasta cuatro sabores; para estos últimos, la cantidad de envases adicionales no puede superar la cantidad de sabores del helado.



a) Escriba el siguiente modelo en Alloy, correspondiente al dominio antes presentado:

```
sig Helado {
              sabores: some Sabor,
              principal: lone Envase,
              adicionales: set Envase
}

abstract sig Sabor { }

sig Crema, Agua in Sabor { }

abstract sig Envase { tam: set Tamanio }

sig Fabrica extends Envase { }
```

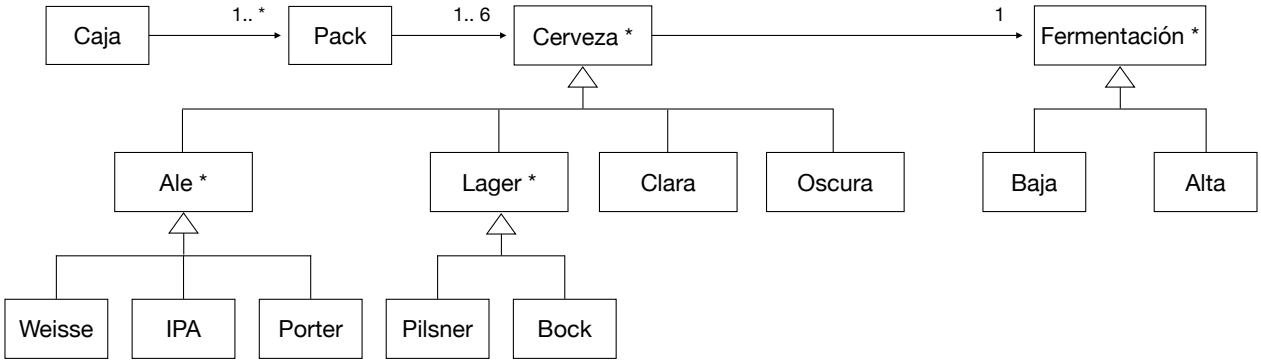
```
abstract sig Sucursal extends Envase { }

sig Cucurucho, Telgopor extends Sucursal { }

abstract sig Tamanio { }

one sig Chico, Mediano, Grande extends Tamanio { }

fact { (Helado.principal in Cucurucho) implies (Helado.adicionales = none) }

fact { some c: Cucurucho | c.tam in (Mediano+Grande) }

fact { all h: Helado | (h.principal in Fabrica) implies (h.sabores !in Agua) }

fact {
       no h: Helado, s: Sabor | (h.principal = Cucurucho) and (s in Crema) and
                                (s in Agua) and (s in h.sabores)
}

fact { no h: Helado, c: Cucurucho | ((h -> c) in principal) and (#h.sabores > 2) }

fact { all t: Telgopor | #((principal.t).adicionales) =< #((principal.t).sabores) }
```

b) Utilice el analizador para validar si el modelo brindado cumple con las características contempladas en el diagrama brindado y su correspondiente descripción.
Para cada comando utilizado en la verificación formal del modelo, deberá explicar el propósito del mismo y el resultado obtenido por el analizador en respuesta a su ejecución.

c) Para cada propiedad o característica deseada y no satisfecha por el modelo (identificada a partir de la validación realizada en el inciso previo), explique qué cambios realizaría en el modelo para que se cumpla.
Análogamente, para cada propiedad o característica no deseada pero satisfecha por el modelo (identificada a partir de la validación realizada en el inciso previo), explique qué cambios efectuaría sobre el modelo para impedirla.

d) Para cada propiedad o característica analizada en el inciso anterior, realice los cambios necesarios en el modelo (ya sea el modelo de base y/o las restricciones brindadas) y valide el modelo resultante.
Para cada comando utilizado en el proceso de validación, explique el propósito del mismo y el resultado obtenido por el analizador en respuesta a su ejecución (de manera análoga a lo realizado en el inciso *b*).

3. Considere el siguiente diagrama, el cual modela información acerca de cervezas de distintos tipos y tonalidades, las temperaturas a las que son fermentadas, y distintas formas de presentación en las que se venden (packs/cajas):



El tipo de toda cerveza es Ale o Lager. En cuanto al tiempo de fermentación, las Ale se fermentan a temperatura alta, mientras que las Lager se fermentan a temperatura baja. Asimismo, toda cerveza tiene una tonalidad, la cual es clara, oscura o intermedia (clara y oscura a la vez). En particular, las cervezas Weisse y Pilsner son claras, mientras que las IPA y Bock son intermedias, y las Porter son oscuras. Por último, existen limitaciones con respecto a la cantidad y características de las cervezas que integran los packs y cajas. Por una parte, la venta de cervezas se realiza en packs de 3 o 6 cervezas, o en cajas de 1 o más packs que contabilizan un total de 6 o 12 cervezas. Además, todas las cervezas de un pack son del mismo tipo o todas poseen la misma tonalidad.

a) Escriba un modelo en Alloy para representar este dominio respetando el diagrama brindado y todas las condiciones indicadas en la descripción.

b) Utilice el analizador para validar si el modelo especificado (tanto el modelo de base que comprende la definición de signaturas y relaciones como las restricciones que haya añadido) cumple con las características contempladas en el diagrama brindado y su correspondiente descripción.
Para cada comando utilizado en la verificación formal del modelo, deberá explicar el propósito del mismo y el resultado obtenido por el analizador en respuesta a su ejecución.

c) Defina una función que permita obtener el conjunto de cervezas que son solo claras y están en un pack de 3 cervezas del mismo tipo, dentro de una caja con un total de 6 cervezas.

d) Utilice el analizador para validar la función definida en el inciso anterior, y complemente la verificación utilizando el evaluador.
Para cada comando utilizado en la validación de la función, deberá explicar el propósito del mismo y el resultado obtenido por el analizador en respuesta a su ejecución, o bien el resultado obtenido al utilizar el evaluador.