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

Métodos Formales para Ingeniería de Software

Segundo Cuatrimestre de 2024

Trabajo Práctico Nº 3: **Alloy: Modelado de Dinámica y Verificación Formal**

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.

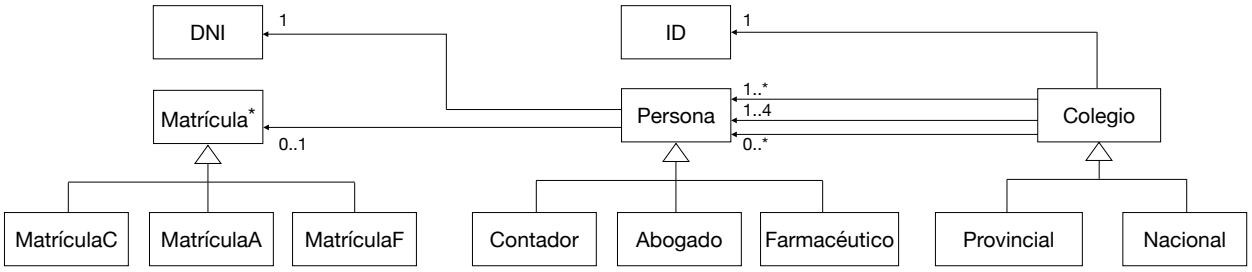
Puede brindar cualquier otra especificación (hecho, aserción, predicado, función, etc.) adicional que considere necesaria y sea sensata.

Deberá dejarse constancia de todos 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 empleado para generar la instancia sobre la cual se utilizó el mismo.

Ejercicios

1. Considere el siguiente diagrama, el cual modela información acerca de colegios de profesionales, sus características, y características de las personas que los conforman:



Toda persona se encuentra identificada por su DNI y tiene a lo sumo una profesión. Por otra parte, una persona puede o no encontrarse matriculada para la profesión que tenga. Cada colegio es de un tipo: provincial o nacional. Los colegios poseen un número que los identifica, y su consejo directivo se encuentra conformado por un conjunto de consejeros titulares y otro conjunto de consejeros suplentes, todos los cuales son además miembros del colegio. Ningún consejero de un Colegio puede ser titular y suplente a la vez. Todos los miembros de un colegio poseen la misma profesión y se encuentran matriculados para dicha profesión, siendo esa profesión la que determina la categoría del colegio. El consejo directivo de un colegio provincial posee entre 1 y 3 consejeros titulares, y la cantidad de consejeros suplentes no puede superar a la cantidad de titulares. Por último, el consejo directivo de un colegio nacional posee entre 1 y 4 consejeros titulares, y un máximo de 2 suplentes.

   (a) Escriba el siguiente modelo en Alloy, correspondiente al dominio antes presentado. Asuma que el mismo es correcto y fue validado en un contexto de modelado estático:

```
sig Colegio {    miembros: some Persona,
                 titulares: some Persona,
                 suplentes: set Persona,
                 id: one ID
}

sig Provincial, Nacional extends Colegio {}

sig ID {}

sig Persona {    dni: one DNI,
                 matricula: lone Matricula
}

sig Contador, Abogado, Farmaceutico extends Persona {}

sig DNI {}

abstract sig Matricula {}

sig MatriculaC, MatriculaA, MatriculaF extends Matricula {}

fact {all disj p1, p2: Persona | p1.dni != p2.dni}

fact {no disj p1, p2: Persona | (some p1.matricula) and (some p2.matricula) and
                                 (p1.matricula = p2.matricula)}

fact {all disj c1, c2: Colegio | c1.id != c2.id}

fact {Colegio = (Provincial+Nacional)}

fact {all c: Colegio | no (c.titulares & c.suplentes)}

fact {all c: Colegio | (c.titulares + c.suplentes) in c.miembros}

fact {all p: Persona | (some (MatriculaC & p.matricula)) implies (p in Contador)}

fact {all p: Persona | (some (MatriculaA & p.matricula)) implies (p in Abogado)}

fact {all p: Persona | (some (MatriculaF & p.matricula)) implies (p in Farmaceutico)}

fact {all p1, p2: Persona, c: Colegio | ((p1 in c.miembros) and (p2 in c.miembros))
                                          implies (mismaProfesion[p1,p2] and
                                                   matriculadosParaMismaProfesion[p1,p2])}

fact {all c: Provincial | (#c.titulares =< 3) and (#c.suplentes =< #c.titulares)}

fact {all c: Nacional | (#c.titulares < 5) and (#c.suplentes =< 2)}

pred mismaProfesion[p1, p2: Persona]
{ (p1+p2 in Contador) or (p1+p2 in Abogado) or (p1+p2 in Farmaceutico) }

pred matriculadosParaMismaProfesion[p1, p2: Persona] {
    ((some (p1.matricula & MatriculaC)) and (some (p2.matricula & MatriculaC))) or
    ((some (p1.matricula & MatriculaA)) and (some (p2.matricula & MatriculaA))) or
    ((some (p1.matricula & MatriculaF)) and (some (p2.matricula & MatriculaF)))
}
```

(b) Incorpore al modelo el siguiente predicado, el cual modela el comportamiento de *añadir una persona al conjunto de miembros de un colegio provincial de contadores*. Esta acción es posible siempre y cuando la persona pertenezca al consejo directivo de un colegio nacional para esa profesión:

```
pred agregarMiembro[c1, c2: Colegio, p: Persona] {
   (no c3: Nacional | (p in c3.(titulares+suplentes))) and
   (p in c2.miembros) and
   (c1.titulares in c2.titulares) and
   (c1.suplentes in c2.suplentes)
}
```

Utilice el analizador para validar si la definición del predicado `agregarMiembro` es correcta, considerando el modelo y la descripción brindada para el predicado.

Deberá dejarse registro de cada comando utilizado en la validación, teniendo en cuenta las siguientes consideraciones:

- Para aquellos comandos que no generen instancias, deberán explicarse los motivos por los cuales no lo hacen.
- Para aquellos comandos que generen instancias en las que se observan irregularidades, deberá dejarse registro de dicha instancia (por ejemplo, mediante una captura de pantalla), describiendo cuáles son las irregularidades o problemas allí observados e indicando cuál fue el comando utilizado para generar dicha instancia; en caso de ser necesario, deberá indicarse también el número de instancia generada por dicho comando (por ejemplo, si se trata de la primera instancia, de la segunda instancia, etc.).

(c) Realice los cambios necesarios en el predicado `agregarMiembro` y/o en el modelo, de manera tal que la nueva definición del predicado sea correcta.

Una vez realizados los cambios necesarios, valide el predicado resultante considerando al menos 3 casos de éxito y 3 casos de no éxito.

(d) Defina una función que permita obtener el conjunto de abogados o farmacéuticos que son consejeros titulares del consejo directivo de al menos un colegio y son consejeros suplentes de a lo sumo un colegio.

Brinde comandos para validar la función definida, y en caso de utilizar el evaluador almacene capturas de pantalla de las pruebas realizadas.

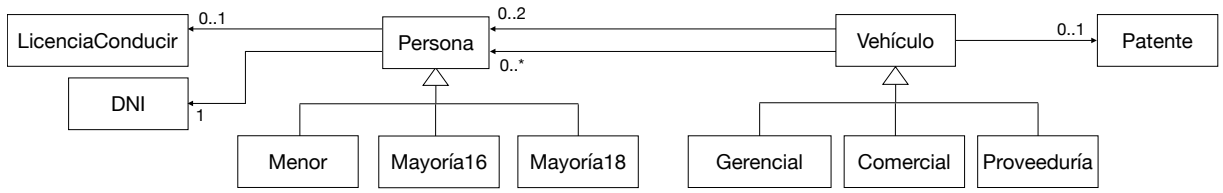
(e) Defina un predicado que modele el comportamiento de *realizar el traspaso de un consejero suplente del consejo directivo de un colegio a su conjunto de consejeros titulares*:

```
suplenteATitular[c1, c2:  Colegio, p:  Persona]
```

Para que dicha acción pueda realizarse la persona no debe formar parte del consejo directivo de un colegio con distinto identificador que el colegio para el cual se está realizando el traspaso. Además, luego del traspaso, el colegio deberá contar con al menos un consejero suplente. Deberá explicitarse toda pre y post-condición asociada a la acción, incluyendo las indicadas en la descripción brindada, así como también las condiciones de marco.

Valide el predicado definido, considerando al menos 3 casos de éxito y 3 casos de no éxito.

2. Considere el siguiente diagrama, el cual modela información acerca de vehículos de una empresa, así como también información sobre sus titulares o personas autorizadas a conducirlos:



Cada vehículo es de un tipo: gerencial, comercial o de proveeduría. Los vehículos con patente poseen entre uno y dos titulares y, posiblemente, un conjunto adicional de personas que también se encuentran autorizadas a conducir el vehículo; los vehículos no patentados no poseen titulares ni autorizados. Cada persona se encuentra identificada por su DNI y puede o no ser poseedora de una licencia para conducir. Asimismo, las personas se encuentran clasificadas de acuerdo a su mayoría de edad, distinguiéndose tres grupos: personas que poseen menos de 16 años, personas que poseen al menos 16 años, y personas que poseen al menos 18 años.

Los titulares de un vehículo deben poseer al menos 18 años, mientras que para las personas adicionalmente autorizadas a conducir un vehículo solo se requiere la mayoría de 16 años. Solo pueden poseer carnet de conducir aquellas personas que tengan al menos 16 años. Los vehículos gerenciales no pueden tener más de un titular. Los vehículos de proveeduría poseen un máximo de 3 autorizados adicionales para su conducción.

(a) Escriba el siguiente modelo en Alloy, correspondiente al dominio antes presentado. Asuma que el mismo es correcto y fue validado en un contexto de modelado estático:

```
sig Vehiculo {
                titulares: set Persona,
                autorizados: set Persona,
                placa: lone Patente
}

sig Proveeduria, Comercial, Gerencial extends Vehiculo {}

sig Patente {}

sig Persona {
               id: one DNI,
               carnet: lone LicenciaConducir
}

sig Mayoria18, Mayoria16, Menor in Persona {}

sig DNI {}

sig LicenciaConducir {}

fact {no Vehiculo - Proveeduria - Comercial - Gerencial}

fact {all v: Vehiculo | (some v.placa) implies (some v.titulares and #v.titulares < 3)}

fact {no v: Vehiculo | some (v.titulares & v.autorizados)}

fact {no v: Vehiculo | (no v.placa) and ((some v.titulares) or (some v.autorizados))}
```

```
fact {no disj p1, p2: Persona | (p1.id = p2.id)}

fact {no Persona - Menor - Mayoria16 - Mayoria18}

fact {no Menor & Mayoria16}

fact {no Menor & Mayoria18}

fact {Mayoria18 in Mayoria16}

fact {all p: Persona| (some titulares.p) implies (p in Mayoria18)}

fact {all p: Persona | (some autorizados.p) implies (p in Mayoria16)}

fact {all p: Persona | (some p.carnet) implies (p in Mayoria16)}

fact {all vg: Gerencial | lone vg.titulares}

fact {all vp: Proveeduria | #(vp.autorizados) < 4}

fact {no disj p1, p2: Persona | (some p1.carnet) and (some p2.carnet) and
                                (p1.carnet = p2.carnet)}

fact {no disj v1, v2: Vehiculo | (some v1.placa) and (some v2.placa) and
                                (v1.placa = v2.placa)}
```

(b) Incorpore al modelo el siguiente predicado, el cual modela el comportamiento de *añadir una persona al conjunto de personas autorizadas a manejar un vehículo de proveeduría.* Esta acción es posible siempre y cuando la persona posea licencia de conducir y la cantidad original de personas autorizadas a manejar el vehículo no supere a la cantidad de titulares del mismo:

```
pred agregarAutorizado[v1, v2: Vehiculo, p: Persona] {
    (one p.carnet) and
    (#v1.autorizados > #v1.titulares) and
    (p in v2.autorizados) and
    (v2.titulares = v1.titulares)
}
```

Utilice el analizador para validar si la definición del predicado `agregarAutorizado` es correcta, considerando el modelo y la descripción brindada para el predicado.
Deberá dejarse registro de cada comando utilizado en la validación, teniendo en cuenta las siguientes consideraciones:

- Para aquellos comandos que no generen instancias, deberán explicarse los motivos por los cuales no lo hacen.
- Para aquellos comandos que generen instancias en las cuales se observan irregularidades, deberá dejarse registro de dicha instancia (por ejemplo, mediante una captura de pantalla), describiendo cuáles son las irregularidades o problemas allí observados e indicando cuál es el comando utilizado para generar dicha instancia; en caso de ser necesario, deberá indicarse también el número de instancia generada por dicho comando (por ejemplo, si se trata de la primera instancia, de la segunda instancia, etc.).

(c) Realice los cambios necesarios en el predicado `agregarAutorizado` y/o en el modelo, de manera tal que la nueva definición del predicado sea correcta.

Una vez realizados los cambios necesarios, valide el predicado resultante considerando al menos 3 casos de éxito y 3 casos de no éxito.

(d) Defina una función que permita obtener el conjunto de personas que poseen al menos 18 años, no tienen carnet de conducir y son titulares algún vehículo comercial o gerencial.

Brinde comandos para validar la función definida, y en caso de utilizar el evaluador almacene capturas de pantalla de las pruebas realizadas.

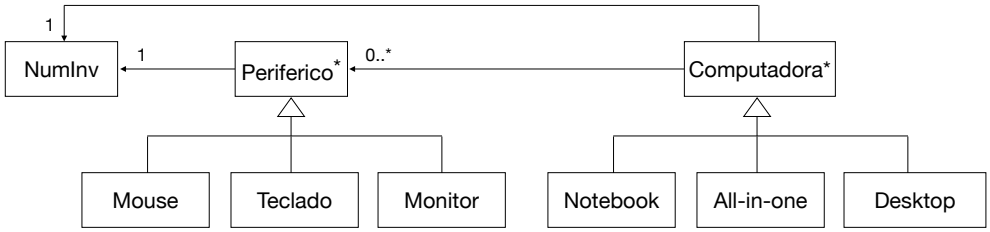
(e) Defina un predicado que modele el comportamiento de realizar el *traspaso de una persona autorizada a conducir un vehículo a su conjunto de titulares*:

```
autorizadoATitular[v1, v2:  Vehiculo, p:  Persona]
```

Para que dicha acción pueda realizarse la persona no debe ser titular de un vehículo de distinto tipo al vehículo para el cual se está realizando el traspaso. Además, luego del traspaso, el vehículo deberá contar con al menos una persona autorizada para manejarlo. Deberá explicitarse toda pre y post-condición asociada a la acción, incluyendo las indicadas en la descripción brindada, así como también las condiciones de marco.

Valide el predicado definido, considerando al menos 3 casos de éxito y 3 casos de no éxito.

3. Considere el siguiente diagrama, el cual modela información acerca de computadoras y algunas de sus características:



Toda computadora y todo periférico se encuentran identificados unívocamente por un número de inventario. Cada computadora es de un tipo: notebook, all-in-one o desktop. Asimismo, los periféricos que poseen las computadoras se categorizan en: mouse, teclado o monitor.

(a) Escriba el siguiente modelo en Alloy, correspondiente al dominio antes presentado. Asuma que el mismo es correcto y fue validado en un contexto de modelado estático:

```
abstract sig Computadora{
                            perifericos: set Periferico,
                            inv_comp: one NumInv
}

sig Notebook, All_In_One, Desktop extends Computadora {}

abstract sig Periferico { inv_perif: one NumInv }

sig Mouse, Teclado, Monitor extends Periferico { }

sig NumInv { }

fact {all disj c1, c2: Computadora | c1.inv_comp != c2.inv_comp}

fact {all disj p1, p2: Periferico | p1.inv_perif != p2.inv_perif}

fact {no c1, c2: Computadora, p: Periferico | (p in c1.perifericos) and
                                              (p in c2.perifericos) and
                                              (c1.inv_comp != c2.inv_comp)}
```

(b) Extienda el modelo brindado añadiendo las siguientes restricciones:

- Las desktop tienen al menos un monitor.
- Las notebooks no tienen mouse ni teclado.
- Las all-in-one y las desktop tienen al menos un teclado y al menos un mouse.
- Ninguna computadora puede tener más de 5 periféricos que sean monitores.

Puede agregar cualquier otra restricción adicional que sea sensata, justificando su inclusión. Luego de realizar los cambios requeridos brinde comandos para validar el modelo modificado, dejando registro del resultado obtenido en cada caso.

(c) Incorpore al modelo resultante del inciso anterior el siguiente predicado, el cual modela el comportamiento de *añadir un periférico a una computadora desktop*. Esta acción es posible siempre y cuando la computadora originalmente posea la misma cantidad de teclados y mouse:

```
pred agregarPeriferico[c1, c2: Computadora, p: Periferico] {
   not(#(c2.perifericos & Mouse) = #(c2.perifericos & Teclado)) and
   (p in c2.perifericos) and
   (c1.perifericos in c2.perifericos)
}
```

Utilice el analizador para validar si la definición del predicado `agregarPeriferico` es correcta, considerando el modelo resultante del inciso *b*) y la descripción brindada para el predicado.

Deberá dejarse registro de cada comando utilizado en la validación, teniendo en cuenta las siguientes consideraciones:

- Para aquellos comandos que no generen instancias, deberán explicarse los motivos por los cuales no lo hacen.
- Para aquellos comandos que generen instancias en las que se observan irregularidades, deberá dejarse registro de dicha instancia (por ejemplo, mediante una captura de pantalla), describiendo cuáles son las irregularidades o problemas allí observados e indicando cuál fue el comando utilizado para generar dicha instancia; en caso de ser necesario, deberá indicarse también el número de instancia generada por dicho comando (por ejemplo, si se trata de la primera instancia, de la segunda instancia, etc.).

(d) Defina un predicado que modele el comportamiento de *quitar un monitor de una all-in-one o de una notebook*

```
quitarMonitor[c1, c2:  Computadora, p:  Periferico]
```

Para que dicha acción pueda realizarse la cantidad de teclados y mouse de la computadora original no puede superar (en forma conjunta) su cantidad de monitores. Además, luego del traspaso, la computadora deberá contar con al menos dos monitores. Deberá explicitarse toda pre y post-condición asociada a la acción, incluyendo las indicadas en la descripción brindada, así como también las condiciones de marco.

Valide el predicado definido, considerando al menos 3 casos de éxito y 3 casos de no éxito.

(e) Incorpore al modelo modificado el siguiente predicado, el cual modela el comportamiento de *reemplazar un periférico por otro del mismo tipo en una all-in-one*. Esta acción es posible siempre y cuando el periférico a reemplazar sea un teclado o un monitor:

```
pred reemplazarPeriferico[c1, c2: Computadora, p1, p2: Periferico]{
    (p1 in c1.perifericos) and
    (p2 !in c1.perifericos) and
    (p1 ! in Teclado + Monitor) and
    (c1.perifericos != c2.perifericos)
    (p2 in c2.perifericos)
}
```

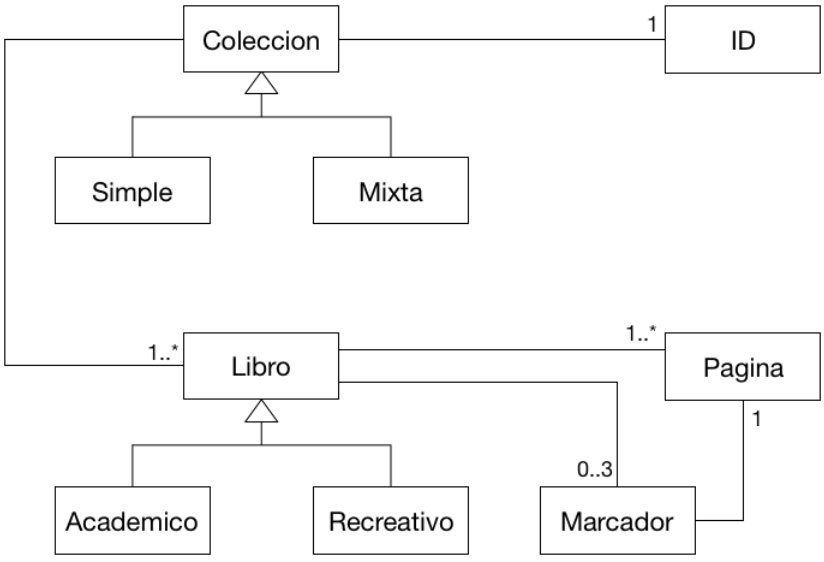
Utilice el analizador para validar si la definición del predicado `reemplazarPeriferico` es correcta, considerando el modelo resultante del inciso *c*) y la descripción brindada para el predicado.
Deberá dejarse registro de cada comando utilizado en la validación, teniendo en cuenta las siguientes consideraciones:

- Para aquellos comandos que no generen instancias, deberán explicarse los motivos por los cuales no lo hacen.
- Para aquellos comandos que generen instancias en las que se observan irregularidades, deberá dejarse registro de dicha instancia (por ejemplo, mediante una captura de pantalla), describiendo cuáles son las irregularidades o problemas allí observados e indicando cuál fue el comando utilizado para generar dicha instancia; en caso de ser necesario, deberá indicarse también el número de instancia generada por dicho comando (por ejemplo, si se trata de la primera instancia, de la segunda instancia, etc.).

(f) Realice los cambios necesarios en el predicado `reemplazarPeriferico` y/o en el modelo resultante de manera tal que la nueva definición del predicado sea correcta.

Una vez realizados los cambios necesarios, valide el predicado resultante considerando al menos 2 casos de éxito y 2 casos de no éxito.

4. 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. Asuma que el mismo es correcto y fue validado en un contexto de modelado estático:

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

sig ID { }

sig Simple, Mixta extends Coleccion { }

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

sig Marcador { pag: Pagina }

sig Academico, Recreativo in Libro { }

sig Pagina { }

fact {no (Coleccion - Simple - Mixta)}

fact { disj[Academico, Recreativo] }

fact {no disj c1, c2: Coleccion | c1.ident = c2.ident}}

fact {all l: Libro | #l.marcadores < 4}

fact {all m: Marcador, l: Libro | (m in l.marcadores) implies (m.pag in l.paginas)}

fact {all s: Simple | no l1, l2: s.librosCol | librosDistintaCategoria[l1, l2]}

pred librosDistintaCategoria[l1, l2: Libro]{
    (l1 in Academico and l2 in Recreativo) or
    (l1 in Academico and l2 in (Libro-Academico-Recreativo)) or
    (l1 in Recreativo and l2 in (Libro-Academico-Recreativo))
}
```

(b) Defina predicados y/o funciones para modelar el siguiente comportamiento. En caso de realizar modificaciones sobre el modelo brindado, justifique los cambios:

- Agregar un libro a una colección de la biblioteca. Si se lo quiere agregar a una colección mixta, la colección resultante (luego de agregarlo) no debe poseer más de dos categorías de libros, considerándose también a "no categorizado" como una categoría.
- Marcar una página de un libro. Como requisito general, la página que sea desea marcar no debe estar referenciada por otro marcador del libro. Además, si el libro no se encuentra al límite de cantidad de marcadores permitidos, simplemente se añade nuevo marcador que referencie a la página deseada. Por otra parte, si el libro ya posee su máximo de marcadores, se reemplaza uno de los marcadores antiguos por un nuevo marcador que referencie a la página deseada.
- Obtener el conjunto de páginas que se encuentran marcadas en libros recreativos pertenecientes a colecciones mixtas de la biblioteca.

Especifique comandos en Alloy para verificar el correcto funcionamiento (considerando todos los casos de éxito y al menos un caso de no éxito) de los predicados y/o funciones definidos en el inciso anterior.