CITS5501 Software Testing and Quality Assurance
Semester 1, 2020
Workshop week 11 – Formal specifications

1 Alloy sigs and properties

How would you translate the following into Alloy syntax? All of these can be done by declaring *sigs* and *properties*.

a. There exist such things as chessboards.
b. There is one, and only one, tortoise in the world.
c. There exists at least one policeman.
d. Files have exactly one parent directory.
e. Directories have at most one parent directory.
f. Configuration files have at least one section.

2 Alloy facts

Recall that in Alloy, *facts* are additional constraints about the world, that aren't expressed in the sigs, and can be used to "tighten" the meaning of your model. (Some constraints could be expressed either in the sig, or as a fact.)

a. Assume we have a sig `LectureTheatre{}` and a sig `Venue{}`.
   Give a fact which constrains every lecture theatre to also be a venue. (Note that we could do this using "extends" in the sig, also. But sometimes it's more convenient to express things using facts, or the constraint we want is too complicated for just "extends".)

b. Assume we have the sigs `Carnivore{}`, `Omnivore{}`, `Herbivore{}`. Write a fact constraining `Omnivore` to be the intersection of `Carnivore` and `Herbivore`.

3 Facts with quantifiers

The facts in the previous section constrain sets (e.g. the set of lecture theatres, or the set of omnivores).

We can also write constraints that apply to every entity *in* some set.

For example, suppose we have the following sigs:

```
sig Activity {}
sig Person { hobbies: set Activity }
sig ComputerScientist extends Person {}
```

We can apply the following constraint: "Computer scientists have no hobbies:"

```
fact {
  all cs : ComputerScientist | #(cs.hobbies) = 0
}
```

In other words: people can have zero or more hobbies; but for all people who are computer scientists, if we look at their hobbies, the cardinality will be 0.

Try extending this model to say:

a. Economists are also people.
b. Economists have at most one hobby.
c. Students are people.
d. Students have at least one hobby.
e. Bots are not people.

4 More quantifiers

Try writing Alloy specifications for each of the following scenarios:

a. Directories can contain files. Both files and directories have a *creation date*. The creation date of a directory is earlier than the creation date of any file contained in the directory.
b. Students can enrol in classes. Each class has a name, and can be either "completed" or "incomplete". All students enrolled in the "programming language theory" class must have completed the "discrete maths" class.

Further exercises

Model the following systems:

1. An *alarm clock* has two sorts of time it can keep track of: the *current* time, and an *alarm* time.

   It *always* has a current time, and *may* have an alarm time.

   State any assumptions you make.

2. A person can have up to two parents (who are also people). No person is their own parent. There exists exactly one person who has no parents.

3. A *contact list* may contains multiple *entries*. Each entry must have a "personName", and may have one or more telephone, street address, or emails.