CITS5501 Software Testing and Quality Assurance
Semester 1, 2020
Week 10 workshop – Formal methods

Exercise 1

Would you use formal methods for any of the following systems? If so, which systems, and why?

a. The next version of *Confectionery Crush Story*, a web– and mobile-app–based puzzle video game your company develops. The game is available for both Android and iOS mobile devices, and the previous version grossed over $US 1 billion in revenue.

b. *Exemplarex*, software produced for Windows and MacOS operating systems and licensed to educational institutions. The software semi-automatically invigilates exams set by the institutions: machine-learning techniques are used to analyse audio and video of exam candidates to identify possible academic misconduct.

c. The online banking website provided by a major Australian bank, EastPac. Over 5 million customers use the website to perform banking transactions on personal or business bank accounts.

d. A radiation therapy system used to treat cancer patients. The system has two principal components:

   - A radiation therapy machine that delivers controlled doses of radiation to tumour sites, controlled by an embedded software system.
   - A treatment database that includes details of the treatment given to each patient.

Exercise 2

Of the formal method techniques we have considered in class, which might be applied to the following systems?

a. Data-analysis software which analyses the results of high-energy physics experiments conducted in particle colliders. Based on data obtained from sensors in the collider, the software attempts to identify *jets* – large numbers of particles all flying in roughly the same direction – using data mining techniques.

   (See here for more details on jets.)

b. A new high-assurance operating system designed to operate voting machines.

c. A database system, which we require should never go into deadlock.

Exercise 3

The following Dafny code is intended to find the position of the largest element of an array. It is only guaranteed to produce a result if the array is *non-empty*, however.

```
method FindMax(arr: array<int>) returns (r: int)
{
  var max_val : int := arr[0];
  var max_idx : int := 0;

  var i : int       := 1;

  while (i < arr.Length)
  {
    if arr[i] > max_val
      {
        max_idx := i;
        max_val := arr[i];
      }
    i := i + 1;
  }
  return max_idx;
}
```

At what points in the code might we insert the following, and what Dafny keywords would be used?

- preconditions
- postconditions
- loop invariants
- assertions

See if you can state what the preconditions and postconditions are (in English is fine).

Challenge exercise: Try verifying the above code using the online Dafny verifier at https://rise4fun.com/Dafny/tutorial. This will require reading the tutorial, however, in order to learn how to use the `forall` keyword, which we have not covered.