

# Exercise 2: Due January 30

## 1. Cartesian products of Intervals and Odd/Even

- a. Define the domain
- b. Show a program and correct property which cannot be proven by the Odd/Even analysis alone and the Interval analysis alone but can be proved by their product
- c. Show an example which requires semantic reductions in order to prove the correctness of the property.
- d. Show an example which requires the use of Reduced Cardinal Power

## 2. CEGAR

- a Calculate the interpolant of " $b \ \&\& \ (!b|c)$ " and " $!c$ " over the joint vocabulary " $c$ "
- b Give an example program and a safety property on which BLAST will fail to prove

Download the TVLA tool and solve **one** of the following projects

### **Project 1: Proving Partial Correctness of a Simple Mark and Sweep Garbage Collection**

1. Remove the focus operations in `stat_set.tvp` and study the resulting analysis
2. What are the difficulties in extending the analysis to handle Garbage Collection Algorithms like Copy Garbage Collection in which the garbage collector can mutate the heap
3. (Bonus) Add actions for showing that the Mark phase must eventually terminate. One way to show that is by showing that the set of nodes reachable from the pointer variable  $x$  (used in the while loop condition in `mark.tvp`) decreases in every loop iteration

### **Project 2: Proving Partial Correctness of Sorting Algorithm**

1. Remove the focus operations in `actionsd.tvp` and study the resulting analysis (

2. Write an improved version of bubble sort in C called smart-bubble-sort which stops once the list is sorted and doesn't compare elements which are already in place (using linked lists and pointers). Then, convert it manually into tvp and run it. Study the results of the analysis
3. (Bonus) Add actions for showing that the loops in insertion sort and bubble sort must eventually terminate. One way to show that is by showing that the set of nodes reachable from the temporary variable  $x$  decreases at every loop iteration