272 – Homework Assignment 3

Winter 2024

Due: Friday, March 15

Do not discuss the problems with anyone other than the instructor.

1. Given the following pieces of code, draw the control flow graphs and give minimal test sets for maximizing the following coverage criteria: statement coverage, branch coverage and path coverage. If there are statements, branches or paths that are not feasible to execute, indicate them. The inputs can take any integer value. Label the basic blocks in your control flow graphs. For each test case show the set of statements, branches or paths it covers using the basic block labels (for example, for the test set for path coverage, show the paths covered for each test case). For path coverage loops should be executed zero and one time.

(a)

```
int test1(int x, int y) {
  int z, w, result;
  if (x > y)
     z = 1;
  else
     z = 0;
  if (x > y + 10)
     w = 10;
  else
     w = 0;
 result = z + w;
 return result;
}
```

(b)

```
int test2(int x, int y) {
  int i, total, out;
  total = 0;
  for (i = 0; i < x; i++) {
    total = total + i;
  }
  out = total;
  if (total < y)
    out = -1;
  return out;
}
```

2.

(a) Consider the following code:

```
int test3(int x, int y) {
  int z = 0;
  if (x > y)
    z = x;
  else
    z = y;
  if (z < 0)
    return -1;
  else
    return z;
}
```

Show the path conditions and the symbolic states generated by classic symbolic execution (without concrete values) starting from the symbolic state $x = m, y = n$.

(b) Consider the following code:

```
void test4(int x, int y) {
    int z = 3 * y;
    if (x == 17) {
        if (x < z + 20) {
           x = y;
        }
    }
}
```

Show the path conditions, symbolic states and the concrete values generated by concolic execution. Assume that the initial concrete values for x and y are 9 and 2, and initial symbolic values are m and n, respectively.

3. For all the path conditions generated in Problem 2.(a) and 2.(b), write the corresponding SMT-LIB formulas, and generate a satisfying model using Z3. Show the SMT formula you wrote and the satisfying model generated by Z3.

You can use the online version of Z3 available here:
`http://compsys-tools.ens-lyon.fr/z3/`

4. Assume that a program crashes with the input string "`(abcde)f`". Also assume that the program crashes with any input string that contains two matching parentheses and it does not crash with any other input. Show an execution of the delta debugging algorithm in this case (show the sequence of inputs that delta debugging algorithm will generate and the classification of each input). Assume that the minimal change is adding one character to the input string, and start with an initial partition where each set adds half of the failure inducing input string given above.