

Roll No: \_\_\_\_\_

**CS6843 Program Analysis at IIT Madras**  
EndSem June 24, 2015

Total Marks: 34

Duration: 90 min

1. [1 mark] Our director Bhaskar Ramamurthi was earlier the Dean of \_\_\_\_\_?
2. (a) [5 marks] For the following set of statements, compute points-to information using Andersen's analysis. Write only the final points-to information.  
a=&b, c=\*d, e=\*f, \*g=d, g=&c, \*e =c,  
f=&h, d=&a, \*c=e, \*i=f, i=&e, h=&j

(b) [5 marks] For the above set of statements, if points-to analysis is solved using a constraint graph based formulation, list all cycles encountered during the analysis. Do not write anything else.

3. [7 marks] Consider an analysis that tracks signs of various integer variables and stores one bit for each variable. If  $\text{bit}(v) == 1$  at a program point, then the variable  $v$  holds a negative value at that point. Otherwise, the variable is zero or positive. Compute the values of these bits for all variables in the following program after each step. Initial values for all bits are zeros. A value of zero indicates a more approximate solution for each bit.

x = y + z;      {bit(x) =      }

w = z - x;      {bit(w) =      }

z = x \* w;      {bit(z) =      }

y = -1;          {bit(y) =      }

++y;            {bit(y) =      }

y = y \* x;      {bit(y) =      }

--y;            {bit(y) =      }

4. [5 marks] For the following program, compute a backward slice for criteria  $\langle 21, m \rangle$ . Simply circle the line numbers. Do not write how you got the slice.

```
1. char c;
2. void main() {
3.     int n = 0;
4.     int m = 1;
5.     int p = 2;
6.     int q = 3;
7.     printf("Do you want to continue? ");
8.     c = getinput();
9.     p -= 4;
10.    while (c == 'y') {
11.        n = getinput();
12.        if (n > 5) {
13.            ++m;
14.            q -= m;
15.        } else {
16.            m -= p;
17.        }
18.        printf("Do you want to continue? ");
19.        c = getinput();
20.    }
21.    printf("m = %d\n", m);
22. }
```

5. [6 marks] Given an array access in a C program with negative index (e.g.  $a[-5]$ ), develop an analysis to check if the access is valid. This can happen when an address of an element is passed to a function, such as  $f(\&a[10])$ . The program contains only integer constants, integer variables, their pointers and their arrays, assignments, if-else, for, and function calls. Describe your analysis using a non-trivial example. In your answer, make sure you describe the analysis, and not only the idea.
6. [5 marks] Design an analysis to find out null pointer dereferences (e.g.,  $*p$  where  $p$  may be null) in a program. Do not worry about the type of the pointer. Ignore context-sensitivity. Describe your analysis using a non-trivial example. Explain limitations of your approach.