Scalable Context-Sensitive Flow Analysis Assignment

Given below is a C program and the type instantiation constraints generated using the rules in figure 3 of the paper.

Program:

```
1  main(){
2          int a,b,c,d,e;
3          int *p,*q,*f;
4          int **x, **y;
5          p = &a;
6          q = &b;
7          x = &q;
8          y = &p;
9          c = foo(x);
10         d = bar(p);
11         e = foo(y);
12         f = *x;
13 }
14 int foo(int **z){
15         return **z;
16 }
17 int bar(int *w){
18         return *w;
19 }
```

Constraints :

$\{\alpha_{foo} = ptr^{l1}(ptr^{l2}(\alpha_z)) \rightarrow \alpha_{ret(foo)},\ \ \alpha_{ret(foo)} = \alpha_z,$
$\alpha_{bar} = ptr^{l3}(\alpha_w) \rightarrow \alpha_{ret(bar)},\ \ \alpha_{ret(bar)} = \alpha_w,$
$\alpha_p = ptr^{la}(\alpha_a),\ \ \alpha_q = ptr^{lb}(\alpha_b),\ \ \alpha_x = ptr^{lq}(\alpha_q),\ \ \alpha_y = ptr^{lp}(\alpha_p),$
$\alpha_{foo} \leq_{+}^{9} \alpha_x \rightarrow^{l9} \alpha_c,\ \ \alpha_{bar} \leq_{+}^{10} \alpha_p \rightarrow^{l10} \alpha_d,$
$\alpha_{foo} \leq_{+}^{11} \alpha_y \rightarrow^{l11} \alpha_e,\ \ \alpha_x = ptr^{l5}(\alpha_\gamma),\ \ \alpha_f = \alpha_\gamma\}$

1. Apply the semi-unification algorithm, given in figure 4 in the paper, on the constraints to generate the *Type Instantiation Graph.* Sample TIGs are given in figures 7 and 8 in the paper.

2. Construct the flow graph for the program using the type instantiation graph, as described in section 4 of the paper. Sample flow graphs may also be seen in figures 7 and 8.

3. Answer the following queries using the flow graph:

   (a) What values flow into the variables c, d, e, f?

(b) Give the final points-to information of the program, i.e. which variable points to which other variables. The answer should be given as the points-to set corresponding to each variable.