SPA2023 期末

选择

1. (Sound/Complete) 的分析需要 (Under/Over Approximate)，得到的结果可能有 (False Negative/Positive)

   括号里各选一种进行配对

2. （多选）下列是格的是

   A. $\langle \mathbb{N}, \leq \rangle$

   B. $\langle \{1, 2, 3, 12, 18, 36\}, | \rangle$，其中 $|$ 为整除关系

   C. S是有限集，$\langle \mathcal{P}(S), \subseteq \rangle$

   D. $\langle \mathbb{N} \times \mathbb{N}, R \rangle$，其中$((a, b), (c, d)) \in R \Leftrightarrow a \leq c \wedge b \leq d$

3. 用格建模迭代算法，格高度为 H，CFG 有 N 个节点，E 条边，迭代求解器最多迭代次数为

   A. H+N　B. H×N　C. H+E　D. H×E

4. （多选）以下哪些分析可以使用 IFDS?

   A. Reaching Definition B. Constant Prop C. Pointer Analysis

5. 以下哪个选项的精度不低于其他选项

   A. 1-object, without heap context

   B. 2-object, with 1-heap

   C. 2-type, with 1-heap

   D. 1-object, with 1-heap

填空

1. 使用 type sensitive 指针分析下列程序，分析到 `y()` 函数内时的 context 为?

```
class X {
  void main() {
    Y a = new Y();
    a.y();
  }
}

class Y {
  void y() {}
}
```

2. SQL 注入破坏了哪种安全性（保密性/完整性）？
3. IFDS 的转移函数满足（）性
4. 列举两个 java 中难以分析的特性
5. CHA 分析下列代码，`b.foo()` 调用目标有?

```
class A { void foo() {} }
class B extends A {}
class C extends B { void foo() {} }
class D extends C { void foo() {} }

void main(){
  B b = new B();
  b.foo();
}
```

6. 对下面的代码进行流敏感、上下文不敏感的过程间常量传播，第 5 行的 OUT 为（），第 10 行的 OUT 为（）；如果进行过程内常量传播，第 5 行的 OUT 中 `c` = ()

```
static void main() {
  int a, b, c;
  a = 7;
  b = 9;
  c = foo(a, b);
  b = 8;
  c = foo(a, b);
}
static int foo(int x, int y) {
  int z = x + y;
  return z;
}
```

简答

1. ICFG 是哪些边+哪些边？Call-to-return edge 的作用是？
2. 指针分析的 key factors 对应的表填空
3. 填写课上说的Dataflow Analysis对比表（只挖了几个空）

问答

1. 手跑 Reaching definition（有 5 个 BB，只用写 OUT 的迭代结果，和 PPT 上例子的难度差不多）
2. 划分 BB

```
xxx
xxx
if xxx goto 8
xxx
xxx
xxx
goto 3
if xxx goto 10
xxx
return
```

3. 分别使用 CI 和 2-callsite, with 1-heap 分析下列程序（填表，有手就行）并画出 CI 的 PFG，以此为例简要说明为何上下文敏感的分析更加精确。

```
void main(){
  Number n1 = new Number();
  Number n2 = new Number();
```

```
  Wrapper w1 = CreateWrapper(n1);
  Wrapper w2 = CreateWrapper(n2);
  Number n3 = getNumber(w1);
  Number n4 = getNumber(w2);
}

Wrapper CreateWrapper(Number p){
  Wrapper w = new Wrappr();
  w.set(p)
  return w;
}

Number getNumber(Wrapper i){
  Number out = i.f;
  return out;
}

Class Wrapper(){
  Number f;

  void set(Number in){
    this.f = in;
  }
}
```

拓展

1. 使用 Datalog 编写 May Available Expression（和课上讲的Available Expression基本一致，除了使用并的方式合并前驱节点的结果）

   EDB包括：`Successor(s, succ)`、`Compute(s, x, op, y)`、`Def(s, v)`

   需要计算的IDB包括：`Gen(s, x, op, y)`、`Kill(s, x, op, y)`、`In(s, x, op, y)`、`Out(s, x, op, y)`

   题中已经给出`Gen(s, x, op, y) <- Compute(s, x, op, y)`

2. 使用类似 Constant Prop 的思想实现变量区间分析（几个填空，很简单）