

Program Analysis (CSE-503)

Assignment 2

Date: 24-Sept-19

User inputs are external dependencies that can be exploited to change the program behaviour. Taint analysis is a popular method to find out which sinks are affected by these inputs. It can locate the variables that can be controlled by the user, tracing the propagation of the taint, assuming user input as tainted. In this assignment, you are required to build your own **intraprocedural taint variable analysis** that traverses and analyzes your program in a backward direction to find out which variables are affecting the sinks. Consider return and print statements as sinks here.

Example:

1.

```
int bar1(int x) {  
    int product, a;  
    a = 10;  
    product = x * a;  
    return product;  
}
```

Output:

In: {}

Unit: return product

Out :{product}

In: {product}

Unit: product = x * a

Out :{product, x, a}

In: {product, x, a}

Unit: a = 10

Out :{product, x}

In: {product, x}

Unit: x := @parameter0: int

Out :{product, x}

//Sinks depend on parameter (source):

x

2.

```
static int foo()  
{  
    Scanner sc = new Scanner(System.in);
```

```

    int z;
    int a = sc.nextInt();
    int b = sc.nextInt();
    int c = 10;
    z = a+b+c;
    return z;
}

```

Output

```

In: {}
Unit: return z
Out :{z}
In: {z}
Unit: z = $i0 + c
Out :{z, $i0, c}
In: {z, $i0, c}
Unit: $i0 = a + b
Out :{z, $i0, c, a, b}
In: {z, $i0, c, a, b}
Unit: c = 10
Out :{z, $i0, b, a}
In: {z, $i0, b, a}
Unit: b = virtualinvoke sc.<java.util.Scanner: int nextInt()>()
Out :{z, $i0, b, a}
In: {z, $i0, b, a}
Unit: a = virtualinvoke sc.<java.util.Scanner: int nextInt()>()
Out :{z, $i0, b, a}
In: {z, $i0, b, a}
Unit: sc = $r0
Out :{z, $i0, b, a}
In: {z, $i0, b, a}
Unit: specialinvoke $r0.<java.util.Scanner: void <init>(java.io.InputStream)>($r1)
Out :{z, $i0, b, a}
In: {z, $i0, b, a}
Unit: $r1 = <java.lang.System: java.io.InputStream in>
Out :{z, $i0, b, a}
In: {z, $i0, b, a}
Unit: $r0 = new java.util.Scanner
Out :{z, $i0, b, a}

```

//Depends on source (inputs)

a, b