Context Sensitive(CoS) SSA for Interprocedural Program Analysis and Optimisation

Supriya Bhide[1], Sathwika Reddy[1], Arpana Prajapati[1]
Pritam Gharat[2], Uday Khedker[1], Alan Mycroft[3]
[1]IIT Bombay,[2]Microsoft Research India,[3]University of Cambridge

1 What is CoS-SSA

- Works at **Interprocedural** level
- Gives **flow and context sensitivity** for free
- Enables sparse interprocedural analyses and optimisations
- Handles **global variables and pointers** context sensitively
- Subsumes classical SSA as a special case

2 How Do We Obtain It

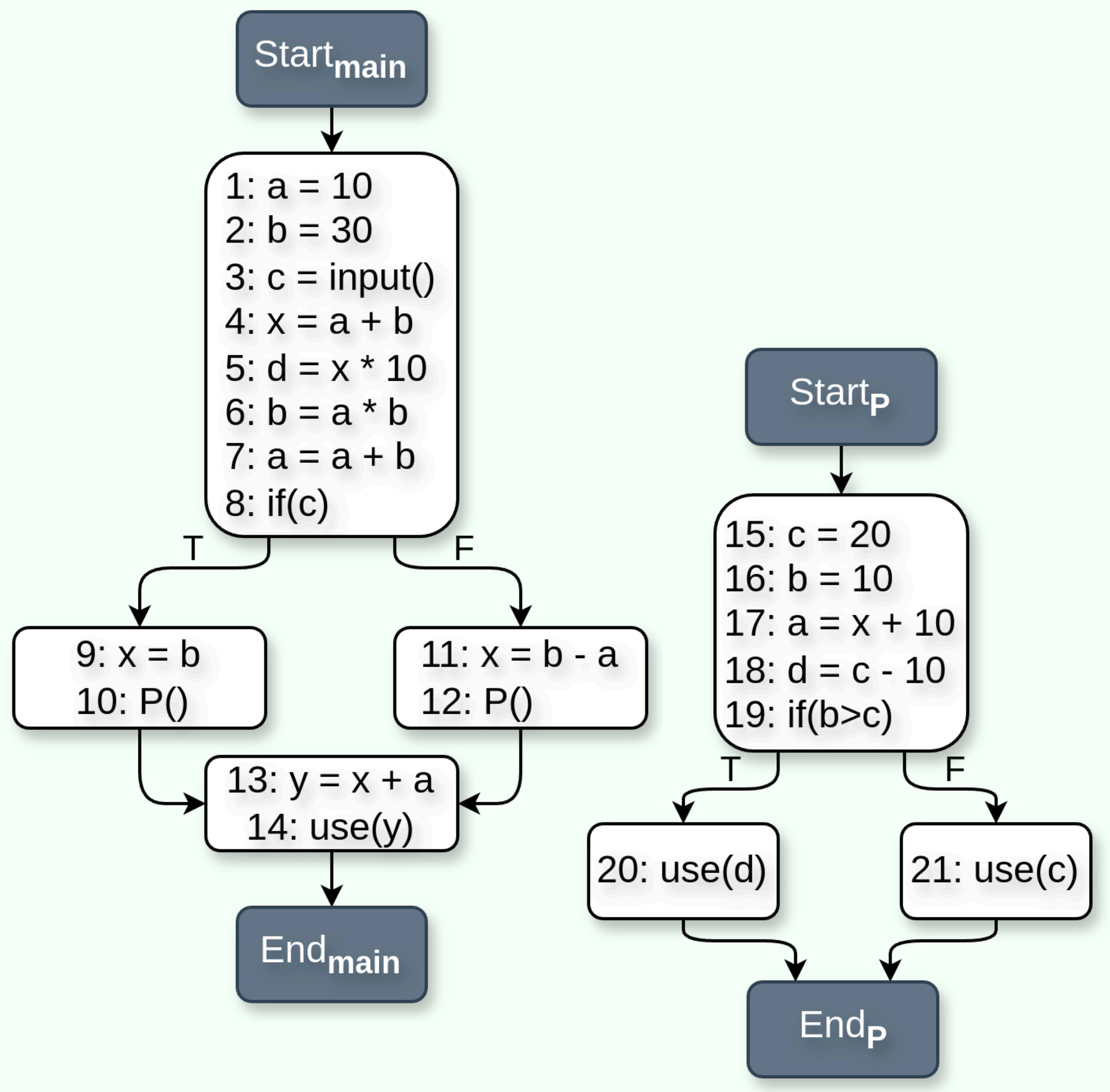
We obtain CoS-SSA by constructing Data Dependence Graph (DDG) and mutating definitions to make them context-sensitive

3 Source Code

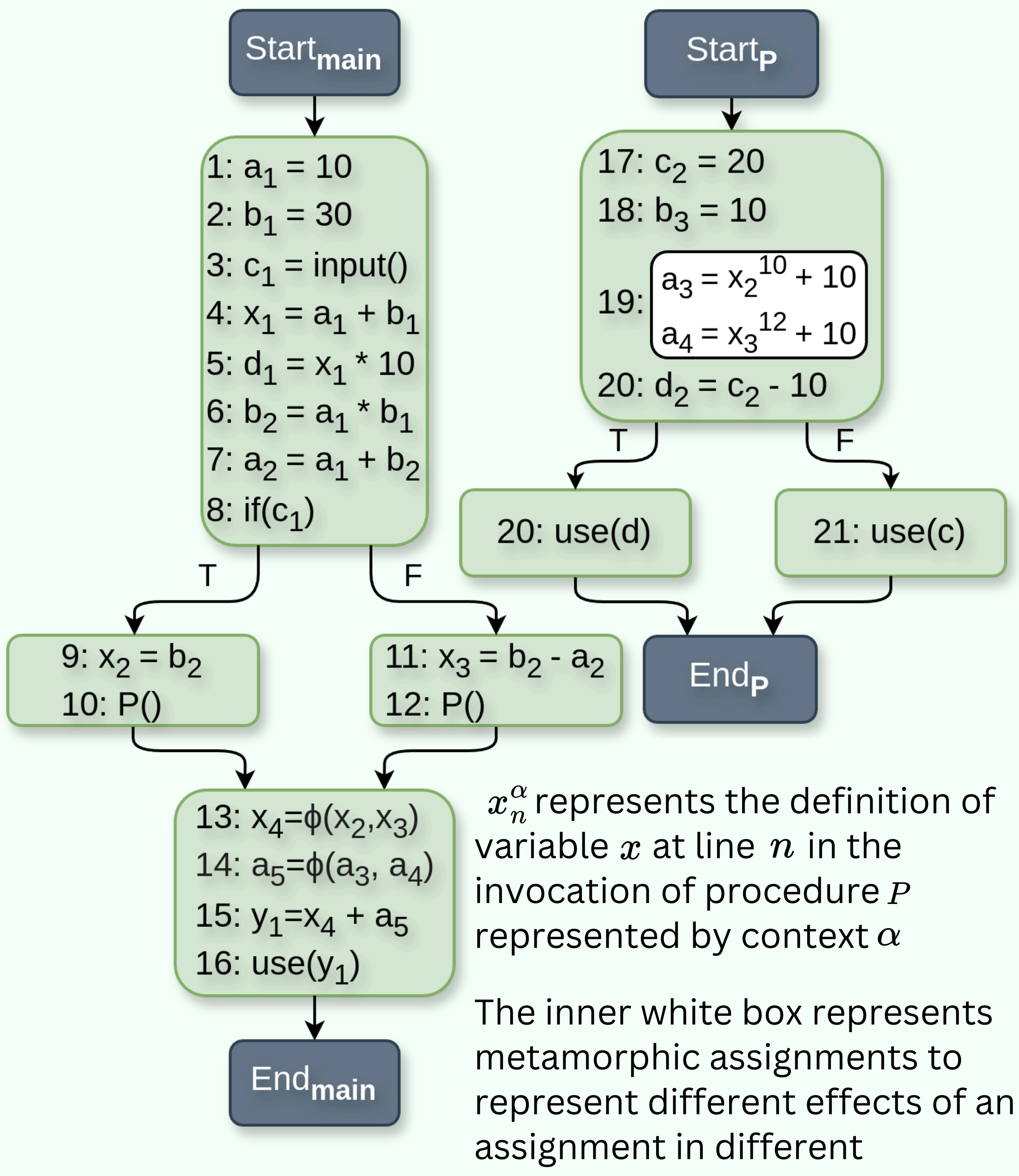
```
int  a,  b,  c,  d,  x,y;

void main()
{
     a  =  10;
     b  =  30;
     c  =  user_input();

     x  =  a  +  b;
     d  =  x  *  10;
     b  =  a  *  b;
     a  =  a  +  b;

     if(c){
            x=b;
            P();
          }
     else{
            x  =  b  -  a;
            P();
         }

     y  =  x  +  a;
     use(y);
}
```

```
void P()
{
    c = 20;
    b = 10;
    a = x + 10;
    d = c - 10;

    if(b>c)
        use(d);
    else
        use(c);
}
```

4 CFG of Our Example



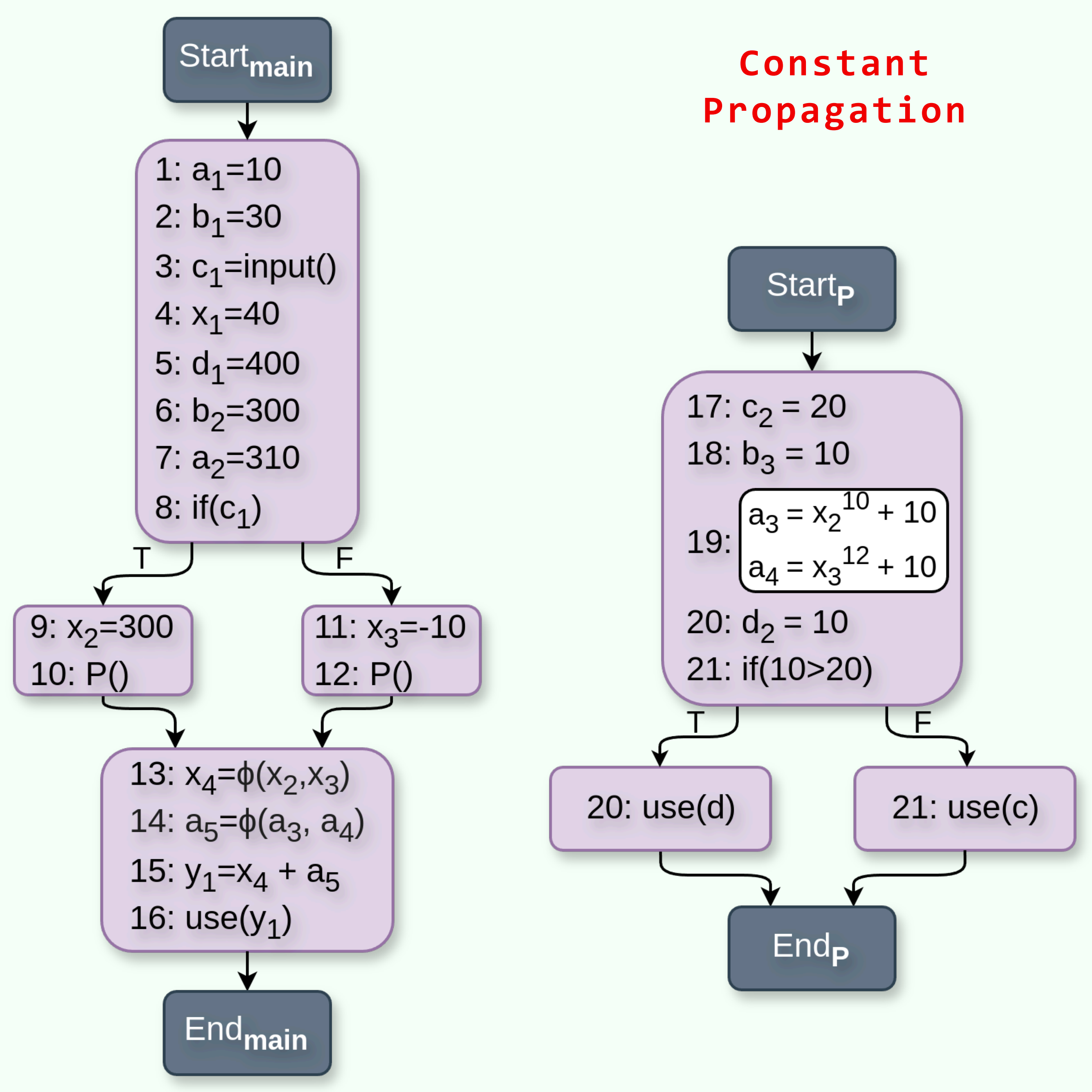
5 CoS-SSA



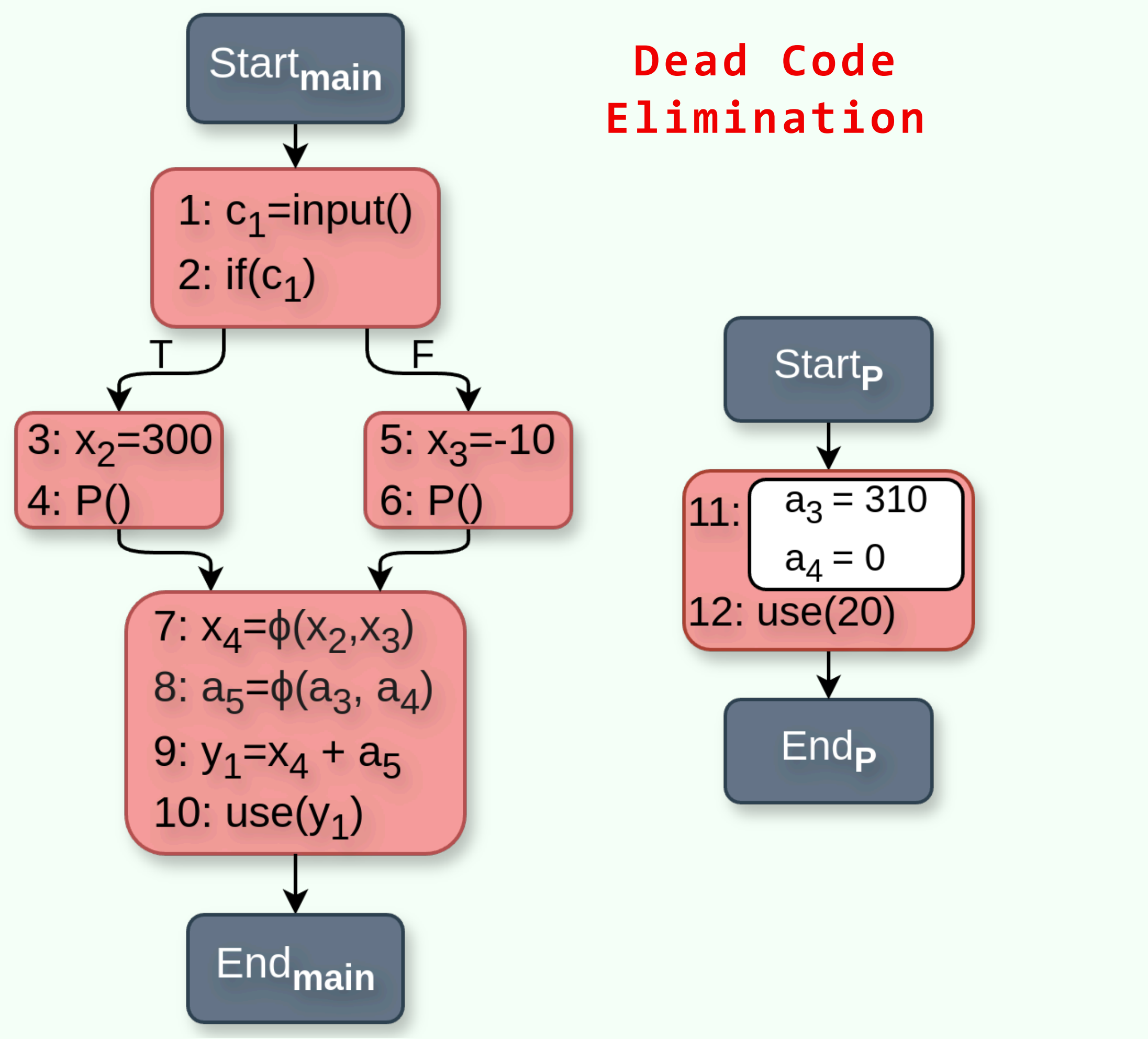
x_n^α represents the definition of variable x at line n in the invocation of procedure P represented by context α

The inner white box represents metamorphic assignments to represent different effects of an assignment in different invocations of the procedure P

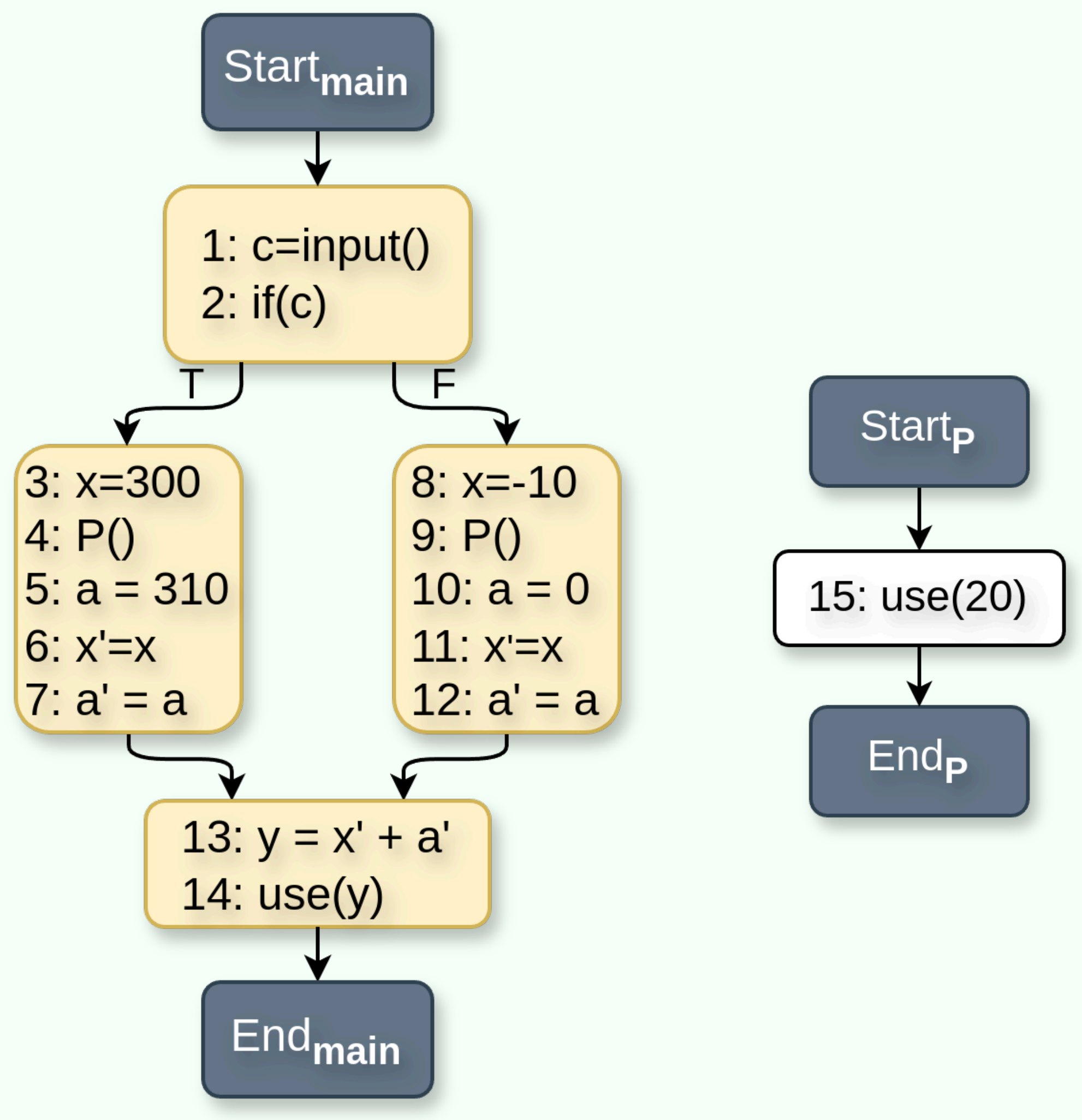
6 Optimised CoS-SSA (1)



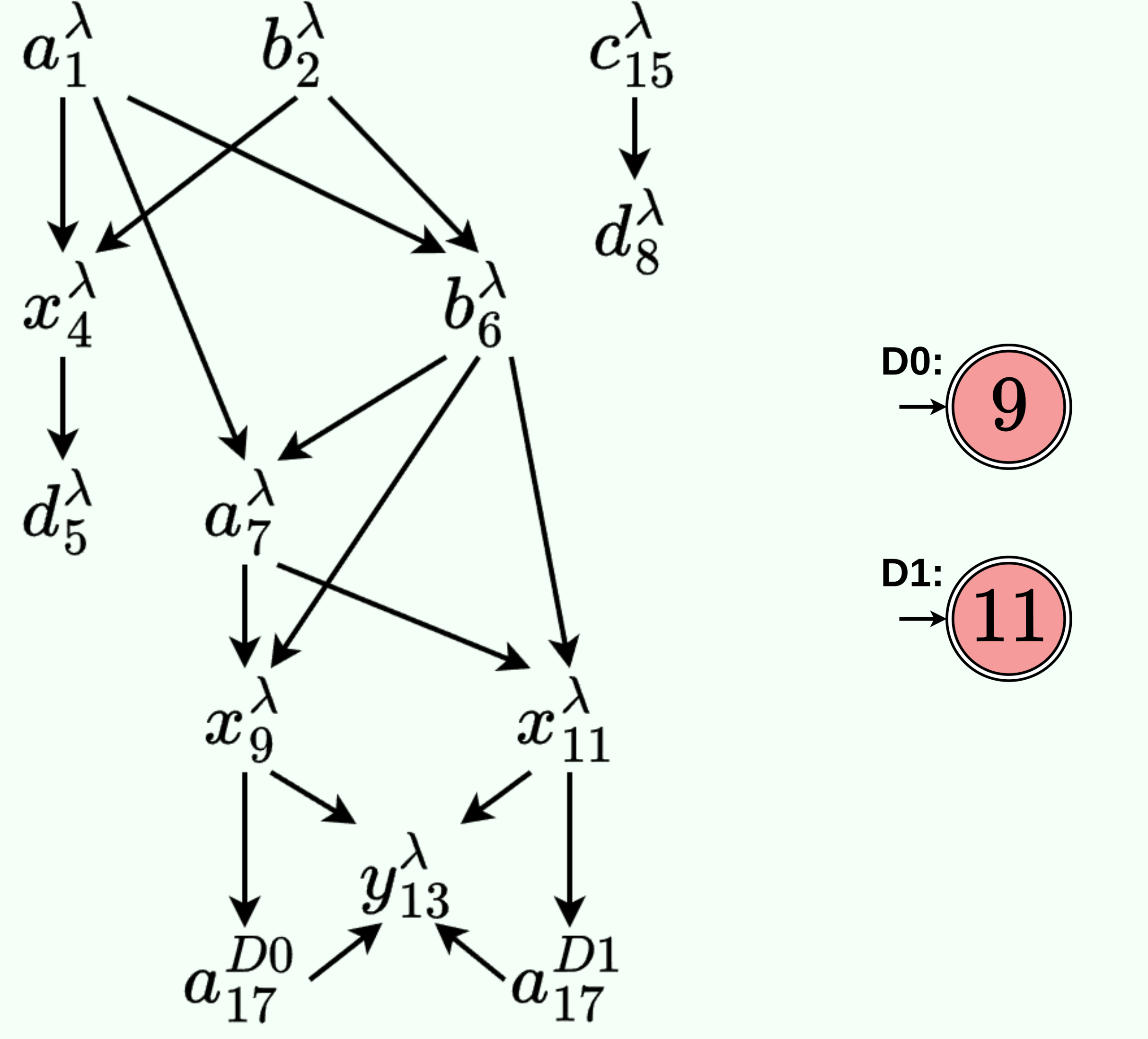
7 Optimised CoS-SSA (2)



8 Optimised CFG



9 Data Dependence Graph



10 Mutation

- We compute the Data Dependence Graph (DDG) using a bottom-up traversal over the callgraph
- We inline the DDG of callee procedures at the respective call sites in the caller procedures
- While doing so, if any definition x_n^α in the callee depends on any definition in the caller we mutate x_n^α to distinguish the dependence of x_n in different invocations of the callee
- Mutation is achieved by updating the context α to include the call site where the inlining occurs.

PLATO Programming Languages Analysis Translation Optimization, CSE IIT Bombay