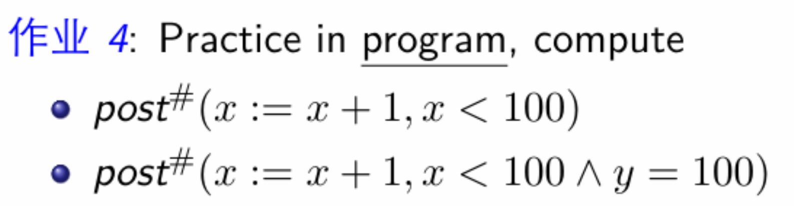
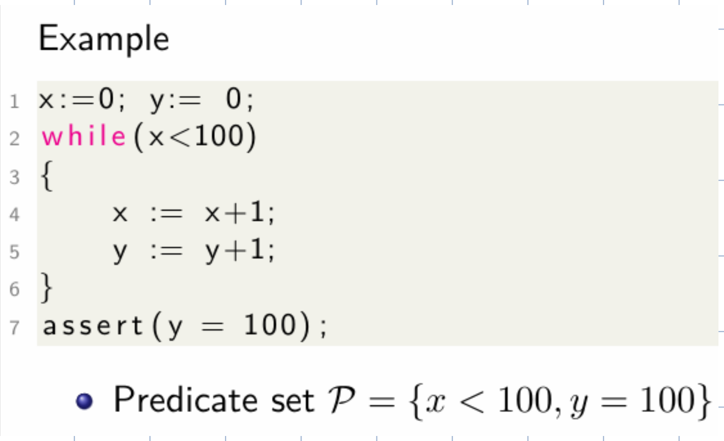
4.



作业 4: Practice in program, compute

- post$^{\#}(x := x + 1, x < 100)$
- post$^{\#}(x := x + 1, x < 100 \wedge y = 100)$



Example

```
x:=0;  y:=  0;
while(x<100)
{
      x  :=  x+1;
      y  :=  y+1;
}
assert(y  =  100);
```

- Predicate set $\mathcal{P} = \{x < 100, y = 100\}$

① $sp(x:=x+1\ ,\ x<100) \Leftrightarrow \exists x_0.\ x_0<100 \wedge x=x_0+1$

可知 $x<101 \nRightarrow x<100$

$x<101 \nRightarrow x \geqslant 100$ 故 $b_1=*$

对于 p_2 无约束，故 $b_2=*$

故 $post\#(x:=x+1\ ,\ x<100)=[*,*]$

② $sp(x:=x+1, x<100 \wedge y=100)$

$\Leftrightarrow \exists x_0, y_0.\ x_0<100 \wedge y_0=100 \wedge x=x_0+1 \wedge y=100$

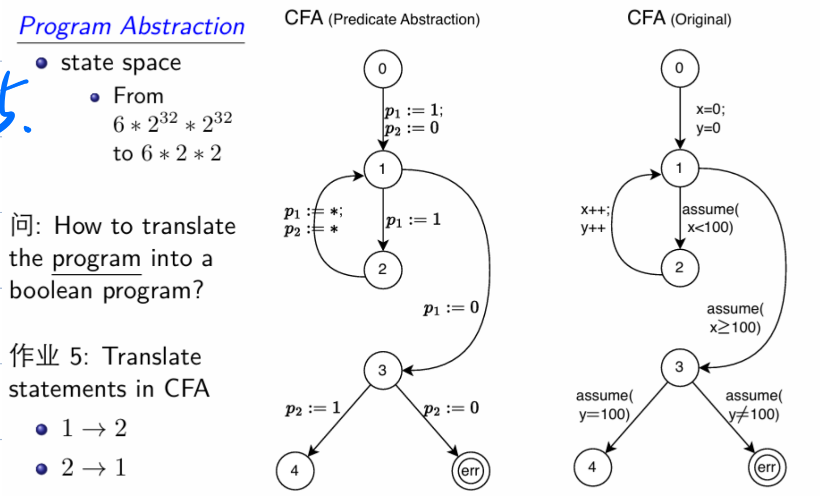
$\Leftrightarrow x<101 \wedge y=100$

同①理 $b_1=*$

$b_2=1$

故 $post\#(x:=x+1, x<100 \wedge y=100)=[*,1]$

5.



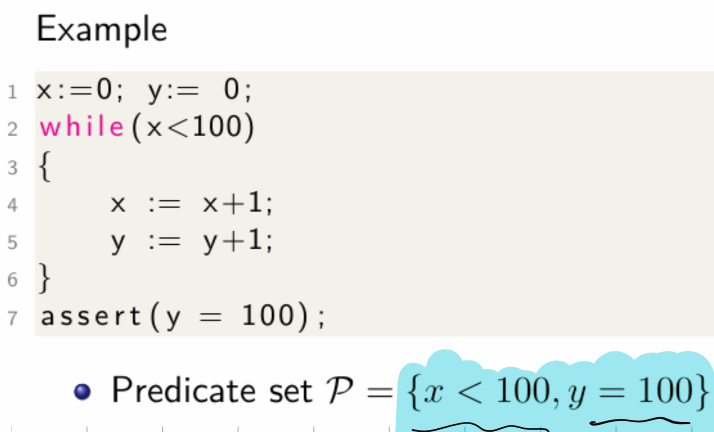
Program Abstraction

- state space
  - From $6 * 2^{32} * 2^{32}$ to $6 * 2 * 2$

问: How to translate the program into a boolean program?

作业 5: Translate statements in CFA

- 1 → 2
- 2 → 1



Example

```
x:=0;  y:=  0;
while(x<100)
{
      x  :=  x+1;
      y  :=  y+1;
}
assert(y  =  100);
```

- Predicate set $\mathcal{P} = \{\underbrace{x < 100}_{p_1}, \underbrace{y = 100}_{p_2}\}$

① 1→2

S: assume (x < 100)

$wp(assume(x<100), x<100) \Leftrightarrow T$

$wp(assume(x<100), y=100) \Leftrightarrow y=100$, $b_2 \Rightarrow (y=100)$

$\neg b_2 \Rightarrow \neg(y=100)$

无需翻译

$b1 := true$

② 2→1

S: $x:=x+1 ; y:=y+1$

对 $x:=x+1$

$\neg b_1 \Rightarrow \neg(x<99)$

$wp(x:=x+1, x<100) \Leftrightarrow x<99$, $b_1 \nRightarrow (x<99)$

$wp(x:x+1, y=100) \Leftrightarrow y=100$, $b_2 \Rightarrow (y=100)$

$\neg b_2 \Rightarrow \neg(y=100)$

```
if (!b1)   b1 := false
else   b1 := *
```

无需翻译

对 $y := y+1$

$wp(y := y+1, x<100) \Leftrightarrow x<100$, $b_1 \Rightarrow (x<100)$

$\neg b_1 \Rightarrow \neg(x<100)$ 无需翻译

$wp(y := y+1, y=100) \Leftrightarrow y=99$, $b_2 \Rightarrow \neg(y=99)$

$\neg b_2 \not\Rightarrow (y=99)$

$\neg b_2 \not\Rightarrow \neg(y=99)$

```
if (b2)   b2 := false
else   b2 := *
```