The difference between

1. invariant
2. inductive invariant

E.g.

$\{x \geq 0 \wedge x \text{ is even}\}$

while $(x>0)$: $\longrightarrow$ $x \geq 0 \wedge x$ is even

```
x = x - 2
if x is odd
    x = -100
```

$\{x \geq 0\}$

$\{x \geq 0 \wedge \underbrace{x > 0}_{\text{loop condition}}\}$ loop body $\{x \geq 0\}$ ✗

$\wedge$ x is even

---

predicate abstraction

$\{pre\}$ stmt $\{true\}$

set of predicates $= \{x > 100,\ y = 0\}$

E.g. $\{x > 100 \wedge y = 0\}$

$x := x + 1$

$\{x > 100 \wedge y = 0\}$

$\{x > 100 \wedge y = 0\}$

$x := x - 1$

$\{\quad y = 0\}$

$\{x > 100 \wedge y = 0\}$

$y = 1$

$\{x > 100 \wedge y \neq 0\}$

$\{x > 100 \wedge y = 0\}$

$x = -10$

$\{x \leq 100 \wedge y = 0\}$

Cartesian predicate abstraction

Back to Horn Clauses

$\{x = 0 \wedge y = 0\}$

while $(n > 0)$

  $x := x + 1$

  $y := y + 1$

  $n := n - 1$

$\{x = 10 \Rightarrow y = 10\}$

$x = y$ is an inductive invariant

Convert to Horn clauses:

initiation:

$$x = 0 \wedge y = 0 \Longrightarrow I(x, y)$$

$x = y$

consecution:

$$I(x, y) \wedge x' = x + 1 \wedge y' = y + 1 \Longrightarrow I(x', y')$$

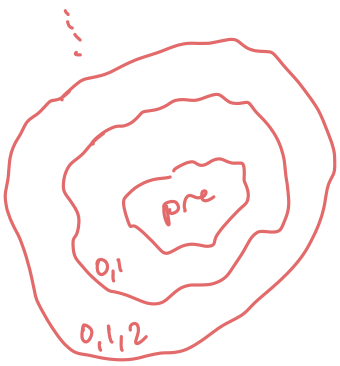
$x \stackrel{?}{=} y'$

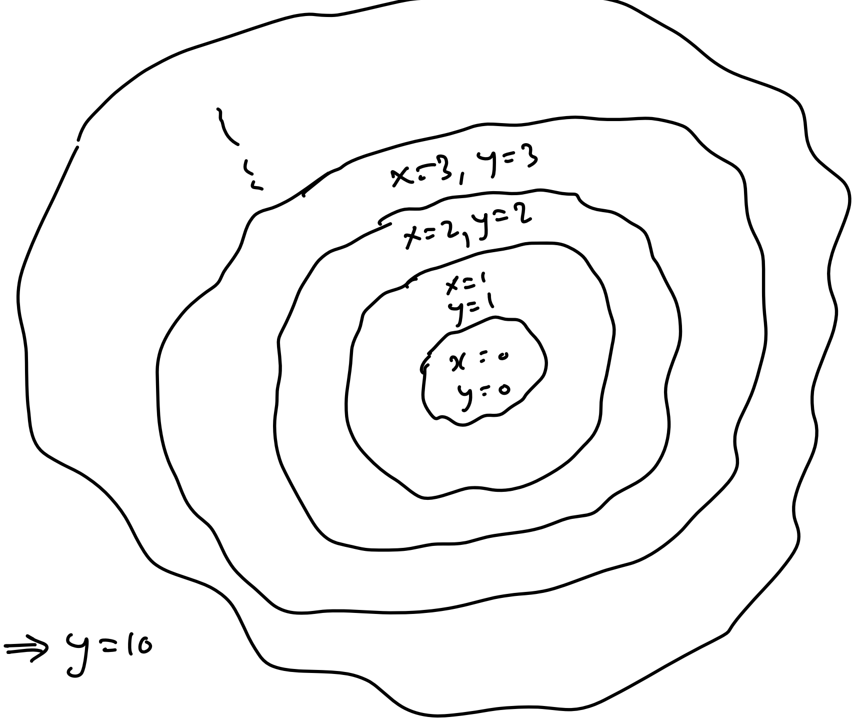
safety

$x = y$

$$I(x, y) \Longrightarrow (x = 10 \Rightarrow y = 10)$$

Visualize invariant





$X=10 \Rightarrow y=10$

FIXPOINT

$I(x,y) = pre$

while not fixpoint

$$I(x',y') = I(x',y') \vee \alpha\underbrace{\left(\exists x,y.\ I(x,y) \wedge x'=x+1 \wedge y'=y+1\right)}_{\text{take one step through the loop starting from } I(x,y)}$$

CHECK IF $I(x,y) \Longrightarrow$ POST CONDITION

E.g. $I = x=0 \wedge y=0$

$I = (x=0 \wedge y=0) \vee (x=1 \wedge y=1)$

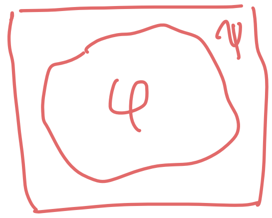
$I = \cdots \vee (x=2 \wedge y=2)$

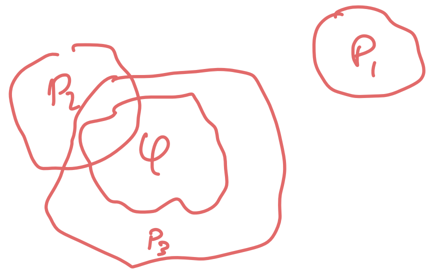
$\vdots$

PREDICATE ABS

predicates = $\{p_1, \dots, p_n\}$

given φ, what is the strongest formula ψ over predicates s.t. $\varphi \Rightarrow \psi$





$$\alpha(\varphi) = \bigwedge_{\substack{P_i \\ \varphi \Rightarrow P_i}} P_i \quad \wedge \bigwedge_{\substack{P_i \\ \varphi \Rightarrow \neg P_i}} \neg P_i$$

Eg. $\{x > 100 \wedge y = 0\}$ $x := x - 1$ $\{ \quad y = 0 \quad \}$

$\varphi = x > 100 \wedge y = 0 \wedge x' = x - 1 \wedge y' = y$

Preds $= \{x' > 100, y' = 0\}$

$\alpha(\varphi) = y = 0$

abstraction function