

# Static Program Analysis

Assignment Project Exam Help

Part 10 - <https://powcoder.com> abstract interpretation

Add WeChat powcoder

<http://cs.au.dk/~amoeller/spa/>

Anders Møller & Michael I. Schwartzbach  
Computer Science, Aarhus University

# Agenda

- **Collecting semantics**  
Assignment Project Exam Help
- Abstraction and concretization  
<https://powcoder.com>
- Soundness  
Add WeChat powcoder
- Optimality

# Program semantics as constraint systems

$ConcreteStates = Vars \rightarrow \mathbb{Z}$   
Assignment Project Exam Help

$\{v\} \subseteq ConcreteStates$   
<https://powcoder.com>

Add WeChat powcoder

# The semantics of expressions

$$ceval : ConcreteStates \times E \rightarrow 2^{\mathbb{Z}}$$

$$ceval(\rho, X) = \{\rho(X)\}$$

$$ceval(\rho, I) = \{I\}$$

$$ceval(\rho, \text{input}) = \mathbb{Z}$$

$$ceval(\rho, E_1 \text{ op } E_2) = \{v_1 \text{ op } v_2 \mid v_1 \in ceval(\rho, E_1) \wedge v_2 \in ceval(\rho, E_2)\}$$

<https://powcoder.com>  
Add WeChat powcoder

$$ceval(R, E) = \bigcup_{\rho \in R} ceval(\rho, E)$$

# Successors and joins

$$csucc: ConcreteStates \times Nodes \rightarrow 2^{Nodes}$$

$$csucc(R, v) = \bigcup_{\rho \in R} csucc(\rho, v)$$

Add WeChat powcoder

$$CJOIN(v) =$$

$$\{\rho \in ConcreteStates \mid \exists w \in Nodes: \rho \in \llbracket w \rrbracket \wedge v \in csucc(\rho, w)\}$$

# Semantics of statements

$$\llbracket X=E \rrbracket = \{ \rho[X \mapsto \text{ceval}(\rho, E)] \mid \rho \in \text{CJOIN}(v) \}$$

$$\llbracket \text{var } X_1, \dots, X_n \rrbracket \stackrel{\text{Assignment Project Exam Help}}{=} \{ \rho[X_1 \mapsto z_1, \dots, X_n \mapsto z_n] \mid \rho \in \text{CJOIN}(v) \wedge z_1 \in \mathbb{Z} \wedge \dots \wedge z_n \in \mathbb{Z} \}$$

<https://powcoder.com>

Add WeChat powcoder

$$\llbracket v \rrbracket = \text{CJOIN}(v)$$

# The resulting constraint system

$$\{v_1\} = cf_1(\{v_1\}, \dots, \{v_n\})$$

$$\{v_2\} = cf_2(\{v_1\}, \dots, \{v_n\})$$

: <https://powcoder.com>

$$\{v_n\} = cf_n(\{v_1\}, \dots, \{v_n\})$$

$$cf(x_1, \dots, x_n) = (cf_1(x_1, \dots, x_n), \dots, cf_n(x_1, \dots, x_n))$$

$$x = cf(x)$$

# Example

```
var x;
x = 0;
while (input) {
  x = x + 2;
}
```

## Assignment Project Exam Help

|                     | <a href="https://powcoder.com">https://powcoder.com</a> |  | solution 1  | solution 2                                  |
|---------------------|---|--|---|---|
| $\{\{entry\}\}$     |   |  | $\{\{\}\}$  | $\{\{\}\}$                                  |
| $\{\{var\ x\}\}$    |   |  | $\{\{x \mapsto z \mid z \in \mathbb{Z}\}\}$         | $\{\{x \mapsto z \mid z \in \mathbb{Z}\}\}$ |
| $\{\{x = 0\}\}$     |   |  | $\{\{x \mapsto 0\}\}$                               | $\{\{x \mapsto 0\}\}$                       |
| $\{\{input\}\}$     |   |  | $\{\{x \mapsto z \mid z \in \{0, 2, 4, \dots\}\}\}$ | $\{\{x \mapsto z \mid z \in \mathbb{Z}\}\}$ |
| $\{\{x = x + 2\}\}$ |   |  | $\{\{x \mapsto z \mid z \in \{2, 4, \dots\}\}\}$    | $\{\{x \mapsto z \mid z \in \mathbb{Z}\}\}$ |
| $\{\{exit\}\}$      |   |  | $\{\{x \mapsto z \mid z \in \{0, 2, 4, \dots\}\}\}$ | $\{\{x \mapsto z \mid z \in \mathbb{Z}\}\}$ |

the least solution



# A fixed point theorem for continuous functions

$f : L \rightarrow L$  is continuous, if  $f(\bigsqcup A) = \bigsqcup_{a \in A} f(a)$  for every  $A \subseteq L$

Assignment Project Exam Help

If  $f$  is continuous:

<https://powcoder.com>

$$\text{fix}(f) = \bigsqcup_{i \geq 0} f^i(\perp)$$

(even when  $L$  has infinite height!)

$cf$  is continuous

# Semantics vs. analysis

Assignment Project Exam Help

<https://powcoder.com>

```
var a,b,c;
a = 42;
b = 87;
if (input) {
    c = a + b;
} else {
    c = a - b;
}
```

$\llbracket b = 87 \rrbracket = \{[a \mapsto 42, b \mapsto 87, c \mapsto z] \mid z \in \mathbb{Z}\}$   
 $\llbracket c = a - b \rrbracket = \{[a \mapsto 42, b \mapsto 87, c \mapsto -45]\}$   
 $\llbracket exit \rrbracket = \{[a \mapsto 42, b \mapsto 87, c \mapsto 129], [a \mapsto 42, b \mapsto 87, c \mapsto -45]\}$

$\llbracket b = 87 \rrbracket = [a \mapsto +, b \mapsto +, c \mapsto \top]$   
 $\llbracket c = a - b \rrbracket = [a \mapsto +, b \mapsto +, c \mapsto \top]$   
 $\llbracket exit \rrbracket = [a \mapsto +, b \mapsto +, c \mapsto \top]$

# Agenda

- Collecting semantics  
Assignment Project Exam Help
- **Abstraction and concretization**  
<https://powcoder.com>
- Soundness  
Add WeChat powcoder
- Optimality

# Abstraction functions for sign analysis

$$\alpha_a : 2^{\mathbb{Z}} \rightarrow \text{Sign}$$

$$\alpha_b : 2^{\text{ConcreteStates}} \rightarrow \text{States}$$

$$\alpha_c : (2^{\text{ConcreteStates}})^n \rightarrow \text{States}^n$$

$$\alpha_a(D) = \begin{cases} \perp & \text{if } D \text{ is empty} \\ + & \text{if } D \text{ is nonempty and contains only positive integers} \\ - & \text{if } D \text{ is nonempty and contains only negative integers} \\ 0 & \text{if } D \text{ is nonempty and contains only the integer 0} \\ \top & \text{otherwise} \end{cases}$$

for any  $D \in 2^{\mathbb{Z}}$

$$\alpha_b(R) = \sigma \text{ where } \sigma(X) = \alpha_a(\{\rho(X) \mid \rho \in R\})$$

for any  $R \subseteq \text{ConcreteStates}$  and  $X \in \text{Vars}$

$$\alpha_c(R_1, \dots, R_n) = (\alpha_b(R_1), \dots, \alpha_b(R_n))$$

for any  $R_1, \dots, R_n \subseteq \text{ConcreteStates}$

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Concretization functions for sign analysis

$$\gamma_a : \text{Sign} \rightarrow 2^{\mathbb{Z}}$$

$$\gamma_b : \text{States} \rightarrow 2^{\text{ConcreteStates}}$$

$$\gamma_c : \text{States}^n \rightarrow (2^{\text{ConcreteStates}})^n$$

$$\gamma_a(s) = \begin{cases} \emptyset & \text{if } s = \perp \\ \{1, 2, 3, \dots\} & \text{if } s = + \\ \{-1, -2, -3, \dots\} & \text{if } s = - \\ \{0\} & \text{if } s = 0 \\ \mathbb{Z} & \text{if } s = \top \end{cases}$$

for any  $s \in \text{Sign}$

$$\gamma_b(\sigma) = \{\rho \in \text{ConcreteStates} \mid \rho(X) \in \gamma_a(\sigma(X)) \text{ for all } X \in \text{Vars}\}$$

for any  $\sigma \in \text{States}$

$$\gamma_c(\sigma_1, \dots, \sigma_n) = (\gamma_b(\sigma_1), \dots, \gamma_b(\sigma_n))$$

for any  $(\sigma_1, \dots, \sigma_n) \in \text{States}^n$

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Galois connections

The pair of monotone functions,  $\alpha$  and  $\gamma$ , is called a *Galois connection* if

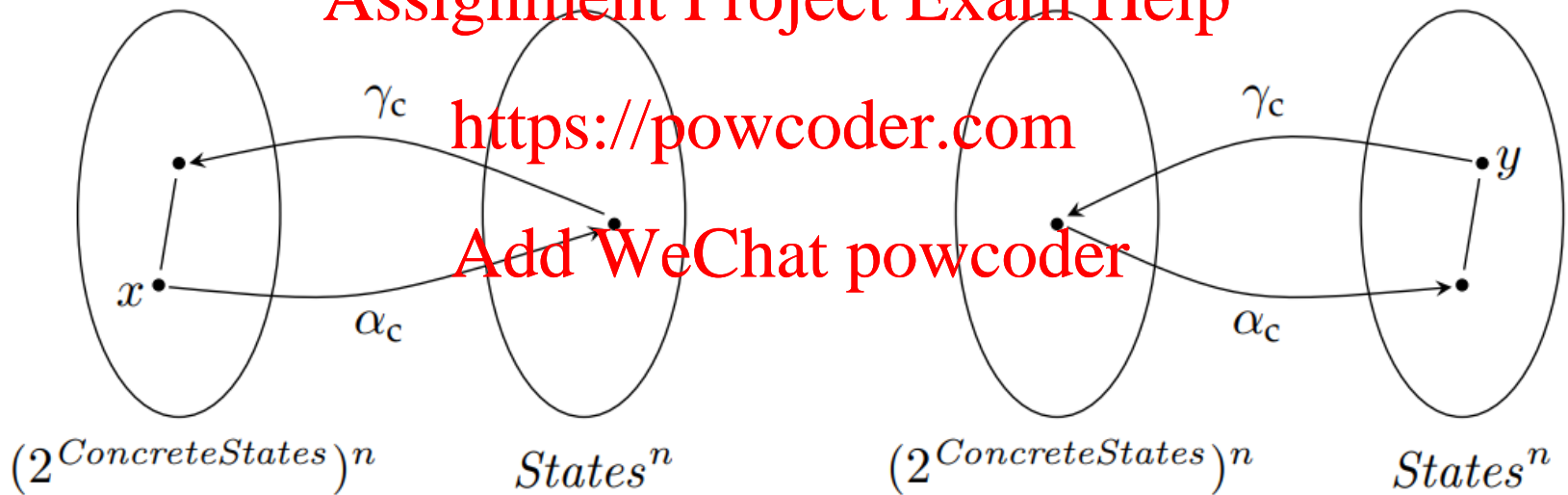
$\gamma \circ \alpha$  is extensive

$\alpha \circ \gamma$  is reductive

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



# Galois connections

For Galois connections, the concretization function uniquely determines the abstraction function and vice versa:

$$\gamma(y) = \bigsqcup_{x \in L_1 \text{ where } \alpha(x) \sqsubseteq y} x$$

Assignment Project Exam Help

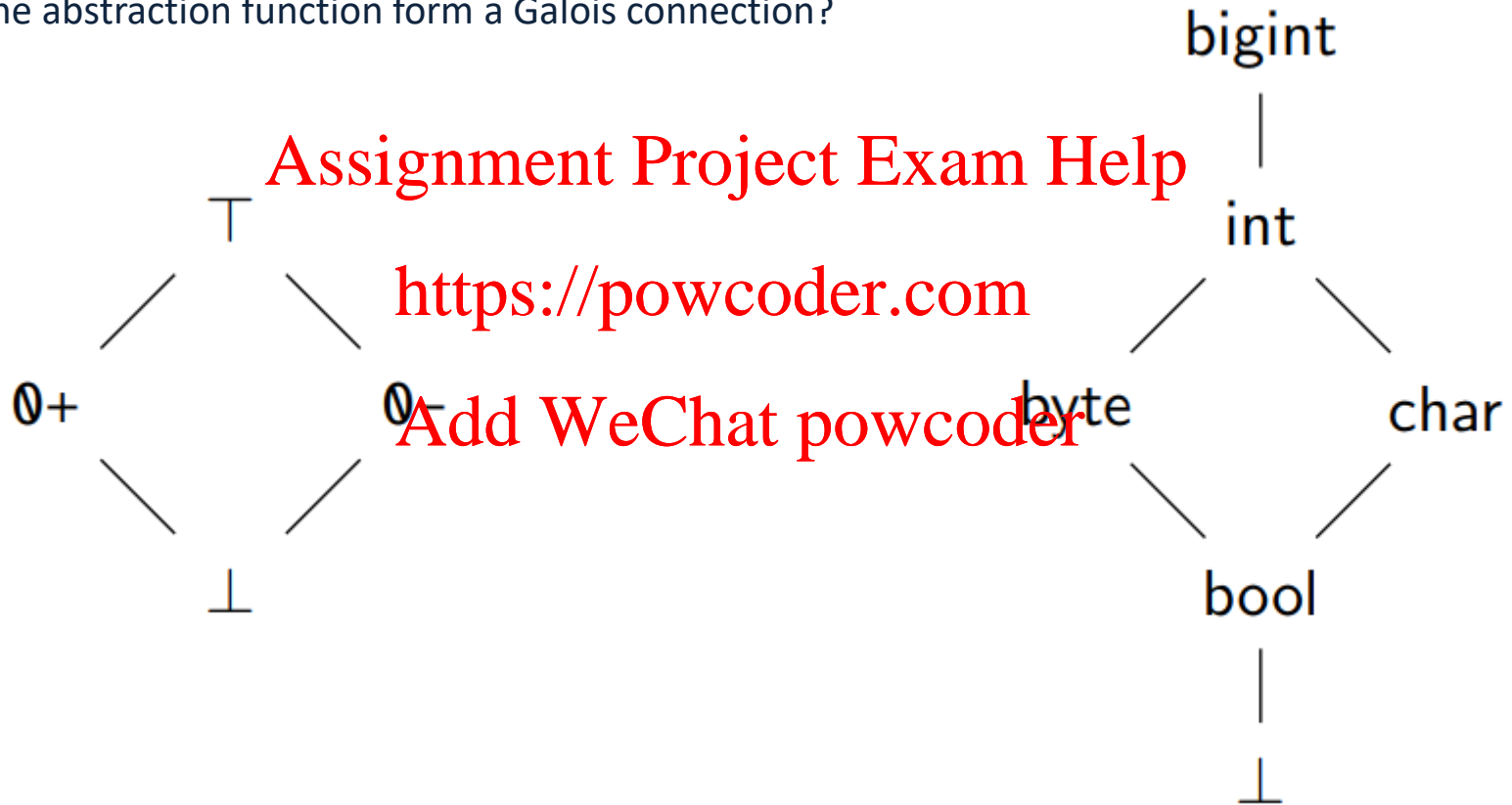
<https://powcoder.com>

Add WeChat powcoder

$$\alpha(x) = \bigsqcap_{y \in L_2 \text{ where } x \sqsubseteq \gamma(y)} y$$

# Galois connections

For each of these two lattices, given the “obvious” concretization function, is there an abstraction function such that the concretization function and the abstraction function form a Galois connection?



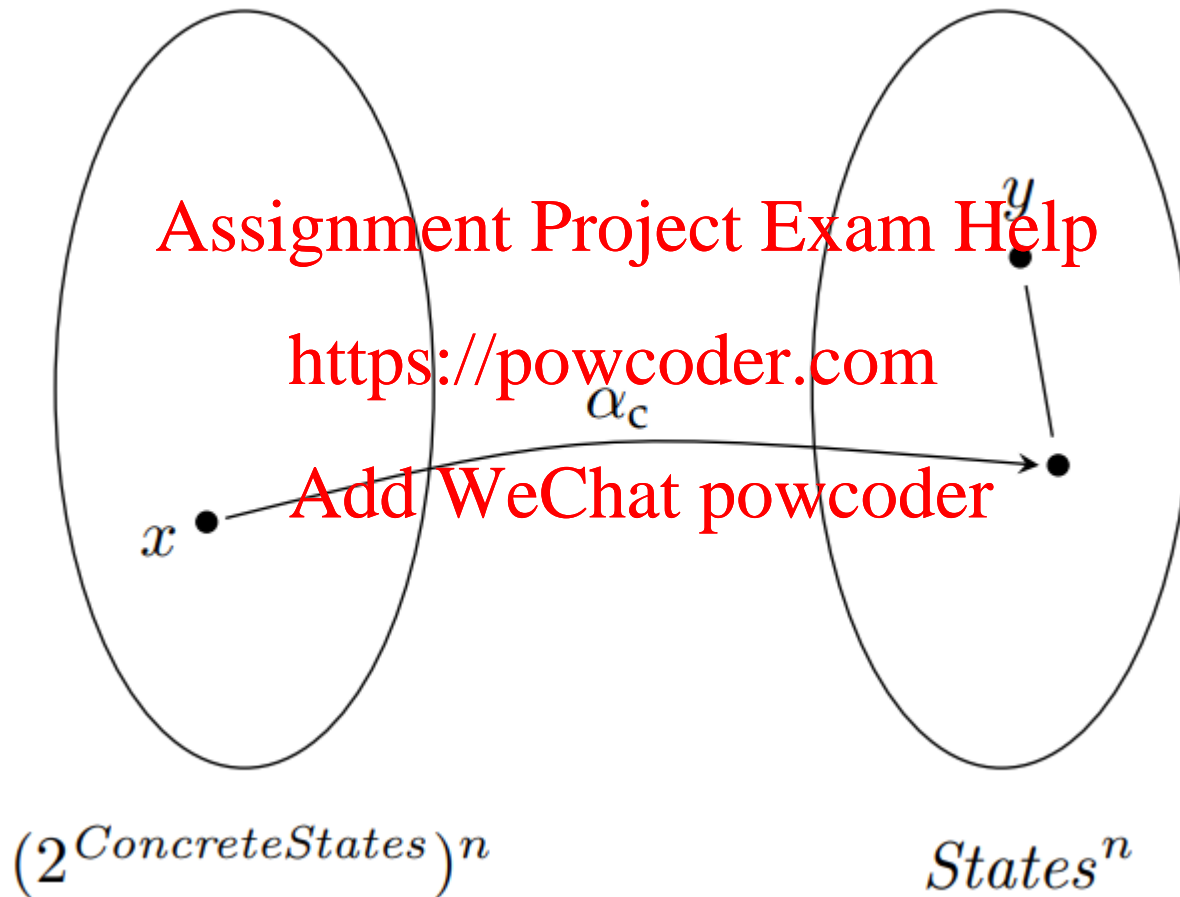


# Agenda

- Collecting semantics  
Assignment Project Exam Help
- Abstraction and concretization  
<https://powcoder.com>
- **Soundness**  
Add WeChat powcoder
- Optimality

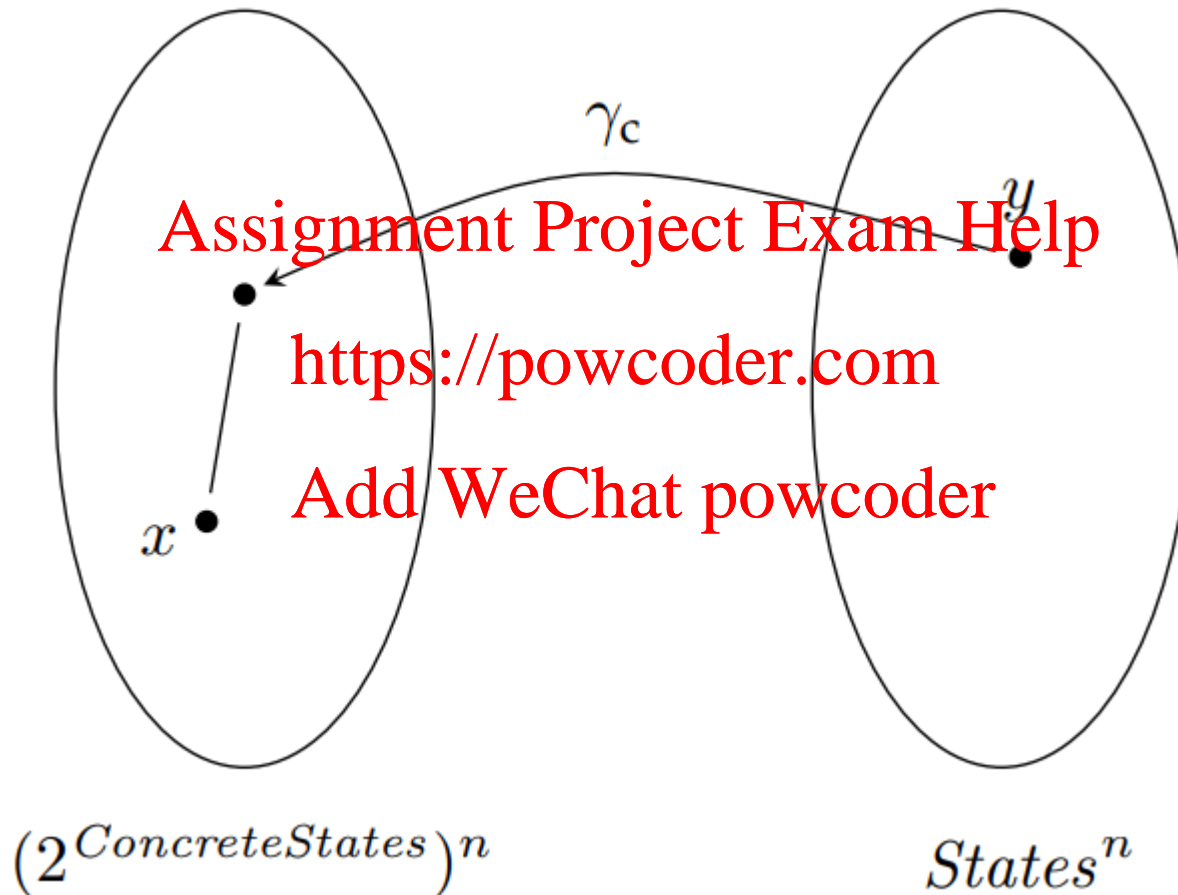
# Soundness

$$\alpha(x) \sqsubseteq y$$



# Soundness

$$x \sqsubseteq \gamma(y)$$



# Safe approximations

$$\alpha_a(\text{ceval}(R, E)) \sqsubseteq \text{eval}(\alpha_b(R), E)$$

Assignment Project Exam Help

$\text{csucc}(R, v) \subseteq \text{succ}(v)$  for any  $R \sqsubseteq \text{ConcreteStates}$

Add WeChat powcoder

$$\alpha_b(\text{CJOIN}(v)) \sqsubseteq \text{JOIN}(v)$$

if  $\alpha_b(\llbracket w \rrbracket) \sqsubseteq \llbracket w \rrbracket$  for all  $w \in \text{Nodes}$ .

# Safe approximations

if  $v$  represents an assignment statement  $X = E$  :

$$cf_v(\{v_1\}, \dots, \{v_n\}) = \{\rho[X \mapsto z] \mid \rho \in CJOIN(v) \wedge z \in ceval(\rho, E)\}$$

$$af_v(\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket) = \sigma[X \mapsto eval(\sigma, E)] \text{ where } \sigma \in JOIN(v)$$

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

$$\alpha_b(cf_v(R_1, \dots, R_n)) \sqsubseteq af_v(\alpha_b(R_1), \dots, \alpha_b(R_n))$$

# The two constraint systems

$$cf(\{v_1\}, \dots, \{v_n\}) = ((cf_{v_1}(\{v_1\}, \dots, \{v_n\}), \dots, cf_{v_n}(\{v_1\}, \dots, \{v_n\})))$$

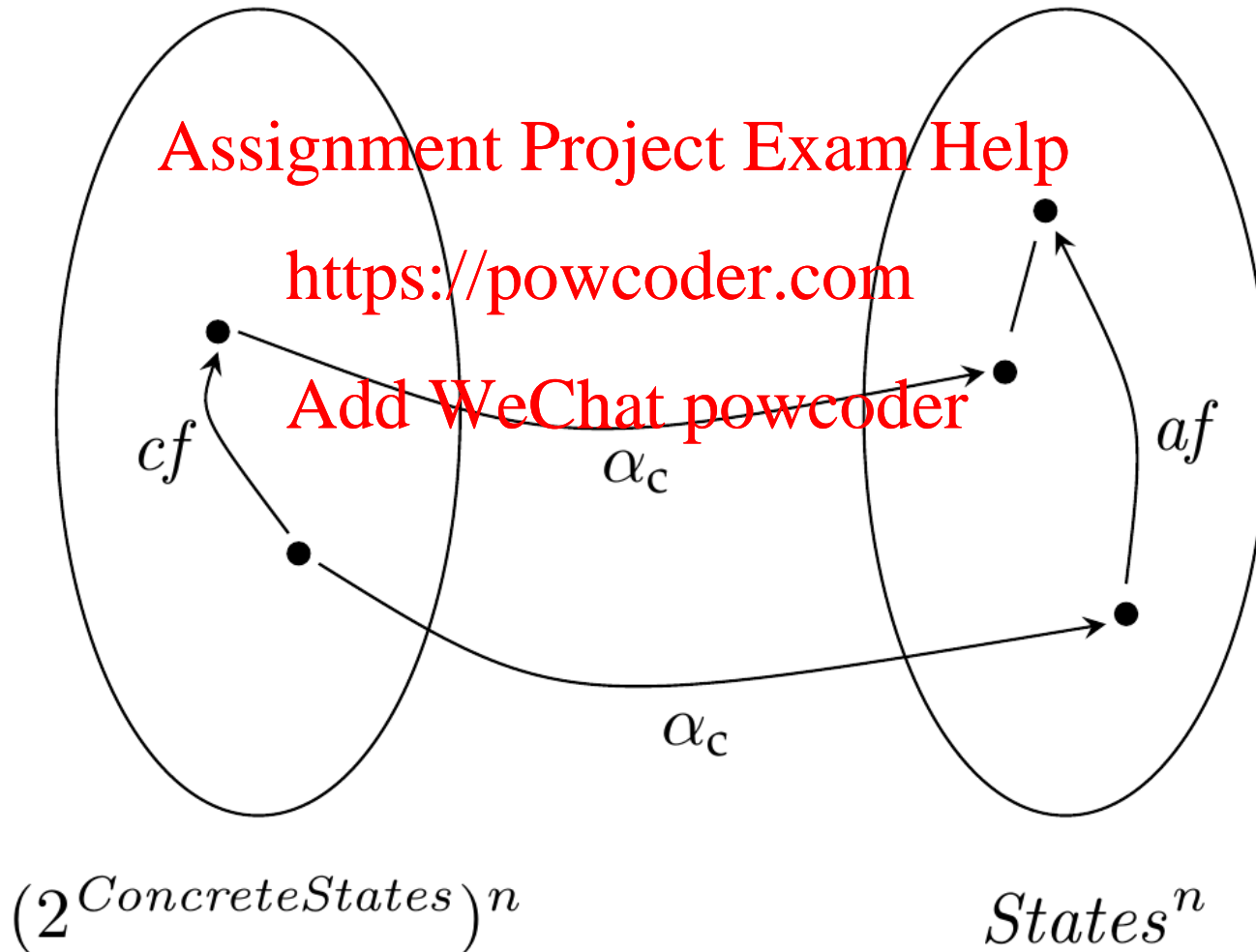
Assignment Project Exam Help

$$af(\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket) = ((af_{v_1}(\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket), \dots, af_{v_n}(\llbracket v_1 \rrbracket, \dots, \llbracket v_n \rrbracket)))$$

Add WeChat powcoder

# Safe approximations

$$\alpha_c(cf(R_1, \dots, R_n)) \sqsubseteq af(\alpha_c(R_1, \dots, R_n))$$



# The soundness theorem

Assignment Project Exam Help  
<https://powcoder.com>  
Let  $L_1$  and  $L_2$  be lattices where  $L_2$  has finite height, assume  $\alpha: L_1 \rightarrow L_2$  and  $\gamma: L_2 \rightarrow L_1$  form a Galois connection,  $cf: L_1 \rightarrow L_1$  is continuous, and  $af: L_2 \rightarrow L_2$  is monotone.

Add WeChat powcoder  
If  $af$  is a sound abstraction of  $cf$ , then  $\alpha(\text{fix}(cf)) \sqsubseteq \text{fix}(af)$ .



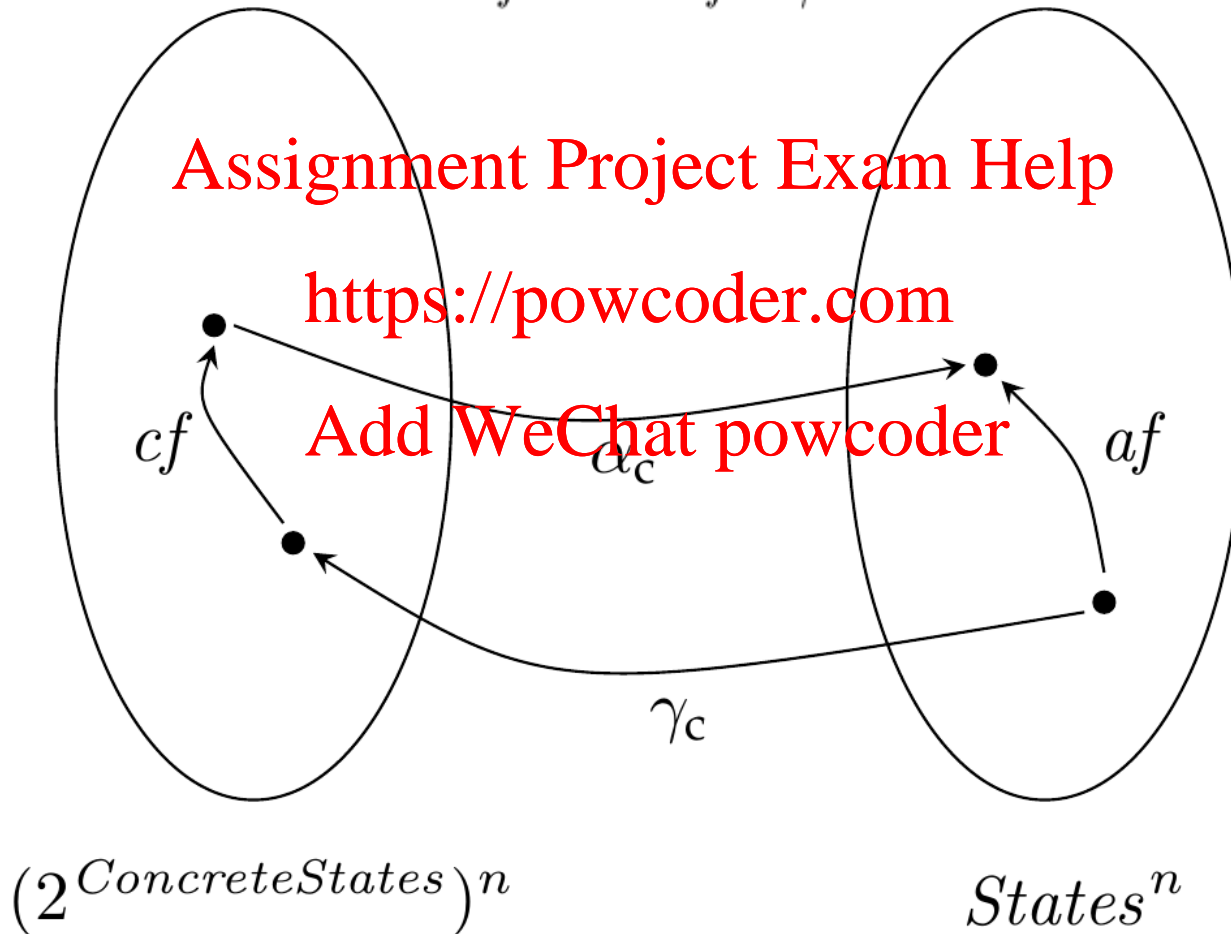
# Agenda

- Collecting semantics  
Assignment Project Exam Help
- Abstraction and concretization  
<https://powcoder.com>
- Soundness  
Add WeChat powcoder
- **Optimality**

# Optimal approximations

$af$  is an *optimal* approximation of  $cf$  if

$$af = \alpha \circ cf \circ \gamma$$



# Optimal approximations in sign analysis?

$\hat{*}$  is optimal:

$$s_1 \hat{*} s_2 = \alpha_a(\gamma_a(s_1) \cdot \gamma_a(s_2))$$

*eval* is not optimal:

$$\sigma(\mathbf{x}) = \top$$

$$eval(\sigma, \mathbf{x} - \mathbf{x}) = \top$$

$$\alpha_b(ceval(\gamma_b(\sigma), \mathbf{x} - \mathbf{x})) = \mathbf{0}$$

Even if we could make *eval* optimal, the analysis result is not always optimal:

```
x = input;
```

```
y = x;
```

```
z = x - y;
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder